Sia R un anello. Una successione di omomorfismi di R-moduli

$$\ldots \longrightarrow \; A_{i-1} \; \stackrel{f_{i-1}}{\longrightarrow} \; A_i \; \stackrel{f_i}{\longrightarrow} \; A_{i+1} \; \longrightarrow \longrightarrow \ldots$$

si dice *esatta in* A_i se l'immagine di f_{i-1} è uguale al nucleo di f_i. La successione si dice *esatta* se è esatta in ogni A_i. Una successione esatta si dice *corta* se ha la forma

$$0 \; \longrightarrow \; A \; \longrightarrow \; B \; \longrightarrow \; C \; \longrightarrow \; 0.$$

Ad ogni due R-moduli A e C il prodotto cartesiano $A \times C$ è associata la successione esatta corta

$$0 \; \longrightarrow \; A \; \stackrel{i}{\longrightarrow} \; A \times C \; \stackrel{p}{\longrightarrow} \; C \; \longrightarrow \; 0,$$

dove $i(a) = (a, 0)$ per ogni $a \in A$ e $p(a, c) = c$ per ogni $(a, c) \in A \times C$. Questo è un esempio di una succesione esatta *spezzata*. In generale, una successione esatta $0 \to A \to B \to C \to 0$ si dice *spezzata* se esistono un isomorfismo $\varphi : B \longrightarrow A \times C$ e un diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \| & & \downarrow \varphi & & \| & & \\ 0 & \longrightarrow & A & \stackrel{i}{\longrightarrow} & A \times C & \stackrel{p}{\longrightarrow} & C & \longrightarrow & 0. \end{array}$$

In realtà, nella definizione sopra non è necessario richiedere che φ sia un isomorfismo. La seguente proposizione dimostra che questo è automatico.

Proposizione 1. *Supponiamo che nel diagramma commutativo di R-moduli*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \stackrel{f}{\longrightarrow} & B & \stackrel{g}{\longrightarrow} & C & \longrightarrow & 0 \\ & & \| & & \downarrow \varphi & & \| & & \\ 0 & \longrightarrow & A & \stackrel{f'}{\longrightarrow} & B' & \stackrel{g'}{\longrightarrow} & C & \longrightarrow & 0. \end{array}$$

le due righe siano esatte. Allora φ è un isomorfismo.

Dimostrazione. La mappa φ è iniettiva: sia $b \in B$ con $\varphi(b) = 0$. Allora anche $g(b) = g'(\varphi(b)) = 0$. In altre parole $b \in \ker g = \operatorname{im} f$. Sia $a \in A$ con $f(a) = b$. Allora $f'(a) = \varphi(f(a)) = \varphi(b) = 0$. Siccome f' è iniettiva, abbiamo che $a = 0$ e quindi $b = f(a) = 0$.

Per vedere che la mappa φ è suriettiva, sia $b' \in B'$ arbitrario. Sia $c = g'(b')$. Siccome g è suriettiva, esiste $b \in B$ con $g(b) = c$. Abbiamo che $g'(\varphi(b)) = g(b) = c$. In altre parole, gli elementi b' e $\varphi(b)$ di B' hanno la stessa immagine in C. Questo vuol dire che $b' - \varphi(b)$ appartiene al nucleo di g. Per l'esattezza della successione abbiamo quindi che $b' - \varphi(b) \in \operatorname{im} f'$. Sia $a \in A$ con $f'(a) = b' - \varphi(b)$.

Adesso consideriamo l'elemento $f(a) - b$ di B e calcoliamo la sua immagine in B': si ha che $\varphi(f(a) + b) = \varphi(f(a)) + \varphi(b) = f'(a) + \varphi(b) = b' - \varphi(b) + \varphi(b) = b'$ come richiesto.

Il seguente criterio è utile.

Proposizione 2. *Sia R un anello e sia*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

una successione esatta di R-moduli. Le seguenti affermazioni sono equivalenti:

(a) La successione si spezza;
(b) Esiste un omomorfismo $h : B \longrightarrow A$ con $h \cdot f = \mathrm{id}_A$;
(c) Esiste un omomorfismo $k : C \longrightarrow B$ con $g \cdot k = \mathrm{id}_C$.

Proof. "(b) $\Rightarrow$ (a)" Definiamo $\varphi : B \longrightarrow A \times C$ tramite $\varphi(b) = (h(b), g(b))$. Poiché $\varphi(f(a)) = (h(f(a)), g(f(a))) = (a, 0) = i(a)$ e $p(\varphi(b)) = g(b)$ il diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \varphi} & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & A \times C & \xrightarrow{p} & C & \longrightarrow & 0. \end{array}$$

commuta, come richiesto.

"(a) $\Rightarrow$ (c)" Supponiamo che la succesione si spezzi. Allora sappiamo che il diagramma precedente è commutativo. Definiamo $k(c) = \varphi^{-1}(0, c)$. Siccome $g = p\varphi$, è ovvio che k è un omomorfismo che soddisfa $g \cdot k = \mathrm{id}_C$.

