CAPITOLO B

Gruppi Abeliani Finitamente Generati

Data la notevole importanza dei gruppi abeliani finitamente generati nello studio delle matematica astratta e della fisica teorica, questo capitolo tratterà la struttura dei:

- gruppi abeliani finiti;
- gruppi abeliani liberi finitamente generati;
- gruppi abeliani misti finitamente generati.

Questa suddivisione ci permette di analizzare i gruppi abeliani finitamente generati in base all'ordine (finito o infinito) dei propri elementi.

Per quanto riguarda i gruppi abeliani finiti, si presentano tre metodi per decomporre un gruppo abeliano finito. Si stabiliscono per tale obbiettivo il teorema fondamentale dei gruppi abeliani finiti, il teorema di decomposizione primaria ciclica ed il suo corollario, la decomposizione in p-gruppi finiti. Con questi teoremi, inoltre, saremo in grado di ottenere il numero di gruppi abeliani tra loro non isomorfi di ordine n, numero naturale fissato, ma ci sarà utile un breve studio sulle partizioni e sulla funzione generatrice che ci permetterà di semplificare notevolmente i vari calcoli.

Proseguiremo lo studio dei gruppi abeliani liberi finitamente generati e dimostreremo che sono il prodotto diretto di un certo numero di gruppi ciclici isomorfi a $(\mathbb{Z}, +)$; mentre per i gruppi abeliani misti finitamente generati dimostreremo che sono isomorfi al prodotto diretto di gruppi ciclici che possono essere p-gruppi (come nel caso dei gruppi abeliani finiti) o sottogruppi isomorfi a $(\mathbb{Z}, +)$ (come nel caso dei gruppi abeliani liberi finitamente generati). Infine, vengono approfonditi le partizioni e teorema di Hall sugli automorfismi dei p-gruppi abeliani finiti.

B1. Teorema fondamentale dei gruppi abeliani finiti

Siano G un gruppo e g un elemento di G. Ricordiamo che *ordine* di g è stato definito come il più piccolo intero positivo n tale che $g^n = e$ ed indicato con

$o(g) = n$. Allora per ogni numero naturale m, vale che $g^{mn} = e$. Viceversa, abbiamo il seguente:

Lemma B1.1. *Siano G un gruppo e $g \in G$ un elemento di ordine finito $o(g) = n < \infty$. Allora per un intero m, valgono:*

(a) *g^m è l'elemento neutro di G se e solo se $n|m$.*
(b) *$o(g^m) = n/\mathrm{mcd}(m, n)$ per qualunque numero intero m diverso da zero.*

DIMOSTRAZIONE. Se $n|m$, esiste un intero ℓ tale che $m = n\ell$. Allora abbiamo che $g^m = (g^n)^\ell = e^\ell = e$. Ora, supponiamo per assurdo che $n \nmid m$, allora esistono q, r interi tali che $m = nq + r$ con $0 < r < n$, quindi $g^m = g^{nq+r} = g^r \cdot (g^n)^q = g^r$. Da qui si evince che se $g^m = e$ vale anche $g^r = e$ con $0 < r < n = o(g)$, che contraddice il fatto che l'ordine di g è uguale ad n.

Sia $d := \mathrm{mcd}(m, n)$, allora esistono m' e n' interi coprimi tali che $m = m'd$ e $n = n'd$. Osserviamo che

$$(g^m)^{n'} = (g^{m' \cdot d})^{n'} = (g^n)^{m'} = e$$

inoltre per ogni k tale che $(g^m)^k = e$ vale che $n'|k$.

Infatti, se $(g^m)^k = e$ si ha $g^{mk} = e$, quindi per l'osservazione precedente $o(g) = n$ e $n|(mk)$ per cui $(n'd)|(m'dk)$ cioè $n'|(m'k)$; essendo n' e m' coprimi, allora $n'|k$. Abbiamo così ottenuto $o(g^m) = n' = n/\mathrm{mcd}(n, m)$. □

Lemma B1.2. *Siano G un gruppo abeliano e $x, y \in G$ due elementi di ordine m e n rispettivamente. Allora*

(a) *l'ordine di xy divide* $\mathrm{mcm}(m, n)$.
(b) *in particolare, si ha che $o(xy) = mn$ se* $\mathrm{mcd}(m, n) = 1$.
(c) *esiste un elemento in G il cui ordine è* $\mathrm{mcm}(m, n)$.

DIMOSTRAZIONE. Ricordando che esistono due interi $m_1, n_1 \in \mathbb{N}$ tali che $\mathrm{mcm}(m, n) = m_1 m = n_1 n$, quindi

$$(xy)^{\mathrm{mcm}(m,n)} = x^{\mathrm{mcm}(m,n)} y^{\mathrm{mcm}(m,n)} = x^{mm_1} y^{nn_1} = e.$$

Per Lemma **B1.1**, $\mathrm{mcm}(m, n)$ è multiplo di $o(xy)$, cioè $o(xy)|\mathrm{mcm}(m, n)$.

Vogliamo ora dimostrare che se $\mathrm{mcd}(m, n) = 1$ vale $o(xy) = mn$. È evidente che $(xy)^{mn} = e$, inoltre mn è il minimo numero verificante la proprietà $(xy)^{mn} = e$. Infatti, se k un generico intero tale che $(xy)^k = e$, dato che G è abeliano vale che $x^k = y^{-k}$. Non sarà difficile verificare che k è un multiplo di mn.

Elevando ambo i membri a m si ottiene $x^{mk} = y^{-mk} = e$ dato che $o(x) = m$, cioè $o(y) = n|(mk)$ per Lemma **B1.1**. Secondo il teorema di Euclide, si ha che $n|k$ dato che $\mathrm{mcd}(m, n) = 1$.

Analogamente, elevando ambo i membri della stessa a n si ha che $x^{nk} = y^{-nk} = e$, quindi $o(x) = m|(nk)$. A questo punto otteniamo che $m|k$.

Richiamando $\mathrm{mcd}(m, n) = 1$, possiamo concludere che $(nm)|k$, cioè ogni intero k tale che $(xy)^k = e$ è multiplo di mn.

Secondo il teorema fondamentale dell'aritmetica, possiamo scrivere

$$m = \prod_k p_k^{\lambda_k} \quad \text{e} \quad n = \prod_k p_k^{\mu_k}$$

dove $\{p_k\}$ sono un numero finito di primi distinti e $\{\lambda_k, \mu_k\}$ numeri interi non negativi.

Allora valgono le seguenti relazioni:

$$\begin{aligned} \mathrm{mcd}(m, n) &= \prod_k p_k^{\min(\lambda_k, \mu_k)}, \\ \mathrm{mcm}(m, n) &= \prod_k p_k^{\max(\lambda_k, \mu_k)}. \end{aligned}$$

Per un sottoinsieme dei numeri naturali definito da

$$\sigma = \{k \mid \lambda_k \geq \mu_k\}$$

introduciamo due divisori di m e n rispettivamente con

$$m' = \prod_{k \in \sigma} p_k^{\lambda_k} \qquad \text{e} \qquad n' = \prod_{k \notin \sigma} p_k^{\mu_k}.$$

Si vede subito che $m'n' = \mathrm{mcm}(m, n)$ con $\mathrm{mcd}(m', n') = 1$.

Per due elementi $x' = x^{m/m'}$ e $y' = y^{n/n'}$, possiamo stabilire i loro ordini come segue:

$$\begin{aligned} o(x') = o\big(x^{m/m'}\big) &= \frac{m}{\mathrm{mcd}(m, m/m')} = m', \\ o(y') = o\big(y^{n/n'}\big) &= \frac{n}{\mathrm{mcd}(n, n/n')} = n'. \end{aligned}$$

Quindi il punto **[b]** appena dimostrato conferma che $x'y'$ ha ordine $m'n' = \mathrm{mcm}(m, n)$. □

Il precedente lemma vale anche indebolendo le sue ipotesi. Infatti la sua tesi è vera anche se G non è abeliano quando x e y sono permutabili.

Lemma B1.3. *Siano G un gruppo abeliano finito e x un elemento di G di ordine massimo. Se y è un qualunque elemento di G, allora l'ordine di y divide l'ordine di x.*

La finitezza di G garantisce l'esistenza di un elemento di ordine massimo; ovviamente possono esistere anche più elementi che hanno lo stesso ordine, anche se l'ordine è massimo.

DIMOSTRAZIONE. Denotiamo con n e m rispettivamente l'ordine di x e y. Supponiamo per assurdo che $m \nmid n$. Sotto queste ipotesi esisterà p primo, tale che

$$\begin{aligned} m = m' \cdot p^{\alpha} : &\qquad \mathrm{mcd}(m', p) = 1, \\ n = n' \cdot p^{\gamma} : &\qquad \mathrm{mcd}(n', p) = 1; \end{aligned}$$

con $\alpha > \gamma$. Introduciamo ora un terzo elemento: $z := x^{p^{\gamma}} y^{m'}$ ed osserviamo che $o(x^{p^{\gamma}}) = n'$ e $o(y^{m'}) = p^{\alpha}$ con $\mathrm{mcd}(n', p^{\alpha}) = 1$. Allora da $\alpha > \gamma$, deduciamo

$$o(z) \;=\; o(x^{p^{\gamma}})\, o(y^{m'}) \;=\; n' p^{\alpha} > n' p^{\gamma} = n = o(x).$$

Questo è assurdo perché x è elemento di ordine massimo. □

Lemma B1.4. *Siano G un gruppo abeliano finito e $H = \langle x \rangle$, con x elemento di G di ordine massimo. Sia Hy un laterale di G/H di ordine m. Allora nel laterale Hy esiste un elemento di ordine m.*

DIMOSTRAZIONE. H è il sottogruppo generato da x che è l'elemento di ordine massimo, $H = \langle x \rangle = \{x^k \mid k = 1, 2, \cdots, o(x)\}$, quindi $|H| = o(x)$.

Prima di tutto, H è un sottogruppo normale di G perché G è abeliano, quindi $(Hy)^m = Hy^m$. Per ipotesi m è l'ordine di Hy, allora $(Hy)^m = Hy^m = H$ cioè $y^m \in H$, per cui esiste $k \in \mathbb{N}$ tale che $y^m = x^k$.

Posto $z := x^{-k/m} y$, dimostriamo che $z \in Hy$ e che $o(z) = m$.

Infatti denotando con n e ℓ rispettivamente l'ordine di x e di y, vale

$$\frac{\ell}{\mathrm{mcd}(\ell, m)} = o(y^m) = o(x^k) = \frac{n}{\mathrm{mcd}(n, k)}.$$

Osserviamo che $(Hy)^{\ell} = Hy^{\ell} = H$ perché $o(y) = \ell$, quindi $m | \ell$ e $\mathrm{mcd}(\ell, m) = m$. Allora abbiamo la seguente implicazione:

$$\frac{k}{m} = \frac{k}{\mathrm{mcd}(n, k)} \cdot \frac{\mathrm{mcd}(n, k)}{m} = \frac{k}{\mathrm{mcd}(n, k)} \frac{\mathrm{mcd}(n, k)}{\mathrm{mcd}(\ell, m)} = \frac{k}{\mathrm{mcd}(n, k)} \cdot \frac{n}{\ell}.$$

Notiamo che $\frac{k}{\text{mcd}(n,k)}$ e $\frac{n}{\ell}$ sono due interi dove l'ultimo lo è per il Lemma **B1.3** perché n è l'ordine massimo degli elementi di G ed ℓ è l'ordine di $y \in G$. Concludendo $-\frac{k}{m}$ è un intero e, per come è definito H, $x^{-\frac{k}{m}}$ è un suo elemento, quindi $z \in Hy$.

Rimane da provare che l'ordine di z è m. Osserviamo che $z^m = (x^{-\frac{k}{m}}y)^m = x^{-k}y^m$, ricordando che $y^m = x^k$, allora $z^m = x^{-k}x^k = e$ da cui $o(z)|m$. Sappiamo che $x^{-\frac{k}{m}}$ appartiene ad H, per cui $Hz = Hx^{-\frac{k}{m}}y = Hy$; conseguentemente $o(Hz) = o(Hy) = m$. Notando che

$$(Hz)^{o(z)} = Hz^{o(z)} = H$$

allora $m|o(z)$, per cui $o(z) = m$. □

Teorema B1.5 (Teorema fondamentale dei gruppi abeliani finiti). *Sia G un gruppo abeliano finito di ordine n. Allora G è isomorfo al prodotto diretto*

$$G \cong G_1 \otimes G_2 \otimes \cdots \otimes G_\ell \qquad (\star\star)$$

di gruppi ciclici G_k di ordini e_k con $k = 1, 2, \cdots, \ell$. Gli interi $\{e_k\}$ godono delle seguenti proprietà:

(a) *e_k divide e_{k-1} per $k = 2, 3, \cdots, \ell$.*
(b) *il prodotto degli $\{e_k\}$ uguaglia l'ordine di G: $n = e_1 e_2 \cdots e_\ell$.*
(c) *gli $\{e_k\}$ sono univocamente determinati dalle proprietà* **[a]** *e* **[b]**, *essi sono denominati* fattori invarianti *del gruppo G.*

DIMOSTRAZIONE. Dimostriamo **[a]** e **[b]** per induzione su n.

