Numero di automorfismi di un gruppo abeliano finito

Giacomo Mezzedimi

8 Ottobre 2014

In questo articolo ci proponiamo di calcolare il numero di automorfismi di un generico gruppo abeliano finito.

Proposizione 1. *Siano H e K gruppi abeliani finiti tali che $(|H|, |K|) = 1$. Allora:*

$$Aut(H \times K) \cong Aut(H) \times Aut(K).$$

Proof. Definiamo $\phi : Aut(H) \times Aut(K) \to Aut(H \times K)$ tale che, dati $\sigma \in Aut(H)$, $\tau \in Aut(K)$, $\phi(\sigma, \tau)(h, k) = (\sigma(h), \tau(k))$ $\forall h \in H, k \in K$.

É evidentemente una buona definizione, in quanto $\sigma(h) \in H$ e $\tau(k) \in K$.

Vediamo che ϕ é un omomorfismo di gruppi:

$$\phi(\sigma_1\sigma_2, \tau_1\tau_2)(h, k) = ((\sigma_1\sigma_2)(h), (\tau_1\tau_2)(k));$$

$$\phi(\sigma_1, \tau_1)\phi(\sigma_2\tau_2)(h, k) = \phi(\sigma_1, \tau_1)(\sigma_2(h), \tau_2(k)) = (\sigma_1(\sigma_2(h)), \tau_1(\tau_2(k))),$$

ed evidentemente i risultati coincidono $\forall \sigma_1, \sigma_2 \in Aut(H)$, $\forall \tau_1, \tau_2 \in Aut(K)$, $\forall h \in H, k \in K$.

Resta da vedere che ϕ é bigettiva: l'iniettivitá é ovvia perché funzioni con le stesse immagini coincidono; vediamo la surgettivitá.

Sia $\psi \in Aut(H \times K)$; poniamo $p = |H|$ e $q = |K|$.

Siano $\pi_H : H \times K \to H$ e $\pi_K : H \times K \to K$ le proiezioni naturali su H e K.

Definiamo $\alpha : K \to H$ tale che $\alpha(k) = \pi_H(\psi(1_H, k))$ e $\beta : H \to K$ tale che $\beta(h) = \pi_K(\psi(h, 1_K))$, dove 1_H é l'identitá di H e 1_K é l'identitá di K.

Allora, $\forall k \in K$:

$$1_H = \pi_H(\psi(1_H, k))^p = \pi_H(\psi(1_H, k)^p) = \pi_H(\psi(1_H, k^p)) = \alpha(k^p),$$

dove le uguaglianze seguono dal fatto che ψ e π_H sono omomorfismi.

Dunque $\{k^p | k \in K\} \subseteq Ker(\alpha)$.

Ma poiché $(p, q) = 1$, allora $\{k^p | k \in K\} = K$, quindi $Ker(\alpha) = K$, cioé α é l'omomorfismo banale.

Analogamente, si prova che β é l'omomorfismo banale.

Poniamo $\psi_H : H \to H$ tale che $\psi_H(h) = \pi_H(\psi(h, 1_K))$ e $\psi_K : K \to K$ tale che $\psi_K(k) = \pi_K(\psi(1_H, k))$.

Allora:

$$\psi(h,k) = \psi(h,1_K)\psi(1_H,k) = (\pi_H(\psi(h,1_K)\psi(1_H,k)), \pi_K(\psi(h,1_K)\psi(1_H,k)) =$$

$$= (\psi_H(h)\alpha(k), \beta(h)\psi_K(k)) = (\psi_H(h), \psi_K(k)) = \phi(\psi_H, \psi_K)(h,k).$$

Resta da vedere che $\psi_H \in Aut(H)$, $\psi_K \in Aut(K)$.

Poiché H e K sono finiti, basta l'iniettivitá.

Sia $\widetilde{h} \in Ker(\psi_H)$; allora:

$$\psi(\widetilde{h}, 1_K) = (\psi_H(\widetilde{h}), \psi_K(1_K)) = (1_H, 1_K),$$

dunque $\widetilde{h} = 1_H$, poiché ψ é iniettiva. □

Corollario. *Siano $H_1, \ldots, H_n$ gruppi abeliani finiti tali che $(|H_i|, |H_j|) = 1$ $\forall i, j$. Allora:*

$$Aut(H_1 \times \ldots \times H_n) \cong Aut(H_1) \times \ldots \times Aut(H_n).$$

Proof. Segue dalla precedente proposizione con un'immediata induzione. □

Teorema (Teorema di struttura per i gruppi abeliani finiti)**.** *Sia G un gruppo abeliano finito. Allora:*

$$G \cong G_{p_1} \times \ldots \times G_{p_n},$$

per certi p_i primi, e:

$$G_p = \mathbb{Z}/p^{e_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{e_k}\mathbb{Z}.$$

Per quanto visto precedentemente, e poiché $(p_i, p_j) = 1$ $\forall i, j$, si ha:

$$Aut(G) \cong Aut(G_{p_1}) \times \ldots \times Aut(G_{p_n}).$$

In particolare:

Corollario. $|Aut(G)| = \prod_{i=1}^{n} |Aut(G_{p_i})|$.

