Università degli studi di Cagliari

Dipartimento di Matematica e Informatica

Tesi di laurea triennale

AUTOMORFISMI DI GRUPPI ABELIANI FINITI

Candidato:
Marco Casula
Matr. 60/64/65275

Relatore:
Prof. Andrea Loi

Anno accademico 2020/2021

Ringraziamenti

Nel giorno di questo mio piccolo traguardo personale vorrei ringraziare innanzitutto il mio relatore, il Prof. Andrea Loi, ambasciatore di un corpo docente che mi ha letteralmente sbalordito in questi 3 anni. Durante la stesura di questo lavoro mi ha continuamente stimolato a crescere professionalmente ma soprattutto umanamente, dandomi consigli e suggerimenti tra cui, primo fra tutti, l'insegnamento che "l'umiltà è alla base di tutto".

Vorrei poi dedicare questa tesi in primis alla mia famiglia, che mi ha sempre lasciato la libertà di inseguire i miei sogni quando tutti avrebbero detto di studiare altro: sono orgoglioso di farne parte.

In secundis non posso non citare tutti i miei amici, di cui non riporto i nomi solo per brevità, ma che in un modo o nell'altro mi hanno sempre aiutato a non isolarmi dalla realtà (rischio che credo sia alto studiando cose troppo astratte) e a farmi divertire nonostante ci vedessimo meno spesso.

Infine ringrazio di cuore Giorgia e la sua bellissima famiglia, ormai parte integrante della mia vita, a cui rivolgo gli auguri per questo traguardo che stiamo raggiungendo insieme e che spero sia il primo di tanti altri.

Marco Casula

Sommario

In questa tesi si studia il gruppo degli automorfismi di un gruppo abeliano finito e viene calcolato il suo ordine.

Abstract

In this thesis we study the Automorphisms' group of a finite Abelian group and we compute its order.

Indice

1 Introduzione

Come introduzione alle classi algebriche astratte, ci si imbatte tipicamente nella classificazione dei gruppi abeliani finiti.

Teorema 1.1 (di decomposizione primaria)**.** *Sia G un gruppo abeliano finito. Allora G è isomorfo al prodotto di gruppi della forma*

$$H_p = \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_n}}$$

dove p è un numero primo e $1 \leq e_1 \leq \cdots \leq e_n$ sono interi positivi.

Molto meno conosciuto, comunque, è il fatto che esista una descrizione di $\mathrm{Aut}(G)$, il gruppo degli automorfismi di G. La prima caratterizzazione completa che è giunta a noi è contenuta in un articolo di Ranum, verso l'inizio del secolo scorso, e solo recentemente è stato scritto l'articolo [1] su cui si basa la nostra esposizione. Il nostro obiettivo è colmare questo vuoto, così da fornire una più moderna e accessibile trattazione.

La nostra caratterizzazione di $\mathrm{Aut}(G)$ è suddivisa in 3 step.

La prima osservazione è che possiamo lavorare con il più elementare gruppo H_p. Questa riduzione è consentita dal fatto che, dati due gruppi con cardinalità coprime (come accade nel nostro caso scrivendo $G = H_p \times H_q \times \cdots \times H_s$), allora *il prodotto dei gruppi di automorfismi coincide col gruppo degli automorfismi del prodotto.*

Successivamente utilizzeremo il Teorema 3.4 per descrivere lo anello degli endomorfismi di H_p come quoziente di un sottoanello delle matrici $\mathbb{Z}^{n\times n}$.

Infine le unità $\mathrm{Aut}(H_p) \subset \mathrm{End}(H_p)$ saranno identificate con questa costruzione.

Come conseguenza della nostra trattazione, otterremo una formula esplicita per il numero di elementi di $\mathrm{Aut}(G)$ per ogni gruppo abeliano finito.

2 Prodotto di Automorfismi

Sia $G = H \times K$ prodotto di gruppi H e K, dove le cardinalità di H, K sono due numeri interi coprimi. E' naturale chiedersi come gli automorfismi di G siano legati a quelli di H e K.

