SOLUBILIDAD DE CIERTOS GRUPOS DE MATRICES SOBRE ANILLOS

Por
Oswaldo Lezama
Luis Guillermo Sepulveda Uribe
Departamento de Matemáticas y Estadística
Universidad Nacional
Bogotá, D. E., Colombia

RESUMEN

Se generalizan algunos resultados encontrados en [3] sobre solubilidad y conteo de grupos matriciales sobre campos a anillos asociativos sometidos a restricciones débiles.

Se calcula además el orden del centro del grupo $UT_n^m(A)$, $1 \leq m \leq n$, A finito.

1. INTRODUCCION.

Sea A un anillo con unidad (no necesariamente conmutativo), $M_n(A)$ el anillo de matrices cuadradas de orden $n \geq 2$ sobre A y $GL_n(A)$ el grupo lineal general de orden n conformado por las matrices inversibles de $M_n(A)$.

En [7] fueron estudiadas algunas propiedades de los siguientes subgrupos de $GL_n(A)$:

- $D_n(A)$, el grupo de matrices diagonales.

- $T_n(A)$, el grupo triangular superior, bajo la hipótesis de que A sea un anillo finito de Dedekind, e.d., para cualesquiera $x, y \in A$ se cumple $xy = 1 \Rightarrow yx = 1$.

- $UT_n(A)$, el grupo unitriangular superior.

- $UT_n^m(A)$, $1 \leq m \leq n$ constituido por las matrices unitriangulares superiores, que tienen $m-1$ diagonales consecutivas nulas por encima de la diagonal principal.

- $E_n(A)$ el grupo elemental, generado por todas las elementales de la forma:

$$T_{ij}(\alpha) = E + \alpha \cdot E_{ij}, \quad \alpha \in A,\ i \neq j,$$

donde

$$E_{ij} = \begin{array}{c} \\ \\ \\ j \\ \\ \end{array} \begin{array}{c} \begin{array}{c} \\ \\ i \\ \\ \\ \end{array} \\ \begin{pmatrix} & \vdots & \\ \cdots & 1 & \cdots \\ & \vdots & \end{pmatrix} \end{array}$$

es decir, E_{ij} coincide con la matriz nula salvo en la entrada (i,j).

Siendo K un cuerpo o un anillo conmutativo, $SL_n(K)$ es el grupo especial lineal, conformado por las matrices de determinante 1.

Al igual que en [7] tratamos aquí de generalizar algunas propiedades consignadas en [3] en forma de ejercicios propuestos. En particular se determina la solubilidad de los grupos enunciados antes, para algunos casos especiales de anillos. Además se calculan los órdenes de dichos grupos y de sus centros en el caso de ciertos anillos finitos.

Una matriz diagonal inversible será denotada por

$$D(\beta_1, \ldots, \beta_n)\ \beta_k \in A^*, \quad 1 \leq k \leq n.$$

El conmutador de un par de elementos a,b de un grupo G es

$$[a,b] = a^{-1}b^{-1}ab.$$

2. CONTEO DE ELEMENTOS

Determinamos los órdenes de los grupos introducidos en [7] parágrafo 2 para algunos casos particulares. Varias de las afirmaciones aquí presentadas aparecen como ejercicios propuestos en [3]. En el presente parágrafo salvo, que se advierta lo contrario, A denota un anillo finito y $n \geq 2$.

El número de elementos de un conjunto S será denotado por $|S|$.

2.1 AFIRMACION. Sea $C(\mathbb{A})$ el centro del anillo $\mathbb{A}$. Entonces

$$|\text{Centro de } M_n(\mathbb{A})| = |C(\mathbb{A})|$$
$$|M_n(\mathbb{A})| = |\mathbb{A}|^{n^2}$$

DEMOSTRACION. Es consecuencia de la proposición 1.2 de [7].

2.2 TEOREMA. [3] Sea K un campo de orden $q = p^m$ con p primo y $m \geq 1$. Entonces

$$|GL_n(K)| = \prod_{k=0}^{n-1} (q^n - q^k)$$

DEMOSTRACION. Sea A una matriz de $GL_n(K)$. Recuerde que A es inversible si y sólo si las filas de A son vectores linealmente independientes de K^n. Denotemos dichas filas por $A_1, \ldots, A_n$. Evidentemente $A_1 \neq 0$. Así pues tenemos $q^n - 1$ posibilidades para A_1. Para A_2 tendriamos q^n posibilidades, pero, en vista de la independencia A_2 no debe ser múltiplo de A_1. Así entonces a cada una de las q^n posibilidades restamos q posibilidades ya que K tiene q elementos.