Se $n = 1$, cioè $|G| = 1$ è banale. Supponiamo vera la tesi per i gruppi di ordine minore di $n > 1$ e dimostriamo la sua veridicità anche per i gruppi di ordine n.

Sia G un gruppo abeliano finito con $|G| = n$, sappiamo che esiste g_1 elemento di massimo ordine in G con $o(g_1) = e_1 > 1$. Definiamo $G_1 = \langle g_1 \rangle$ dato che G è abeliano allora G_1 è sottogruppo normale di G. Possiamo allora formare il gruppo quoziente G/G_1, per il Teorema **A1.7** di Lagrange si ha che $|G/G_1| = n/e_1 < n$. Applicando ora l'ipotesi induttiva al gruppo G/G_1:

$$G/G_1 \cong H_2 \otimes H_3 \otimes \cdots \otimes H_\ell$$

dove H_k è un gruppo ciclico per ogni $k = 2, 3, \cdots, \ell$, cioè esiste un $h_k \in G$ tale che $H_k = \langle h_k G_1 \rangle$ con $|H_k| = e_k$. Inoltre, si ha ovviamente $|G/G_1| = e_2 \cdots e_\ell = n/e_1$ e $e_k|e_{k-1}$ per $k = 3, 4, \cdots, \ell$.

Per il Lemma **B1.4** in ogni laterale $h_k G_1$ esiste un elemento g_k avente ordine e_k. Denotiamo con G_k il gruppo ciclico generato da g_k, allora per ogni $k = 2, 3, \cdots, \ell$ si ha che $G_k \cong H_k$ con $|G_k| = e_k$ e $e_{k+1}|e_k$. Ponendo

$H = G_2 \cdot G_3 \cdots G_\ell$, vogliamo dimostrare $H = G_2 \otimes G_3 \otimes \cdots \otimes G_\ell$ verificando che $|H| = e_2 \cdot e_3 \cdots e_\ell$ per la caratterizzazione del prodotto diretto.

Consideriamo la restrizione ad H dell'epimorfismo canonico

$$\phi : G \longrightarrow G/G_1 \quad \text{tale che} \quad \phi(g) = gG_1.$$

Osserviamo che ogni elemento di H può essere scritto come $h = g_2^{\gamma_2} g_3^{\gamma_3} \cdots g_\ell^{\gamma_\ell}$ perché $H = G_2 \cdot G_3 \cdots G_\ell = \langle g_2 \rangle \cdot \langle g_3 \rangle \cdots \langle g_\ell \rangle$, per cui la sua immagine è $\phi_{|H}(h) = (g_2^{\gamma_2} G_1)(g_3^{\gamma_3} G_1) \cdots (g_\ell^{\gamma_\ell} G_1)$. Per ogni $k = 2, 3, \cdots, \ell$, l'elemento g_k è nel laterale $h_k G_1$ con $o(g_k) = e_k$, allora $g_k G_1 = h_k G_1$ e $g_k^{\gamma_k} G_1 \subseteq \langle h_k G_1 \rangle$, quindi

$$\phi_{|H}(h) \in \langle h_2 G_1 \rangle \cdot \langle h_3 G_1 \rangle \cdots \langle h_\ell G_1 \rangle = H_2 \otimes H_3 \otimes \cdots \otimes H_\ell \cong G/G_1.$$

Si osserva che $|\phi(H)| = |G/G_1|$ perché

$$\begin{aligned} \phi(H) &= \phi(\langle g_2 \rangle) \cdot \phi(\langle g_3 \rangle) \cdots \phi(\langle g_\ell \rangle) \\ &= \langle g_2 G_1 \rangle \cdot \langle g_3 G_1 \rangle \cdots \langle g_\ell G_1 \rangle \\ &= \langle h_2 G_1 \rangle \cdot \langle h_3 G_1 \rangle \cdots \langle h_\ell G_1 \rangle \\ &= H_2 \otimes H_3 \otimes \cdots \otimes H_\ell \cong G/G_1. \end{aligned}$$

Quindi la funzione è suriettiva, da cui si ottiene $|H| \geq |\phi(H)| = e_2 e_3 \cdots e_\ell$, dato che è assurdo che un insieme abbia meno elementi della sua immagine. Ricordando come è definita H, si ha che $|H| \leq e_2 e_3 \cdots e_\ell$ per cui si conferma l'uguaglianza $|H| = e_2 e_3 \cdots e_\ell$. Secondo il Corollario **A4.3** H è il prodotto diretto degli $\{G_i\}$:

$$H = G_2 \otimes G_3 \otimes \cdots \otimes G_\ell.$$

Ora verifichiamo che $G = HG_1$. Infatti $HG_1 \subseteq G$ perché $H \leq G$ e $G_1 \leq G$. Inoltre si ha che $HG_1 \supseteq G$ visto che se $g \in G$ esiste $h \in H$ tale che $hG_1 = \phi(g) = gG_1$ allora esiste $g' \in G_1$ tale che $g = hg'$ per cui $g \in HG_1$.

Secondo l'isomorfismo $H \cong G/G_1$, sappiamo ora che $|H| = |G/G_1| = |HG_1/G_1|$, inoltre G_1 è sottogruppo normale di G e $H \leq G$; allora per il Teorema **A3.4** di isomorfismo $HG_1/G_1 \cong H/(H \cap G_1)$, quindi $|H \cap G_1| = 1$ cioè $H \cap G_1 = \{e\}$.

Per la caratterizzazione del prodotto diretto, abbiamo $G \cong H \otimes G_1$. Dato che $H \cong G_2 \otimes \cdots \otimes G_\ell$ allora $G \cong G_1 \otimes G_2 \otimes \cdots \otimes G_\ell$ con $|G_k| = e_k$ per ogni $k = 1, 2, \cdots, \ell$. Si verificano anche $e_k | e_{k-1}$ per $k = 2, 3, \cdots, \ell$ utilizzando il fatto che e_1 è ordine massimo quindi $e_2 | e_1$ e l'ipotesi induttiva applicata a $G/G_1 \cong H_2 \otimes H_3 \otimes \cdots \otimes H_\ell$.

Abbiamo così dimostrato le prime due tesi. Rimane solo da verificare l'ultima; ovvero l'unicità.

Supponiamo che $G \cong G_1 \otimes G_2 \otimes \cdots \otimes G_\ell$ ed anche $G \cong G'_1 \otimes G'_2 \otimes \cdots \otimes G'_{\ell'}$ con $|G_\ell| > 1$ e $|G'_{\ell'}| > 1$ tali che valgano **[a]** e **[b]** per entrambe. Senza perdere di generalità, si assume che $\ell \leq \ell'$. Allora

$$G_1 = \langle g_1 \rangle \quad \text{con } g_1 \text{ elemento di ordine massimo in } G \Rightarrow e'_1 | e_1,$$
$$G'_1 = \langle g'_1 \rangle \quad \text{con } g'_1 \text{ elemento di ordine massimo in } G \Rightarrow e_1 | e'_1;$$

quindi $e_1 = e'_1$, allora $G_1 \cong G'_1$ e $G/G_1 \cong G/G'_1$ ovvero

$$G_2 \otimes G_3 \otimes \cdots \otimes G_\ell \cong G'_2 \otimes \cdots \otimes G'_{\ell'}.$$

Ripetiamo il procedimento

$$G_2 = \langle g_2 \rangle \text{ con } g_2 \text{ elemento di ordine massimo in } G_2 \otimes G_3 \otimes \cdots \otimes G_\ell,$$
$$G'_2 = \langle g'_2 \rangle \text{ con } g'_2 \text{ elemento di ordine massimo in } G'_2 \otimes G'_3 \otimes \cdots \otimes G'_{\ell'};$$

quindi $e_2 = e'_2$, ed analogamente

$$G_1 \otimes G_2 \cong G'_1 \otimes G'_2$$

il che implica

$$G_3 \otimes G_4 \otimes \cdots \otimes G_\ell \cong G'_3 \otimes \cdots \otimes G'_{\ell'}.$$

Continuando a ripetere il procedimento per $G_3, G_4, G_5, \cdots$ fino a G_ℓ, otteniamo $G_\ell \cong G'_\ell \otimes \cdots \otimes G'_{\ell'}$. Analogamente $e_\ell = e'_\ell$ e $G_\ell \cong G'_\ell$ per cui risulta

$$G_\ell/G_\ell = \{e\} = G'_\ell \otimes \cdots \otimes G'_{\ell'}/G'_\ell$$

ciò significa $\ell = \ell'$. Ricapitolando possiamo concludere che $|G_k| = |G'_k|$ per ogni $k = 1, 2, \cdots, \ell = \ell'$. □

B2. p-gruppi e decomposizione primaria ciclica

Denotiamo con $\mathbb{P}$ l'insieme dei numeri primi. Fissato un numero primo $p \in \mathbb{P}$, un *p-elemento* di un gruppo G è un elemento il cui ordine è una potenza di p. Se tutti gli elementi di G tranne l'elemento neutro sono p-elementi allora G si dice *p-gruppo*.

L'esempio più semplice è il gruppo di Klein che è un p-gruppo con $p = 2$. Infatti, fissate nel piano due rette perpendicolari a e b, e detto c il loro punto d'intersezione, le riflessioni $\sigma_a, \sigma_b, \sigma_c$ rispetto ad a, b, c formano un gruppo abeliano di ordine 4 assieme alla funzione identica I. Si osserva che ogni riflessione è l'inversa di se stessa, perché $\sigma_a \sigma_a = \sigma_a \sigma_a^{-1} = I$ quindi $o(\sigma_a) = 2$ ed analogamente per $o(\sigma_c) = 2$ con $\sigma_c = \sigma_a \cdot \sigma_b$. Conseguentemente questo gruppo è formato esclusivamente da p-elementi con $p = 2$.

Denotiamo con $(U_n, \cdot)$ il gruppo delle n-sime radici dell'unità. Quando $n = 9$, si ha che $(U_9, \cdot)$ è un p-gruppo con $p = 3$, che è isomorfo al gruppo

$(\mathbb{Z}_9, +)$. In generale, per ogni $n = p^k$, con p primo i gruppi $(U_n, \cdot)$ e $(\mathbb{Z}_n, +)$ sono dei p-gruppi.

Teorema B2.1 (Cauchy). *Se p è un primo che divide l'ordine di un gruppo finito G, allora esiste in G un sottogruppo di ordine p.*

DIMOSTRAZIONE. Sia G un gruppo, $|G| = n < \infty$ e sia $p \in \mathbb{P}$ tale che $p|n$. Dimostrando che G contiene un elemento x di ordine p, si ottiene l'esistenza in G di un sottogruppo di ordine p, il sottogruppo generato dall'elemento x. Costruiamo un insieme di p-uple di elementi di G:

$$\Omega := \{(x_1, x_2, \cdots, x_p) \in G^p \mid x_1 x_2 \cdots x_p = e\}.$$

Essendo G finito possiamo contare le p-uple che formano Ω. Variando un solo elemento nella p-upla, ad esempio x_1, otteniamo n p-uple distinte, perché x_1 può variare in G in n modi. Variando due elementi si hanno n^2 p-uple distinte. Procedendo in questo modo arriveremo a variare i primi $p-1$ elementi ottenendo n^{p-1} p-uple distinte. L'ultimo elemento della p-upla invece non può variare perché deve essere $x_p = (x_1 x_2 \cdots x_{p-1})^{-1}$ in modo che la p-upla stia in Ω. Dunque $\Omega = n^{p-1}$. Definiamo ora una permutazione π su Ω tale che:

$$\pi(x_1, x_2, \cdots, x_p) := (x_2, x_3, \cdots x_p, x_1).$$

Osserviamo che il gruppo ciclico generato da π ha ordine p. Infatti, per $k = 1, 2, \cdots, p$ si vede facilmente che

$$\pi^k(x_1, x_2, \cdots, x_p) = (x_{k+1}, x_{k+2}, \cdots, x_p, x_1, x_2, \cdots, x_k)$$

e π^p è evidentemente la permutazione identica.

