Topologia 2
(Appendice)
vers. 24.3.2009

Gruppi Infiniti

Dikran Dikranjan

March 24, 2009

1 Introduzione

Lo scopo di questi appunti è di dare un primo approccio ai gruppi infiniti (prevalentemente abeliani) presentando brevemente alcuni classi importanti di gruppi abeliani infiniti. Cominciamo con alcuni prerequisiti sugli inisemi ed i numeri cardinali. Nel §2 sono definiti le somme dirette ed i prodotti diretti, i limiti diretti ed i limiti inversi. Nel §3 dedicheremo l'attenzione agli spazi vettoriali, dimostrando che base e dimensioni di possono definire in ogni spazio vettoriale e la dimensione di uno spazio vettoriale lo determina a meno di isomorfismo. Nel §4 vengono definiti i gruppi abeliani liberi che hanno molte proprietà in commune con gli spazi vettoriali. Tramite i gruppi liberi si introduce il rango libero di un gruppo abeliano. Nel §5 sono stati descritti i gruppi finitamente generati (sono somme dirette finite di gruppi ciclici). I gruppi divisibili, presentati come controparte omologica dei i gruppi liberi, sono studiati nel §7. Riusciremo a dare una classificazione dei gruppi divisibili a meno di isomorfismo tramite il rango libero ed una serie di invarianti cardinali dei gruppi abeliani – i p-ranghi, definiti per ogni numero primo p. L'ultimo capitolo contiene un esempio di gruppi indecomponibili.

Contents

1 Introduzione **1**
1.1 Prerequisiti sugli insiemi . . . 2

2 Somme dirette e prodotti diretti **2**
2.1 Addendi diretti . . . 3
2.2 Limiti diretti e limiti inversi . . . 4
2.3 Prodotto tensoriale di gruppi abeliani . . . 5
2.4 Sottogruppi funtoriali dei gruppi abeliani . . . 5

3 La struttura degli spazi vettoriali **6**
3.1 Dimensione di uno spazio vettoriale . . . 7
3.2 Moduli . . . 8

4 Rango libero di un gruppo abeliano **8**
4.1 Gruppi liberi abeliani . . . 8

5 Gruppi abeliani finitamente generati **10**

6 Il p-rango **11**
6.1 Zoccolo di un gruppo abeliano . . . 11
6.2 Gruppi abeliani di esponente finito . . . 12
6.3 Sottogruppi essenziali . . . 12

7 Gruppi divisibili **13**
7.1 Struttura dei gruppi abeliani divisibili . . . 14

8 Epilogo **14**
8.1 Gruppi indecomponibili . . . 14
8.2 L'anello di endomorfismi di un gruppo abeliano . . . 14
8.3 I numeri p-adici . . . 16

1.1 Prerequisiti sugli insiemi

Nel seguito denotiamo con $\mathbb{P}$ l'insieme dei numeri primi.

Sia $\{X_i\}_{i\in I}$ una famiglia arbitraria di insiemi non-vuoti. Il *prodotto cartesiano* di questa famiglia è l'insieme X avente come elementi le funzioni di scelta $f : I \to \bigcup_{i\in I} X_i$, con $f(i) \in X_i$ per ogni $i \in I$ [1]. Per gli elementi $f, g \in X$ scriveremo anche brevemente f_i e g_i invece di $f(i)$ e $g(i)$ e allora scriveremo (f_i) per la funzione f. Per ogni $i \in I$ si definisce la proiezione $p_i : \prod_{i\in I} X_i \to X_i$ ponendo $p_i(f) = f_i$.

Se I è finito, diciamo $I = \{1, 2, \ldots, n\}$, scriveremo anche $X_1 \times \ldots \times X_n$ invece di $\prod_{i\in I} X_i$ o $\prod_{i=1}^n X_i$.

Per un insieme X denoteremo, come sempre, con $|X|$ la cardinalità di X, con $P(X)$ l'insieme delle parti di X e con $P_f(X)$ l'insieme delle parti finite di X. Scriviamo:

- $|X| = |Y|$, se esiste una biezione $X \to Y$ (e diciamo che X e Y sono equipotenti);
- $|X| \leq |Y|$ (o anche $|Y| \geq |X|$), se esiste una iniezione $X \to Y$ (o, equivalentemente, se esiste una suriezione $X \to Y$);
- $|X| < |Y|$ (o anche $|Y| > |X|$), se vale $X \leq Y$, ma non vale $|X| = |Y|$.

Si pone $|P(X)| = 2^{|X|}$, per il teorema di Cantor si ha $2^{|X|} > |X|$. Vediamo nel seguito che per X infinito $P_f(X)$ e X sono equipotenti (Teorema 1.4)s.

Teorema 1.1. [4, Teor. 1.78 e 1.79] *Se X e Y sono insiemi di cui almeno uno infinito, allora*

$$|X \cup Y| = |X \times Y| = \max\{|X|, |Y|\}.$$

Corollario 1.2. *$|X \times \mathbb{N}| = |X|$ per ogni insieme infinito X.*

Corollario 1.3. *Per una famiglia di insiemi $\{X_n\}_{n\in\mathbb{N}}$ tali che l'insieme X_0 è infinito e $|X_n| \leq |X_0|$ per ogni $n \in \mathbb{N}$, si ha $|\bigcup_{n\in\mathbb{N}} X_n| \leq |X_0|$.*

Dimostrazione. Basta notare che esiste una suriezione $X \times \mathbb{N} \to \bigcup_{n\in\mathbb{N}} X_n$ e applicare il corollario precedente. QED

Teorema 1.4. *$|P_f(X)| = |X|$ per ogni insieme infinito X.*

Dimostrazione. Per ogni $n \in \mathbb{N}$ positivo denotimo con $[X]^n$ l'insieme $\{A \in P_f(X) : |A| = n\}$. Chiaramente,

$$P_f(X) = \bigcup_{n\in\mathbb{N}} [X]^n \tag{1}$$

e $[X]^1$ si può identificare con X, quindi esiste una iniezione $X \to P_f(X)$. Pertanto $|X| \leq |P_f(X)|$. Per verificare la disuguaglianza $|X| \geq |P_f(X)|$ basta applicare (1) e il corollario precedente. A questo scopo dobbiamo verificare che $|[X]^n| \leq |X|$ per ogni $n > 0$. Poichè esiste una suriezione $X^n \to [X]^n$, abbiamo $|[X]^n| \leq |X^n|$. Per concludere, notiamo che $|[X]^n| = |X|$ per il Teorema 1.1. QED

2 Somme dirette e prodotti diretti

Cominciamo richiamando i prodotti diretti e le somme dirette.

Sia $\{G_i\}_{i\in I}$ una famiglia arbitraria di gruppi. Il *prodotto diretto* di questa famiglia è il gruppo avente come supporto il prodotto cartesiano $G = \prod_{i\in I} G_i$ e prodotto definito con $(f \cdot g)_i = f_i \cdot g_i$; l'elemento neutro di G è $e = (e_i)$, dove e_i è l'elemento neutro di G_i. Per ogni $i \in I$ la proiezione $p_i : \prod_{i\in I} G_i \to G_i$ è un omomorfismo.

Teorema 2.1. *Sia G un gruppo e siano N_i, $i = 1, 2, \ldots, n$ sottogruppi normali di G. Allora vale $G \cong \prod_{i\in 1}^n N_i$ se e solo se $G = N_1 N_2 \ldots N_n$ e $N_i \cap N_1 N_2 \ldots N_{i-1} N_{i+1} \ldots N_n = \{e\}$ for ogni $i = 1, 2, \ldots, n$.*

Dimostrazione. Il caso $n = 1$ è banale, il caso $n = 2$ è noto dal corso di Algebra. Per $n > 2$ la dimostrazione procede per induzione, usando il caso $n = 2$. QED

Sia H un gruppo e sia $\{G_i\}_{i\in I}$ una famiglia arbitraria di gruppi. Per un omomorfismo $h : H \to \prod_{i\in I} G_i$ la composizione $h_i = p_i \circ h$ è un omomorfismo $h_i : H \to G_i$ per ogni $i \in I$. Viceversa, per ogni famiglia di omomorfimi $h_i : H \to G_i$, $i \in I$, esiste un unico omomorfismo $h : H \to \prod_{i\in I} G_i$ tale che $p_i \circ h = h_i$ per ogni $i \in I$, che chiameremo l'*omomorfismo diagonale* degli h_i (ovviamente, basta porre $h(x) = (h_i(x)) \in \prod_{i\in I} G_i$ for $x \in H$).

Nel caso in cui I sia infinito introduciamo anche la *somma diretta* definita come segue: per una funzione $g = (g_i) \in \prod_{i\in I} G_i$ sia $supp(g) = \{i \in I : g_i \neq e_i\}$. Denotiamo con $\bigoplus_{i\in I} G_i$ l'insieme $\{g \in \prod_{i\in I} G_i : |supp(g)| < \infty\}$. È facile vedere che $\bigoplus_{i\in I} G_i$ è un sottogruppo normale del prodotto diretto $\prod_{i\in I} G_i$, che chiameremo *somma diretta* della famiglia $\{G_i\}_{i\in I}$. Questa terminologia sarà adottata esclusivamente nel caso abeliano.

[1] Il prodotto cartesiano non è vuoto grazie all'assioma di scelta.

Teorema 2.2. *Sia G un gruppo e sia $\{N_i : i \in I\}$ una famiglia di sottogruppi normali di G. Allora vale $G \cong \bigoplus_{i\in I} N_i$ se e solo se G coincide con il sottogruppo generato dalla famiglia $\{N_i : i \in I\}$ e per ogni sottoinsieme finito $\{i_0, i_1, i_2, \dots, i_n\}$ di I vale $N_{i_0} \cap N_{i_1} N_{i_2} \dots N_{i_n} = \{e\}$.*

Quando tutti i gruppi G_i coincidono con lo stesso gruppo G_0 scriveremo al posto di $\prod_I G_0$ anche G_0^I, e al posto di $\bigoplus_I G_0$ anche $G_0^{(I)}$. È facile vedere (Esercizio 2.4) che se I e J sono insiemi equipotenti, allora $G_0^I \cong G_0^J$ e $G_0^{(I)} \cong G_0^{(J)}$. Questo ci suggerisce di usare, posto $\alpha = |I|$, anche la notazione G_0^α per G_0^I, e la notazione $G_0^{(\alpha)}$ oppure $\bigoplus_\alpha G_0$ al posto di $G_0^{(I)}$, quando l'insieme degli indici I non è rilevante. L'importanza delle somme dirette di questo tipo particolare si vede meglio nel paragrafo successivo.

Lemma 2.3. *Sia $\{G_i\}_{i\in I}$ una famiglia di gruppi e sia N_i un sottogruppo normale di G_i per ogni $i \in I$. Allora:*

(a) $N = \prod_{i\in I} N_i$ è un sottogruppo normale di $G = \prod_{i\in I} G_i$ e $G/N \cong \prod_{i\in I} G_i/N_i$;

(b) $\bigoplus_{i\in I} N_i$ è un sottogruppo normale di $\bigoplus_{i\in I} G_i$ e $(\bigoplus_{i\in I} G_i)/(\bigoplus_{i\in I} N_i) \cong \bigoplus_{i\in I} G_i/N_i$.

Dimostrazione. (a) Per $i \in I$ sia $\phi_i : G_i \to G_i/N_i$ l'omomorfismo canonico e sia $h_i = \phi_i \circ p_i : G \to G_i/N_i$. Allora l'omomorfismo diagonale $h : G \to \prod_{i\in I} G_i/N_i$ ha nucleo N, quindi l'isomorfismo desiderato segue dal primo torema dell'omomorfismo.

(b) Segue da (a) e dall'uguaglianza $N \cap \bigoplus_{i\in I} G_i = \bigoplus_{i\in I} N_i$. QED

Esercizio 2.4. *Siano $\{G_i\}_{i\in I}$ e $\{H_j\}_{j\in J}$ due famiglie di gruppi tali che esiste una biezione $\xi : I \to J$ con $G_i \cong H_{\xi(i)}$ per ogni $i \in I$. Allora $\prod_{i\in I} G_i \cong \prod_{j\in J} H_j$.*

Esercizio 2.5. *Sia K un sottogruppo del prodotto diretto $G\times H$ che contiene il sottogruppo G. Allora $K = G\times(K\cap H)$.*

Esercizio 2.6. *Sia G_0 un gruppo e sia I in insieme. Allora per $G = \bigoplus_I G_0$ si ha:*

(a) $|G| = |G_0|^{|I|}$, quando G_0 e I sono finiti;

(b) $|G| = |G_0|$, quando G_0 è infinito e I è al più numerabile;

(c) $|G| = |I|$, quando I è infinito e G_0 è al più numerabile;

(d) $|G| = \max\{|G_0|, |I|\}$, quando almeno uno tra G_0 e I è infinito.