En total A_2 presenta $q^n - q$ escogencias. Para A_3 debemos restar q^2 valores de q^n, ya que A_3 no puede ser combinación lineal de A_1 y A_2.

De esta forma encontramos el orden de $GL_n(K)$ como el producto de las posibilidades encontradas.

2.3 PROPOSICION. [3] Sea p primo y $m \geq 1$.

$$|GL_n(\mathbb{Z}_{p^m})| = \prod_{k=0}^{n-1} (p^{mn} - p^{mn-m+k})$$

DEMOSTRACION. Nótese en primer lugar que siendo $\mathbb{A}_1 \to \mathbb{A}_2$ un homomorfismo sobreyectivo de anillos se inducen de manera natural los homomorfismos

$$\mathbb{A}_1^* \to \mathbb{A}_2^*, \quad M_n(\mathbb{A}_1) \to M_n(\mathbb{A}_2).$$

de grupos y anillos respectivamente, donde el segundo de ellos es también sobreyectivo. ($\mathbb{A}^*$ denota el grupo de elementos inversibles del anillo $\mathbb{A}$.)

Consideremos en particular el homomorfismo natural de anillos.

$$\mathbb{Z}_{p^m} \to \mathbb{Z}_p, \quad \bar{k} = k + < p^m >, k \in \mathbb{Z}$$
$$\bar{k} \mapsto \tilde{k}, \quad \tilde{k} = k + < p >.$$

Se induce entonces el homorfismo natural de grupos

$$GL_n(\mathbb{Z}_{p^m}) \xrightarrow{j} GL_n(\mathbb{Z}_p),$$
$$\overline{A} = (\overline{a}_{ij}) \mapsto \tilde{A} = (\tilde{a}_{ij}).$$

Comprobemos que j es sobreyectivo.Según 3.1 de [7], cada elemento $\tilde{A} \in GL_n(\mathbb{Z}_p)$ es producto de elementales y una matriz diagonal

$$D(\beta) = E + (\beta - 1)E_{nn}, \quad 1 \leq \beta \leq p-1.$$

Evidentemente cada elemental de $GL_n(\mathbb{Z}_p)$ es imagen mediante j de una elemental de $GL_n(\mathbb{Z}_{p^m})$. Basta entonces encontrar una preimagen para $D(\beta)$.

Para cada $m \geq 1$ la matriz.

$$\overline{A} = \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & \ddots & & \\ & & & p+1 & p(p-\beta) \\ 0 & & & p & (p-1)(p-\beta) \end{pmatrix} \in GL_n(\mathbb{Z}_{p^m}).$$

En efecto, $\det \overline{A} = (p+1)(p-1)(p-\beta) - p^2(p-\beta) = \beta - p$, donde $(\beta - p, p^m) = 1$, es decir, $\det\overline{A} \in \mathbb{Z}_{p^m}^*$. Claramente $J(\overline{A}) = D(\beta)$.

Por el teorema fundamental de homomorfismo

$$|GL_n(\mathbb{Z}_{p^m})| = |GL_n(\mathbb{Z}_p)| \cdot |N(j)|$$
$$N(j) = \{\overline{X} = (\overline{x}_{ij} \in GL_n(\mathbb{Z}_{p^m}) \mid x_{ii} \equiv 1(p),\ x_{ii} \equiv 0(p),\ i \neq j\}$$

Notemos que cada matriz $\overline{X} = (\overline{x}_{ij}) \in M_n(\mathbb{Z}_{p^m})$ que cumpla las dos condiciones anteriores es inversible.

La primera condición indica que $\overline{x}_{ii} \in \mathbb{Z}_{p^m}^*, 1 \leq i \leq n$.

Ahora, sea $\overline{B} =: (\overline{b}_{ij}) =: \overline{X}D(\overline{x}_{11}^{-1}, \ldots, \overline{x}_{nn}^{-1})$.

Entonces, $b_{ii} = 1, 1 \leq i \leq n$, $b_{ij} \equiv 0(p)$, $i \neq j$. Es decir $\overline{B}$ es de la forma $\overline{B} = E + \overline{C}$ con $\overline{C} \in M_n(< p >) = \mathrm{Rad}(M_n(\mathbb{Z}_{p^m}))$, el radical de Jacobson ([2],[4]).

Resulta así que $\overline{B}$ es inversible y en consecuencia $\overline{X}$ es también inversible.

