"SUBGRUPOS CONGRUENTES DE GRUPOS CLÁSSICOS"

JOSÉ MARQUES DE MENDONÇA[a]
NARESH KUMAR SHARMA[a]

RESUMO

Calculamos os índices dos subgrupos congruentes $Sl_n(D,I)$, $Gl_n(D,I)$, $Sp_n(D,I)$ e $So_n(D,I)$ dos grupos linear especial $Sl_n(D)$, linear geral $Gl_n(D)$, simplético $Sp_n(D)$ e ortogonal $So_n(D)$, respectivamente. Aqui I é um ideal de D, anel dos inteiros de um corpo global K. O grupo ortogonal $So_n(D)$ é tratado sob a forma quadrática, definida por $\begin{bmatrix} O & I_n \\ I_n & O \end{bmatrix}$ *Por motivos técnicos, no processo de indução do caso ortogonal, para n = 2 todos os ideais de D são supostos principais. Estudamos, também, a aplicação projeção de $Sl_n(D)$, $Gl_n(D)$, $Sp_n(D)$ e $So_n(D)$ aos grupos correspondentes, $Sl_n(D/I)$, $Gl_n(D/I)$, $Sp_n(D/I)$ e $So_n(D/I)$, definidos sobre o anel quociente D/I. Simultaneamente, obtemos um conjunto de geradores para cada um dos grupos.*

PALAVRAS-CHAVE: *Grupos e Anéis; Corpo Global; Teoria de Congruências de matrizes; Álgebra Linear em Domínios de Integridade.*

1 – INTRODUÇÃO

Seja $F_q[t]$, o anel dos polinômios sobre o corpo finito F_q, com q elementos e K um corpo global, isto é, uma extensão finita do corpo dos racionais Q ou do $F_q(t)$, corpo quociente de $F_q[t]$. O anel dos inteiros I_K de K consiste daqueles elementos α de K que satisfaz $a_0 + a_1\alpha + \ldots + \alpha^n = 0$, para algum $n \geqslant 1$, com $a_0, \ldots, a_{n-1}$ em Z, conjunto dos inteiros, se a característica de K, ch(K), é O e em $F_q[t]$, no caso contrário. É fato que $I_K = D$ é domínio de integridade e que qualquer ideal não-trivial, diferente de D e {O}, é produto finito único, a menos de ordem, dos ideais primos. Em D $(S_1, \ldots S_r, a_1, \ldots a_t)$ para $r + t \geqslant 1$, significa o mínimo ideal contendo subconjuntos $S_1, \ldots, S_r$ de D e elementos $a_1, \ldots, a_t$ de D. Se H é um subgrupo do grupo G, [G:H] significa o índice de H em G. A mesma notação permanece no caso de I ser ideal de D. Acontece que se I é um ideal não-nulo de D, então

[a] Depto. de Matemática — CCE / Universidade Estadual de Londrina.

Semina, 10(4):249-259, 1989

$[D:I]$ é finito e $[D:I_1I_2] = [D:I_1] \cdot [D:I_2]$ se $(I_1, I_2) = (1)$.

Seja K um corpo global e $I_K = D$ o anel dos inteiros de K. $M_{n,n}(d)$ é o conjunto das matrizes $A = (a_{ij})$ do tipo n x n com $a_{ij} \in D$. Se I_n e O_n representam a matriz identidade e a matriz nula, respectivamente, do tipo n x n,

define-se $J_n = \begin{bmatrix} O_n & I_n \\ \cdot & \cdot \\ I_n & O_n \end{bmatrix}$, $\bar{J}_n = \begin{bmatrix} O_n & I_n \\ \cdot & \cdot \\ I_n & O_n \end{bmatrix}$

Consideremos G um dos seguintes grupos clássicos:

Linear Especial: $Sl_n(D) = \{A \in M_{n,n}(D) : \det A = 1\}$,
Linear Geral: $Gl_n(D) = \{A \in M_{n,n}(D) : \exists\ B \in M_{n,n}(D)$ com $AB = I_n\}$,
Simplético: $Sp_n(D) = \{A \in M_{2n,\,2n}(D) : A^t J_n A = J_n\}$, e
Ortogonal: $So_n(D) = \{A \in Ms_{2n,2n}(D) : A^t \bar{J}_n A = \bar{J}_n\}$
(Veja Weil [12], para mais detalhes).

Para um ideal I de D, matrizes $A = (a_{ij})$ e $B = (b_{ij})$ do tipo m xn, sobre D, então $A \equiv B \pmod I$ se, e somente se, $a_{ij} \in I$. Consideremos os subgrupos congruentes:

$Sl_n(D,I) = \{A \in Sl_n(D) : A \equiv I_n \pmod I\}$,
$Gl_n(D,I) = \{A \in Gl_n(D) : A \equiv I_n \pmod I\}$,
$Sp_n(D,I) = \{A \in Sp_n(D) : A \equiv I_{2n} \pmod I\}$, e
$So_n(D,I) = \{A \in So_n(D) : A \equiv I_{2n} \pmod I\}$.

Em virtude das aplicações na aritmética analítica, veja Gunning [4] e Ogg [10], é importante calcular os índices de $Sl_n(D,I)$, $Gl_n(D,I)$, $Sp_n(D,I)$ e $So_n(D,I)$ em $Sl_n(D)$, $Gl_n(D)$, $Sp_n(D)$ e $So_n(D)$, respectivamente, se I é não trivial, que é um dos objetivos deste trabalho. O caso em que K é o corpo dos números racionais foi tratados por Köecher [6]. Para o tratamento de casos especiais dos grupos linear especial e simplético, remetemos a Newman [9].

Em cada caso, este problema é reduzido, a determinar uma condição necessária e suficiente para que uma coluna do tipo próprio sobre D, seja igual à primeira coluna de algum elemento do grupo. Depois temos que contar quantas colunas, incongruentes modulo I, sujeitas à esta condição já obtida. Além disso para cada uma dessas colunas precisamos contar quantos elementos incongruentes módulo I o grupo possui. Por razões técnicas, todos os ideais de D são, no caso do grupo ortogonal, e n = 2, supostos principais.

Ao mesmo tempo, é interessante estudar a aplicação projeção dos grupos $Sl_n(D)$, $Gl_n(D)$, $Sp_n(D)$ e $So_n(D)$ nos grupos correspondentes $Sl_n(D/I)$, $Gl_n(D/I)$, $Sp_n(D/I)$ e $So_n(D/I)$, definidos sobre o anel quociente D/I. Nem sempre estas projeções são sobrejetoras. Mais precisamente, isto só ocorre no caso dos grupos $Sl_n(D)$ e $Sp_n(D)$. Para casos especiais do grupo $Sl_n(D)$, veja Witt [13]. Simultaneamente, determinamos um conjunto de geradores de cada grupo.