Lemma 2.1. *Siano H, K gruppi fiiniti con $|H| = n$, $|K| = m$, $(n, m) = 1$. Allora*

$$\mathrm{Aut}(H) \times \mathrm{Aut}(K) \simeq \mathrm{Aut}(H \times K)$$

Dimostrazione. Siano $\alpha \in \mathrm{Aut}(H)$ e $\beta \in \mathrm{Aut}(K)$ e definiamo $\Phi(\alpha, \beta) \in \mathrm{Aut}(H \times K)$ come $\Phi(\alpha, \beta)(h, k) = (\alpha(h), \beta(k))$. Si ha che:

- $\Phi(\alpha, \beta)$ *è omomorfismo*:

$$\begin{aligned}\Phi(\alpha,\beta)[(h_1,k_1)(h_2,k_2)] &= \Phi(\alpha,\beta)(h_1h_2, k_1k_2)\\ &= (\alpha(h_1h_2), \beta(k_1k_2))\\ &= (\alpha(h_1)\alpha(h_2), \beta(k_1)\beta(k_2))\\ &= (\alpha(h_1), \beta(k_1))(\alpha(h_2), \beta(k_2))\\ &= \Phi(\alpha,\beta)(h_1,k_1)\Phi(\alpha,\beta)(h_2,k_2)\end{aligned}$$

- $\Phi(\alpha, \beta)$ *è suriettiva*: preso $(h, k) \in H \times K$ allora $h \in H, k \in K$. Pertanto poichè α, β sono automorfismi $\exists \bar{h} \in H, \bar{k} \in K$ tali che $\alpha(\bar{h}) = h \wedge \beta(\bar{k}) = k$ quindi

$$\Phi(\alpha, \beta)(\bar{h}, \bar{k}) = (\alpha(\bar{h}), \beta(\bar{k})) = (h, k)$$

- $\Phi(\alpha, \beta)$ *è iniettiva*: siano $(h_1, k_1), (h_2, k_2) \in H \times K$ tali che $\Phi(\alpha, \beta)(h_i, k_i) = (x, y),\ i = 1, 2$ (ossia hanno stessa immagine tramite $\Phi(\alpha, \beta)$). Allora

$$\begin{aligned}(\alpha(h_1), \beta(k_1)) = (\alpha(h_2), \beta(k_2)) &\implies \alpha(h_1) = \alpha(h_2) \wedge \beta(k_1) = \beta(k_2)\\ &\implies h_1 = h_2 \wedge k_1 = k_2\end{aligned}$$

  per l'iniettività di α, β e $\Phi(\alpha, \beta)$ è iniettiva.

Siano $id_H \in \mathrm{Aut}(H), id_K \in \mathrm{Aut}(K)$ gli automorfismi identità di H, K. Per provare che Φ è omomorfismo, si osservi che $\Phi(id_H, id_K) = id_{H\times K}$ e che

$$\begin{aligned}\Phi(\alpha_1\alpha_2, \beta_1\beta_2)(h,k) &= (\alpha_1\alpha_2(h), \beta_1\beta_2(k))\\ &= \Phi(\alpha_1,\beta_1)(\alpha_2(h), \beta_2(k))\\ &= \Phi(\alpha_1,\beta_1)\Phi(\alpha_2,\beta_2)(h,k)\end{aligned}$$

$\forall \alpha_1, \alpha_2 \in \mathrm{Aut}(H), \beta_1, \beta_2 \in \mathrm{Aut}(K), (h, k) \in H \times K$.

Ora, Φ è in particolare un isomorfismo. E' chiaro che Φ sia iniettiva, infatti dati $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in \mathrm{Aut}(H \times K)$ tali che la loro immagine tramite Φ coincida, allora

$$\begin{aligned} \Phi(\alpha_1, \beta_1)(h,k) = \Phi(\alpha_2, \beta_2)(h,k) &\implies (\alpha_1(h), \beta_1(k)) = (\alpha_2(h), \beta_2(k)) \\ &\implies \alpha_1(h) = \alpha_2(h) \quad \wedge \quad \beta_1(k) = \beta_2(k) \\ &\implies \alpha_1 = \alpha_2 \quad \wedge \quad \beta_1 = \beta_2 \end{aligned}$$

per l'arbitrarietà di h, k, ossia Φ è iniettiva.

Resta perciò da mostrare la suriettività. Posti $n = |H|, m = |K|$ e indicate con π_H, π_K le proiezioni canoniche, fissiamo $\omega \in \mathrm{Aut}(H \times K)$ e consideriamo l'omomorfismo $\gamma \colon K \to H$ dato da $\gamma(k) = \pi_H(\omega(1_H, k))$ dove 1_H è l'elemento neutro di H.

