15

CUARTO COLOQUIO LATINOAMERICANO DE ALGEBRA

Mendoza, Argentina

CUARTO COLOQUIO LATINOAMERICANO DE ALGEBRA - 1984.

EXTENSIONES CUATERNIONICAS

FERNANDO RODRÍGUEZ VILLEGAS

Con el número dos nace la pena.
L. Marechal.

En general resulta relativamente difícil dar ejemplos de extensiones Galoisianas de cuerpos cuyo grupo de Galois sea el grupo cuaterniónico $\mathbb{H}$; en comparación, por ejemplo, con el mismo problema planteado para D_4: grupo de simetrías del cuadrado.

En los apuntes del curso de Teoría de Galois del Dr. Gentile se encuentra un ejemplo extraído de un artículo de Martinet (1) y mi intención es generalizar el procedimiento ahí utilizado, a cierta familia de grupos, que incluye a $\mathbb{H}$ y D_4 .

En función de ciertos parámetros, se da la forma general de las extensiones de Galois cuyo grupo pertenece a dicha familia; luego, en términos de una forma cuadrática sobre $\mathbb{Z}/2\mathbb{Z}$, se dan condiciones suficientes sobre los parámetros para que el grupo sea el requerido.

1. Los dos únicos grupos no conmutativos de orden 8: $\mathbb{H}$ y D_4 verifican ambos una sucesión exacta del siguiente tipo:

1.1. $0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{i} G \xrightarrow{\pi} (\mathbb{Z}/2\mathbb{Z})^n \to 0$

con $n = 2$.

Consideremos, entonces, la familia $\mathcal{G}$ de grupos G que

verifiquen esta sucesión para algún $n \in \mathbf{N}$.
Sea ahora L/k una extensión Galoisiana de cuerpos con $2 \neq 0$, tal que:

$Gal(L/k) \simeq G \in \mathbf{G}$

La sucesión 1.1. implica, por el teorema de Galois, que:

1.2.
$$\begin{array}{l} L = F(\sqrt{\alpha}) \qquad \alpha \in \dot{F} \setminus \dot{F}2 \\ \quad | \\ \quad F \\ \quad | \\ \quad k \end{array}$$

Donde $Gal(L/F) \simeq \mathbb{Z}/2\mathbb{Z}$ y $Gal(F/k) \simeq (\mathbb{Z}/2\mathbb{Z})^n$
De la siguiente proposición obtenemos lo necesario sobre la extensión F/k. Digamos primero que interpretaremos al grupo $\dot{k}/\dot{k}^2$, de clases de cuadrados de k como un $\mathbb{Z}/2\mathbb{Z}$ espacio vectorial y que dado $x \in \dot{k}$, (x) notará su clase en $\dot{k}/\dot{k}^2$.

2.3. PROPOSICION:

(1) $K(\sqrt{x_1},\ldots,\sqrt{x_n}) = k(\sqrt{y_1},\ldots\sqrt{y_n})$ sii $\{(x_1),\ldots,(x_n)\}$ y $\{(y_1),\ldots,(y_n)\}$ generan el mismo subespacio $V \subseteq \dot{k}/\dot{k}^2$. Tiene sentido, entonces, notar con $k(\sqrt{v})$ a esa extensión.

(ii) $k(\sqrt{V})/k$ es de Galois con:
$Gal(k(\sqrt{V})/k) \simeq (\mathbb{Z}/2\mathbb{Z})^n$; $n = \dim_{\mathbb{Z}/2\mathbb{Z}}(V)$

(iii) $(k(\sqrt{V})^2 \cap \dot{k})/\dot{k}^2 = V$

(iv) Si F/k es una extensión Galoisiana con $Gal(F/k) \simeq (\mathbb{Z}/2\mathbb{Z})^n$ entonces $\exists$ V subespacio de dimensión n de $\dot{k}/\dot{k}^2$, tal que $F = k(\sqrt{V})$.

Podemos ahora afirmar que $\exists$ $(x1), \ldots, (xn) \in \dot{k}/\dot{k}^2$ linealmente independientes sobre $\mathbf{Z}/2\mathbf{Z}$ tal que $F = k(\sqrt{x1},\ldots,\sqrt{xn})$
Obtenemos la siguiente versión de 1.2.

1.4.
$$\begin{array}{ll} L = F(\sqrt{\alpha}) & \alpha \in \dot{F} \setminus \dot{F}^2 \\ \Big| & \\ F = K(\sqrt{x1},\ldots,\sqrt{xn}) & x1,\ldots,xn \in \dot{k} \setminus \dot{k}^2 \\ \Big| & \\ K & \end{array}$$

1.5. LEMA:

Sea F/k de Galois con $gal(F/k) = G$ y $\alpha \in \dot{F} \setminus \dot{F}^2$.
Entonces: $F(\sqrt{\alpha})\ k$ es de Galois sii $\alpha.\alpha^{\sigma} \in \dot{F}^2$, $\forall\ \sigma \in G$.

Tenemos entonces las condiciones necesarias y suficientes, sobre los parámetros $x1,\ldots,xn,\alpha$ para que L/k sea de Galois. $(L = F(\sqrt{\alpha}), \alpha \in \dot{F} \setminus \dot{F}^2)$ y $Gal\ (L/k) \in \mathbf{G}$.