"(c) $\Rightarrow$ (b)" Per ogni $b \in B$ abbiamo che $b - k(g(b))$ appartiene al nucleo di g e per l'esattezza della successione, $b - k(g(b))$ appartiene quindi a $\operatorname{im} f$. Sia $a \in A$ l'unico elemento con $f(a) = b - k(g(b))$. Allora la mappa $h : B \longrightarrow A$ definita da $h(b) = a$ è un omomorfismo. Verifichiamo ora che $h \cdot f = \mathrm{id}_A$. Sia $a \in A$. Allora $h(f(a)) = a'$, dove a' è l'unico elemento di A con $f(a') = f(a) - k(g(f(a)))$. Poiché $g(f(a)) = 0$, si ha che $f(a') = f(a)$. Dall'iniettività di f segue che $a' = a$ come richiesto.

Lemma 3. *Sia p un numero primo. Per ogni gruppo abeliano finito A abbiamo un isomorfismo*

$$A \cong P \times Q$$

dove P è un gruppo di ordine una potenza di p e Q è un gruppo di ordine non divisibile per p.

Proof. Scriviamo $\#A = p^k m$ dove p non divide m. Per il Teorema di Lagrange abbiamo quindi che $(p^k m) \cdot a = 0$ per ogni $a \in A$. Sia $P = \{a \in A : \text{l'ordine di } a \text{ è una potenza di } p\}$ e sia $Q = \{a \in A : p \text{ non divide } \mathrm{ord}(a)\}$. Facciamo vedere che la mappa naturale

$$P \times Q \longrightarrow A,$$

data da $(b, c) \mapsto b + c$, è un isomorfismo di gruppi. È chiaro che si tratta di un omomorfismo. Se (b, c) sta nel nucleo, allora $b = -c$ è contenuto in $P \cap Q = \{0\}$. La mappa è quindi iniettiva. Per vedere che la mappa è anche suriettiva, procediamo come segue: per Bézout esistono $\lambda, m \in \mathbf{Z}$ con $\lambda p^k + \mu m = 1$. Sia $a \in A$ un elemento arbitrario. Scriviamo $a = 1 \cdot a = \mu m a + \lambda p^k a$. L'elemento $b = \mu m a$ appartiene a P mentre $c = \lambda p^k a$ appartiene

a Q. Questo segue dal fatto che $p^k b = p^k(\mu m a) = \mu(p^k m)a = 0$ e $mc = m(\lambda p^k a) = \lambda(p^k m)a = 0$.

Questo conclude la dimostrazione del lemma.

Lemma 4. *Siano q, m interi positivi e supponiamo che la successione*

$$0 \longrightarrow \mathbf{Z}_q \xrightarrow{f} A \xrightarrow{g} \mathbf{Z}_m \longrightarrow 0$$

sia esatta. Allora, se q annulla A, la successione si spezza.

Proof. Per la Proposizione 2 basta costruire un omomorfismo $k : \mathbf{Z}_m \longrightarrow A$ con la proprietà che $g \cdot k$ è l'identità su $\mathbf{Z}_m$. Siccome $\mathbf{Z}_m$ è un gruppo ciclico generato da $\overline{1}$, un tale omomorfismo k è determinato da $a = k(\overline{1})$. Siccome $g(a) = g(k(\overline{1})) = \overline{1}$, l'elemento $a \in A$ deve avere lo stesso ordine di $\overline{1}$, vale a dire m. Viceversa, per ogni $a \in A$ di ordine m con $g(a) = \overline{1}$, la mappa $k : \mathbf{Z}_m \longrightarrow A$ definita da $k(\overline{1}) = a$ è un omomorfismo ben definito con la proprietà che $g \cdot k = \mathrm{id}_{\mathbf{Z}_m}$.

Dunque, per costruire l'omomorfismo k, ci resta da esibire un elemento $a \in A$ di ordine m con $g(a) = \overline{1}$. L'immagine $f(\mathbf{Z}_q)$ è un sottogruppo ciclico di A di ordine q. Sia y un generatore. Sia $x \in A$ un qualsiasi elemento di A con $g(x) = \overline{1}$. Allora mx appartiene al nucleo di g e per l'esattezza della successione abbiamo che $\ker g = \mathrm{im}\, f = \langle y \rangle$ e quindi $mx = ky$ per un $k \in \mathbf{Z}$.

