Grupo Multiplicativo de um Corpo Finito

Luan Pereira Bezerra (R.A.: 117681)
Otávio Marçal Leandro Gomide (R.A.: 103696)
Patrícia Marçal (R.A.: 103718)
Priscilla Lima Galcino (R.A.: 103822)

10 de dezembro de 2012

Grupo Multiplicativo de um Corpo Finito

Definição 1. *Seja G um conjunto munido com uma operação binária (g,h)$\longmapsto$ g.h que satisfaz as seguintes condições:*

1. $\forall\ f,\ g,\ h:\ (g.h).f = g.(h.f)$
2. *Existe elemento neutro* $1 \in G$ *tal que* $\forall\ g \in G:\ 1.g = g.1 = g$
3. $\forall\ g \in G, \exists h \in G$ *tal que* $:\ g.h = h.g = 1$, *dizemos que h é o inverso de g e o denotamos por* g^{-1}

Então, dizemos que (G, ·) é um ***grupo multiplicativo****.*

Definição 2. *Seja G um grupo e H um subconjunto não vazio de G, dizemos que H é um* ***subgrupo*** *de G se:*

1. $\forall g,\ h \in H$ *temos que* $gh \in H$
2. $\forall h \in H,\ h^{-1} \in H$

Definição 3. *Seja G um grupo. Se a cardinalidade de G, denotada por |G|, é finita, dizemos que G é um grupo finito. Neste caso, dizemos que |G| é a* ***ordem*** *de G.*

Definição 4. *Seja G um grupo multiplicativo. Dado* $g \in G$, *definimos a* ***ordem do elemento*** *g, denotada por |g|, como o menor inteiro positivo m tal que* $g^m = 1$.

Teorema 1. *(****Lagrange****) Seja (G, ·) um grupo multiplicativo de ordem n, e* $g \in G$. *Então, a ordem do elemento g divide n.*

Demonstração. Seja $|g| = r$, e considere o subconjunto $H := \{1,\ g,\ g^2, \ldots,\ g^{r-1}\}$.

Claramente, H é um subgrupo de G, pois $g^{a+b} = g^a g^b$. Assim, se $a+b < r$, então $g^a g^b \in H$, e se $a + b \geq r$, pelo algoritmo de Euclides para $\mathbb{Z}$, temos que $a + b = qr + s$, com $0 \leq s < r$. Logo:

$$g^a g^b = g^{a+b} = g^{qr+s} = (g^r)^q g^s = 1^q + g^s = g^s \in H$$

$$g^{-a} = (g^a)^{-1}\ e\ g^{-a} = g^{r-a-r} = g^{r-a} g^{-r} = g^{r-a} 1 = g^{r-a} \in H$$

Definimos a seguinte relação:

$$f' \sim f \iff f' \in fH := \{f,\ fg, \ldots,\ fg^{r-1}\}$$

Como H é subgrupo, a relação $\sim$ é claramente reflexiva, simétrica e transitiva. Portanto $\sim$ é uma relação de equivalência e, deste modo, divide os

elementos de G em classes de equivalência disjuntas 2-2, que são dadas por fH com $f \in G$.

Claramente, $|fH| = r,\ \forall f \in G$, deste modo, $|G| = \sum_{f \in T} |fH|$, onde T é o conjunto dos representantes das classes de equivalência de G. Logo, $|G| = r\alpha$, onde α é a cardinalidade de T. Portanto, r *divide* $|G| = n$.

Deste modo, a ordem do elemento g divide n.

□

Corolário 1. *Seja $b \in \mathbb{Z}_n^*$. Então $b^{\phi(n)} \equiv 1\ (mod\ n)$, onde ϕ é a* ***função de Euler****.*

Demonstração. Sabemos que $\mathbb{Z}_n^* := \{a \in \mathbb{Z}_n;\ mdc(a,n) = 1\}$ é um grupo multiplicativo, e a função de Euler ϕ é definida como:

$$\phi(n) := |\{x \in \mathbb{Z};\ 0 < x < n\ e\ mdc(x,n) = 1\}|,\ \forall n \in \mathbb{N}.$$

Assim, $\phi(n) = |\mathbb{Z}_n^*|$.

Seja $b \in \mathbb{Z}_n^*$, pelo Teorema (1), $|b| = r$ divide $|\mathbb{Z}_n^*| = \phi(n)$. Deste modo:

$$b^{\phi(n)} \equiv b^{r\alpha} \equiv (b^r)^\alpha \equiv 1^\alpha \equiv 1\ (mod\ n)$$

□

Corolário 2. *(**Teorema de Euler**) Seja $\mathbb{F}$ um corpo finito com q elementos e seja $b \in \mathbb{F}^*$. Então a ordem de b divide $(q-1)$ e $b^{q-1} = 1$.*

Demonstração. $(\mathbb{F}^*, \cdot)$ é um grupo multiplicativo com $q-1$ elementos. □

Corolário 3. *(**Fermat**) Suponha que p seja primo e $b \in \mathbb{Z}_p$. Então $b^p \equiv b$ (* mod p *).*

Demonstração. $\mathbb{Z}_p$ é um corpo finito com p elementos. Para $b = 0$, a congruência é válida. Se $b \neq 0$, então $b \in \mathbb{Z}_p^*$ e este corolário será válido pelo Teorema de Euler (2). □

Proposição 1. *Suponha que G seja um grupo finito e $b \in G$. Então a ordem de b divide todo inteiro r, tal que $b^r = 1$.*

