MÁRIO BIAZZI (*)

T E O R E M A

D E

C H E V A L L E Y

ABSTRACT

The important theorem of Chevalley (that deals with the roots of the homogeneous polynimials without a continual term) in the finite fields has several demonstrations. Let's see two of them through distinct ways: one by congruence and the other by working directhy with polynimials in a finite field.

RESUMO:

O importante teorema de Chevalley (que trata das raízes dos polinômios homogêneos sem termo constante) nos corpos finitos tem inúmeras demonstrações. Vejamos duas delas por caminhos distintos: por congruências e trabalhando diretamente com polinômios, num -- corpo finito.

(*) Professor titular de Instrumentação para o Ensino, nesta Faculdade.

TEOREMA DE CHEVALLEY

1a. parte

1. Preliminares

Consideremos congruências mod p, p primo.

As classes de restos, mod p, formam um corpo finito, com p elementos. Ao corpo das classes de restos mod p representaremos Z_p.

Definição: Dois polinômios F e G do anel de Z_p são congruentes se os coeficientes dos termos correspondentes dos dois polinômios são congruentes, módulo p.

Definição: Se para qualquer conjunto de valores $c_1,\dots,c_r$, temos,

$$F(c_1,\dots,c_r) \equiv G(c_1,\dots,c_r) \pmod p$$

então escrevemos $F \sim G$ e dizemos que F e G são equivalentes.

Se $F \equiv G \pmod p$, então $F \sim G$. A recíproca não é verdadeira. x^p e x são equivalentes, pelo pequeno teorema de Fermat, mas não são congruentes, por definição.

Definição: Polinômio reduzido

Se o grau de F em cada uma de suas variáveis x_i, é inferior ou igual p-1 dizemos que F é um polinômio reduzido.

<u>OBS. 1:</u> É interessante observar que se $\alpha_i, \ldots, \alpha_p$, são elementos de Z_p, então o polinômio $(x-\alpha_1)\ldots(x-\alpha_p)$ tem todos os coeficientes não-nulos mas tem valor zero para todo elemento do corpo.

<u>TEOREMA 1</u>

Todo polinômio F é equivalente a um polinômio reduzido F* cujo grau total não é maior que o de F.

Se qualquer variável x_i do polinômio F tem um expoente não menor que p, usamos o pequeno teorema de Fermat e $x_i^p \sim x_i$. Se x_i^s com $s > p$;

$s \geqslant p-1 \quad s = (p-1)q+r \quad \text{com } o \leqslant r < p-1$

$x_i^s = (x_i^{p-1})^q . x_i^r = x_i^r \quad e \quad x_i^s = x_i^r, \text{ com } r < p-1$

Já que a equivalência é preservada na adição e na multiplicação obtemos um polinômio equivalente a F e com grau menor que p. É o reduzido F* de F.

<u>TEOREMA 2</u>

Se dois polinômios reduzidos são equivalentes, eles são congruentes.

Indução finita sobre o número de variáveis.

É suficiente mostrar que se F é reduzido e

$F \sim 0$ então $F \equiv 0 \pmod p$ pois se

$H \sim G$

$H - G \sim 0$, e se

F

$F \sim 0$; $F \equiv 0 \pmod p$ então

$H - G \equiv 0 \pmod p$ e $H \equiv G \pmod p$

$n = 1$ grau $(F(x)) < p$ e $F \sim 0$; $F(c) \equiv 0 \pmod p$

para todo $c \in Z_p$. Mas então F tem mais raizes (p)

que seu grau. Isto só é possível se todos os coeficientes de F são divisíveis por p, isto é,

$F \equiv 0 \pmod p$

$n > 2$, arbitrário

Escrevemos F na forma

$$F(x_1, \ldots, x_n) = A_o(x_1, \ldots, x_{n-1}) + A_1(x, \ldots, x_{n-1})\, x_n +$$

$$\ldots + A_{p-1}(x_1, \ldots, x_{n-1})\, x_n^{p-1}$$

Escolhendo um conjunto arbitrário

$x_1 = c_1, \ldots, x_{n-1} = c_{n-1}$ e supondo $A_o(c_1, \ldots, c_{n-1}) = a_o$

$$A_1(c_1, \ldots, c_{n-1}) = a_1$$

$$- - - - - - - - - - -$$

$A_{p-1}(c_1, \ldots, c_{n-1}) = a_{p-1}$, temos

$F(c_1,\ldots,c_{n-1}, x_n) = a_o + a_1 x_n + \ldots a_{p-1} x_n^{p-1}$ que é um polinômio em x_n equivalente à zero, pois, $F \sim 0$.