La observación anterior permite calcular el orden del núcleo de j. Tenemos

$$|N(j)| = (\text{número de soluciones de } a \equiv 1(p))^{n^2}$$
$$= (\text{número de soluciones de } a \equiv o(p))^{n(n-1)}$$
$$|N(j)| = (p^{m-1})^{n^2}(p^{m-1})^{n(n-1)} = (p^{mn-n})^n.$$

Aplicando el teorema 2.2, encontramos

$$\begin{aligned}|GL_n(\mathbb{Z}_{p^m})| &= (\prod_{k=0}^{n-1}(p^n - p^k))(p^{mn-n})^n \\ &= (p^n - p^0)(p^{mn-n})(p^n - p)(p^{mn-n})\cdots(p^n - p^{n-1})(p^{mn-n} \\ &= (p^{mn} - p^{mn-n+0})(p^{mn} - p^{mn-n+1})\cdots(p^{mn} - p^{mn-n+(n-1)}) \\ &= \prod_{k=0}^{n-1}(p^{mn} - p^{mn-n+k}).\end{aligned}$$

La proposición anterior permite calcular el orden de $GL_n(\mathbb{Z}_m)$ para cada $(m \geq 2)$. En efecto sea

(1) $$m = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$$

La descomposición prima de m. Del teorema chino de residuos ([5]) resulta el isomorfisomo de anillos

(2) $$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{\alpha_r}}$$

y éste a su vez induce el isomorfismo natural de grupos.

$$GL_n(\mathbb{Z}_m) \cong GL_n(\mathbb{Z}_{p_1^{\alpha_1}}) \oplus \cdots \oplus GL_n(\mathbb{Z}_{p_r^{\alpha_r}})$$

Hemos probado el siguiente resultado.

2.4 COROLARIO. Sea $m \geq 2$ con desomposición prima (1). Entonces

$$|GL_n(\mathbb{Z}_m)| = \prod_{j=1}^{r}\prod_{k=0}^{n-1}(p_j^{\alpha_j n} - p_j^{\alpha_j n - n + k})$$

2.5 COROLARIO. [3]

(i) Sea K un campo de orden $q = p^m$ con p primo y $m \geq 1$. Entonces,

$$|SL_n(K)| = \frac{1}{q-1}\prod_{k=0}^{n-1}(q^n - q^k).$$

(ii) $|SL_n(\mathbb{Z}p^m)| = \frac{1}{p^{n-1}(p-1)}\prod_{k=0}^{n-1}(p^{mn} - p^{mn-n+k})$, $m \geq 1$

(iii) Sea $m \geq 2$ con descomposición prima (1), entonces

$$|SL_n(\mathbb{Z}_m)| = \frac{1}{\prod_{j=1}^{r} p_j^{\alpha_j - 1}(p_j - 1)}\prod_{j=1}^{r}\prod_{k=0}^{n-1}(p_j^{\alpha_j n} - p_j^{\alpha_j n - n + k}).$$

DEMOSTRACION. En los tres casos basta considerar la función determinante y tener en cuenta que

(i) $|K^*| = q - 1$

(ii) $\mathbf{Z}^*_{p^m} = \{x \mid 1 \leq x < p^m,\ p \nmid x\}$,

(iii) (2) induce el isomorfismo de grupos

$$\mathbf{Z}^*_m \cong \mathbf{Z}^*_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbf{Z}^*_{p_r^{\alpha_r}}$$

y por lo tanto

$$|\mathbf{Z}^*_m| = \prod_{j=1}^{r} |\mathbf{Z}^*_{p_j^{\alpha_j}}| = \prod_{j=1}^{r} p_j^{\alpha_j - 1}(p_j - 1).$$

2.6 TEOREMA. Sea A un anillo. Entonces

$$|D_n(A)| = |A^*|^n$$

DEMOSTRACION. Es consecuencia de corolario 2.2 de [7].

2.7 TEOREMA. Sea A un anillo. Entonces

$$|T_n(A)| = |A^*|^n |A|^{\frac{n(n-1)}{2}}$$

DEMOSTRACION. Como advertimos al comienzo de este parágrafo A se supone finito y por lo tanto noeteriano. Según [6] A es finito de Dedekind. Resta aplicar la proposición 2.3 de [7].