2.1 Addendi diretti

Un sottogruppo H di un gruppo G si dice *addendo diretto*, se esiste un altro sottogruppo K di G tale che $G \cong H \times K = H \oplus K$. Nel seguito daremo delle condizioni che assicurano che un dato sottogruppo H è un addendo diretto.

Definizione 2.7. Per un omorfismo $q : G_1 \to G_2$:

(a) un omomorfismo $s : G_2 \to G_1$ si dice *sezione*, se $q \circ s = id_{G_2}$.

(b) un omomorfismo $r : G_2 \to G_1$ si dice *retrazione*, se $r \circ q = id_{G_1}$.

Chiaramente,

(i) se esiste una sezione $s : G_2 \to G_1$, allora q è suriettivo (essendo $q \circ s = id_{G_2}$ surriettivo);

(ii) se esiste una retrazione $r : G_2 \to G_1$, allora q è iniettivo (essendo $r \circ q = id_{G_1}$ iniettivo).

Teorema 2.8. *Per un sottogruppo di un gruppo abeliano le seguenti condizioni sono equivalenti:*

(a) H è un addendo diretto di G;

(b) l'omomorfismo canonico $q : G \to G/H$ possiede una sezione s;

(c) l'inclusione $j : H \to G$ possiede una retrazione r.

Nel caso (b) risulta $G \cong H \times Im\, s$, nel caso (c) risulta $G \cong H \times Im\, r$.

DIMOSTRAZIONE.
QED

Per un gruppo abeliano G e suo sottogruppo H consideriamo spesso l'omomorfismo inclusione $j : H \to G$ e l'omomorfismo canonico $q : G \to G/H$. Sappiamo che j è iniettiva, mentre q è suriettiva. Inoltre, $\operatorname{Im} j = \ker q$. In generale, una sequenza di omomorfismi $G_1 \xrightarrow{j} G \xrightarrow{q} G_2$ si dice *esatta*, se $\operatorname{Im} j = \ker q$. Chiaramente, $0 \to G \xrightarrow{j} G_2$ è esatta se e solo se j è iniettiva, mentre $G_1 \xrightarrow{q} G \to 0$ è esatta se e solo se q è suriettiva.

Una sequenza di omomorfismi

$$0 \to G_1 \xrightarrow{j} G \xrightarrow{q} G_2 \to 0 \tag{1}$$

si dice *esatta corta*, se le sequenze $0 \to G_1 \xrightarrow{j} G$, $G_1 \xrightarrow{f} G \xrightarrow{h} G_2$ e $G \xrightarrow{q} G_2 \to 0$ sono esatte (ovvero $\operatorname{Im} j = \ker q$, j è iniettiva e q è suriettiva). Diciamo che la (1) ammette una sezione, se q ammette una sezione $s : G/H \to G$. Per il teorema 2.8, vale $G \cong H \times \operatorname{Im} s$ in tal caso, e si dice che la successione (1) *si spezza*. .

Vogliamo capire meglio le successioni che si spezzano. Ogni somma diretta (prodotto diretto) $G = G_1 \times G_2$ dà luogo a due successioni esatte corte

$$0 \to G_1 \xrightarrow{j_i} G \xrightarrow{p_2} G_2 \to 0 \quad \text{e} \quad 0 \to G_2 \xrightarrow{j_2} G \xrightarrow{p_1} G_1 \to 0, \tag{2}$$

dove p_i $(i = 1, 2)$ sono le proiezioni, mentre j_i sono le canoniche immersioni $j_i : G_i \to G$. Per le composizioni tra questi omomorfismi valgono le sequenti relazioni

$$p_2 \circ j_1 = 0, \quad p_1 \circ j_2 = 0, \quad p_i \circ j_i = id_{G_i}, \ \ i = 1, 2. \tag{$*$}$$

Chiaramente, (*) implica che j_i è una sezione per p_i.

2.2 Limiti diretti e limiti inversi

Adesso vediamo un esempio importante. Sia G un gruppo abeliano e sia p un numero primo. Denoteremo con $t_p(G)$ il sottogruppo di G degli elementi p-periodici. Denoteremo con $t(G)$ il sottogruppo degli elementi periodici di G.

Lemma 2.9. *Per ogni gruppo abeliano G si ha $t(G) = \bigoplus_{p \in \mathbb{P}} t_p(G)$.*

DIMOSTRAZIONE. Basta notare che per ogni insieme $\{p_0, p_1, \ldots, p_n\}$ di numeri primi si ha $t_{p_0}(G) \cap \bigoplus_{i=1}^{n} t_{p_i}(G) = 0$ e applicare Teorema 2.2. QED

Esempio 2.10. Sia p un numero primo. Il sottogruppo $t_p(\mathbb{Q}/\mathbb{Z})$ chiameremo gruppo di Prüfer e denoteremo con $\mathbb{Z}(p^\infty)$. Denotando $c_n = \frac{1}{p^n}$ per ogni $n > 0$, è facile notare che

(a) $pc_n = c_{n-1}$ per tutti $n > 1$ e $pc_1 = 0$;

(b) l'insieme $\{c_n : n > 0\}$ genera $\mathbb{Z}(p^\infty)$;

(c) ogni sottogruppo proprio di $\mathbb{Z}(p^\infty)$ ha la forma $\langle c_n \rangle \cong \mathbb{Z}_{p^n}$.

(d) $\mathbb{Q}/\mathbb{Z} \cong \bigoplus_p \mathbb{Z}(p^\infty)$ (segue immediatamente dal Lemma 2.9).

Questo esempio ci suggerisce di definire una costruzione simile per ogni famiglia $\{G_n : n > 0\}$ di gruppi e ogni famiglia $i_n : G_n \to G_{n+1}$ $(n > 0)$ di omomorfismi iniettivi. Senza ledere la generalità identificheremo ogni gruppo G_n con il sottogruppo $i_n(G_n)$ di G_{n+1}, identificando poi G_{n-1} con il sottogruppo $i_n(i_{n-1}(G_{n-1}))$ di G_{n+1}, ecc. In questo modo si ha una catena di sottogruppi

$$G_1 \leq G_2 \leq \ldots \leq G_n \leq \ldots$$

L'unione $G = \bigcup_{n=1}^{\infty} G_n$ acquista una struttura naturale di gruppo, definendo per $x \in G_n$ e $y \in G_m$ il prodotto xy nel gruppo G_k, dove $k = \max\{n, m\}$. Chiameremo G *limite diretto* della famiglia $\{G_n : n > 0\}$ e lo denoteremo con $G = \varinjlim G_n$ (o con $G = \varinjlim (G_n, i_n)$, quando sarà necessario indicare esplicitamente anche la famiglia degli omomorfismi i_n).

Esercizio 2.11. *(a) Per ogni $n > 0$ sia $i_n : \mathbb{Z} \to \mathbb{Z}$ l'omomorfismo definito con $i_n(x) = nx$. Provare che $\varinjlim (G_n, i_n) \cong \mathbb{Q}$, dove $G_n = \mathbb{Z}$ per ogni n.*

(b) Sia p un numero primo e sia $i_n : \mathbb{Z} \to \mathbb{Z}$ l'omomorfismo definito con $i_n(x) = px$ per ogni $n > 0$. Provare che $\varinjlim (G_n, i_n)$, dove $G_n = \mathbb{Z}$ per ogni n, coincide con il sottogruppo $\mathbb{Q}_p$ di $\mathbb{Q}$ delle frazioni del tipo $\frac{a}{p^n}$, $a, n \in \mathbb{Z}$, e $\mathbb{Q}_p/\mathbb{Z} \cong \mathbb{Z}(p^\infty)$.

Sia $\{G_n : n > 0\}$ una famiglia di gruppi e sia $f_n : G_{n+1} \to G_n$ $(n > 0)$ una famiglia di omomorfismi. Sia $\varprojlim G_n$ il sottogruppo del prodotto diretto $G = \prod_n G_n$ che consiste di tutti gli elementi $x = (x_n) \in G$ tali che

$$x_n = f_n(x_{n+1}) \text{ (cioè, } p_n \circ f_n(x) = p_{n+1}(x)) \text{ per ogni } n > 0.$$

Chiameremo $\varprojlim G_n$ *limito inverso* della famiglia $\{G_n : n > 0\}$ e lo denoteremo anche con $G = \varprojlim (G_n, f_n)$, quando sarà necessario indicare esplicitamente anche la famiglia degli omomorfismi f_n.

Osservazione 2.12. In generale i limiti diretti ed i limiti inversi vengono definiti in modo più generale che vogliamo solo accennare qui, ma non sarà usato nel seguito. Un insieme parzialmente ordinato $(I, \leq)$ di dice *diretto a destra*, se per ogni coppia $i, j \in I$ esiste un $k \in I$ con $i \leq k$ e $j \leq k$.

(a) Un *sistema diretto* indiciato con $(I, \leq)$ è una famiglia di gruppi $\{G_i : i \in I\}$ e omomorfismi $\nu_{ij} : G_i \to G_j$ per ogni coppia $i \leq j$ in I tali che per ogni terna di indici $i \leq j \leq k$ vale $\nu_{jk} \circ \nu_{ij} = \nu_{ik}$. Adesso il limite diretto $G = \varinjlim (G_i, \nu_{ij})$ di questo sistema diretto è il quoziente del gruppo $\bigoplus_{i \in I} G_i$ rispetto al sottogruppo generato da tutte le differenze $x - \nu_{ij}(x)$ al variare $i \leq j$ in I e $x \in G_i$ (qui, come al solito identifichiamo i gruppi G_i con sottogruppi di $\bigoplus_{i \in I} G_i$ nel modo ovvio).

(b) Un *sistema inverso* indiciato con $(I, \leq)$ è una famiglia di gruppi $\{G_i : i \in I\}$ e omomorfismi $\nu_{ij} : G_j \to G_i$ per ogni coppia $i \leq j$ in I tali che per ogni terna di indici $i \leq j \leq k$ vale $\nu_{ij} \circ \nu_{jk} = \nu_{ik}$. Adesso il limite inverso $G = \varprojlim (G_i, \nu_{ij})$ di questo sistema diretto è il sottogruppo del gruppo $G = \prod_{i \in I} G_i$ che consiste di tutti gli elementi $x = (x_i) \in G$ tali che $\nu_{ij}(x_j) = x_i$ al variare $i \leq j$ in I.

2.3 Prodotto tensoriale di gruppi abeliani

Siano G e H due gruppi abeliani, vogliamo definire uno nuovo gruppo abeliano $G \otimes H$, detto *prodotto tensoriale* di G e H, in modo tale che

a) esiste un'applicazione bilineare $t : G \times H \to G \otimes H$ tale che $G \otimes H$ generato dall'insieme $\{t(u, v) : u \in G,\ v \in H\}$;

b) se $f : G \times H \to K$ un'applicazione bilineare allora esiste un'unico omomorfismo $\bar{f} : G \otimes H \to K$ tale che $f = \bar{f} \circ t$.

Solitamente $t(u, v)$ si denota con $u \otimes v$. Allora la propietà (a) si può esprimere più dettagliatamente nel modo seguente:

$$(u_1 + u_2) \otimes v = u_1 \otimes v + v_2 \otimes v$$

$$u \otimes (v_1 + v_2) = u \otimes v_1 + u \otimes v_2$$

$$n(u \otimes v) = (nu) \otimes v = u \otimes (nv)$$

con $u_i \in U$, $v_j \in V$, $n \in \mathbb{Z}$.

Se $u_1, \ldots, u_n$ e $v_1, \ldots, v_m$ sono generatori di G e H rispettivamente, allora si vede facilmente che

$$u_1 \otimes v_1, \ldots, u_1 \otimes v_m,\ u_2 \otimes v_1, \ldots, u_2 \otimes v_m, \ldots, u_n \otimes v_1, \ldots, u_n \otimes v_m$$

generano il prodotto tensoriale $U \otimes_F V$ di U e V.

Diamo adesso degli esempi di prodotti tensoriali di gruppi abeliani.

Esempio 2.13. (a) $G \otimes \mathbb{Z} \cong G \cong \mathbb{Z} \otimes G$;

(b) se G è di esponente n e H è di esponente m, con m, n coprimi, allora $G \otimes H \cong 0$.

(c) se G è di torsione, allora $G \otimes \mathbb{Q} \cong 0$;

(d) se G è senza torsione, allora $V = G \otimes \mathbb{Q}$ è spazio vettoriale su $\mathbb{Q}$ e $\dim_{\mathbb{Q}} V = r_0(G)$.

2.4 Sottogruppi funtoriali dei gruppi abeliani

Definizione 2.14. Pensiamo di aver assegnato un sottogruppo $\rho(G)$ ad ogni gruppo abeliano. Si dice che $\rho(G)$ è un *sottogruppo funtoriale*, se per ogni omomorfismo $f : G \to H$ tra due gruppi abeliani vale $f(\rho(G)) \subseteq \rho(H)$.

