Università degli Studi di Padova
Dipartimento di Matematica 'Tullio Levi-Civita'
Corso di Laurea in Matematica

Purità e compattezza algebrica per gruppi abeliani

RELATRICE **Prof.ssa Silvana Bazzoni**
CANDIDATO **Marco Morosin**
1146942

18.10.2019

Indice

Introduzione

Lo scopo di questo testo è presentare la nozione di purità, usualmente studiata in teoria dei moduli, nell'ambito più ristretto dei gruppi abeliani. In effetti, essa nasce proprio in questo contesto, ad opera di Prüfer nel 1923.

La purità descrive una particolare 'modalità' in cui un sottogruppo è contenuto nell'intero gruppo. Per esempio, il modo 'più semplice' in cui questo avviene è quando un sottogruppo è addendo diretto, perché in tal caso lo studio del gruppo è ricondotto allo studio delle sue componenti. La proprietà di purità è un indebolimento della proprietà di essere addendo diretto e, sotto opportune condizioni, è equivalente; il secondo capitolo è dedicato allo studio di queste condizioni.

Il terzo capitolo è dedicato allo studio delle classi di gruppi definibili in termini di purità, precisamente quelli che hanno la proprietà iniettiva o proiettiva rispetto a un particolare tipo di sequenze esatte, dette *pure-esatte*. Questo è interessante per diversi motivi. In primo luogo, si evidenzia una 'asimmetria' della dualità: vedremo che i puri-proiettivi sono semplicemente le somme dirette di gruppi ciclici, mentre i puri-iniettivi, sebbene 'duali' dei primi, hanno una caratterizzazione più complicata, e per questo occupano l'intero ultimo capitolo. Mostreremo che i puri-iniettivi sono esattamente i gruppi *algebricamente compatti* e li osserveremo sotto diversi aspetti, algebrici e topologici. Proprio grazie al loro studio topologico riusciremo poi a darne una caratterizzazione semplice, in termini di completezza, che ci porterà a concludere con un teorema di struttura.

Infine, il motivo per cui questo studio è interessante, come tesi triennale, è che il percorso per giungere a questi risultati richiede la conoscenza di diverse nozioni importanti non affrontate nel corso di laurea, per esempio: il teorema di struttura dei gruppi abeliani finitamente generati, lo studio dei gruppi divisibili, l'uso di topologie lineari su un gruppo e i loro completamenti. Per questo motivo il primo capitolo, di preliminari, occupa una parte rilevante del testo.

Capitolo 1

Preliminari

Nella seguente trattazione, A indicherà sempre il gruppo abeliano $(A, +)$.

Definiamo i seguenti insiemi:

$$nA = \{na \mid a \in A\} \qquad\qquad A[n] = \{a \in A \mid na = 0\}$$

e diciamo che un gruppo A è *limitato* o, più precisamente, *n-limitato*, se esiste $n \in \mathbb{Z} \setminus \{0\}$ tale che $nA = \{0\}$, cioè $A = A[n]$.

Indichiamo l'ordine di un elemento a con la notazione $\mathrm{o}(a)$. La *torsione* di A è il suo sottoinsieme (sottogruppo se A è abeliano)

$$\mathrm{T}(A) = \bigcup_{n \geq 0} A[n],$$

cioè l'insieme degli elementi di A di ordine finito. Se $T(A) = A$ diciamo che A è (un gruppo) *di torsione*; se $T(A) = \{0\}$ diciamo che A è *senza torsione*; se $\{0\} < T(A) < A$ diciamo che A è un gruppo *misto*. Gruppi limitati, per esempio, sono gruppi di torsione.

Chiamiamo *p-altezza* di $a \in A$ il più grande naturale r tale che $p^r x = a$ abbia soluzione in A (la poniamo uguale a ∞ se esiste soluzione per ogni r). La indichiamo con $\mathrm{h_p}(a)$.

1.1 Generatori e cogeneratori

[In questo testo, indicheremo il gruppo ciclico di ordine $n \in \mathbb{N}$ indifferentemente con $\mathbb{Z}(n)$ o con $\mathbb{Z}/n\mathbb{Z}$].

Sappiamo che un gruppo A si dice *ciclico* se $A = \langle a \rangle$, esiste $a \in A$, e diciamo che un tale a è un *generatore* del gruppo. Vale la caratterizzazione: un gruppo è ciclico se e solo se esiste $a \in A$ tale che, per ogni gruppo A' e ogni omomorfismo $\phi\colon A' \to A$, $a \in \operatorname{im} \phi$ implica ϕ suriettivo. Questa caratterizzazione permette di dualizzare la nozione di gruppo ciclico: un gruppo A si dice *cociclico* se esiste $a \in A$ tale che, per ogni gruppo A' e ogni omomorfismo $\phi\colon A \to A'$, $a \notin \ker \phi$ implica ϕ iniettivo. Chiamiamo a un *cogeneratore* del gruppo.

1.1.1 Lemma. *Un gruppo A è cociclico se e solo se l'intersezione di tutti i suoi sottogruppi non banali è non banale.*

Dimostrazione. Se A è cociclico con cogeneratore a, ogni suo sottogruppo non banale contiene a: infatti, B è nucleo del morfismo $\phi\colon A \to A/B$, $x \mapsto x + B$ e, essendo $B = \ker\phi$ non banale e A cociclico, dev'essere $a \in \ker\phi = B$. Viceversa, dato un gruppo A, esista $a \neq 0$ appartenente all'intersezione di tutti i suoi sottogruppi non banali; mostriamo che a è cogeneratore di A. Consideriamo un morfismo $\phi\colon A \to A'$: se $a \notin \ker\phi$, essendo $\ker\phi \leq A$, $\ker\phi$ dev'essere banale. $\square$

1.1.2 Lemma. *Sia $a \in A \setminus \{0\}$ e sia $M \leq A$ massimale tra i sottogruppi che non contengono a. Allora A/M è cociclico.*

Dimostrazione. Per la proprietà di massimalità, ogni sottogruppo di A contenente propriamente M contiene a; di conseguenza ogni sottogruppo non nullo di A/M contiene $a + M$, dunque A/M è cociclico per il lemma 1.1.1. $\square$

1.1.3 Definizione. Indichiamo con $\mathbb{Z}(p^\infty)$ il *p-gruppo quasiciclico* (o p-gruppo di Prüfer), che può essere definito nei seguenti modi equivalenti:

- $\mathbb{Z}(p^\infty) = \bigcup_{n\in\mathbb{N}} \mathbb{Z}(p^n)$, dove un gruppo ciclico di ordine p^{n-1} è visto come sottogruppo del gruppo ciclico di ordine p^n; l'inclusione fa corrispondere a un generatore c_{n-1} di $\mathbb{Z}(p^{n-1})$ l'elemento $pc_n \in \mathbb{Z}(p^n)$ dove c_n è un generatore di $\mathbb{Z}(p^n)$.
- $\mathbb{Z}(p^\infty) = \bigcup_{n\in\mathbb{N}} \{\xi \in \mathbb{C} \mid \xi^{p^n} = 1\}$, unione su n dei gruppi (moltiplicativi) delle radici p^n-esime dell'unità;
- $\mathbb{Z}(p^\infty) = \langle c_1, c_2, \cdots \mid pc_1 = 0,\ pc_{n+1} = c_n\ \forall n \geq 1\rangle$;
- $\mathbb{Z}(p^\infty) = \mathbb{Z}[1/p]/\mathbb{Z}$, dove $(\mathbb{Z}[1/p], +)$ è il gruppo dei razionali che hanno per denominatori (nella forma ridotta ai minimi termini) potenze di p;

è l'unico p-gruppo abeliano infinito localmente ciclico (ogni sottogruppo finitamente generato è ciclico).

1.1.4 Teorema. *Un gruppo è cociclico se e solo se è isomorfo a $\mathbb{Z}(p^k)$ con k naturale o al gruppo quasiciclico $\mathbb{Z}(p^\infty)$.*

Dimostrazione. $\mathbb{Z}(p^k)$ con $k \in \mathbb{N}$ è generato da un elemento a di ordine p^k e ha come unici sottogruppi

$$\{0\} < \langle p^{k-1}a\rangle < \cdots < \langle pa\rangle < \langle a\rangle$$

quindi $\langle p^{k-1}a\rangle$ è il suo minimo sottogruppo non banale. Nel gruppo quasiciclico $\mathbb{Z}(p^\infty)$, inoltre, ogni sottogruppo proprio è ciclico di ordine p^k per qualche k.

Viceversa, sia $c \in C$ un cogeneratore di C. Allora c è contenuto in ogni sottogruppo non banale e $\langle c\rangle$ è il più piccolo sottogruppo non banale: segue che c ha ordine primo p e che C non contiene elementi di ordine infinito, né di ordine primo $q \neq p$; quindi C è un p-gruppo. Dimostriamo per induzione che, per ogni n, C ha un unico sottogruppo ciclico di ordine p^n. Il caso $n = 0$ è banale; per ipotesi induttiva, C contenga un unico sottogruppo C_n di ordine p^n, ciclico generato da $\langle c_n\rangle$. Mostriamo quindi che $A, B \leq C$ con $|A| = |B| = p^{n+1}$ implica $A = B$. Siano $a \in A\backslash C_n$, $b \in B\backslash C_n$; allora $a, b \notin C_n$ implica $o(a) = o(b) = p^{n+1}$, quindi $pa, pb \in C_n$, diciamo $pa = rc_n$, $pb = sc_n$ per opportuni r, s coprimi con p. Scegliamo r', s' tali che $rr' = 1 = ss' \bmod p^n$, così $a' := r'a$, $b' := s'b$ soddisfano

$\langle a' \rangle = \langle a \rangle, pa' = c_n, \langle b' \rangle = \langle b \rangle, pb' = c_n$. Si ha $p(a' - b') = 0$, $a' - b' = tc_n$ per qualche intero t, quindi $a' = b' + tpb'$, $b' = a' - tpa'$ e $\langle a' \rangle = \langle b' \rangle$ e si conclude $A = \langle a \rangle = \langle b \rangle = B$ come voluto. $\square$

Più in generale: se $A = \langle S \rangle$ con $S \subseteq A$, S finito, A si dice *finitamente generato*. Vale la caratterizzazione: $S \subseteq A$ è un insieme di generatori per A se e solo se, per ogni gruppo A' e ogni omomorfismo $\phi\colon A' \to A$, $S \subseteq \operatorname{im} \phi$ implica ϕ suriettivo. Dualizzando: $S \subseteq A$ è un insieme di cogeneratori per A se e solo se, per ogni gruppo A' e ogni omomorfismo $\phi\colon A \to A'$, $S \cap \ker \phi \in \{\emptyset, \{0\}\}$ implica ϕ iniettivo. Se esiste un tale S finito, A si dice *finitamente cogenerato*.

1.2 Proprietà iniettiva e proprietà proiettiva

1.2.1 Definizione. Una sequenza

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0 \tag{1.1}$$

si dice *esatta* se $\ker \alpha = \{0\}$, $\operatorname{im} \alpha = \ker \beta$, $\operatorname{im} \beta = C$.

Senza perdita di generalità, poiché $A \cong \alpha(A)$ e $C \cong B/\ker(\beta)$, possiamo supporre che una generica sequenza esatta sia del tipo

$$0 \longrightarrow A \overset{\iota}{\hookrightarrow} B \overset{\pi}{\twoheadrightarrow} B/A \longrightarrow 0$$

con A sottogruppo di B, ι inclusione e π proiezione sul quoziente, e lo faremo ove questo semplifichi le notazioni.

1.2.2 Definizione. Diciamo che un gruppo G ha la *proprietà iniettiva* rispetto alla sequenza (1.1) se per ogni morfismo $\phi\colon A \to G$ esiste $\psi\colon B \to G$ tale che $\psi\alpha = \phi$, ovvero tale che il seguente diagramma sia commutativo:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\alpha"] \arrow[d, "\phi"] & B \arrow[r, "\beta"] \arrow[dl, dashed, "\psi"] & C \arrow[r] & 0 \\
& G & & &
\end{tikzcd}$$

Dualmente, diciamo che un gruppo G ha la *proprietà proiettiva* se per ogni morfismo $\phi\colon G \to C$ esiste $\psi\colon G \to B$ tale che $\beta\psi = \phi$, ovvero tale che il seguente diagramma sia commutativo:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r, "\beta"] & C \arrow[r] & 0 \\
& & & G \arrow[u, "\phi"] \arrow[ul, dashed, "\psi"] &
\end{tikzcd}$$

1.2.3 Definizione. Un gruppo G si dice *iniettivo* se ha la proprietà iniettiva rispetto a ogni sequenza esatta. Si dice *proiettivo* se ha la proprietà proiettiva rispetto a ogni sequenza esatta.

1.3 Somme dirette e prodotti diretti

1.3.1 Definizione (Somma diretta interna)**.** Dato A, se esiste una famiglia di suoi sottogruppi B_i (indiciata su I arbitrario) tale che

$$\sum_i B_i = A \qquad \text{e} \qquad B_j \cap \sum_{i \neq j} B_i = \{0\}$$

si dice che A è *somma diretta (interna)* dei sottogruppi B_i (indicata con $A = \bigoplus_i B_i$) e che ogni B_i è un suo *addendo diretto.*

Ogni elemento di A si scrive in modo unico come somma di elementi di elementi dei B_i, cioè $a = b_{i_1} + \cdots + b_{i_k}$ per qualche intero k e alcuni $i_j \in I$, $j = 1, \ldots, k$.

Una somma diretta $A = \bigoplus B_i$ definisce una famiglia di epimorfismi $\pi_i \colon A \to B_i$, $(b_{i_1} + \cdots + b_{i_k}) \mapsto b_i$ con le proprietà:

1. $\pi_i \pi_i = \pi_i$ (idempotenza; chiamiamo *proiezione* un morfismo che soddisfi questa proprietà);
2. $\pi_i \pi_j = 0$ se $i \neq j$ (ortogonalità);
3. $\sum_{i \in I} \pi_i = 1_A$;

e, per famiglie infinite, anche

4. $\pi_i(a) = 0$ per quasi tutti gli $i \in I$.

Viceversa:

1.3.2 Lemma. *Se, dato A, esiste una famiglia di endomorfismi di A con queste proprietà, allora $A = \bigoplus_i \operatorname{im} \pi_i$.*

Dimostrazione. Verifichiamo che $A \subseteq \sum_i \operatorname{im} \pi_i$ (l'altra inclusione è ovvia): dato $a \in A$ si ha $a = \sum_i \pi_i(a)$ per la condizione (3) e $\sum_i \pi_i(a) = \sum_{k=1}^n \pi_{i_k}(a)$ (esistono n e i_k per $k = 1 \cdots n$) per la condizione (4), quindi $a \in \sum_i \operatorname{im} \pi_i$. Se poi $a \in \operatorname{im} \pi_i \cap \sum_{j \neq i} \operatorname{im} \pi_j$ allora $a = \pi_i(x_i) = \sum_{k=1}^n \pi_{j_k}(x_{j_k})$ ($j_k \neq i$ per ogni $k = 1, \ldots, n$), quindi usando (1) e (2) si ha

$$a = \pi_i(x_i) = \pi_i(\pi_i(x_i)) = \pi_i(\sum_{k=1}^n \pi_{j_k}(x_{j_k})) = \sum_{k=1}^n \pi_i(\pi_{j_k}(x_{j_k})) = 0$$

. □

1.3.3 Corollario. *Se π è endomorfismo di A idempotente (i.e. una proiezione), allora* $\operatorname{im} \pi$ *è addendo diretto di A.*

Dimostrazione. I due morfismi π e $1_A - \pi$ soddisfano le proprietà descritte sopra. Dunque $A = \operatorname{im} \pi \oplus \operatorname{im} 1_A - \pi = \operatorname{im} \pi \oplus \ker \pi$. □

1.3.4 Corollario. *Se B è sottogruppo di A, sono equivalenti:*

- *B è addendo diretto di A;*
- *l'identità 1_B può essere fattorizzata come $B \xrightarrow{\iota} A \xrightarrow{\pi} B$, ove ι è l'inclusione.*

Dimostrazione. Se B è addendo diretto di A, si prende come π la proiezione suriettiva sul sottogruppo B. Viceversa, data la fattorizzazione, $\pi \restriction_B$ è idempotente e ha come immagine B, e si conclude per il corollario 1.3.3. □

1.3.5 Lemma. *Se $A = B \oplus C$, allora $C \cong A/B$*

Dimostrazione. Se $A = B \oplus C$ è definita la proiezione $\pi_C\colon A \to C$, $a = b+c \mapsto c$, suriettiva con nucleo B, quindi $C = \operatorname{im} \pi_C = A/\ker \pi_C = A/B$. □

1.3.6 Definizione (Prodotto diretto)**.** Data una famiglia di gruppi $\{B_i\}_i$ (indiciata su i arbitrario), il prodotto cartesiano $\prod_i B_i$ è dotato di una struttura di gruppo con l'operazione $(\cdots b_i \cdots) + (\cdots b'_i \cdots) = (\cdots b_i + b'_i \cdots)$. Chiamiamo questo gruppo il *prodotto diretto* dei gruppi B_i.