Pelo já visto (n=1)

$A_o (c_1 \ldots c_{n-1}) \equiv 0 \pmod p$

$a_1 (c_1 \ldots c_{n-1}) \equiv 0 \pmod p$

- - - - - - - - - - - - - - -

$A_{p-1} (c_1,\ldots,c_{n-1}) \equiv 0 \pmod p$

isto é, $A_o \sim 0$, $A_{p-1} \sim 0$ já que $c_1,\ldots,c_{n-1}$ são arbitrários

São polinômios em n-1 variáveis. Pela hipótese de indução o teorema está demonstrado pois de

$$A_o \equiv 0 \pmod p$$

$$A_1 \equiv 0 \pmod p$$

- - - - - - - -

$$A_{p-1} \equiv 0 \pmod p$$

segue que $F \equiv 0 \pmod p$

<u>TEOREMA 3</u>

Se a congruência $F(x_1,\ldots,x_n) \equiv 0 \pmod p$ tem pelo menos uma solução e o grau do polinômio F é menor que o número de variáveis, então a congruência tem ao menos duas soluções.

Demonstremos por redução ao absurdo.

Suponhamos que o polinômio $F(x_1,\dots,x_n)$ com grau total $\underline{r}$ é tal que $F(x_1,\dots,x_n) \equiv 0 \pmod p$ tenha uma única solução,

$x_1 \equiv a_1 \pmod p \;\dots\; x_n \equiv a_n \pmod p$

Construamos $H(x_1,\dots,x_n) = 1-(F(x_1,\dots,x_n))^{p-1}$

Pelo pequeno teorema de Fermat e pela construção de F, temos

$$H(x_1,\dots,x_n) = \begin{cases} 1 \text{ para } x_1\equiv a_1,\dots,x_n\equiv a_n \pmod p \\ 0 \text{ nos demais casos} \end{cases}$$

Chamemos H* o polinômio reduzido equivalente à H.

Pelo teorema 1, H* assume os mesmos valores que H.

Por outro lado podemos explicitamente construir um polinômio reduzido tomando os mesmos valores.

$$\prod_{i=1}^{n} (1-(x_i-a_i)^{p-1})$$

Pelo teorema 2, temos

$$H^* \equiv \prod_{i=1}^{n} (1-(x_i-a_i)^{p-1}) \pmod p$$

Do teorema 1 segue que o grau de H^* não é maior que o grau de H, isto é, não é maior que $r(p-1)$

O grau de π é igual a $n(p-1)$

Se os polinômios são congruentes, pelo visto acima $n(p-1) \leqslant r(p-1)$ e sendo $p \geqslant 2$,

$n \leqslant r$

Absurdo. Basta lembrarmos da hipótese que $r < n$.

A solução não é única, cqd.

Corolário (Teorema de Chevalley)

Se $F(x_1,\ldots,x_n)$ é uma forma de grau menor que n então a congruência

$$F(x_1,\ldots,x_n) \equiv 0 \pmod p$$

tem solução não-zero.

A existência de solução não trivial segue do teorema 3 já que uma solução, a zero, sempre existe, pois F é uma forma.

TEOREMA 4 (Teorema de Warning)

O número de soluções da congruência $F(x_1,\ldots,x_n) \equiv 0 \pmod p$ é divisível por p, desde que o grau do polinômio $F(x_1,\ldots x_n)$ seja menor que n.

Suponhamos que a congruência tenha s soluções,

$A_i = (a_1^{(i)},\ldots,a_n^{(i)})$ $(i=1, 2, \ldots, s)$

Tomemos $H = 1-F^{p-1}$

É claro que

$$H(x) = \begin{cases} 1 \text{ se } X \equiv A_i \pmod p & (i=1,\ldots,s) \\ 0, \text{ nos outros casos} \end{cases}$$

onde X é a n-upla $(x_1,\ldots,x_n) \in Z_p^{(n)}$. Para qualquer

$A = (a_1,\ldots,a_n)$ formamos o polinômio

$$D_A\ (x_1,\ldots,x_n) = \prod_{j=1}^{n}\ (1-(x_j-a_j)^{p-1})$$

É claro que

$$D_A\ (X) = \begin{cases} 1 \text{ para } X \equiv A \pmod p \\ 0, \text{ nos outros casos} \end{cases}$$

Seja

$$H^*\ (x_1,\ldots,x_n) = D_{A_1}\ (x_1,\ldots,x_n) + \ldots + D_{A_s}\ (x_1,\ldots,x_n)$$

As congruências que definem D_A mostram que H^* toma os mesmos valores que H para qualquer valor de $x_1,\ldots x_n$, isto é, $H^* \sim H$.