Si ha che

$$\{\, k^n \mid k \in K \,\} \subseteq \mathrm{Ker}(\gamma)$$

infatti

$$\gamma(k^n) = \pi_H(\omega(1_H, k^n)) = \pi_H(\omega(1_H, k)^n) = \pi_H(\omega(1_H, k))^n = 1_H$$

dove nell'ultima uguaglianza abbiamo sfruttato il Teorema di Lagrange. Inoltre, poichè $(n, m) = 1$, l'insieme $\{\, k^n \mid k \in K \,\}$ ha m elementi. Se consideriamo infatti l'applicazione $f \colon K \to K$ definita come $f(k) = k^n$, essa è iniettiva in quanto

$$k^n \in \mathrm{Ker}(f) \iff k^n = 1_K \iff o(k) \mid n$$

ma poichè, sempre per il Teorema di Lagrange, deve essere anche $o(k) \mid m$ allora si ottiene che $o(k) = 1$ ossia $k = 1_K$; di conseguenza f è anche suriettiva quindi

$$\{\, k^n \mid k \in K \,\} = \mathrm{Im}(f) = K$$

Conseguentemente, segue che $\mathrm{Ker}(\gamma) = K$ e γ è l'omomorfismo banale (ossia $\gamma(k) = 1_H, \ \forall k \in K$). Similmente, $\delta \colon H \to K$ dato da $\delta(h) = \pi_K(\omega(h, 1_K))$ è banale ($\delta(h) = 1_K, \ \forall h \in H$). Infine, definiamo gli endomorfismi di H e K come

$$\omega_H(h) = \pi_H(\omega(h, 1_K)) \qquad \omega_K(k) = \pi_K(\omega(1_H, k))$$

e con questa costruzione e per quanto sopra abbiamo che

$$\omega(h,k) = \omega(h, 1_K)\omega(1_H, k) = (\omega_H(h), \omega_K(k)) = \Phi(\omega_H, \omega_K)(h,k)$$

$\forall h \in H, k \in K$.

Resta da provare che ω_H, ω_K sono automorfismi, ma poichè H, K hanno cardinalità finita è sufficiente mostrarne l'iniettività. A tal scopo supponiamo che $h \in \mathrm{Ker}(\omega_H)$. Allora $\omega(h, 1_K) = (1_H, 1_K)$ ossia, poichè ω è automorfismo, $h = 1_H$ il che implica che $\mathrm{Ker}(\omega_H) = \{1_H\}$ da cui ω_H è iniettiva. Analogamente si dimostra che $\omega_K \in \mathrm{Aut}(K)$, e questo completa la dimostrazione. $\square$

Sia ora p un numero primo. L'ordine di $H_p = \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_n}}$ è (si vede facilmente) $p^{e_1+\cdots+e_n}$. Poichè G è isomorfo ad un prodotto finito di gruppi della forma H_p con un insieme di p distinti, il Lemma 2.1 implica, come accennato nell'introduzione, che studiare $\mathrm{Aut}(H_p)$ non lede la generalità per caratterizzare $\mathrm{Aut}(G)$. Di conseguenza ci concentreremo sulla caratterizzazione del gruppo $\mathrm{Aut}(H_p)$ con p primo e $1 \leq e_1 \leq \cdots \leq e_n$ interi positivi.

3 Endomorfismi di H_p

Per poter sviluppare la nostra caratterizzazione, sarà necessario dare una descrizione di $E_p = \mathrm{End}(H_p)$, l'anello degli endomorfismi di H_p. Gli elementi di E_p sono omomorfismi di gruppi da H_p in sè, con le operazioni di composizione e addizione, dove quest'ultima è definita come

$$(A + B)(h) := A(h) + B(h)$$

dove $A, B \in \mathrm{End}(H_p), h \in H_p$. Questo anello si comporta similmente agli anelli di matrici, con qualche notevole differenza che discutiamo qui sotto.

Il gruppo ciclico $C_{p^{e_i}} = \mathbb{Z}_{p^{e_i}}$ corrisponde al gruppo additivo degli interi modulo p^{e_i}, di cui denoteremo con g_i il generico generatore.

Con questa rappresentazione, un elemento di H_p è un vettore colonna $(\overline{h_1}, \ldots, \overline{h_n})^T$ in cui ogni $\overline{h_i} \in \mathbb{Z}_{p^{e_i}}$ e $h_i \in \mathbb{Z}$ è un rappresentante.

