# MODULE FINIT GENERATE PESTE INELE PRINCIPALE

## 1. Module libere

*În acest curs, dacă nu se menţionează altfel, inelele sunt commutative şi unitare cu* $1 \neq 0$.

Pentru început vom discuta despre module libere peste inele principale (pe scurt, PID) şi despre submodulele lor. De ce ne interesează acestea? Pentru că orice modul este izomorf cu un modul factor al unui modul liber. Mai precis:

**Proposition 1.1.** *Fie $R$ un inel şi $M$ un $R$-modul. Atunci există un $R$-modul liber $F$ şi un morfism surjectiv de $R$-module $\varphi : F \to M$.*

*Proof.* Fie $(x_i)_{i\in I}$ un sistem de generatori pentru $M$ şi $F = R^{(I)}$. Definim $\varphi(e_i) = x_i$ pentru orice $i \in I$. □

**Corollary 1.2.** *Orice modul este izomorf cu un modul factor al unui modul liber.*

*Proof.* Se foloseşte propoziţia anterioară şi teorema fundamentală de izomorfism pentru module. □

Deoarece $M \simeq F/L$, unde $L$ este submodul al lui $F$, ne întrebăm acum ce se poate spune despre submodulele modulelor libere. O observaţie imediată este aceea că submodulele modulelor libere nu sunt neapărat module libere. De exemplu, orice ideal al unui inel $R$ este submodul al modulului liber $R$. Însă un ideal $\neq (0)$ este $R$-modul liber dacă şi numai dacă este ideal principal generat de un non-divizor al lui zero. Deci nu orice ideal este modul liber.

**Examples 1.3.** (i) $R = \mathbb{Z}[X]$, $I = (2, X)$;
(ii) $R = \mathbb{Z}_6$, $I = \hat{2}\mathbb{Z}_6$. (În acest caz $I$ este chiar sumand direct.)

**Proposition 1.4.** *Fie $R$ un inel comutativ unitar cu proprietatea că orice submodul al unui modul liber este liber. Atunci $R$ este PID.*

*Proof.* Să arătăm că $R$ este inel integru. Fie $a \in R$, $a \neq 0$. Considerăm $I = (a)$ şi acesta trebuie să fie generat de un non-divizor al lui zero. Rezultă imediat că $a$ este non-divizor al lui zero, deci orice element nenul al lui $R$ este non-divizor al lui zero. □

Şi mai important încă, dacă inelul este principal, atunci orice submodul al unui modul liber este liber. Începem prin a demonstra cazul în care modulul liber este de rang finit.

**Theorem 1.5.** *Fie $R$ PID, $F$ $R$-modul liber de rang $n$ şi $L$ submodul al lui $F$. Atunci $L$ este liber de rang $\leq n$.*

*Proof.* Vom face inducţie după $n$.

Dacă $n = 1$, atunci $F \simeq R$ şi deci $L$ este izomorf cu un ideal al lui $R$. Cum $R$ este PID, rezultă că $L = 0$ sau $L \simeq R$.

Dacă $n > 1$, fie $e_1, \dots, e_n$ bază pentru $F$. Aşadar $F = Re_1 \dotplus \cdots \dotplus Re_n$ (sumă directă internă). Fie $F' = Re_1 \dotplus \cdots \dotplus Re_{n-1}$. Avem două cazuri:
(i) $L \subset F'$; se aplică ipoteza de inducţie.
(ii) $L \not\subset F'$; considerăm $L \cap F' \subset F'$ şi din ipoteza de inducţie deducem că $L \cap F'$ este liber de rang $m - 1 \leq n - 1$. Să observăm că $0 \neq (L + F')/F' \leq F/F' \simeq Re_n$, deci $(L + F')/F'$ este liber de rang 1.

Fie $f_1, \dots, f_{m-1}$ bază în $L \cap F'$ şi $f_m \in L$ astfel încât $\hat{f}_m$ este bază în $(L + F')/F'$. Se arată acum că $f_1, \dots, f_m$ este bază în $L$. □

Această demonstraţie se poate extinde la cazul general în care modulul liber nu mai este neapărat de rang finit.