Esempio 2.15. Sia G un gruppo abeliano G.

(a) Per ogni intero m poniamo $mG = \{mx : x \in G\}$. Allora mG è un sottogruppo funtoriale.

(b) Per ogni intero m poniamo $G[m] = \{mx : x \in G\}$. Allora $G[m]$ è un sottogruppo funtoriale.

(c) $t(G)$ è un sottogruppo funtoriale.

(c) $t_p(G)$ è un sottogruppo funtoriale per ogni primo p.

Esercizio 2.16. *Provare che* $t(G) = \bigcup_n G[n!]$.

Esercizio 2.17. *Provare che* $mG = G/G[m]$.

3 La struttura degli spazi vettoriali

Nel seguito K sarà un campo arbitrario. Studieremo spazi vettoriali su K come esempio di struttura algebrica pienamante classificabile a meno di isomorfismo tramite un solo invariante cardinale – la *dimensione* dello spazio.

Ricordiamo che uno spazio vettoriale V su K è un gruppo abeliano $(V, +)$ munito di una "motliplcazione con scalari di K", ovvero un'applicazione $K \times V \to V$, per la quale denoteremo con λv il prodotto dello scalare $\lambda \in K$ e il vettore $v \in V$, soggetto alle seguenti quattro assiomi per $\lambda, \mu \in K$ ed i vettori $u, v \in V$:

(a) $\lambda(u + v) = \lambda u + \lambda v$;

(b) $(\lambda + \mu)u = \lambda u + \mu u$;

(c) $\lambda(\mu u) = (\lambda u \mu)u$;

(d) $1.u = u$.

Se U, V sono spazi vettoriali, un omomorfismo di spazi vettoriali $f : U \to V$ è un omomorfismo dei gruppi abeliani $(U, +)$ e $(V, +)$ tale che $f(\lambda v) = \lambda f(v)$ per ogni $\lambda \in K$.

Per una famiglia $\{V_i : i \in I\}$ di spazi vettoriali il prodotto diretto $V = \prod_{i\in I} V_i$ dei gruppi $(V_i, +)$ ammette anche una struttura naturale di spazio vettoriale (per $f = (f_i) \in V$ e $r \in K$ si pone $rf = (rf_i)$). Nello stesso modo come per il prodotto diretto, anche la somma diretta $\bigoplus_{i\in I} V_i$ risulta spazio vettoriale, infatti sottospazio del prodotto V. Prendendo tutti gli $V_i = K$, ricaviamo lo spazio $\bigoplus_I K$. Come detto in precedenza, questo spazio dipende solo dalla cardinalità dell'insieme I, e pertanto sarà denotato anche con $\bigoplus_\alpha K$, dove $\alpha = |I|$. Vedremo nel seguito che a meno di isomorfismo, ogni spazio vettoriale ha questa forma per opportuno numero cardinale α. Nel caso di $\alpha = n$ finito, questo spazio coincide con il prodotto diretto K^n. In questo caso lo spazio si dice di avere dimensione n e può essere generato da n vettori linearmente indipendenti che formano una base dello spazio.

Vedremo nel seguito che anche gli spazi vettoriali che non sono finitamente generati permettono di introdurre i concetti di dimensione e base, ma adesso questi sono infiniti.

Sia V uno spazio lineare sul campo K. Un sottoinsieme M di V si dice *indipendente* se ogni sottoinsieme finito $b_1, \dots, b_s$ di M è linearmente indipendente. Diremo che M è *massimale* se non è contenuto propriamente in alcun sottoinsieme indipendente di V.

Esempio 3.1. (a) Per ogni vettore $v \neq 0$ in V, il singoletto $\{v\}$ è un sottoinsieme indipendente di V.

(b) Sia B un sottoinsieme indipendente di V. Allora per ogni spazio vettoriale U e per ogni applicazione $l : B \to U$ esiste un unico omomorfismo $\tilde{l} : W \to U$ che estende l, dove W è il sottospazio di V generato da B. Infatti, per ogni $v \in W$ esiste un insieme finito $b_1, \dots, b_n \in B$ e scalari $\lambda_1, \dots, \lambda_n$ tali che $v = \sum_{i=1}^n \lambda_i b_i$. Inoltre, $b_1, \dots, b_n \in B$ e gli scalari $\lambda_1, \dots, \lambda_n$ sono univocamente determinati da v. Poniamo $\tilde{l}(v) = \sum_{i=1}^n \lambda_i v(b_i)$. Si verifica immediatamente che $\tilde{l}$ è l'omomorfismo desiderato.

Lemma 3.2. *Sia M un sottoinsieme indipendente di V. Allora M è massimale se e solo se genera V come sottospazio vettoriale.*

Dimostrazione. Se M genera V come sottospazio vettoriale, allora per ogni vettore $v \in V \setminus M$ esistono degli scalari $k_i \in K$ e $b_i \in M$ con $v = \sum_i k_i b_i$. QED

Un sottoinsieme indipendente massimale di V sarà chiamato *base di Hamel*, o semplicemente *base*. Nel seguente teorema dimostriamo che ogni spazio vettoriale possiede una base.

Teorema 3.1. *Ogni sottoinsieme indipendente di V è contenuto in un sottoinsieme indipendente massimale.*

Dimostrazione. Sia I_0 in insieme indipendente di V e sia $\mathcal{I}$ la famiglia degli sottoinsiemi indipendenti di G contenenti I_0. Essa non è vuota essendo $I_0 \in \mathcal{I}$. Ordiniamo $\mathcal{I}$ rispetto all'inclusione $\subseteq$. Applicando il lemma di Zorn all'insieme ordinato $(\mathcal{I}, \subseteq)$ troviamo un sottoinsieme indipendente massimale contenente I_0. QED

Dimostreremo adesso un corollario importante del teorema.

Corollario 3.3. *Sia $f : U \to V$ un'omomorfismo di spazi vettoriali:*

(a) se $q : W \to V$ è un omomorfismo suriettivo di spazi vettoriali, allora esiste un omomorfismo di spazi vettoriali $\tilde{f} : U \to W$ tale che $q \circ \tilde{f} = f$;

(a) se $j : U \to W$ è un omomorfismo iniettivo di spazi vettoriali, allora esiste un omomorfismo di spazi vettoriali $\bar{f} : W \to V$ tale che $\bar{f} \circ j = f$.

DIMOSTRAZIONE. (a) Sia B una base di U. Per le surrietività di q esiste un'applicazione $h : f(B) \to W$ tale che $(q \circ h \circ f)(b) = f(b)$ per ogni $b \in B$. Per l'Esempio 3.1(b) esiste un omomorfismo $\bar{f}$ che estende $h \circ f : B \to W$.

(b) Usando il teorema 3.1 possiamo scegliere una base B di W tale che $B_0 = B \cap j(U)$ è una base di $j(U)$. Defininiamo $h : B \to V$ ponendo $h(j(b)) = f(b)$ per tutti $b \in B_0$ e $h(b) = 0$ per tutti $b \in B \setminus j(B_0) = B \setminus j(U)$. Per l'esempio 3.1 (b) esiste un omomorfismo $\bar{h} : W \to V$ che estendo h, e naturalmente anche f. QED

Corollario 3.4. *Ogni sottospazio di uno spazio vettoriale è un adendo diretto.*

3.1 Dimensione di uno spazio vettoriale

Per definire la dimensione abbiamo bisogno del seguente

Lemma 3.5. *Siano B e B_1 due basi di Hamel dello spazio vettoriale V. Allora $|B| = |B_1|$.*

DIMOSTRAZIONE. Notiamo adesso che per ogni $b \in B$ esiste un insieme finito $F_b \subseteq B_1$ tale che $b \in \langle F_b \rangle$ – il sottospazio generato da F_b. Poichè B è indipendente, per un dato $F \in P_f(B_1)$ esistono al più un numero finito di elemeni $b \in B$ tale che $F = F_b$. Denotiamo con $h : B \to P_f(B_1)$ l'applicazione $b \mapsto F_b$ così definita. Allora la sua immagine $h(B)$ è equipotente a B (essendo tutti $h^{-1}(F)$ finiti). Quindi $|B| \leq |P_f(B_1)| = |B_1|$. Abbiamo così dimostrato che $|B| \leq |B_1|$. Nello stesso modo si dimostra che $|B_1| \leq |B|$. QED

Definiamo adesso la *dimensione* $\dim_K V$ come la cardinalità di qualsiasi base di Hamel di V su K.

Nel seguente teorema dimostriamo che la dimensione di uno spazio vettoriale lo determina a meno di isomorfismo.

Teorema 3.6. *(1) Sia α un numero cardinale. Allora* $\dim K^{(\alpha)} = \alpha$.

(2) Sia V uno spazio vettoriale sul campo K di dimensione α. Allora $V \cong \bigoplus_\alpha K$.

DIMOSTRAZIONE. (1) Fissiamo un insieme di indici I con $|I| = \alpha$. Allora $K^{(\alpha)} = \bigoplus_I K$. Sia b_i un vettore non-nullo nella i-esima copia di K in $\bigoplus_I K$, cioè $\bigoplus_I K = \bigoplus_{i \in I} K \cdot b_i$, dove $K \cdot b_i$ è la retta generata da b_i. Allora $B = \{b_i : i \in I\}$ è una base $\bigoplus_{i \in I} K$ di cardinalità α. Quindi, $\dim \bigoplus_{i \in I} K = \alpha$.

(2) Sia B una base di V di cardinalità α. Allora $V \cong \bigoplus_B K \cong \bigoplus_\alpha K$, con isomorfismo $f : V \to \bigoplus_B K$ definito tramite $f(v) = \sum_i k_i f(b_i)$ qualora $v = \sum_i k_i b_i$, con $k_i \in K$. QED

Il seguente corollario ci fa vedere che gli spazi vettoriali ubbidiscono la stessa "legge di dichotomia" come gli insiemi.

Corollario 3.7. *Siano U e V spazi vettoriali, allora V è isomorfo a qualche sottospazio di U, oppure U è isomorfo a qualche sottospazio di V.*

A volte è più facile calcolare la cardinalità di uno spazio vettoriale che la sua dimensione. A questo scopo daremo l'espressione della cardinalità tramite la dimensione. Ovviamente, per ogni spazio vettoriale V vale sempre $|V| \geq \dim V$, visto che $\dim B = |B| \leq |V|$, dove B è una base di V. Nel caso di dimensione finita la cardialità si calcola facilmente con $|K^n| = |K|^n$, ma da questa formula è possibile ricavare n conoscendo $|K|$ solamente quando K è finito. Nel case di spazi vettoriali infiniti (e in particolare, campo K infinito), si ha $|V| = |K| \cdot \dim V$, come si vede nell'esercizio seguente:

Esercizio 3.8. *Sia V uno spazio vettoriale su K di dimensione infinita. Dimostrare che* $|V| = \max\{\dim V, |K|\}$. *In particolare, per K numerabile si ha* $\dim V = |V|$.

Esercizio 3.9. *(1) Calcolare le dimensioni* $\dim_{\mathbb{Q}} \mathbb{R}$, $\dim_{\mathbb{Q}} \mathbb{C}$, $\dim_{\mathbb{Q}} \bar{\mathbb{Q}}$ *e* $\dim_{\bar{\mathbb{Q}}} \mathbb{C}$, *dove $\bar{\mathbb{Q}}$ è la chiusura algebrica di $\mathbb{Q}$.*

(2) Sia K un campo.

(2a) Calcolare la dimensione di $K[x]$ su K.

(2b) Sia V uno spazio vettriale sul campo K e sia V^* la spazio delle funzioni lineari $f : V \to K$. Dimostrare che $V^* \cong K^{\dim V}$. In particolare, $V^* \cong V$ se e solo se $\dim V < \infty$.

SUGGERIMENTI. (1) Dimostrare che i polinomi $1, x, x^2, \ldots, x^n, \ldots$ formano una base di $K[x]$.

(2) Applicare l'esercizio 3.8.

(3) Sia B una base di V. Allora, per l'esempio 3.1 (b), esiste una biezione tra K^B (l'insieme delle funzioni $f : B \to K$) e l'insieme V^* degli omomorfismi $V \to K$. Non è difficile vedere che tale biezione è un isomorfismo. QED

Esempio 3.10. Sia F un'estensione del campo K. Allora per un elemento $\alpha \in F$ is ha:

(a) $\dim_K K(\alpha) < \infty$ se e solo se α àlgebrico su K;

(b) $\dim_K K(\alpha)$ è infinita se e solo se α è trascendente su K. In tal caso $\dim_K K(\alpha)$ è numerabile.

3.2 Moduli

Ora introduciamo un concetto che generalizza simultaneamente i gruppi abeliani e gli spazi vettoriali.