Definizione 3.1. Con queste notazioni, definiamo il seguente insieme di matrici:

$$R_p = \left\{ (a_{ij}) \in \mathbb{Z}^{n\times n} \;\middle|\; p^{e_i - e_j} \mid a_{ij} \quad \forall i, j \text{ tali che } 1 \leq j \leq i \leq n \right\}$$

Esempio 3.2. Siano $n = 3, e_1 = 1, e_2 = 2, e_3 = 5$, allora:

$$R_p = \left\{ B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ pb_{21} & b_{22} & b_{23} \\ p^4 b_{31} & p^3 b_{32} & b_{33} \end{bmatrix} \;\middle|\; b_{ij} \in \mathbb{Z} \right\}$$

In generale, è chiaro che R_p è chiuso rispetto alla addizione e che la matrice identità $I_n \in R_p$, infatti data δ_{ij} un' entrata di I_n, allora

- $i = j \Rightarrow p^{e_i - e_i} = p^0 = 1 \mid 1 = \delta_{ii}$
- $i > j \Rightarrow p^{e_i - e_j} \mid 0 = \delta_{ij}$

Risulta che, con anche la moltiplicazione matriciale, questo insieme è un anello, come dimostra il seguente lemma:

Lemma 3.3. *R_p è un anello rispetto alle operazioni di somma e prodotto matriciale.*

Dimostrazione. Siano $A, B \in R_p$. La chiusura rispetto all'operazione di somma è un facile esercizio (in particolare rispetto all'addizione questo è un gruppo abeliano). Ponendo $A = (a_{ij}), B = (b_{jk})$, le condizioni che $p^{e_i - e_j}$ divida a_{ij}, $p^{e_j - e_k}$ divida b_{jk}, $\forall i, j, k$ implicano che

$$p^{e_i - e_k} = p^{e_i - e_j} p^{e_j - e_k} \mid a_{ij} b_{jk}$$

ossia R_p è chiuso anche rispetto al prodotto. □

Sia $\pi_i \colon \mathbb{Z} \to \mathbb{Z}_{p^{e_i}}$ la proiezione canonica sul quoziente data da $\pi_i(h) = \bar{h}$, e sia $\pi \colon \mathbb{Z}^n \to H_p$ l'omomorfismo dato da

$$\pi(h_1, \dots, h_n)^T = (\pi_1(h_1), \dots, \pi_n(h_n))^T = (\overline{h_1}, \dots, \overline{h_n})^T$$

Potremmo dare ora una descrizione di E_p come un quoziente dell'anello delle matrici R_p. In altri termini, il prossimo teorema dice che un endomorfismo di H_p è il prodotto tra una matrice $A \in R_p$ e un vettore di rappresentanti interi (delle classi modulo p^{e_i}), seguito dalla proiezione π.

Teorema 3.4. *L'applicazione* $\Psi \colon R_p \to \mathrm{End}(H_p)$ *data da*

$$\Psi(A)(\overline{h_1}, \dots, \overline{h_n})^T = \pi(A(h_1, \dots, h_n)^T)$$

è un omomorfismo suriettivo di anelli.

Dimostrazione. Per prima cosa verifichiamo che $\Psi(A)$ è ben definita come applicazione da H_p in sè. Sia $A = (a_{ij}) \in R_p$ e supponiamo che $(\overline{r_1}, \dots, \overline{r_n})^T = (\overline{s_1}, \dots, \overline{s_n})^T$ con r_i, s_i interi, ossia $p^{e_i} \mid r_i - s_i \quad \forall i = 1, \dots, n$. La k-esima entrata del vettore dato dalla differenza $\pi(A(r_1, \dots, r_n)^T) - \pi(A(s_1, \dots, s_n)^T)$ è

$$\begin{aligned}\pi_k\Big(\sum_{i=1}^n a_{ki} r_i\Big) - \pi_k\Big(\sum_{i=1}^n a_{ki} s_i\Big) &= \pi_k\Big(\sum_{i=1}^n a_{ki} r_i - \sum_{i=1}^n a_{ki} s_i\Big) \\ &= \sum_{i=1}^n \pi_k\Big(\frac{a_{ki}}{p^{e_k - e_i}} p^{e_k - e_i}(r_i - s_i)\Big) = \bar{0}\end{aligned}$$

in quanto $p^{e_k} \mid p^{e_k - e_i}(r_i - s_i)$ per $k < i$ e $p^{e_k} \mid (r_i - s_i)$ per $k \geq i$. Inoltre, poichè π, A sono entrambe lineari, segue che $\Psi(A)$ è lineare, perciò $\Psi(A) \in \mathrm{End}(H_p), \ \forall A \in R_p$ e Ψ è ben definita.

