NOTAS DE MATEMATICAS

No. 99

SOBRE EL NUMERO DE VECTORES ISOTROPOS EN CUERPOS FINITOS

POR

FRANCISCO RIVERO

UNIVERSIDAD DE LOS ANDES
FACULTAD DE CIENCIAS
DEPARTAMENTO DE MATEMATICA
MERIDA VENEZUELA

1988

INTRODUCCION

En este trabajo se obtienen algunas fórmulas para contar el número de vectores isótropos de la forma cuadrática traza sobre un cuerpo finito . Las técnicas utilizadas aquí son del álgebra lineal , puesto que todo cuerpo finito E de p^n elementos , se puede mirar como un espacio vectorial sobre el cuerpo primo F de p elementos .

Existen otros métodos de conteo de vectores isotrópos de una forma cuadrática diagonalizada del tipo

$$q(x) = x_1^2 + x_2^2 + \ldots + \varepsilon x_n^2 ,$$

donde x_i está en F , para toda $1 \leq i \leq n$ y ε es un representante del cociente F^*/ F^{*2} . Por ejemplo , ver Jacobson [5] , Capítulo 6 .

La forma cuadrática traza es de mucha utilidad cuando se estudian espacios cuadráticos del tipo (q , V) donde V es un espacio vectorial sobre un cuerpo E , el cual es a su vez una extensión de F. En esta situación q induce una forma cuadrática $q' : V \longrightarrow F$ definida por $q' = Tr \circ q$.

Otro aspecto importante consiste en la posibilidad de representar elementos en el espacio dual de E , mediante la traza . Si se tiene una aplicación lineal $\varphi : E \longrightarrow F$,

entonces existe un elemento x en E tal que para todo y en E se cumple $\varphi(y) = Tr(xy)$.

Finalmente , si la forma cuadrática traza se diagonaliza se tiene entonces para cada vector $x = (x_1, \ldots, x_n)$ en E

$$Tr(x^2) = a_1 x_1^2 + a_2 x_2^2 + \ldots + a_n x_n^2$$

donde los a_i estan en F .

Luego cada vector isótropo en E , es una solución de la ecuación

$$a_1 x_1^2 + \ldots + a_n x_n^2 = 0 .$$

Este tipo de problema ha sido bastante estudiado desde Gauss , hasta Siegel y Weill . En 1949 Weill publicó unos resultados en relación a este problema en su famoso articulo " Sobre el número de soluciones de ecuaciones en cuerpos finitos " .

1. CONTANDO VECTORES ISOTROPOS EN LA TRAZA

Sea p un número primo y n cualquier número natural. Consideremos $F = F_p$ un cuerpo finito de p elementos y sea $E = F_p n$ una extensión de F de grado n.

La <u>aplicación lineal Traza</u> de E sobre F , se define mediante

$$Tr : E \longrightarrow F$$

$$x \longrightarrow Tr\ (x)\ ,$$

donde

$$Tr\ (x) = \sum \sigma\ (x)\ ,$$

σ recorre todos los elementos del grupo de Galois Gal(E : F).

Considerando E como un espacio vectorial sobre F , se puede definir una <u>forma bilineal simétrica</u> b , sobre E mediante

$$b : ExE \longrightarrow F$$

$$b\ (x,y) = Tr\ (xy).$$

Esta forma bilineal induce una <u>forma cuadrática</u> q sobre E por medio de

$$q : E \longrightarrow F$$

$$q\ (x) = b\ (x,x\ ) = Tr\ (x^2)\ .$$

De esta forma se obtiene un <u>espacio cuadrático</u> (E , q),

al cual denotaremos simplemente por la letra E , cuando no haya riesgo de confusión.

Un vector v en E se llama <u>vector isótropo</u> si $v \neq 0$ y además $q(v) = 0$.

El objetivo de este trabajo es hallar el número de vectores isótropos de E , para todos los valores de p y n.

Asumiremos que p es un número primo distinto de dos . El caso $p = 2$ merece un tratamiento especial y será estudiado al final .

Nótese que para todo vector isótropo v se tiene que v^2 pertenece al núcleo de la traza . Si $N(E,q)$ denota el número de vectores isótropos en E , y τ es el número de cuadrados , distintos de cero en el núcleo de la traza , se obtiene entonces $N(E, q) = 2\tau$.