Fissata la p-upla $(x_1, x_2, \cdots, x_p)$ chiamiamo $\mathcal{C}$ l'insieme delle sue permutazioni tramite π^k con $k = 1, 2, \cdots, p$. Per ogni $k = 1, 2, \cdots, p$ si ha che

$$x_1 = x_2 = \cdots = x_p \quad \Longrightarrow \quad \pi^k(x_1, x_2, \cdots, x_p) = (x_1, x_2, \cdots, x_p)$$

cioè tutte le le permutazioni sono uguali: $|\mathcal{C}| = 1$.

Se invece in $(x_1, x_2, \cdots, x_p)$ esistono due componenti distinte, dette x_i e x_j con $i < j$ si ha che $|\mathcal{C}| = p$. Infatti, se per assurdo fosse $|\mathcal{C}| < p$ allora esisterebbero $\imath$ e $\jmath$ con $\imath < \jmath$ tali che

$$\pi^\imath(x_1, x_2, \cdots, x_p) = \pi^\jmath(x_1, x_2, \cdots, x_p)$$

che equivale alla seguente

$$(x_1, x_2, \cdots, x_p) = \pi^{\jmath-\imath}(x_1, x_2, \cdots, x_p).$$

Allora π^{j-i} genera un sottogruppo invariante di $\langle\pi\rangle$ di ordine p. Ricordiamo che $\langle\pi^{j-i}\rangle \neq \{id = \pi^p\}$ in quanto $i \neq j$. Dunque $\langle\pi^{j-i}\rangle = \{\pi\}$ che implica

$$\pi^{i-1}(x_1, x_2, \cdots, x_p) = \pi^{j-1}(x_1, x_2, \cdots, x_p).$$

Secondo la definizione di π

$$\begin{aligned} \pi^{i-1}(x_1, x_2, \cdots, x_p) &= (x_i, x_{i+1} \cdots, x_p, x_1, x_2, \cdots, x_{i-1}), \\ \pi^{j-1}(x_1, x_2, \cdots, x_p) &= (x_j, x_{j+1} \cdots, x_p, x_1, x_2, \cdots, x_{j-1}); \end{aligned}$$

si stabilisce $x_i = x_j$, che è assurdo.

Concludendo possiamo dividere Ω in due classi distinte: Ω_1 formata dalle p-uple tali che $|\mathcal{C}| = 1$ e Ω_2 formata dalle p-uple tali che $|\mathcal{C}| = p$. Siano r ed s rispettivamente le cardinalità di tali classi, allora $|\Omega| = r + s$, cioè $n^{p-1} = r + s$. Per ipotesi $p|n$ per cui $p|n^{p-1} = r + s$, s è multiplo di p perché ogni membro di Ω_2 genera una classe di p membri, quindi $p|r$ dove $r \neq 0$ perché $(e, e, \cdots, e) \in \Omega_1$. Allora esistono altri membri con componenti identici, ma diversi dall'elemento neutro in Ω_1.

Sia $(x, x, \cdots, x)$ un membro di Ω_1 con $x \neq e$, sappiamo che $x^p = e$ per cui $o(x)|p$ ed essendo $p \in \mathbb{P}$ e $o(x) \neq 1$ si ha $o(x) = p$. Dunque $\langle x\rangle$ è un sottogruppo di ordine p in G. □

Corollario B2.2. *Sia G un p-gruppo finito, allora l'ordine di G è una potenza di p.*

DIMOSTRAZIONE. Supponiamo $|G| = n$. Sia $q \in \mathbb{P}$ tale che $q|n$. Per il teorema di Cauchy esiste in G un sottogruppo di ordine q, e, come abbiamo visto, esso è il sottogruppo ciclico $\langle x\rangle$ dove x è un q-elemento. Osserviamo che x deve essere un p-elemento perché G è un p-gruppo, ovvero $p = q$. Riassumendo, per ogni $q \in \mathbb{P}$ tale che $q|n$, si ha che $p = q$. Ne segue che n contiene nella sua fattorizzazione in numeri primi solo p ripetuto un certo numero di volte, ovvero n è una potenza di p. □

OSSERVAZIONE: Siano $\ell_1, \ell_2, \cdots, \ell_n$ coprimi, cioè $\mathrm{mcd}(\ell_1, \ell_2, \cdots, \ell_n) = 1$, allora esistono n interi $\lambda_1, \lambda_2, \cdots, \lambda_n$ non tutti nulli tali che $\sum_{k=1}^{n} \ell_k \lambda_k = 1$.

DIMOSTRAZIONE. Dimostriamo la tesi per induzione su m.

Per $n = 2$, la tesi è un fatto già conosciuto. Ora supponiamo vera la tesi per n numeri interi e dimostriamo che vale per $n+1$. Siano $\ell_0, \ell_1, \ell_2, \cdots, \ell_n$ interi coprimi e sia $d := \mathrm{mcd}(\ell_1, \ell_2, \cdots, \ell_n)$, si ha che $\mathrm{mcd}(\ell_0, d) = 1$ per cui esistono λ_0, β interi tali che $\ell_0\lambda_0 + d\beta = 1$. Applichiamo l'ipotesi induttiva

a $\{\ell_1/d, \ell_2/d, \cdots, \ell_n/d\}$, che sono banalmente coprimi ed otteniamo che esistono $\mu_1, \mu_2, \cdots, \mu_n$ interi non tutti nulli tali che

$$\sum_{k=1}^{n} \frac{\ell_k}{d}\mu_k = 1 \quad \Longrightarrow \quad \sum_{k=1}^{n} \ell_k \mu_k = d \quad \Longrightarrow \quad \ell_0\lambda_0 + \beta \sum_{k=1}^{n} \ell_k \mu_k = 1$$

definendo $\lambda_k := \beta\mu_k$ per ogni $k = 1, 2, \cdots, n$ si ha $\sum_{k=0}^{n} \ell_k \lambda_k = 1$. □

Lemma B2.3. *Siano G un gruppo e g un elemento di ordine finito. Allora*

(a) *se $o(g) = mn$, con m e n primi tra loro, allora g si scrive in modo unico come prodotto di due elementi x e y di potenze di g, i quali sono permutabili e di ordine m e n rispettivamente.*

(b) *se $o(g) = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$ è la scomposizione di $o(g)$ in fattori primi con $p_1, p_2, \cdots, p_n$ distinti, g si scrive in modo unico come prodotto di n elementi $x_1, x_2, \cdots, x_n$ di potenze di g, i quali sono a due a due permutabili e di ordini $p_1^{m_1}$, $p_2^{m_2}, \cdots, p_n^{m_n}$ rispettivamente.*

DIMOSTRAZIONE. Verifichiamo separatamente le due tesi.

[a] Da $(m, n) = 1$ segue l'esistenza di α, γ interi tali che $m\alpha + n\gamma = 1$. Definendo $x := g^{n\gamma}$ e $y := g^{m\alpha}$, possiamo allora verificare che $xy = yx = g^{m\alpha+n\gamma} = g$, perciò g si scrivere come prodotto di xy o di yx, dove x e y sono potenze di g.

Resta da dimostrare che $o(x) = m$ e $o(y) = n$ e che x ed y sono gli unici elementi di questo tipo. Vale che

$$x^m = (g^{n\gamma})^m = (g^{mn})^\gamma = e \quad \Longrightarrow \quad o(x)|m;$$
$$y^n = (g^{m\alpha})^n = (g^{mn})^\alpha = e \quad \Longrightarrow \quad o(y)|n.$$

Per il Lemma **B1.2**, segue

$$mn = o(g) = o(xy) \mid \mathrm{mcm}\{o(x), o(y)\} \mid mn.$$

Allora $o(xy) = o(x)o(y) = mn$ quindi $o(x) = m$ e $o(y) = n$.

Infine, dobbiamo provare l'unicità; supponiamo che $g = xy$ ed anche $g = x_1y_1$ tali che $o(x) = o(x_1) = m$ e $o(y) = o(y_1) = n$. Allora da $xy = g = x_1y_1$ otteniamo $x_1^{-1}x = y_1y^{-1}$ moltiplicando a sinistra per x_1^{-1} e a destra per y^{-1}. Posto $z = x_1^{-1}x = y_1y^{-1}$ vale che $o(z)|m$ e $o(z)|n$, in quanto $z^m = (x_1^{-1}x)^m = x_1^{-m}x^m = e$, ed inoltre $z^n = (y_1y^{-1})^n = y_1^n y^{-n} = e$, quindi $o(z)$ è comune divisore di m ed n, ma $\mathrm{mcd}(m, n) = 1$ quindi $o(z) = 1$ che equivale a dire $x = x_1$ e $y = y_1$.

[b] Definendo

$$\ell_k := \frac{o(g)}{p_k^{m_k}} \quad \text{per} \quad k = 1, 2, \cdots, n$$

osserviamo che

$$\ell_k = \frac{o(g)}{p_k^{m_k}} = \prod_{\substack{i=1 \\ i\neq k}}^{n} p_i^{m_i} \qquad \Longrightarrow \qquad p_k \nmid \ell_k$$

per cui non esiste nessun p_k divisore comune per $\{\ell_k\}_{k=1}^n$ e dunque si ha che $\text{mcd}(\ell_1, \ell_2, \cdots, \ell_n) = 1$. Per l'osservazione precedente esistono $\lambda_1, \lambda_2, \cdots, \lambda_n$ interi tali che $\sum_{k=1}^n \ell_k \lambda_k = 1$. Ponendo $x_k = g^{\ell_k \lambda_k}$ per ogni $k = 1, 2, \cdots, n$, si ha che

$$g = x_1 x_2 \cdots x_\ell = g^{\ell_1 \lambda_1} g^{\ell_2 \lambda_2} \cdots g^{\ell_n \lambda_n}.$$

Verifichiamo ora che $o(x_k) = p_k^{m_k}$ per ogni $k = 1, 2, \cdots, n$.

$$x_k^{p_k^{m_k}} = (g^{\ell_k \lambda_k})^{p_k^{m_k}} = (g^{o(g)})^{\lambda_k} = e$$

quindi $o(x_k) | p_k^{m_k}$ per ogni $k = 1, 2, \cdots, n$. Per il Lemma **B1.2**

$$o(g) = o(x_1 x_2 \cdots x_n) \mid \text{mcm}\{o(x_1), o(x_2), \cdots, o(x_n)\}$$

$$= o(x_1) o(x_2) \cdots o(x_m) \mid o(g) = \prod_{k=1}^{n} p_k^{m_k}$$

ne segue

$$o(x_1) o(x_2) \cdots o(x_n) = o(g) = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}.$$

Quindi $o(x_k) = p_k^{m_k}$ per ogni $k = 1, 2, \cdots, n$.

Resta ora da provare l'unicità. Sia $g = x_1 x_2 \cdots x_n$ ed anche che $g = y_1 y_2 \cdots y_n$ con $o(x_k) = o(y_k) = p_k^{m_k}$ per ogni $k = 1, 2, \cdots, n$. Da

$$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_n$$

si ha che

$$x_k y_k^{-1} = \prod_{\substack{i=1 \\ i\neq k}}^{n} x_i^{-1} y_i \quad \text{per ogni} \quad k = 1, 2, \cdots, n.$$

Posto

$$z_k = x_k y_k^{-1} = \prod_{\substack{i=1 \\ i\neq k}}^{n} x_i^{-1} y_i \quad \text{si osserva che} \quad o(z_k) | p_k^{m_k} \quad \text{e} \quad o(z_k) | \ell_k.$$

Notando $o(x_k) = o(y_k) = p_k^{m_k}$, si ha che

$$z_k^{p_k^{m_k}} = (x_k y_k^{-1})^{p_k^{m_k}} = x_k^{p_k^{m_k}} y_k^{-p_k^{m_k}} = e \quad \text{e} \quad z_k^{\ell_k} = \prod_{\substack{i=1 \\ i\neq k}}^{n} (x_i^{-1} y_i)^{\ell_k} = e$$

dove l'ultimo passaggio si giustifica col fatto che ℓ_k è un multiplo di $p_i^{m_i}$ per $i \neq k$. Ricordando che $\text{mcd}(\ell_k, p_k^{m_k}) = 1$ si ha $o(z_k) = 1$ che equivale a $x_k = y_k$ per $k = 1, 2, \cdots, n$. □

Teorema B2.4 (Decomposizione primaria ciclica). *Un gruppo abeliano finito G è isomorfo al prodotto diretto di p-gruppi ciclici, gli ordini dei quali sono univocamente determinati. Tali ordini dei p-gruppi ciclici si chiamano* divisori elementari *di G.*

DIMOSTRAZIONE. Sia $|G| = \prod_{k=1}^{n} p_k^{m_k}$, dove $\{p_k\}_{k=1}^{n}$ sono i numeri primi distinti e $\{m_k\}_{k=1}^{n}$ sono i numeri naturali. Per il Teorema fondamentale **B1.5** dei gruppi abeliani finiti, vale che $G \cong G_1 \otimes G_2 \otimes \cdots \otimes G_\ell$ dove G_k è un gruppo ciclico con $|G_k| = e_k$ per $k = 1, 2, \cdots, \ell$ che soddisfano $|G| = e_1 e_2 \cdots e_\ell$ e $e_k | e_{k-1}$ per $k = 2, 3, \cdots, \ell$.