Sono definite le proiezioni π_i, suriettive, e le inclusioni ι_i, iniettive:

$$\begin{aligned} \pi_i\colon \prod_{i\in I} B_i &\to B_i & \qquad \iota_i\colon B_i &\to \prod_{i\in I} B_i \\ (\cdots b_i \cdots) &\mapsto b_i & b_i &\mapsto (0 \cdots b_i \cdots 0) \end{aligned}$$

Gli $\iota_i(B_i)$ sono sottogruppi di $\prod_i B_i$ isomorfi ai B_i, e generano il seguente sottogruppo del prodotto diretto:

1.3.7 Definizione (Somma diretta esterna)**.** Chiamiamo *somma diretta (esterna)* dei gruppi B_i il sottogruppo

$$\bigoplus_{i\in I} B_i := \{(\cdots b_i \cdots) \in \prod_{i\in I} B_i \mid b_i = 0 \text{ per quasi ogni } i \in I\} = \langle \iota_i(B_i)\rangle_i$$

di $\prod_i B_i$.

Il gruppo $\bigoplus_i B_i$ può essere visto come la somma diretta interna dei suoi sottogruppi $\iota_i(B_i)$ e, viceversa, un gruppo A che sia somma diretta interna dei suoi sottogruppi B_i è isomorfo alla somma diretta esterna dei gruppi B_i.

Dimostriamo ora alcuni risultati importanti, che saranno utili in seguito.

1.3.8 Definizione. Chiamiamo *gruppo abeliano libero* una somma diretta di gruppi ciclici infiniti, cioè $F = \bigoplus_i \langle x_i \rangle$ con $\mathrm{o}(x_i) = \infty$. In tal caso si dice anche che F è libero sull'insieme $X = \{x_i \mid i \in I\}$, e che X è un insieme libero di generatori per F. Un gruppo libero F è, a meno di isomorfismo, determinato univocamente dal numero cardinale dell'insieme I.

Dato un insieme di generatori $X = \{x_i \mid i \in I\}$, $\langle X \rangle$ è un gruppo abeliano libero su X se e solo se, per ogni gruppo abeliano A, ogni mappa $X \to A$ ha una e una sola estensione a un omomorfismo $F \to A$. Di conseguenza, ogni gruppo abeliano è immagine omomorfa di un gruppo abeliano libero: se A ha al più $\mathfrak{m}$ generatori a_i, consideriamo una mappa $x_i \mapsto a_i$ ed estendiamola a un omomorfismo $\psi\colon F \to A$, cosicché $A = \psi(F) \cong F/\ker \psi$.

1.3.9 Lemma. *Se B è sottogruppo di A tale che A/B è un gruppo libero, B è addendo diretto di A.*

Dimostrazione. Se $A/B = \bigoplus_i \langle a_i + B \rangle$ è gruppo abeliano libero, allora $A = \langle a_i \rangle_i \oplus B$. Infatti $A = \langle a_i \rangle_i + B$ perché $a \in A$ implica $a + B = a_1 + \cdots + a_k + B$ e quindi $a = a_1 + \cdots + a_k + b$ per un $b \in B$; inoltre $\langle a_i \rangle_i \cap B = \{0\}$ segue da $\mathrm{o}(a_i + B) = \infty$. □

1.3.10 Teorema. *Sottogruppi di gruppi liberi sono gruppi liberi.*

Dimostrazione. Sia $F = \bigoplus_{i \in I} \langle a_i \rangle$ gruppo abeliano libero, e sia I ben ordinato. Sia I l'insieme degli ordinali $< \alpha$. Per $\beta \leq \alpha$ definiamo $F_\beta = \bigoplus_{\gamma < \beta} \langle a_\gamma \rangle$. Dato $H \leq F$, poniamo $H_\beta = H \cap F_\beta$. Abbiamo $H_\beta = H_{\beta+1} \cap F_\beta$ e quindi

$$\frac{H_{\beta+1}}{H_\beta} = \frac{H_{\beta+1}}{(H_{\beta+1} \cap F_\beta)} \cong \frac{(H_{\beta+1} + F_\beta)}{F_\beta} \leq \frac{F_{\beta+1}}{F_\beta} \cong \langle a_\beta \rangle$$

e ci sono quindi due possibilità: $H_{\beta+1} = H_\beta$ oppure $H_{\beta+1}/H_\beta$ è ciclico infinito. In ogni caso, per il precedente lemma, $H_{\beta+1} = H_\beta \oplus \langle b_\beta \rangle$ per un $b_\beta \in H_{\beta+1}$ (eventualmente $b_\beta = 0$, nel primo caso). Segue che gli elementi $\langle b_\beta \rangle$ generano la somma diretta $\bigoplus_\beta \langle b_\beta \rangle$ e questa dev'essere $= H$, perché $H = \bigcup_\beta H_\beta$. □

1.3.11 Teorema. *Un gruppo abeliano è libero se e solo se è proiettivo.*

Dimostrazione. Consideriamo F abeliano libero sull'insieme $\{x_i \mid i \in I\}$ e un morfismo ϕ come nel seguente

$$\begin{tikzcd} B \arrow[r, two heads, "\beta"] & C \\ & F \arrow[u, "\phi"'] \arrow[ul, dashed, "\psi"] \end{tikzcd}$$

Per suriettività di β, per ogni i esiste $b_i \in B$ tale che $\beta(b_i) = \phi(x_i)$. Si può definire uno e un solo $\psi \colon F \to B$ che rispetti $\psi(x_i) = b_i$ per ogni i, e tale ψ soddisfa $\beta\psi = \phi$ come voluto.

Viceversa, sia A proiettivo e $\beta \colon F \to A$ epimorfismo con F abeliano libero. Per la proprietà proiettiva

$$\begin{tikzcd} F \arrow[r, two heads, "\beta"] & A \\ & A \arrow[u, "1_A"'] \arrow[ul, dashed, "\psi"] \end{tikzcd}$$

esiste ψ tale che $\beta\psi = 1_A$. Quindi (corollario 1.3.4) $A \cong \psi(A)$ è addendo diretto di F, quindi per il teorema precedente è un gruppo libero. □

Abbiamo il seguente fondamentale

1.3.12 Teorema (di struttura dei gruppi abeliani finitamente generati)**.** *Un gruppo abeliano A è finitamente generato se e solo se è somma diretta finita di gruppi ciclici, e si può scegliere una decomposizione del tipo*

$$\mathbb{Z}^{\oplus r} \oplus \mathbb{Z}(p_1^{n_1}) \oplus \cdots \oplus \mathbb{Z}(p_k^{n_k})$$

con i p_i primi non necessariamente distinti.

Usiamo un lemma preliminare:

1.3.13 Lemma. *Se* $A = \langle a_1, \dots, a_k \rangle$*, dati* $n_1, \dots, n_k \in \mathbb{N}$ *con* $(n_1, \dots, n_k) = 1$*, allora esistono* $b_1, \dots, b_k \in A$ *tali che*

$$A = \langle b_1, \dots, b_k \rangle \text{ con } b_1 = n_1 a_1 + \cdots + n_k a_k.$$

Dimostrazione. Per induzione su $n = n_1 + \cdots + n_k$. Se $n = 1$ allora a meno di riordinamenti è $n = n_1 = 1$ e basta prendere $b_i = a_i$ per ogni i. Sia $n > 1$: possiamo supporre $n_1 \geq n_2 > 0$. Allora

- $(n_1 - n_2, n_2, \dots, n_k) = 1$
- $(n_1 - n_2) + n_2 + \cdots + n_k < n$
- $A = \langle a_1, a_1 + a_2, \dots, a_k \rangle$

e quindi per ipotesi induttiva esistono $b_1, \dots, b_k \in A$ tali che

$$\begin{aligned} A = \langle b_1, \dots, b_k \rangle \text{ con } b_1 &= (n_1 - n_2) a_1 + n_2 (a_1 + a_2) + \cdots + n_k a_k = \\ &= n_1 a_1 + \cdots + n_k a_k. \end{aligned}$$

□

Dimostrazione del teorema 1.3.12. Ovviamente una somma diretta finita di gruppi ciclici $\langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle$ è finitamente generata da $\{x_1, \dots, x_n\}$.

Viceversa, sia A finitamente generato e sia n il minimo numero di generatori di A. Se $n = 1$ allora $A = \langle x_1 \rangle$. Supponiamo ora $n > 1$ e scegliamo un sistema di n generatori $\{x_1, \dots, x_n\}$ tale che x_1 abbia ordine minimo. Mostriamo che $A = \langle x_1 \rangle \oplus \langle x_2, \dots, x_n \rangle$, da cui la conclusione applicando l'ipotesi induttiva a $\langle x_2, \dots, x_n \rangle$.
Se tale somma non è diretta, esistono $c_i \in \mathbb{Z}$ tali che

$$c_1 x_1 + \cdots + c_n x_k = 0, \quad c_1 x_1 \neq 0$$

e, a meno di cambiare i segni di qualche x_i, possiamo supporre i $c_i \in \mathbb{N}$ e $c_1 < \mathrm{o}(x_1)$. Sia $c = (c_1, \dots, c_n)$, $c_i = q_i c$; per il lemma precedente, esiste un sistema di generatori tale che

$$A = \langle b_1, \dots, b_k \rangle \quad \text{con} \quad b_1 = q_1 a_1 + \cdots + q_k a_k,$$

da cui

$$c b_1 = c_1 a_1 + \cdots + c_k a_k = 0,$$

e quindi $\mathrm{o}(b) \leq c \leq c_1 < \mathrm{o}(x_1)$ contraddice la scelta di $\{x_1, \dots, x_n\}$. La scelta di una decomposizione come quella descritta nell'enunciato segue osservando che, se c'è un addendo $\langle x \rangle$ con $\mathrm{o}(x) = p^n m$ e $(m, p) = 1$, allora $\langle x \rangle = \langle mx \rangle \oplus \langle p^n x \rangle \cong \mathbb{Z}/p^n\mathbb{Z} \oplus \langle p^n x \rangle$; basta allora iterare il ragionamento. □

Vale un teorema analogo, di cui tralasciamo la dimostrazione, per i gruppi finitamente cogenerati: *un gruppo abeliano A è finitamente cogenerato se e solo se è somma diretta finita di gruppi cociclici.*

1.3.14 Teorema. *Un gruppo di torsione A è somma diretta di p-gruppi A_p (detti p-componenti) per alcuni primi p, determinati univocamente da A.*

Dimostrazione. Sia $A_p = \{a \in A \mid \mathrm{o}(a) = p^k,\ \exists k \in \mathbb{Z}\}$, non vuoto in quanto $0 \in A_p$. Si vede facilmente che $A_p \leq A$, e che $A_p \cap (A_{p_1} + \cdots + A_{p_k}) = \{0\}$ se $p \neq p_1, \ldots, p_k$, dunque gli A_p generano la somma diretta $\bigoplus_p A_p \leq A$; vogliamo mostrare $\bigoplus_p A_p \geq A$. Sia $a \in A$, $\mathrm{o}(a) = m = p_1^{r_1} \cdots p_n^{r_n}$ con primi distinti. Gli interi $m_i = mp_i^{-r_i}$ $(i = 1, \ldots, n)$ sono primi tra loro, quindi $a = s_1 m_1 a + \cdots + s_n m_n a$ per opportuni s_i; si noti che $m_i a \in A_{p_i}$. Questo mostra che $a \in A_{p_1} + \cdots + A_{p_n} \leq \bigoplus_p A_p$.
Mostriamo l'unicità degli A_p: se $A = \bigoplus_p B_p$ è un'altra decomposizione in p-gruppi, $B_p \leq A_p$ per definizione di A_p, ma, poiché $\bigoplus_p A_p = \bigoplus_p B_p$, deve aversi l'uguaglianza per ogni p. □

1.3.15 Teorema (Kulikov)**.** *Sia A un p-gruppo. Allora A è somma diretta di gruppi ciclici se e solo se*

$$A = \bigcup_{n \geq 1} A_n \qquad \text{con } A_1 \leq A_2 \leq \cdots \leq A_n \leq \cdots \leq A$$

tali che gli elementi non nulli di A_n abbiano p-altezze minori di un intero k_n.

Dimostrazione. Se un p-gruppo A è somma diretta di gruppi ciclici, definiamo B_i come la somma diretta di tutte le componenti dello stesso ordine p^i. Allora $A_n = B_1 \oplus \cdots \oplus B_n$ soddisfa la condizione enunciata, e possiamo prendere $k_n = n$.

Viceversa, siano A_i come nell'enunciato. Eventualmente aggiungendo qualche $\{0\}$ all'inizio della catena, o ripetendo qualche A_i un numero finito di volte, non lede la generalità assumere $k_n = n$, ovvero $A_n \cap p^n A = \{0\}$, per ogni n. Consideriamo l'insieme delle catene

$$\mathscr{P} = \{C_1 \leq \ldots C_n \leq \cdots \mid A_n \leq C_n,\ C_n \cap p^n A = \{0\}\}$$

con l'ordine parziale

$$\{C_i\}_i \leq \{D_i\}_i \text{ se e solo se } C_n \leq D_n \text{ per ogni } n.$$

$(\mathscr{P}, \leq)$ è induttivo, quindi per il lemma di Zorn esiste una catena $\{M_i\}_i$ massimale.
Per ogni n, sia L_n sottoinsieme linearmente indipendente massimale di $M_n[p] \cap p^{n-1}A$, e sia $L = \bigcup_n L_n$. Dato $l_i \in L$ con $h_i = \mathrm{h_p}(l_i)$, sia $a_i \in A$ tale che $p^{m_i} a_i = l_i$. Mostriamo $\bigoplus_i \langle a_i \rangle = A$.
Mostriamo per induzione che $\langle L \rangle = A[p]$. Si ha $\langle L_n \rangle = M_n[p] \cap p^{n-1}A$ per la proprietà di massimalità. Gli elementi $\neq 0$ di $\langle L_n \rangle$ hanno altezza $n-1$, quindi $\langle L \rangle = \bigoplus_n \langle L_n \rangle$. Il caso base, ovvero $a \in A[p] \cap M_1$ implica $a \in \langle L \rangle$, è soddisfatto.
Per ipotesi induttiva, $a \in A[p] \cap M_n$ implica $a \in \langle L \rangle$. Consideriamo $b \in M_{n+1}[p] \backslash M_n$; $b \notin M_n$ implica $\langle M_n, b \rangle \cap p^n A \neq 0$, quindi sia $0 \neq g + kb = c \in p^n A$ per un $g \in M_n$, e supponiamo anche che $k = 1$ (perché in caso contrario possiamo moltiplicare per un k' tale che $kk' \equiv 1 \bmod p$). $c \in M_{n+1}$ e $\mathrm{h_p}(c) \geq n$, quindi (essendo $M_i \cap p^i A = \{0\}$) $\mathrm{o}(c) = p$ e $\mathrm{h_p}(c) = n$. Dunque $c \in \langle L_{n+1} \rangle$. Inoltre, le relazioni $pg = pc - pb = 0$ e $g \in M_n$, insieme all'ipotesi induttiva, implicano $g \in \langle L \rangle$. Allora $b = c - g \in \langle L \rangle$, da cui $\langle L \rangle = A[p]$.
Supponiamo ora che ogni $a \in A$ con $\mathrm{o}(a) \leq p^n$ appartenga a $\bigoplus_i \langle a_i \rangle$; sia $b \in A$ con $\mathrm{o}(b) = p^{n+1}$, $n \geq 1$. Come già mostrato, $p^n b \in \langle L \rangle$ e quindi

$p^n b = h_1 l_1 + \cdots + h_k l_k$ per alcuni $l_i \in L$. Sia $\mathrm{h_p}(l_i) \geq n$ per $i = 1, \ldots, j$ e $\mathrm{h_p}(l_i) \leq n - 1$ per $i = j+1, \ldots, n$ (per qualche $j \leq n$). Se scriviamo $h_i l_i = p^n h_i' a_i$ per $i = 1, \ldots, j$, allora abbiamo

$$p^n(b - h_1' a_1 - \cdots - h_j' a_j) = h_{j+1} l_{j+1} + \cdots + h_k l_k \in M_{n-1}.$$

La condizione $M_i \cap p^i A = \{0\}$ implica che $b - h_1' a_1 - \cdots - h_j' a_j$ ha ordine $\leq p^n$, quindi è in $\bigoplus_i \langle a_i \rangle$, quindi $b \in \bigoplus_i \langle a_i \rangle$. □

1.3.16 Teorema. *Sottogruppi di somme dirette di gruppi ciclici sono somme dirette di gruppi ciclici.*

Dimostrazione. Caso 1: A è somma diretta di p-gruppi ciclici. Allora, $A = \bigcup_{n \geq 1} A_n$ con gli A_n come nel teorema precedente. Sia $B \leq A$: allora $B = \bigcup_{n \geq 1} B_n$ con $B_n = B \cap A_n$ che soddisfano le ipotesi del teorema precedente, da cui si conclude che B è somma diretta di gruppi ciclici.
Caso generale: sia $T = \mathrm{T}(A)$: si ha $\mathrm{T}(B) = T \cap B$ e $B/(B \cap T) \cong (B+T)/T \leq A/T$, che è un gruppo libero. Allora $B/(B \cap T)$ è un gruppo libero, e quindi esiste un gruppo libero C tale che $B = (B \cap T) \oplus C$. $(B \cap T)$ è somma diretta di p-gruppi ciclici, perché di torsione, mentre C è somma diretta di gruppi ciclici infiniti, perché gruppo libero. □

1.3.17 Definizione. Un sottogruppo B di A si dice *pienamente invariante* se $\phi(B) \leq B$ per ogni ϕ endomorfismo di A.