2.8 TEOREMA. Sea A un anillo. Entonces para $1 \leq m \leq 2$

$$|UT^m_n(A)| = |A|^{\frac{(n-m+1)(n-m)}{2}}$$

DEMOSTRACION. Basta contar el número de entradas del ángulo superior derecho de $UT^m_n(A)$:

$$UT^m_n(A) = \begin{pmatrix} 1 & & & n-m \\ & \ddots & & \\ & & \ddots & \leftarrow \frac{(n-m)(n-m+1)}{2} \\ & & & n-m \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

Aplicando los resultados del parágrafo 4 en [7] se obtienen inmediatamente las siguientes conclusiones.

2.9 TEOREMA. Sea A un anillo, $C(A)$ su centro y $Z(A^*)$ el centro del grupo A^*. Entonces

(i) $|Z(GL_n(A))| = |C(A)^*|$

(ii) $|Z(D_n(A))| = |Z(A^*)|^n$

(iii) Si en A existe $\alpha_0 \in A^*$ tal que $(\alpha_0 - 1) \in A^*$ o bien $|A^*| \geq 2$ y A^* no posee divisores de cero, entonces

$$|Z(T_n(A))| = |C(A)^*|$$

(iv) Si $m > \frac{n}{2}$

$$|Z(UT_n^m(A))| = |A|^{\frac{(n-m+1)(n-m)}{2}}$$

Si $m \leq \frac{n+1}{3}$

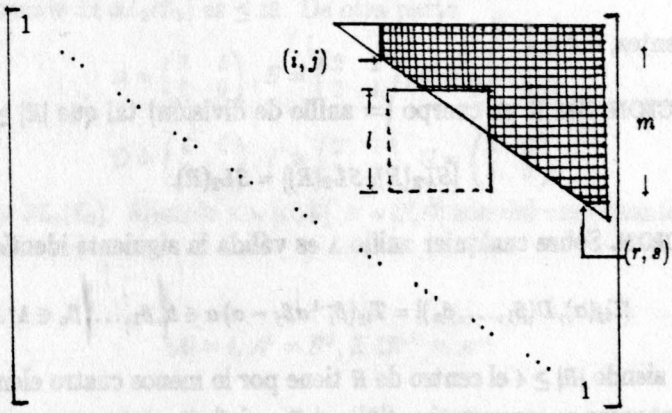
$$|Z(UT_n^m(A))| = |A|^{m^2}$$

(v) Si $\frac{n+1}{3} < m \leq \frac{n}{2}$

$$|Z(UT_n^m(A))| = |A|^t \quad \text{con } t = \frac{2m^2 - (3m-n-1)(3m-n)}{2}$$

DEMOSTRACION. (i) - (iv) son evidentes a partir de los resultados del parágrafo 4 en [7]. Para la prueba de (v) basta contar el número de vértices del retículo conformado por la intersección del retículo triangular de $UT_n^m(A)$ y el retículo cuadrado del centralizador de $UT_n^m(A)$ (ver 4.9 y (9.b)en [7].).

Nótese que para la primera diagonal no nula de $UT_n^m(A)$ la diferencia de índices de columna y fila es m, con lo cual calculamos los valores de i y s en el siguiente diagrama:



$i = n - 2m + 1, \quad j = n - m + 1, \quad r = m, \quad s = 2m$

$l = m - (n - 2m + 1)$

El número de vértices del retículo sombreado es igual a $m^2 - \frac{t^2+1}{2}$. Nos resta calcular el orden del centro del grupo especial lineal. Lo hacemos en un caso muy particular.

2.10 EJEMPLO. [3] Sea K un campo de orden q. Entonces $|\mathbf{Z}(SL_n(K))| = \text{m.c.d}\ (n, q-1)$. Según [3]

$$\mathbf{Z}(SL_n(K)) = \{D(a,\ldots,a) \mid a^n = 1,\ a \in K\}$$

Denotemos $H = \{a \in K \mid a^n = 1\}$ y veamos que $|H| = \text{m.c.d}\ (n, q-1)$. Como H es un subgrupo de K^*, entonces $|H|\,|(q-1)$; además como K^* es ciclico, H es también ciclico y existe $a_0 \in H$ tal que $|a_0| = |H|$. Pero $a_0^n = 1$, luego $|H|\,|n$.

De otra parte, sea s entero positivo tal que $s|(q-1)$ y $s|n$. Existe en K^* un subgrupo G de orden s, $G = < b >, b^s = 1$; resulta $b^n = 1$ y por tanto $b \in H$, de donde $s\,|\,|H|$.