Dato che $|G| = e_1 e_2 \cdots e_\ell$, è evidente che e_i è prodotto di alcuni primi nella decomposizione di $|G|$, così $e_i = \prod_{k=1}^{n} p_k^{m_{ki}}$ per $i = 1, 2, \cdots, \ell$ (banalmente $m_{ki} \leq m_k$ per $k = 1, 2, \cdots, n$ e $i = 1, 2, \cdots, \ell$).

Consideriamo ciascuno di tali gruppi ciclici $G_i = \langle g_i \rangle$ con $g_i \in G$ ed $o(g_i) = e_i$, per il Lemma **B2.3** esistono n elementi $g_{i1}, g_{i2}, \cdots, g_{in} \in G$ tali che $o(g_{ik}) = p_k^{m_{ki}}$ e $g_i = g_{i1} g_{i2} \cdots g_{in}$. Per il Corollario **A4.3**, $G_i = \langle g_i \rangle$ è isomorfo al prodotto dei p_k-gruppi ciclici $\langle g_{ik} \rangle$ con $k = 1, 2, \cdots, n$. Applicando il teorema fondamentale dei gruppi abeliani finiti, otteniamo la decomposizione primaria ciclica come segue:

$$G \cong \bigotimes_{i=1}^{\ell} G_i \cong \bigotimes_{i=1}^{\ell} \bigotimes_{k=1}^{n} \langle g_{ik} \rangle.$$

L'unicità dei divisori elementari discende banalmente dall'unicità dei fattori invarianti e_i e dall'unicità della loro decomposizione in fattori primi. □

Corollario B2.5 (Decomposizione in p-gruppi). *Un gruppo abeliano finito è isomorfo al prodotto diretto di p-sottogruppi, gli ordini dei quali sono univocamente determinati.*

DIMOSTRAZIONE. Raggruppando i componenti del doppio prodotto diretto nel teorema della primaria ciclica, si ha che

$$G \cong \bigotimes_{i=1}^{\ell} \bigotimes_{k=1}^{n} \langle g_{ik} \rangle \cong \bigotimes_{k=1}^{n} \left\{ \bigotimes_{i=1}^{\ell} \langle g_{ik} \rangle \right\}$$

dove il prodotto interno nelle parentesi graffe è un p_k-gruppo finito. □

B3. Fattori invarianti e divisori elementari

Per decomporre un generico gruppo abeliano finito di ordine n e per trovare quindi, quanti sono i gruppi abeliani di ordine n a meno di isomorfismi, si hanno a disposizione tre metodi dati dai seguenti teoremi:

- Il teorema fondamentale dei gruppi abeliani finiti: **B1.5**.
- Il teorema di decomposizione primaria ciclica: **B2.4**.
- Il corollario di decomposizione in p-gruppi: **B2.5**.

Esempio B3.1 (p-gruppo abeliano finito). *Sia $m = p^n$ con p primo. Secondo il Teorema* **B1.5**, *i fattori invarianti di un gruppo abeliano di ordine p^n hanno le forme:*

$$e_k = p^{\lambda_k} \quad con \quad \begin{cases} \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell > 0, \\ \lambda_1 + \lambda_2 + \cdots + \lambda_\ell = n; \end{cases}$$

essi sono anche i divisori elementari. Dunque, esiste una corrispondenza fra i gruppi abeliani non isomorfi di ordine p^n e l'insieme delle successioni $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n > 0$ con $\lambda_1 + \lambda_2 + \cdots + \lambda_n = n$.

Esempio B3.2. *Sia $m = 36 = 2^2 \cdot 3^2$. La seguente tabella illustra la struttura dei gruppi abeliani di ordine 36, dove si denota con C_n un gruppo ciclico di ordine n:*

No	Fattori Invarianti	Divisori Elementari
C_6	2×3	2, 3
C_6	2×3	2, 3
C_{18}	2×3^2	2, 3^2
C_2	2	2
C_{12}	$2^2 \times 3$	2^2, 3
C_3	3	3
C_{36}	$2^2 \times 3^2$	2^2, 3^2

Dunque esistono 4 gruppi abeliani non isomorfi di ordine 36:

$$\begin{aligned} G_1 &\cong C_6 \otimes C_6, \\ G_2 &\cong C_{18} \otimes C_2, \\ G_3 &\cong C_{12} \otimes C_3, \\ G_4 &\cong C_{36}. \end{aligned}$$

Analogamente i gruppi abeliani non isomorfi di ordine 36 hanno decomposizione primaria ciclica come segue:

$$\begin{aligned} G_1 &\cong C_2 \otimes C_2 \otimes C_3 \otimes C_3, \\ G_2 &\cong C_2 \otimes C_2 \otimes C_9, \\ G_3 &\cong C_3 \otimes C_3 \otimes C_4, \\ G_4 &\cong C_4 \otimes C_9. \end{aligned}$$

Esempio B3.3. *Sia $m = p^2q^3$ con p e q primi distinti. Esistono 6 gruppi abeliani non isomorfi di ordine p^2q^3. Vengono tabulati i fattori invarianti e i divisori elementari rispettivemente come segue:*

No	Fattori Invarianti	Divisori Elementari
C_{pq}	pq	$p,\ q$
C_{pq}	pq	$p,\ q$
C_q	q	q
C_{pq^2}	pq^2	$p,\ q^2$
C_{pq}	pq	$p,\ q$
C_{pq^3}	pq^3	$p,\ q^3$
C_p	p	p
C_{p^2q}	p^2q	$p^2,\ q$
C_q	q	q
C_q	q	q
$C_{p^2q^2}$	p^2q^2	$p^2,\ q^2$
C_q	q	q
$C_{p^2q^3}$	p^2q^3	$p^2,\ q^3$

Secondo il teorema dei gruppi abeliani, abbiamo le seguenti decomposizioni:

$$\begin{aligned} H_1 &\cong C_{pq} \otimes C_{pq} \otimes C_q, \\ H_2 &\cong C_{pq^2} \otimes C_{pq}, \\ H_3 &\cong C_{pq^3} \otimes C_p, \\ H_4 &\cong C_{p^2q} \otimes C_q \otimes C_q, \\ H_5 &\cong C_{p^2q^2} \otimes C_q, \\ H_6 &\cong C_{p^2q^3}. \end{aligned}$$

Resta da provare

$$H_k \cap \langle H_i \mid i \neq k \text{ con } 1 \leq i \leq n \rangle \;=\; \{e\}$$

con "e" elemento neutro di G. Supponiamo per assurdo che esista un elemento $y \neq e$ appartenente all'intersezione, allora esistono gli interi $\{m_k\}_{k=1}^{n}$ non tutti nulli tali che

$$y \;=\; x_k^{-m_k} \;=\; x_1^{m_1} x_2^{m_2} \cdots x_{k-1}^{m_{k-1}} x_{k+1}^{m_{k+1}} \cdots x_n^{m_n}$$

per cui valgono le ipotesi del teorema precedente:

$$x_1^{m_1} x_2^{m_2} \cdots x_{k-1}^{m_{k-1}} \cdot x_k^{m_k} \cdot x_{k+1}^{m_{k+1}} \cdots x_n^{m_n} \;=\; e$$

il quale garantisce l'esistenza di un elemento di periodo finito, diverso dall'elemento neutro in G. Questo è assurdo perché G è privo di torsione. □

Corollario B4.4. *Sia G un gruppo abeliano libero* (privo di torsione) *e finitamente generato. Se valgono*

$$\begin{aligned} G &\cong H_1 \otimes H_2 \otimes \cdots \otimes H_m, \\ G &\cong K_1 \otimes K_2 \otimes \cdots \otimes K_n; \end{aligned}$$

dove H_i e K_j sono gruppi ciclici infiniti, allora $m = n$.

DIMOSTRAZIONE. Supponiamo per assurdo che $m \neq n$ e ipotizziamo $m > n$ senza perdere di generalità. Sia x_i il generatore di H_i e y_j quello di K_j, allora $\{x_i\}_{i=1}^{m}$ e $\{y_j\}_{j=1}^{n}$ sono due sistemi di generatori per G; conseguentemente ogni generatore dei due sistemi si può esprimere in funzione degli elementi dell'altro sistema, in particolare per ogni x_i esistono s_{ij} interi tali che $x_i = \prod_{j=1}^{n} y_j^{s_{ij}}$. Consideriamo la matrice di elementi s_{ij}, questa è una matrice di ordine $m \times n$. Il numero delle righe è maggiore di quello delle colonne, per cui le m righe sono linearmente dipendenti, cioè esistono m numeri interi $\{r_i\}_{i=1}^{m}$ non tutti nulli tali che

$$\sum_{i=1}^{m} r_i \cdot s_{ij} \;=\; 0 \quad \text{per} \quad j = 1, 2, \cdots, n.$$

Si osserva che

$$\begin{aligned} x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m} \;&=\; \prod_{i=1}^{m} \Big\{ \prod_{j=1}^{n} y_j^{s_{ij}} \Big\}^{r_i} \;=\; \prod_{i=1}^{m} \prod_{j=1}^{n} y_j^{r_i s_{ij}} \\ &=\; \prod_{j=1}^{n} \prod_{i=1}^{m} y_j^{r_i s_{ij}} \;=\; \prod_{j=1}^{n} y_j^{\sum_{i=1}^{m} r_i s_{ij}} \end{aligned}$$

per cui si ottiene

$$x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m} \;=\; \prod_{j=1}^{n} y_j^{0} \;=\; e.$$

Ora, supponendo $r_1 \neq 0$, possiamo riformulare

$$x_1^{r_1} = \prod_{i=2}^{m} x_i^{-r_i} \quad \Longrightarrow \quad H_1 \bigcap \langle H_i \mid i = 2, 3, \cdots, m \rangle = \langle x_1^{r_1} \rangle \neq \{e\}.$$

Quest'ultimo è in contraddizione con il fatto che G è prodotto diretto di H_i con $i = 1, 2, \cdots, m$. In conclusione, abbiamo dimostrato $m = n$. □

Teorema B4.5. *Sia G un gruppo abeliano finitamente generato. Allora G è isomorfo al prodotto diretto di gruppi ciclici, nel quale ciascun fattore è o un p-gruppo ciclico oppure è isomorfo al gruppo $\mathbb{Z}$.*

DIMOSTRAZIONE. Sia T l'insieme di tutti gli elementi di G di periodo finito. Si dimostra banalmente che T è gruppo abeliano:

- $T \neq \emptyset$ perché $e \in T$;
- Per ogni $x \in T$, vale anche $x^{-1} \in T$;
- $\forall x, y \in T$, il loro prodotto è permutabile: $x \cdot y = y \cdot x$;
- $\forall x, y \in T$, si ha che $x \cdot y \in T$ (infatti il prodotto di due elementi di periodo finito ha periodo finito).

T viene detto *sottogruppo di torsione di G*. Si osserva che $T \subseteq G$ e G finitamente generato, allora anche T sarà finitamente generato, inoltre ogni generatore di T è di periodo finito, quindi genera un numero finito di elementi, in conclusione T è finito.