Dunque ci limitiamo a studiare il numero di automorfismi di gruppi del tipo:

$$G_p = \mathbb{Z}/p^{e_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{e_k}\mathbb{Z}.$$

Notazione. *Denotiamo con* $\pi_i : \mathbb{Z} \to \mathbb{Z}/p^{e_i}\mathbb{Z}$ *la proiezione* $\pi_i(a) = \overline{a}$*, dove* $\overline{a}$ *é la classe di* a *modulo* p^{e_i}*. Allo stesso modo* $\pi : \mathbb{Z}^k \to G_p$ *é la proiezione tale che* $\pi(a_1, \ldots, a_k) = (\overline{a_1}, \ldots, \overline{a_k})$*.*

Proposizione 2. *Siano* $a, b \in \mathbb{N}$ *tali che* $a < b$*. Allora:*

$$\varphi : \mathbb{Z}/p^a\mathbb{Z} \to \mathbb{Z}/p^b\mathbb{Z} | \varphi(\overline{1}) = \overline{m},$$

é un omomorfismo $\iff$ $p^{b-a}|m$*.*

Proof. $\Rightarrow$) Poiché φ é un omomorfismo, allora $ord(\overline{m})|ord(\overline{1})$, cioé $ord(\overline{m})|p^a$. Sia $ord(\overline{m}) = p^s$, con $s \leq a$. Allora $p^s\overline{m} = \overline{0}$, cioé $p^b|p^s m \Rightarrow p^{b-s}|m \Rightarrow p^{b-a}|p^{b-s}|m$.

$\Leftarrow$) L'immagine di $\overline{1}$ é ben definita, poiché, se $m = p^{b-a}k$, allora $p^a\overline{m} = \overline{0}$, quindi $ord(\overline{m})|p^a = ord(\overline{1})$. Dominio e codominio sono ciclici, quindi tutto l'omomorfismo é definito ($\varphi(\overline{k}) = \overline{k} \cdot \overline{m}$). □

Proposizione 3. $\varphi : \mathbb{Z}/p^a\mathbb{Z} \to \mathbb{Z}/p^{e_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{e_k}\mathbb{Z}$ *tale che* $\varphi(\overline{1}) = (\overline{m_1}, \ldots, \overline{m_k})$ *é un omomorfismo* $\iff$ $p^{e_i-a}|m_i \ \forall e_i > a$*.*

Proof. Per definire φ basta definirlo su ciascuna componente, quindi la proposizione segue da quella precedente. □

Notazione. *Data una matrice* $A = (a_{ij})$ $k \times k$*, denotiamo* $\pi(A) = (\overline{a_{ij}})$*, dove la riga* i*-esima é modulo* p^{e_i}*.*

Rappresenteremo un endomorfismo $\phi \in End(G_p)$ come una matrice.

Diremo che $M_\phi = (a_{ij})$ rappresenta ϕ se $\pi(M_\phi)\overline{b_i} = \phi(\overline{b_i})$ $\forall i$, dove $\overline{b_i}$ é il vettore con tutti 0 e 1 nella i-esima componente

Infatti in questo modo viene definito tutto l'endomorfismo, in quanto una matrice é un'applicazione lineare.

Dunque π é un omomorfismo.

Da ora in poi considereremo $e_i \geq e_j$ se $i \geq j$.

Proposizione 4. $A = (a_{ij})$ *rappresenta un certo* $\phi \in End(G_p)$ $\iff$ $p^{e_i-e_j}|a_{ij}$ *se* $e_i \geq e_j$ *(cioé* $i \geq j$*).*

Proof. ϕ viene definito dalla immagini di e_i $\forall i$, dunque la proposizione segue immediatamente da (Prop. 3). □

Proposizione 5. $A = (a_{ij})$ *rappresenta l'omomorfismo banale* $\iff$ $p^{e_i}|a_{ij}$ $\forall i, j$*.*

Proof. Le due implicazioni sono ovvie, poiché se la riga i-esima é divisibile per p^{e_i}, allora in $\pi(A)$ la riga i-esima é nulla modulo p^{e_i}. □

Notazione. *Sia* $F : \mathcal{M}_k(\mathbb{Z}) \to \mathcal{M}_k(\mathbb{F}_p)$ *tale che* $F((a_{ij})) = ([a_{ij}]_p)$*, dove* $[a]_p$ *é la classe di* a *modulo* p*.*

Proposizione 6. *F é un omomorfismo surgettivo.*

Proof. Immediata verifica. □

Proposizione 7. *Sia* $A = (a_{ij}) \in \mathcal{M}_k(\mathbb{Z})$ *e sia* $\pi(A)$ *l'endomorfismo di* G_p *rappresentato da* A*. Allora:*

$$\pi(A) \in Aut(G_p) \iff F(A) \in GL_k(\mathbb{F}_p).$$

Proof. $\Rightarrow$) $\pi(A) \in Aut(G_p) \Rightarrow A \in GL_k(\mathbb{Z})$, poiché se A non fosse invertibile, si avrebbe che $\exists v \in Ker(A)$, $v \neq 0$, cioé che $\pi(A)(\overline{v}) = (\overline{0}, \ldots, \overline{0})$, assurdo, poiché $\pi(A) \in Aut(G_p)$.