1.3.18 Lemma. *Se $A = B \oplus C$ e F è sottogruppo pienamente invariante di A, allora*

$$F = (F \cap B) \oplus (F \cap C).$$

Dimostrazione. Per la totale invarianza di F, si ha $\pi_B(F), \pi_C(F) \leq F$, quindi $\pi_B(F) \leq F \cap B$ e $\pi_C(F) \leq F \cap C$; inoltre $F = \pi_B(F) \oplus \pi_C(F)$. Allora $F \leq (F \cap B) \oplus (F \cap C)$, mentre l'altra disugualianza è ovvia. □

1.4 Divisibilità

1.4.1 Definizione. Diciamo che $n \in \mathbb{Z}$ divide $a \in A$ (e scriviamo $n \mid a$) se $nx = a$ ha soluzione in A. Diciamo che un gruppo A è *divisibile* se $n \mid a$ per ogni $a \in A$ e ogni $n \in \mathbb{Z} \setminus \{0\}$. Diciamo che A è *ridotto* se non ha sottogruppi divisibili non banali.

Evidentemente, A è divisibile se e solo se $nA = A$ per ogni $n \in A$. Valgono i seguenti importanti risultati:

1.4.2 Teorema. *Un gruppo è divisibile se e solo se è iniettivo.*

Dimostrazione. Sia A iniettivo. Presi arbitrariamente $a \in A$ e $n \in \mathbb{Z} \setminus \{0\}$, mostriamo che $n \mid a$. Sia $\phi \colon n\mathbb{Z} \to A$ definito da $\phi(n) = a$. Per la proprietà iniettiva, esiste ψ come nel seguente diagramma

$$\begin{tikzcd} n\mathbb{Z} \arrow[r, hook, "\iota"] \arrow[d, "\phi"'] & \mathbb{Z} \arrow[dl, dashed, "\psi"] \\ A & \end{tikzcd}$$

e quindi $a = \phi(n) = \psi\iota(n) = \psi(n) = n\psi(1)$.

Viceversa, sia D divisibile; vogliamo dimostrare l'esistenza di un morfismo ψ che renda commutativo

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\iota"] \arrow[d, "\phi"] & B \arrow[r, "\pi"] \arrow[dl, dashed, "\psi"] & B/A \arrow[r] & 0 \\ & D & & & \end{tikzcd}$$

L'insieme

$$\mathscr{P} = \{(G, \theta) \mid A \leq G \leq B, \quad \theta\colon G \to D, \quad \theta \restriction_A = \phi\}$$

con l'ordine parziale

$$(G, \theta) \leq (G', \theta') \iff G \leq G', \quad \theta' \restriction_G = \theta$$

è non vuoto (perché $(A, \phi) \in \mathscr{P}$) e induttivo (data una catena (G_i, θ_i) un maggiorante è $G = \bigcup_i G_i$ ed è definita in modo naturale $\theta\colon G \to D$), quindi per il lemma di Zorn esiste (G_0, θ_0) massimale in $\mathscr{P}$.
Mostriamo che $G_0 = B$. Supponiamo esista $b \in B \setminus G_0$. Si possono presentare due casi: se $nb \in G_0$ per qualche $n > 0$ (supponiamo n sia il minimo naturale per cui ciò accade), allora, detto $g = nb$, per divisibilità di D esiste $d \in D$ tale che $nx = \theta_0(g)$. La funzione

$$\begin{aligned} G_0 + \langle b \rangle &\longrightarrow D & \qquad (g \in G_0, \quad 0 \leq t < n) \\ x + tb &\longmapsto \theta_0(x) + td & \end{aligned}$$

è un omomorfismo che estende θ_0, contraddicendo la massimalità. Se invece $nb \in G_0$ soltanto per $n = 0$, allora basta mappare b in 0, e si estende θ_0 a

$$\begin{aligned} G_0 \oplus \langle b \rangle &\longrightarrow D & \qquad (g \in G_0, \quad t \in \mathbb{Z}) \\ x + tb &\longmapsto \theta_0(x) & \end{aligned}$$

contraddicendo ancora la massimalità. Dunque $G_0 = B$, $\theta_0 = \psi$. □

1.4.3 Teorema. *Sottogruppi divisibili sono addendi diretti.*

Dimostrazione. Sia $D \leq A$, D divisibile. Per la proprietà iniettiva dei gruppi divisibili, esiste ψ che faccia commutare

$$\begin{tikzcd} D \arrow[r, hook, "\iota"] \arrow[d, "1_D"'] & A \arrow[dl, dashed, "\psi"] \\ D & \end{tikzcd}$$

quindi otteniamo una fattorizzazione dell'identità 1_D e concludiamo per il corollario 1.3.4. □

1.4.4 Teorema. *Ogni gruppo è somma diretta di un gruppo divisibile e un gruppo ridotto.*

Dimostrazione. Sia A un gruppo abeliano; il sottogruppo D di A generato da tutti i sottogruppi divisibili di A è ancora divisibile ed è l'unico sottogruppo divisibile massimale di A. Per il teorema precedente $A = D \oplus R$ dove R non ha sottogruppi divisibili non banali. □

1.4.5 Teorema. *Ogni gruppo abeliano è sottogruppo di un gruppo divisibile.*

Dimostrazione. Ogni gruppo abeliano libero lo è, essendo $\mathbb{Z}^{\oplus r} \leq \mathbb{Q}^{\oplus r}$. Dato un gruppo arbitrario A, scriviamolo come $A \cong F/N$ con F gruppo libero (abbiamo mostrato infatti che ogni gruppo abeliano è immagine omomorfa di un gruppo abeliano libero), cosicché $F \leq D$, $A \cong F/N \leq D/N$ con D e D/N divisibili. □

1.4.6 Teorema. *Sia D un gruppo; le seguenti condizioni sono equivalenti:*

1. *A è divisibile;*
2. *A è iniettivo;*
3. *A è addendo diretto di ogni gruppo che lo contiene come sottogruppo.*

Dimostrazione. Abbiamo già mostrato l'equivalenza tra le prime due condizioni e che entrambe implicano l'ultima. Supponiamo ora (3). Per il teorema precedente esiste D divisibile con $A \leq D$. A è addendo diretto di D per ipotesi, e quindi per ogni n

$$A \oplus A' = D = nD = nA \oplus nA'$$

e quindi $A = nA$, cioè A è divisibile. □

1.4.7 Teorema (di struttura dei gruppi divisibili)**.** *Un gruppo abeliano è divisibile se e solo se è somma diretta di copie di $\mathbb{Q}$ e di gruppi quasiciclici, cioè è della forma*

$$D = \mathbb{Q}^{\oplus\alpha} \oplus \bigoplus_p (\mathbb{Z}(p^\infty)^{\oplus\beta_p}).$$

Dimostrazione. Ogni gruppo della forma data è divisbile, perché $\mathbb{Q}$ e $\mathbb{Z}(p^\infty)$ sono divisibili e somme dirette di divisibili sono divisibili. Viceversa, sia D divisibile e sia $T = \mathrm{T}(D)$. T è divisible: per ogni $t \in T$ e $n \in \mathbb{Z}$ esiste $x \in D$ tale che $nx = t$ e, detto $o = \mathrm{o}(t)$, si ha $onx = ot = 0$ e quindi $x \in T$. Per il teorema 1.3.14, T è somma diretta delle sue p-componenti e, per il teorema 1.4.3, T è addendo diretto di G. Pertanto è sufficiente mostrare il teorema in due casi: quando D p-gruppo e quando D è senza torsione.
Sia D un p-gruppo divisible; $G[p]$ è un $\mathbb{F}_p$-spazio vettoriale. Sia $\mathfrak{m} = \dim_{\mathbb{F}_p}(G)$ e sia $G^* = \bigoplus_{\mathfrak{m}} \mathbb{Z}(p^\infty)$ somma diretta di $\mathfrak{m}$ copie di p-gruppi quasiciclici. Anche $G^*[p]$ è un $\mathbb{F}_p$-spazio vettoriale, ed esiste un morfismo iniettivo $\phi\colon G^*[p] \to G$ tale che $\phi(G^*[p]) = G[p]$. Grazie all'iniettività di D, possiamo estendere ϕ a un omomorfismo $\psi\colon G^* \to G$:

$$\begin{tikzcd} 0 \arrow[r] & G^*[p] \arrow[r, "\iota"] \arrow[d, "\phi"] & G^* \arrow[r, "\pi"] \arrow[dl, dashed, "\psi"] & G^*[p]/G^* \arrow[r] & 0 \\ & G & & & \end{tikzcd}$$

Se $\ker\psi \neq \{0\}$ allora $\ker\psi$ contiene un elemento di ordine p, quindi un elemento di $G^*[p]$, e ϕ non sarebbe iniettivo. Se $\operatorname{im}\psi \neq G$, allora $\operatorname{im}\psi$, essendo divisibile (perché immagine di un divisibile), sarebbe addendo diretto proprio di $G = \operatorname{im}\psi \oplus H$ per un $H \neq \{0\}$; allora H conterrebbe un elemento di ordine p non appartenente a $\operatorname{im}\psi$, ma $G[p] = \phi(G^*[p]) \subseteq \operatorname{im}\phi \subseteq \operatorname{im}\psi$, cioè ogni elemento di ordine p deve appartenere a $\operatorname{im}\psi$: assurdo. Allora ψ è isomorfismo e si

conclude.
Nel secondo caso, sia D senza torsione e divisibile; allora D è un $\mathbb{Q}$-spazio vettoriale, potendo definire $\frac{1}{n}g$ ($n \in \mathbb{Z} \setminus \{0\}$) come l'unico $g' \in D$ tale che $g = ng'$ (l'esistenza segue dalla divisibilità di D, l'unicità segue dal fatto che se $g' = nx = nx'$ allora $x - x' = 0$ essendo D senza torsione). Essendo un $\mathbb{Q}$-spazio vettoriale, D è somma diretta di $\dim_{\mathbb{Q}}(D)$ copie di $\mathbb{Q}$. □

1.5 Gruppi dotati di topologie lineari

Dato un sottoinsieme $\mathscr{B}$ del reticolo dei sottogruppi di A che sia base per un filtro (quindi $\mathscr{B} \neq \emptyset$ e ogni intersezione finita di elementi di $\mathscr{B}$ contiene un elemento di $\mathscr{B}$), possiamo scegliere $\mathscr{B}$ come base di intorni di 0; allora, dato $a \in A$, possiamo scegliere come base di intorni di a le classi laterali $a + U$ al variare di $U \in \mathscr{B}$. Le topologie così definite sono chiamate *topologie lineari*.

Mostriamo che gli aperti per tali topologie sono unioni di classi laterali $a+U$ con $U \in \mathscr{B}$. L'intersezione tra due classi laterali $(a_1+U_1)\cap(a_2+U_2)$ è l'insieme vuoto oppure una classe laterale mod $U_1 \cap U_2$: si vede infatti che se $a := a_1+u_1 = a_2 + u_2 \in (a_1 + U_1) \cap (a_2 + U_2)$, allora $a_1 + U_1 = a + U_1$, $a_2 + U_2 = a + U_2$, da cui $(a_1 + U_1) \cap (a_2 + U_2) = (a + U_1) \cap (a + U_2) = a + (U_1 \cap U_2)$. Essendo $U_1 \cap U_2 \in \mathscr{B}$, si conclude.

Tali topologie sono sempre continue, ovvero rendono continue le operazioni $+\colon (x, y) \mapsto x + y$ e $-\colon x \mapsto -x$: infatti la preimmagine $+^{\leftarrow}(a + U)$ di un generico aperto è tale che se (x, y) le appartiene, ovvero $x + y \in a + U$, allora $x + y + U \subseteq a + U$, cioè ogni punto della preimmagine ha un intorno contenuto in essa, che quindi è aperta. Analogamente se $x \in -^{\leftarrow}(a+U)$ si ha $-x \in a+U$ e quindi $-x + U \subseteq a + U$.

Sono Hausdorff se e solo se $\bigcap_{U\in\mathscr{B}} U = \{0\}$. Se $\bigcap_{U\in\mathscr{B}} U \neq \{0\}$, e quindi $\bigcap_{U\in\mathscr{B}} U \ni u$ per qualche $u \neq 0$, allora 0 e u non possono avere intorni disgiunti essendo che $U_1 \cap (u + U_2) \ni u$ per ogni U_1, $U_2 \in \mathscr{B}$. Viceversa, supponiamo $\bigcap_{U\in\mathscr{B}} U = \{0\}$ e mostriamo che per ogni $x \neq y$ possiamo scegliere U_1, U_2 tali che $(x + U_1) \cap (y + U_2) \neq \emptyset$, cioè $x - y \notin U_1 + U_2$. Infatti, se esistessero x, y tali che $x - y \in U_1 + U_2$ per ogni U_1, $U_2 \in \mathscr{B}$ allora scegliendo $U_1 = \{0\}$ si otterrebbe $x - y \in U_2$ per ogni U_2, ovvero $\bigcap_{U\in\mathscr{B}} U \ni x - y \neq 0$.

Si ottiene la topologia discreta quando $\{0\} \in \mathscr{B}$, perché in tal caso il filtro generato da $\mathscr{B}$ contiene l'intero reticolo dei sottogruppi di A.