As notações usadas são de acordo com o Herstein [5] e Lang [7]. Caso o leitor queira mais detalhes sobre assunto pode utilizar como referencia Viswanathan [11] para a teoria de congruências, Cassels-Frohlich [2] para corpos globais e Endler [3] e Atiyah-MacDonald [1] para ideais em I_K.

A maior parte deste trabalho serviu como tese de mestrado para o primeiro autor sob orientação do segundo autor. Queremos, nesta oportunidade agradecer o apoio que a Coordenadoria de Pesquisa e Pós-Graduação da UEL nos dispensou durante o desenvolvimento do trabalho e também ao Departamento de Matemática da UEL que nos incentivou nesta realização.

2 – GRUPO LINEAR ESPECIAL

Nosso principal interesse é calcular o índice $l_n(I) = [Sl_n(D):Sl_n(D,I)]$t no caso em que $D = I_K$, para algum corpo global K. Caso $1 \leftarrow I$ é trivial, pois $Sl_n(D) = Sl_n(D,I)$, isto é, $l_n(I) = 1$, para qualquer n. Daqui para a frente, sempre $1 \leftarrow I$. Observemos que, se $A, B \leftarrow Sl_n(D)$, $AB^{-1} \leftarrow Sl_n(D)$ se, e somente se, $AB^{-1} \equiv I_n \pmod I$, isto é $A \equiv B \pmod I$. Para calcular $l_n(I)$, precisamos contar o número das matrizes de $Sl_n(D)$ incongruentes módulo I.

Proposição 1.1. Se $X = \begin{bmatrix} a_1 \\ \cdot \\ \cdot \\ \cdot \\ a_n \end{bmatrix}$; com $a_i \in D$,

e $n \geqslant 2$, então existe uma matriz $A \in Sl_n(D)$, com primeira coluna de A igual X se, e somente se,

$$(a_1, \ldots, a_n) = (1),$$

Prova: Caso n = 2 é trivial. Para o caso geral precisamos do seguinte:

Lema 1.1.1. Se $n \geqslant 2$, $X = \begin{bmatrix} a_1 \\ \cdot \\ \cdot \\ \cdot \\ a_n \end{bmatrix}$, $a_i \in D$,

tal que $(a_1, \ldots, a_n) = (1)$, então existem em $Sl_n(D)$ matrizes elementares $E_1, \ldots, E_r$, tais que

$$E_r \ldots E_1 \cdot \begin{bmatrix} a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_n \end{bmatrix} = \begin{bmatrix} a_1' \\ a_2' \\ \cdot \\ \cdot \\ \cdot \\ a_n' \end{bmatrix}$$

com $(a_1', a_2') = (1)$.

Seja $B_o = E_r \ldots E_2 . E_1$, que pertence $Sl_n(D)$.

Seja $X_1 = B_o X = \begin{bmatrix} a_1 \\ a_2 \\ . \\ . \\ . \\ a_n \end{bmatrix}$,

sabemos que $(a_1; a_2) = (1)$, então existem z e t, tais que

$$\det \begin{bmatrix} a_1 & t \\ a_2 & z \end{bmatrix} = 1$$

e teremos em $Sl_n(D)$ a matriz B_1 com a primeira coluna X_1, onde

$$B_1 = \begin{bmatrix} a_1 & t & 0 & \cdots & 0 \\ a_2 & z & 0 & \cdots & 0 \\ a_3 & 0 & 1 & & \\ . & & & & \\ . & & & & \\ . & & & & \\ a_n & 0 & & & 1 \end{bmatrix}$$

A matriz requerida é $B_o^{-1} B_1$.

Apresentaremos agora, um resultado necessário para o processo de contagem.

Proposição 1.2. Seja $(a_1, \ldots, a_n, I) = (1)$, para $n \geqslant 2$, então existem $y_1, \ldots, y_n \in I$, tais que

$$(a_1 + y_1, \ldots, a_n + y_n) = (1).$$

Proposição 1.3. Seja $n \geqslant 2$ e I um ideal do domínio D. Então o número de n-uplas $(a_1, \ldots, a_n)$, com $a_i \in D$, e $(a_1, \ldots, a_n, I) = (1)$ incongruentes módulo I é

$$\prod_j (p_j^n - 1).(p_j)^{(m_j - 1).n},$$

onde $p_j = [D:P_j']$. se $I = \prod_j P_j^{m_j}$ com $m_j \geqslant 1$.

Como consequência imediata da proposição 1.2 e da proposição 1.3 temos:

Corolário 1.3.1. Seja $n \geqslant 2$ e I um ideal em D. Então o número de n-uplas $(a_1, \ldots, a_n)$ com $(a_1, \ldots, a_n) = (1)$ incongruentes módulo I é

$$\prod_j (p_j^n - 1) \cdot (p_j)^{(m_j - 1).n}$$

Proposição 1.4. Seja $n \geqslant 2$,

$$X_1 = \begin{bmatrix} 1 \\ 0 \\ . \\ . \\ . \\ 0 \end{bmatrix},$$

e seja S = $A \in Sl_n(D) : X_1$ é a 1a. coluna de A . Então S tem $[D:I]^{n-1} \lambda_{n-1}$ matrizes incongruentes módulo I.

A prova desta proposição é uma consequência imediata do lema que segue:

Lema 1.4.1. Se $n \geqslant 2$ e $\bar{A} \in M_{n-1,n-1}(D)$, então

$$A = \begin{bmatrix} 1 & x_2 & \cdots & x_n \\ 0 & & & \\ . & & \bar{A} & \\ 0 & & & \end{bmatrix} \in Sl_n(D)$$

se, e somente se, $\bar{A} \in Sl_{n-1}(D)$, e $x_2, \ldots, x_n \in D$.

Proposição 1.5. Sejam as colunas

$$X_1 = \begin{bmatrix} 1 \\ 0 \\ . \\ . \\ . \\ 0 \end{bmatrix} \text{ e } X_2 = \begin{bmatrix} a_1 \\ a_2 \\ . \\ . \\ . \\ a_n \end{bmatrix}, \text{ com } (a_{11} -, a_n) = (1)$$

e sejam os conjuntos

S = $A \in Sl_n(D) : X_1$ é a 1a. coluna de A ,

e T = $B \in Sl_n(D) : X_2$ é a 1a. coluna de B .