**Theorem 1.6.** *Fie $R$ PID, $F$ $R$-modul liber şi $L$ un submodul al lui $F$. Atunci $L$ este liber de rang* $\leq \operatorname{rang} F$.

*Proof.* Fie $(e_i)_{i \in I}$ o bază a lui $F$. Vom considera că $I$ este bine ordonată, adică este total ordonată şi orice submulţime nevidă a sa are un cel mai mic element. Pentru orice $i \in I$ definim $F'_i = \bigoplus_{j<i} Re_j$ şi $F_i = \bigoplus_{j \leq i} Re_j = F'_i \oplus Re_i$. Să observăm că $F = \bigcup_{i \in I} F_i$. Definim $L'_i = L \cap F'_i$ şi $L_i = L \cap F_i$. Deoarece $L'_i = L_i \cap F'_i$ avem că $L_i/L'_i = L_i/L_i \cap F'_i \simeq (L_i + F'_i)/F'_i \leq F_i/F'_i \simeq Re_i$. Acum există două posibilităţi: $L_i = L'_i$ sau $L_i = L'_i \oplus Rf_i$ unde $\hat{f}_i$ este bază în $L_i/L'_i$.

Arătăm că $L$ este modul liber de bază $(f_i)$. De aici va rezulta imediat că $\operatorname{rang} L \leq \operatorname{rang} F$.

Cum $F = \bigcup_{i \in I} F_i$ orice element $x \in F$ se găseşte într-un $F_i$. Deoarece $I$ este bine ordonată există un cel mai mic indice $i \in I$ cu proprietatea că $x \in F_i$ şi notăm acest indice cu $i(x)$. Să observăm că dacă $x \in L'_i$, atunci $i(x) < i$. Fie $L^*$ submodulul lui $L$ generat de toţi $f_i$. Să presupunem că $L^* \subsetneq L$. Fie $j$ cel mai mic element al mulţimii $\{i(x) : x \in L - L^*\}$ şi fie $y \in L - L^*$ cu $i(y) = j$. Vom avea $y \in L_j$ (deoarece $i(y) = j$) şi astfel $y = x' + af_j$ cu $x' \in L'_j$ şi $a \in R$. De aici obţinem $x' = y - af_j \in L'_j$ şi $x' \notin L^*$, altfel $y \in L^*$ (deoarece $f_j \in L^*$). Cum $i(x') < j$, am ajuns la o contradicţie. În concluzie, $L^* = L$, deci $(f_i)$ este un sistem de generatori pentru $L$.

Rămâne de demonstrat că $(f_i)$ este sistem liniar independent. Să presupunem că $a_1 f_{i_1} + \cdots + a_n f_{i_n} = 0$. Aranjăm indicii aşa încât $i_1 < \cdots < i_n$. Dacă $a_n \neq 0$, atunci $a_n f_{i_n} \in L'_{i_n} \cap Rf_{i_n} = \{0\}$, contradicţie. Deci $a_k = 0$ pentru orice $k = 1, \dots, n$. □

Folosindu-ne de forma diagonal-canonică (*Smith Normal Form*) a matricelor cu elemente într-un PID vom arăta că teorema 1.5 poate fi enunţată într-o formă mult mai precisă, şi anume:

**Theorem 1.7.** *Fie $R$ PID, $F$ $R$-modul liber de rang $n$ şi $L$ submodul al lui $F$. Atunci există o bază $f_1, \dots, f_n$ a lui $F$ şi $d_i \in R$, $d_i \neq 0$, $1 \leq i \leq m \leq n$ cu $d_1 \mid \cdots \mid d_m$ astfel încât $d_1 f_1, \dots, d_m f_m$ să fie bază pentru $L$.*