Per provare la suriettività di Ψ, sia $\omega_i = (0, \dots, 0, g_i, 0, \dots, 0)^T$ il vettore con g_i nell'i-esima componente e zero altrove. Un endomorfismo $M \in \mathrm{End}(H_p)$ è determinato dall'immagine di ciascun ω_i: infatti poichè gli endomorfismi sono in particolare omomorfismi, essi sono lineari rispetto all'operazione del gruppo, ossia se $\overline{h_i}$ è la i-esima entrata di un vettore di $H_p, \exists z \in \mathbb{Z}$ tale che $\overline{h_i} = z g_i$, da cui segue che

$$M(\overline{h_i}) = M(z g_i) = z M(g_i) = z M(\omega_i)$$

ossia $M(\overline{h_i})$ dipende dall'immagine degli ω_i (N.B: con abuso di notazione si è indicato con $M(\overline{h_i})$ l'immagine tramite M del vettore $(0, \dots, 0, \overline{h_i}, 0, \dots, 0)$).

Inoltre se $M(\omega_j) = (\overline{h_{1j}}, \dots, \overline{h_{nj}})^T = \pi(h_{1j}, \dots, h_{nj})^T$ per qualche intero h_{ij}, allora

$$0 = M(0) = M(p^{e_j} \omega_j) = M\omega_j + \dots + M\omega_j = (\overline{p^{e_j} h_{1j}}, \dots, \overline{p^{e_j} h_{nj}})^T$$

da cui segue che $p^{e_i} \mid p^{e_j} h_{ij},\ \forall i,j$, ossia $p^{e_i - e_j} \mid h_{ij}$ per $i \geq j$. Ottenendo così la matrice $H = (h_{ij}) \in R_p$ abbiamo che $\Psi(H) = M$ per costruzione, e questo prova che Ψ è suriettiva.

Resta infine da mostrare che Ψ è omomorfismo di anelli. Chiaramente $\Psi(I_n) = id_{E_p}$ e anche $\Psi(A+B) = \Psi(A) + \Psi(B)$. Ciò può essere visto con un calcolo diretto:

$$\begin{aligned} \Psi(I_n)(\overline{h_1}, \ldots, \overline{h_n})^T &= \pi(I_n(h_1, \ldots, h_n)^T) = \pi((h_1, \ldots, h_n)^T) \\ &= (\overline{h_1}, \ldots, \overline{h_n})^T \implies \Psi(I_n) = id_{E_p} \end{aligned}$$

$$\begin{aligned} \Psi(A+B)(\overline{h_1}, \ldots, \overline{h_n})^T &= \pi((A+B)(h_1, \ldots, h_n)) \\ &= \pi(A(h_1, \ldots, h_n)^T + B(h_1, \ldots, h_n)^T) \\ &= \pi(A(h_1, \ldots, h_n)^T) + \pi(B(h_1, \ldots, h_n)^T) \\ &= \Psi(A)(\overline{h_1}, \ldots, \overline{h_n})^T + \Psi(B)(\overline{h_1}, \ldots, \overline{h_n})^T \end{aligned}$$

Se poi $A, B \in R_p$ allora si verifica facilmente che $\Psi(AB)$ è la composizione degli endomorfismi $\Psi(A) \circ \Psi(B)$ per le proprietà del prodotto matriciale. Quindi Ψ è omomorfismo di anelli. □

Data questa descrizione di $\mathrm{End}(H_p)$, si possono caratterizzare quegli endomorfismi che in particolare appartengono a $\mathrm{Aut}(H_p)$. Prima di iniziare questa discussione, il lettore faccia riferimento al Primo Teorema di Omomorfismo [2, pag. 232].

Calcoliamo quindi il nucleo dell'applicazione Ψ definita nel Teorema 3.4.