Então existe uma bijeção $f : S \to T$ tal que

$$A_1 \equiv A_2 \pmod{I} \Leftrightarrow f(A_1) \equiv (A_2) \pmod{I}$$

Assim, S e T têm o mesmo número de matrizes incongruentes mod I.

Para concluir a contagem do caso do grupo $Sl_n(D)$, é de muita utilidade a seguinte:

Proposição 1.6. Se $f : Sl_n(D) \to Sl_n(D/I)$,

$$(a_{ij}) \to (\bar{a}_{ij})$$

então f é sobrejetora.

Corolário 1.6.1. Existe um isomorfismo

$$\bar{f} : Sl_n(D)/Sl_n(D,I) \to Sl_n(D/I)$$

onde $\bar{f}$ ((cl(A)). Aqui, cl(A) = H.A = BA : $B \in Sl_n(D,I)$, com $H = Sl_n(D,I)$ e , ainda mais, $\bar{f}$ (A) = (a_{ij}) se $A = (a_{ij})$ pertencer a $Sl_n(D)$.

Corolário 1.6.2. Sejam

$$X_1 = \begin{bmatrix} 1 \\ 0 \\ . \\ . \\ . \\ 0 \end{bmatrix}, X_2 = \begin{bmatrix} a_1 \\ . \\ . \\ . \\ . \\ a_n \end{bmatrix},$$

com $X_1 \equiv X_2$ (mod. I),

S = $A \in Sl_n(D) : X_1$ é 1a. coluna de A , e

T = $A \in Sl_n(D) : X_2$ é 1a. coluna de A

Então se $A \in T$, existe $A_o \in S$ tal que $A \equiv A_o$ (mod. I)

Uma consequência do corolário 1.6.2. é

Corolário 1.6.3. Sejam

$$\bar{X}_1 = \begin{bmatrix} c_1 \\ . \\ . \\ . \\ c_n \end{bmatrix}, \bar{X}_2 = \begin{bmatrix} d_1 \\ . \\ . \\ . \\ d_n \end{bmatrix} \in M_{n,1}(D),$$

tais que

$$\bar{X}_1 \equiv \bar{X}_2 \pmod{I} \text{ e } (c_1, \ldots, c_n) = (d_1, \ldots, d_n) = (1),$$

$S_1 = \{ B \in Sl_n(D) : \bar{X}_1 \text{ é a 1a. coluna de } B \}$,

$T_1 = \{ B \in Sl_n(D) : \bar{X}_2 \text{ é a 1a coluna de } B \}$.

Então se $B \in T$, existe $B_o \in S_1$ tal que $B \equiv B_o \pmod{I}$.

Teorema 1. (i) para $n \geqslant 2$, temos

$$l_n(I) = ([D:I]^{n-1} \prod_j (p_j^n - 1)(p_j)^{n(M_j-1)}) \, l_{n-1}(I)$$

onde

$$l_n(I) = [Sl_n(D):Sl_n(D,I)], \; I = \prod_j P_j^{mj} \text{ e } p_j = [D:P_j]$$

(ii) $l_1(I) = 1$ para qualquer I.

Prova: (i) É uma consequência imediata do corolário 1.3.1, das proposições 1.4 e 1.5 e dos corolários 1.6.2. e 1.6.3. (ii) E um caso particular, pois $[\ a\ ] \in Sl_n(D)$ se, e somente se, $a = 1$.

Como consequência de nosso trabalho, apresentamos, a seguir, resultado sobre um conjunto de geradores para o grupo $Sl_n(D)$.

Proposição 1.7. Se $n \geqslant 2$, $Sl_n(D)$ é gerado pelo conjunto S(n), o qual consiste dos elementos do tipo $E_{i(-1)}E_{ij}$, $E_{ij(c)}$, com $1 \leqslant i < j \leqslant n$ e $Sl_2(D)$. Aqui A em $Sl_2(D)$ é identificado em $Sl_n(D)$ como

$$\begin{bmatrix} A & 0 \\ 0 & I_{n-2} \end{bmatrix}, \text{ se } n \geqslant 2 \; ;$$

e E_{ij}, $E_{ij(c)}$, $E_{i(c)}$ são matrizes elementares.

Corolário 1.7.1. Se $n \geqslant 2$, $Sl_n(D)$ é gerado pelo subconjunto $\hat{S}(n)$, que consiste de $Sl_2(D)$ e $E_{i(-1)}E_{ij}$.

No caso em que D = Z, temos:

Proposição 1.8. $Sl_2(Z)$ é gerado pelo subconjunto $\hat{S}(2)$ que consiste de $E = E_{1(-1)}$ e $E_{12}(1)$.

2 – GRUPO LINEAR GERAL

Nosso objetivo, novamente, é o de calcular o índice $l_n(I) = [Gl_n(D):Gl_n(D,I)]$ no caso em que $D = I_K$ para algum corpo global.

Proposição 2.1. Se $X = \begin{bmatrix} a_1 \\ . \\ . \\ . \\ a_n \end{bmatrix}$; com $a_i \in I_K$,

com $n \geqslant 2$, então existe uma matriz $A \in Gl_n(D)$ com a primeira coluna de A sendo a coluna X se, e somente se,

$$(a_1, \ldots, a_n) = (1).$$

Proposição 2.2. Seja $n \geqslant 2$,

$$X_1 = \begin{bmatrix} 1 \\ 0 \\ . \\ . \\ . \\ 0 \end{bmatrix},$$

e seja $S = \{ A \in Gl_n(D) : X_1 \text{ é a 1a. coluna de } A \}$, então S tem $[D:I]_{n-1}.l_{n-1}$ matrizes incongruentes módulo I.

A proposição 2.2. é conseqüência imediata do

Lema 2.2.1. Seja $n \geqslant 2$ e $\tilde{A} \in M_{n-1,n-1}(D)$, então

$$A = \left[\begin{array}{c|ccc} 1 & x_2 & \ldots & x_n \\ \hline 0 & & & \\ . & & \tilde{A} & \\ . & & & \\ 0 & & & \end{array}\right] \in Gl_n(D)$$

se, e somente se, $\tilde{A} \in Gl_{n-1}(D)$, com $x_1, \ldots, x_n \in D$.

Como no caso do $Sl_n(D)$, temos as duas proposições:

Proposição 2.3. Sejam as colunas

$$X_1 = \begin{bmatrix} 1 \\ 0 \\ . \\ . \\ . \\ 0 \end{bmatrix} \text{ e } X_2 = \begin{bmatrix} a_1 \\ a_2 \\ . \\ . \\ . \\ a_n \end{bmatrix},$$

e sejam os conjuntos $S = \{ A \in Gl_n(D) : X_1 \text{ é a 1a. coluna de } A \}$,

e $T = \{ A \in Gl_n(D) : X_2 \text{ é a 1a. coluna de } A \}$.