*Proof.* Fie $x_1, \dots, x_n$ bază a lui $F$ şi $y_1, \dots, y_m$ bază a lui $L$. Scriem $y_i = \sum_{j=1}^n a_{ij} x_j$, $i = 1, \dots, m$. În acest fel am construit o matrice $A = (a_{ij}) \in M_{m \times n}(R)$. Această matrice este aritmetic echivalentă cu o matrice diagonal-canonică, deci există $U \in GL_m(R)$, $V \in GL_n(R)$ astfel încât $UAV = \operatorname{diag}(d_1, \dots, d_r)$, unde $d_i \neq 0$ şi $d_1 \mid \cdots \mid d_r$. Fie $D = \operatorname{diag}(d_1, \dots, d_r)$. Din $UAV = D$ rezultă $A = U^{-1}DV^{-1}$. Cum

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

obţinem

$$U \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = DV^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Fie

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} := V^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

şi

$$\begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix} := U \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}.$$

Din lema 1.8 rezultă că $e_1, \dots, e_m$ este bază în $L$ iar $f_1, \dots, f_n$ este bază în $F$. Deoarece

$$\begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix} := D \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}$$

vom avea că $e_i = d_i f_i$, $i = 1, \dots, r$ şi $r = m$ (altfel am avea vectori nuli în baza lui $L$). □

**Lemma 1.8.** *Fie $R$ un inel comutativ unitar, $M$ un $R$-modul, $x_1, \dots, x_n \in M$, $U \in GL_n(R)$, $U = (u_{ij})$ şi $y_i = \sum_{j=1}^{n} u_{ij} x_j$, $i = 1, \dots, n$. Atunci $x_1, \dots, x_n$ este sistem de generatori (sistem liniar independent, bază) dacă şi numai dacă $y_1, \dots, y_n$ este sistem de generatori (sistem liniar independent, bază).*

*Proof.* Exerciţiu. □

## 2. Anulatori şi torsiune

**Definition 2.1.** *Fie $R$ un inel comutativ şi unitar, $M$ un $R$-modul şi $x \in M$. Mulţimea* $\operatorname{Ann}_R(x) = \{a \in R : ax = 0\}$ *se numeşte* anulatorul *lui $x$. Mulţimea* $\operatorname{Ann}_R(M) = \bigcap_{x \in M} \operatorname{Ann}_R(x)$ *se numeşte* anulatorul *lui $M$.*

**Example 2.2.** Considerăm $\mathbb{Z}$-modulul $\mathbb{Z}_4$. Avem $\operatorname{Ann}_{\mathbb{Z}}(\hat{2}) = 2\mathbb{Z}$ şi $\operatorname{Ann}_{\mathbb{Z}}(\mathbb{Z}_4) = 4\mathbb{Z}$.

**Definition 2.3.** *Fie $R$ inel integru şi $M$ un $R$-modul. Un element $x \in M$ se numeşte* torsionat *dacă există $a \in R$, $a \neq 0$ astfel încât $ax = 0$. Mulţimea elementelor torsionate se notează cu $t(M)$ şi se numeşte* submodulul de torsiune *al lui $M$.*

**Example 2.4.** Considerăm $\mathbb{Z}$-modulul $\mathbb{Z} \times \mathbb{Z}_6$. Elementul $(0, \hat{3})$ este torsionat, deoarece $2(0, \hat{3}) = (0, \hat{0})$. Pe de altă parte, elementul $(1, \hat{3})$ nu este torsionat. Avem că $t(\mathbb{Z} \times \mathbb{Z}_6) = \{0\} \times \mathbb{Z}_6$.

**Remarks 2.5.** (i) $\operatorname{Ann}_R(x)$ este ideal al lui $R$.
(ii) $t(M)$ este submodul al lui $M$.
(iii) $x$ este torsionat dacă şi numai dacă $\operatorname{Ann}_R(x) \neq 0$.
(iv) $t(M/t(M)) = 0$.

**Definition 2.6.** *Fie $R$ inel integru şi $M$ un $R$-modul. Dacă $t(M) = M$, atunci $M$ se numeşte* modul de torsiune *iar dacă $t(M) = 0$, atunci $M$ se numeşte* modul fără torsiune.