1.5.1 Esempio. Avrà rilevanza la *topologia $\mathbb{Z}$-adica*, ottenuta scegliendo come base di intorni di 0 l'insieme

$$\mathscr{B} = \{nA \mid n \in \mathbb{Z}, n \neq 0\}$$

In base a quanto detto prima, tale topologia è Hausdorff se e solo se

$$A^1 := \bigcap_{n>0} nA = \{0\}$$

ed è discreta se e solo se $nA = \{0\}$ per qualche n, cioè se e solo se A è limitato. La chiusura di $B \leq A$ è data da

$$\overline{B} = \bigcap_{n>0} (B + nA)$$

e quindi B è chiuso se e solo se $(A/B)^1 = \{0\}$. Analogamente, chiamiamo *topologia p-adica* quella ottenuta da

$$\mathscr{B} = \{p^n A \mid n \in \mathbb{Z}, n \geq 0\}.$$

Sia $\mathscr{B} = \{U_i \mid i \in I\}$ e dotiamo I dell'ordine parziale definito da

$$i \leq j \iff U_i \geq U_j$$

Essendo $\mathscr{B}$ base di un filtro, per ogni U_i, U_j esiste U_n tale che $U_n \leq U_i \cap U_j$, cioè, per ogni $i, j \in I$ esiste $n \in I$ tale che $i, j \leq n$, cioè $(I, \leq)$ è un insieme *filtrante (verso l'alto)*. Allora, applicando le classiche definizioni topologiche, diciamo che una rete $\{a_i\}_{i \in I}$ converge ad $a \in A$ se per ogni intorno $a + U_i$ esiste $\bar{i}$ tale che $a_j \in a + U_i$ per ogni $j \geq \bar{i}$, ovvero

$$\text{per ogni } i \text{ esiste } \bar{i} \text{ tale che } a_j - a \in U_i \text{ per ogni } j \geq \bar{i};$$

diciamo che converge in maniera 'pulita' se possiamo scegliere $\bar{i} = i$, cioè

$$\text{per ogni } i \text{ si ha } a_j - a \in U_i \text{ per ogni } j \geq i.$$

Su un gruppo dotato di una topologia lineare, sono definite la proprietà di Cauchy per una rete e la nozione di completezza. Diciamo che una rete è *di Cauchy* se

$$\text{per ogni } i \text{ esiste } \bar{i} \text{ tale che } a_j - a_k \in U_i \text{ per ogni } j, k \geq \bar{i}.$$

Osservando che, essendo U_i un sottogruppo, le condizioni $a_j - a_{\bar{i}} \in U_i$ e $a_k - a_{\bar{i}} \in U_i$ implicano $a_j - a_k \in U_i$, è sufficiente definire la proprietà di Cauchy come

$$\text{per ogni } i \text{ esiste } \bar{i} \text{ tale che } a_j - a_{\bar{i}} \in U_i \text{ per ogni } j \geq \bar{i}.$$

Possiamo anche qui facilitare la discussione considerando reti 'pulite', cioè che ci permettano di scegliere $\bar{i} = i$:

$$\text{per ogni } i \text{ si ha } a_j - a_i \in U_i \text{ per ogni } j \geq i.$$

Reti di Cauchy pulite e convergenti convergono in maniera pulita: se $a_j - a \in U_i$, allora $a_j - a_i \in U_i$ implica $a_i - a \in U_i$, e quindi $a_j - a_i \in U_i$ $(j \geq i)$ implica $a_j - a \in U_i$ per ogni $i \geq i$.

Per topologie lineari Hausdorff, definiamo la nozione di completezza: un gruppo A è completo in una data topologia (di Hausdorff) se ogni rete di Cauchy in A ha limite in A.

Osservazione. In seguito, ogni volta che parleremo di completezza (o di compattezza), assumeremo automaticamente che la topologia in questione sia Hausdorff; in altre parole, *completo* significherà *Hausdorff e completo* e analogamente per quanto riguarda la compattezza.

Data una famiglia di gruppi topologici (A_j, τ_j), $j \in J$, possiamo definire sul prodotto diretto $\prod_{j \in J} A_j$: la *topologia prodotto*, i cui aperti di base sono del tipo

$$\{\bigcap_{j \in F} \pi_j^{\leftarrow}(U_j) \mid F \subseteq J, \quad |F| < \infty, \quad U_j \in \tau_j \, \forall j \in F\}.$$

Definiamo anche la *topologia box*, più fine, nel seguente modo: se ogni A_j ha base di intorni $\{U_{ji}\}_i$, che supponiamo indiciati sullo stesso J, allora una base di intorni per la topologia box è formata da $\{\prod_{j\in J} U_{ji}\}_i$. Il vantaggio della topologia box è che una rete $\{g_i\}_i$ in $\prod_{j\in J} A_j$ è di Cauchy se e solo se ogni rete $\{\pi_j(g_i)\}_i$ e di Cauchy in A_j per τ_j. Notare che abbiamo definito la topologia box richiedendo che l'indice i sia lo stesso in ogni componente di un intorno di base $\prod_{j\in J} U_{ji}$, quindi la topologia dipende da come sono indiciati gli U_{ji}; in questo modo è banale il seguente:

1.5.2 Esempio. Se τ_j è la topologia $\mathbb{Z}$-adica per ogni j, allora la topologia box è la topologia $\mathbb{Z}$-adica del prodotto diretto.

Dimostrazione. Chiaramente ogni intorno nella topologia $\mathbb{Z}$-adica del prodotto è intorno nella topologia box, essendo $n\prod_{j\in J} A_j = \prod_{j\in J} nA_j$. Viceversa, un intorno per la topologia box è del tipo $\prod_{j\in J} U_{ji} = \prod_{j\in J} U_{jn} = \prod_{j\in J} nA_j = n\prod_{j\in J} A_j$. □

1.5.3 Lemma. *Un prodotto diretto è completo nella topologia box se e solo se ogni componente lo è.*

Dimostrazione. Sia $G = \prod_i A_j$ completo nella topologia box. Se $\{a_i^j\}_i$ è una rete di Cauchy in A_j, allora $\{\iota_j(a_i^j)\}_i$ è una rete di Cauchy in G (ι_j è l'inclusione in G), e quindi tende a un limite $g_j \in G$; ma allora $\pi_j(g_j)$ è il limite di $\{a_i^j\}_i$. Viceversa, supponiamo ogni A_j completo. Consideriamo una rete 'pulita' $\{g_i\}_i$ in G; se $a_j \in A_j$ è limite di $\{\pi_j(g_i)\}_i$, scelto $g \in G$ tale che $\pi_j(g) = a_j$, g è limite di $\{g_i\}_i$. □

1.5.4 Corollario. *Un prodotto diretto è completo nella topologia $\mathbb{Z}$-adica (risp. p-adica) se e solo se ogni componente è completa nella propria topologia $\mathbb{Z}$-adica (risp. p-adica).*

Dimostrazione. Per l'esempio 1.5.2, se ogni fattore ha la topologia $\mathbb{Z}$-adica (risp. p-adica), allora la topologia box del prodotto diretto è la sua topologia $\mathbb{Z}$-adica (risp. p-adica). Si conclude applicando il lemma. □

1.6 Completamenti e limiti inversi

Descriviamo due modi per costruire il *completamento* di un gruppo topologico, ovvero un gruppo topologico completo che contenga il gruppo di partenza come suo sottogruppo denso (e che dimostreremo poi essere unico a meno di omeomorfismi). Il primo modo è basato sulle reti di Cauchy.

Sia A gruppo topologico, $\{U_i\}_i$ base di intorni di 0; identifichiamo le reti in A con elementi di $A^{|I|} = \prod_{i\in I} A$. Siano poi $C \leq A^{|I|}$ il sottogruppo delle reti di Cauchy, $E \leq C$ il sottogruppo delle reti convergenti a 0. Consideriamo il seguente gruppo topologico, Hausdorff (con la topologia quoziente indotta da $A^{|I|}$ con la sua topologia box o prodotto — si verifica che la topologia indotta è la stessa):

$$\widehat{A} = C/E$$

e mostriamo che è un completamento di A. Il morfismo

$$\begin{aligned} \mu\colon A &\longrightarrow \widehat{A} \\ a &\longmapsto (a\cdots a\cdots) + E \end{aligned}$$

è omeomorfismo tra A e $\mu(A)$ e quest'ultimo è denso in $\widehat{A}$: dati $(\cdots a_i \cdots)_i + E \in \widehat{A}$ e un intorno U di 0 in $A^{|I|}$, $\mu(a_i)$ appartiene all'intorno di $(\cdots a_i \cdots)_i + E$ corrispondente a U. Essendo $\mu(A)$ denso in $\widehat{A}$, per mostrare la completezza è sufficiente verificare la convergenza di reti in $\mu(A)$ a elementi di $\widehat{A}$: se $\{\mu(a_i)\}_i$ è rete di Cauchy 'pulita' in $\mu(A)$ (per una opportuna rete di Cauchy $\{a_i\}_i$ in A), allora $(\cdots a_i \cdots)_i + E \in \widehat{A}$ è il suo limite, cioè

$$(a_i \cdots a_i \cdots) + E \xrightarrow[i\to\infty]{} (\cdots a_j \cdots)_{j\in I} + E$$

Per la seconda costruzione, abbiamo bisogno della nozione di *limite inverso*:

1.6.1 Definizione. Sia I insieme filtrante di indici, $\{A_i\}_{i\in I}$ famiglia di gruppi, $\{\pi_{ij}\colon A_j \to A_i\}_{i\le j}$ morfismi tali che $\pi_{ii} = 1_{A_i}$ per ogni i e $\pi_{ij}\pi_{jk} = \pi_{ik}$ per ogni $i \le j \le k$. Allora chiamiamo *limite inverso* del sistema $\{A_i, \pi_{ij}\}$ il gruppo

$$\varprojlim_I A_i = \{(\cdots a_i \cdots) \in \prod_{i\in I} A_i \mid \pi_{ij}(a_j) = a_i \text{ se } i \le j\}$$

Sia ora A gruppo topologico con $\{U_i\}_{i\in I}$ come base di intorni di 0 e siano $\pi_{ij}\colon A/U_j \to A/U_i$ definite per ogni $i \le j$ da $\pi_{ij}(a + U_j) = a + U_i$. Poniamo $\widehat{L} = \varprojlim_I (A/U_i)$ e

$$\begin{aligned} \alpha\colon A &\longrightarrow \widehat{L} \\ a &\longmapsto (\cdots a + U_i \cdots)_i. \end{aligned}$$

Per mostrare che anche $\widehat{L}$ è completamento di A, dimostriamo il seguente:

1.6.2 Teorema. *Esiste un omeomorfismo $\lambda\colon \widehat{A} \to \widehat{L}$ tale che $\lambda\mu = \alpha$.*

Dimostrazione. Definiamo

$$\begin{aligned} \lambda\colon \widehat{A} &\longrightarrow \widehat{L} \\ (\cdots a_i \cdots)_i + E &\longmapsto (\cdots a_i + U_i \cdots)_i, \end{aligned}$$

notando che $(\cdots a_i + U_i \cdots)_i \in \widehat{L}$ poichè $a_j + U_i = \pi_{ij}(a_j + U_j) = a_i + U_i$ per $j \ge i$. La suriettività di λ segue dal fatto che, per ogni $(\cdots a_i + U_i \cdots)_i \in \widehat{L}$, essendo $a_j + U_i = a_i + U_i$ per ogni $j \ge i$, $\{a_i\}_i$ è rete di Cauchy 'pulita' in A. L'iniettività segue dal fatto che se $\{a'_i\}_i$ è un altro insieme di rappresentanti delle classi A/U_i, allora $a_j + U_i = a_i + U_i = a'_i + U_i = a_j + U_i$ quindi $a_j - a'_j \in U_i$ se $j \ge i$, cioè $(a_i - a'_i)_i \in E$, ovvero $(\cdots a_i \cdots)_i + E = (\cdots a'_i \cdots)_i + E$. □

Mostriamo infine che il completamento è unico a meno di omeomorfismo. Questo segue dalla seguente proprietà universale di $\widehat{A}$:

1.6.3 Teorema. *Per ogni gruppo completo G e ogni omomorfismo continuo $\phi\colon A \to G$, esiste un unico omomorfismo continuo $\widehat{\phi}\colon \widehat{A} \to G$ tale che $\widehat{\phi}\mu = \phi$.*

Dimostrazione. Sia $\{a_i\}_i$ rete di Cauchy in A, convergente in $\widehat{A}$ ad $\widehat{a} \in \widehat{A}$. Per continuità di ϕ, $\{\phi(a_i)\}_i$ dev'essere di Cauchy in G, e avere quindi limite $g \in G$. Allora definiamo $\widehat{\phi}$ tramite $\widehat{\phi}\colon \widehat{a} \mapsto g$. □

Concludiamo la sezione con un lemma a cui faremo riferimento.

1.6.4 Lemma. *Il limite inverso A^* di un sistema di gruppi topologici Hausdorff A_i e omomorfismi continui π_{ij} è un sottogruppo chiuso di $\prod_i A_i$ nella topologia prodotto, e le mappe di proiezione $\pi_i \colon A^* \to A_i$ sono continue.*

Dimostrazione. Se $(\cdots a_i \cdots) \in (\prod_i A_i) \backslash A^*$ allora esistono $i, j \in I$ con $i < j$ tali che $a_i \neq \pi_{ij}(a_j)$; allora, essendo A_i Hausdorff, esistono $U, V \subseteq A_i$, $U \cap V = \emptyset$, tali che $a_i \in U$, $\pi_{ij}(a_j) \in V$. L'insieme

$$\{(\cdots b_i \cdots) \in \prod_{i \in I} A_i \mid b_i \in U, \pi_{ij}(b_j) \in V\}$$

è aperto in $\prod_i A_i$ e disgiunto da A^*. L'ultima affermazione segue dalla continuità delle proiezioni canoniche $\prod_i A_i \to A_i$. $\square$

1.6.5 Esempio (Interi p-adici)**.** Il gruppo (o l'anello) J_p degli interi p-adici può essere definito come $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$, ovvero come il completamento di $\mathbb{Z}$ nella topologia p-adica. Per la proprietà del limite inverso, deve essere $a_i + \mathbb{Z}/p^i\mathbb{Z} = a_j + \mathbb{Z}/p^i\mathbb{Z}$ se $i \leq j$, quindi ogni elemento di J_p ha come n-esima componente

$$b_0 + b_1 p + \cdots + b_{n-1}p^{n-1} + \mathbb{Z}/p^n\mathbb{Z}$$

per una successione $\{b_i\}_i \subseteq \{0, \ldots, p-1\}$, quindi un elemento di J_p ha la forma

$$(b_0 + \mathbb{Z}/p\mathbb{Z}, \ldots, b_0 + b_1 p + \cdots + b_{n-1}p^{n-1} + \mathbb{Z}/p^n\mathbb{Z}, \ldots).$$

Viceversa, per ogni serie formale $b_0 + b_1 p + \cdots + b_{n-1}p^{n-1} + \ldots$, il vettore che ha per componente n-esima la classe di equivalenza mod $p^n\mathbb{Z}$ della ridotta $(n-1)$-esima della serie, identifica un elemento del limite inverso J_p. Quindi gli elementi di J_p possono essere pensati anche come serie formali nell'indeterminata p.

Capitolo 2

Sottogruppi puri

2.0.1 Definizione. Diciamo che un sottogruppo B di un gruppo abeliano A è *puro* in A se vale una delle seguenti condizioni equivalenti:

- per ogni $n \in \mathbb{Z}$ e $b \in B$, se $n \mid b$ in A allora $n \mid b$ in B;
- per ogni $n \in \mathbb{Z}$ e $b \in B$, se $nx = b$ ha soluzione in A, allora ha soluzione in B;
- per ogni $n \in \mathbb{Z}$, $nB = B \cap nA$.

Si parla di *p-purità* se, nella definizione data, a n sostituiamo p^n.

Dall'ultima espressione scritta si vede che la condizione può anche essere espressa così: B è puro in A se e solo se la topologia $\mathbb{Z}$-adica di B coincide con la topologia indotta su B dalla topologia $\mathbb{Z}$-adica di A. L'inclusione $nB \subseteq B \cap nA$ è ovvia; la purità consiste appunto nell'inclusione opposta.

Anticipiamo che un'ulteriore condizione equivalente consiste nel considerare, invece di una singola equazione $nx = b$, un sistema di equazioni in un numero finito di incognite. Questa equivalenza non è immediata e sarà dimostrata nel teorema 2.2.4, ma la citiamo subito in quanto è una possibile definizione di purità nell'ambito più generale dei sottomoduli:

- ogni sistema $\sum_{j=1}^{n} n_{ij}x_j = b_i$ $(b_i \in B,\ i = 1, \ldots, m)$ risolvibile in A è risolvibile anche in B.

2.0.2 Esempio. *Addendi diretti sono sottogruppi puri.* Infatti, sia $A = B \oplus C$, $b \in B$ tale che $nx = b$ per un $x \in A$. x si scrive in modo unico come $x = b' + c'$, quindi $b = nb' + nc'$; poiché $B \cap C = \{0\}$, si ha $nc' = b - nb' = 0$, quindi $nx = b$ ammette soluzione b' in B.