Poiché A è annullato da q, anche $\mathbf{Z}_m$ lo è. Questo implica che m divide q. Poiché q annulla A, possiamo quindi scrivere

$$0 = qx = \frac{q}{m} mx = \frac{q}{m} ky.$$

Poiché y ha ordine q, questa uguaglianza implica che q divide $\frac{q}{m}k$ e quindi m divide k. Verifichiamo che

$$a = x - \frac{k}{m} y$$

è l'elemento cercato. Abbiamo che $g(a) = g(x) - \frac{k}{m} g(y)$. Poiché $y \in \mathrm{im}\, f$, abbiamo che $g(y) = 0$ e quindi $g(a) = g(x) = \overline{1}$. L'ordine di a è dunque divisible per m. Dal fatto che

$$ma = m(x - \frac{k}{m} y) = mx - ky = 0,$$

segue che l'ordine di a *è uguale* a m come richiesto.

Teorema 5. *Sia A un gruppo abeliano finito. Allora A è prodotto di gruppi ciclici.*

Proof. Consideriamo prima il caso in cui l'ordine di A è una potenza di un numero primo p. Procediamo per induzione rispetto a $\#A$. Se A ha ordine p, allora A è ciclico e il teorema vale. Se $\#A > p$, allora scegliamo un elemento $a \in A$ di ordine massimale q. Allora q annulla A. Abbiamo la seguente successione esatta:

$$0 \longrightarrow \langle a \rangle \longrightarrow A \longrightarrow A\,/\langle a \rangle \longrightarrow 0.$$

Per induzione il teorema vale per il gruppo più piccolo $A/\langle a\rangle$. Abbiamo quindi la seguente successione esatta

$$0 \longrightarrow \langle a\rangle \longrightarrow A \xrightarrow{g} \prod_{i=1}^{t} \mathbf{Z}_{m_i} \longrightarrow 0. \qquad (*)$$

Per ogni i con $1 \leq i \leq t$ definiamo

$$A_i = g^{-1}(\{0\} \times \ldots \times \{0\} \times \mathbf{Z}_{m_i} \times \{0\} \times \ldots \times \{0\}),$$

e indichiamo con $\pi_i : \prod_{i=1}^{t} \mathbf{Z}_{m_i} \longrightarrow \mathbf{Z}_{m_i}$ è la proiezione sull'i-esima coordinata. Allora A_i contiene a e la successione

$$0 \longrightarrow \langle a\rangle \longrightarrow A_i \xrightarrow{\pi_i g} \mathbf{Z}_{m_i} \longrightarrow 0 \qquad (**)$$

è esatta. Infatti, se $a \in A_i$ appartiene al nucleo di $\pi_i g$, allora $g(a)$ ha *tutte* le coordinate uguali a zero e quindi a appartiene a $\ker g = \langle a\rangle$.

Siccome $\langle a\rangle$ è ciclico di ordine q e $A_i \subset A$ è annullato da q, possiamo applicare il Lemma 4. Vediamo che per ogni i con $1 \leq i \leq t$ la successione $(**)$ si spezza. Per la Proposizione 2 esistono quindi omomorfismi $\varphi_i : \mathbf{Z}_{m_i} \longrightarrow A_i$ con la proprietà che $\pi_i g \varphi_i$ è l'identità su $\mathbf{Z}_{m_i}$. Adesso 'incolliamo' gli omomorfismi φ_i e definiamo l'omomorfismo $\varphi : \prod_{i=1}^{t} \mathbf{Z}_{m_i} \longrightarrow A$ mediante

$$\varphi(x_1, \ldots, x_t) \;=\; \sum_{i=1}^{t} \varphi_i(x_i).$$

Affermiamo che $g\varphi$ è l'identità su $\prod_{i=1}^{t} \mathbf{Z}_{m_i}$. Per verifichare questo, basta controllare che le coordinate di $(x_1, \ldots, x_t)$ e $g\varphi(x_1, \ldots, x_t)$ sono uguali, ossia $\pi_j g\varphi(x_1, \ldots, x_t) = x_j$ per ogni j. Infatti, abbiamo che

$$\pi_j g\varphi(x_1, \ldots, x_t) \;=\; \sum_{i=1}^{t} \pi_j g\varphi_i(x_i) \;=\; \pi_j g\varphi_j(x_j) \;=\; x_j,$$

ove la seconda ugualianza segue dal fatto che $\varphi_i(x_i)$ sta in A_i e quindi $g\varphi_i(x_i)$ appartiene al gruppo $\{0\} \times \ldots \times \{0\} \times \mathbf{Z}_{m_i} \times \{0\} \times \ldots \times \{0\}$. Questo implica che la proiezione π_j manda $g\varphi_i(x_i)$ in zero per $i \neq j$.

Il criterio della Proposizione 2 implica adesso che la successione $(*)$ si spezza e quindi

$$A = \langle a\rangle \times \prod_{i=1}^{t} \mathbf{Z}_{m_i}$$

è un prodotto di gruppi ciclici.

Adesso abbiamo dimostrato il teorema per gruppi di ordine una potenza di un numero primo. Poiché il Lemma 3 ci permette di scrivere ogni gruppo abeliano finito come prodotto di tali gruppi, concludiamo che il teorema vale per ogni gruppo abeliano finito, come richiesto.