**Example 2.7.** (i) Orice grup abelian finit este $\mathbb{Z}$-modul de torsiune.
(ii) Orice modul liber peste un inel integru este fără torsiune.
(iii) $\mathbb{Q}$ este $\mathbb{Z}$-modul fără torsiune, dar nu este liber.

**Proposition 2.8.** *Dacă $R$ este inel integru şi $M$ este un $R$-modul finit generat fără torsiune, atunci $M$ este izomorf cu un submodul al unui modul liber de rang finit.*

*Proof.* Fie $x_1, \dots, x_n$ un sistem de generatori (nenuli) pentru $M$. Deoarece $M$ este fără torsiune, submulţimile $\{x_i\}$ sunt liniar independente. Dintre submulţimile liniar independente ale mulţimii $\{x_1, \dots, x_n\}$ alegem una maximală, să zicem $\{x_1, \dots, x_m\}$, $1 \leq m \leq n$. Pentru orice $i \geq 1$ submulţimea $\{x_1, \dots, x_m, x_{m+i}\}$ este liniar dependentă, deci există $a_{i1}, \dots, a_{im}, a_i \in R$, $a_i \neq 0$, astfel încât $a_i x_{m+i} = \sum_{j=1}^m a_{ij} x_j$. Fie $a = a_1 \cdots a_{n-m}$. Atunci $a \neq 0$ şi $a x_{m+i} = \sum_{j=1}^m b_{ij} x_j$, unde $b_{ij} = (a/a_i) a_{ij} \in R$.

Aşadar $aM \subseteq F$, unde $F = Rx_1 + \cdots + Rx_m$. Evident $F$ este liber iar aplicaţia $f : M \to F$ dată prin $f(x) = ax$ este morfism injectiv. □

De aici se obţine că modulele finit generate şi fără torsiune peste un PID sunt libere.

**Corollary 2.9.** *Fie $R$ PID şi $M$ $R$-modul finit generat nenul. Dacă $M$ este fără torsiune, atunci $M$ este liber.*

*Proof.* Rezultă din propoziţia de mai sus folosind teorema 1.5. □

## 3. Teorema factorilor invarianţi

Mai întâi vom arăta că orice modul finit generat peste un PID este sumă directă finită de (sub)module ciclice.

**Lemma 3.1.** *Un $R$-modul este ciclic dacă şi numai dacă este izomorf cu un $R/I$, unde $I$ este ideal al lui $R$.*

*Proof.* $R/I$ este evident $R$-modul ciclic. Reciproc, fie $M = Rx$ un $R$-modul ciclic. Definim $\varphi : R \to Rx$ prin $\varphi(a) = ax$. Acesta este un morfism surjectiv de module şi $\ker \varphi = \operatorname{Ann}(x)$, deci $Rx \simeq R/\operatorname{Ann}(x)$. □

**Exercise 3.2.** (i) Fie $M, M'$ două $R$-module izomorfe. Arătaţi că $\operatorname{Ann}_R(M) = \operatorname{Ann}_R(M')$ şi $aM \simeq aM'$, pentru orice $a \in R$.

(ii) Arătaţi că dacă $I, J$ sunt ideale ale unui inel comutativ unitar $R$ care au proprietatea că $R/I \simeq R/J$ (izomorfism de $R$-module), atunci $I = J$.
(iii) Daţi exemple care să arate că proprietatea de la (ii) nu este adevărată pentru izomorfisme de inele.

**Theorem 3.3.** *Fie $R$ PID şi $M$ $R$-modul finit generat nenul. Există $x_1, \dots, x_n \in M$ astfel încât:*
*(i) $M = Rx_1 \dot{+} \cdots \dot{+} Rx_n$.*
*(ii) $R \supsetneq \operatorname{Ann}(x_1) \supseteq \cdots \supseteq \operatorname{Ann}(x_n)$.*

*Proof.* Deoarece $M$ este finit generat există $z_1, \dots, z_n \in M$ astfel încât $M = Rz_1 + \cdots + Rz_n$. Definim $\varphi : F = R^n \to M$ prin $\varphi(e_i) = z_i$. Deducem că $M \simeq F/L$, unde $L = \ker \varphi$. Din teorema 1.7 ştim că există o bază $f_1, \dots, f_n$ a lui $F$ şi $d_i \in R$, $d_i \neq 0$, $1 \leq i \leq m \leq n$ cu $d_1 \mid \cdots \mid d_m$ astfel încât $d_1 f_1, \dots, d_m f_m$ să fie bază pentru $L$. Fie $x_i = \varphi(f_i)$, $i = 1, \dots, n$.