Dato che T è sottogruppo normale (in quanto è abeliano) possiamo considerare il gruppo quoziente G/T. Si dimostra che G/T è un gruppo finitamente generato ed è privo di torsione. L'unico elemento di periodo finito di G/T è il suo elemento neutro, T. Infatti, sia Tx un generico elemento di G/T, se questo è di ordine finito, esiste un numero naturale ℓ tale che $(Tx)^\ell = T$, ma ciò significa che $Tx^\ell = T$, il che avviene se $x^\ell \in T$. Per definizione di T si ha che x^ℓ è di periodo finito quindi anche x è di periodo finito. Allora $x \in T$ e $Tx = T$, cioè l'elemento neutro del gruppo quoziente. G/T è gruppo abeliano libero finitamente generato per cui valgono le ipotesi del Teorema **B4.3** e del Corollario **B4.4** pertanto esiste un unico numero naturale n minimo tale che G/T è isomorfo al prodotto diretto di n gruppi ciclici, quindi

$$G/T = \langle Tx_1 \rangle \otimes \langle Tx_2 \rangle \otimes \cdots \otimes \langle Tx_n \rangle.$$

Ora definiamo un sottogruppo di G con

$$H = \langle x_1 \rangle \cdot \langle x_2 \rangle \cdots \langle x_n \rangle.$$

È facile verificare che questo è un prodotto diretto

$$H = \langle x_1 \rangle \otimes \langle x_2 \rangle \otimes \cdots \otimes \langle x_n \rangle.$$

Infatti, tutti i gruppi ciclici $\{\langle x_i\rangle\}_{i=1}^{n}$ sono normali, inoltre, l'intersezione tra $\langle x_j\rangle$ ed il sottogruppo generato dagli $\langle x_i\rangle$ con $i \neq j$ è composta dal solo elemento neutro. Altrimenti avremo un elemento in comune della forma

$$x_j^{-m_j} = \prod_{i\neq j} x_i^{m_i}$$

dove $m_1, m_2, \cdots, m_n$ sono numeri interi non tutti nulli; il che equivale alla relazione

$$x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n} = e \quad \Longrightarrow \quad Tx_1^{m_1} \cdot Tx_2^{m_2} \cdots Tx_n^{m_n} = T.$$

Questo è assurdo perché G/T è prodotto diretto dei gruppi ciclici $\langle Tx_i\rangle$ con $i = 1, 2, \cdots, n$.

Analogamente si verifica che H è privo di torsione, perciò $T \cap H = \{e\}$. Per confermare che G è prodotto diretto di T e H, dobbiamo provare prima di tutto che $G = TH$.

Per ogni $g \in G$, abbiamo che $g \in Tg \in G/T$. Allora esistono n numeri interi $\{\ell_i\}_{i=1}^{n}$ tali che

$$Tg = Tx_1^{\ell_1} \cdot Tx_2^{\ell_2} \cdots Tx_n^{\ell_n} = Th \quad \text{con} \quad h = x_1^{\ell_1} x_2^{\ell_2} \cdots x_n^{\ell_n} \in H.$$

Questa relazione significa che esiste $t \in T$ tale che $g = th$. Così abbiamo dimostrato che $G = TH$.

Dato che T è un gruppo abeliano finito, allora T è prodotto diretto di p-gruppi ciclici secondo la decomposizione primaria ciclica. Inoltre, H è un gruppo abeliano finitamente generato privo di torsione, quindi H è prodotto diretto di gruppi ciclici isomorfi a $(\mathbb{Z}, +)$.

In conclusione, G è isomorfo al prodotto diretto di gruppi ciclici, nel quale ciascun fattore è o un p-gruppo ciclico oppure è isomorfo al gruppo $\mathbb{Z}$. □

B5. Partizioni e numero dei gruppi abeliani finiti

Definizione B5.1. *Un p-gruppo abeliano finito di divisori elementari* (fattori invarianti) $\{p^{\lambda_k}\}_{k=1}^{\ell}$ *con* $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell > 0$ *si dice p-gruppo di* tipo $(\lambda_1, \lambda_2, \cdots, \lambda_\ell)$.

Sia G un p-gruppo abeliano finito, allora esiste $n \in \mathbb{N}$ tale che $|G| = p^n$. Per il Teorema **B1.5** si ha che $G \cong G_1 \otimes G_2 \otimes \cdots \otimes G_\ell$, dove G_k è un gruppo ciclico di ordine e_k con $k = 1, 2, \cdots, \ell$ che soddisfano $p^n = |G| = e_1 e_2 \cdots e_\ell$ e $e_k | e_{k-1}$ per $k = 2, 3, \cdots, \ell$. Allora ogni e_k è una potenza di p con $e_k = p^{\lambda_k}$, per cui $p^n = p^{\lambda_1} p^{\lambda_2} \cdots p^{\lambda_\ell}$ e $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell > 0$. Perciò i fattori

invarianti sono $\left\{p^{\lambda_k}\right\}_{k=1}^{\ell}$ si ha che i gruppi ciclici G_k sono p-gruppi. Per il Teorema **B2.4** di decomposizione primaria ciclica, questi fattori invarianti coincidono con i divisori elementari di G ordinati in modo decrescente.

OSSERVAZIONE: Siano G e G' due p-gruppi abeliani finiti, rispettivamente di tipo $(\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ e $(\lambda'_1, \lambda'_2, \cdots, \lambda'_{\ell'})$ aventi medesimo ordine $|G| = |G'| = p^n$, allora

$$G \cong G' \iff (\lambda_1, \lambda_2, \cdots, \lambda_\ell) = (\lambda'_1, \lambda'_2, \cdots, \lambda'_{\ell'}).$$

Infatti, se $G \cong G'$ consideriamo le decomposizioni in p-gruppi ciclici

$$G_1 \otimes G_2 \otimes \cdots \otimes G_\ell \cong G'_1 \otimes G'_2 \otimes \cdots \otimes G'_{\ell'}$$

dove G_i e G'_j sono ciclici con

$$|G_i| = p^{\lambda_i} \quad \text{per} \quad 1 \le i \le \ell: \quad n = \sum \lambda_i, \quad \lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_\ell > 0;$$
$$|G'_j| = p^{\lambda'_j} \quad \text{per} \quad 1 \le j \le \ell': \quad n = \sum \lambda'_j, \quad \lambda'_1 \ge \lambda'_2 \ge \cdots \ge \lambda'_{\ell'} > 0.$$

Questo significa che tali p-gruppi G_k e G'_k sono corrispondentemente isomorfi, per cui hanno stesso ordine e allora i fattori invarianti di G e G' sono gli stessi.

Viceversa, siano G_k e G'_k i p_k-gruppi ciclici avente ordine p^{λ_k} con $\lambda_k = \lambda'_k$ per $k = 1, 2, \cdots, \ell = \ell'$. Allora G e G' sono isomorfi.

Definizione B5.2. *Sia n un numero intero positivo. Si dice che λ è una* partizione *di n, indicata con $\lambda \vdash n$, se λ è una sequenza $(\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ tale che $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_\ell > 0$ e $n = |\lambda| := \sum_{k=1}^{\ell} \lambda_k$. Ogni λ_k viene detto* parte *della partizione ed $\ell := \ell(\lambda)$ è la* lunghezza *della partizione.*

Lemma B5.3. *Il numero dei p-gruppi abeliani* (non isomorfi) *di ordine p^n è dato da $p(n)$, il numero delle partizioni di n.*

DIMOSTRAZIONE. Per l'osservazione precedente due p-gruppi abeliani finiti dello stesso ordine p^n sono non isomorfi se e solo se sono di tipo diverso. Allora l'insieme dei p-gruppi abeliani (non isomorfi) di ordine p^n è formato da tutti i tipi differenti di p-gruppo abeliano di ordine p^n. Quindi la cardinalità di questo insieme è data dal numero di sequenze distinte $(\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ che si possono formare con $n = \sum_{k=1}^{\ell} \lambda_k$ ed $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_\ell = 0$. Queste infatti definiscono i differenti tipi $(\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ di p-gruppo. Per definizione di partizione si ha poi la tesi. □

Lemma B5.4. *Il numero dei gruppi abeliani* (non isomorfi) *di ordine n, dove $n = p_1^{n_1} p_2^{n_2} \cdots p_\ell^{n_\ell}$ con $\{p_i\}_{i=1}^{\ell}$ primi distinti è dato dal prodotto dei*

DIMOSTRAZIONE. Sia G un gruppo abeliano finito. Per il Corollario **B2.5**, esistono p_k-gruppi H_k tali che $|H_k| = p_k^{n_k}$ con $k = 1, 2, \cdots, \ell$ ed il loro prodotto diretto:

$$G \cong H_1 \otimes H_2 \otimes \cdots \otimes H_\ell.$$

Dato che per ogni H_k con $k = 1, 2, \cdots, \ell$, il numero dei p_k-gruppi di ordine $p_k^{n_k}$ tra loro non isomorfi è uguale a $p(n_k)$. Ogni componente nel prodotto diretto ha una struttura algebrica indipendente dagli altri. Allora i gruppi abeliani di ordine n (non isomorfi) sono in numero $\prod_{k=1}^{\ell} p(n_k)$. □

Ricordando l'Esempio **B3.3**. Avevamo trovato 6 gruppi abeliani di ordine $m = p^2q^3$: infatti per il Lemma **B5.4**, $p(2)\,p(3) = 2 \cdot 3 = 6$ come si può facilmente vedere:

$$2:\ 2 = 2,\ 2 = 1+1 \quad \text{e} \quad 3:\ 3 = 3,\ 3 = 2+1,\ 3 = 1+1+1.$$

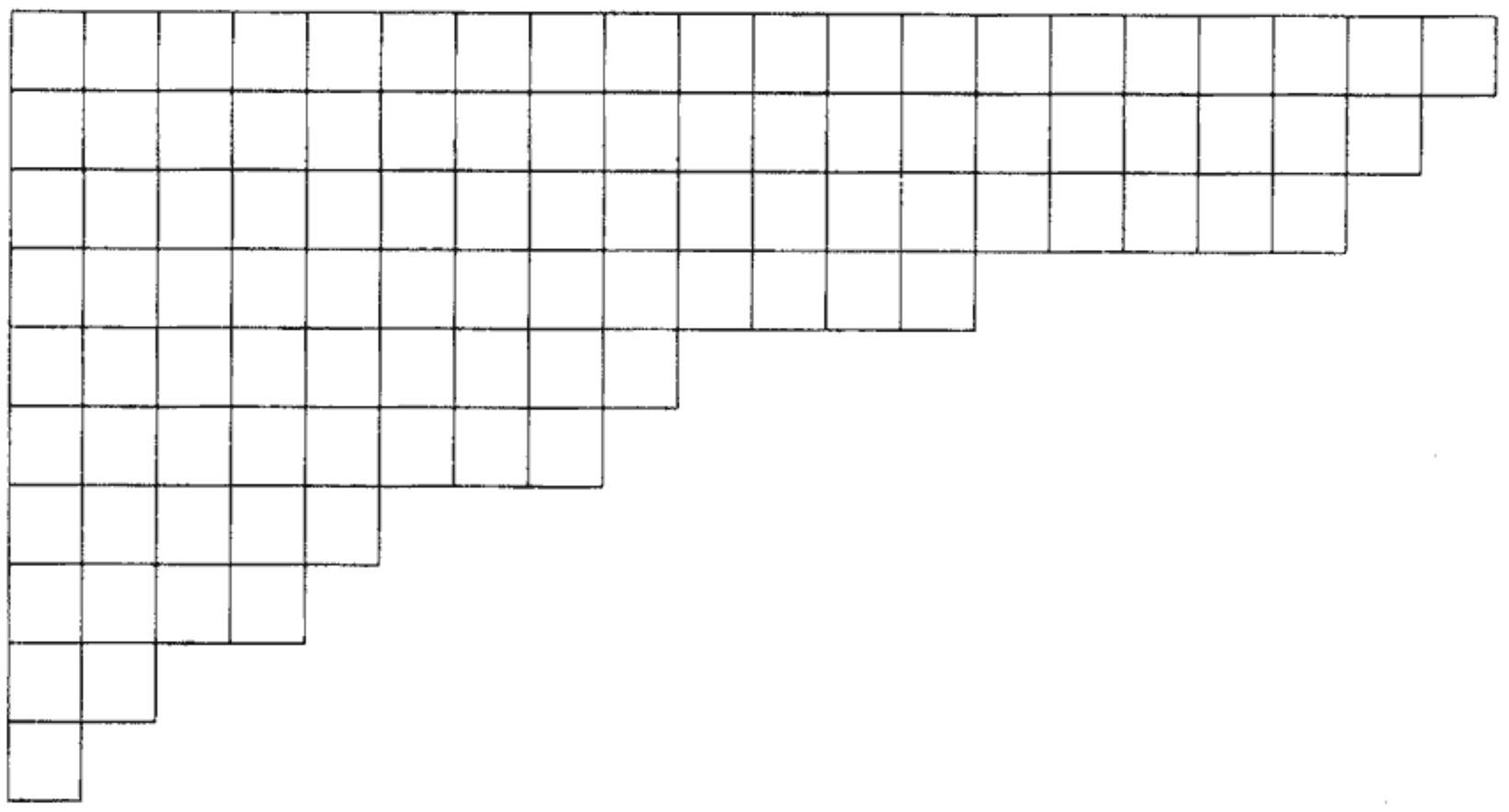
Per $m = 36$ ne avevamo trovati 4 precedentemente, infatti $36 = 2^2 \cdot 3^2$ e $4 = p(2)\,p(2) = 2 \cdot 2$. È evidente che trovare il numero delle partizioni di $n_1, n_2, \cdots, n_m$ non è sempre facile e immediato come negli esempi appena visti, per questo è indispensabile uno studio a parte delle partizioni. Se, ad esempio, $n = 5$ si hanno 7 partizioni distinte:

