6

Moduluak

6.1. Moduluak, oinarrizko propietateak eta adibideak

Moduluak beste egitura aljebraiko baten adibidea dira, bektore-espazioen kontzeptuaren hedapen bat, alegia. Bektore-espazioetan eskalarrek gorputz bat osatu behar badute, moduluetan nahikoa da eraztun bat izatea.

6.1. Definizioa. Izan bitez $(M, +)$ talde abeldarra eta A eraztuna, eta demagun badagoela biderketa bat definiturik, $a \in A$ eta $x \in M$ bakoitzari $ax \in M$ elementu bat esleitzen diona. Orduan, M A-ren gainean *modulua* dela esango dugu (edo, laburkiago, A-modulua dela) baldintza hauek betetzen badira:

(i) $a(x + y) = ax + ay$, $a \in A$ eta $x, y \in M$ guztietarako.
(ii) $(a + b)x = ax + bx$, $a, b \in A$ eta $x \in M$ guztietarako.
(iii) $(ab)x = a(bx)$, $a, b \in A$ eta $x \in M$ guztietarako.
(iv) $1x = x$, $x \in M$ guztietarako. (Hemen, jakina, 1 A-ko identitatea da.)

Orduan, A-ko elementuei *eskalar* deitzen diegu.

6.2. Adibideak. 1) K gorputz baten gainean, moduluak bektore-espazioak besterik ez dira.

2) Izan bedi M edozein talde abeldar. Orduan $nx \in M$ definituta dago $n \in \mathbb{Z}$ eta $x \in M$ guztietarako, eta moduluaren definizioaren baldintzak argi eta garbi betetzen dira. Beraz, talde abeldar guztiak $\mathbb{Z}$-moduluak dira modu naturalean.

3) Bereziki, A edozein eraztun izanda ere, A-moduluak $\mathbb{Z}$-moduluak dira.

4) Baldin eta $A \subseteq B$ eraztunak badira eta M B-modulua bada, orduan A-modulua ere bada. Adibidez, $\mathbb{Z}[i] \subseteq \mathbb{C}$ denez eta $\mathbb{C}^n$ $\mathbb{C}$-modulua denez, orduan $\mathbb{C}^n$ $\mathbb{Z}[i]$-modulua ere badela esan dezakegu.

5) Izan bedi A edozein eraztun. Orduan, A bera A-modulua da, bere baitako batuketarekin eta biderketarekin.

6) Baldin eta $M_1, \dots, M_n$ A-moduluak badira, orduan $M_1 \times \cdots \times M_n$ biderkadura cartesiarra ere A-modulua da, batuketa osagaiz osagai egiten badugu, eta A-ko elementuak eta tuplak honela biderkatzen baditugu:

$$a(x_1, \dots, x_n) = (ax_1, \dots, ax_n), \quad a \in A \text{ eta } x_1 \in M_1, \dots, x_n \in M_n \text{ guztietarako.}$$

7) Izan bedi V bektore-espazioa K gorputzaren gainean, eta finka dezagun $\varphi : V \longrightarrow V$ endomorfismoa. Orduan, V modulua da $K[X]$-ren gainean, polinomioen

eta bektoreen arteko biderketa honela definitzen badugu:

$$f(X)v = f(\varphi)(v), \quad f(X) \in K[X] \text{ eta } v \in V \text{ guztietarako.}$$

Hau da, v-ri $f(\varphi)$ endomorfismoa aplikatzen diogu. (Gogoratu nola definitzen den $f(\varphi)$: baldin eta $f(X) = a_n X^n + \cdots + a_1 X + a_0$ bada, orduan $f(\varphi) = a_n \varphi^n + \cdots + a_1 \varphi + a_0 1_V$ dugu.)

8) $M = \{0\}$ talde tribiala modulua da A edozein eraztunen gainean, $a0 = 0$ definituz $a \in A$ guztietarako. Horri *modulu tribial* edo *modulu nulu* deitzen zaio.

Orain moduluen oinarrizko propietate batzuk emango ditugu.