3 CONMUTANTES.

Estudiamos ahora los conmutantes de los grupos introducidos en el primer parágrafo. Se obtendrán además algunas relaciones de solubilidad.

3.1 TEOREMA. [1] Sea Λ un anillo y $n \geq 3$. Entonces

$$[E_n(\Lambda), E_n(\Lambda)] = E_n(\Lambda).$$

DEMOSTRACION. Tomando $\beta = 1$ en (1) encontramos que cada elemental es un comutador.

(1) $$T_{ij}(\alpha\beta) = [T_{ik}(\alpha), T_{kj}(\beta)]$$

con i,j,k diferentes, $\alpha, \beta \in \Lambda$.

3.2 PROPOSICION. Sea R un cuerpo (= anillo de división) tal que $|R| \geq 4$. Entonces

$$[SL_2(R), SL_2(R)] = SL_2(R).$$

DEMOSTRACION. Sobre cualquier anillo Λ es válida la siguiente identidad

(2) $$[T_{ij}(\alpha), D(\beta_1,\ldots,\beta_n)] = T_{ij}(\beta_i^{-1}\alpha\beta_j - \alpha)\ \alpha \in \Lambda, \beta_1,\ldots,\beta_n \in \Lambda^*.$$

De otra parte, siendo $|R| \geq 4$ el centro de R tiene por lo menos cuatro elementos. En efecto, si R es finito entonces es conmutativo ([2]); si R es infinito entonces su subcampo primo Q (racionales) está contenido en el centro de R.

Existe α_0 no nulo en el centro de R tal que $\alpha_0^2 - 1 \neq 0$,caso contario el centro de R tendría a lo sumo 3 elementos, en contra de lo establecido anteriormente. Hagamos en (2), $n = 2$, $\beta_1 = \alpha_0$, $\beta_2 = \alpha_0^{-1}$.

$$T_{21}(\alpha) = [T_{21}((\alpha_0^2 - 1)^{-1}\alpha), D(\alpha_0, \alpha_0^{-1})], \alpha \in R$$

De manera similar se establece que $T_{12}(\alpha)$ es un conmutador de $SL_2(R)$.

3.3 PROPOSICION

(a) $[SL_2(\mathbb{Z}_2), SL_2(\mathbb{Z}_2)] = \left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\right\}$

(b) $[SL_2(\mathbb{Z}_3), SL_2(\mathbb{Z}_3)] \cong D_3$ (Grupo de Hamilton).

DEMOSTRACION. (a) Nótese que

$$SL_2(\mathbb{Z}_2) = GL_2(\mathbb{Z}_2)$$

y es un grupo no abeliano de orden 6, es decir, isomorfo a S_3, el grupo simétrico de grado 3. Resulta entonces que el conmutante de $SL_2(\mathbb{Z}_2)$ y por lo tanto de $GL_2(\mathbb{Z}_2))$ es isomorfo a el grupo alternante A_3 de grado 3, y en consecuencia es de orden 3.La matriz $\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix} \in SL_2(\mathbb{Z}_2)$ es de orden 3. Puesto que en S_3 sólo hay un subgrupo de orden 3 la parte (a) queda demostrada.

(b) De acuerdo al corolario 2.5 $SL_2(\mathbb{Z}_3)$ es de orden $24 = 2^3 \cdot 3$. Según un teorema de Burnside, los grupos de orden $p^\alpha q^\beta$, con p,q primos diferentes, son solubles ([8]). Por lo anterior el orden del conmutante de $SL_2(\mathbb{Z}_3)$ es ≤ 12. De otra parte

$$A = \begin{pmatrix}0 & 1\\ 2 & 0\end{pmatrix}, B = \begin{pmatrix}2 & 2\\ 2 & 1\end{pmatrix}, C = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$$

$$D = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, F = \begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}, G = \begin{pmatrix}2 & 2\\ 1 & 0\end{pmatrix}$$

Son elementos de $SL_2(\mathbb{Z}_3)$. Además $A = [C, D]$, $B = [F, G]$ son del conmutante.

También

$$|A| = 4, A^2 = B^2, BAB^{-1} = A^{-1} \tag{3}$$

Resulta entonces que el subgrupo generado por A y B está en el conmutante;pero según (3) este subgrupo es isomorfo a Q_3, el cual tiene orden 8.