5=5	5	(5)
5=4+1	4≥ 1	(4,1)
5=3+2	3≥ 2	(3,2)
5=3+1+1	3 ≥ 1 ≥ 1	(3,1,1)
5=2+2+1	2 ≥ 2 ≥ 1	(2,2,1)
5=2+1+1+1	2 ≥ 1 ≥ 1 ≥ 1	(2,1,1,1)
5=1+1+1+1+1	1 ≥ 1 ≥ 1 ≥ 1 ≥ 1	(1,1,1,1,1)

È possibile rappresentare le partizioni di un numero naturale tramite il così detto *diagramma di Ferrers* cioè tramite caselle o scatole. Per esempio, una partizione λ di 99 con

$$\lambda = (20, 19, 18, 13, 9, 8, 5, 4, 2, 1)$$

viene illustrata come segue:



Quando il diagramma di Ferrers viene letto secondo le colonne (invece delle righe), la partizione corrispondente si chiama la *partizione coniugata*. Per esempio, la partizione coniugata alla λ di 99 risulta come segue:

$$\lambda' = (10, 9, 8, 8, 7, 6, 6, 6, 5, 4, 4, 4, 4, 3, 3, 3, 3, 3, 2, 1).$$

Inoltre ogni partizione di n può essere scritta come $(1^{m_1}, 2^{m_2}, \cdots, n^{m_n})$ con $n = \sum_{k=1}^{n} km_k$. Dunque possiamo anche scrivere le due partizioni λ e λ':

$$\begin{aligned} \lambda &= (1^1, 2^1, 4^1, 5^1, 8^1, 9^1, 13^1, 18^1, 19^1, 20^1), \\ \lambda' &= (1^1, 2^1, 3^5, 4^4, 5^1, 6^3, 7^1, 8^2, 9^1, 10^1). \end{aligned}$$

Analogamente, le sette partizioni di 5 vengono tabulate come segue:

$(1^0, 2^0, 3^0, 4^0, 5^1)$	5=5	(5)
$(1^1, 2^0, 3^0, 4^1, 5^0)$	$5 = 1 \times 1 + 1 \times 4$	(4,1)
$(1^0, 2^1, 3^1, 4^0, 5^0)$	$5 = 1 \times 2 + 1 \times 3$	(3,2)
$(1^2, 2^0, 3^1, 4^0, 5^0)$	$5 = 2 \times 1 + 1 \times 3$	(3,1,1)
$(1^1, 2^2, 3^0, 4^0, 5^0)$	$5 = 1 \times 1 + 2 \times 2$	(2,2,1)
$(1^3, 2^1, 3^0, 4^0, 5^0)$	$5 = 3 \times 1 + 1 \times 2$	(2,1,1,1)
$(1^5, 2^0, 3^0, 4^0, 5^0)$	$5 = 5 \times 1$	(1,1,1,1,1)

Quindi possiamo dire che $(1^{m_1}, 2^{m_2}, \cdots, n^{m_n})$ è una rappresentazione della partizione del numero naturale $n = \sum_{k=1}^{n} km_k$, dove per $1 \leq k \leq n$ si indica con $m_k \in \mathbb{N}_0$ il numero delle copie di parte k. Da ciò otteniamo che il numero delle partizioni di n è dato dal numero delle successioni $\{m_k\}_{k=0}^{n}$ tali che $n = \sum_{k=1}^{n} km_k$.

Sfruttando delle nozioni analitiche si riesce a trovare un metodo pratico per il calcolo di $p(n)$. Definiamo *funzione generatrice* della successione esplicita $\{c_k\}_{k=0}^{\infty}$ tramite la serie formale di potenze $f(x) = \sum_{k=0}^{\infty} c_k x^k$. Il coefficiente c_k di x^k in $f(x)$ viene indicato con $[x^k]f(x)$. Siano $\mathbb{N}$ l'insieme dei numeri naturali e $\mathbb{S}$ un sottoinsieme di $\mathbb{N}$. Denotiamo con $p(n|\mathbb{S})$ il numero delle partizioni di n con le parti in $\mathbb{S}$. Ovviamente si ha che $p(n) = p(n|\mathbb{N})$. Prima di tutto, vogliamo dimostrare che la funzione generatrice per $p(n|\mathbb{S})$ risulta il seguente prodotto:

$$G(q|\mathbb{S}) := \sum_{n=0}^{\infty} p(n|\mathbb{S})q^n \;=\; \prod_{k\in\mathbb{S}}^{\infty} \frac{1}{1-q^k}.$$

Volendo trovare il coefficiente di q^n, è inutile considerare nella somma e/o nel prodotto gli indici superiori ad n, quindi

$$p(n|\mathbb{S}) \;=\; [q^n]G(q|\mathbb{S}) \;=\; [q^n] \prod_{\substack{k\in\mathbb{S}\\ k\le n}} \frac{1}{1-q^k}.$$

Sostituendo y con q^k nella serie

$$1/(1-y) \;=\; \sum_{m=0}^{\infty} y^m$$

otteniamo

$$1/(1-q^k) \;=\; \sum_{m=0}^{\infty} q^{km}$$

da cui risulta

$$p(n|\mathbb{S}) = [q^n] \prod_{\substack{k\in\mathbb{S}\\ k\le n}} \frac{1}{1-q^k} = [q^n] \prod_{\substack{k\in\mathbb{S}\\ k\le n}} \sum_{m_k=0}^{n} q^{km_k}.$$

Allora il coefficiente di q^n è proprio il numero delle successioni $\{m_k\}$ con $k \in \mathbb{S}$ e $k \le n$ tale che $\sum_{k=0}^{n} km_k = n$, cioè il numero $p(n|\mathbb{S})$ delle partizioni di n con le parti in $\mathbb{S}$. □

Esempio B5.5. *Calcoliamo il numero dei gruppi abeliani non isomorfi di ordine* $n = 10.668.672$.

♢ Scomponiamo in fattori primi il numero n:

$$10.668.672 = 2^7 \cdot 3^5 \cdot 7^3.$$

♢ Calcoliamo il numero delle partizioni di $7, 5, 3$:

$$p(7) \;=\; 15, \qquad p(5) \;=\; 7, \qquad p(3) \;=\; 3.$$

$\diamondsuit$ Moltiplichiamoli per ottenere il numero dei gruppi abeliani non isomorfi di ordine 10.668.672:

$$p(7)p(5)p(3) = 315.$$

Ci limitiamo a prendere $p(5)$ come un esempio per mostrare come si calcola $p(n)$ per un fissato n:

$$p(5) = [q^5] \prod_{k=1}^{5} \frac{1}{1-q^k} = [q^5] \left\{ \frac{1}{1-q} \cdot \frac{1}{1-q^2} \cdot \frac{1}{1-q^3} \cdot \frac{1}{1-q^4} \cdot \frac{1}{1-q^5} \right\}$$

dalle nozioni di analisi appena viste abbiamo:

$$\begin{aligned}
\frac{1}{1-q} &= \sum_{m_1=0}^{\infty} q^{m_1} &&= 1 + q + q^2 + q^3 + q^4 + q^5 + (q^6 + \cdots), \\
\frac{1}{1-q^2} &= \sum_{m_2=0}^{\infty} q^{2m_2} &&= 1 + q^2 + q^4 + (q^6 + \cdots), \\
\frac{1}{1-q^3} &= \sum_{m_3=0}^{\infty} q^{3m_3} &&= 1 + q^3 + (q^6 + \cdots), \\
\frac{1}{1-q^4} &= \sum_{m_4=0}^{\infty} q^{4m_4} &&= 1 + q^4 + (q^8 + \cdots), \\
\frac{1}{1-q^5} &= \sum_{m_5=0}^{\infty} q^{5m_5} &&= 1 + q^5 + (q^{10} + \cdots).
\end{aligned}$$

ovviamente ciò che è in parentesi non viene preso in considerazione, in quanto gli esponenti sono maggiori di 5; successivamente dovremo fare i prodotti ed anche in quel caso ci dovremo ricordare di eliminare i termini con esponente maggiore di 5, ottenendo così

$$p(5) = [q^5]\{1 + q + 2q^2 + 3q^3 + 5q^4 + 7q^5\} = 7.$$

Denotiamo inoltre con $p_m(n|\mathbb{S})$ il numero delle partizioni di n con m parti in $\mathbb{S}$. Possiamo analogamente dimostrare che la funzione generatrice bivariata è uguale al prodotto:

$$\sum_{m,n=0}^{\infty} p_m(n|\mathbb{S}) q^n x^m = \prod_{k\in\mathbb{S}}^{\infty} \frac{1}{1-q^k x}.$$

In particolare, la funzione generatrice delle partizioni con i diagrammi di Ferrers contenuti nel rettangolo $m \times n$ risulta il seguente coefficiente binomiale gaussiano:

$$\sum_{\lambda \subseteq [m\times n]} q^{|\lambda|} = \begin{bmatrix} m+n \\ m \end{bmatrix} = \frac{(q;q)_{m+n}}{(q;q)_m (q;q)_n}.$$

DIMOSTRAZIONE. Secondo la funzione generatrice bivariata, si vede facilmente che la funzione generatrice delle partizioni con i diagrammi di Ferrers contenuti nel rettangolo $m \times n$ è uguale al coefficiente $[x^m]\frac{1}{(x;q)_{n+1}}$.

Consideriamo le serie di Maclaurin

$$\frac{1}{(x;q)_{n+1}} = \sum_{m=0}^{\infty} \mathcal{A}_m x^m \quad \text{e} \quad \frac{1}{(qx;q)_{n+1}} = \sum_{m=0}^{\infty} \mathcal{A}_m (qx)^m.$$

Moltiplicando le due equazioni con $1-x$ e $1-q^{n+1}x$ rispettivamente, otteniamo la relazione:

$$\frac{1}{(qx;q)_n} = (1-x)\sum_{m=0}^{\infty} \mathcal{A}_m x^m = (1-q^{n+1}x)\sum_{m=0}^{\infty} \mathcal{A}_m (qx)^m.$$

Estraendo il coefficiente di x^m, abbiamo la relazione ricorrente:

$$\mathcal{A}_m - \mathcal{A}_{m-1} = q^m \mathcal{A}_m - q^{m+n}\mathcal{A}_{m-1} \quad \Longleftrightarrow \quad \mathcal{A}_m = \mathcal{A}_{m-1}\frac{1-q^{m+n}}{1-q^m}.$$

Iterando quest'ultima relazione per m-volte, si deduce che

$$\mathcal{A}_m = \mathcal{A}_0 \begin{bmatrix} m+n \\ m \end{bmatrix} \qquad \text{con} \qquad \mathcal{A}_0 = 1$$

dove $\mathcal{A}_0 = 1$ viene confermato ponendo $x = 0$ nelle serie di Maclaurin. □

B6. Automorfismi dei p-gruppi e teorema di Hall

Siano p un primo e n un numero naturale. Allora il numero dei gruppi abeliani (non isomorfi) di ordine p^n è uguale a $p(n)$, il numero delle partizioni di n. Indichiamo con q il reciproco di p, cioè $pq = 1$. Allora il fattoriale crescente di ordine n in base q viene definito come segue:

$$(q;q)_0 = 1 \quad \text{e} \quad (q;q)_n = (1-q)(1-q^2)\cdots(1-q^n) \quad \text{per} \quad n \in \mathbb{N}.$$

Lemma B6.1 (Hall, 1938). *Sia G un p-gruppo abeliano di ordine p^n con il tipo $(1^{m_1}2^{m_2}\cdots\ell^{m_\ell})$ dove $n = \sum_{k=1}^{n} k m_k$. Allora l'ordine del gruppo degli automorfismi di G è dato dal seguente prodotto:*

$$|\operatorname{Aut} G| \;=\; \prod_{k=1}^{\ell} p^{\lambda_k^2}(q;q)_{m_k}$$

dove $\lambda := (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ è la partizione coniugata alla $(1^{m_1}2^{m_2}\cdots\ell^{m_\ell})$.