2.0.3 Esempio. *Il sottogruppo di torsione di un gruppo abeliano è un sottogruppo puro.* Infatti, sia $nx = t \in \mathrm{T}(A)$ per un $x \in A$ e sia $o = \mathrm{o}(t)$; allora $onx = ot = 0$ quindi anche x ha ordine finito, cioè $x \in \mathrm{T}(A)$.

In generale, però, come mostra il seguente esempio, un sottogruppo di torsione non è un addendo diretto, e quindi segue che un sottogruppo puro non è, in generale, un addendo diretto.

2.0.4 Esempio. Sia $C = \prod_{i=1}^{\infty} \langle x_i \rangle$ con $\mathrm{o}(x_i) = p^i$, p primo. Allora $\mathrm{T}(C)$ non è addendo diretto di C.

Dimostrazione. Sia $y = (0, px_2, 0, p^2x_4, 0, p^3x_6, \dots)$ il vettore con i-esima componente $p^{i/2}x_i$ per i pari e 0 per i dispari. Mostriamo che $y \notin \mathrm{T}(C)$:

$$\begin{aligned}\mathrm{o}(y) = m \neq \infty \iff mp^jx_{2j} = 0 \text{ per ogni } j &\iff p^{2j} \mid mp^j \text{ per ogni } j \\ &\iff p^j \mid m \text{ per ogni } j,\end{aligned}$$

che è impossibile.

Inoltre $y \in p^nC + \mathrm{T}(C)$ per ogni n, infatti

$$\begin{aligned} y = (0, px_2, \dots, p^{n-1}x_{2(n-1)}, 0, 0, \dots)+ \\ + p^n(0, 0, \dots, x_{2n}, 0, px_{2(n+1)}, \dots) \end{aligned}$$

e il primo addendo appartiene alla torsione avendo ordine p^{n-1}. Questo significa che $y + \mathrm{T}(C)$ è un elemento di $C/\mathrm{T}(C)$ non nullo e con p-altezza infinita.

Se $\mathrm{T}(C)$ fosse addendo diretto di C, allora $C = \mathrm{T}(C) \oplus B$, con $B \cong C/\mathrm{T}(C)$ per il lemma 1.3.5. L'elemento di B corrispondente a $y+T$ tramite l'isomorfismo $B \cong C/\mathrm{T}(C)$ è anch'esso non nullo con p-altezza infinita. Ma C non può contenere un tale elemento perché, se $z \in C$ ha una i-esima componente non nulla, allora $p^ix \neq z$ per ogni x avendo p^ix i-esima componente nulla. □

Possiamo quindi considerare la proprietà di essere sottogruppo puro come un indebolimento della proprietà di essere addendo diretto ed esaminare la relazione tra le due, dando dei criteri per verificare quando sono equivalenti.

Iniziamo enunciando una proprietà di base della purità, che useremo in seguito:

2.0.5 Lemma. *Siano B e C sottogruppi di A, con $C \leq B \leq A$. Allora valgono:*

1. *se C è puro in B e B è puro in A, allora C è puro in A:*

2. *se B è puro in A, allora B/C è puro in A/C;*

3. *se C è puro in A e B/C è puro in A/C, allora B è puro in A.*

Dimostrazione.

1. $nC = C \cap nB$, $nB = B \cap nA$, quindi $nC = C \cap B \cap nA = C \cap nA$;

2. si ha $n\frac{B}{C} = \frac{nB+C}{C} = \frac{(B \cap nA)+C}{C} = \frac{(B+C)\cap(nA+C)}{C} = \frac{B}{C} \cap \frac{nA+C}{C} = \frac{B}{C} \cap n\frac{A}{C}$;

3. supponiamo $nx = b$ ammetta soluzione $a \in A$, allora $n(a + C) = b + C$; per purità di B/C esiste b' tale che $n(b' + C) = b + C$, quindi $nb' = b + c$ per un $c \in C$, quindi $n(b' - a) = c$; per purità di C si ha $c = nc'$ per un $c' \in C$, e quindi $n(b' - c') = na = b$, cioè $nx = b$ ha soluzione $b' - c' \in B$.

□

2.1 Gruppi limitati

2.1.1 Teorema. *Un sottogruppo puro limitato è un addendo diretto.*

Notiamo intanto che la tesi è vera in un caso particolare:

2.1.2 Lemma. *Se un sottogruppo B di A è somma diretta di gruppi ciclici dello stesso ordine p^k, sono equivalenti:*

1. *B è p-puro in A;*
2. *B è addendo diretto di A;*
3. *B è puro in A.*

Dimostrazione. ($1 \implies 2$) B p-puro in A significa $p^n B = B \cap p^n A$ per ogni n, quindi anche per $n = k$, ed essendo per ipotesi $p^k B = 0$ si ha $0 = B \cap p^k A$. Sia C un sottogruppo di A massimale per la proprietà di essere disgiunto da B (un tale C esiste per il lemma di Zorn); allora $p^k A \leq C$.

Siano $a \in A$, $b \in B$, $c \in C$ tali che $pa = b+c$; allora $p^{k-1}b+p^{k-1}c = p^k a \in C$ implica $p^{k-1}b = 0$ e quindi, per le ipotesi su B, esiste $b' \in B$ tale che $b = pb'$. Vogliamo mostrare che $A = B \oplus C$; questo segue da un lemma tecnico:

Siano A, B, C, a, b, c, p come nelle ipotesi precedenti; allora: $A = B \oplus C$ se e solo se $pa = b + c$ implica $b = pb'$ per qualche $b' \in B$.

Il 'solo se' è facile; ci interessa dimostrare il 'se'. Se $pa = b + c$ implica $b = pb'$, allora $p(a - b') = c \in C$. Mostriamo intanto che $a - b' \in B \oplus C$: se $a - b' \notin C$, allora $\langle C, a - b'\rangle$ contiene strettamente C e quindi, per la proprietà di C, contiene un elemento non nullo $b'' = k(a - b') + c' \in B$ per un $c' \in C$ e un $k \in \mathbb{Z}$, con necessariamente $(k, p) = 1$ (altrimenti anche $k(a - b') \in C$ e quindi $b'' \notin B$), quindi esistono r, $s \in \mathbb{Z}$ tali che $rk + sp = 1$, da cui $a - b' = rk(a - b') + sp(a - b') = r(b'' - c) + sp(a - b') \in B \oplus C$ come volevamo.

Ora, da $a - b' \in B \oplus C$ segue $a \in B \oplus C$ e quindi $A/(B \oplus C)$ non contiene elementi di ordine primo. Preso un arbitrario $x \in A \setminus (B \oplus C)$, ragionando come prima si vede che $\langle C, x\rangle$ contiene un elemento $b''' = lx + c''$. $l \neq 0$ perché $B \cap C = \{0\}$, quindi $lx = b''' - c'' \in B \oplus C$: il fatto che per un arbitrario $x \in A$ esista l tale che $lx \in B \oplus C$ significa che $A/(B \oplus C)$ è di torsione, ma avevamo dimostrato che non contiene elementi di ordine primo, quindi non contiene elementi di ordine non banale, cioè $A/(B \oplus C) = \{0\}$ che è quanto voluto.

Le implicazioni ($2 \implies 3$) e ($3 \implies 1$) sono banali. □

Per dimostrare il teorema 2.1.1 ci serviamo dell'importante risultato seguente, la cui dimostrazione è facile grazie al criterio di Kulikov 1.3.15:

2.1.3 Teorema (I teorema di Prüfer)**.** *Un gruppo limitato è somma diretta di gruppi ciclici.*

Dimostrazione. Un gruppo limitato A è in particolare un gruppo di torsione, quindi per il teorema 1.3.14 è somma diretta di p-gruppi A_p. Poiché un p-gruppo ha un sottogruppo di ogni ordine che divida l'ordine del gruppo, ogni A_p può essere scritto come unione di una catena ascendente di suoi sottogruppi.

Inoltre gli elementi di un p-gruppo hanno p-altezze finite. Pertanto, applicando il teorema 1.3.15, si conclude che gli A_p sono somme dirette di gruppi ciclici; quindi A è somma diretta di gruppi ciclici. □

Possiamo ora dimostrare il teorema 2.1.1:

Dimostrazione del teorema 2.1.1. Per il teorema 2.1.3 possiamo scrivere $B = B_1 \oplus B_2$ con B_1 somma di ciclici dello stesso ordine p^k e B_2 tale che l'estremo superiore degli ordini dei suoi elementi sia minore di quello di B.

Se B è puro in A, allora B_1 è puro in A (lemma 2.0.5, 1) e per il lemma 2.1.2 si ha $A = B_1 \oplus A_1$, quindi $B = B_1 \oplus B_2'$ con $B_2' = B \cap A_1 \cong B_2$.

B_2' è puro in A_1 e, per induzione, è suo addendo diretto (chiamiamo A_2 il suo complementare), quindi

$$A = B_1 \oplus A_1 = B_1 \oplus B_2' \oplus A_2 = B \oplus A_2$$

che è la tesi. □

Questo criterio sarà generalizzato quando parleremo di gruppi algebricamente compatti, di cui i gruppi limitati sono un caso particolare.

Dal teorema appena dimostrato segue la caratterizzazione della purità che servirà in seguito:

2.1.4 Lemma. *Se B è sottogruppo di A, sono equivalenti:*

1. *B è puro in A;*
2. *B/nB è addendo diretto di A/nB per ogni $n > 0$;*
3. *se $C \leq B$ con B/C finitamente cogenerato, allora B/C è addendo diretto di A/C.*

Dimostrazione. ($1 \implies 2$) La purità si conserva nel passaggio ai quozienti, per il lemma 2.0.5, quindi il sottogruppo B/nB è puro in A/nB; essendo anche n-limitato, è addendo diretto per il teorema 2.1.1.

($2 \implies 3$) Possiamo supporre B/C ridotto: infatti, se avesse un sottogruppo divisibile D/C (supponiamolo massimale e quindi complementare di un sottogruppo ridotto R/C), esso sarebbe iniettivo e quindi addendo diretto di ogni gruppo che lo contiene, quindi $B/C = D/C \oplus R/C$ e $A/C = D/C \oplus A'/C$, e ci siamo ricondotti a verificare se R/C è addendo diretto di A/C. Sia quindi B/C ridotto; allora esiste un intero $n > 0$ tale che $n(B/C) = \{0\}$, cioè $nB \leq C$ e, per ipotesi, B/nB è addendo diretto di A/nB. Passando al modulo C, si trova B/C addendo diretto di A/C.

($3 \implies 1$) Supponiamo per assurdo che $nx = b \in B$ abbia soluzione in A e non in B: allora $b \notin nB$. Sia C sottogruppo di B contenente nB e massimale tra i sottogruppi di B che non contengono b: allora B/C è cociclico. Per ipotesi è addendo diretto di A/C, quindi è anche puro in A/C, cioè $n\frac{B}{C} = n\frac{A}{C} \cap \frac{B}{C}$ ovvero $\frac{nA+C}{C} \cap \frac{B}{C} = \frac{nB+C}{C} = \frac{C}{C} = \{0\}$. Detta $a \in A$ la soluzione di $nx = b$, si ha $na = b$ e $na + C = b + C \in \frac{nA+C}{C} \cap \frac{B}{C} = \{0\}$, ma $b + C \neq 0$ per come abbiamo scelto C: assurdo. □

2.2 Quozienti modulo sottogruppi puri

Vogliamo dimostrare il seguente criterio:

2.2.1 Teorema. *Se B è un sottogruppo puro di A tale che A/B è somma diretta di gruppi ciclici, allora B è addendo diretto di A.*

Partiamo da una caratterizzazione della purità:

2.2.2 Lemma. *Un sottogruppo B di A è puro se e solo se ogni classe laterale $a + B$ contiene un elemento $a + b$ con lo stesso ordine di $a + B$ (visto come elemento del quoziente).*

Dimostrazione. Sia B puro in A, $a + B \in A/B$. Se $\mathrm{o}(a + B) = \infty$, allora $na \notin B$ per ogni $n \in \mathbb{N}$, quindi $na \neq 0$ per ogni $n \in \mathbb{N}$, quindi $\mathrm{o}(a) = \infty$. Se $\mathrm{o}(a + B) = n \in \mathbb{N}$, $na =: b \in B$; per purità di B allora $na = nb'$ con $b' \in B$, da cui $n(a - b') = 0$. Inoltre n è il più piccolo naturale tale che $na = nb$ perché, essendo $\mathrm{o}(a + B) = n$, se $m < n$ allora $ma \notin B$, quindi $ma \neq mb$. Dunque $\mathrm{o}(a - b') = n$.

Viceversa, per ogni $b \in B$, se l'equazione $nx = b$ ha soluzione $a \in A$, allora: per ipotesi in $a + B$ esiste $a + b'$ con $\mathrm{o}(a + b') = \mathrm{o}(a + B) =: n'$, ed essendo $na = b \in B$ si ha $n' \mid n$; allora $0 = n(a + b') = na + nb' = b + nb'$, quindi $-b'$ è soluzione in B. □

Dimostrazione del teorema 2.2.1. Sia B puro in A e $A/B = \bigoplus_i \langle \overline{a_i} \rangle$. Scegliamo per ogni classe $\overline{a_i}$ un rappresentante a_i con la proprietà $\mathrm{o}(a_i) = \mathrm{o}(\overline{a_i})$, che esiste per il lemma. Sia G l'insieme di tali rappresentanti. Allora $A = \langle G \rangle + B$; inoltre $\langle G \rangle \cap B = \{0\}$, infatti: se $x \in \langle G \rangle$ allora

$$x = n_1 a_{i_1} + \cdots + n_k a_{i_k}$$

e, se vale anche $x \in B$,

$$\overline{x} = n_1 \overline{a_{i_1}} + \cdots + n_k \overline{a_{i_k}} = \overline{0}$$

Essendo A/B una somma diretta, per ogni j dev'essere $n_j \overline{a_{i_j}} = \overline{0}$, cioè, poiché gli ordini delle classi e dei rappresentanti coincidono, $n_j a_{i_j} = 0$ per ogni j, da cui segue $x = 0$. Quindi $A = \langle G \rangle \oplus B$. □

Dal teorema appena dimostrato segue una caratterizzazione della purità, duale del lemma 2.1.4, che servirà in seguito:

2.2.3 Lemma. *Se B è sottogruppo di A, definiamo $n^{-1}B \coloneqq \{x \in A \mid nx \in B\}$; sono equivalenti:*

1. *B è puro in A;*
2. *B è addendo diretto di $n^{-1}B$ per ogni $n > 0$;*
3. *se $B \leq C \leq A$ con C/B finitamente generato, allora B è addendo diretto di C.*

Dimostrazione. ($1 \implies 2$) $(n^{-1}B)/B$ è limitato e quindi somma diretta di ciclici per il teorema 2.1.3; allora B è addendo diretto di $n^{-1}B$ per il teorema 2.2.1.

($2 \implies 3$) Sia vero (2) e supponiamo le ipotesi di (3). C/B, essendo finitamente generato, è somma diretta finita di ciclici per il teorema 1.3.12. Se essi non sono tutti finiti, segue facilmente dal lemma 1.3.9 che B è addendo diretto di C. Quindi assumiamo C/B finito: allora esiste $n > 0$ tale che $n(C/B) = \{0\}$ ovvero tale che $nC \leq B$ cioè $C \leq n^{-1}B$. Per ipotesi (2) B è addendo diretto di $n^{-1}B$: si ha quindi $B \leq C \leq n^{-1}B = B \oplus B'$, da cui segue facilmente che B è addendo diretto di C.

($3 \implies 1$) Dato $a \in A$, $\frac{\langle a\rangle + B}{B}$ è finitamente generato e quindi, se vale (3), $\langle a\rangle + B = \langle h\rangle \oplus B$ con $h \in A$. Allora $a + B = h + B$ ha ordine n se e solo se $nh \in B$, che è vero se e solo se $nh = 0$, quindi $\mathrm{o}(a + B) = \mathrm{o}(h)$. Questo mostra che ogni classe in A/B contiene un elemento dello stesso ordine della classe, e questo equivale alla purità di A in B per il lemma 2.2.2. □

Grazie al lemma 2.2.3 possiamo dimostrare la caratterizzazione della purità attraverso sistemi di equazioni, citata all'inizio della sezione:

2.2.4 Teorema. *Un sottogruppo B di A è puro se e solo se ogni sistema*

$$\sum_{j=1}^{n} n_{ij}x_j = b_i \qquad\qquad (b_i \in B,\ i = 1, \ldots, m)$$

risolvibile in A è risolvibile anche in B.

