Congresso de Pesquisa, Ensino e Extensão

conpeex

ANAIS DO IX CONPPEX

Congresso de Pesquisa, Ensino e Extensão

Economia verde, sustentabilidade e desenvolvimento social

22 a 26 de outubro de 2012

PROGRAMA DE INICIAÇÃO CIENTÍFICA E MESTRADO

PICME

Apoio:

FUNAPE Fundação de Apoio à Pesquisa - UFG

FAPEG Fundação de Amparo à Pesquisa do Estado de Goiás

Governo de Goiás

CAPES

CNPq Conselho Nacional de Desenvolvimento Científico e Tecnológico

Realização:

UFG Universidade Federal de Goiás

POLINÔMIOS CICLOTÔMICOS E TEOREMA DE WEDDERBURN

Matheus Dantas e Lima (mathmatematica@gmail.com)
Orientadora: Prof[a]. Dr[a]. Shirlei Serconek (shirlei@mat.ufg.br)
Instituto de Matemática e Estatística

1. INTRODUÇÃO

Este trabalho apresenta uma breve noção de polinômios ciclotômicos e o Teorema de Wedderburn, um importante resultado de classificação de anéis.

2. DEFINIÇÕES E RESULTADOS PRELIMINARES

Definição 2.1 Seja K um anel de divisão e F um corpo, $F \subset K$. A dimensão de K como um F-espaço vetorial é o grau de K sobre F e será denotada por $[K : F]$.

Lema 2.1 Seja F um corpo finito com q elementos e suponha que $F \subset D$, onde D é um anel de divisão finito. Então D tem q^n elementos, onde $n = [D : F]$.

Lema 2.2 Seja D um anel de divisão e sejam $Z = \{d \in D; dz = zd, \forall z \in D\}$ e $C_D(a) = \{d \in D; ad = da\}$. Então, Z é corpo e $C_D(a)$ é anel de divisão.

Definição 2.2 O corpo Z do lema 2.2 é dito o centro de D. O anel de divisão $C_D(a)$ do lema 2.2 é dito o centralizador de a em D.

Definição 2.3 Seja G um grupo. A cardinalidade de G será chamada a *ordem* de G e será denotada por $|G|$.

Teorema de Lagrange Sejam G um grupo finito e H um subgrupo de G. Então a ordem de H divide a ordem de G.

Equação das classes de conjugação Seja G um grupo finito e $Z(G)$ seu centro. Então,

$$|G| = |Z(G)| + \sum_{\substack{x_i \in G \\ x_i \notin Z(G)}} |C_{x_i}|,$$

onde os x_i são representantes de classes de conjugação distintas.

Teorema 2.1 Sejam G um grupo e C_a uma classe de conjugação de G com representante a. Então, $|C_a| = [G : C_G(a)]$, onde $C_G(a)$ é o centralizador de a no grupo G.

Teorema 2.2 Seja F um corpo e G um subgrupo finito do grupo multiplicativo dos elementos não nulos de F. Então G é um grupo cíclico.

Lema 2.3 Seja q um número inteiro positivo e suponha que $q^n - 1$ divida $q^m - 1$, onde m e n são inteiros positivos. Então n divide m.

3. POLINÔMIOS CICLOTÔMICOS

Considere o polinômio $p(x) = x^n - 1$ como um elemento de $\mathbb{C}[x]$, onde $\mathbb{C}$ denota o conjunto dos números complexos. Em $\mathbb{C}[x]$, $x^n - 1 = \prod(x - \lambda)$, onde λ é um número complexo que satisfaz o polinômio $p(x)$.

Definição 3.1 Um número complexo ζ é dito raiz n-ésima primitiva da unidade se $\zeta^n = 1$ mas $\zeta^m \neq 1$, para todo m, $m < n$ $(m, n \in \mathbb{Z}_+^*)$.

Os números complexos satisfazendo o polinômio $p(x) = x^n - 1$ formam um subgrupo finito, sob a multiplicação, do grupo $\mathbb{C}^*$; logo, pelo Teorema 2.2, esse subgrupo é cíclico.

Definição 3.2 Seja U_n o conjunto de todas as n-ésimas raízes primitivas da unidade. O polinômio

$$\phi_n(x) = \prod_{\zeta \in U_n} (x - \zeta) = \prod_{\substack{s=1 \\ m.d.c.(s,n)=1}}^{n} (x - \zeta^s)$$

é chamado o n-ésimo polinômio ciclotômico.