DIMOSTRAZIONE. Determiniamo l'ordine degli automofismi del gruppo abeliano G di ordine p^n secondo il tipo di G, cioè, le partizioni di n.

[A] Sia G ciclico di tipo (n). Allora ogni automorfismo di G è identificabile con un generatore di G. Dunque l'ordine di $\operatorname{Aut} G$ risulta come segue:

$$|\operatorname{Aut} G| = \varphi(p^n) = p^n(1-q) = p^n(q;q)_1.$$

[B] Sia G un *gruppo elementare* di tipo (1^n). Allora G è prodotto diretto

$$G \cong \bigotimes_{k=1}^{n} H_k \quad \text{dove} \quad H_k = \langle x_k \rangle \quad \text{con} \quad o(x_k) = p.$$

È facile vedere che tutti gli elementi diversi dal'elemento neutro hanno l'ordine p. Ogni automorfismo ψ di G è determinato dalle immagini dei generatori $\{x_k\}_{k=1}^n$ come segue:

$$\begin{aligned}
&\psi(x_1) \in G\backslash\{e\} && \Longrightarrow \quad |\psi(x_1)| = p^n - 1;\\
&\psi(x_2) \in G\backslash\langle\psi(x_1)\rangle && \Longrightarrow \quad |\psi(x_2)| = p^n - p;\\
&\psi(x_3) \in G\backslash\langle\psi(x_1,x_2)\rangle && \Longrightarrow \quad |\psi(x_3)| = p^n - p^2;\\
&\qquad\vdots && \quad\vdots \qquad\qquad \vdots\\
&\psi(x_n) \in G\backslash\big\langle\psi(\{x_k|1\le k<n\})\big\rangle && \Longrightarrow \quad |\psi(x_n)| = p^n - p^{n-1}.
\end{aligned}$$

Allora l'ordine di $\operatorname{Aut} G$ uguaglia il prodotto:

$$|\operatorname{Aut} G| = \prod_{k=1}^{n}(p^n - p^{n-k}) = p^{n^2}(q;q)_n.$$

[C] Sia G di tipo (ℓ^m) con $n = m\ell$. Allora G è prodotto diretto

$$G \cong \bigotimes_{k=1}^{m} H_k \quad \text{dove} \quad H_k = \langle x_k \rangle \quad \text{con} \quad o(x_k) = p^\ell.$$

Definiamo il sottoinsieme di G con $\Omega_k := \{x \in G \mid o(x) < p^k\}$. Allora ogni automorfismo ψ di G è determinato dalle immagini dei generatori $\{x_k\}_{k=1}^m$ con $o(\psi(x_k)) = p^\ell$:

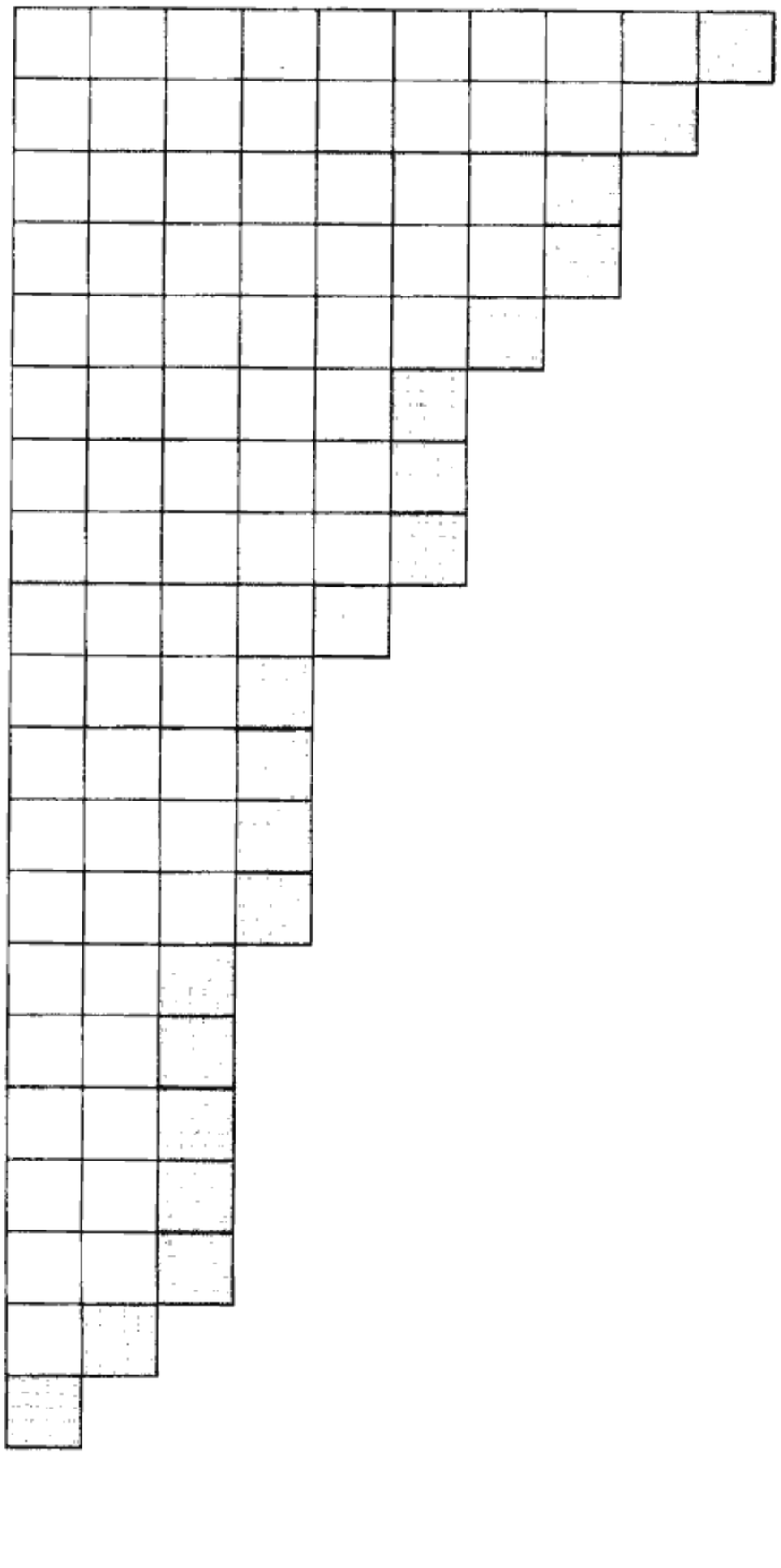
$$\begin{aligned}
&\psi(x_1) \in G\backslash\Omega_\ell && \Longrightarrow \quad |\psi(x_1)| = p^n - p^{n-m};\\
&\psi(x_2) \in G\backslash\langle\Omega_\ell,\psi(x_1)\rangle && \Longrightarrow \quad |\psi(x_2)| = p^n - p^{n-m+1};\\
&\psi(x_3) \in G\backslash\langle\Omega_\ell,\psi(x_1,x_2)\rangle && \Longrightarrow \quad |\psi(x_3)| = p^n - p^{n-m+2};\\
&\qquad\vdots && \quad\vdots \qquad\qquad \vdots\\
&\psi(x_m) \in G\backslash\big\langle\Omega_\ell,\psi(\{x_k|1\le k<m\})\big\rangle && \Longrightarrow \quad |\psi(x_m)| = p^n - p^{n-1}.
\end{aligned}$$

Allora l'ordine di $\operatorname{Aut} G$ uguaglia il prodotto:

$$|\operatorname{Aut} G| = \prod_{k=1}^{m} (p^n - p^{n-k}) = p^{mn}(q;q)_m.$$

In generale, sia G di tipo $(1^{m_1}2^{m_2}\cdots\ell^{m_\ell})$ con $n = \sum_{k=1}^{\ell} km_k$. Allora G è prodotto diretto

$$G \cong \bigotimes_{k=1}^{\ell} \bigotimes_{i=1}^{m_k} H_{ki} \quad \text{dove} \quad H_{ki} = \langle x_{ki} \rangle \quad \text{con} \quad o(x_{ki}) = p^k.$$



Indichiamo con

$$\lambda := (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell)$$

la partizione coniugata alla

$$(1^{m_1}2^{m_2}\cdots\ell^{m_\ell}).$$

Allora non è difficile stabilire le relazioni:

$\lambda_k = \sum_{j=k}^{\ell} m_j$ per $1 \leq k \leq \ell$.

Indichiamo inoltre per semplicità con X_k e X_k^ν dei sottoinsiemi dei generatori nel modo seguente:

$$X_k = \{x_{ki} | 1 \leq i \leq m_k\};$$

$$X_k^\nu = \{x_{ki} | 1 \leq i \leq \nu\}.$$

Allora ogni automorfismo ψ di G è determinato dalle immagini dei generatori $\{x_{ki}\}$ con $o(\psi(x_{ki})) = p^k$ per ogni k e i soggetti alle condizioni $1 \leq i \leq m_k$ e $1 \leq k \leq \ell$.

Prima vediamo le immagini dei generatori dell'ordine massimo p^ℓ:

$$\begin{aligned}
&\psi(x_{\ell 1}) \in G\backslash\Omega_\ell && \Longrightarrow && |\psi(x_{\ell 1})| = p^n - p^{n-m_\ell};\\
&\psi(x_{\ell 2}) \in G\backslash\langle\Omega_\ell, \psi(X_\ell^1)\rangle && \Longrightarrow && |\psi(x_{\ell 2})| = p^n - p^{n-m_\ell+1};\\
&\psi(x_{\ell 3}) \in G\backslash\langle\Omega_\ell, \psi(X_\ell^2)\rangle && \Longrightarrow && |\psi(x_{\ell 3})| = p^n - p^{n-m_\ell+2};\\
&\quad\vdots && \quad\vdots && \quad\vdots\\
&\psi(x_{\ell m_\ell}) \in G\backslash\langle\Omega_\ell, \psi(X_\ell^{m_\ell-1})\rangle && \Longrightarrow && |\psi(x_{\ell m_\ell})| = p^n - p^{n-1}.
\end{aligned}$$

Allora la cardinalità degli automorfismi determinati dai generatori di ordine p^ℓ risulta il seguente prodotto:

$$\big|\psi(X_\ell)\big| = \prod_{i=1}^{m_\ell}(p^n - p^{n-i}) = p^{nm_\ell}(q;q)_{m_\ell}.$$

Per i generatori di ordine $p^{\ell-1}$, si ha che

$$\begin{aligned}
&\psi(x_{\ell-1,1}) \in \Omega_\ell\backslash\langle\Omega_{\ell-1}, \psi(X_\ell)\rangle\\
&\qquad\Longrightarrow \quad |\psi(x_{\ell-1,1})| = p^{n-\lambda_\ell} - p^{n-\lambda_{\ell-1}};\\
&\psi(x_{\ell-1,2}) \in \Omega_\ell\backslash\langle\Omega_{\ell-1}, \psi(X_\ell, X_{\ell-1}^1)\rangle\\
&\qquad\Longrightarrow \quad |\psi(x_{\ell-1,2})| = p^{n-\lambda_\ell} - p^{n-\lambda_{\ell-1}+1};\\
&\psi(x_{\ell-1,3}) \in \Omega_\ell\backslash\langle\Omega_{\ell-1}, \psi(X_\ell, X_{\ell-1}^2)\rangle\\
&\qquad\Longrightarrow \quad |\psi(x_{\ell-1,3})| = p^{n-\lambda_\ell} - p^{n-\lambda_{\ell-1}+2};\\
&\quad\vdots \qquad\quad \vdots \qquad\quad \vdots\\
&\psi(x_{\ell-1,m_{\ell-1}}) \in \Omega_\ell\backslash\langle\Omega_{\ell-1}, \psi(X_\ell, X_{\ell-1}^{m_{\ell-1}-1})\rangle\\
&\qquad\Longrightarrow \quad |\psi(x_{\ell-1,m_{\ell-1}})| = p^{n-\lambda_\ell} - p^{n-\lambda_\ell-1}.
\end{aligned}$$

Allora la cardinalità degli automorfismi determinati dai generatori di ordine $p^{\ell-1}$ risulta il seguente prodotto:

$$\big|\psi(X_{\ell-1})\big| = \prod_{i=1}^{m_{\ell-1}}(p^{n-\lambda_\ell} - p^{n-i-\lambda_\ell}) = p^{(n-\lambda_\ell)m_{\ell-1}}(q;q)_{m_{\ell-1}}.$$