En lo sucesivo se obtendrán fórmulas para el cálculo de τ , con lo cual se podrá determinar $N(E,q)$.

2. ALGUNOS CASOS ELEMENTALES

En primer lugar, cuando $n = 1$ se tiene $E = F$. En este caso la forma cuadrática traza está dada por $q(x) = x^2$. Luego se tendrá $q(v) = 0$ si y sólo si $v = 0$. Por lo tanto se concluye $N(E, q) = 0$, para $n = 1$.

Para estudiar el caso $n = 2$, necesitamos la siguiente

PROPOSICION 1 . Sea E una extensión de grado dos de $F = F_p$.

Denotemos por τ al número de cuadrados no nulos en el núcleo de la traza $Tr : E \longrightarrow F$. Se tiene entonces :

i) $\tau = 0$, si -1 es un cuadrado en F,

ii) $\tau = p - 1$, si -1 no es un cuadrado en F.

DEMOSTRACION : Nótese que E se puede representar en la forma $E = F(\theta)$, donde θ satisface un polinomio irreducible de grado dos sobre F del tipo $x^2 - \alpha$, con α en F.

Si se mira al cuerpo E como un espacio vectorial sobre F, se tiene la siguiente descomposición :

$$E = F \oplus F\theta.$$

Luego la aplicación lineal traza viene dada por

$$Tr : E \longrightarrow F$$

$$x = a + b\theta \longrightarrow 2a.$$

Por lo tanto el núcleo de la traza se puede escribir como

$$\text{Ker } Tr = \{ x \in E \mid x = b\theta , \ b \in F \}.$$

Denotemos por E^2 al conjunto de todos los cuadrados en E, y sea $x \in \text{Ker } Tr \cap E^2$. Luego existen elementos b,c y d en F , tales que

$$x = b\theta = (c + d\theta)^2 = c^2 + d^2\alpha + 2cd\theta .$$

Igualando términos semejantes nos quedan las ecuaciones

$$c^2 + d^2\alpha = 0 \qquad (1)$$

$$2cd = b \qquad (2)$$

Observese que si $x \neq 0$, entonces se tendrá $c \neq 0$ y $d \neq 0$ De esto se sigue $\alpha = -(c/d)^2$, usando (1). Luego si -1 es un cuadrado en F se va a obtener que α es un cuadrado en F , lo cual contradice la elección de α . Concluimos entonces que la única posibilidad para x es 0 , en este caso . Con esto se prueba la parte i).

A fin de probar la parte ii) , veremos que para cualquier elección de $b \neq 0$ en F , se pueden escoger c y d en F tal que $(c + d\theta)^2 = b\theta$.

Supongamos que en el sistema de ecuaciones 1), 2) se tiene que b es fijo. Entonces el sistema se puede expresar como

$$-(c/d)^2 = \alpha \qquad (3),$$

$$c\,d = b/2 \qquad (4).$$

Poniendo $t = c/d$ en ambas ecuaciones tenemos

$$-t^2 = \alpha \qquad (5)$$

$$t\,d^2 = b/2 \qquad (6).$$

Se ve entonces que hay dos soluciones : t y -t para la parte 5) . Nótese que cuando d recorre F entonces los valores de $t\,d^2$ y $-t\,d^2$ recorren tambien F . Luego se puede hallar d en F tal que la ecuación 6) se satisface . Por lo tanto el sistema original tiene solución para toda $b \neq 0$ en F. Con esto se demuestra la parte ii). □

3. CASO GENERAL : EXTENSIONES DE GRADO IMPAR

Denotaremos por F^2 al conjunto de todos los cuadrados de elementos de F .

LEMA 1. Sea E una extensión finita de grado n , del cuerpo $F = F_p$. Entonces

i) $E^2 \cap F = F$, si n es par ,

ii) $E^2 \cap F = F^2$, si n es impar.

DEMOSTRACION. La parte i) es equivalente a afirmar que todos los elementos del cuerpo base F son cuadrados , cuando se los mira en el cuerpo E.

Puesto que toda extensión de F de grado par ,contiene una extensión de grado dos , haremos la prueba sólo para el caso n = 2 . El caso general se sigue entonces fácilmente de este caso especial.