Lemma 3.5. *Il nucleo di Ψ è dato dall'insieme delle matrici $A = (a_{ij}) \in R_p$ tali che $p^{e_i} \mid a_{ij},\ \forall i,j$.*

Dimostrazione. Come prima sia $\omega_j = (0, \ldots, 0, g_j, 0, \ldots, 0)^T \in H_p$ un vettore con g_j nella j-esima entrata e zero altrove. Se $A = (a_{ij}) \in R_p$ ha la proprietà che $p^{e_i} \mid a_{ij},\ \forall i,j$ allora

$$\Psi(A)(\omega_j) = (\pi_1(a_{1j}), \ldots, \pi_n(a_{nj})) = 0$$

In particolare, poichè ogni $h \in H_p$ è una combinazione lineare a coefficienti interi degli ω_j, segue che $\Psi(A)h = 0,\ \forall h \in H_p$ ossia

$$\{\ A = (a_{ij}) \in R_p \mid p^{e_i} \mid a_{ij} \quad \forall i,j\ \} \subseteq \mathrm{Ker}(\Psi)$$

Viceversa sia $A = (a_{ij}) \in R_p$ tale che $\Psi(A)\omega_j = 0,\ \forall \omega_j$, ossia per i calcoli precedenti ogni a_{ij} è divisibile per p^{e_i} e

$$\mathrm{Ker}(\Psi) \subseteq \{\ A = (a_{ij}) \in R_p \mid p^{e_i} \mid a_{ij} \quad \forall i,j\ \}$$

□

Il Teorema 3.4 ed il Lemma 3.5 danno insieme una caratterizzazione esplicita dell'anello $\mathrm{End}(H_p)$ come quoziente $R_p/\ker(\Psi)$.

Proseguendo questa discussione, calcoliamo $\mathrm{Aut}(H_p)$ (le unità di $\mathrm{End}(H_p)$): a tal scopo premettiamo i seguenti due lemmi, il primo dei quali deriva dalla teoria elementare delle matrici.

Lemma 3.6 (Matrice aggiunta)**.** *Sia $A \in \mathbb{Z}^{n\times n}$ con $\det(A) \neq 0$. Allora $\exists! B \in \mathbb{Q}^{n\times n}$ (detta* matrice aggiunta *di A) tale che*

$$AB = BA = \det(A) I_n$$

Inoltre B ha entrate in $\mathbb{Z}$, ossia $B \in \mathbb{Z}^{n\times n}$.

Dimostrazione. Deriva direttamente dal fatto che l'inversa di A è $A^*/\det(A)$ dove A^* indica la matrice dei cofattori di A le cui entrate, essendo i complementi algebrici ottenuti tramite somme e prodotti delle entrate di A, sono numeri interi, ossia A^* è la matrice cercata. □

Lemma 3.7. *Una matrice A appartiene a R_p se e solo se esiste una decomposizione*

$$A = PA'P^{-1}$$

in cui $A' \in \mathbb{Z}^{n\times n}$ e $P = diag(p^{e_1}, \ldots, p^{e_n})$.

Dimostrazione. Sia $A = (a_{ij}) \in R_p$. Allora $p^{e_i - e_j} \mid a_{ij}$ ossia esiste $\alpha_{ij} \in \mathbb{Z}$ tale che $a_{ij} = p^{e_i - e_j}\alpha_{ij}$. Segue che

$$a_{ij} = p^{e_i} \cdot \alpha_{ij} \cdot \frac{1}{p^{e_j}} = [PA'P^{-1}]_{ij}$$

con $A' = (\alpha_{ij})$ e $P = \mathrm{diag}(p^{e_1}, \ldots, p^{e_n})$.

Viceversa se $A = PA'P^{-1}$ con A', P come nell'enunciato allora

$$a_{ij} = p^{e_i} \cdot \alpha_{ij} \cdot \frac{1}{p^{e_j}} = p^{e_i - e_j}\alpha_{ij}$$

ossia $p^{e_i - e_j} \mid a_{ij}$ e $A \in R_p$, come volevasi dimostrare. □

Ponendo $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$, il seguente è una descrizione completa di $\mathrm{Aut}(H_p)$.

Teorema 3.8. *Un endomorfismo $M = \Psi(A)$ è un automorfismo se e solo se $A(\mathrm{mod} p) \in GL_n(\mathbb{F}_p)$.*

Dimostrazione. Iniziamo con una piccola premessa. Fissata una matrice $A \in R_p$ con $\det(A) \neq 0$, per il Lemma 3.6 $\exists B \in \mathbb{Z}^{n\times n}$ tale che $AB = BA = \det(A) I_n$. Vorremmo mostrare che B è in particolare un elemento di R_p. Per dimostrarlo sia $A = PA'P^{-1}$ per qualche $A' \in \mathbb{Z}^{n\times n}$ e sia $B' \in \mathbb{Z}^{n\times n}$ tale che $A'B' = B'A' = \det(A') I_n$ (sempre per il Lemma 3.6).