Per i generatori di ordine $p^{\ell-2}$, si ha che

$$\begin{aligned}
&\psi(x_{\ell-2,1}) \in \Omega_{\ell-1}\big\backslash\big\langle \Omega_{\ell-2}, \psi(X_\ell, X_{\ell-1})\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{\ell-2,1})| = p^{n-\lambda_\ell-\lambda_{\ell-1}} - p^{n-\lambda_\ell-\lambda_{\ell-1}-m_{\ell-2}}; \\
&\psi(x_{\ell-2,2}) \in \Omega_{\ell-1}\big\backslash\big\langle \Omega_{\ell-2}, \psi(X_\ell, X_{\ell-1}, X^1_{\ell-2})\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{\ell-2,2})| = p^{n-\lambda_\ell-\lambda_{\ell-1}} - p^{n-\lambda_\ell-\lambda_{\ell-1}-m_{\ell-2}+1}; \\
&\psi(x_{\ell-2,3}) \in \Omega_{\ell-1}\big\backslash\big\langle \Omega_{\ell-2}, \psi(X_\ell, X^2_{\ell-1}, X^2_{\ell-2})\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{\ell-1,3})| = p^{n-\lambda_\ell-\lambda_{\ell-1}} - p^{n-\lambda_\ell-\lambda_{\ell-1}-m_{\ell-2}+2}; \\
&\quad\vdots \qquad\qquad\quad \vdots \qquad\qquad\quad \vdots \\
&\psi(x_{\ell-2,m_{\ell-2}}) \in \Omega_{\ell-1}\big\backslash\big\langle \Omega_{\ell-2}, \psi(X_\ell, X_{\ell-1}, X^{m_{\ell-2}-1}_{\ell-2})\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{\ell-2,m_{\ell-2}})| = p^{n-\lambda_\ell-\lambda_{\ell-1}} - p^{n-\lambda_\ell-\lambda_{\ell-1}-1}.
\end{aligned}$$

Allora la cardinalità degli automorfismi determinati dai generatori di ordine $p^{\ell-2}$ risulta il seguente prodotto:

$$\big|\psi(X_{\ell-2})\big| = \prod_{i=1}^{m_{\ell-2}} (p^{n-\lambda_\ell-\lambda_{\ell-1}} - p^{n-i-\lambda_\ell-\lambda_{\ell-1}}) = p^{(n-\lambda_\ell-\lambda_{\ell-1})m_{\ell-2}}(q;q)_{m_{\ell-2}}.$$

Dopo aver calcolato le cardinalità degli automorfismi determinati dai generatori $\{X_\ell, X_{\ell-1}, \cdots, X_{k+1}\}$, possiamo proseguire a valutare quella degli automorfismi determinati dai generatori di ordine p^k:

$$\begin{aligned}
&\psi(x_{k,1}) \in \Omega_{k+1}\big\backslash\big\langle \Omega_k, \psi(X_j | k < j \le \ell)\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{k,1})| = p^{\sum_{j\le k}\lambda_j} - p^{\sum_{j\le k}\lambda_j - m_k}; \\
&\psi(x_{k,2}) \in \Omega_{k+1}\big\backslash\big\langle \Omega_k, \psi(X^1_k, X_j | k < j \le \ell)\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{k,2})| = p^{\sum_{j\le k}\lambda_j} - p^{\sum_{j\le k}\lambda_j - m_k+1}; \\
&\psi(x_{k,3}) \in \Omega_{k+1}\big\backslash\big\langle \Omega_k, \psi(X^2_k, X_j | k < j \le \ell)\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{k,3})| = p^{\sum_{j\le k}\lambda_j} - p^{\sum_{j\le k}\lambda_j - m_k+2}; \\
&\quad\vdots \qquad\qquad\quad \vdots \qquad\qquad\quad \vdots \\
&\psi(x_{k,m_k}) \in \Omega_{k+1}\big\backslash\big\langle \Omega_k, \psi(X^{m_k-1}_k, X_j | k < j \le \ell)\big\rangle \\
&\qquad\qquad \Longrightarrow \quad |\psi(x_{k,m_k})| = p^{\sum_{j\le k}\lambda_j} - p^{\sum_{j\le k}\lambda_j - 1}.
\end{aligned}$$

Allora la cardinalità degli automorfismi determinati dai generatori di ordine p^k risulta il seguente prodotto:

$$\big|\psi(X_k)\big| = \prod_{i=1}^{m_k} (p^{\sum_{j\le k}\lambda_j} - p^{\sum_{j\le k}\lambda_j - i}) = p^{m_k\sum_{j\le k}\lambda_j}(q;q)_{m_k}.$$

Infine, la cardinalità degli automorfismi determinati dai generatori di ordine p risulta il seguente prodotto:

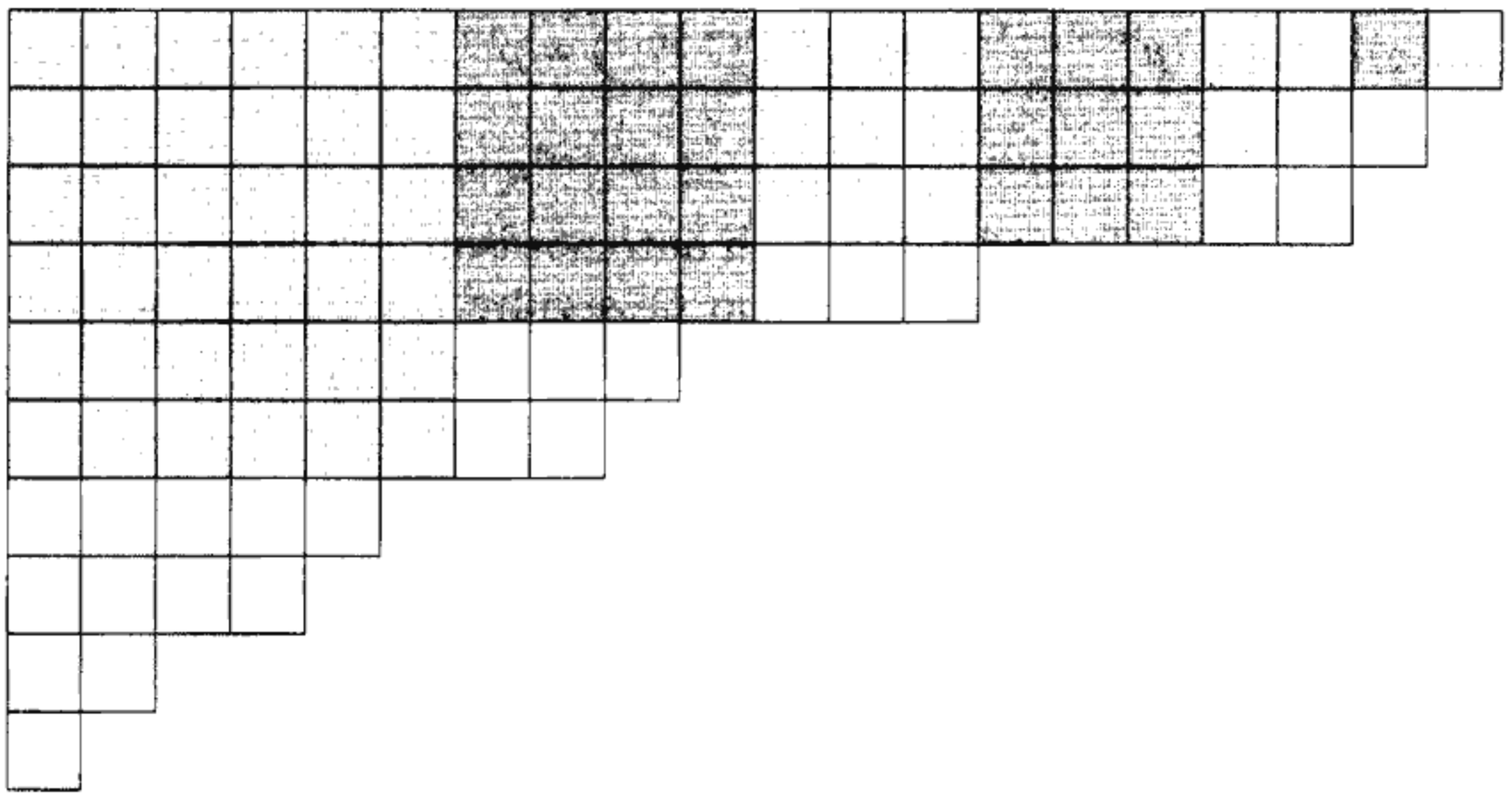
$$\left|\psi(X_1)\right| = \prod_{i=1}^{m_1}(p^{\lambda_1} - p^{\lambda_1 - i}) = p^{\lambda_1 m_1}(q;q)_{m_1}.$$

Ricapitolando quanto fatto, per un gruppo abeliano G di ordine p^n con il tipo $(1^{m_1}2^{m_2}\cdots\ell^{m_\ell})$, l'ordine del gruppo degli automorfismi di G è dato dal seguente prodotto:

$$|\mathrm{Aut}\, G| = \prod_{k=1}^{\ell} p^{m_k \sum_{j\le k}\lambda_j}(q;q)_{m_k} = \prod_{k=1}^{\ell} p^{\lambda_k^2}(q;q)_{m_k}$$

dove abbiamo applicato la seguente identità:

$$\sum_{k=1}^{\ell} m_k \sum_{j=1}^{k}\lambda_j = \sum_{j=1}^{\ell}\lambda_j \sum_{k=j}^{\ell}(\lambda_k - \lambda_{k+1}) = \sum_{j=1}^{\ell}\lambda_j^2. \qquad \square$$



Si osserva che la frazione $\frac{q^n}{(q;q)_n}$ è la funzione generatrice delle partizioni con la parte massimale uguale a n. Classifichiamo le partizioni secondo i quadrati di Durfee, i cui lati formano una partizione λ di n. Nella figura viene illustrata $n = 20$ e $\lambda = (6,4,3,3,2,1,1)$. La funzione generatrice per il primo quadrato di Durfee λ_1^2 e le partizioni sotto esso risulta $\frac{q^{\lambda_1^2}}{(q;q)_{\lambda_1}}$. La funzione generatrice per il secondo quadrato di Durfee λ_2^2 e le partizioni sotto esso risulta $\begin{bmatrix}\lambda_1\\ \lambda_2\end{bmatrix} q^{\lambda_2^2}$. In generale, la funzione generatrice per il k-esimo quadrato di Durfee λ_k^2 e le partizioni sotto esso risulta $\begin{bmatrix}\lambda_{k-1}\\ \lambda_k\end{bmatrix} q^{\lambda_k^2}$. Quindi

la funzione generatrice delle partizioni con i quadrati di Durfee determinati dalla partizione $\lambda \vdash n$ è data dal seguente prodotto:

$$\frac{q^{\lambda_1^2}}{(q;q)_{\lambda_1}} \prod_{k=2}^{\ell(\lambda)} \begin{bmatrix} \lambda_{k-1} \\ \lambda_k \end{bmatrix} q^{\lambda_k^2} = \prod_{k=1}^{\ell(\lambda)} \frac{q^{\lambda_k^2}}{(q;q)_{\lambda_k - \lambda_{k+1}}}.$$

Sommando su tutte le partizioni $\lambda \vdash n$, otteniamo l'identità:

$$\frac{q^n}{(q;q)_n} = \sum_{\lambda \vdash n} \prod_{k=1}^{\ell(\lambda)} \frac{q^{\lambda_k^2}}{(q;q)_{\lambda_k - \lambda_{k+1}}}.$$

Combinando quest'identità con il Lemma **B6.1**, abbiamo subito il seguente importante risultato.

Teorema B6.2 (Hall, 1938). *Sia Λ_n l'insieme dei gruppi abeliani* (non isomorfi) *di ordine p^n. Allora vale la seguente identità:*

$$\frac{q^n}{(q;q)_n} = \sum_{G \in \Lambda_n} \frac{1}{|\mathrm{Aut}\, G|}.$$

Classificando le partizioni secondo la parte massimale, si deduce conseguentemente un ulteriore risultato tramite la formula di Eulero.

Corollario B6.3 (Funzione generatrice).

$$\frac{1}{(qx;q)_\infty} = \sum_{n=0}^{\infty} \frac{(qx)^n}{(q;q)_n} = \sum_{n=1}^{\infty} \sum_{G \in \Lambda_n} \frac{x^n}{|\mathrm{Aut}\, G|}.$$

□