Arătăm că $M = Rx_1 \dot{+} \cdots \dot{+} Rx_n$. Deoarece $\varphi$ este surjecţie rezultă $M = Rx_1 + \cdots + Rx_n$. Rămâne de arătat că suma este directă. Fie $y_i \in Rx_i$ cu $\sum_{i=1}^n y_i = 0$. Scriem $y_i = a_i x_i$ şi din $\sum_{i=1}^n a_i x_i = 0$ deducem că $\sum_{i=1}^n a_i \varphi(f_i) = 0$, adică $\sum_{i=1}^n a_i f_i \in \ker \varphi = L$. Cum $d_1 f_1, \dots, d_m f_m$ este bază pentru $L$ obţinem că $\sum_{i=1}^n a_i f_i = \sum_{i=1}^m b_i d_i f_i$, aşadar $a_i = b_i d_i$ pentru $i = 1, \dots, m$ şi $a_i = 0$ pentru $i = m+1, \dots, n$, deci $y_i = 0$ pentru $i = m+1, \dots, n$. Pentru $i = 1, \dots, m$ scriem $y_i = a_i x_i = b_i d_i \varphi(f_i) = b_i \varphi(d_i f_i) = 0$ (deoarece $d_i f_i \in \ker \varphi$).

Ultimul pas al demonstraţiei este să arătăm că $\operatorname{Ann}(x_i) = (d_i)$ pentru $i = 1, \dots, m$ şi $\operatorname{Ann}(x_i) = (0)$ pentru $i = m+1, \dots, n$.
Pentru $i = 1, \dots, m$ scriem $d_i x_i = d_i \varphi(f_i) = \varphi(d_i f_i) = 0$, deci $d_i \in \operatorname{Ann}(x_i)$. Reciproc, fie $a \in \operatorname{Ann}(x_i)$. Rezultă că $a x_i = 0$, adică $a f_i \in \ker \varphi$. Aceasta înseamnă că putem scrie $a f_i = \sum_{j=1}^m c_j d_j f_j$ şi de aici obţinem $a = c_i d_i \in (d_i)$.
Pentru $i = m+1, \dots, n$ din $a \in \operatorname{Ann}(x_i)$ obţinem, procedând ca mai sus, $a = 0$.

Deoarece $d_1 \mid \cdots \mid d_m$ şi $\operatorname{Ann}(x_i) = (d_i)$ pentru $i = 1, \dots, m$, rezultă $\operatorname{Ann}(x_1) \supseteq \cdots \supseteq \operatorname{Ann}(x_m) \supsetneq \operatorname{Ann}(x_{m+1}) = \cdots = \operatorname{Ann}(x_n) = (0)$. (Dacă $\operatorname{Ann}(x_1) = R$, adică $d_1$ este inversabil, atunci $x_1 = 0$ şi-l putem scoate din sistemul de generatori. Procedând astfel cu toţi $x_i = 0$ putem presupune din start că $\operatorname{Ann}(x_1) \neq R$.) □

**Theorem 3.4.** (Teorema factorilor invarianţi)
*Fie $R$ PID şi $M$ $R$-modul finit generat nenul. Există $m, n \in \mathbb{N}$, $m \leq n$, există $x_1, \dots, x_m \in M$ şi există $d_1, \dots, d_m \in R$ nenule şi neinversabile cu $d_1 \mid \cdots \mid d_m$ astfel încât:*
*(i) $M = Rx_1 \dot{+} \cdots \dot{+} Rx_n$.*
*(ii) $\operatorname{Ann}(x_i) = (d_i)$ pentru $i = 1, \dots, m$ şi $\operatorname{Ann}(x_i) = (0)$ pentru $i = m+1, \dots, n$.*