Dimostrazione. Sia B puro in A e sia $(a_j)_{j=1\ldots m}$ soluzione in A. Posto $C = \langle B, a_1, \ldots, a_m\rangle$, allora C/B è finitamente generato e quindi B è addendo diretto di C per il lemma 2.2.3; diciamo $C = B \oplus B'$. Le proiezioni su B degli a_j danno allora una soluzione in B:

$$b_i = \sum_{j=1}^{n} n_{ij}a_j = \sum_{j=1}^{n} n_{ij}(\pi_B(a_j) + \pi_{B'}(a_j)) = \sum_{j=1}^{n} n_{ij}(\pi_B(a_j)) + \sum_{j=1}^{n} n_{ij}(\pi_{B'}(a_j)) \in B + B'$$

e per le proprietà di somma diretta dev'essere quindi $\sum_{j=1}^{n} n_{ij}(\pi_{B'}(a_j)) = 0$ e $b_i = \sum_{j=1}^{n} n_{ij}(\pi_B(a_j))$, come volevasi dimostrare.

L'altra implicazione è banale: se ogni tale sistema risolvibile in A è risolvibile in B, questo vale anche per la singola equazione a una incognita $nx = b$, e si ritrova la definizione di purità data inizialmente. □

2.3 Altri risultati

Concludiamo il capitolo con un esempio.

2.3.1 Esempio (Gruppi elementari)**.** Un gruppo A contiene solo sottogruppi puri se e solo se ogni elemento di A ha ordine intero privo di quadrati (cioè nessun primo della sua fattorizzazione ha esponente > 1; chiamiamo gruppo *elementare* un gruppo con questa proprietà).

Dimostrazione. Se A è un gruppo elementare, è di torsione e quindi per il teorema 1.3.14 è somma diretta delle sue p-componenti, che sono p-gruppi elementari, ovvero gruppi in cui ogni elemento non nullo ha ordine p.

Mostriamo ora che ogni p-gruppo elementare è somma diretta di gruppi ciclici di ordine p. Un p-gruppo elementare A_p è un $\mathbb{F}_p$-spazio vettoriale, infatti per ogni $a \in A_p$ si ha $na = ma$ se e solo se $n \equiv m \mod p$, cioè se e solo se n e m rappresentano lo stesso elemento di $\mathbb{F}_p$. Si verificano immediatamente gli assiomi di spazio vettoriale. Allora, se $(a_{p,i})_{i\in I}$ è una sua base, $A_p = \bigoplus_{i\in I}\langle a_{p,i}\rangle = \bigoplus_{i\in I} C_{p,i}$ è somma diretta di gruppi ciclici di ordine p, quindi A è somma diretta di gruppi ciclici con ordini primi:

$$A = \bigoplus_p A_p = \bigoplus_p (\bigoplus_i C_{p,i})$$

Sia ora $B \leq A$. Per il teorema 1.3.16, B è somma diretta di gruppi ciclici, e quindi

$$B = \bigoplus_p (\bigoplus_i B_{p,i}) = \bigoplus_p B_p$$

ove $B_{p,i} \in \{\{0\}, C_{p,i}\}$ e B_p è la p-componente di H. Per ogni p, B_p è sottogruppo di A_p, che è $\mathbb{F}_p$-spazio vettoriale, quindi B_p è suo sottospazio vettoriale, quindi è suo addendo diretto: $A_p = B_p \oplus H_p$, esistono H_p. Allora:

$$A = \bigoplus_p A_p = \bigoplus_p (B_p \oplus H_p) = (\bigoplus_p B_p) \oplus (\bigoplus_p H_p) = B \oplus (\bigoplus_p H_p)$$

Quindi B è addendo diretto di A, dunque è puro in A.

Viceversa, sia A tale che ogni suo sottogruppo è puro. Allora, per ogni $C \leq B \leq A$, si ha anche C puro in B: infatti, se fosse $nC \subset C \cap nB$, avremmo $C \cap nA = nC \subset C \cap nB$, che è assurdo perché $C \cap nA \supseteq C \cap nB$. Applichiamo questo fatto ai sottogruppi $\langle px\rangle \leq \langle x\rangle$, per un generico $x \in A$ e un primo p:

$$\langle npx\rangle = n\langle px\rangle = \langle px\rangle \cap n\langle x\rangle = \langle px\rangle \cap \langle nx\rangle = \langle \mathrm{mcm}(n,p)x\rangle$$

per ogni n. Se n è tale che $p \mid n$ si trova $\langle npx\rangle = \langle nx\rangle$, che vale solo se $\langle nx\rangle = \{0\}$, quindi $\mathrm{o}(x)$ è finito. Sia ora p un primo tale che $\mathrm{o}(x) = pk$; vogliamo mostrare che $p \nmid k$. Se fosse $p \mid k$, sarebbe $\{0\} = \langle kpx\rangle = \langle kx\rangle \neq \{0\}$: assurdo. $\square$

Capitolo 3

Pura iniettività e pura proiettività

3.1 Sequenze pure-esatte

3.1.1 Definizione. Una sequenza esatta

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

si dice si dice *pura-esatta* se $\operatorname{im}\alpha$ è puro in B.

Se scegliamo una sequenza esatta del tipo

$$0 \longrightarrow A \xhookrightarrow{\iota} B \xrightarrow{\pi} B/A \longrightarrow 0 \tag{3.1}$$

con A sottogruppo di B, ι inclusione e π proiezione sul quoziente, essa è pura-esatta se e solo se A è puro in B.

3.1.2 Teorema. *Una sequenza esatta* (3.1) *è pura-esatta se e solo se ogni gruppo ciclico G ha la proprietà proiettiva.*

Dimostrazione. Siano $G = \langle g \rangle$ e

$$\begin{aligned} \phi\colon G &\longrightarrow B/A \\ g &\longmapsto b + A \end{aligned}$$

e consideriamo il diagramma con riga pura-esatta

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, hook, "\iota"] & B \arrow[r, two heads, "\pi"] & B/A \arrow[r] & 0 \\ & & & G \arrow[u, "\phi"] \arrow[ul, dashed, "\psi"] & \end{tikzcd}$$

Se $G \cong \mathbb{Z}$, allora è ben definito $\psi\colon G \to B$, $\psi(g) = b$ e $\psi(g) + A = \phi(g)$. Se $\mathrm{o}(g) = n$, allora $nb \in A \cap nB = nA$, quindi $nb = na$ per qualche $a \in A$. $\psi\colon G \to B$, $\psi(g) = b - a$ è ben definito e $\psi(g) + A = b + A$.

Viceversa supponiamo che ogni gruppo ciclico abbia la proprietà proiettiva rispetto a (3.1). Sia $nb = a \in A$; allora $n(b + A) = 0$. Si considerino $G = \mathbb{Z}/n\mathbb{Z}$ e

$$\begin{aligned} \phi\colon G &\longrightarrow B/A \\ 1 + n\mathbb{Z} &\longmapsto b + A, \end{aligned}$$

che è ben definita. Per ipotesi esiste $\psi\colon G \to B$ tale che $\pi\psi = \phi$. Sia $b' = \psi(1 + n\mathbb{Z})$; allora $nb' = 0$ e $b' + A = b + A$, cioè $b - b' \in A$ e $n(b - b') = nb$, quindi A è puro in B. □

Abbiamo poi il teorema duale:

3.1.3 Teorema. *Una sequenza esatta* (3.1) *è pura-esatta se e solo se ogni gruppo cociclico G ha la proprietà iniettiva.*

Dimostrazione. Proviamo innanzitutto che possiamo supporre ϕ suriettivo. Infatti, se a G sostituiamo $\operatorname{im}\phi$, che è cociclico essendo sottogruppo di un cociclico (lemma 1.1.1), e a ϕ sostituiamo $\phi'\colon A \to \operatorname{im}\phi$, che è suriettivo, allora per ipotesi esiste $\psi'\colon B \to \operatorname{im}\phi$ che rende commutativo il diagramma; estendendo il codominio di ψ' a G si ottiene il morfismo ψ che fa commutare il diagramma originale.

Notiamo ora che una somma diretta finita ha la proprietà iniettiva se e solo se la ha ogni sua componente: se G_1 e G_2 hanno la proprietà iniettiva, dato $\phi\colon A \to G_1 \oplus G_2$ con $\phi(a) = \phi_1(a) \oplus \phi_2(a)$ ($\phi_i(a) \in G_i$), per ipotesi esistono ψ_1 e ψ_2 tali che $\psi_i(\alpha(a)) = \phi_i(a)$ e basta prendere $\psi = \psi_1 \oplus \psi_2$; viceversa, se $G_1 \oplus G_2$ ha la proprietà iniettiva, dato $\phi_i\colon A \to G_i$, basta estendere il codominio di ϕ_i a $G_1 \oplus G_2$ (chiamiamo $\widetilde{\phi}_i$ l'estensione), allora per ipotesi esiste ψ tale che $\psi(\alpha(a)) = \widetilde{\phi}_i(a)$, ma $\widetilde{\phi}_i(a) = \phi_i(a)$. Quindi, poiché le somme dirette finite di gruppi cociclici sono esattamente i gruppi finitamente cogenerati, è equivalente considerare l'asserto sostituendo 'finitamente cogenerato' a 'cociclico'.

Consideriamo i due diagrammi seguenti.

$$\begin{tikzcd} A \arrow[rr, hook, "\iota"] \arrow[dr, "\phi"'] & & B \arrow[dl, dashed, "\psi"] \\ & G & \end{tikzcd} \tag{3.2}$$

$$\begin{tikzcd} \dfrac{A}{\ker\phi} \arrow[rr, hook, "\overline{\iota}"] \arrow[dr, "\overline{\phi}"', "\sim"] & & \dfrac{B}{\ker\phi} \arrow[dl, dashed, "\overline{\psi}"] \\ & G & \end{tikzcd} \tag{3.3}$$

Ricordando che $G \cong A/\ker\phi$ per suriettività di ϕ, vediamo che la proprietà iniettiva, cioè l'esistenza di ψ che renda 3.2 commutativo, è equivalente all'esistenza di $\overline{\psi}$ che renda commutativo 3.3, dove

$$\overline{\phi}\colon x + \ker\phi \mapsto \phi(x) \qquad \overline{\iota}\colon x + \ker\phi \mapsto x + \ker\phi$$

Infatti, se 3.2 commuta, allora il morfismo

$$\overline{\psi}\colon y + \ker\phi \mapsto \psi(y)$$

è ben definito: sia $y + \ker\phi = y' + \ker\phi$, allora $\ker\phi \ni y - y' = k$ e quindi $\psi(y - y') = \psi(k) = \phi(k) = 0$ da cui $\psi(y) = \psi(y')$. È poi evidente che faccia commutare 3.3. Viceversa: se, per ogni ϕ, esiste $\overline{\psi}$ che faccia commutare 3.3, allora definiamo

$$\psi\colon y \mapsto \overline{\psi}(y + \ker\phi)$$

e troviamo per ogni $x \in A$

$$\begin{aligned}\psi(x) = \overline{\psi}(x + \ker\phi) = \overline{\psi}(x + \ker\phi) = \\ = \overline{\psi}(x + \ker\phi) = \overline{\phi}(x + \ker\phi) = \phi(x)\end{aligned}$$

cioè ψ rende 3.2 commutativo.

L'esistenza del diagramma commutativo 3.3 equivale a sua volta all'esistenza di una fattorizzazione dell'identità su $A/\ker\phi$, dopo averlo identificato con G. Per il corollario 1.3.4, questo equivale ad affermare che $A/\ker\phi$ è addendo diretto di $B/\ker\phi$. Per il lemma 2.1.4, questo equivale alla purità di A in B, che è la tesi. □

3.2 Pura iniettività e pura proiettività

Abbiamo dimostrato che i gruppi cociclici (risp. ciclici) hanno la proprietà iniettiva (risp. proiettiva) rispetto a sequenze pure-esatte. Vogliamo trovare ora tutti i gruppi che abbiano la proprietà iniettiva o proiettiva rispetto a sequenze pure-esatte.

3.2.1 Definizione. Un gruppo G si dice *puro-iniettivo* se ha la proprietà iniettiva rispetto a ogni sequenza pura-esatta. Si dice *puro-proiettivo* se ha la proprietà proiettiva rispetto a ogni sequenza pura-esatta.

3.2.2 Teorema. *Un gruppo è puro-proiettivo se e solo se è somma diretta di gruppi ciclici.*

Dimostrazione. Consideriamo il diagramma con riga pura-esatta

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\alpha"] & B \arrow[r, "\beta"] & C \arrow[r] & 0 \\
 & & & \bigoplus_i \langle g_i \rangle \arrow[u, "\phi"] & \\
 & & & \langle g_i \rangle \arrow[u, hook] \arrow[uul, dashed, "\psi_i"] &
\end{tikzcd}$$

Per il teorema 3.1.2, per ogni i esistono $\psi_i\colon \langle g_i\rangle \to B$ tali che $\phi(g_i) = \beta(\psi_i(g_i))$. Allora definiamo

$$\psi\colon G \longrightarrow B \quad \text{tale che} \quad \psi\Big(\sum_{j=1}^{k} n_{i_j} g_{i_j}\Big) = \sum_{j=1}^{k} n_{i_j} \psi_{i_j}(g_{i_j})$$

Si ha facilmente la commutatività (alleggeriamo la scrittura): $\beta(\psi(g_1 + g_2)) = \beta(\psi_1(g_1) + \psi_2(g_2)) = \beta(\psi_1(g_1)) + \beta(\psi_2(g_2)) = \phi(g_1) + \phi(g_2) = \phi(g_1 + g_2)$.

Viceversa, sia $G = \{g_i \mid i \in I\}$ puro-proiettivo. Si consideri il gruppo $\bigoplus_{i\in I}\langle g_i\rangle$ e il morfismo suriettivo

$$\begin{aligned} \zeta\colon \bigoplus_{i\in I}\langle g_i\rangle &\longrightarrow G \\ g_{i_1} \oplus \cdots \oplus g_{i_k} &\longmapsto \sum_{j=1}^{k} g_{i_j} \end{aligned}$$

Mostriamo che $\ker\zeta$ è puro in $\bigoplus_i\langle g_i\rangle$: supponiamo $ng = k \in \ker\zeta$ per $g \in \bigoplus_i\langle g_i\rangle$. $\zeta(g) \in G$, quindi $\zeta(g) = g_i$ per qualche i, e inoltre $\zeta(g) = g_i = \zeta(g_i)$; quindi $g - g_i \in \ker\zeta$, e da $0 = \zeta(k) = n\zeta(g) = ng_i$ si ha $n(g - g_i) = ng = k$. Quindi, il seguente diagramma ha riga pura esatta e, essendo G puro-proiettivo per ipotesi, esiste ψ che lo renda commutativo:

$$\begin{tikzcd} 0 \arrow[r] & \ker\zeta \arrow[r, "\iota"] & \bigoplus_i\langle g_i\rangle \arrow[r, "\zeta"] & G \arrow[r] & 0 \\ & & & G \arrow[u, "1_G"'] \arrow[ul, dashed, "\psi"] & \end{tikzcd}$$

Essendo $\zeta\psi = 1_G$, ψ è iniettiva, quindi $G \cong \psi(G) \leq \bigoplus_i\langle g_i\rangle$, cioè G è (isomorfo a) un sottogruppo di una somma diretta di ciclici, quindi è anch'esso somma diretta di ciclici (per il teorema 1.3.16). $\square$

3.2.3 Teorema. *Un gruppo è puro-iniettivo se e solo se è addendo diretto di un prodotto diretto di gruppi cociclici.*

Dimostrazione. Supponiamo G addendo diretto di $\prod_i C_i$, C_i cociclici. Quindi $\prod_i C_i = G \oplus H$ per qualche H; abbiamo poi i morfismi di proiezione e inclusione associati al prodotto diretto e quelli associati alla somma diretta

$$\begin{aligned} \pi_i\colon \prod_{i\in I} C_i &\longrightarrow C_i \\ (\cdots c_i \cdots) &\longmapsto c_i \end{aligned} \qquad \begin{aligned} \iota_i\colon C_i &\longrightarrow \prod_{i\in I} C_i \\ c_i &\longmapsto (0 \cdots c_i \cdots 0) \end{aligned}$$

$$\begin{aligned} \pi\colon \prod_{i\in I} C_i &\longrightarrow G \\ g + h &\longmapsto g \end{aligned} \qquad \begin{aligned} \iota\colon G &\longrightarrow \prod_{i\in I} C_i \\ g &\longmapsto g \end{aligned}$$

Consideriamo ora il diagramma seguente (con riga pura-esatta):

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\alpha"] \arrow[d, "\phi"'] & B \arrow[r, "\beta"] \arrow[ddd, dashed, "\psi_i"] & C \arrow[r] & 0 \\ & G \arrow[d, hook, "\iota"'] & & & \\ & \prod_i C_i \arrow[d, two heads, "\pi_i"'] & & & \\ & C_i & & & \end{tikzcd}$$

Per il teorema 3.1.3, per ogni i esistono $\psi_i\colon B \to C_i$ tali che $\psi_i\alpha = \pi_i\iota\phi$. Allora se definiamo

$$\begin{aligned}\psi\colon B &\longrightarrow \prod_{i\in I} C_i\\ b &\longmapsto (\cdots \psi_i(b)\cdots)\end{aligned}$$

otteniamo $\psi_i = \pi_i\psi$ e quindi $\pi_i\psi\alpha = \psi_i\alpha = \pi_i\iota\phi$ per ogni i, da cui $\iota\phi = \psi\alpha$. Essendo poi $\pi\iota = 1_G$, è $\phi = \pi\iota\phi = \pi\psi\alpha$, quindi $\pi\psi\colon B \to G$ è un morfismo che soddisfa la richiesta.