6.3. Proposizioa. *Izan bitez A eraztuna eta M A-modulua. Orduan:*

(i) $0x = 0$, *$x \in M$ guztietarako.*
(ii) $a0 = 0$, *$a \in A$ guztietarako.*
(iii) $(-a)x = a(-x) = -ax$, *$a \in A$ eta $x \in M$ guztietarako.*

Bektore-espazioetan ezaguna da $\lambda v = 0$ baldintzatik, $\lambda \in K$ eta $v \in V$ izanik, $\lambda = 0$ edo $v = 0$ ondorioztatzen dela. Ekar dezagun gogora nola frogatzen den propietate hori. Nahikoa da $v = 0$ dela ikustea $\lambda \neq 0$ den baldintzapean. Orduan K gorputza izategatik, existitzen da λ^{-1}, λ-ren alderantzizkoa biderketarekiko. Orain, $\lambda v = 0$ berdintza λ^{-1}-ez biderkatuz, $v = 0$ lortzen dugu. Froga horrek ez du funtzionatzen A-moduluetan, $a \in A$ elementu batek ez baitu zertan alderantzizkoa izan, $a \neq 0$ bada ere. Are gehiago, goian aipatutako propietatea faltsua da moduluetan, hau da:

$$ax = 0, \quad a \in A \text{ eta } x \in M \text{ izanik} \quad \not\Longrightarrow \quad a = 0 \text{ edo } x = 0,$$

hurrengo adibideak erakusten duen bezala.

6.4. Adibidea. $\mathbb{Z}/4\mathbb{Z}$ modulua da $\mathbb{Z}$-ren gainean, eta horretan $2 \cdot \overline{2} = \overline{0}$ berdintza dugu. Hala ere, $2 \neq 0$ dugu $\mathbb{Z}$-n eta $\overline{2} \neq \overline{0}$ $\mathbb{Z}/4\mathbb{Z}$-n.

Hala ere, garbi dago ondorengo emaitza positiboa dugula.

6.5. Proposizioa. *Izan bitez A eraztuna eta M A-modulua. Baldin eta $ax = 0$ bada, $a \in A^\times$ izanik, orduan $x = 0$ dugu.*

6.2. Azpimoduluak eta zatidura moduluak

6.6. Definizioa. Izan bitez M A-modulua eta $N \subseteq M$. Orduan, N M-ren *azpimodulua* dela esango dugu, eta $N \leq M$ idatziko dugu, N A-modulua baldin bada M-ren batuketarekin eta eskalarrezko biderketarekin.

Garbi dago N M-ren azpimodulua dela baldin eta soilik baldin bi baldintza hauek betetzen badira:

(i) N M-ren azpitaldea da batuketarekiko.

(ii) $ax \in N$ dugu $a \in A$ eta $x \in N$ guztietarako.

Horrenbestez, emaitza hau lortzen dugu.

6.7. Teorema. *Izan bitez M A-modulua eta N M-ren azpimultzo ez-hutsa. Orduan, baliokideak dira:*

(i) *N M-ren azpimodulua da.*
(ii) *$x + y \in N$ eta $ax \in N$, $a \in A$ eta $x, y \in N$ guztietarako.*
(iii) *$ax + by \in N$, $a, b \in A$ eta $x, y \in N$ guztietarako.*

6.8. Adibideak. 1) Talde abeldar bat $\mathbb{Z}$-modulu gisa ikusten dugunean, horren azpimoduluak azpitaldeak besterik ez dira.

2) Bektore-espazio baten azpimoduluak azpiespazioak besterik ez dira.

3) A eraztuna A-modulu gisa ikusten dugunean, A-ren azpimoduluak A-ren idealak dira.

4) Baldin eta $\varphi : V \longrightarrow V$ bektore-espazio baten endomorfismoa bada, eta V-ri $K[X]$-moduluaren egitura ematen badiogu φ erabiliz, orduan V-ren azpimoduluak V-ren azpiespazio φ-aldagaitzak dira.

5) Edozein modulutan, $\{0\}$ azpimodulua da. Bestalde, 0 batuketarekiko neutroa azpimodulu guztietan dago.