Nel seguito R sarà un anello unitario. Un R-modulo (sinistro) è un gruppo abeliano $(M,+)$ munito di una "motliplcazione con scalari di R", ovvero un'applicazione $R \times M \to M$, per la quale denoteremo con rx il prodotto dello scalare $r \in R$ e l'elemento $x \in M$, soggetto alle seguenti quattro assiomi per $\lambda, \mu \in K$ e il vettore $u, v \in V$:

(a) $r(u+v) = \lambda u + \lambda v$;

(b) $(r+s)u = ru + su$;

(c) $r(su) = (rs)u$;

(d) $1.u = u$.

Se M, N sono R-moduli, un omomorfismo di spazi vettoriali $f : M \to N$ è un omomorfismo dei gruppi abeliani $(M,+)$ e $(N,+)$ tale che $f(rx) = rf(x)$ per ogni $r \in R$ e $x \in M$.

Per una famiglia $\{M_i : i \in I\}$ di R-moduli il prodotto diretto $M = \prod_{i\in I} M_i$ dei gruppi $(M_i,+)$ ammette anche una struttura naturale di R-modulo (per $f = (f_i) \in M$ e $r \in R$ si pone $rf = (rf_i)$). Nello stesso modo come per il prodotto diretto, anche la somma diretta $\bigoplus_{i\in I} M_i$ risulta un R-modulo, infatti sottomodulo del prodotto M. Prendendo tutti gli $M_i = R$, ricaviamo il R-modulo $\bigoplus_I R$. Come detto in precedenza, questo R-modulo dipende solo dalla cardinalità dell'insieme I, e pertanto sarà denotato anche con $\bigoplus_\alpha R$, dove $\alpha = |I|$. Ogni R-modulo di questa forma si dice *R-modulo libero*. Così, con $R = \mathbb{Z}$ otteniamo come $\mathbb{Z}$-moduli i gruppi abeliani (gli $\mathbb{Z}$-moduli liberi sono i gruppi abeliani liberi, vedi Definizione 4.1). Nel caso quando $R = K$ è un campo, i R-moduli sono gli spazi vettoriali sopra K.

4 Rango libero di un gruppo abeliano

4.1 Gruppi liberi abeliani

Adesso introduciamo una classe di gruppi abeliani che ricorda gli spazi vettoriali.

Definizione 4.1. Un gruppo abeliano si dice *libero*, se esiste un insieme non-vuoto I tale che $G \cong \bigoplus_I \mathbb{Z}$.

In particolare, $\mathbb{Z}$, e anche tutte le potenze finite[2] $\mathbb{Z}^n$ sono gruppi abeliani liberi.

In altre parole, un gruppo abeliano F è libero se e solo se esistono un cardinale α e un isomorfismo $F \cong \bigoplus_\alpha \mathbb{Z}$. Tale numero cardinale α è univocamente determinato dal gruppo F. Infatti, se α è infinito, abbiamo $\alpha = |F|$. Se invece $\alpha < \infty$, abbiamo di nuovo unicità per il seguente lemma che vale anche nel caso infinito:

Lemma 4.2. *Se $\mathbb{Z}^{(n)} \cong \mathbb{Z}^{(m)}$ per due numeri cardinali n, m allora $m = n$.*

Dimostrazione. Supponiamo che $f : \mathbb{Z}^{(n)} \to \mathbb{Z}^{(m)}$ sia un isomorfismo. Allora fissiamo un numero primo p e notiamo che per ogni isomorfismo gruppale $g : G_1 \to G_2$ si ha $g(pG_1) = pG_2$ e quindi $G_1/pG_1 \cong G_2/pG_2$. Nel nostro caso abbiamo $\mathbb{Z}_p^{(n)} \cong \mathbb{Z}_p^{(m)}$ e contando gli elementi dei rispettivi gruppi concludiamo che $n = m$. QED

Denotiamo con $r_0(F)$ il numero cardinale α così determinato da $F \cong \bigoplus_\alpha \mathbb{Z}$.

Un sottoinsieme M di un gruppo abeliano G si dice *indipendente* se $\sum_i n_i b_i = 0$ per $b_1, \dots, b_s \in M$ e $n_1, \dots, n_s \in \mathbb{Z}$ implica $b_1 = \cdots = b_s = 0$. Diremo che M è *massimale* se non è contenuto propriamente in alcun sottoinsieme indipendente di G.

Lemma 4.3. *Se un sottoinsieme M di un gruppo abeliano G è indipendente, allora il sottogruppo $\langle M \rangle$ di G generato da M è libero.*

Usandlo il lemma si vede che un gruppo abeliano è libero se e solo se se ha un sistema di generatori che formano un sottoinsieme indipendente. Tale sistema sarà chiamato anche *base* di F.

Esercizio 4.4. *Sia $n \in \mathbb{N}$ e sia M un sottoinsieme indipendente di $\mathbb{Z}^n$. Dimostrare che $|M| \leq n$.*

Suggerimenti. Supponiamo che $|M| > n$ e siano $\{v_0, v_1, \dots, v_n\} \subseteq M$. Consideriamo $v_0, v_1, \dots, v_n$ come vettori delle spazio vettoriale $\mathbb{Q}^n$ su $\mathbb{Q}$. Possiamo trovare una combinazione lineare $\sum_i m_i v_i = 0$ con $m_0, \dots, m_s \in \mathbb{Q}$, ma non è restrittivo supporre che $m_i \in \mathbb{Z}$. Quindi $\{v_0, v_1, \dots, v_n\}$ e in particolare M, non sono indipendente. QED

Lemma 4.5. *Sia M un sottoinsieme indipendente di G. Allora M è massimale se e solo se per ogni $x \in G$ esiste un intero positivo n tale che $nx \in \langle M \rangle$.*

[2] Il gruppo $\mathbb{Z}^{\mathbb{N}}$, noto come *gruppo di Specker*, non è libero anche se ogni sottogruppo numerabile di $\mathbb{Z}^{\mathbb{N}}$è libero [5, Theorem 19.2].

Lemma 4.6. *Ogni sottoinsieme indipendente di G è contenuto in un sottoinsieme indipendente massimale.*

DIMOSTRAZIONE. Si applichi il lemma di Zorn alla famiglia non vuota degli sottoinsiemi indipendenti di G ordinata rispetto all'inclusione. QED

Adesso dimostreremo una proprietà dei gruppi abeliani liberi duale alla proprietà dei gruppi divisibili vista nel Teorema 7.5. A questo scopo serve il seguente lemma:

Lemma 4.7. *Sia F un gruppo abeliano libero con insieme indipendente di generatori X e sia G un gruppo abeliano. Allora ogni applicazione $f : X \to G$ si estende ad un omomorfismo gruppale $\bar{f} : F \to G$.*

SUGGERIMENTI. Ogni elemento g di F si può scrivere in modo unico come $g = \sum_{i=1}^{n} k_i x_i$, $x_i \in X$, $k_i \in \mathbb{N}$. Poniamo allora $\bar{f}(g) := \sum_{i=1}^{n} k_i f(x_i)$. QED

Teorema 4.8. *Sia G un gruppo abeliano e sia H un sottogruppo di G tale che il quoziente G/H è libero. Allora esiste un sottogruppo N di G tale che $G \cong N \times H$.*

DIMOSTRAZIONE. Sia $g : G \to G/H$ l'omomorfismo canonico e sia X un insieme indipendente di generatori del gruppo abeliano libero G/H. Per ogni $x \in X$ esiste un $a_x \in G$ con $g(a_x) = x$. Per l'applicazione $f : G/H \to G$ definita con $f(x) = a_x$ esiste un omomorfismo $f : G/H \to G$ che la estende. Poichè X genera G/H e $g(f(x)) = x$ per ogni $x \in X$, si ha $gf = id_{G/H}$. Chiaramente il sottogruppo $N = f(G/H)$ interseca H in 0. Quindi $G \cong N \times H$. QED

Lemma 4.9. *Sia G un gruppo abeliano e siano M e M_1 due sottoinsiemi indipendenti massimali di G. Allora $|M| = |M_1|$.*

DIMOSTRAZIONE. Se una delle cardinalità, diciamo $\alpha = |M|$, è finita ragioniamo così. Siano $v_1, \ldots, v_m$ elementi distinti di M_1. Dal Lemma 4.5 segue che esiste $n \in \mathbb{N}$ positivo con $nv_1, \ldots, nv_m \in M$. Poichè questo insieme è ovviamente indipendente, per l'Esercizio 4.4 il sottoinsieme $\{nv_1, \ldots, nv_\alpha\}$ di $\langle M \rangle \cong \mathbb{Z}^\alpha$ deve avere cardinalità $\leq \alpha$. Allora $m \leq \alpha$. Questo dimostra $|M_1| \leq |M|$, analogamente dimostriamo $|M| \leq |M_1|$.

Supponiamo che $\alpha = |M|$ è infinito, allora anche $|M_1|$ è infinito. Consideriamo i sottogruppi $F = \langle M \rangle$ e $F_1 = \langle M_1 \rangle$. Chiaramente, $|F| = |M| = \alpha$. Per la massimalità di M_1 per ogni $b \in M$ esiste $n_b > 0$ tale che $n_b b \in F_1$. Per $x = \sum_{i=1} k_i b_i \in F$ poniamo $f(x) = \sum_{i=1} k_i n_{b_i} b_i \in F_1$. Così $f : F \to F_1$ risulta un omomorfismo iniettivo. Quindi, $\alpha = |F| = |f(F)| \leq |M_1|$. In modo analogo anche $|M_1| \leq |M| = \alpha$. QED

Rango libero di un gruppo abeliano G si chiama la cardinalità di un qualunque sottoinsieme indipendente massimale di G. Denoteremo con $r_0(G)$ il rango libero di G e spesso diremo semplicemente *rango* di G.

Esercizio 4.10. *Sia G un gruppo abeliano e $f : G \to G/t(G)$ l'omomorfismo canonico. Allora un insieme $M \subseteq G$ è indipendente se e solo se $f(M)$ è un insieme indipendente di $G/t(G)$.*

Lemma 4.11. *Se G è un gruppo abeliano e H è un sottogruppo di G, dimostrare che $r_0(G) = r_0(G/H) + r_0(H)$.*

DIMOSTRAZIONE. Si scelga un insieme indipendente massimale M_0 in H e un insieme indipendente massimale $\tilde{M}$ in G/H. Sia $q : G \to G/H$ l'omomorphism canonico. Si scelga un insieme M_1 in G tale che $q \restriction_{M_1} : M_1 \to \tilde{M}$ è una biezione (questo è possibile perchè q è suriettiva). Ora $M = M_0 \cup M_1$ è un indipendente massimale in G. Infatti, per vedere che M è indipendente supponiamo che $\sum_{i=1}^{n} k_i b_i + \sum_{j=1}^{n} m_j b_j^* = 0$, con $k_i, m_j \in \mathbb{Z}$ e $b_i \in M_0, b_j^* \in M_1$. Proiettando in G/H tramite q troviamo $\sum_{j=1}^{n} m_j q(b_j^*) = 0$ e quindi tutti $b_j^* = 0$. Ora resta $\sum_{i=1}^{n} k_i b_i = 0$ e per l'indipendenza di M_0 conculdiamo che tutti $k_i = 0$. Pertanto, M è indipendente. Supponiamo che $y \in G \setminus M$. Se $y \in H$, allora $M_0 \cup \{y\}$ non è indipendente, quindi tantomeno $M \cup \{y\}$ non è indipendente. Se $y \not\in H$, allora $q(y) \neq 0$ in G/H. Essendo $\tilde{M}$ un insieme indipendente massimale in G/H, l'insieme $\tilde{M} \cup \{q(y)\}$ o coincide con $\tilde{M}$ o non e' indipendente. In entrambi i casi esiste $k \neq 0$ in $\mathbb{Z}$ tale che $kq(y) \in \langle \tilde{M} \rangle$ e quindi $ky \in \langle M_1 \rangle + H$ in G. Pertanto esiste $h \in H$ tale che $ky - h \in \langle M_1 \rangle$. Essendo M_0 un insieme indipendente massimale in H, esiste $m \neq 0$ in $\mathbb{Z}$ con $mh \in \langle \tilde{M}_0 \rangle$. Quindi, $mky \in \langle M \rangle$ e $M \cup \{y\}$ non è indipendente. QED

Esercizio 4.12. *Siano G ed H gruppi abeliani. Dimostrare che $r_0(G \times H) = r_0(G) + r_0(H)$ senza far ricorso al lemma precedente.*

Esercizio 4.13. *Sia G un gruppo abeliano senza torsione. Dimostrare che $|G| = r_0(G) \cdot \aleph_0$.*

Esercizio 4.14. *Calcolare $r_0(\mathbb{Z}^{\aleph_0})$ e $r_0(\mathbb{Z}^{(\aleph_0)})$.*

Esercizio 4.15. *Sia K un campo di caratteristica 0. Dimostrare che $r_0(K, +) = \dim_{\mathbb{Q}} K$.*

Esercizio 4.16. * *Se G è un gruppo abeliano senza torsione, allora $r_0(G) = \dim_{\mathbb{Q}} G \otimes \mathbb{Q}$.*

5 Gruppi abeliani finitamente generati

L'obbietivo principale di questo paragrafo è la descrizioen della struttura dei gruppi abeliani finitamente generati tramite il seguente:

Teorema 5.1. *Sia G un gruppo abeliano finitamente generato. Allora G è somma diretta di gruppi ciclici.*

Corollario 5.2. (Teorema di Frobenius-Stickelberger) *Ogni gruppo abeliano finito è prodotto diretto di gruppi ciclici.*

Vedremo nel seguito che la conclusione di questo corollario rimane vera sotto ipotesi più generali (Teorema 6.7).