De acuerdo al Teorema 3.1, tenemos

(4) $$E_n(A) \subseteq [GL_n(A), GL_n(A)], \text{ para } n \geq 3 \text{ y cualquier anillo } A$$

Si K es un cuerpo o un anillo conmutativo para el cual $E_n(K) = SL_n(K)$, entonces, teniendo en cuenta que

(5) $$\det[A, B] = 1,$$

para cualesquiera $A, B \in GL_n(K)$ resulta $[GL_n(K), GL_n(K)] \subseteq SL_n(K)$. De (4) se obtiene entonces el siguiente resultado.

3.4 TEOREMA. Sea $n \geq 3$ y K un cuerpo o un anillo conmutativo para el cual $SL_n(K) = E_n(K)$. Entonces

$$[GL_n(K), GL_n(K)] = SL_n(K).$$

3.5 PROPOSICION. (a) Sea K un cuerpo tal que $|K| \geq 3$.

Entonces

$$[GL_2(K), GL_2(K)] = SL_2(K).$$

(b) $[Gl_2(\mathbb{Z}_2), GL_2(\mathbb{Z}_2)] = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$

DEMOSTRACION. (a) Según (5) la inclusión de izquierda a derecha se cumple. Para la otra inclusión se tiene el siguiente hecho más general ([9]): Sea A un anillo tal que existe $\alpha_0 \in A^*$ con $(\alpha_0 - 1) \in A^*$. Entonces $E_2(A) \subseteq [GL_2(A), GL_2(A)]$. En efecto, sea $\alpha \in A$, entonces.

$$T_{12}(\alpha) = [T_{12}(\alpha(\alpha_0 - 1)^{-1}, D(1, \alpha_0)]$$

$$T_{21}(\alpha) = [T_{21}\{(\alpha_0 - 1)^{-1}\alpha), D(\alpha_0^{-1}, 1)]$$

(b) Es consecuencia de 3.3. **3.6 TEOREMA.** Sean $n \geq 2$ y K un anillo conmutativo para el cual existe $\alpha_0 \in K^*$ con $(\alpha_0 - 1) \in K^*$. Entonces

$$[T_n(K), T_n(K)] = UT_n(K).$$

DEMOSTRACION. Para la demostración de este teorema necesitamos un hecho preliminar.

3.7 PROPOSICION. Sea A un anillo finito de Dedekind ([7]), $n \geq 2$. Entonces para cada $1 \leq m \leq n$, $UT_n^m(A) \trianglelefteq T_n(A)$

Además,

$$UT_n(A) = UT_n^1(A) \trianglerighteq UT_n^2(A) \trianglerighteq \cdots \trianglerighteq UT_n^n(A) = \{E\}$$

DEMOSTRACION. Sean $A = (a_{ij}) \in UT_n^m(A), B = (b_{ij}) \in T_n(A)$. Según el corolario 3.4 de [7] y (5) también de [7], A es producto finito de elementales de la forma.

$$T_{ij}(\alpha), \quad j - i \geq m, \quad \alpha \in A$$

y B es un producto

$$B = D(b_1, \ldots, b_n)T_1 \ldots T_r$$

donde cada T es un elemental de la forma $T_{ij}(\beta)$, $j > i$, $\beta \in A$.

Por otra parte se tiene la siguiente identidad válida en cualquier anillo A

$$D(b_1, \ldots, b_n)T_{ij}(\alpha) = T_{ij}(b_i \alpha b_j^{-1})D(b_1, \ldots, b_n),$$

con $\alpha \in A$, $b_k \in A^*$, $1 \leq k \leq n$.

Según lo anterior, para establecer que $B^{-1}AB$ yace en $UT_n^m(A)$ es suficiente mostrar que

$$T_{ij}(-\beta)T_{rs}(\alpha)T_{ij}(\beta) \in UT_n^m(A) \tag{6}$$

siendo $\alpha, \beta \in A$, $j > i$, $s - r \geq m$.

Con respecto a los índices consideremos los siguientes casos posibles

$j \neq r$, $s \neq i$. El producto en (6) da $T_{rs}(\alpha)$

$j = r$, $s \neq i$. El producto en(6) es $T_{is}(-\beta\alpha)T_{rs}(\alpha)$.Como $j > i$ entonces $-i > -j$; también como $j = r$ entonces $s - j \geq m$. Resulta $s - j - i > m - j$ y, sumando j, obtenemos $s - i > m$. De aquí (6) tiene lugar.