*Mai mult, numerele $m, n$ şi elementele $d_1, \dots, d_m$ sunt unic determinate de $M$ (acestea din urmă până la o asociere în divizibilitate).*

*Proof.* Existenţa se obţine imediat din teorema 3.3. □

**Definition 3.5.** *Elementele $d_1, \dots, d_m$ se numesc* factorii invarianţi *ai lui $M$.*

**Corollary 3.6.** *Fie $R$ PID şi $M$ $R$-modul finit generat nenul. Atunci exisă şi sunt unice $m, n \in \mathbb{N}$, $m \leq n$ şi elementele $d_1, \dots, d_m \in R$ nenule şi neinversabile cu*

$d_1 \mid \cdots \mid d_m$ *astfel încât*

$$M \simeq R/(d_1) \oplus \cdots \oplus R/(d_m) \oplus R^{n-m}.$$

**Remarks 3.7.** (i) $t(M) = Rx_1 \dotplus \cdots \dotplus Rx_m$ iar $M/t(M) \simeq R^{n-m}$. ($n-m$ se numeşte *rangul* lui $M$.)

**Exercise 3.8.** Arătaţi că rangul unui modul finit generat $M$ peste un PID coincide cu numărul maxim de elemente liniar independente din $M$.

**Exercise 3.9.** Fie $M$ un $R$-modul şi $(N_i)_{i\in I}$ o familie de $R$-module. Atunci
(i) $\operatorname{Hom}_R(\bigoplus_{i\in I} N_i, M) \simeq \prod_{i\in I} \operatorname{Hom}_R(N_i, M)$;
(ii) $\operatorname{Hom}_R(M, \prod_{i\in I} N_i) \simeq \prod_{i\in I} \operatorname{Hom}_R(M, N_i)$.

**Exercise 3.10.** Fie $M$ un $R$-modul şi $I \subseteq R$ un ideal. Atunci $\operatorname{Hom}_R(R/I, M) \simeq (0 :_M I)$, unde $(0 :_M I) = \{x \in M : Ix = 0\}$.

*Proof.* Să demonstrăm unicitatea. Aceasta se reduce la a arăta că dacă

$$R/(d_1) \oplus \cdots \oplus R/(d_m) \simeq R/(d'_1) \oplus \cdots \oplus R/(d'_{m'}),$$

unde $d_1, \dots, d_m, d'_1, \dots, d'_{m'} \in R$ sunt nenule şi neinversabile cu $d_1 \mid \cdots \mid d_m$ şi $d'_1 \mid \cdots \mid d'_{m'}$, atunci $m = m'$ şi $(d_1) = (d'_1), \dots, (d_m) = (d'_m)$.

Mai întâi să arătăm că $m = m'$. Pentru aceasta considerăm $p$ un divizor prim al lui $d_1$. Vom avea

$$\operatorname{Hom}_R(R/(p), R/(d_1) \oplus \cdots \oplus R/(d_m)) \simeq \operatorname{Hom}_R(R/(p), R/(d'_1) \oplus \cdots \oplus R/(d'_{m'}).$$

Folosind exerciţiul 3.9(ii) deducem

$$\operatorname{Hom}_R(R/(p), R/(d_1)) \oplus \cdots \oplus \operatorname{Hom}_R(R/(p), R/(d_m)) \simeq$$
$$\operatorname{Hom}_R(R/(p), R/(d'_1)) \oplus \cdots \oplus \operatorname{Hom}_R(R/(p), R/(d'_{m'})).$$

Din exerciţiul 3.10 deducem că $\operatorname{Hom}_R(R/(p), R/(d)) \simeq (0 :_{R/(d)} p) = \{\bar{a} \in R/(d) : pa \in (d)\}$. Acum sunt două posibilităţi:
$(p, d) = 1$, caz în care $(0 :_{R/(d)} p) = 0$, sau
$(p, d) \neq 1$, adică $p \mid d$, caz în care obţinem $(0 :_{R/(d)} p) = (d/p)/(d) \simeq R/(p)$.