Viceversa, sia G puro-iniettivo. Sia $\prod_{i\in I}(G/H_i)$ la famiglia dei quozienti cociclici di G e ζ definito come

$$\begin{aligned}\zeta\colon G &\longrightarrow \prod_{i\in I}(G/H_i)\\ g &\longmapsto (\cdots g + H_i \cdots)\end{aligned}$$

ζ è iniettivo, infatti: se $(\cdots g + H_i \cdots) = (\cdots H_i \cdots)$, allora $g \in \bigcap H_i$; se $g \neq 0$ e M è sottogruppo di G massimale tra quelli che escludono g, allora G/M è cociclico (lemma 1.1.2) e $g \notin M$, contraddizione.
Mostriamo che $\operatorname{im}\zeta$ è puro in $\prod_i(G/H_i)$ (è sufficiente verificare la p-purità per un primo generico). Sia $g \in G \setminus p^nG$, ovvero $p^nx = g$ non ha soluzione in G e quindi (usando l'iniettività di ζ) neanche $p^n\zeta(x) = \zeta(g)$, ovvero $p^ny = \zeta(g)$ non ha soluzione in $\operatorname{im}\zeta$; vogliamo mostrare che allora $p^ny = \zeta(g)$ non ha soluzione neanche in $\prod_i(G/H_i)$. Scegliamo M massimale tra i sottogruppi di G tali che $p^nG \leq M$ e $g \notin M$. G/M è cociclico (lemma 1.1.2), quindi $G/M = \mathbb{Z}(p^k)$ (teorema 1.1.4) e da $p^nG \leq M$ segue $k \leq n$. Poiché $G/M = G/H_i$ per qualche i, e $\mathrm{h_p}(g + M) = k - 1 < n$, segue che

$$p^nx + H_i = p^nx + M \neq g + M = g + H_i$$

per ogni $x \in G$, quindi

$$p^n(\cdots x + H_i \cdots) \neq (\cdots g + H_i \cdots) = \zeta(g)$$

per ogni $x \in G$, quindi $p^ny \neq \zeta(g)$ per ogni $y \in \prod_i(G/H_i)$.
Quindi, il seguente diagramma ha riga pura-esatta e, essendo G puro-iniettivo per ipotesi, esiste ψ che lo renda commutativo:

$$\begin{tikzcd} 0 \arrow[r] & G \arrow[r, "\zeta"] \arrow[d, "1_G"] & \prod_i(G/H_i) \arrow[r, "\pi"] \arrow[dl, dashed, "\psi"] & \dfrac{\prod_i(G/H_i)}{\operatorname{im}\zeta} \arrow[r] & 0 \\ & G & & & \end{tikzcd}$$

$\psi\zeta = 1_G$ è una fattorizzazione dell'identità su G e, essendo ζ iniettiva, $G \cong \zeta(G) \leq \prod_i(G/H_i)$. Per il corollario 1.3.4, $\zeta(G)$ è addendo diretto di $\prod_i(G/H_i)$; quindi G è (isomorfo a) un addendo diretto di $\prod_i(G/H_i)$. $\square$

Dedichiamo allo studio di questi gruppi il prossimo capitolo.

Capitolo 4

Gruppi algebricamente compatti

Ricordiamo che: ogni volta che parleremo di compattezza o completezza, assumeremo che la topologia in questione sia Hausdorff.

4.0.1 Definizione. Diciamo che un gruppo A è *algebricamente compatto* se è addendo diretto di un gruppo che ammette una topologia compatta.

Il prossimo risultato mostra come la nozione di gruppo algebricamente compatto si presti ad essere osservata sotto molteplici aspetti, algebrici e topologici.

4.0.2 Teorema. *Per un gruppo abeliano A, le seguenti condizioni sono equivalenti:*

1. *A è puro-iniettivo;*
2. *A è addendo diretto di ogni gruppo di cui è sottogruppo puro;*
3. *A è addendo diretto di un prodotto diretto di gruppi cociclici;*
4. *A è addendo diretto di un gruppo che ammette una topologia compatta;*
5. *se ogni sottosistema finito di un sistema su A ha soluzione in A, allora il sistema ammette soluzione in A.*

Dimostrazione. (1 $\implies$ 2) Sia G un gruppo che contiene A. Il seguente diagramma

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\iota"] \arrow[d, "1_A"'] & G \arrow[r, "\pi"] \arrow[dl, dashed, "\psi"] & G/A \arrow[r] & 0 \\ & A & & & \end{tikzcd}$$

ha riga pura-esatta, quindi per pura-iniettività di A esiste ψ che dia la fattorizzazione di 1_A descritta, quindi A è addendo diretto di G, per il corollario 1.3.4.

(2 $\implies$ 3) Consideriamo il prodotto diretto $\prod_{i \in I}(A/H_i)$ di tutti i quozienti

cociclici di A e ζ definito come

$$\begin{aligned} \zeta\colon A &\longrightarrow \prod_{i\in I}(A/H_i) \\ a &\longmapsto (\cdots a + H_i \cdots) \end{aligned}$$

come nella dimostrazione del teorema 3.2.3, dove abbiamo provato che ζ è iniettiva e $\operatorname{im}\zeta \cong A$ è puro in $\prod_{i\in I}(A/H_i)$, cioè A è sottogruppo puro di un prodotto diretto di gruppi cociclici. Usando l'ipotesi (2), A è suo addendo diretto.

($3 \implies 4$) Mostriamo che i gruppi cociclici sono addendi diretti di gruppi che ammettono una topologia compatta. Allora seguirà facilmente (4): infatti, dato $\prod_i C_i = A \oplus A'$ con C_i cociclico per ogni i, avremo $K_i = C_i \oplus C_i'$ con K_i compatto, quindi

$$\prod_i K_i = \prod_i (C_i \oplus C_i') = (\prod_i C_i) \oplus (\prod_i C_i') = A \oplus A' \oplus \prod_i C_i'$$

sarà compatto (perché prodotto di compatti), con A come addendo diretto. Sappiamo che i gruppi cociclici sono esattamente i gruppi isomorfi a $\mathbb{Z}(p^k)$ dove k è naturale o ∞. Se k è naturale, $\mathbb{Z}(p^k)$ è finito e quindi compatto nella topologia discreta. Per quanto riguarda $\mathbb{Z}(p^\infty)$, esso è addendo diretto di $\mathbb{R}/\mathbb{Z}$, che è compatto (per l'usuale topologia indotta dalla topologia euclidea). Infatti, sia $G = \mathbb{R}/\mathbb{Z}$:

$$G = \mathrm{T}(G) \oplus G/\mathrm{T}(G) = \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Q} \cong \bigoplus_p \mathbb{Z}(p^\infty) \oplus \mathbb{R}/\mathbb{Q}.$$

($4 \implies 5$) Consideriamo il sistema

$$\sum_{j\in J} n_{ij}x_j = a_i \qquad (a_i \in A,\ i \in I,\ \text{fissato } i \text{ sia } n_{ij} = 0 \text{ per quasi ogni } j)$$

e supponiamo che ogni suo sottosistema finito ammetta soluzione in A. Per l'ipotesi (4) esiste un gruppo A' tale che $K = A \oplus A'$ ammetta una topologia compatta. Consideriamo il sistema come sistema su K; siano $(\cdots c_{ij} \cdots)_j \in K^{|J|}$ una soluzione dell'equazione i-esima, e X_i l'insieme di tali soluzioni. $K^{|J|}$ è compatto nella topologia prodotto, perché prodotto di compatti; X_i è chiuso, essendo definito da un'equazione. La condizione di risolubilità di ogni sottosistema finito implica che $\bigcap_{i\in F} X_i \neq \emptyset$ per ogni F sottoinsieme finito di I, ma allora, per compattezza di $K^{|J|}$, si ha anche $\bigcap_{i\in I} X_i \neq \emptyset$, cioè esiste una soluzione del sistema in K. Tale soluzione ha la forma $(\cdots c_j + c_j' \cdots) \in K^{|J|}$; allora $(\cdots c_j \cdots) \in A^{|J|}$ è soluzione in A, essendo

$$\sum_{j\in J} n_{ij}(c_j + c_j') = (\sum_{j\in J} n_{ij}c_j) + (\sum_{j\in J} n_{ij}c_j') = a_i \in A$$

e quindi

$$\sum_{j\in J} n_{ij}c_j' = 0$$

da cui la tesi.

($5 \implies 1$) Consideriamo il seguente diagramma con riga pura-esatta

$$\begin{tikzcd} 0 \arrow[r] & B \arrow[r, "\iota"] \arrow[d, "\phi"'] & C \arrow[r, "\pi"] & C/B \arrow[r] & 0 \\ & A & & & \end{tikzcd}$$

dove $C/B = \langle c_j + B \rangle_{j \in J}$ per opportuni rappresentanti $c_j \in C$. Siano poi

$$\sum_{j \in J} n_{ij} c_j = b_i \in B \qquad (i \in I)$$

le equazioni che definiscono le relazioni tra i c_j e gli elementi, chiamiamoli b_i di B. Consideriamo poi il sistema

$$\sum_{j \in J} n_{ij} x_j = \phi(b_i) \in A \qquad (i \in I)$$

Consideriamone un sottosistema finito: esso ha un numero finito di incognite $x_{j_1}, \ldots, x_{j_m}$. Se poniamo $B' = \langle B, c_{j_1}, \cdots, c_{j_m} \rangle$, allora B è addendo diretto di B' (per il lemma 2.2.3, poiché $B \leq B' \leq C$ con B puro in C e B'/B finitamente generato), cioè $B' = B \oplus C'$. Allora $c_{j_k} \in B'$ e le immagini tramite ϕ delle B-componenti $\pi_B(c_{j_k})$ dei c_{j_k} forniscono una soluzione in A del sottosistema. Usando l'ipotesi (5), l'intero sistema ha soluzione $(a_j)_{j \in J}$ in A. Definendo $\psi \colon C \to A$ tale che $\psi(c_j) = a_j$ si ottiene la commutatività del diagramma, quindi la pura-iniettività di A. □

4.0.3 Esempio. Abbiamo dimostrato che un gruppo è divisibile se e solo se è addendo diretto di ogni gruppo di cui è sottogruppo (teorema 1.4.6); di conseguenza, ogni gruppo divisibile è algebricamente compatto. Per il teorema 2.1.1, ogni gruppo limitato è algebricamente compatto.

Il teorema mostra in particolare che i gruppi algebricamente compatti sono esattamente i gruppi puri-iniettivi. L'equivalenza tra (1) e (2) mostra poi una analogia tra gruppi divisibili e gruppi algebricamente compatti: i gruppi divisibili sono esattamente quelli iniettivi, cioè esattamente quelli con la proprietà di essere addendi diretti di ogni gruppo di cui sono sottogruppi (teorema 1.4.6); gli algebricamente compatti sono esattamente quelli puri-iniettivi, cioè esattamente quelli con la proprietà di essere addendi diretti di ogni gruppo di cui sono sottogruppi puri.

4.0.4 Corollario. *Un prodotto diretto di gruppi è algebricamente compatto se e solo se lo è ogni sua componente.*

Dimostrazione. Se ogni A_i è compatto allora $K_i = A_i \oplus A'_i$ con K_i compatto, da cui

$$\prod_i K_i = \prod_i (A_i \oplus A'_i) = (\prod_i A_i) \oplus (\prod_i A'_i)$$

che è compatto nella topologia prodotto perché prodotto di compatti, quindi $\prod_i A_i$ è algebricamente compatto. Viceversa, sia $\prod_i A_i$ algebricamente compatto: si ha

$$K = (\prod_i A_i) \oplus A' \cong A_j \oplus (\prod_{i \neq j} A_i) \oplus A'$$

e con K compatto; quindi ogni A_j è algebricamente compatto. □

4.0.5 Corollario. *Un gruppo ridotto algebricamente compatto è addendo diretto di un prodotto diretto di p-gruppi ciclici.*

Dimostrazione. Se A è algebricamente compatto, per la condizione (3) del teorema precedente vale $A \oplus A' = C = C_1 \oplus C_2$ con C_1 prodotto diretto di gruppi ciclici $\mathbb{Z}(p^k)$, C_2 prodotto diretto di gruppi quasiciclici $\mathbb{Z}(p^\infty)$. C_2 è il sottogruppo divisibile massimale di C, quindi è pienamente invariante, infatti se $n \mid x$ allora $x = nx'$ da cui $\phi(x) = n\phi(x')$ e quindi $n \mid \phi(x)$. Allora, per il lemma 1.3.18, $C_2 = (C_2 \cap A) \oplus (C_2 \cap B)$; ma $C_2 \cap A = \{0\}$, essendo C_2 divisibile e A ridotto per ipotesi. Quindi $C_2 \leq B$ e A è addendo diretto di $A \oplus (A'/C_2) \cong C_1$, prodotto di p-gruppi ciclici. □

Il seguente lemma tecnico mostra che possiamo indebolire la definizione di compattezza algebrica (vale ovviamente il 'se e solo se'). Lo useremo nel prossimo paragrafo.

4.0.6 Lemma. *Sia A addendo diretto di ogni gruppo G tale che A è puro in G e $G/A \cong \mathbb{Q}$ o $G/A \cong \mathbb{Z}(p^\infty)$ per qualche p. Allora A è algebricamente compatto.*

Dimostrazione. Grazie alla struttura dei gruppi divisibili, è sufficiente supporre che A sia addendo diretto di ogni gruppo in cui è puro con quoziente divisibile. Dobbiamo dimostrare che A è addendo diretto di ogni gruppo G in cui è contenuto come sottogruppo puro. Sia dunque A puro in G.
Consideriamo prima il caso in cui G/A è di torsione, e prendiamone un sottogruppo B/A che sia *basico*, ovvero con le seguenti proprietà:

1. è puro in G/A,
2. è somma diretta di ciclici,
3. ha quoziente $(G/A)/(B/A)$ divisibile.

Da A puro in G e da (1), segue grazie al lemma 2.0.5 che B è puro in G; quindi A è puro in B, perché $B \supseteq nA = nA \cap B = (A \cap nG) \cap B = A \cap nB$.
Da A puro in B e da (2), segue grazie al teorema 2.2.1 che A è addendo diretto di B, diciamo $B = A \oplus B'$ per un $B' \leq B$.
Da B puro in G segue B/B' puro in G/B', e il quoziente è divisibile per (3) essendo $(G/B')/(B/B') \cong G/B \cong (G/A)/(B/A)$. Per l'ipotesi, allora, B/B' è addendo diretto di G/B', diciamo $G/B' = B/B' \oplus G'/B'$ per un $G' \leq G$.
Otteniamo
$$G = B + G' = A \oplus B' + G' = A + G'$$
e
$$A \cap G' = (A \cap B) \cap G' = A \cap (B \cap G') = A \cap B' = \{0\},$$
da cui $G = A \oplus G'$.