6.9. Teorema (Azpimoduluen arteko eragiketak)**.** *Izan bitez M A-modulua, eta L eta N M-ren azpimoduluak. Orduan, $L + N$ eta $L \cap N$ ere M-ren azpimoduluak dira.*

Aurreko teorema orokortu daiteke $\{N_i\}_{i \in I}$ M-ren azpimoduluen familia baten kasura. Orduan, $\cap_{i \in I} N_i$ M-ren azpimodulua da, eta baita $\sum_{i \in I} N_i$ batura ere. Azken kasuan, garrantzitsuena da $\sum_{i \in I} N_i$ batura *zer den* ulertzea I indizeen multzoa infinitua denean. Jakina, M moduluaren barruan ezin da batura infiniturik egin (testuinguru abstraktu honetan ez dugu serieen konbergentziaren kontzeptua eskura). Hori dela eta, $\sum_{i \in I} N_i$ baturako elementuak $\sum_{i \in I} x_i$ bezalako baturak dira, $x_i \in N_i$ izanik $i \in I$ guztietarako, eta $x_i \neq 0$ izanik bakarrik *indize kopuru finitu baterako*.

Izan bitez M modulua eta $X \subseteq M$. Normalean, X ez da M-ren azpimodulua izango, baina beti erabil daiteke X azpimodulu bat *sortzeko*. Izan ere, X barruan duten azpimodulu guztien ebakidura azpimodulua denez, hori da X barruan duen azpimodulurik txikiena.

6.10. Definizioa. Izan bitez M A-modulua eta $X \subseteq M$. Orduan, X barruan duten azpimodulu guztien ebakidurari *X-k sortutako azpimodulua* deitzen diogu, eta $\langle X \rangle$ ikurra erabiliko dugu hori adierazteko.

Azpimarratu behar bada A-moduluekin ari garela, eta ez beste egitura mota batekin, orduan $\langle X \rangle_A$ idatz dezakegu $\langle X \rangle$-ren ordez.

6.11. Teorema (Sortutako azpimoduluaren elementuak)**.** *Izan bitez M A-modulua eta $X \subseteq M$. Orduan,*

$$\langle X \rangle = \{a_1 x_1 + \cdots + a_r x_r \mid a_i \in A,\ x_i \in X,\ r \in \mathbb{N}\}$$

dugu. Hau da, X-k sortzen duen azpimoduluaren elementuak X-ko elementuen multiploen baturak dira (multiploak A-ko elementuekin biderkatuz egiten dira). Bereziki:

(i) $\langle x \rangle = \{ax \mid a \in A\}$. *Azpimodulu hori Ax ikurraren bidez ere adierazten dugu.*
(ii) $\langle x_1, \ldots, x_n \rangle = \{a_1 x_1 + \cdots + a_n x_n \mid a_i \in A\} = Ax_1 + \cdots + Ax_n$.

6.12. Adibideak. 1) Talde abeldar bat $\mathbb{Z}$-modulu gisa ikusten dugunean, orduan X azpimultzo batek sortzen duen azpimodulua eta sortzen duen azpitaldea bat datoz. Era berean, K gorputzaren gaineko bektore-espazio bat K-modulu gisa ikusten dugunean, sortutako azpimodulua sortutako azpiespazioa besterik ez da.

2) Izan bedi $\varphi : V \longrightarrow V$ aplikazio lineala, eta ikus dezagun V bektore-espazioa $K[X]$-modulu gisa φ erabiliz. Orduan, $S \subseteq V$ azpimultzoak sortzen duen azpimodulua ez da S-k sortzen duen azpiespazioa, baizik eta

$$\{\varphi^n(v) \mid v \in S, n \in \mathbb{N} \cup \{0\}\}$$

irudiek sortzen duten azpiespazioa.

6.13. Definizioa. Izan bedi M A-modulua. Orduan:

(i) M *ziklikoa* dela esaten dugu elementu bakar baten bidez sor badaiteke.
(ii) M *finituki sortua* dela esaten dugu elementu-kopuru finitu baten bidez sor badaiteke.