Então existe uma bijeção $f : S \to T$ tal que

$$A_1 \equiv A_2 \pmod{I} \Leftrightarrow f(A_1) \equiv f(A_2) \pmod{I}$$

Para concluir a contagem no caso do $Gl_n(D)$, precisamos

Proposição 2.4. Seja $n \geqslant 2$, e

$$X_1 = \begin{bmatrix} 1 \\ 0 \\ . \\ . \\ . \\ 0 \end{bmatrix}, \quad X_2 = \begin{bmatrix} a_1 \\ a_2 \\ . \\ . \\ . \\ a_n \end{bmatrix}$$

com $X_1 \equiv X_2 \pmod I$. Seja

$S = A \in Gl_n(D) : X_1$ é 1a. coluna de A

$T = A \in Gl_n(D) : X_2$ é 1a. coluna de A

então existe $A_o \in T$ e existe $B_o \in S$ tal que

$A_o \equiv B_o \pmod I$.

Observemos que a analoga da proposição 1.7. não é válida no caso de $Gl_n(D)$. Mais precisamente, se I é um ideal do dominio D e $\bar{A} = (\bar{a}_{ij}) \in Gl_n(D/I)$, nem sempre existe $A = (a_{ij})$ em $Gl_n(D)$ tal que $(a_{ij}) \doteq (\bar{a}_{ij})$. A melhor maneira é dar exemplo:

Exemplo 1. Sejam $D = Z = I_Q$, $n = 1$ e $I = 10Z$. Então (3) pertence a $Gl_1(Z/10Z)$. Mas não existe $(a_{11}) \in Gl_1(Z)$ tal que $(\bar{a}_{11}) = (\bar{3})$, pois para que $(\bar{a}_{11}) \in Gl_1(D)$ é necessário que $a_{11} = 1$ ou -1, e nem $1 \equiv 3 \pmod{10}$ nem $-1 \equiv 3 \pmod{10}$.

Teorema 2. (i) Se $n \geqslant 2$, então

$$l_n(I) = [D:I]^{n-1} \cdot \prod_j (P_j^n - 1).(P_j)^{(m_j-1).n.l_{n-1}(I)}$$

onde $l_n(I) = [Gl_n(D):Gl_n(D,I)]$,

$$I = \prod_j P_j^{mj} \text{ e } p_j = [D:P_j]$$

(ii) $l_1(I) = [U:U_I]$, onde U é o grupo das unidades de $D = I_K$ e

$$U_I = u \in U : u \equiv 1 \pmod I$$

Prova: (i) É consequência do corolário 1.3.1. e das proposição 2.1 a 2.4. (ii) $[u]$ pertence a $Gl_n(D)$ se, e somente se, $u \in U$. $[u] \in Gl_n(D,I)$ se, e somente se, $u \in U_I$. Agora (ii) é trivial.

Analogamente ao caso de $Sl_n(D)$, temos

Proposição 2.5. Se $n \geqslant 2$, $Gl_n(D)$ é gerado pelos elementos de S (n) que consiste de E_{ij}, $E_{ij(c)}$, com $1 \leqslant i < j \leqslant n$; e (u) para $u \in U$ e $Sl_2(D)$. Aqui $Sl_2(D)$ é identificado em $Gl_n(D)$ como

$$\begin{bmatrix} A & 0 \\ 0 & I_{n-2} \end{bmatrix}, \text{ se } n \geqslant 2 \text{ e } e(u) = \left[\begin{array}{c|ccc} u & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \end{array}\right]$$

3 – GRUPO SIMPLETICO

Indicaremos por $P_n'(I) = [Sp_n(D):Sp_n(D,I)]$.

Proposição 3.1. Seja

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

$X = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ uma 2n-coluna, com elementos de D

então existe uma matriz $M \in Sp_n(D)$ com a primeira coluna X se, e somente se, $(x_1, \ldots, x_n, y_1, \ldots, y_n) = (1)$

Prova:

($\Rightarrow$) Se existe uma matriz $M \in Sp_n(D)$, então $M \in Gl_{2n}(D)$, implica que $(x_1, \ldots, x_n, y_1, \ldots, y)) = (1)$, conforme estudo de $Gl_n(D)$.

($\Leftarrow$) E preciso provar

Lema 3.1.1. Sejam A, B, C, D, U e $V \in M_{n,n}(D)$, então:

(i) $\begin{bmatrix} A & B \\ C & D \end{bmatrix} \in Sp_n(D)$

se, e somente se, $\begin{cases} a)\ A^tC = C^tA \\ b)\ -C^tB + A^tD = I_n, \text{ e} \\ c)\ D^tB = B^tD \end{cases}$

(ii) $\begin{bmatrix} U & 0 \\ 0 & V \end{bmatrix} \in Sp_n(Z)$ se, e somente se $VU^t = I_n$

(iii) $\begin{bmatrix} I_n & B \\ 0 & I_n \end{bmatrix} \in Sp_n(D)$ se, e somente se, $B = B^t$

(iv) $\begin{bmatrix} 0 & U \\ V & 0 \end{bmatrix} \in Sp_n(D)$ se, e somente se, $UV^t \doteq -I_n$

(v) $\begin{bmatrix} I_n & 0 \\ B & I_n \end{bmatrix} \in Sp_n(D)$ se, e somente se, $B = B^t$

Voltando à prova da proposição 3.1., temos:

Caso 1: $(x_1, \ldots, x_n) = (1)$.

Fácil usando (ii) e (v) do lema 3.1.1.

Caso 2: $(x_1, \ldots, x_n) \neq (1)$.

Subcaso 1: $n = 1$. Precisamos do lema seguinte:

Lema 3.1.2.

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Sp_n(D)$ se, e somente se, $ad - bc = 1$.

Subcaso 2: $n \geqslant 2$. Para tratar este subcaso, que é geral, precisamos do lema a seguir, que pode ser provado usando o lema 3.1.1.