Per la dimostrazione del Teorema 5.1 avremo bisogno del lemma seguente:

Lemma 5.3. *Se $n \in \mathbb{N}$ e $\beta = (b_1, \ldots, b_n) \in \mathbb{Z}^n$ è tale che il MCD dei $b_1, \ldots, b_n$ è 1, allora β può essere completato ad una base di $\mathbb{Z}^n$.*

Dimostrazione. Sia $m = \sum_{i=1}^n |b_i|$. Se $m = 1$, allora l'asserto è banalmente vero. Notiamo che le coordinate $b_1, \ldots, b_n$ di β sono relativi alla base canonica $\mathcal{B}$

$$e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_1 = (0, 0, \ldots, 0, 1),$$

di $\mathbb{Z}^n$. Se in qualche base $\mathcal{B}_1 = \{f_1, f_2, \ldots, f_n\}$ di $\mathbb{Z}^n$ β ha coordinate $b'_1, \ldots, b'_n$ con $m = \sum_{i=1}^n |b'_i| = 1$, allora l'asserto è vero come prima. Si procede per induzione su

$$m = \min \left\{ \sum_{i=1}^n |b'_i| : \text{ dove } b'_1, \ldots, b'_n \text{ sono le coordinate in qualche base } \mathcal{B} \text{ di } \mathbb{Z}^n \right\}.$$

Abbiamo già visto che il caso $m = 1$ banale. Supponiamo $m > 1$, allora esistono almeno due indici $i \neq j$ con $b_i \neq 0$ e $b_j \neq 0$. Senza ledere la generalità supponiamo che $i = 1$ e $j = 2$. Inoltre, $|b_1| \geq |b_2| > 0$. Allora, sia ha $|b_1 + b_2| < |b_1$, oppure $|b_1 - b_2| < |n_1$. Supponiamo che valga $|b_1 + b_2| < |b_1$. Ora cambiamo la base canonica $\mathcal{B}$

$$e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_1 = (0, 0, \ldots, 0, 1),$$

di $\mathbb{Z}^n$, introducendo una nuova base $\mathcal{B}_1 = \{f_1, f_2, \ldots, f_n\}$ definita con

$$f_1 = e_1, f_2 = e_2 - e_1, f_3 = e_3, \ldots, f_n = e_n.$$

In questa base si ha $\beta = (b_1 + b_2)f_1 + b_2 f_2 + b_3 f_3 + \ldots + b_n f_n$. In altra parole, nella base $\mathcal{B}_1$ l'elemento β ha coordinate $(b_1 + b_2, b_2, b_3, \ldots, b_n)$ con rispettiva somma

$$|b_1 + b_2| + |b_2| + |b_3| + \ldots + |b_n| < |b_1| + |b_2| + |b_3| + \ldots + |b_n| = m.$$

Poiché il MCD dei $b_1 + b_2, b_2, b_3, \ldots, b_n$ è sempre 1, per l'ipotesi induttiva β può essere completato ad una base di $\mathbb{Z}^n$. QED

Il passo successivo è il caso del teorema senza torsione:

Lemma 5.4. *Sia G un gruppo abeliano senza torsione finitamente generato. Allora $G \cong \mathbb{Z}^n$, dove $n = r(G) < \infty$.*

Dimostrazione. Sia G un gruppo abeliano finitamente generato e sia $f : \mathbb{Z}^n \to G$ un omomorfismo suriettivo con n minimale. Allora per il sottogruppo $A = \ker f$ di $\mathbb{Z}^n$ il quoziente $\mathbb{Z}^n/A \cong G$ è senza torsione. Basta dimostrare che A è uguale a 0. In caso contrario si sceglie un elemento non nullo $\beta = (b_1, \ldots, b_n) \in A$. Sia m il MCD dei $b_1, \ldots, b_n$. Allora $b_i = mb'_i$ per $i = 1, 2, , \ldots, n$ e il MCD dei $b'_1, \ldots, b'_n$ è 1. Poniamo $\gamma = (b'_1, \ldots, b'_n) \in \mathbb{Z}^n$. Allora $\beta = m\gamma$ e quindi $mf(\gamma) = 0$ in G. Essendo G senza torsione, concludiamo che $f(\gamma) = 0$, i,.e., $\gamma \in A$. Per il Lemma 5.3 esiste un sottogruppo libero $B \cong \mathbb{Z}^{n-1}$ di $\mathbb{Z}^n$ tale che $\mathbb{Z}^n = \langle\gamma\rangle \times B$, quindi $\mathbb{Z}^n/\langle\gamma\rangle \cong B \cong \mathbb{Z}^{n-1}$. Poichè $\gamma \in A$, $\langle\gamma\rangle \leq A$ e di conseguenza il quoziente $\mathbb{Z}^n/A$ risulta essere isomorfo al quoziente di $\mathbb{Z}^n/\langle\gamma\rangle \cong \mathbb{Z}^{n-1}$ rispetto al sottogruppo $A/\langle\gamma\rangle$. Quindi esiste un omomorfismo suriettivo $\mathbb{Z}^{n-1} \to G$ contatriamente alla scelta di n – assurdo.

Quindi $A = 0$ e $G \cong \mathbb{Z}^n$. QED

Dimostrazione del Teorema 5.1: Sia G un gruppo abeliano finitamente generato e sia $f : \mathbb{Z}^n \to G$ un omomorfismo suriettivo. Sia $A = \ker f$ e $B = \{x \in \mathbb{Z}^n : (\exists k \in \mathbb{N})kx \in A\}$. Allora $f(B) = t(G)$. D'altra parte il quoziente $\mathbb{Z}^n/B \cong G/t(G)$ è senza torsione e finitamente generato, quindi $G/t(G) \cong \mathbb{Z}^k$ è libero per il Lemma 5.4. Per il Teorema 4.8 abbiamo $\mathbb{Z}^n \cong B \times \mathbb{Z}^k$ e $G \cong t(G) \times \mathbb{Z}^k$. In particolare, sia B che $t(G)$ sono finitamente generati essendo isomorfi a quozienti di gruppi finitamente generati. Allora $t(G)$ è di esponente finita (se $t(G) = \langle g_1, \ldots, g_s\rangle$, allora il minimo commune multiplo c di tutti periodi $o(g_i)$ soddisfa $c \cdot t(G) = 0$). Quindi, il Teorema 6.7 implica che anche $t(G)$ è somma diretta di gruppi ciclici (finiti). •

Un sottogruppo di un gruppo libero abeliano è libero. Noi lo dimostreremo solo nel caso di rango finito nella seguente forma più precisa.

Teorema 5.5. *Sia F_n un gruppo abeliano libero di rango finito n e sia A un sottogruppo di F_n. Allora A è libero ed i gruppi F_n e A possiedono delle basi $\{a_1, \dots, a_k\}$ e $\{f_1, \dots, f_n\}$ soddisfacenti alle condizioni: $k \leq n$, $a_i = m_i f_i$ per $1 \leq i \leq k$ e $m_i | m_{i+1}$ per $1 \leq i \leq k-1$.*

DIMOSTRAZIONE. Procediamo per induzione su n. Il caso $n = 1$ è banale. Supponiamo che $n > 1$ e il teorema sia vero per $n-1$. Tra tutte le basi di $\mathbb{Z}^n$ e tutti gli elementi non-nulli di A scegliamo la base $\mathcal{B} = f_1^*, b_2, \dots, b_n$ e un elemento $a_1 \in A$ tali che il coefficiente m_1 nella combinazione lineare $a_1 = m_1 f_1 + \sum_{i=2}^n s_i b_i$ sia positivo e minimale. Notiamo che questa scelta si può supporre ulteriormente che m_1 divide s_i per tutti $2 \leq i \leq n$. Infatti, se $s_i = q_i m_1 + r_i$ con $0 \leq r_i < m_1$ per tutti $2 \leq i \leq n$, poniamo $f_1 = f_1^* + \sum_{i=2}^n b_i f_i$. Allora avremo $a = m_1 f_1 + \sum_{i=2}^n r_i f_i$ con $0 \leq r_i < m_1$. Per la scelta di $\mathcal{B}$ avremo tutti $r_i = 0$ e $a_1 = m_1 f_1$.

Sia $F_{n-1} = \langle b_2 \dots, b_n \rangle$ e $B = A \cap F_{n-1}$. Allora $\langle a_1 \rangle \cap B = 0$ e quindi $\langle a_1 \rangle + B = \langle a_1 \rangle \oplus B$. Dimostreremo che $A = \langle a_1 \rangle \oplus B$. Allora a B si potrà applicare l'ipotesi induttiva. Sia $a \in A$. Allora $a = m f_1' + b$, con $b \in B$. Sia $m = q m_1 + r$ con $0 \leq r < m_1$. Allora $a' = a - q a_1 \in A$ e $a' = r f_1 + b$. Per la scelta di $\mathcal{B}$ e a_1 si ha $r = 0$ e quindi $m_1 | m$. Quindi $a = q a_1 + b \in \langle a_1 \rangle \oplus B$.

Per l'ipotesi induttiva F_{n-1} ha una base $f_2, \dots, f_n$ e B una base $a_2, \dots, a_k$ tali che

$$a_i = m_i f_i \ \text{ per } \ 2 \leq i \leq k \quad \text{e} \quad m_i | m_{i+1} \ \text{ per } \ 2 \leq i < k.$$

Ora resta a vedere che $m_1 | m_2$. Sia $m_2 = q m_1 + r$ con $0 \leq r < m_1$. Allora $a_2 - a_1 \in A$, e $a_2 - a_1 = m_2 f_2 - m_1 f_1 = m_1(q f_2 - f_1) + r f_2$. Quindi nella base $q f_2 - f_1, f_2, f_3, \dots, f_n$ il coefficiente relativo a $q f_2 - f_1'$ risulta essere $r < m_1$. Per la scelta di $\mathcal{B}$ si avrà $r = 0$, cioè, m_1 divide m_2. QED

Seconda dimostrazione del Teorema 5.1: Come corollario si ottiene una nuova dimostarzione del Teorema 5.1. Infatti, si presenti G come quoziente di un gruppo libero abeliano di rango finito F_n e si applichi il Teorema 4.8 e l'Esercizio 2.3.

Corollario 5.6. *Ogni sottogruppo di un gruppo abeliano libero finitamente generato è libero.*

Il seguente esercizio è caso particolare di un risultato molto più generale. Provare a dimostrarlo direttamente, senza ricorso al Teorema 5.5:

Corollario 5.7. *Sia $n \in \mathbb{N}$. Allora ogni sottogruppo di $\mathbb{Z}^n$ è finitamente generato.*

6 Il p-rango

6.1 Zoccolo di un gruppo abeliano

Sia G un gruppo abeliano e sia p un numero primo. Poniamo $Soc(G) = \bigoplus_p G[p]$. I gruppi abeliani del tipo $G = Soc(G)$ si chiamano anche *semisemplici*.

Ovviamente il sottogruppo $G[p]$ di un gruppo abeliano G è uno spazio vettoriale sul campo $\mathbb{F}_p$. La dimensione $\dim_{\mathbb{F}_p} G[p]$ si chiama *p-rango* di G e si denota con $r_p(G)$. Chiaremante $G[p] \cong \bigoplus_{r_p(G)} \mathbb{Z}_p$.