Ma allora $\exists B \in \mathcal{M}_k(\mathbb{Z})$ tale che $AB = BA = I$.

Questo implica che $F(A)F(B) = F(I)$, cioé che $F(A) \in GL_k(\mathbb{F}_p)$.

$\Leftarrow$) Se $F(A) \in GL_k(\mathbb{F}_p)$, allora $\exists B^* \in GL_k(\mathbb{F}_p)$ tale che $F(A)B^* = F(I)$.

Ma F é surgettiva, quindi $\exists B | F(B) = B^*$.

Allora $F(AB) = F(A)F(B) = F(I)$, quindi:

$$AB = I + pC,$$

con $C \in \mathcal{M}_k(\mathbb{Z})$.

Vediamo che $(AB)^{p^k} = I + p^{k+1}C_k^*$, per una certa matrice C^*, $\forall k$.

Poiché abbiamo visto che una matrice pensata come endomorfismo é nulla se le righe sono divisibili per una certa potenza di p, allora per un certo k avremo che $\pi(p^{k+1}C_k^*)$ é l'endomorfismo nullo.

Quindi $\exists k$ tale che:

$$\pi((AB)^{p^k}) = \pi(I),$$

che implica immediatamente che $\pi(A) \in Aut(G_p)$. □

Dunque segue immediatamente che:

Corollario. $|Aut(G_p)| = |\{\pi(M) \in End(G_p) | F(M) \in GL_k(\mathbb{F}_p)\}|$.

Quindi cerchiamo di contare le matrici $A = (a_{ij})$ tali che $p^{e_i - e_j} | a_{ij}$ se $i \geq j$ che sono invertibili in $GL_k(\mathbb{F}_p)$.

Supponiamo che la lista $[e_1, \ldots, e_k]$ sia cosí composta:
$[r_1, \ldots, r_1, r_2, \ldots, r_2, \ldots, r_z, \ldots, r_z]$, dove il numero r_i si ripete s_i volte.

Allora una tale matrice si presenta in questa forma:

$$F(A) = \left(\begin{array}{c|c|c} J_1 & * & * \\ \hline 0 & \ddots & * \\ \hline 0 & 0 & J_z \end{array}\right)$$

Gli 0 sotto i blocchi della diagonale derivano dal fatto che $p^{e_i-e_j}|a_{ij}$ e $e_i > e_j$, dunque c'é almeno un fattore p.

Sulla sovradiagonale ci puó essere qualsiasi numero, con la condizione che $\det(F(A)) \neq 0$.

Questa condizione é equivalente a:

$$\det(J_i) \neq 0, \forall 1 \leq i \leq z.$$

L'i-esimo blocco diagonale é un blocco $s_i \times s_i$, dunque le scelte totali per l'i-esimo blocco diagonale (affinché sia invertibile) sono:

$$(p^{s_i} - 1)(p^{s_i} - p) \dots (p^{s_i} - p^{s_i-1}) = \prod_{j=0}^{s_i-1} (p^{s_i} - p^j),$$

poiché il primo vettore colonna deve essere $\neq 0$, il secondo non deve appartenere alla retta generata dal primo e cosí via.

Dunque in totale le scelte per i blocchi diagonali sono:

$$\prod_{i=1}^{z} \prod_{j=0}^{s_i-1} (p^{s_i} - p^j).$$

A questo punto dobbiamo moltiplicare queste possibilitá per tutte le scelte sulla sovradiagonale, che sono:

$$\prod_{t=1}^{z-1} p^{s_t(\sum_{d=t+1}^{z} s_d)}.$$

A questo punto la parte diversa da 0 si solleva secondo un fattore p^{e_i-1} per ogni elemento della riga i-esima, mentre la parte uguale a 0 si solleva secondo un fattore $p^{e_i-(e_i-e_j)} = p^{e_j}$ per ogni elemento della riga j-esima.

Dunque:

$$|Aut(G_p)| = \prod_{i=1}^{z} \prod_{j=0}^{s_i-1} (p^{(r_i-1)s_i}(p^{s_i} - p^j)) \prod_{t=1}^{z-1} p^{r_t s_t (k-l_t)} \prod_{c=1}^{z-1} \prod_{d=1}^{s_c} p^{e_j(k-l_d)},$$

dove $l_t = s_1 + \ldots + s_t$.

REFERENCES:
http://www.msri.org/people/members/chillar/files/autabeliangrps.pdf per (Prop. 1).