Lema 3.1.3. Seja $n \geqslant 2$ e

$$X = [x_1 \ldots x_n \; y_1 \ldots y_n]^t \in M_{2n,1}(D)$$

com $(x_1, \ldots, x_n, y_1, \ldots, y_n) = (1)$. Então, existe $A_1 \in Sp_n(D)$ tal que

$$A_1 X = \begin{bmatrix} x_1' \\ \cdot \\ \cdot \\ x_n' \\ y_1' \\ \cdot \\ \cdot \\ y_n' \end{bmatrix} \text{ com } (x_1', \ldots, x_n') = (1).$$

Agora voltemos à demonstração da proposição 3.1. para o caso 2. Se $n \geqslant 2$ então pelo lema 3.1.3., existe A_1 em $Sp_n(D)$ tal que

$$A_1 X = \begin{bmatrix} x_1' \\ \cdot \\ \cdot \\ x_n' \\ y_1' \\ \cdot \\ \cdot \\ y_n' \end{bmatrix}, \text{ com } (x_1', \ldots, x_n) = (1).$$

Pelo caso 1 desta proposição, existe $A \in Sp_n(D)$ com primeira coluna $A_1 X$. Assim $A_1^{-1} A \in Sp_n(D)$ com primeira coluna igual a X.

Proposição 3.2. Seja $n \geqslant 2$,

$X_1 = [1\,0 \ldots 0\;0 \ldots 0]^t$,
e $S = \{A \in Sp_n(D) : X_1$ é a 1a. coluna de $A\}$, então S tem $[D:I]^{2n-1} \cdot p_{n-1}(I)$ matrizes incongruentes módulo I.

Prova: Para provar esta proposição precisamos do

Lema 3.2.1. Sejam $A, B, C, D \in M_{n,n}(D)$, e

$$A = \left[\begin{array}{c|c} 1 & z_2 \ldots z_n \\ \hline 0 & \\ \cdot & \tilde{A} \\ \cdot & \\ 0 & \end{array}\right], \; B = \left[\begin{array}{c|c} t_1 & t_2 \ldots t_n \\ \hline t_2' & \\ \cdot & \tilde{B} \\ \cdot & \\ t_n' & \end{array}\right],$$

$$C = \left[\begin{array}{c|c} 0 & u_2 \ldots u_n \\ \hline \cdot & \\ \cdot & \tilde{C} \\ \cdot & \\ 0 & \end{array}\right], \; D = \left[\begin{array}{c|c} w_1 & w_2 \ldots w_n \\ \hline w_2' & \\ \cdot & \tilde{D} \\ \cdot & \\ w_n' & \end{array}\right],$$

Então $\begin{bmatrix} A & B \\ C & D \end{bmatrix} \in Sp_n(D)$ se, e somente, as seguintes condições são satisfeitas:

(i) A matriz $\begin{bmatrix} \tilde{A} & \tilde{B} \\ \tilde{C} & \tilde{D} \end{bmatrix} \in Sp_{n-1}(D)$

(iii) $w_1 = 1, w_2 = \ldots = w_n = 0$
$u_2 = 0 = \ldots = u_n$

(iii) $$\begin{bmatrix} z_2 \\ \cdot \\ \cdot \\ \cdot \\ z_n \end{bmatrix} = -\tilde{A}^t \begin{bmatrix} w_2' \\ \cdot \\ \cdot \\ \cdot \\ w_n \end{bmatrix} - \tilde{C}^t \begin{bmatrix} t_2' \\ \cdot \\ \cdot \\ \cdot \\ t_n' \end{bmatrix}$$

(iv) $[t_2 \ldots t_n] = [t_2' \ldots t_n'] \tilde{D} - [w_2' \ldots w_n'] \tilde{B}$

Agora pela definição, existem $P_{n-1}(I)$ matrizes $\begin{bmatrix} \tilde{A} & \tilde{B} \\ \tilde{C} & \tilde{D} \end{bmatrix}$ em $Sp_{n-1}(D)$ incongruentes modulo I.

Para cada $\begin{bmatrix} \tilde{A} & \tilde{B} \\ \tilde{C} & \tilde{D} \end{bmatrix}$ em $Sp_{n-1}(D)$, módulo I,

existem $[D:I]^{n-1}$ incongruencias de cada $[t_2' \ldots t_n']$ e de $[w_2' \ldots w_n]$. Além disso, módulo I, $[z_2 \ldots z_n]$ e $[t_2 \ldots t_n]$ ficam determinados por $[w_2' \ldots w_n]$, $[t_2' \ldots t_n']$, $\tilde{A}, \tilde{B}, \tilde{C}$ e $\tilde{D}$. Portanto S tem $[D:I]^{2(n-1)} \cdot P_{n-1}(I)$ elementos incongruentes módulo I.

Proposição 3.3. Sejam

$$X_1 = \begin{bmatrix} 1 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix}, \quad X_2 = \begin{bmatrix} a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_n \\ b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_n \end{bmatrix}$$

tal que $(a_1, \ldots, a_n, b_1, \ldots, b_n) = (1)$. Seja, ainda

$S = A \in Sp_n(D) : X_1$ é a 1a. coluna de A

$T = B \in Sp_n(D) : X_2$ é a 1a. coluna de B

Então existe uma bijeção $f : S \to T$, tal que

$$A_1 \equiv A_2 \pmod{I} \Leftrightarrow f(A_1) \equiv f(A_2) \pmod{I}$$

Como no caso do $Sl_n(D)$, temos:

Proposição 3.4. Seja

$$f : Sp_n(D) \to Sp_n(D/I)$$
$$(a_{ij}) \to (\bar{a}_{ij})$$

Então f é um homomorfismo do grupo $Sp_n(D)$ em $Sp_n(D/I)$. Além disso f sobrejetora.

A maneira de provar é por indução matemática, com validade para n = 1, sendo baseado no lema 3.1.2.

Corolário 3.4.1. Existe um isomorfismo

$$f : Sp_n(D)/Sp_n(D/I) \to Sp_n(D/I),$$

onde $\bar{f}(\mathrm{cl}(A)) = \bar{A}$. Aqui, $\mathrm{cl}(A) = H.A. = B.A : B \in H$, com $H = Sp_n(D,I)$ e $\bar{A} = (\bar{a}_{ij})$ se $A = (a_{i,j}) \in Sp_n(D)$.

Corolário 3.4.2. Seja $n \geqslant 2$ e

$$X_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad X_2 = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \\ a_{n+1} \\ \vdots \\ a_{2n} \end{bmatrix},$$

Com $X_1 \equiv X_2 \pmod{I}$. Seja, também,

$S = A \in Sp_n(D) : X_1$ é 1a. coluna de A e

$T = A \in Sp_n(D) : X_2$ é 1a. coluna de A

Então se $A \in T$, existe $A_0 \in S$ tal que $A \equiv A_0 \pmod{I}$.

Teorema 3.

(i) Para $n \geqslant 2$, temos

$$p'_n(I) = \prod_j (p_j^{2n} - 1).(p_j)^{(m_j-1).2n} \cdot [D:I]^{2(n-1)} \; p'_{n-1}(I)$$

(ii) $p'_1(I) = 1_2(I)$

Prova: (i) É uma consequência das proposições 3.2., 3.3. e do corolários 1.3.1. 3.4.2..