Esempio 6.1. *Il gruppo di Prüfer ha $r_p(\mathbb{Z}(p^\infty)) = 1$. Infatti, basta notare che $(\mathbb{Z}(p^\infty))[p] \cong \mathbb{Z}_p$.*

Esercizio 6.2. *Sia p un numero primo. Calcolare $r_p(\mathbb{Q}^*, \cdot)$, $r_p(\mathbb{R}^*, \cdot)$ e $r_p(\mathbb{C}^*, \cdot)$.*

Esercizio 6.3. *Sia $\{G_i\}_{i \in I}$ una famiglia di gruppi abeliani e sia p un numero primo. Dimostrare che*

$$\left(\prod_{i \in I} G_i\right)[p] = \prod_{i \in I} G_i[p], \ \left(\bigoplus_{i \in I} G_i\right)[p] = \bigoplus_{i \in I} G_i[p] \text{ e } Soc\left(\bigoplus_{i \in I} G_i\right) = \bigoplus_{i \in I} \left(Soc(G_i)\right).$$

Dimostrare che $Soc\left(\prod_{i \in I} G_i\right) \subseteq \prod_{i \in I} \left(Soc(G_i)\right)$ e dare un esempio di quando l'uguaglanza fallisce.

Esercizio 6.4. *Siano G ed H gruppi abeliani e sia p un numero primo. Dimostrare che $r_p(G \times H) = r_p(G) + r_p(H)$.*

Esercizio 6.5. *Sia p un numero primo. Calcolare $r_p(\mathbb{Z}_p^{\mathbb{N}})$ e $r_p((\mathbb{Q}/\mathbb{Z})^{\mathbb{N}})$.*

6.2 Gruppi abeliani di esponente finito

Il seguente teorema di Prüfer descrive la struttura dei gruppi abeliani di esponente finito.

Lemma 6.6. *Sia p un numero primo e sia G un gruppo abeliano di esponente p^n, $n \in \mathbb{N}$. Allora G è somma diretta di gruppi ciclici.*

Dimostrazione. Per $n = 1$ l'asserto segue dal ... perchè G è una spazio vettoriale sul campo finito $\mathbb{F}_p$. Sia $n > 1$ e supponiamo che l'asserto sia vero per $n-1$. Il gruppo $G_1 = pG$ è di espenente p^{n-1} e per l'ipotesi induttiva sarà soma diretta di sottogruppi ciclici – $G_1 = \oplus_{i\in I}\langle a_i\rangle$. Ora $a_i = px_i$ per ogni $i \in I$, con $x_i \in G$. Allora anche la somma H dei sottogruppi $\langle x_i\rangle$ è diretta. Per il lemma di Zorn esiste un sottogruppo B di G con $B \cap H = 0$ e massimale con questa proprietà. Dimostriamo che $G = B + H$ (ovviamente questa somma e diretta).

Prima vediamo che $Soc(G) \subseteq B + H$. Sia $g \in Soc(G)$ e supponiamo che $g \notin B$. Allora $g \neq 0$ e $B_1 = B + \langle g\rangle$ contiene propriamente B. Quindi $B_1 \cap H \neq 0$, sia $0 \neq h \in H \cap B_1$. Allora $h = h_1 + kg$ con $0 < k < p$. Quindi $\langle g\rangle = \langle k \cdot g\rangle \subseteq B + H$. Quindi $g \in B + H$.

Sia adesso $g \in G$ arbitrario. Allora $pg \in pH$ e quindi $pg = ph$ per qualche $h \in H$. Allora $g_1 = g - h \in Soc(G) \subseteq H + B$.

Abbiamo così dimostrato $G = B \oplus H$, e pertanto $pB = 0$ perchè $pG = pB \oplus pH$ e $pG = pH$. Allora B è somma diretta di gruppi ciclici essendo uno spazio vettoriale su $\mathbb{F}_p$. QED

Teorema 6.7. (Prüfer) *Sia n un numero naturale positivo e sia G un gruppo abeliano di esponente n. Allora G è somma diretta di gruppi ciclici.*

Dimostrazione. Ovviamente ciascuna delle componenti primarie di G è di esponente finita, quindi si applica il Lemma 6.6. QED

Notiamo che per il gruppo G di esponente n il teorema garantisce una presentazione $G = \bigoplus_{i\in I}\mathbb{Z}_{m_i}$. Siccome ogni m_i è un divisore di n ci saranno solo un numero finiti di gruppi ciclici diversi in questa somma diretta. In altre parole, passando alla componente primaria $t_p(G)$, possiamo scrivere $t_p(G) = \bigoplus_{i=1}^{k_p}\mathbb{Z}_{p^i}^{(\alpha_{p,i})}$. Quindi,

$$G = \bigoplus_p \bigoplus_{i=1}^{k_p} \mathbb{Z}_{p^i}^{(\alpha_{p,i})}, \tag{2}$$

dove i numeri cardinali $\alpha_{p,i}$ $(i = 1, 2, \ldots, k_p)$, noti come *invarianti di Ulm-Kaplansky*, possono essere non-nulli solo per un numero finito di primi p.

6.3 Sottogruppi essenziali

Un sottogruppo H di G dicesi *essenziale* se per ogni sottogruppo normale non-banale N di G si ha $N \cap H \neq \{1\}$.

Esercizio 6.8. *Sia G un gruppo abeliano periodico. Dimostrare che $Soc(G)$ è un sottogruppo essenziale di G. Per ogni primo p dimostrare che $Soc_p(G)$ è un sottogruppo essenziale di $t_p(G)$.*

Esercizio 6.9. *Dimostrare che ogni sottogruppo non-nullo (in particolare, $\mathbb{Z}$) è essenziale di $\mathbb{Q}$. Dimostrare che ogni sottogruppo non-ciclico di $\mathbb{Q}^2$ è essenziale.*

Esercizio 6.10. *Sia G un gruppo abeliano. (a) Dimostrare che G è sottogruppo essenziale in se stesso. Dimostrare che G non ha sottogruppi essenziali propri se e solo se $G = Soc(G)$.*

Lemma 6.11. *Sia $f : G \to G_1$ un omomorfismo di gruppi. Se H è un sottogruppo essenziale di G e la restrizione $f|_H$ è iniettiva, allora f è un monomorfismo.*

Dimostrazione. Applicare la definizione al sottogruppo normale $N = \ker f$. QED

Esercizio 6.12. *Dimostrare che il Lemma 6.11 si inverte: se H ha questa proprietà* per tutti *gli omomorfismi f di dominio G, allora H è essenziale.*

Esercizio 6.13. *Sia G un gruppo, H un sottogruppo essenziale di G e G_1 un gruppo abeliano. Se due omomorfismi $f, g : G \to G_1$ coincidono su H, allora $f = g$.*

Suggerimenti. Considerare l'omomorfismo $h : G \to G_1$ definito da $h(x) = f(x) - g(x)$. QED

Esercizio 6.14. *Sia G un gruppo abeliano senza torsione.*

(a) Sia M un sottoinsieme indipendente di G. Dimostrare che M è massimale se e solo se il sottogruppo $\langle M\rangle$ è essenziale.

(b) Sia H un sottogruppo di G. Dimostrare che H è essenziale se e solo se il gruppo quoziente G/H è periodico.

Esercizio 6.15. *Sia G un gruppo abeliano e sia H un sottogruppo di G. Dimostrare che H è essenziale se e solo se H contiene $Soc\,(G)$ ed un sottoinsieme indipendente massimale di G.*

Esercizio 6.16. *Sia G un gruppo abeliano e sia H un sottogruppo di G. Dimostrare che ogni gruppo abeliano contiene un sottogruppo essenziale che è somma diretta di gruppi ciclici.*

Esercizio 6.17. *Se G e H sono gruppi abeliani, N e K sono sottogruppi essenziali di G e H rispettivamente, allora $N \times K$ è un sottogruppo essenziale di $G \times H$.*

Esercizio 6.18. *Sia $\{G_i\}_{i\in I}$ una famiglia di gruppi abeliani e sia H_i un sottogruppo essenziale di G_i per ogni $i \in I$. Allora $\oplus_{i\in I}H_i$ è un sottogruppo essenziale di $\oplus_{i\in I}G_i$. Si può estendere questa affermazione anche ai prodotti diretti?*

Suggerimenti. Notare che mentre $\mathbb{Z}$ è un sottogruppo essenziale di $\mathbb{Q}$, il sottogruppo $\mathbb{Z}^{\mathbb{N}}$ di $\mathbb{Q}^{\mathbb{N}}$ non è essenziale. QED

7 Gruppi divisibili

Un gruppo si dice *divisibile* si per ogni $x \in G$ e $n \in \mathbb{Z}$ positivo esiste $y \in G$ tale che $x = y^n$. Chiaramente il gruppo banale è divisibile; è facile vedere che i gruppi divisibili non-banali sono infiniti.

Esempio 7.1. Non è difficile vedere che i seguenti gruppi sono divisibili: $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\bar{\mathbb{Q}}^*, .)$, $(\mathbb{C}^*, \cdot)$ e $\mathbb{Z}(p^\infty)$ mentre i gruppi $(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \cdot)$ e $(\mathbb{R}^*, \cdot)$ non sono divisibili.

Osservazione 7.2. I gruppi divisibili D sono legati alla proprietà di estensione degli omomorfismi (con valori in D) nel modo seguente. Un gruppo D è divisibile se e solo se per ogni sottogruppo H di $\mathbb{Z}$ ogni omomorfismo $f : H \to D$ si estende ad un omomorfismo $\bar{f} : \mathbb{Z} \to D$. (Infatti, se $H = m\mathbb{Z} \neq 0$ e $f(m) = a \in D$, esiste $x \in D$ con $mx = a$. Ponendo $\bar{f}(1) = x$ otteniamo l'estensione desiderata $\bar{f} : \mathbb{Z} \to D$. D'altra parte, se $m \neq 0$ a $a \in D$, per risolvere l'equazione $mx = a$ si estende l' omomorfismo $f : m\mathbb{Z} \to D$ definito con $f(m) = a$ e si prende $x = \bar{f}(1)$, dove $\bar{f} : \mathbb{Z} \to D$ estende f.)

Lemma 7.3. *(a) La classe dei gruppi divisibili è chiusa per passaggio a prodotti diretti, quozienti e somme dirette.*

(b) Se N è un sottogruppo centrale divisibile di un gruppo G tale che il quoziente G/N sia divisibile, allora anche il gruppo G è divisibile.

Adesso estendiamo la proprietà di estensione dell'osservazione 7.2 nel caso generale.

Teorema 7.4. *Sia D un gruppo abeliano divisibile, sia G un gruppo abeliano e sia $f : H \to D$ un omomorfismo con H un sottogruppo di G. Allora esiste un estensione $\bar{f} : G \to D$ di f su tutto il gruppo G.*

La dimostrazione di questo teorema si può trovare in [2].

Ora vediamo che i sottogruppi divisibili sono sempre addendi diretti.

Teorema 7.5. *Sia G un gruppo abeliano e sia D un sottogruppo divisibile di G. Allora esiste un sottogruppo H di G tale che $G \cong D \times H$.*

Dimostrazione. Si estenda a tutto il gruppo G l'omomorfismo $f : D \to G$ definito con $f(x) = x$ per $x \in D$. Se $\bar{f}$ è questa estensione, si ponga $H := \ker \bar{f}$. Allora $G = D + H$ e $D \cap H = 0$, di conseguenza $G \cong D \times H$. QED

Corollario 7.6. *Sia D un gruppo abeliano divisibile. Allora $D \cong t(D) \times \mathbb{Q}^{(r_0(D))}$.*

Dimostrazione. Dimostriamo inanzitutto che $D \cong t(D) \times (D/t(D))$. Questo segue dal teorema 7.5 a dal fatto che $t(D)$ è divisibile. Infatti, se $a \in t(D)$ e $n > 0$, allora esiste $x \in D$ con $nx = a$. Se $ka = 0$, allora $knx = 0$ e quindi $x \in t(D)$. QED

Corollario 7.7. *Sia G un gruppo abeliano e D un sottogruppo divisibile di G. Allora D è essenziale se e solo se $D = G$.*

Dimostrazione. Supponiamo che $D \neq G$. Allora, per il teorema precedente esiste un sottogruppo $H \neq 0$ di G tale che $G \cong D \times H$. Allora, $H \cap D = 0$, assurdo perchè D è essenziale in G. QED

Esercizio 7.8. *Dimostrare che se $(K,+,\cdot)$ è un campo, allora $(K,+)$ è divisibile. Se K è algebricamente chiuso, allora anche $(K^*,\cdot)$ è divisibile.*

Esercizio 7.9. *Dimostrare che i gruppi $SL_n(\mathbb{R})$, $UT_n(\mathbb{R})$, $SO_n(\mathbb{R})$ e $U_n(\mathbb{C})$ sono divisibili, mentre $GL_n(\mathbb{R})$, $T_n(\mathbb{R})$, $O_n(\mathbb{R})$ non sono divisibili.*

Osservazione 7.10. (a) I gruppi finitamente generati abeliani non-banali sono mai divisibili e lo stesso vale per i gruppi di esponente finitio.