Sia dunque $C = PB'P^{-1}$. Poichè $\det(A) = \det(A')$ segue che

$$AC = (PA'P^{-1})(PB'P^{-1}) = PA'B'P^{-1} = \det(A)I_n = PB'A'P^{-1} = CA$$

ma per l'unicità di B segue dal lemma che $B = C = PB'P^{-1}$ ossia $B \in R_p$ per il Lemma 3.7.

Dimostriamo dunque il teorema:

"$\Longleftarrow$"

Supponiamo che $p \nmid \det(A)$, allora $A \pmod p \in GL_n(\mathbb{F}_p)$ (infatti $\det(A) \neq 0$ e A è invertibile) e sia $s \in \mathbb{Z}$ l'inverso di $\det(A)$ modulo p^{e_n} (il quale esiste poichè $p \nmid \det(A)$ e p è primo, perciò $(p, \det(A)) = 1$ e $(p^{e_n}, \det(A)) = 1$). Notiamo che vale anche che $\det(A) \cdot s \equiv 1 \pmod{p^{e_j}}$, $\forall 1 \leq j \leq n$. Sia B la matrice aggiunta di A come definita nel Lemma 3.6. Definiamo $A^{(-1)} := sB$ e mostriamo che la sua immagine tramite Ψ è l'inversa dell'endomorfismo $\Psi(A)$, infatti

$$\Psi(A^{(-1)}) \circ \Psi(A) = \Psi(A^{(-1)}A) = \Psi(AA^{(-1)}) = \Psi(s \cdot \det(A)I_n) = id_{E_p}$$

quindi $\Psi(A) \in \mathrm{Aut}(H_p)$.

"$\Longrightarrow$"

Viceversa se $\Psi(A) = M$ e $\Psi(C) = M^{-1}$ (ossia esiste inversa di $\Psi(A)$ ed essa è automorfismo), allora

$$\Psi(AC - I_n) = \Psi(AC) - id_{E_p} = 0$$

ossia $AC - I_n \in \mathrm{Ker}(\Psi) = \{ X = (x_{ij}) \in R_p \mid p^{e_i} \mid x_{ij},\ \forall i, j \}$ per il Lemma 3.5, ossia $p \mid (AC - I_n)_{ij}$ da cui $AC \equiv I_n \pmod p$. Di conseguenza

$$1 = \det(I_n) \equiv \det(AC) = \det(A)\det(C) \pmod p$$

quindi in particolare $p \nmid \det(A)$ ed il teorema segue. □

Come semplice applicazione di quanto appena visto, consideriamo il caso in cui $e_i = 1$, $\forall i = 1, \ldots, n$. In tal caso H_p può essere visto come il più familiare spazio vettoriale $\mathbb{F}_p^n$ e $\mathrm{End}(H_p) \simeq M_n(\mathbb{F}_p)$, anello delle matrici $n \times n$ a coefficienti sul campo $\mathbb{F}_p$.

Il Teorema 3.8 diventa allora la semplice affermazione che $\mathrm{Aut}(H_p)$ corrisponde all'insieme $GL_n(\mathbb{F}_p) \subset M_n(\mathbb{F}_p)$ delle matrici invertibili.

4 Cardinalità degli automorfismi di H_p

Per convincere ulteriormente il lettore dell'utilità del Teorema 3.8, esporremo brevemente come contare il numero di elementi in $\mathrm{Aut}(H_p)$ usando tale caratterizzazione. Invocando il Lemma 2.1, si può trovare una formula esplicita per calcolare il numero di automorfismi di un qualsiasi gruppo abeliano finito. Si seguono due passaggi:

1. trovare tutti gli elementi di $GL_n(\mathbb{F}_p)$ che possono essere estesi ad una matrice $A \in R_p$ che rappresenti un endomorfismo;
2. calcolare tutti i modi distinti di estendere ogni elemento ad un automorfismo.

Definiamo i seguenti $2n$ numeri:

$$d_k = \max\{\, l : e_l = e_k \,\} \qquad c_k = \min\{\, l : e_l = e_k \,\}$$

Ovviamente poichè $e_k = e_k$ si ha che $d_k \geq k \quad \wedge \quad c_k \leq k$.