$j \neq r$, $s = i$. En este caso, (6) toma la forma, $T_{rj}(\alpha\beta)T_{rl}(\alpha)$. Puesto que $j > i$ entonces $j - r > i - r = s - r \geq m$ y el producto yace en $UT_n^m(A)$ $j = r, s = i$. Se descarta esta posibilidad ya que en caso contrario se tendría $i - j = s - r \geq m \geq 1 > 0$

Regresamos a la demostración del teorema. Para mostrar la inclusión $[T_n(K), T_n(K)] \subseteq UT_n(K)$ basta mostrar que $[a, b] \in UT_n(K)$ para cada par de generadores $a, b \in T_n(K)$.

En efecto, cada generador z de $[T_n(K), T_n(K)]$ es de la forma

$$z = [a_1^{\pm 1} \cdots a_n^{\pm 1}, b_1^{\pm 1} \cdots b_m^{\pm 1}]^{\pm 1},$$

donde a_i, b_j son generadores de $T_n(K)$. Teniendo en cuenta que

$$[a, b]^{-1} = [b, a] \tag{7}$$

y siendo a generador de $T_n(K)$, a^{-1} también lo es, podemos considerar que x es de la forma

$$x = [a_1 \cdots a_n, b_1 \cdots b_m].$$

Se tiene además la siguiente identidad en cualquier grupo

$$[ab, c] = b^{-1}[a, c]b[b, c]. \tag{8}$$

Resulta, entonces,

$$x = a_n^{-1}[a_1 \cdots a_{n-1}, b_1 \cdots b_m]a_n[a_n, b_1 \cdots b_m].$$

De (7) y de la proposición 3.7 entonces la demostración se reduce a establecer que $[a, b] \in UT_n(K)$ con a,b generadores de $T_n(K)$. Ahora si a y b son diagonales se sigue que $[a, b] = E \in U_n(K)$. Si a es elemental y b diagonal, según (2) el conmutador es de $UT_n(K)$. Si a es diagonal y b es elemental, de acuerdo a (7), éste se reduce al caso anterior.

$$a = T_{ij}(\alpha),\ b = T_{rs}(\beta),\ j > i\ \ s > r.$$

$$[T_{ij}(\alpha), T_{rs}(\beta)] = \begin{cases} E, & j \neq r,\ i \neq s \\ T_{rj}(-\beta\alpha), & j \neq r,\ i = s \\ T_{is}(\alpha\beta), & j = r,\ i \neq s \end{cases} \tag{9}$$

El caso $j = r, i = s$ se descarta ya que $j > i > j$, causa contradicción. (Nótese que (9) es válida en cualquier anillo Λ).

Los tres casos de (9) conducen a que $[a, b] \in UT_n(K)$. Si $j \neq r, i = s$ entonces $j > i = s > r$; si $j = r, i \neq s$ entonces $s > r = j > i$.

La otra inclusión es consecuencia de la fórmula

$$T_{ij}(\alpha) = [T_{ij}(\alpha(\alpha_0 - 1)^{-1}, D(1, \ldots, \underset{\substack{\uparrow \\ i}}{\alpha_0}, \ldots, \underset{\substack{\uparrow \\ j}}{1})],$$

válida en todo anillo Λ que cumpla la condición del teorema.

El anillo $\mathbb{Z}_2$ no cumple la condición del teorema 3.6 sin embargo $T_n(\mathbb{Z}_2) = UT_n(\mathbb{Z}_2)$ y el conmutante será considerado en el siguiente teorema. **3.8 TEOREMA.** Sea Λ un anillo cualquiera, $n \geq 2$. Entonces

$$[UT_n^r(\Lambda), UT_n^s(\Lambda)] = UT_n^{r+s}(\Lambda)$$

$1 \leq r, s, \leq n$, $UT_n^k(\Lambda) = \{E\}$ para $k \geq n$

DEMOSTRACION. Consideremos inicialmente el caso $n = 2$. Tenemos

$$UT_2(\Lambda) = \{T_{12}(\alpha) \mid \alpha \in \Lambda\},\ UT_2^2(\Lambda) = \{E\}.$$

La conmutatividad de estos grupos garantiza la afirmación del teorema.

Sea ahora $n \geq 3$. La inclusión de izquierda a derecha se puede mostrar razonando como en la demostración del teorema 3.6 y teniendo en cuenta que $UT_n^{r+s}(\Lambda)$ es normal tanto en $UT_n^r(\Lambda)$ como en $UT_n^s(\Lambda)$ (proposición 3.7). Por tanto es suficiente mostrar que $[a,b] \in UT_n^{r+s}(\Lambda)$ para $a \in UT_n^r(\Lambda)$ y $b \in UT_n^s(\Lambda)$. Para tal efecto, sean $T_{ik}(\alpha) \in UT_n^r(\Lambda)$, $T_{jl}(\beta) \in UT_n^s(\Lambda)$ y $[T_{ik}(\alpha), T_{jl}(\beta)]$ el conmutador.