(b) Sia R un anello unitario. Un R-modulo D si dice *iniettivo*, so per ogni sottomodulo H di qualche R-modulo M e per ogni omomorfismo $f : H \to D$ esiste un estensione $\bar{f} : M \to D$ di f su tutto il modulo G. Il teorema 7.4 fa vedere come i gruppi abeliani divisibili sono iniettivi visti come $\mathbb{Z}$-moduli. D'altra parte, dall'osservazione 7.2 si vede che ogno gruppo abeliano iniettivo è divisibile. Quindi, i gruppi abeliani iniettivi coicidono proprio con i gruppi abeliani divisibili. D'altra parte, secondo 3.3 tutti gli spazi vettoriali sopra un campo K sono iniettivi visti come K-moduli.

7.1 Struttura dei gruppi abeliani divisibili

Il seguente teorema descrive la struttura di un grupo abeliano divisibile tramite il suo tango libero e tramite i suoi p-ranghi.

Teorema 7.11. *Sia D un gruppo abeliano divisibile con $\alpha = r_0(D)$ e $\alpha_p = r_p(D)$. Allora*

$$D \cong \mathbb{Q}^{(\alpha)} \oplus (\bigoplus_p \mathbb{Z}(p^\infty)^{(\alpha_p)}). \tag{1}$$

Dimostrazione. Per il Corollario 7.6 basta dimostrare che $t_p(D)$ è isomorfo al gruppo $G_p = \mathbb{Z}(p^\infty)^{(\alpha_p)}$ per ogni primo p. Notiamo che il gruppo G_p è divisibile (cf. Lemma 7.3). D'altra parte $Soc(t_p(D)) \cong \mathbb{Z}_p^{(\alpha_p)} \cong Soc(G_p)$. Fissiamo un isomorfismo $j : Soc(t_p(D)) \to Soc(G_p)$. Allora l'omomorfismo $j : Soc(t_p(D)) \to G_p$ si può estendere a tutto il gruppo $t_p(G)$. Sia $j_1 : t_p(G) \to G_p$ questa estensione. Poiché la restrizione j di j_1 su $Soc(t_p(G))$ è mono, anche j_1 è un monomorfismo. Ma allora $j_1 : t_p(G) \to j_1(t_p(G))$ è un isomorfismo, quindi il sottogruppo $j_1(t_p(G))$ di G_p è divisibile. Poichè esso contiene $Soc(G_p)$, sarà anche essenziale, Allora l'Esercizio 6.10 implica $j_1(t_p(G)) = G_p$. QED

Teorema 7.12. *Per ogni gruppo abeliano G esiste un monomorfismo $j : G \to D$, dove D è un gruppo abeliano divisibile e $j(G)$ è un sottogruppo essenziale di D.*

Dimostrazione. Si scelga un sottoinsieme indipendente massimale M di G. Allora il sottogruppo $F = \langle M \rangle$ di G è libero ed il sottogruppo $H = Soc(G) + F$ di G è essenziale. Si scelga il gruppo divisibile D come nel (1) con $\alpha = |M|$ e $\alpha_p = r_p(G)$. Allora $Soc(D) \cong Soc(G)$ ed il sottogruppo $K = \mathbb{Z}^{(\alpha)}$ di $\mathbb{Q}^{(\alpha)}$ è essenziale in $\mathbb{Q}^{(\alpha)}$ (Es. 6.18). Quindi $H = Soc(G) \oplus F$ è isomorfo al sottogruppo essenziale $Soc(D) \oplus K$ di D (Es. 6.15). Fissiamo un isomorfismo $i : H \to Soc(D) \oplus K$. Poichè D è divisibile, esiste per il Teorema 7.4 un estensione $j : G \to D$. Adesso $j(G)$ è essenziale perché contiene $i(G) = Soc(D) \oplus K$. Per il Lemma 6.11 j è anche un monomorfismo, perché la sua restrizione i su H è un monomorfismo. QED

Il gruppo divisibile D costruito nel teorema precedente si chiama inviluppo dibisibile di G e si denota con $D(G)$.

Esercizio 7.13. *Dimostrare che l'inviluppo dibisibile $D(G)$ di G è determinato univocamente a menso di isomorfismo, cioè se $j' : G \to D'$ è un altro monomorfismo tale che D' è divisibile e $j'(G)$ è un sottogruppo essenziale di D', allora esiste un isomorfismo $f : D \to D'$ tale che $f \circ j = j'$.*

Esercizio 7.14. *Dimostrare che $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_{p^n}$ e $\mathbb{Z}(p^\infty)$ sono indecomponibili in prodotto diretto di sottogruppi propri.*

Esercizio 7.15. *Dimostrare che ogni gruppo abeliano G è isomorfo ad un sottogruppo di una somma diretta di gruppi abeliani numerabili*

Suggerimenti. Applicare al gruppo $D(G)$ il Teorema 7.11. QED

8 Epilogo

8.1 Gruppi indecomponibili

Abbiamo visto che i gruppi finitamente generati, i gruppi divisibili ed i gruppi liberi[3] sono somme dirette di gruppi abbastanza semplici, addirittura indecomponibili:

[3] vedi anche Es. 6.16 ed il Teorema 6.7.

Esercizio 8.1. *Dimostrare che $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_{p^n}$ e $\mathbb{Z}(p^\infty)$ sono indecomponibili in prodotto diretto di sottogruppi propri.*

Tuttavia, non tutti i gruppi abeliani sono somme dirette di gruppi ciclici o copie di $\mathbb{Q}$ o $\mathbb{Z}(p^\infty)$. Esistono gruppi abeliani (abbastanza grandi) che sono indecomponibili pur non essendo isomorfi a nessuno dei gruppi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_{p^n}$ e $\mathbb{Z}(p^\infty)$ (per esempio il gruppo $\mathbb{J}_p$ degli interi p-adici che costruiremo nel paragrafo successivo (Teorema 8.15), ma esistono anche degli esempi molto più piccoli, per esempio sottogruppi di $\mathbb{Q}^2$).

8.2 L'anello di endomorfismi di un gruppo abeliano

Definizione 8.2. Sia G un gruppo. Denotiamo ***l'anello degli endomorfismi*** di G con:

$$\mathrm{End}(G) := \{\xi \colon G \to G \mid \xi \text{ un omomorfismo}\}.$$

Infatti tale insieme dotato delle due operazioni:

1. $(\xi + \eta)(x) := \xi(x) + \eta(x) \quad \forall x \in G$
2. $(\xi\eta)(x) = (\xi \cdot \eta)(x) := (\xi \circ \eta)(x) = \xi\Big(\eta(x)\Big) \quad \forall x \in G$

risulta essere un anello unitario, dove:

- $0 \colon G \to G$, $0(x) := 0 \quad \forall x \in G$ è l'elemento neutro per la somma,
- $id \colon G \to G$, $id(x) := x \quad \forall x \in G$ è l'elemento neutro per il prodotto.

Nel seguito identifichiamo il gruppo abeliano ciclico $\mathbb{Z}_m$ con l'anello quoziente $\mathbb{Z}/m\mathbb{Z}$ per ogni $m \in \mathbb{N}^*$.

Esempio 8.3. Avremo che

(1) $\mathrm{End}(\mathbb{Z}) \cong \mathbb{Z}$,

(2) $\mathrm{End}(\mathbb{Z}_m) \cong \mathbb{Z}/m\mathbb{Z}$ per ogni $m \in \mathbb{N}^*$.

Proof. (1) Consideriamo innanzitutto $\mathrm{End}(\mathbb{Z})$. Allora per ogni arbitrario endomorfismo $\phi \in \mathrm{End}(\mathbb{Z})$ porremo $\phi(1) := m \in \mathbb{Z}$. Osserviamo allora che $\forall\, x \in \mathbb{Z}$, $\phi(x) = \phi(x \cdot 1) = x\,\phi(1) = xm$. Ne segue che l'applicazione $\theta : \mathrm{End}(\mathbb{Z}) \longrightarrow \mathbb{Z}$ definita con $\phi \longmapsto m$ è un isomorfismo di anelli.

(2) Fissiamo $m \in \mathbb{N}^*$ e consideriamo un arbitrario endomorfismo $\xi \in \mathrm{End}(\mathbb{Z}_m)$. Poniamo dunque e_m il generatore canonico di $\mathbb{Z}_m$ e quindi $c := \xi(e_m)$ la sua immagine tramite ξ. Allora l'applicazione $\theta_m : \mathrm{End}(\mathbb{Z}_m) \longrightarrow \mathbb{Z}_m$ definita con $\xi_m \longmapsto c$ un isomorfismo di anelli (ovviamente suriettiva ed facile verificare che $\ker\theta_m = \{0\}$).
QED

Lemma 8.4. *Consideriamo ora un gruppo abeliano G. Fissiamo un intero n e consideriamo l'omomorfismo $\mathrm{End}(G) \ni \mu_n \colon G \to G$, tale che: $\mu_n(x) = nx$. Allora l'applicazione $\Psi : \mathbb{Z} \to \mathrm{End}(G)$ definita con $n \mapsto \mu_n$ è un omomorfismo di anelli.*

Proof. Fissati arbitrari $n, m \in \mathbb{Z}$, dobbiamo dimostrare che:

1. $\Psi(n+m) = \mu_{n+m} = \mu_n + \mu_m = \Psi(n) + \Psi(m)$,
2. $\Psi(nm) = \mu_{nm} = \mu_n\mu_m = \Psi(n)\Psi(m)$;

ma ciò è vero perchè $\forall x \in G$ valgono:

- $\mu_{n+m}(x) = (n+m)x = nx + mx = \mu_n(x) + \mu_m(x)$;
- $\mu_{nm}(x) = nmx = n(mx) = n\Big(\mu_m(x)\Big) = \mu_n\Big(\mu_m(x)\Big) = \mu_n\mu_m(x)$.

QED

Osserviamo inoltre che:

- $\mathbb{Z} \ni 0 \mapsto \mu_0 = 0 \in \mathrm{End}(G)$ (per 1.),
- $\mathbb{Z} \ni 1 \mapsto \mu_1 = id \in \mathrm{End}(G)$.

Lemma 8.5. *Se $\ker\Psi \neq 0$, allora $\ker\Psi = m\mathbb{Z}$, dove m è il più piccolo intero positivo tale che $m \in \ker\Psi$. Di conseguenza, $\Psi(\mathbb{Z}) \cong \mathbb{Z}_m$.*

Proof. E' immediato dato che tutti i sottogruppi di $\mathbb{Z}$ devono essere del tipo $m\mathbb{Z}$. Ora per vedere che $\Psi(\mathbb{Z}) \cong \mathbb{Z}_m$ basta applicare il 1^o Teorema di Omomorfismo. QED

Teorema 8.6. *Dimostrare che un gruppo abeliano G è decomponibile se e solo se l'anello $End(G)$ ha idempotenti*[4] *non-banali.*

Dimostrazione. Sia $G = A \oplus B$, con $A \neq 0$ e $B \neq 0$. Sia $e : G \to G$ l'endomorfismo definito con $e(a, b) = (a, 0)$. Ovviamente, $e^2 = e$, $e \neq 0$ e $e \neq id_G$. Quindi, $e \in \mathrm{End}(G)$ è un idempotente non banale.

Supponiamo ora che $e \in \mathrm{End}(G)$ sia un idempotente non banale. Allora $A = \ker e \neq G$. Poniamo $B = e(G)$. Se $z \in A \cap B$, allora $z = e(x)$ per qualche $x \in G$. Quindi $e(z) = e^2(x) = e(x) = z$. D'altra parte, $e(z) = 0$. Quindi, $z = 0$. Pertanto, $A \cap B = 0$. Se $x \in G$, allora $x - e(x) \in A$ in quanto $e(x - e(x)) = e(x) - e^2(x) = 0$. Quindi, da $x = e(x) + (x - e(x))$ deduciamo che $G = A + B$. Questo dimosra che $G \cong A \oplus B$. QED

8.3 I numeri p-adici

Adesso descriveremo l'anello $A = End(\mathbb{Z}(p^\infty))$. Sia $\alpha \in End(\mathbb{Z}(p^\infty))$. Allora

$$\alpha(c_n) = k_n c_n \tag{1}$$

e la successione $k = (k_n)$ soddisfa

$$k_{n+1} \equiv k_n (mod\, p^n). \tag{$*$}$$

Viceversa, ogni successione $k = (k_n)$ che soddisfa (*) definisce un endomorfismo α_k con (1). Per due successioni $k = (k_n)$ e $k' = (k'_n)$ poniamo $k \equiv k'$ se $k_n \equiv k'_n (mod\, p^n)$ per ogni n. È chiaro che due successioni k e k' definiscono lo stesso endomorfismo se e solo se $k \equiv k'$. Sia B il sottoinsieme dell'anello $\mathbb{Z}^{\mathbb{N}}$ determinato dalla condizione (*). Allora B è un sottoanello e la posizione $\mu(k) = \alpha_k$ definisce un omomorfismo suriettivo di anelli $\mu : B \to A$. Sia J l'ideale $p\mathbb{Z} \times p^2\mathbb{Z} \times \ldots \times p^n\mathbb{Z} \times \ldots$ dell'anello $\mathbb{Z}^{\mathbb{N}}$ e $I = J \cap B$. Allora I è un ideale di B per il quale $k - k' \in I$ se e solo se $k \equiv k'$. In altre parole, $I = \ker \mu$.

