NOTAS DE ENSINO

MATEMÁTICA UNIVERSITÁRIA
nº 24/25 – junho/dezembro 1998 – pp. 70-72

A unicidade dos coeficientes de torção de grupos abelianos finitamente gerados

Gervasio G. Bastos

Apresentamos uma prova simples para a unicidade dos coeficientes de torção de grupos abelianos finitamente gerados.

Usaremos notação aditiva para grupos abelianos. Os *coeficientes de torção* de um grupo abeliano finito G são definidos como uma seqüência de números inteiros $d_1, ..., d_r > 1$ tais que $d_1|d_2...|d_r$, e tem-se uma decomposição $G = H_1 \bigoplus H_2 \bigoplus ... \bigoplus H_r$ (*) onde H_i é um subgrupo cíclico de ordem $|H_i| = d_i$ $(i = 1, ..., r)$. Em particular, a definição exclui a possibilidade de somandos triviais. A título de simplificação D. B. Surowski (veja referência abaixo) apresenta uma demonstração indutiva incluindo certa identificação de grupos e uma interessante propriedade de cancelamento em somas diretas de grupos cíclicos. Sua argumentação parte do fato que d_r é o *expoente de* G (= menor inteiro $m \geq 1$ tal que $mx = 0$ para todo $x \in G$). Nesse sentido sua prova *parte de cima para baixo*. Nossa prova é bem mais simples e, como veremos, *parte de baixo para cima*.

Teorema (unicidade dos coeficientes de torção) *A seqüência $d_1, \ldots, d_r$ em (*) é um invariante de G (isto é, enquanto várias decomposições (*) podem ocorrer, os inteiros d_i dependem somente de G).*

*D*emonstração: Utilizaremos indução finita sobre a ordem de G. Quando $|G| = 1$ nosso resultado é verdadeiro por por vacuidade. Para G não trivial aplicaremos a hipótese de indução para grupos com ordem $< |G|$. Com efeito, suponhamos $H_1 \bigoplus ... \bigoplus H_r = G = H'_1 \bigoplus ...H'_s$ duas decomposições como em (*), onde $|H_i| = d_i > 1$ e $|H'_j| = d'_j > 1$. Para cada inteiro $d \geq 1$ e cada subgrupo H de G , denotaremos $dH = \{dx : x \in H\}$ o qual, como se sabe, é um subgrupo de G. Lembramos que todo grupo cíclico finito de ordem n é, a menos de isomorfismo, o grupo $\mathbb{Z}_n$ das classes residuais de inteiros módulo $n \geq 1$, e para cada inteiro $d \geq 1$ tem-se: $d\mathbb{Z}_n \cong \mathbb{Z}_{n/d'}$, onde $d' = mdc(n, d)$.

Afirmação: Os inteiros d_1 e d'_1 *não podem ser* relativamente primos; mais precisamente, d_1 e d'_1 possuem os mesmos divisores primos.