Sea entonces $E = F(\theta)$, donde θ satisface el polinomio irreducible $x^2 - \alpha$ sobre F, siendo α no cuadrado en F. Obsérvese que F^2 representa el conjunto de todos los cuadrados en F, y $\alpha F^2 = \{ \alpha a \mid a \in F \}$ representa al conjunto de todos los no cuadrados en F. Luego se tendrá

$$F = F^2 \cup \alpha F^2. \qquad (1)$$

Puesto que α es un cuadrado en E , se sigue de (1) que todos los elementos en F son cuadrados en E. Esto concluye la

prueba de i).

La parte ii) equivale a decir que los elementos no cuadrados de F , son no cuadrados al considerarlos como elementos en E.

La prueba será por contradicción.

Supóngase que a ϵ F es no cuadrado en F , pero es un cuadrado en E. Esto es, existe un β en E tal que $\beta^2 = a$. Luego el polinomio $x^2 - a$ es irreducible en F . Consideremos el cuerpo K = F (β) , el cual es una extensión de grado dos de F , y esta contenido en E. Se tiene entonces la siguiente relación entre los grados

$$[E : F] = [E : K] [K : F] = 2 [E : K].$$

Esto contradice la condición [E : F] = n impar . Por lo tanto la parte ii) queda probada. □

Recordemos que si E es una extensión finita de F , se puede considerar a E como un espacio vectorial sobre F . En este sentido se tiene la siguiente :

<u>DEFINICION</u> Sea a un elemento distinto de cero en E . Entonces la <u>recta a través del origen</u> dada por a , F a se define mediante

$$F a = \{ ax \mid x \epsilon F \} .$$

El número total de rectas a través del origen , el cual denotaremos por s , está dado por

$$s = \frac{|E| - 1}{|F| - 1} = \frac{p^n - 1}{p - 1} = p^{n-1} + \ldots + p + 1 .$$

LEMA 2 Sea E una extensión de F de grado impar . Entonces para todo entero positivo k , con $k \leq s$, se tiene que existen elementos $y_1 , \ldots , y_k$ en E tales que

i) Cada y_i es un cuadrado en E

ii) Los y_i yacen en rectas diferentes , esto es si $i \neq j$ se debe tener $F\, y_i \neq F\, y_j$, para todo $i,j \leq k$.

iii) El conjunto formado por la unión de las k rectas

$$E_k = F\, y_1 \cup F\, y_2 \cup \ldots . \cup F\, y_k$$

satisface lo siguiente : La mitad de los elementos no nulos son cuadrados en E_k , y la otra mitad son no cuadrados .

DEMOSTRACION . Si E = F , basta tomar $y_1 = 1$, para probar el resultado.

Supóngase que $E \neq F$, entonces usaremos inducción sobre k Si k = 1 , tómese $y_1 = 1$. Claramente , i) y ii) se satisfacen Para probar iii) se observa que $E_1 = F\, 1 = F$. Obviamente , la mitad de los elementos no nulos de E_1 son cuadrados en E y la otra mitad son no cuadrados. Con esto queda probada la parte iii)

Supongamos ahora que para $t < k$, existen elementos $y_1 , \ldots , y_t$ verificando las propiedades i) - iii) . En el cuerpo E la mitad de los elementos no nulos son cuadrados y

lo mismo se cumple para E_t . De acuerdo a esto , se deduce la existencia de un elemento y_{t+1} en $E \setminus E_t$, el cual es un cuadrado en E . Afirmamos entonces que los elementos $y_1,\ldots,y_{t+1}$ satisfacen i) - iii)

Claramente i) es cierto por la forma como se escogió y_{t+1} También ii) es fácil de verificar. Finalmente se tiene

$$E_{t+1} = E_t \cup F\, y_{t+1} ,$$

Notar que en la recta $F\, y_{t+1}$ la mitad de los elementos no nulos son cuadrados , al igual que en E_t . Por lo tanto E_{t+1} satisface la tercera condición . Con esto queda probado el lema . □

COROLARIO 1 Sea n impar y E una extensión de grado n de F . Sea s el número de rectas a traves del origen en E. Entonces existen elementos $y_1 ,\ldots., y_s$ en E , tales que

i) Cada y_i es un cuadrado en E .

ii) $F\, y_i \cap F\, y_j = \{ 0 \}$, para toda $i \neq j$, $i,j \leq s$.

iii) $E = F\, y_1 \cup F\, y_2 \cup \ldots. \cup F\, y_s$.