Applicando adesso il teorema dell'omomorfismo otteniamo il seguente isomorfismo $A \cong B/I$.

L'anello B/I sarà chiamato *anello dei numeri p-adici interi* e denotato con $\mathbb{J}_p$. Ovvamente, l'anello $\mathbb{J}_p$ si può "vedere" anche come il sottoanello $\bar{B}$ del quoziente $\mathbb{Z}^{\mathbb{N}}/J \cong \mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \ldots \times \mathbb{Z}_{p^n} \times \ldots$ definito con

$$\bar{B} = \{x = (x_n) \in \prod_n \mathbb{Z}_{p^n} : \varphi_n(x_{n+1}) = x_n\},$$

dove $\varphi_n : \mathbb{Z}_{p^{n+1}} \to \mathbb{Z}_{p^n}$ è l'omomorfismo canonico con nucleo l'ideale principale (p^n) dell'anello $\mathbb{Z}_{p^{n+1}}$.

Lemma 8.7. *$\mathbb{J}_p$ è un dominio.*

Dimostrazione. Se $\alpha \in \mathbb{J}_p$ e $\alpha \neq 0$ allora esiste n tale che $\alpha(c_n) \neq 0$. Chiaramente $\alpha(c_m) \neq 0$ anche per tutti $m \geq n$. Ora sia $\beta \in \mathbb{J}_p$ e $\beta \neq 0$. Non è retsrittivo pensare che esiste un m tale che $\alpha(c_m) \neq 0$ e $\beta(c_m) \neq 0$, quindi

$$p^m \not| k_m \text{ e } p^m \not| k'_m. \tag{2}$$

Ora non è difficile vedere che $\alpha(\beta(c_{2m})) = k_m k'_m c_{2m} \neq 0$. Infatti, dalle congruenze $k_m \equiv_{p^m} k_{2m}$ e $k'_m \equiv_{p^m} k'_{2m}$ si ricava, moltiplicando, $k_m k'_m \equiv_{p^{2m}} k_{2m} k'_{2m}$. Ora (2) implica $p^{2m} \not| k_{2m} k'_{2m}$, e quindi $\alpha(\beta(c_{2m})) \neq 0$. QED

Sia $L = \{\alpha \in A : \alpha(c_1) = 0\}$. Allora

Esercizio 8.8. *$\mathbb{J}_p^* = \mathbb{J}_p \setminus L$.*

Suggerimenti. Sia $\alpha \in \mathbb{J}_p$ e $\alpha \notin L$. Allora $\alpha(c_1) = k_1 c_1 \neq 0$, quindi p non divide k_1. Pertanto esiste k'_1 con $k_1 k'_1 \equiv 1 (mod\, p)$. Supponiamo che per qualche $n > 1$ abbiamo gia trovato $k'_1, \ldots, k'_n$ tali che vale (*) per k'_i con $i = 1, \ldots, n-1$ e

$$k_i k'_i \equiv 1 (mod\, p^i) \text{ per } i = 1, \ldots, n. \tag{3}$$

Allora cercheremo k'_{n+1} della forma $k'_{n+1} = k'_n + p^n t$. Per (*) applicata alla successione k abbiamo $k_{n+1} = k_n + ap^n$ e per (3) si ha $k_n k'_n = 1 + bp^n$ con opportuni $a, b \in \mathbb{Z}$. Quindi

$$k_{n+1} k'_{n+1} \equiv_{p^{n+1}} k_n k'_n + p^n(ak'_n + tk_n) \equiv_{p^{n+1}} 1 + p^n(ak'_n + k_n t + b).$$

Ora essendo k_n congruro a k_1 modulo p si ha $p \not| k_n$, quindi si può risolvere la congruenza $ak'_n + k_n t + b \equiv_p 0$. Allora, con t ricavato da questa congruenza, avremo $k_{n+1} k'_{n+1} \equiv_{p^{n+1}} 1$. Così abbiamo costruito un elemento $k' = (k'_n) \in B$ tale che $kk' \equiv 1$. Quindi l'endomorfismo $\beta = \mu(k')$ soddisfa $\beta\alpha = 1$. QED

[4] [4, Definition 10.19].

Lemma 8.9. *Sia $\alpha \in L$ con $\alpha(c_i) = 0$ per $i = 1, \ldots, n$ e $\alpha(c_{n+1}) \neq 0$. Allora $\alpha = p^n\beta$ per qualche $\beta \in \mathbb{J}_p^*$.*

SUGGERIMENTI. Siano $\alpha = \mu(k)$ e $\beta = \mu(k')$ con $k, k' \in B$. Poichè siamo liberi a scegliere k_i modulo p^i, possiamo prendere ovviamente $k_1 = \ldots = k_n = 0$. Ora (*) ci dà $p^n | k_M$ per tutti $m > n$ e p^{n+1} non divide k_{n+1} per $\alpha(c_{n+1}) \neq 0$. Poniamo $k'_i = k_{n+1}p^{-n}$. Allora k'_1 non si divide a p e $k'_n \equiv k'_{n+1} (mod\, p^n)$. Quindi $k' = (k'_n)$ determina una successione di B che definisce un automorfismo $\beta = \mu(k')$. Ovvamente $\alpha = p^n\beta$. QED

Esercizio 8.10. *$L = p\mathbb{J}_p$ è un ideale principale.*

SUGGERIMENTI. Sia $\alpha \in L$, allora $\alpha(c_1) = 0$. Supponiamo che $\alpha(c_i) = 0$ per $i = 1, \ldots, n$ e $\alpha(c_{n+1} \neq 0$. Per il Lemma 8.9 sappiamo che $\alpha = p^n\beta$ per qualche $\beta \in \mathbb{J}_p^*$. QED

Sia $\alpha \neq 0$, e sia $\alpha = p^{v(\alpha)}\beta$ la rappresentazione determinata dal Lemma 8.9.

Esercizio 8.11. *Dimostrare che per la funzione $v : \mathbb{J}_p \setminus \{0\} \to \mathbb{N}$ così definita si ha $v(\alpha) \leq v(\beta)$ se e solo se $\alpha|\beta$.*

Esercizio 8.12. *Dimostrare che per $\alpha, \beta \in \mathbb{J}_p \setminus \{0\}$ sia ha*

$$v(\alpha\beta) = v(\alpha) + v(\beta). \tag{4}$$

Dare una dimostrazione del Lemma 8.7 basata sull'equazione (4).

Esercizio 8.13. *Dimostrare che $p^n\mathbb{J}_p$ sono gli unici ideali non-nulli di $\mathbb{J}_p$.*

SUGGERIMENTI. Sia I un ideale non-nullo e per $\alpha \in I$, $\alpha \neq 0$, sia $\alpha = p^{v(\alpha)}\beta$ la rappresentazione determinata dal Lemma 8.9. Scegliamo $\alpha_0 \in I$ non-nullo con $v(\alpha_0)$ minimo. Allora $I = (\alpha_0) = (p^{v(\alpha_0)})$. QED

Teorema 8.14. *$\mathbb{J}_p$ è un dominio euclideo.*

DIMOSTRAZIONE. Notiamo che per $\alpha, \beta \in \mathbb{J}_p \setminus \{0\}$ si ha sempre o $\alpha|\beta$ o $\beta|\alpha$. Non è difficile verificare che la funzione $v : \mathbb{J}_p \setminus \{0\} \to \mathbb{N}$ definita sopra serve per verficare la condizione nella definizione di dominio euclideo. QED

Teorema 8.15. *$\mathbb{J}_p/p\mathbb{J}_p \cong \mathbb{Z}_p$. Di conseguenza il gruppo $(\mathbb{J}_p, +)$ è indecomponibile.*

SUGGERIMENTI. L'isomorfismo segue dal teorema dell'omomorfismo applicato all'omomorfismo suriettivo $\rho : \mathbb{J}_p \to \mathbb{Z}_p$ definito con $\rho(\alpha) := \alpha(c_1)$ per ogni $\alpha \in \mathbb{J}_p$. Ora supponiamo che $\mathbb{J}_p = A \oplus B$. Allora $p\mathbb{J}_p = pA \oplus pB$ e quindi $\mathbb{J}_p/p\mathbb{J}_p \cong A/pA \oplus B/pB$. Poiche $\mathbb{J}_p/p\mathbb{J}_p \cong \mathbb{Z}_p$ ed entrambi A/pA e B/pB sono somme dirette di copie di $\mathbb{Z}_p$, concludiamo che o $A/pA = 0$ o $B/pB = 0$. Supponiamo che $A/pA = 0$. Ora dimostreremo che anche $A = 0$. Infatti, $A/pA = 0$ implica $A = pA$ e quindi

$$A = p^n A \text{ per ogni } n \in \mathbb{N}. \tag{5}$$

Supponiamo ad assurdo che $A \neq 0$ e sia $\alpha \in A$, $\alpha \neq 0$. Per il Lemma 8.9 esiste $\beta \in \mathbb{J}_p^*$ e $n \in \mathbb{N}$ con $\alpha = p^n\beta$. Adesso (5) implica $\alpha \in p^{n+1}A$ e quindi $p^n\beta \in p^{n+1}A$ e di conseguenza $\beta \in pA$ perchè A è un dominio (Lemma 8.7) – assurdo. QED

Esercizio 8.16. *Dimostrare che $(\mathbb{J}_p, +)$ è indecomponibile usando che l'anello $End(\mathbb{J}_p, +)$ è isomorfo all'anello $\mathbb{J}_p$.*

SUGGERIMENTI. Ovviamente, il gruppo $\mathbb{Z}(p^\infty)$ è indecomponibile, quindi l'anello $\mathbb{J}_p = End(\mathbb{Z}(p^\infty))$ non ha idempotenti non banali per il Teorema 8.6. Per lo stesso teorema e per l'isomorfismo $\mathbb{J}_p \cong End(\mathbb{J}_p)$ concludiamo che $(\mathbb{J}_p, +)$ è indecomponibile. QED

Esercizio 8.17. *Dimostrare che se $\xi^p = 1$ per $\xi \in \mathbb{J}_p$ allora $\xi = 1$.*

Esercizio 8.18. *Sia G un gruppo divisibile e sia $\{G_n\}_{n=1}^\infty$ una famiglia di sottogruppi di G tali che*

(a) $G_1 \leq G_2 \leq \ldots \leq G_n \leq \ldots$;

(b) G_n è un sottogruppo pienamente invariante di G (e di conseguenza anche di G_{n+1}) per ogni $n \in \mathbb{N}^*$;

(c) G risulta limite diretto della famiglia, cioè $G = \varinjlim G_n$.

Allora

(i) per ogni $n \in \mathbb{N}^*$ la restrizione $\varrho_n \colon \mathrm{End}(G_{n+1}) \longrightarrow \mathrm{End}(G_n)$, definita con $\xi_{n+1} \longmapsto \xi_{n+1}|_{G_n}$ è un omomorfismo di anelli;

(ii) gli omomorfismi ϱ_n danno luogo ad un omomorfiso di anelli che risulta un isomorfismo:

$$\mathrm{End}(G) \cong \varprojlim \Big(\mathrm{End}(G_n), \varrho_n\Big), \tag{1}$$

SUGGERIMENTI. (a)

(b) Per definire l'omomorfismo $\rho : \mathrm{End}(G) \to \varprojlim \Big(\mathrm{End}(G_n), \varrho_n\Big)$ applicare ... alla famiglia di omomorfismi $\rho_n : \mathrm{End}(\varinjlim G_n) \to \mathrm{End}(G_n)$, definiti dal fatto che essendo G_n è un sottogruppo pienamente invariante di G per ogni n, per ogni $\varphi \in \mathrm{End}(G)$ vale $\varphi(G_n) \leq G_n$. Questo definisce l'endomorfismo restrizione $\varphi \restriction_{G_n} \colon G_n \to G_n$. QED

References

[1] D. Dikranjan, Appunti di Topologia 2, 2006/2007.

[2] D. Dikranjan, Introduction to Topological Groups, 2008.

[3] D. Dikranjan, Iv. Prodanov e L. Stoyanov, *Topological Groups: Characters, Dualities and Minimal Group Topologies,* Pure and Applied Mathematics, Vol. **130**, Marcel Dekker Inc., New York-Basel, 1989, pp. 287+x.

[4] D. Dikranjan e M. S. Lucido, *Aritmetica e Algebra*, Liguori, Naples, 2007, pp. xvi +399.

[5] L. Fuchs, *Infinite Abelian groups*, vol. I, Academic Press New York and London, 1973.