Cum $p$ a fost ales divizor al lui $d_1$ avem că

$$\operatorname{Hom}_R(R/(p), R/(d_1)) \oplus \cdots \oplus \operatorname{Hom}_R(R/(p), R/(d_m)) \simeq (R/(p))^m.$$

Deoarece $R/(p)$ este corp iar izomorfismul de mai sus este izomorfism de $R/(p)$-spaţii vectoriale, rezultă că $p$ divide exact $m$ dintre elementele $d'_1, \dots, d'_{m'}$. În particular, $m \leq m'$. Un argument similar implică $m' \leq m$, deci egalitate.

Pentru a demonstra că $(d_i) = (d'_i)$ pentru orice $i = 1, \dots, m$ să începem prin a observa că $(d_m) = (d'_m)$ deoarece $(d_m) = \operatorname{Ann}_R(R/(d_1) \oplus \cdots \oplus R/(d_m))$ şi $(d'_m) = \operatorname{Ann}_R(R/(d'_1) \oplus \cdots \oplus R/(d'_m))$ (vezi exerciţiul 3.2(i)). Fie acum $1 \leq j < m$ minimal cu proprietatea că $(d_j) \neq (d'_j)$ şi fie $a \in (d_j) \setminus (d'_j)$. Din

$$R/(d_1) \oplus \cdots \oplus R/(d_m) \simeq R/(d'_1) \oplus \cdots \oplus R/(d'_m)$$

obţinem

$$a(R/(d_1) \oplus \cdots \oplus R/(d_m)) \simeq a(R/(d'_1) \oplus \cdots \oplus R/(d'_m)),$$

adică

$$a(R/(d_1)) \oplus \cdots \oplus a(R/(d_m)) \simeq a(R/(d'_1)) \oplus \cdots \oplus a(R/(d'_m)).$$

Dar $a(R/(d)) = 0$ dacă $a \in (d)$, aşadar

$$a(R/(d_{j+1})) \oplus \cdots \oplus a(R/(d_m)) \simeq a(R/(d'_j)) \oplus \cdots \oplus a(R/(d'_m)).$$

Dacă $a \neq (d)$, atunci $a(R/(d)) = ((a) + (d))/(d) = (a, d)/(d) \simeq R/(\delta)$, unde $\delta = d/(a, d)$. Obţinem astfel

$$R/(\delta_{j+1}) \oplus \cdots \oplus R/(\delta_m) \simeq R/(\delta'_j) \oplus \cdots \oplus R/(\delta'_m),$$

unde $\delta_i = d_i/\gcd(a, d_i)$ iar $\delta'_i = d'_i/\gcd(a, d'_i)$. Este uşor de văzut că $\delta_{j+1} \mid \cdots \mid \delta_m$ şi $\delta'_j \mid \cdots \mid \delta'_m$. Mai mult, $\delta'_j$ nu este inversabil deoarece $a \notin (d'_j)$. Este posibil ca anumiţi $\delta_i$, $i = j+1, \ldots, m$ să fie inversabili, dar cu siguranţă nu toţi fiindcă $(\delta_m) = (\delta'_m)$. Acum putem aplica prima parte a acestei demonstraţii în care am arătat că un astfel de izomorfism conduce la egalitatea numărului de factori în cele două sume directe, ceea ce în acest caz este imposibil. În concluzie, $(d_i) = (d'_i)$ pentru orice $i = 1, \ldots, m$. $\square$

**Remark 3.11.** Demonstraţia de mai sus se poate lesne generaliza pentru a obţine următorul rezultat:

Fie $R$ un inel comutativ unitar şi $R \neq I_1 \supseteq \cdots \supseteq I_m \neq 0$, $R \neq J_1 \supseteq \cdots \supseteq J_n \neq 0$ două şiruri descrescătoare de ideale cu proprietatea că

$$R/I_1 \oplus \cdots \oplus R/I_m \simeq R/J_1 \oplus \cdots \oplus R/J_n.$$

Atunci $m = n$ şi $I_i = J_i$ pentru orice $i = 1, \ldots, m$.