Demonstração. Seja d a ordem de b, assim $d \leq r$. Se r for dividido por d, teremos a igualdade: $r = d \cdot s + t$, com $0 \leq t \leq d$ sendo o resto e para algum s. Então:

$$1 = b^r = b^{d \cdot s + t} = b^{d \cdot s} \cdot b^t = (b^d)^s \cdot b^t = b^t$$

Como t é estritamente menor que d, isto somente é possível se $t = 0$. □

Proposição 2. *Suponha que G seja um grupo finito e $b \in G$ com ordem igual a r. Seja k um inteiro positivo e considere um elemento $a = b^k \in G$. Então a ordem de $a = b^k$ é igual a:*

$$\frac{r}{mdc(k,r)}.$$

Demonstração. Como $(b^k)^{\frac{r}{mdc(k,r)}} = (b^r)^{\frac{k}{mdc(k,r)}} = 1$, a partir da Proposição (1), temos que a ordem de $a = b^k$ divide o inteiro $\frac{r}{mdc(k,r)}$. Para provar a recíproca, denotamos a ordem de a por t. Então:

$$1 = (b^k)^t = b^{kt}$$

Por isso, r divide $(k \cdot t)$. Então é necessário que: $\frac{r}{mdc(k,r)}$ divida t, que é a ordem de $a = b^k$. □

Para inteiros positivos k, n, denotaremos $k \mid n$, se k dividir n.

Proposição 3. *Seja $n \in \mathbb{N}$, então $\sum_{k|n} \phi(k) = n$.*

Demonstração. Seja d um inteiro tal que $d \mid n$. Defina $A_d = \{r \in \mathbb{Z} \,|\, 1 \leq r \leq n \ , \ mdc(r,n) = d\}$, ou equivalentemente, se $r = ld$, com $l \in \mathbb{Z}$,

$$A_d = \{r \in \mathbb{Z} \,|\, 1 \leq l \leq \frac{n}{d} \ , \ mdc(l, \frac{n}{d}) = 1\}.$$

Logo, $|A_d| = \phi(\frac{n}{d})$.

Observe que se $d \neq d'$, então $A_d \cap A_{d'} = \emptyset$. Ademais $\bigcup_{d|n} A_d = \{r \,|\, 1 \leq r \leq n\}$. Assim:

$$n = \sum_{d|n} |A_d| = \sum_{d|n} \phi(\frac{n}{d}) = \sum_{\frac{n}{d}|n} \phi(\frac{n}{d}) = \sum_{k|n} \phi(k)$$

□

Proposição 4. *Suponha que $\mathbb{F}$ seja um corpo finito com q elementos. Seja d um divisor de $q-1$, então existem $\phi(d)$ elementos em $\mathbb{F}$ com ordem igual a d.*

Demonstração. Seja $a \in \mathbb{F}^*$ tal que a ordem de a é igual a d, então $d \mid (q-1)$. Denote $B_d = \{x \in \mathbb{F} \,|\, ordem\ de\ x = d\}$.

Pela Proposição (2), temos

$$\{a^k \,|\, mdc(k,d) = 1\} \subseteq B_d.$$

Como $\{1, a, a^2, \cdots, a^{d-1}\} \subseteq \{x \in \mathbb{F}^* \,|\, x^d = 1\}$, onde $|\{1, a, \cdots, a^{d-1}\}| = d$ e $|\{x \in \mathbb{F}^* \,|\, x^d = 1\}| \leq d$, temos igualdade de conjuntos.

Logo, $B_d \subseteq \{x \in \mathbb{F}^* \,|\, x^d = 1\} = \{1, a, \cdots, a^{d-1}\}$, e segue que $B_d = \{a^k \,|\, mdc(k, d) = 1\}$, donde $|B_d| = \phi(d)$.

Suponha que d é um divisor arbitrário de $q-1$. Se $B_d = \emptyset$, então $|B_d| = 0$. Se $B_d \neq \emptyset$, então $|B_d| = \phi(d)$. Assim:

$$q - 1 = |\mathbb{F}| = \sum_{d|(q-1)} |B_d| \leq \sum_{d|(q-1)} \phi(d).$$

Pela Proposição (3), $\sum_{d|(q-1)} \phi(d) = q - 1$. Portanto,

$$\sum_{d|(q-1)} \phi(d) = \sum_{d|(q-1)} |B_d| = q - 1,$$

e isto ocorre apenas quando $|B_d| = \phi(d)$ para todos os divisores d de $q-1$. □

Definição 5. *Um grupo G é **cíclico** se existe $g \in G$ tal que $\forall h \in G$ há um inteiro k satisfazendo $h = g^k$. Neste caso, dizemos que g é um elemento **gerador** de G, ou ainda, que G é gerado por g.*

Corolário 4. *Suponha que $\mathbb{F}$ seja um corpo finito. Então, o grupo multiplicativo $(\mathbb{F}^*, \cdot)$ é um grupo cíclico.*

Demonstração. Denote $|\mathbb{F}| = q$. Pela Proposição (4), existem $\phi(q-1)$ elementos de ordem $q-1$ em $\mathbb{F}^*$. Então, cada um desses elementos é um gerador de $\mathbb{F}^*$. □

Referências

[1] I. N. Herstein *Topics in Algebra*, John Wiley & Sons, Inc. (1975).

[2] *Finite Field*, $http://en.wikipedia.org/wiki/Finite_field$ (2012).

[3] *Structure of Finite Fields*, $www.tcs.hut.fi/Studies/T-79.5501/2005AUT/lectures/finitefields.pdf$ (2005).

[4] T. W. Judson *Abstract Algebra - Theory and Applications*, *abstract.ups.edu/* (2009).