Si $k = j$, $i \neq l$ entonces según (9) dicho conmutador es $T_{il}(\alpha\beta)$, $k-1 \geq r$, $l-k \geq s$ y $l-i \geq r+s$, así el conmutador está en $UT_n^{r+s}(\Lambda)$.

Para $k \neq j, l \neq i$ el conmutador es $E \in UT_n^{r+s}(\Lambda)$.

Finalmente si $k \neq j$, $l = i$, encontramos $T_{jk}(-\beta\alpha) \in UT_n^{r+s}(\Lambda)$ ya que $k-i \geq r, i-j \geq s$ y por tanto $k-j \geq r+s$.

$UT_n^{r+s}(\Lambda) \subseteq [UT_n^r(\Lambda) \cdot UT_n^s(\Lambda)]$.

Examinemos los generadores de $UT_n^{r+s}(\Lambda)$. Sea $T_{ij}(\alpha) \in UT_n^{r+s}(\Lambda)$. Como $j-i \geq r+s > s$, entonces, $j-s > i > 0$. Sea $k =: j-s$, entonces $k-i = j-i-s \geq r+s-s = r$; $j-k = s$ y según (9)

$$T_{ij}(\alpha) = [T_{ik}(\alpha), T_{kj}(1)] \in UT_n^r(\Lambda), UT_n^s(\Lambda)]$$

3.9 OBSERVACION. Del isomorfismo $D_n(\Lambda) \cong \Lambda^* \times \cdots \times \Lambda^*$, se desprende $[D_n(\Lambda), D_n(\Lambda)] \cong [\Lambda^*, \Lambda^*] \times \cdots \times [\Lambda^*, \Lambda^*]$, siendo Λ un anillo cualquiera.

Los resultados precedentes sirven para determinar la solubilidad en algunos casos particulares.

3.10 COROLARIO (a) Sea Λ un anillo cualquiera y $n \geq 3$. Entonces $E_n(\Lambda)$ no es soluble.

(b) Sea K un cuerpo tal que $|K| \geq 4$. Entonces $SL_2(K)$ no es soluble.

(c) $SL_2(\mathbb{Z}_3)$, $SL_2(\mathbb{Z}_2)$ son solubles.

(d) Sea K un cuerpo o un anillo conmutativo para el cual $SL_n(K) = E_n(K)$. Entonces para $n \geq 3$, $GL_n(K)$ no es soluble.

(e) Sea K un cuerpo, $|K| \geq 4$. Entonces $GL_2(K)$ no es soluble.

(f) $GL_2(\mathbb{Z}_2)$, $GL_2(\mathbb{Z}_3)$ son solubles.

(g) Sea K un anillo conmutativo con elemento α_0 tal que $\alpha_0,(\alpha_0 - 1) \in K^*$. Entonces $T_n(K)$ es soluble para $n \geq 2$.

(h) Sea A un anillo cualquiera y $n \geq 2$. Entonces $UT_n^m(A)$ es soluble para cada $1 \leq m \leq n$.

(i) Sea A un anillo cualquiera y $n \geq 2$. Entonces $D_n(A)$ es soluble si y sólo si A^* es soluble.

BIBLIOGRAFIA

[1] BASS, H. Algebraic K - Theory. Benjamin, New York, 1968

[2] HERSTEIN, I.N., Noncomuntative Rings. Wiley, 1968.

[3] KARGAPOLOV M.I. and MERZJAKOV JU. I. Fundamentals of the Theory of Groups. 2nd ed., Springer, New York 1979.

[4] KASH, F. Moduln and Ringe. Teubner, Stutgart, 1977.

[5] LANG, S. Algebra. Reading, Adison Wesley, 1965.

[6] LEZAMA, O., Generalización de los anillos débilmente finitos, Anales del VI Coloquio Latinoamericano de Algebra, Córdova, Argentina, 1986 (en imprenta).

[7] LEZAMA O., VASQUEZ M.O.,Grupos de matrices sobre anillos (por aparecer).

[8] ROBINSON, D. A. Course in the Theory of Groups. Springer, New York, 1982.

[9] SUPRUNENKO, D.A. Grupos de Matrices. Nauka, Moscú, 1972.