Da definição acima, temos que

$$\phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\ d<n} \phi_d(x)}$$

Exemplos

- $\phi_1(x) = x - 1$

- $\phi_2(x) = \dfrac{x^2-1}{x-1} = x+1$
- $\phi_3(x) = \dfrac{x^3-1}{x-1} = x^2+x+1$
- $\phi_6(x) = \dfrac{x^6-1}{(x-1)(x+2)(x^2+x+1)} = x^2-x+1$

Reagrupando os termos de forma conveniente no polinômio $p(x)$ obtemos

$$x^n - 1 = \prod_{d|n} \phi_d(x)$$

Vamos agora expor mais dois resultados necessários à demonstração do Teorema de Wedderburn.

Teorema 3.1 Para cada $n \geq 1$, $\phi_n(x)$ é mônico, com coeficientes inteiros.

Demonstração Por indução sobre n. Para $n = 1$, $\phi_1(x) = x - 1$, que é mônico, com coeficientes inteiros. Suponha agora que o teorema vale para $n = r - 1$. Então $\phi_n(x)$ é mônico para todo r, $r|n, r \neq n$. Daí temos que:

$$x^n - 1 = \prod_{d|n} \phi_d(x) = \phi_n(x)g(x)$$

onde $g(x)$ é mônico e com coeficientes inteiros, pela hipótese de indução. Comparando os coeficientes, concluímos que $\phi_n(x)$ é mônico e com coeficientes inteiros, encerrando a demonstração.

Teorema 3.2 Se $d|n$, $d \neq n$, então $\phi_n(x) \left| \dfrac{x^n-1}{x^d-1} \right.$.

4. TEOREMA DE WEDDERBURN

Pequeno Teorema de Wedderburn Todo anel de divisão finito é um corpo.

Demonstração: Seja D um anel de divisão finito e seja Z seu centro (pelo Lema 2.2, Z é corpo). Suponhamos que $|Z| = q$ e que $[D : Z] = n$. Então, pelo Lema 2.1, $|D| = q^n$.

Seja $C_D(a)$ o centralizador de a em D. Então, $C_D(a)$ é um anel de divisão que contém Z e, portanto, $C_D(a)$ é um Z-espaço vetorial. Assim, pelo Lema 2.1, $|C_D(a)| = q^{m(a)}$, onde $m(a) = [C_D(a) : Z]$. Afirmamos que $m(a)$ divide n. Para ver isso, seja $C_D(a)^*$, o conjunto dos elementos não-nulos de $C_D(a)$. Como $C_D(a)$ é anel de divisão, $C_D(a)^*$ é subgrupo de D^* e, pelo

Teorema de Lagrange, $|C_D(a)^*|$ divide $|D^*|$, isto é, $q^{m(a)}-1$ divide q^n-1. Então, pelo Lema 2.3, $m(a)$ divide n.

Consideremos agora a equação de classes do grupo D^*. O centro de D^* é Z^*, donde $|Z^*|=q-1$. Para cada elemento a de D^*, $|C_D(a)^*|=q^{m(a)}-1$, para algum $m(a)\in\mathbb{Z}$.
Pelo Teorema 2.1, $|C_a|=[D^*:C_D(a)^*]=\dfrac{q^n-1}{q^{m(a)}-1}$, onde C_a é a classe de conjugação de a em D^*. Desse modo, a equação de classes do grupo D^* é

$$q^n-1=q-1+\sum_{\substack{m(a)|n\\ m(a)\neq n}}\frac{q^n-1}{q^{m(a)}-1}$$

Seja agora $\phi_n(x)$ o n-ésimo polinômio ciclotômico. Pelo Teorema 3.1, $\phi_n(q)$ é inteiro e, pelo Teorema 3.2, $\phi_n(q)$ divide $\dfrac{q^n-1}{q^{m(a)}-1}$, para cada $m(a)$, onde $m(a)|n$ e $m(a)\neq n$. Temos ainda que $\phi_n(q)$ divide q^n-1 pois $\phi_n(x)$ divide x^n-1. Sendo assim, $\phi_n(q)$ divide $q-1$ (pela equação das classes de conjugação).

Por definição,

$$\phi_n(x)=\prod_{\substack{s=1\\ m.d.c.(s,n)=1}}^{n}(x-\zeta^s)$$

onde ζ é uma n-ésima raiz da unidade. Então, temos que

$$|\phi_n(q)|=\prod_{\substack{s=1\\ m.d.c.(s,n)=1}}^{n}|q-\zeta^s|\geq\prod_{\substack{s=1\\ m.d.c.(s,n)=1}}^{n}(q-1)\geq q-1$$

Mas $\phi_n(q)$ divide $q-1$ e, então, $\phi_n(q)=q-1$. Portanto, $n=1$ e $D=Z$, encerrando a demonstração.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] HERSTEIN, I. N. Topics in Algebra. Chicago: University of Chicago, 1975.

[2] LAM, T. Y. A first course in non-commutative rings. New York: Springer-Verlag, 1991.

[3] LIDL,RUDOLF AND NIEDERREITER, HARALD Finite fields. Cambridge: Cambridge University Press, 1997.