DEMOSTRACION Usar el lema 2 en el caso de $k = s$. □

COROLARIO 2 Sea n impar y E una extensión de grado n de F. Sea $Tr : E \longrightarrow F$ la aplicación lineal traza . Entonces se tiene

$$| \text{Ker Tr} \cap E^2 | = \frac{p^{n-1} + 1}{2} .$$

DEMOSTRACION Puesto que la traza es una aplicación F -lineal se sigue que el núcleo de la misma consiste de una unión de rectas . De acuerdo al corolario 1 se pueden tomar elementos $y_{i_1}, \ldots, y_{i_k}$, los cuales son cuadrados en E y además satisfacen

$$\text{Ker Tr} = F\, y_{i_1} \cup F\, y_{i_2} \ldots \cup F\, y_{i_k} .$$

Podemos afirmar entonces , usando el mismo razonamiento del lema 2 , que la mitad de los elementos no nulos del núcleo son cuadrados y la otra mitad son no cuadrados . Por lo tanto se obtiene

$$| \text{Ker Tr} \cap E^2 | = \frac{| \text{Ker Tr} | - 1}{2} + 1$$

$$= \frac{p^{n-1} + 1}{2} .$$

Con esto finaliza la prueba. □

CASO GENERAL : EXTENSIONES DE GRADO PAR

LEMA 3 Sea n par , $n > 2$ y E una extensión finita de F , de grado n . Entonces existe un subcuerpo K de E , el cual es una extensión de F , y tal que $[E:K] = 2$.

DEMOSTRACION Consideremos el grupo de Galois $G = \text{Gal} (E : F)$ el cual es cíclico de orden n . Además $G = \langle \varphi \rangle$, donde φ

es la aplicación de Frobenius definida mediante

$$\varphi : E \longrightarrow E$$

$$x \longrightarrow x^p .$$

Entonces el subgrupo $H = \langle \varphi^2 \rangle$ tiene orden $n/2$. Usando el teorema fundamental de la teoria de Galois se deduce la existencia de un cuerpo K , tal que $F \subset K \subset E$ y además

$$[K:F] = n/2 \quad y \quad [E:K] = 2 .$$

El cuerpo K se define explícitamente

$$K = \{ x \in E \mid \mu (x) = x \text{ , para todo } \mu \text{ en } H \}.$$

Con esto queda probado el lema . □

COMENTARIO Notemos que E es una extensión de grado dos de K y por lo tanto existe un elemento θ en E , tal que E se descompone como K- espacio vectorial

$$E = K + K\,\theta.$$

A continuación invocaremos un resultado muy bien conocidos acerca de la traza .(Ver [2] ,Capitulo 4).

Si se tienen E y K dos extensiones de F , como se vió en el lema anterior , se definen dos trazas

$$Tr \frac{E}{F} : E \longrightarrow F$$

$$x \longrightarrow \sum \sigma (x),$$

donde σ recorre el grupo $G = Gal (E:F)$,

y

$$\mathrm{Tr}\ \frac{E}{K} : E \longrightarrow K$$
$$a + b\,\theta \longrightarrow 2a.$$

Estas dos trazas estan relacionadas mediante

$$\mathrm{Tr}\ \frac{E}{F} = \mathrm{Tr}\ \frac{K}{F} \circ \mathrm{Tr}\ \frac{E}{K}\ .$$

De aqui se sigue $\mathrm{Ker}\ \mathrm{Tr}\ \frac{E}{K} \subset \mathrm{Ker}\ \mathrm{Tr}\ \frac{E}{F}$. Si miramos a E como un grupo aditivo , se tiene

$$E = K + K\,\theta = K + \mathrm{Ker}\ \mathrm{Tr}\ \frac{E}{K}$$

de donde se sigue

$$E = \sum_{a \in K} a + \mathrm{Ker}\ \mathrm{Tr}\ \frac{E}{K} \qquad (1)$$

Analogamente , existen elementos a_1 ,...., a_k en K tales que

$$\mathrm{Ker}\ \mathrm{Tr}\ \frac{E}{F} = \sum_{i=1}^{k} a_i + \mathrm{Ker}\ \mathrm{Tr}\ \frac{E}{K}\ , \quad (2)$$

donde k ,el número de distintas clases laterales , esta dado por

$$k = |\ \mathrm{Ker}\ \mathrm{Tr}\ \frac{E}{F}\ | \ / \ |\ \mathrm{Ker}\ \mathrm{Tr}\ \frac{E}{K}\ | = p^{n-1} / p^{n/2}$$

esto es

$$k = p^{n/2-1}\ .$$

A continuación contaremos el número de cuadrados en el núcleo de la traza de E sobre F , apoyándonos en las fórmulas (1) y (2) .