Consideriamo ora il caso in cui G/A è senza torsione. Per il teorema 1.4.5, $G/A \leq D$ per un divisibile D, anch'esso senza torsione. Se troviamo $H \geq G$ tale che $H/A \cong D$ abbiamo concluso, perché avremmo A puro in H ($nh = a \in A$ per $h \in H$ implica passando al quoziente $n\overline{h} = \overline{a} = \overline{0}$, ma essendo H/A senza torsione dev'essere $\overline{h} = \overline{0}$ cioè $h \in A$), quindi per ipotesi A addendo diretto di

H e quindi anche di G. Mostriamo dunque che esiste un tale H con il seguente lemma, di valenza generale:

Siano G un gruppo, $A \leq G$, D tale che $G/A \leq D$; allora D è isomorfo al quoziente su A di un opportuno gruppo contenente G, cioè esiste un gruppo H tale che $G \leq H$, $D \cong H/A$.

Dimostrazione. La situazione è riassunta dal diagramma in figura. La sequenza superiore è esatta per ipotesi; vogliamo mostrare l'esistenza di H che renda esatta quella inferiore.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \hookrightarrow & G & \twoheadrightarrow & G/A & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A & \hookrightarrow & H & \twoheadrightarrow & D & \longrightarrow & 0 \end{array}$$

Sia $G \leq D'$ con D' divisibile; allora $G/A \leq D'/A$. Se G/A non si può estendere in D'/A a un gruppo isomorfo a D, basta trovare D'' divisibile tale che questo sia possibile in $(D'/A) \oplus D''$. Se $H/A \cong D$ e contiene G/A, allora H $(\leq D' \oplus D'')$ è un gruppo con la proprietà richiesta.

Infine, se G/A è un gruppo misto con torsione T/A, allora A è puro in T e quindi per il primo caso si ha $T = A \oplus T'$; $(G/A)/(T/A) \cong G/T$ è senza torsione con T puro in G, quindi per il secondo caso $G = T \oplus G'$. Dunque $G = A \oplus (T' \oplus G')$ e si conclude. □

4.1 Caratterizzazioni topologiche

I prossimi risultati caratterizzano i gruppi algebricamente compatti in termini di completezza nella topologia $\mathbb{Z}$-adica. Grazie alla decomposizione di un gruppo abeliano come somma diretta di un gruppo divisibile e un gruppo ridotto (teorema 1.4.4), essendo già nota la struttura dei gruppi divisibili (teorema 1.4.7), è sufficiente descrivere i gruppi algebricamente compatti ridotti.

4.1.1 Teorema. *Un gruppo è ridotto algebricamente compatto se e solo se è completo nella topologia $\mathbb{Z}$-adica.*

Serve prima un semplice lemma:

4.1.2 Lemma. *Sia A un gruppo abeliano dotato della topologia $\mathbb{Z}$-adica, e sia $B \leq A$; allora B è denso in A se e solo se A/B è divisibile.*

Dimostrazione. Mostriamo che $n(A/B) = A/B$ per ogni $n \neq 0$ se e solo se $(a + nA) \cap B \neq \emptyset$ per ogni $a \in A$ e per ogni $n \neq 0$. Si ha $n(A/B) = A/B$ per ogni $n \neq 0$ (cioè $(nA + B)/B = A/B$) se e solo se per ogni $a \in A$ e $n \neq 0$ esiste $a' \in A$ tale che $a + B = na' + B$ cioè se e solo se $a - na' \in (a + nA) \cap B$. □

Dimostrazione del teorema 4.1.1. Sia A ridotto algebricamente compatto; per il corollario 4.0.5, $\prod_{i,j} \mathbb{Z}(p_i^{k_j}) = A \oplus A'$ per alcuni p_i primi e k_j interi. Ogni $\mathbb{Z}(p^k)$ è completo nella topologia $\mathbb{Z}$-adica (perché discreto), quindi (applicando il corollario 1.5.4) $\prod_{i,j} \mathbb{Z}(p_i^{k_j}) = A \oplus A' \cong A \times A'$ lo è e quindi anche A.

Viceversa, sia A completo nella topologia $\mathbb{Z}$-adica. Essendo Hausdorff, si ha $\bigcap_{n>0} nA = \{0\}$, e questo mostra che A non ha sottogruppi B tali che $nB = B$ per ogni n, ovvero sottogruppi divisibili, quindi A è ridotto. Sia $G \geq A$ tale che

A è puro in G e G/A è divisibile. Per il lemma 4.0.6, basta mostrare che A è addendo diretto di G. Dividiamo la dimostrazione in due casi.
Nel primo caso, sia G Hausdorff nella topologia $\mathbb{Z}$-adica. Per densità di A in G (lemma 4.1.2), ogni $g \in G$ è limite di una rete in A e, essendo la topologia $\mathbb{Z}$-adica a base numerabile di intorni, basta considerare limiti di successioni. La purità di A in G implica che G induce su A la topologia $\mathbb{Z}$-adica di A, quindi una tale successione è di Cauchy in A. Per ipotesi di completezza di A, la successione converge in A; essendo G Hausdorff, essa converge unicamente a g. Allora $g \in A$ e $G = A$, dunque la tesi è banalmente verificata.
Supponiamo ora che G non sia Hausdorff. Posto $G^1 = \bigcap_{n>0} nG$, G/G^1 è comunque Hausdorff e contiene A come sottogruppo puro:

$$G/G^1 \geq (A + G^1)/G^1 \cong A/(G^1 \cap A) = A$$

(l'ultimo passaggio segue dalla purità di A in G e dal fatto che A è Hausdorff: $G^1 \cap A = (\bigcap_{n>0} nG) \cap A = \bigcap_{n>0}(nG \cap A) = \bigcap_{n>0} nA = \{0\}$). Per il caso precedente abbiamo $G = A + G^1$, e abbiamo appena mostrato che la somma è diretta. $\square$

Un verso del teorema può essere migliorato affermando che *se un gruppo è completo in una qualsiasi topologia meno fine della topologia $\mathbb{Z}$-adica, allora è un gruppo ridotto algebricamente compatto*, e questo segue da:

4.1.3 Lemma. *Un gruppo A completo in una topologia Hausdorff meno fine della topologia $\mathbb{Z}$-adica è completo anche nella topologia $\mathbb{Z}$-adica.*

Dimostrazione. Sia $\{a_n\}_n$ una successione di Cauchy nella topologia $\mathbb{Z}$-adica; possiamo supporre che la successione sia 'pulita' nel senso definito nella sezione 1.5, ovvero $a_n - a_m \in U_n (= n!A)$ per ogni $m \geq n$. Supponiamo in particolare che

$$a_n - a_{n+1} = n!g_n, \text{ esiste } g_n \in A.$$

Definiamo

$$b_{nk} = g_n + (n+1)g_{n+1} + \cdots + (n+1)\cdots(n+k)g_{n+k},$$

allora

$$\begin{aligned} b_{nk} - b_{nj} = (n+1)\cdots(n+j+1)g_{n+j+1} + \ldots \\ \ldots + (n+1)\cdots(n+k)g_{n+k} \in j!A \end{aligned}$$

per ogni $k \geq j$, essendo

$$j! \mid (n+1)\cdots(n+j) = j!\binom{n+j}{j};$$

dunque $\{b_{nk}\}_k$ è di Cauchy. Inoltre $a_n = n!b_{nk} + a_{n+k+1}$ per ogni n, k. Poiché le successioni $\{a_n\}_n$ e $\{b_{nk}\}_k$ sono ancora di Cauchy in topologie meno fini della $\mathbb{Z}$-adica, per l'ipotesi di completezza esistono i loro limiti a e b_n rispetto a tali topologie. Allora se $k \to \infty$ troviamo $a_n = n!b_n + a$, quindi $a - a_n \in n!A$ e quindi a è limite di $\{a_n\}_n$ anche nella topologia $\mathbb{Z}$-adica. $\square$

4.1.4 Teorema. *Il limite inverso di gruppi ridotti algebricamente compatti è un gruppo ridotto algebricamente compatto.*

Dimostrazione. Il prodotto diretto di gruppi ridotti algebricamente compatti è ridotto, e algebricamente compatto perché ogni componente lo è (corollario 4.0.4), cioè è completo nella topologia $\mathbb{Z}$-adica (teorema 4.1.1); allora, essendo il limite inverso un sottospazio chiuso del prodotto diretto (lemma 1.6.4), è anch'esso completo nella topologia indotta (in generale meno fine della sua topologia $\mathbb{Z}$-adica), e quindi algebricamente compatto ridotto (lemma 4.1.3, teorema 4.1.1). $\square$

Segue in particolare che:

4.1.5 Esempio. Il gruppo J_p degli interi p-adici è algebricamente compatto, in quanto limite diretto dei gruppi $\mathbb{Z}/p^n\mathbb{Z}$ che sono ridotti, essendo finiti, e algebricamente compatti, essendo limitati (teorema 2.1.1).

Studiamo ora il completamento di un gruppo A rispetto alla topologia $\mathbb{Z}$-adica.

4.1.6 Teorema. *Sia A un gruppo, $\widehat{A} = \varprojlim_n A/nA$,*

$$\begin{aligned} \mu\colon A &\longrightarrow \widehat{A} \\ a &\longmapsto (\cdots a + nA \cdots) \end{aligned}$$

Allora:

1. *$\widehat{A}$ è completo nella topologia $\mathbb{Z}$-adica;*
2. $\ker\mu = A^1$*;*
3. *$\mu(A)$ è puro in $\widehat{A}$;*
4. *$\widehat{A}/\mu(A)$ è divisibile.*

Dimostrazione. (1) segue da quanto detto sui completamenti, oppure osservando che gli A/nA sono ridotti e algebricamente compatti, e applicando il teorema 4.1.4.

(2) $\mu(a) = 0$ se e solo se $a \in nA$ per ogni n, se e solo se $a \in \bigcap_{n>0} nA = A^1$.

(3) supponiamo $m\widehat{a} = \mu(a)$ (con $a \in A$, $\widehat{a} = (\cdots a_n + nA \cdots) \in \widehat{A}$), cioè $(\cdots ma_n + nA \cdots) = (\cdots a + nA \cdots)$, cioè $ma_n - a \in nA$ per ogni n. Allora, scegliendo $n = m$, si ha $ma_m - a \in mA$ e quindi $a = ma'$ per qualche $a' \in A$, quindi $\mu(a) = \mu(ma') = m\mu(a')$ come si voleva.

(4) per quanto detto nella sezione sui completamenti, $\mu(A)$ è denso in $\widehat{A}$ per la topologia indotta su $\widehat{A}$ dal prodotto diretto; mostriamo che tale topologia è la topologia $\mathbb{Z}$-adica di $\widehat{A}$, così, per il lemma 4.1.2, la divisibilità di $\widehat{A}/\mu(A)$ equivarrà alla densità di $\mu(A)$ in $\widehat{A}$, già nota.
Essendo gli A/nA limitati, e quindi discreti, una prebase di intorni di 0 per $\widehat{A}$ è costituita dagli $U_n = \pi_n^{\leftarrow}(0)$, con $\pi_n\colon \widehat{A} \to A/nA$ n-esima proiezione canonica; mostriamo $U_n = n\widehat{A}$. L'inclusione $n\widehat{A} \leq U_n$ segue banalmente dal fatto che $na_n + nA = nA$ è lo zero di A/nA. Mostriamo $n\widehat{A} \geq U_n$: sia $\widehat{a} = (\cdots a_m + mA \cdots) \in U_n$, cioè $a_n \in nA$, supponiamo $a_n = 0$. Per la proprietà del limite inverso, $a_j + A_i = a_i + A_i$ per ogni $i \leq j$, quindi per ogni m si ha $a_{(m+1)!n} - a_{m!n} \in m!nA$, cioè per ogni m esiste $c_m \in A$ tale che

$$a_{(m+1)!n} - a_{m!n} = m!nc_m.$$

Definiamo $b_1 = 0$, $b_{m+1} = b_m + m!c_m$ se $m > 1$. Allora si mostra per induzione che

$$a_{m!n} = nb_m$$

per ogni $m \geq 1$. Se $\widehat{b} = (\cdots b_m + m!A \cdots) \in \widehat{A}$, allora $n\widehat{b} = \widehat{a}$, quindi $U_n \leq n\widehat{A}$. □

4.1.7 Teorema (di struttura dei gruppi algebricamente compatti)**.** *A è un gruppo ridotto algebricamente compatto se e solo se*

$$A = \prod_p A_p$$

(con prodotto esteso a tutti i primi), con ogni A_p completo nella sua topologia p-adica e determinato univocamente da A.

Dimostrazione. Sia A algebricamente compatto ridotto; allora $C = A \oplus B$ con C prodotto diretto di p-gruppi ciclici (corollario 4.0.5). $C = \prod_p C_p$ dove indichiamo con C_p il prodotto diretto dei p-gruppi con lo stesso p. I C_p sono pienamente invarianti in C, quindi $C_p = (A \cap C_p) \oplus (B \cap C_p) =: A_p \oplus B_p$. Segue

$$C = \prod_p C_p = \prod_p (A_p \oplus B_p) = (\prod_p A_p) \oplus (\prod_p B_p)$$

Dotiamo C della topologia $\mathbb{Z}$-adica; siano poi $P = \prod_p A_p$, $S = \bigoplus_p A_p$. P/S è divisibile (infatti $n(P/S) = (nP + S)/S = P/S$ segue da $(nP + S) = P$, visto che se $n = p_1^{n_1} \cdots p_k^{n_k}$ allora nP differisce da P solo sulle componenti $A_{p_1}, \dots, A_{p_k}$, che sono in numero finito). Allora S è denso in $P \leq C$ (lemma 4.1.2), quindi $P \leq \overline{S}$ (chiusura in C). Si ha poi

$$(C/A)^1 \cong B^1 = \{0\}$$

per la proprietà di Hausdorff, e quindi (esempio 1.5.1) A è chiuso in C, da cui

$$P \leq \overline{S} \leq \overline{A} = A,$$

quindi $\prod_p A_p \leq A$. Analogamente $\prod_p B_p \leq B$, e quindi valgono le uguaglianze. Allora, per un generico primo q, si ha

$$A = \prod_p A_p \cong A_q \oplus (\prod_{p \neq q} A_p),$$

cioè A_q è addendo diretto di A, completo nella topologia $\mathbb{Z}$-adica essendo ridotto algebricamente compatto, quindi A_q è completo nella sua topologia $\mathbb{Z}$-adica, che coincide con la sua topologia q-adica, essendo A_q un q-gruppo.

Viceversa, sia A_p completo nella sua topologia p-adica. Indichiamo con J_p l'anello degli interi p-adici (descritto nell'esempio 1.6.5). Consideriamo A_p come modulo su J_p: se $a \in A_p$, $\pi = s_0 + \cdots + s_n p^n + \cdots \in J_p$, allora la successione

$$s_0 a \qquad (s_0 + s_1 p)a \qquad \cdots \qquad (s_0 + s_1 p + \cdots + s_n p^n)a \qquad \cdots$$

è di Cauchy in A_p, quindi per completezza ha limite, che denotiamo con $\pi a \in A_p$. In questo modo A_p è un J_p-modulo unitario, da cui concludiamo che $qA_p = A_p$ per ogni primo $q \neq p$, e quindi la topologia $\mathbb{Z}$-adica di A_p coincide con la sua topologia p-adica. Allora A_p è completo nella sua topologia $\mathbb{Z}$-adica e quindi ridotto algebricamente compatto (teorema 4.1.1); si conclude che $\prod_p A_p$ lo è (corollario 4.0.4).

Infine, essendo $qA_p = A_p$ per ogni primo $q \neq p$ e $\bigcap_{k>0} p^k A_p = \{0\}$, si ha $A_p = \bigcap_{q \neq p} q^k$ per ogni $k > 0$, da cui l'unicità delle componenti A_p. $\square$

Bibliografia

[1] László Fuchs, *Infinite Abelian Groups, Volume 1*. Elsevier, 1970.

[2] Derek J. S. Robinson, *A Course in the Theory of Groups*. Springer, 1996.

[3] A. G. Kurosh, *The Theory of Groups*. AMS Chelsea Publishing, 1955.

[4] *Exercises in Abelian Group Theory*. Springer, 2003.