(ii) Se n = 1, é consequência do fato que $Sp_1(D) = Sl_2(D)$.

Uma conseguência da demonstração da proposição 3.1. é

Proposição 3.5. $Sp_n(D)$ é gerado pelo conjunto T (n), que consiste de

$$i(Sl_2(D)), \quad \begin{bmatrix} U & 0 \\ 0 & (U^{-1})^t \end{bmatrix}, \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}, \begin{bmatrix} I_n & B \\ 0 & I_n \end{bmatrix},$$

com $B = B^t \in M_{n,n}(D)$, $U \in Gl_n(D)$, e i é uma aplicação definida como

$$i(A) = \left[\begin{array}{ccc|c} & & & 0 \\ & & & \vdots \\ & I_{n-1} & & \vdots \\ & & & 0 \\ \hline 0 & \ldots & 0a & 0 \ldots 0 \; b \\ \hline & & & 0 \\ & 0 & & \vdots \\ & & I_{n-1} & \vdots \\ & & & 0 \\ & & & c \quad d \end{array}\right] \text{ se } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Sl_2(D)$$

e $n \geqslant 2$. $i(A) = A$ se $n = 1$.

4 – GRUPO ORTOGONAL

Indicaremos por $r_n(I) = [So_n(D):So_n(D,I)]$. Daqui para frente, suporemos que $ch(D) \neq 2$.

Proposição 4.1. Seja

$$X = \begin{bmatrix} a_1 \\ \vdots \\ a_n \\ b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} X_1 \\ X_2 \end{bmatrix}$$

uma coluna com elementos de um domínio D.

a) Se existe $A \in So_n(D)$ com a primeira coluna igual a X, então:

$$(p1)\,(a_1, \ldots, a_n, b_1, \ldots, b_n) = (1).$$

$$(p2)\ a_1b_1 + \ldots + a_nb_n = 0, \text{ isto é}$$

$$X_1^t X_2 + X_2^t X_1 = 0.$$

b) Se $n \neq 2$ e satisfaz (p1) e (p2) então existe A com primeira coluna igual a X.

c) Se $n = 2$, então (b) é verdadeiro se D é D.I.P. (Domínio de Ideais Principais).

Prova:

($\Rightarrow$) É fácil provar comparando determinantes e os primeiros elementos da primeira coluna de $A^t J_n A$ e J_n.

($\Leftarrow$) Para provar a suficiência desta condição, precisamos:

Lema 4.1.1. Sejam U, V, W, B_1, B_2, B_3 e B_4 pertencentes a $M_{n,n}(D)$, então:

$$\text{(i) } A = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix} \in So_n(D) \Leftrightarrow \begin{cases} B_3^t B_1 + B_1^t B_3 = 0 \\ B_3^t B_2 + B_1^t B_4 = I_n \\ B_4^t B2 + B_2^t B_4 = 0 \end{cases}$$

$$\text{(ii) } A = \begin{bmatrix} U & 0 \\ 0 & V \end{bmatrix} \in So_n(D) \Leftrightarrow VU^t = I_n$$

$$\text{(iii) } A = \begin{bmatrix} I_n & 0 \\ W & I_n \end{bmatrix} \in So_n(D) \Leftrightarrow W^t + W = 0$$

$$\text{(iv) } A = \begin{bmatrix} I_n & W \\ 0 & I_n \end{bmatrix} \in So_n(D) \Leftrightarrow W^t + W = 0$$

$$\text{(v) } A = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix} \in So_n(D)$$

Uma consequência do lema 4.1.1. é

Lema 4.1.2: Se $X = [X_1\ X_2]^t$ satisfaz a propriedades (p1) e (p2), $A \in So_n(D)$, então AX satisfaz as propriedades (p1) e (p2).

Agora vamos provas a condição de suficiência da proposição 4.1.:

Caso 1: $(a_1, \ldots, a_n) = (1)$.

Este caso é fácil por causa de (ii) e (iii) do Lema 4.1.1.

Para tratar o caso geral, precisamos do lema seguinte, que é bastante técnico (veja Mendonça[8]).

Lema 4.1.3. Se $n \geq 3$.

$$X = \begin{bmatrix} a_1 \\ . \\ . \\ . \\ a_n \\ a_n \\ b_1 \\ . \\ . \\ . \\ b_n \end{bmatrix}$$

com $a_1b_1 + \ldots + a_nb_n = 0$ e $(a_1, \ldots, a_n, b_1, \ldots, b_n) = (1)$ e $S = \{A \in So_n(D) : A \text{ tem 1a. coluna } [1\ 0 \ldots 0\ 0 \ldots 0]^t\}$. Então existe $A \in S$ tal que $AX = [a'_1, \ldots a'_n, b'_1, \ldots, b'_n]^t$, com $(a'_1, \ldots, a'_n) = 1$.

Como consequência deste lema, pelo caso 1, já tratado, da condição de suficiência da proposição 4.1., existe $A_1 \in So_n(D)$ com 1^a coluna AX. Assim $A^{-1}A_1 \in So_n(D)$ com 1^a coluna X.

Para $n = 2$, o domínio D é admitido como D.I.P. Por causa da generalidade do argumento, provemos a condição de suficiência, no caso de D ser D.I.P. para $n \geq 2$.

Primeiro consideremos que $a_1 = \ldots = a_n = 0$ e $(b_1, \ldots, b_n) = (1)$. Neste caso existe $V \in Sl_n(D)$ com tal que

$$\begin{bmatrix} 0 & (V^{-1})^t \\ V & 0 \end{bmatrix}$$

pertence a $So_n(D)$ com primeira coluna igual a X. No outro caso se

$$a_1D + \ldots + a_nD = d\,D, \text{ com } d \neq 0.$$

existe $x_1, \ldots, x_n$ e $y_1, \ldots, y_n \leftarrow D$ tal que

$$a_1 = x_1d, \ldots, a_n = x_nd$$

$$a_1y_1 + \ldots + a_ny_n = d$$

isto é $x_1y_1 + \ldots + x_ny_n = 1$

Seja $U \in Sl_n(D)$, com primeira coluna

$$[x_1 \ldots x_n]^t$$

para que $M_1 = \begin{bmatrix} U^{-1} & 0 \\ 0 & U^t \end{bmatrix}$ pertence a $So_n(D)$. Assim

$$M_1X = M_1 \cdot \begin{bmatrix} a_1 \\ a_2 \\ . \\ . \\ . \\ a_n \\ b_1 \\ . \\ . \\ . \\ b_n \end{bmatrix} = \begin{bmatrix} d \\ 0 \\ . \\ . \\ . \\ 0 \\ b'_1 \\ . \\ . \\ . \\ b'_n \end{bmatrix} = X_1, \text{ para algum } b'_1, \ldots, b'_n \leftarrow D$$