<u>NOTACION</u> : Al igual que antes , sean E y K dos extensiones de F , tales que $F \subset K \subset E$ y $[\ F: K\ ] = n/2$, $[\ E:K\ ] = 2$. En-

tonces se tienen las notaciones :

τ = número de cuadrados no nulos en Ker Tr $\frac{E}{F}$.

τ_K = número de cuadrados no nulos en Ker Tr $\frac{E}{K}$.

LEMA 4 . Con las notaciones anteriores se tiene

i) $\tau_K = 0$, si -1 es un cuadrado en F ó $n/2$ es par ,

ii) $\tau_K = |K| - 1$, si -1 no es un cuadrado en F y $n/2$ es impar.

DEMOSTRACION . Obsérvese primero que E es una extensión de grado dos de K y que por lo tanto se pueden usar los resultados de la proposición 1 . De acuerdo a esto se tendrá $\tau_K = 0$, si -1 es un cuadrado en K o $\tau_K = |K| - 1$ en caso contrario . Aplicar ahora el lema 1 a los cuerpos K y F , con lo cual se obtiene :

-1 es un cuadrado en K , si y sólo si -1 es un cuadrado en F ó $[K:F] = n/2$ es par .

Con esto queda concluida la prueba. □

LEMA 5 Sea a en K , $a \neq 0$. Entonces el número t de cuadrados en cualquier clase lateral $\bar{a} = a + \text{Ker Tr } \frac{E}{K}$, viene dado por

$$t = \frac{p^n - 1 - 2\,\tau_K}{2\,(p^{n/2} - 1)} .$$

Además , este número no depende del elemento a .

DEMOSTRACION . Probaremos primero que dadas dos clases laterales distintas $\bar{a}_1$ y $\bar{a}_2$, existe una biyección entre ellas que envia cuadrados en cuadrados y no cuadrados en no cuadrados .

Consideremos

$$\pi : a_1 + \text{Ker Tr}\,\frac{E}{K} \longrightarrow a_2 + \text{Ker Tr}\,\frac{E}{K}$$

$$x \longrightarrow a_2\, a_1^{-1}\, x \ .$$

Entonces π es claramente una biyección . Por otro lado el elemento $a_1\, a_2^{-1}$ es un cuadrado en E , de acuerdo al lema 1 , por lo tanto $a_1\, a_2^{-1}\, x$ es un cuadrado en E si y sólo si x es un cuadrado en E. En otras palabras , π manda cuadrados en cuadrados y no cuadrados en no cuadrados.

Finalmente recordemos la relación 1)

$$E = \bigcup_{a \in K} a + \text{Ker Tr}\,\frac{E}{K}$$

Contando los cuadrados no nulos en ambos lados tenemos

$$| E^2 | - 1 = (|K| - 1)\, t + \tau_K$$

$$\frac{p^n - 1}{2} = (p^{n/2} - 1)\, t + \tau_K$$

De donde se sigue

$$t = \frac{p^n - 1 - 2\,\tau_K}{2\,(p^{n/2} - 1)} \ . \ \square$$

PROPOSICION 3 . Sea E una extensión de grado n del cuerpo F, con n par , entonces el número de cuadrados en el núcleo de

la traza $Tr : E \longrightarrow F$, el cual se denota por τ viene expresado por

i) $$\tau = \frac{p^{n-1} - p^{n/2} + p^{n/2-1} - 1}{2} ,$$

si $n/2$ es par ó -1 es un cuadrado en F .

ii) $$\tau = \frac{p^{n-1} + p^{n/2} - p^{n/2-1} - 1}{2} ,$$

si $n/2$ es impar y -1 no es un cuadrado en F .

DEMOSTRACION i) Hemos visto al comienzo de esta sección que el núcleo de la traza se descompone en clases laterales

$$\text{Ker } Tr_F^E = \sum_{i=1}^{k} a_i + \text{Ker } Tr_K^E , \quad (3)$$

donde $k = p^{n/2-1}$.