2. Supongamos tener, entonces, $(x1),\ldots,(xn) \in \dot{k}/\dot{k}^2$ linealmente independientes y consideremos $\alpha \in \dot{F} \setminus \dot{F}^2$ de la siguiente forma

$$\alpha = \alpha_1 \cdot \alpha_2 , \ldots , \alpha_n$$

con $\alpha_i \in k(\sqrt{x_i})$ y $\alpha_i \cdot \alpha_i^{\sigma_i} \in \dot{F}^2$

donde $\sigma_i \in Gal(F/k)$ definido por

$$\sqrt{x_j}^{\sigma_i} = (-1)^{\delta_{ij}} \sqrt{x_j}$$

Es fácil verificar que $\alpha \cdot \alpha^{\sigma} \in \dot{F}^2$, $\forall\ \sigma \in Gal(F/k)$; es decir, satisface las condiciones requeridas en 1.5.

Como $\alpha_i \cdot \alpha_i^{\sigma_i} \in \dot{k}$ y por hipótesis también pertenece a F podemos aplicar 1.3.(iii) obteniendo:

$$\alpha_i \cdot \alpha_i^{\sigma_i} = x_1^{\eta_{i1}} \cdot x_2^{\eta_{i2}}, \ldots, x_n^{\eta_{in}} \cdot c^2$$

$c \in \dot{k}$ y $\eta_{ij} \in \mathbb{Z}/2\mathbb{Z}$

Ahora si $\tilde{\sigma} \in Gal(L/k)$ es tal que

$$\pi(\tilde{\sigma}) = \sigma = \sigma_1^{\varepsilon_1}, \ldots, \sigma_n^{\varepsilon_n}$$

con $\varepsilon_i \in \mathbb{Z}/2\mathbb{Z}$ no todos nulos, se demuestra que:

$o(\tilde{\sigma}) = 2^{1+q(\sigma)}$, orden del elemento $\tilde{\sigma}$

Donde $q(\sigma) = \sum_{i,j} \eta_{ij} \cdot \varepsilon_i \cdot \varepsilon_j$

$q = (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$

q es una forma cuadrática sobre $\mathbb{Z}/2\mathbb{Z}$

3. Se puede demostrar también que q no sólo describe el orden de los elementos $\tilde{\sigma} \in Gal(L/k)$ sino que además caracteriza a dicho grupo, en el sentido siguiente:

3.1. PROPOSICION:

(i) Sea $G \in \mathbf{G}$, (es decir $0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\mu} G \xrightarrow{\pi} (\mathbb{Z}/2\mathbb{Z})^n \to 0$ es exacta) entonces $\exists !$ q forma cuadrática sobre $\mathbb{Z}/2\mathbb{Z}$ tal que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} x & G & \xrightarrow{\pi} & (\mathbb{Z}/2\mathbb{Z})^n \\ \downarrow & \downarrow & & \downarrow q \\ x^2 & G & \xleftarrow{u} & (\mathbb{Z}/2\mathbb{Z}) \end{array}$$

(ii) Dada $q:(\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$ forma cuadrática existe $G \in \mathbf{G}$ tal que G,q verifican el diagrama anterior.

(iii) $G_1 \in \mathbf{G}$ de forma q_1 , $G_2 \in \mathbf{G}$ de forma q_2 son isomorfos sii los espacios cuadráticos

$((\mathbb{Z}/2\mathbb{Z})^n, q_1)$ y $((\mathbb{Z}/2\mathbb{Z})^n, q_2)$ son isométricos.

4. APLICACION.

$n = 2$, $k = \mathbb{Q}$, $x_1 = 2$, $x_2 = 3$

$\alpha_1 = 2 + \sqrt{2}$, $\alpha_2 = 3 + \sqrt{3}$

$$\sigma_1: \begin{matrix} \sqrt{2} & -\sqrt{2} \\ \sqrt{3} & \sqrt{3} \end{matrix} \qquad \sigma_2: \begin{matrix} \sqrt{2} & \sqrt{2} \\ \sqrt{3} & -\sqrt{3} \end{matrix}$$

Deducimos que:

$$\alpha_1 \cdot \alpha_1^{\sigma_1} = 2 \quad , \quad \alpha_2 \cdot \alpha_2^{\sigma_2} = 2.3 \quad , \quad \therefore (\eta_{ij}) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

y entonces:

$$q(\sigma_1) = (1,0)\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1$$

$$q(\sigma_2) = (0,1)\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = 1$$

$$q(\sigma, \sigma_2) = (1,1)\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1$$

Por lo tanto existen 6 elementos de orden 4 en Gal(L/k) distintos y como este grupo es de orden 8 , es necesariamente H .

CONCLUSION:

$$\begin{array}{l} L = F(\sqrt{(2+\sqrt{2}).(3+\sqrt{3})}) \\ \quad\quad | \\ F = \mathbb{Q}(\sqrt{2},\sqrt{3}) \ . \\ \quad\quad | \\ \quad \mathbb{Q} \end{array}$$

$$Gal(L/\mathbb{Q}) \simeq H \quad .$$

REFERENCIAS.

[1] Jacques Martinete, Modules sur l'algebre de groupe quaternionique Annales Scientifiques de L'Ecole Normale Superieure, 4 serie, t. 4, Fac. 3, 1971.

Estos trabajos fueron preparados -para su posterior impresión- en el Centro Latinoamericano de Matemática e Informática por Carlos H. Medrano.