Semina, 10(4):249-259, 1989

Pelo lema 4.1.2. $b'_1 = 0$ e $(d, b'_2, \ldots, b'_n) = (1)$.
Agora, em $So_n(D)$, se

$$M_2 = \left[\begin{array}{cccc|cccc} 0 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ 0 & & & & 0 & & & 0 \\ \cdot & & & & \cdot & & & \cdot \\ \cdot & & & & \cdot & & n-1 & \cdot \\ \cdot & & I_{n-1} & & \cdot & & & \cdot \\ 0 & & & & 0 & & & 0 \\ \hline 1 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ 0 & & & & 0 & & & \\ \cdot & & & & \cdot & & & \\ \cdot & & n-1 & & \cdot & & I_{n-1} & \\ \cdot & & & & \cdot & & & \\ 0 & & & & 0 & & & \end{array}\right]$$

Assim,

$$X_2 = M_2 X_1 = [\,0 \ldots 0\ d\ b'_2 \ldots b'_n\,]^t.$$

Agora existe $M_2 \in So_n(D)$ com primeira coluna X_2 e $M_1^{-1} M_2^{-1} M_3 \in So_n(D)$ com primeira coluna $M_1^{-1} M_2^{-1} X_2 = X$.

Proposição 4.2. Sejam $a_1, \ldots, a_n, b_1, \ldots, b_n \in D$; I um ideal de D e $n \geqslant 2$. Se $(a_1, \ldots, a_n, b_1, \ldots, b_n, I) = (1)$. e $a_1 b_1 + \ldots + a_n b_n \equiv 0 \pmod I$. Então existem $a'_i \equiv a_i \pmod I$ e $b'_i \equiv b'_i \pmod I$ tais que
$(a'_1, \ldots, a'_n, b'_1, \ldots, b'_n) = (1)$, e
$a'_1 b'_1 + \ldots + a'_n b'_n = 0$

Proposição 4.3. Seja $n \geqslant 2$; $I = P_1^{m_1} \ldots P_s^{m_s}$, com $s \geqslant 1$ e $m_1, \ldots, m_s \geqslant 1$, um ideal de D. Então o número das 2n-uplas $(a_1, \ldots, a_n, b_1, \ldots, b_n)$ em $M_{1,2n}(D)$, incongruentes módulo I que satisfazem as condições:

(i) $(a_1, \ldots, a_n, b_1, \ldots, b_n, I) = (1)$, e
(ii) $(a_1 b_1 + \ldots + a_n b_n) \equiv 0 \pmod I$,

é $\prod_j (p_j^n - 1)(p_j)^{m_j - 1)(2n-1)}(p_j^{n-1} + 1)$

Proposição 4.4. Seja $n \geqslant 2$,
$X_1 = [1\,0 \ldots 0 \quad 0 \ldots 0]^t$,
$S = \{A \in So_n(D) : X_1$ é a 1a. coluna de $A\}$. Então S possui $\prod_j (p_j)^{2(n-1)m_j} r_{n-1}(I)$ matrizes incongruentes módulo I, se

$I = \prod p_j^{m_j}$ e $p_j = [D:P_j]$.
$1 \leqslant j \leqslant s$

Prova: Para provar esta proposição precisamos do Lema
Lema 4.4.1. Seja A, B, C, D $\in M_{n,n}(D)$ e

$$A = \left[\begin{array}{c|c} 1 & z_2 \ldots z_n \\ \hline 0 & \\ \cdot & \tilde{A} \\ \cdot & \\ 0 & \end{array}\right] \quad B = \left[\begin{array}{c|c} t_1 & t_2 \ldots t_n \\ \hline t_2 & \\ \cdot & \tilde{B} \\ \cdot & \\ t_n & \end{array}\right]$$

$$C = \left[\begin{array}{c|c} 0 & u_2 \ldots u_n \\ \hline \cdot & \\ \cdot & \tilde{C} \\ \cdot & \\ 0 & \end{array}\right] \quad D = \left[\begin{array}{c|c} w_1 & w_2 \ldots w_n \\ \hline w'_2 & \\ \cdot & \tilde{D} \\ \cdot & \\ w'_n & \end{array}\right]$$

Então $\begin{bmatrix} A & B \\ C & D \end{bmatrix} \in So_n(D)$ se, e somente, as seguintes condições são satisfeitas:

(i) A matriz $\begin{bmatrix} \tilde{A} & \tilde{B} \\ \tilde{C} & \tilde{D} \end{bmatrix} \in So_{n-1}(D)$

(ii) $w_1 = 1, w_2 = \ldots = w_n = 0$
$u_2 = 0 = \ldots = u_n$

(iii) $[t_2 \ldots t_n] = -[w'_2 \ldots w'_n]\tilde{B} - [t'_2 \ldots t'_n]\tilde{D}$
$t_1 = -(w'_2 t'_2 + \ldots + w'_n t'_n)$

(iv) $[z_1 \ldots z_n] = -[w'_2 \ldots w'_n]\tilde{A} - [t'_2 \ldots t'_n]\tilde{C}$

Agora pela definição existem em $So_{n-1}(D)$ $r_{n-1}(I)$ matrizes $\begin{bmatrix} \tilde{A} & \tilde{B} \\ \tilde{C} & \tilde{D} \end{bmatrix}$ incongruentes módulo I. para cada $\begin{bmatrix} \tilde{A} & \tilde{B} \\ \tilde{C} & \tilde{D} \end{bmatrix}$

em $So_n(D)$ módulo I, existem $[D:I]^{n-1}$ incongruencias de cada $[t'_2 \ldots t'_n]$ e $[w'_2 \ldots w'_n]$. Além disso, módulo I, t_1, $[z_2 \ldots z_n]$ $[t_2 \ldots t_n]$ ficam determinados por $[t'_2 \ldots t'_n]$, $[w'_2 \ldots w'_n]$, $\tilde{A}$, $\tilde{B}$, $\tilde{C}$ e $\tilde{D}$. Portanto S possui $r_{n-1}(I)$. $[D:I]^{2(n-1)}$ elementos incongruentes módulo I.

Como nos outros grupos, temos

Proposição 4.5. Seja $n \geqslant 2$,

$$X_1 = \begin{bmatrix} 1 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix}, \quad X_2 = \begin{bmatrix} a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_n \\ b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_n \end{bmatrix} \in M_{2n,1}(D)$$

tal que $(a_1, \ldots, a_n, b_1, \ldots, b_n) = (1)$, e $a_1b_1 + \ldots + a_nb_n = 0$.