Contaremos los cuadrados en ambos lados de la ecuación (3) . Se tiene entonces

$$\tau = \#\text{ cuadrados en Ker } Tr_K^E +$$

$$(k-1)\ \#\text{cuadrados en } a + \text{Ker } Tr_K^E , \ a \neq 0$$

$$= \tau_K + (p^{n/2-1} - 1)\left[\frac{p^n - 1 - 2\tau_K}{2(p^{n/2} - 1)}\right] \quad (4)$$

De acuerdo al lema 4 tenemos $\tau_K = 0$; lo cual puede ser reemplazado en (4) para obtener

$$\tau = \frac{(p^{n/2-1} - 1)(p^n - 1)}{2(p^{n/2} - 1)}$$

$$= \frac{(p^{n/2-1} - 1)(p^{n/2} + 1)}{2}$$

$$= \frac{p^{n-1} - p^{n/2} + p^{n/2-1} - 1}{2} .$$

ii) En este caso se tiene $\tau_K = |K| - 1 = p^{n/2} - 1$. Al sustituir τ_K en (4) nos queda

$$\tau = p^{n/2} - 1 + (p^{n/2-1} - 1) \left[\frac{p^n - 1 - 2 (p^{n/2} - 1)}{2 (p^{n/2} - 1)} \right]$$

$$= p^{n/2} - 1 + (p^{n/2 -1} - 1) \left[\frac{p^{n/2} + 1 - 2}{2} \right]$$

$$= p^{n/2} - 1 + \frac{p^{n-1} - p^{n/2} - p^{n/2-1} - 1}{2}$$

$$= \frac{p^{n-1} + p^{n/2} - p^{n/2-1} - 1}{2} .$$

Con esto el caso ii) queda probado . □

5 CASO ESPECIAL p = 2

Sea $F = F_2$ un cuerpo de dos elementos y E una extensión de grado n de F. Al igual que antes , nuestro objetivo será contar el número de cuadrados en el núcleo de la traza .

LEMA 6 . Si la característica del cuerpo E es igual a dos , entonces todos los elementos de E son cuadrados.

DEMOSTRACION . Consideremos la aplicación

$$\varphi : E \longrightarrow E$$

$$x \longrightarrow x2 .$$

Entonces se verifica $\varphi (x_1) = \varphi (x_2)$, si y sólo si

$x_1 = x_2$, para x_1 y x_2 en E . Para ver esto , nótese que $x = -x$, para todo x en E . Luego se sigue que φ es inyectiva y por lo tanto sobre . Esto termina la demostración . □

PROPOSICION 4 . Sea E una extensión de grado n de $F = F_2$. Luego el número de vectores isótropos de la forma cuadrática traza , viene dado por

$$N(E, q) = 2^{n-1} - 1 .$$

DEMOSTRACION . Obsérvese primero que hay tantos vectores isótropos en E como cuadrados no nulos en el núcleo de la traza . De acuerdo a esto y al lema anterior , se tiene

$$\begin{aligned} \#\text{ vectores isótropos} &= |\ \text{Ker Tr} \cap E^2\ | - 1 \\ &= |\ \text{Ker Tr}\ | - 1 \\ &= 2^{n-1} - 1 . \ \square \end{aligned}$$

6 RESUMEN

Podemos juntar todos los casos de n y p en una tabla. Como siempre E es una extensión de grado n del cuerpo primo $F = F_p$ y N (E ,q) denota el número de vectores isótropos de la forma cuadrática traza.

Se tiene entonces :

p	n	N (E,q)
$p \neq 2$	1	0
$p \neq 2$	n impar	$p^{n-1} - 1$
$p \neq 2$	n par , n/2 impar y -1 no cuadrado en F	$p^{n-1} + p^{n/2} - p^{n/2 - 1} - 1$
$p \neq 2$	n par , n/2 par ó -1 cuadrado en F	$p^{n-1} - p^{n/2} + p^{n/2-1} - 1$
$p = 2$	$n > 0$	$2^{n-1} - 1$

BIBLIOGRAFIA

[1] T.Y.Lam — The algebraic theory of quadratic forms
W.A.Benjamin - 1973 . New York.

[2] S.Lang — Algebra - Addison Wesley - 1965 - New York

[3] P.Conner and Robert Perlis — A survey of trace forms on algebraic numbers - World scientific - 1984 - Singapur.

[4] I.Kaplansky — Linear algebra & Geometry .
Alyn and Bacon - Boston - 1969.

[5] N.Jacobson — Basic algebra vol I .
W.H.Freeman - 1974 - San Francisco.