Sendo cada um dos polinômios D_{A_i} reduzido, então H^* também é, pelos teoremas 1 e 2, seu grau não excede o grau de H que é igual a $n(p-1)$

Cada D_{A_i} tem grau $n(p-1)$; nominalmente o termo

$(-1)^n(x_1x_2\ldots x_n)^{p-1}$ e temos s desses termos.

Como H^* tem grau menor que $n(p-1)$, o coeficiente desse tal termo tem que ser necessariamente $s\equiv 0 \pmod p$, o que demonstra o teorema.

2a. parte

1. Preliminares

Seja K corpo finito, onde $K = F_q$ com $q=p^f$, p primo e f inteiro positivo.

Definição: 1. Chama-se função polinominal associada a F a aplicação $x\to F(x)$ de K^n em K.

Se esta função polinominal é nula, dizemos que o polinômio F é identicamente nulo.

Observação 1: Todo polinômio F se escreve de uma e uma única maneira; $F = F^* + G$, com F^* o reduzido e G identicamente nulo e o $g(F^*) \leq g(F)$

2. O teorema de Chevalley-Warning

Teorema de Warning

Sejam $F_1,\ldots,F_s$, uma família de s polinômios pertencentes ao anel K (x) de graus $d_1,\ldots,d_s$ respectivamente. Seja ainda V o conjunto das soluções do sistema de equações

$$F_1 = 0,\ldots,F_s=0$$

que pertencem a K^n. Sejam enfim N = card(V) o número de soluções do sistema, em K^n e $d = d_1+\ldots+d_s$ a soma dos graus dos polinômios F_i. Então, se $n > d$, o número N é divisível por p, característica do corpo K.

Introduzamos os dois seguintes polinômios:

$$\overline{F} = (1-F_1^{q-1})\ldots(1-F_s^{q-1})$$

$$\text{e } F_V = \sum_{a\in V} (1-(x_1-a_1)^{q-1}\ldots(1-(x_n-a_n)^{q-1})$$

Temos imediatamente que $\overline{F}$ e F_V tem valor 1 para todo ponto de V e 0 para todos os outros.

O polinômio $G = \overline{F}-F_V$ é identicamente nulo e $\overline{F} = F_V+G$, onde F_V é o reduzido de $\overline{F}$ o que implica $g(F_V) \leq g(\overline{F})$

$$g(F_V) \leq d_1(q-1)+\ldots+d_s(q-1) = d(q-1) < n(q-1)$$

Mas F_V possue o monômio $\pm (x_1^{q-1}\ldots x_n^{q-1})$ de grau $n(q-1)$; o coeficiente desse monômio igual à $(-1)^n N$, deve ser nulo no corpo K de característica p; ou seja N deve ser divisível por p.

Corolário (Teorema de Chevalley)

Mesmos dados e hipóteses ($n>d$) que o teorema anterior.

Se, mais, temos os polinômios F_j $(j=1,\ldots,s)$ sem termo constante, então o sistema admite em $K^{(n)}$ uma solução outra que a solução trivial $(0,0,\ldots,0)$.

Se não existe termo constante temos que $(0,\ldots,0)$ é solução do sistema e logo pertence a V, então $N \geq 1$. Mas N é divisível por p (teorema) donde $N \geq p$ e $N-1 \geq p-1 \geq 2-1 = 1$

$N-1$ é o número de soluções não triviais cqd.

O teorema e seu corolário se aplicam em particular no caso em que $s=1$, de um único polinômio de grau $\underline{d}$ com $\underline{n}$ variáveis e tal que $n > d$. Assim toda forma quadrática com 3 ou mais variáveis, admite solução não trivial num corpo finito K, bem como toda forma cúbica com 4 ou mais variáveis.

BIBLIOGRAFIA

1. Borevich Shafarevich: "Number Theory", Academic Press, N.York, 1970.
2. Joly I.R. "Equations et varietés Algébriques sur un corp fini". Paris, 1968.