Seja $S = A \in So_n(D) : X_1$ é 1a. coluna de A
$T = B \in So_n(D) : X_2$ é 1a. coluna de B .

Então existe uma bijeção $f : S \to T$, tal que

$$A_1 \equiv A_2 \pmod I \Leftrightarrow f(A_1) \equiv f(A_2) \pmod I.$$

Ao contrário do que acontece no caso de $Sp_n(D)$ ou $Sl_n(D)$ nem sempre aplicação projeção

$$f : So_n(D) \to So_n(D/I)$$

é sobrejetora. Como exemplo consideremos o casos de $n = 1$, $D = I_Q = Z$, $I = 10Z$. É fácil verificar que

$$\begin{bmatrix} 8 & 5 \\ 5 & 2 \end{bmatrix} \in So_n(Z/10Z)$$

mas não existe

$$\begin{matrix} a & b \\ c & d \end{matrix} \in So_1(Z) \text{ tal que } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 8 & 5 \\ 5 & 2 \end{bmatrix} \pmod{10}$$

É assim, pois $U(Z) = 1, -1$ e

Proposição 4.6. Seja D um domínio de integridade com $ch(D) \neq 2$, então $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in So_1(D)$ se, e somente se,

é da forma $\begin{bmatrix} u & 0 \\ 0 & u^{-1} \end{bmatrix}$ ou $\begin{bmatrix} 0 & u^{-1} \\ u & 0 \end{bmatrix}$ para algum $u \in U$,

grupo das unidades de D.

Proposição 4.7. Sejam $n > 2$, D um dominio de integridade, I um ideal de D,

$$X_1 = \begin{bmatrix} 1 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix}, \quad X_2 = \begin{bmatrix} a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_n \\ b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_n \end{bmatrix}$$

com $X_1 \equiv X_2 \pmod I$,
(i) $a_1b_1 + \ldots + a_nb_n = 0$;
(ii) $(a_1, \ldots, a_n, b_1, \ldots, b_n) = (1)$;
(iii) $S = A \in So_n(D) : X_1$ é 1a. coluna de A ;
(iv) $T = B \in So_n(D) : X_2$ é 1a. coluna de A .
Então existe $A \in T$ e $A_o \in S$ tal que $A \equiv A_o \pmod I$.

Corolário 4.7.1. Mantendo as condições e notações da proposição 4.7., acontece que se $A' \in T$, então existe $A'_o \in S$ tal que $A' \equiv A'_o \pmod I$.

Teorema 4. Seja I um ideal de D, com $I \neq D \neq 0$, então

(i) se $n > 2$, $r_n(I) = [So_n(D) : So_n(D,I)] =$

$$= \prod_j (p_j^n - 1)\,(p_j)^{(Mj-1)(2n-1)}(p_j^{n-1} + 1).(p_j)^{2(n-1)}\, m_j.r_{n-1}(I)$$

(ii) Se $n = 1$, $r_1(I) = 2[U:U(I)]$

O Teorema 4 é consequencia das proposição 4.1. a 4.7.

Como consequencia da prova da Prop. 4.1., também temos

Proposição 4.8. Seja D.I.P. então $So_n(D)$ é gerado por R(n) que consiste de

$$\begin{bmatrix} V & 0 \\ 0 & (V^{-1})^t \end{bmatrix}, \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}, \begin{bmatrix} I_n & B \\ 0 & I_n \end{bmatrix},$$

e $R_n = \begin{bmatrix} I_{n-1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & I_{n-1} & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

onde $B^t = -B \in M_{n,n}(D)$ e $V \in Gl_n(D)$.

ABSTRACT

We calculate the indices of congruence subgroups, $Sl_n(D,I)$, $Gl_n(D,I)$, $Sp_n(D,I)$ and $So_n(D,I)$ of special linear group $Sl_n(D)$, general linear group $Gl_n(D)$, simpletic group $Sp_n(D)$ and orthogonal group $So_n(D)$, respectively. Here I is an ideal of D, the ring of integer of a global field K. The Othogonal group $So_n(D)$ is

$$\begin{matrix} O & I_n \end{matrix}$$

taken over quadratic form defined by For technical reasons, in the induction process,

$$\begin{matrix} I_n & O \end{matrix}$$

all ideals of D are assumed to be principal, for n= 2, in the ortogonal case. We also study the projection maps from $Sl_n(D)$, $Gl_n(D)$, $Sp_n(D)$ and $So_n(D)$ to corresponding groups $Sl_n(D/I)$, $Gl_n(D/I)$, $Sp_n(D/I)$ and $So_n(D/I)$, defined over quocient ring D/I. A generating set for each of these groups is also determined.

KEY WORDS: *Groups and rings; Global field; Theory of congruence of matrices; Linear algebra in integral domain.*

1 – ATIYAH, M.F. & MACDONALD, I.G. *Introduction to Commutative Algebra.* Addison Wesley, 1969.

2 – CASSELLS, J.W.S. & FROHLICH, A. (editors) *Algebraic Number Teory.* Academic Press, 1977.

3 – ENDLER, I. *Teoria dos Números Algébricos.* (Projeto Euclides), IMPA, 1986.

4 – GUNNING, R.C. *Lectures on Modular Forms.* Princeton Univ. Press, Princeton, 1962.

5 – HERSTEIN, I.N. *Topics in Algebra.* Blaisdell Publishing Co., 1964.

6 – KOECHER, M. *Zur Theorie der Modulformen n–ten Grades I. Math. Zeit.*, 399-416, 1954.

7 – LANG, S. *Algebra.* Addison Wesley, 1965.

8 – MENDONÇA, J. Marques *Subgrupos Congruentes de Grupos Classicos.* Londrina, UEL, 1988. Tese (Mestrado em Matemática.

9 – NEWMAN, M. *Integral Matrices.* Academic Press, 1972.

10 – OGG, A. *Modular Forms and Dirichlet Series.* Benjamin Inc., 1969.

11 – VISWANATHAN, T.M. *Introdução à Algebra e Aritmética.* Monografias de Matemática, IMPA, 1979.

12 – WEIL, A. *Adeles and Algebraic Groups, Lecture Notes.* Institute for Advanced Study, Princeton, 1961.

13 – WITT, E. Eine Identitat Zwischen Modulform Zweiten Grades. *Abh. Math. Semi.*, Hamburg, *14*, 323-337, 1941.

Recebido para publicação em 31.10.89