Supondo o contrário, existiria um primo p tal que $p|d_1$ e $p \nmid d'_1$, por exemplo. Como $p||G|$ existe $1 \leq \mu \leq s$ tal que $p|d'_j$ se e somente se $j > \mu$. Assim, $|pH'_j| = d'_j$ para $j \leq \mu$ e $|pH'_j| = \frac{d'_j}{p}$ para $j > \mu$. Temos $d'_\mu|d'_{\mu+1}$ e como $mdc(d'_\mu, p) = 1$ segue que $d'_\mu|\frac{d'_{\mu+1}}{p}$; além disso temos $\frac{d'_{\mu+1}}{p}|\frac{d'_{\mu+2}}{p}|...|\frac{d'_s}{p}$ (é claro que esta notação só faz sentido se $s > \mu + 1$; se não paramos em $\frac{d'_{\mu+1}}{p} = \frac{d'_s}{p}$) e $\frac{d_1}{p}|\frac{d_2}{p}|...|\frac{d_r}{p}$. Como $pH'_1 \neq \{0\}$ tem-se $pG = pH'_1 \bigoplus ... \bigoplus pH'_s \neq \{0\}$. Assim, existe $1 \leq \lambda < r$ tal que $p = d_i$ para $1 \leq i \leq \lambda$, e $p < d_i$ para $\lambda + 1 \leq i \leq r$, donde $pH_{\lambda+1} \bigoplus ... \bigoplus pH_r = pG = pH'_1 \bigoplus ... \bigoplus pH'_s$. Notemos que $1 < \frac{d_{\lambda+1}}{p}|\frac{d_{\lambda+2}}{p}|...|\frac{d_r}{p}$ e $1 < d'_1|d'_2|...|d'_\mu|\frac{d'_{\mu+1}}{p}|...|\frac{d'_s}{p}$ são os coeficientes de torção de pG, e temos $1 < |pG| < |G|$. Segue-se pela hipótese de indução que $r - \lambda = s$, e $\frac{d_{\lambda+1} \cdots d_r}{p^s} = \frac{d'_1 \cdot ... \cdot d'_\mu \cdot d'_{\mu+1} \cdot ... \cdot d'_s}{p^{s-\mu}}$. Daí, segue-se $|G| \geqslant d_{\lambda+1} \cdot ... \cdot d_r = d'_1 \cdot ... \cdot d'_s \cdot p^\mu = |G| \cdot p^\mu$, e como $\mu \geqslant 1$ temos um absurdo.

Dividimos agora nossa prova em dois casos.

Caso 1: d_1 e d'_1 não são primos. Pela afirmação existe um primo p dividindo (propriamente) d_1 e d'_1. Neste caso temos $pH_1 \bigoplus ... \bigoplus pH_r = pG = pH'_1 \bigoplus ... \bigoplus pH'_s$ e $1 < |pG| < |G|$. Segue-se por indução que $r = s$ and $\frac{d_i}{p} = \frac{d'_i}{p}$, isto é, $d_i = d'_i$ $(i = 1, ..., r)$.

Caso 2: d_1 ou d'_1 é primo. Então, pela afirmação, devemos ter $d_1 = d'_1 = d($ primo$)$, e assim existem $1 \leqslant \lambda \leqslant r$, e $1 \leqslant \mu \leqslant s$, tais que $(d_i = d'_j = d) \Leftrightarrow (i \leqslant \lambda$ e $j \leqslant \mu)$. A condição $\lambda = r$ (analogamente quando $\mu = s$) implica $\{0\} = dG = dH'_1 \bigoplus ... \bigoplus dH'_s$, isto é, $d'_j = d$ para todo j. Portanto, $d^r = |G| = d^s$, isto é, $r = s$. Resta examinar a possibilidade $\lambda < r$ and $\mu < s$. Ora, neste caso $dH_{\lambda+1} \bigoplus ... \bigoplus dH_r = dG = dH'_{\mu+1} \bigoplus ... \bigoplus dH'_s$, com $1 < |dG| < |G|$. Ainda por indução obtemos $r - \lambda = s - \mu := t$ e $\frac{d_{\lambda+k}}{d} = \frac{d_{\mu+k}}{d}$, isto é, $d_{\lambda+k} = d_{\mu+k}$ $(k =$

$1, ..., t)$. Segue-se finalmente $d^\lambda \cdot d_{\lambda+1} \cdot ... \cdot d_{\lambda+t} = d^\mu \cdot d_{\mu+1} \cdot ... \cdot d_{\mu+t}$, o que implica $\lambda = \mu$, isto é, $r = s$ e $d_i = d'_i$ para cada $i = 1, ..., r$.

Referência

D.B. Surowski, *The uniqueness aspect of the fundamental theorem of finite abelian groups*. Amer. Math. Monthly, *102,No.2* (1995), pp.162-163.