Dobbiamo trovare tutte le matrici $M \in GL_n(\mathbb{F}_p)$ della forma

$$M = \begin{bmatrix} m_{11} & m_{12} & \dots & m_{1n} \\ \vdots & & & \vdots \\ m_{d_1 1} & & & \vdots \\ 0 & m_{d_2 2} & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & m_{d_n n} \end{bmatrix} = \begin{bmatrix} m_{1e_1} & \dots & \dots & \dots & \dots & m_{1n} \\ \vdots & m_{2e_2} & & & & \vdots \\ \vdots & & \ddots & & & \vdots \\ 0 & \dots & & m_{ne_n} & \dots & m_{nn} \end{bmatrix}$$

Si veda [2, pag. 136] per il successivo lemma. Riportiamo qui tale risultato per comodità del lettore.

Lemma 4.1. *Si ha che l'anello $GL_n(\mathbb{F}_p)$ ha cardinalità pari a*

$$|GL_n(\mathbb{F}_p)| = \prod_{k=1}^{n} (p^n - p^{k-1})$$

Dimostrazione. Affinchè una matrice M appartenga a $GL_n(\mathbb{F}_p)$ deve essere $\det(M) \neq 0$, ossia per la definizione di determinante questo implica che, se denotiamo con $\alpha_i = (a_{i1}, \dots, a_{in})$ l'i-esimo vettore riga per $i = 1, \dots, n$, allora i vettori $\alpha_1, \dots, \alpha_n$ sono linearmente indipendenti. Pertanto contiamo quante scelte si hanno per ogni riga.

Per la prima riga α_1 abbiamo $p^n - 1$ scelte. Il vettore α_2 non deve appartenere al sottospazio generato da α_1, quindi abbiamo $p^n - p$ scelte. Il vettore α_i non deve essere combinazione lineare dei precedenti vettori $\alpha_1, \dots, \alpha_{i-1}$ già fissati, cioè non deve appartenere al sottospazio vettoriale

da essi generato che deve avere dimensione $i-1$. Quindi si hanno $p^n - p^{i-1}$ scelte per l'i-esimo vettore riga α_i. Concludiamo che

$$|GL_n(\mathbb{F}_p)| = (p^n-1)(p^n-p)(p^n-p^2)\dots(p^n-p^{n-2})(p^n-p^{n-1})$$

□

Abbiamo così che, per le matrici della forma sopra, esse sono in numero pari a $\prod_{k=1}^{n}(p^{d_k}-p^{k-1})$ se richiediamo solo colonne linearmente indipendenti come nella dimostrazione del Lemma 4.1.

Per estendere poi ogni elemento m_{ij} da $\overline{m_{ij}} \in \mathbb{Z}_p$ a $\overline{a_{ij}} \in p^{e_i-e_j}\mathbb{Z}_{p^{e_i}}$ tale che $a_{ij} \equiv m_{ij} \pmod{p}$ ci sono p^{e_j} modi per farlo per le entrate necessariamente nulle (ad esempio quelle che si ottengono quando $e_i > e_j$), cosicchè ogni elemento di $p^{e_i-e_j}\mathbb{Z}/p^{e_i}\mathbb{Z}$ lo verificherà, oltre ai p^{e_i-1} modi per le entrate non necessariamente nulle ($e_i \leq e_j$) così da poter aggiungere ogni elemento di $p\mathbb{Z}/p^{e_i}\mathbb{Z}$.

Quanto appena detto prova il seguente risultato:

Teorema 4.2. *Il gruppo abeliano $H_p = \mathbb{Z}_{p^{e_1}} \times \dots \times \mathbb{Z}_{p^{e_n}}$ ha un numero di automorfismi pari a*

$$|\operatorname{Aut}(H_p)| = \prod_{k=1}^{n}(p^{d_k}-p^{k-1}) \prod_{j=1}^{n}(p^{e_j})^{n-d_j} \prod_{i=1}^{n}(p^{e_i-1})^{n-c_i+1}$$

Riferimenti bibliografici

[1] Christopher J. Hillar, Darren L. Rhea (2007), *Automorphisms of Finite Abelian Groups*, Mathematical Association of America.

[2] Dikran Dikranjan, Maria Silvia Lucido (2007), *Aritmetica e algebra*, Liguori Editore.