Izan bitez M A-modulua eta N M-ren azpimodulua. Talde abeldar batean azpitalde guztiak normalak direnez, M/N zatidura taldea era dezakegu batuketarekiko, $(x + N) + (y + N) = (x + y) + N$ erregelaren bitartez. Gainera, A-ko elementuen eta M/N-ko elementuen arteko biderketa honela definitzen badugu,

$$a(x + N) = ax + N, \quad a \in A \text{ eta } x \in M \text{ guztietarako,}$$

erraz ikus daiteke eragiketa hori ondo definituta dagoela.

6.14. Teorema. *Izan bitez M A-modulua eta N M-ren azpimodulua. Orduan, goian aipatutako eragiketekin, M/N A-modulua da. Hori M-ren eta N-ren arteko* zatidura modulua *dela esango dugu.*

Beste egitura aljebraiko batzuetan bezala, ohikoa da M/N zatidurako elementuak $\overline{x}$ moduan idaztea, behintzat ez badago zalantzarik N zein den. Orduan, $M/N = \{\overline{x} \mid x \in M\}$ dugu, eta

$$\overline{x} = \overline{y} \iff x - y \in N.$$

Bereziki, $\overline{x} = \overline{0}$ dugu baldin eta soilik baldin $x \in N$ bada. Gainera, marraren notazioarekin, M/N zatidurako eragiketak honela daude definituta:

$$\overline{x} + \overline{y} = \overline{x+y} \quad \text{eta} \quad a\overline{x} = \overline{ax}.$$

6.15. Adibidea. Izan bitez V bektore-espazioa eta $\varphi : V \longrightarrow V$ aplikazio lineala, eta eman diezaiogun V-ri $K[X]$-moduluaren egitura φ erabiliz. Orduan, W V-ren azpimodulua bada (hau da, azpiespazio φ-aldagaitza), V/W-ren egitura $K[X]$-modulu gisa

$$\begin{array}{rccc} \overline{\varphi} : & V/W & \longrightarrow & V/W \\ & \overline{v} & \longmapsto & \overline{\varphi(v)} \end{array}$$

endomorfismoaren bitartez lortzen dugu.

6.16. Teorema (Korrespondentziaren teorema)**.** *Izan bitez M A-modulua eta N M-ren azpimodulua. Orduan, badago banan-banako korrespondentzia bat N barruan duten M-ren azpimoduluen eta M/N-ren azpimoduluen artean, $L \mapsto L/N$ erregelaren bitartez emanda.*

6.3. Modulu-homomorfismoak

6.17. Definizioa. Izan bitez M_1 eta M_2 A-moduluak. Orduan, $\varphi : M_1 \longrightarrow M_2$ aplikazio bat *modulu-homomorfismoa* dela esango dugu bi baldintza hauek betetzen badira:

(i) $\varphi(x+y) = \varphi(x) + \varphi(y)$, $x, y \in M_1$ guztietarako.
(ii) $\varphi(ax) = a\varphi(x)$, $a \in A$ eta $x \in M_1$ guztietarako.

Homomorfismo bat *isomorfismoa* da bijektiboa bada. Orduan, M_1 eta M_2 *isomorfoak* direla esango dugu eta $M_1 \cong M_2$ idatziko dugu.

Baldin eta $\varphi : M_1 \longrightarrow M_2$ homomorfismoa bada, orduan:

(a) φ *monomorfismoa* dela esaten dugu φ injektiboa bada.
(b) φ *epimorfismoa* dela esaten dugu φ supraiektiboa bada.
(c) φ M_1-en *endomorfismoa* dela diogu $M_1 = M_2$ bada.
(d) φ M_1-en *automorfismoa* dela diogu $M_1 = M_2$ bada eta, horrez gain, φ bijektiboa bada.

6.18. Adibideak. 1) Izan bitez K gorputza eta V_1, V_2 bi bektore-espazio K-ren gainean. Orduan, $\varphi : V_1 \longmapsto V_2$ aplikazioa modulu-homomorfismoa da baldin eta soilik baldin aplikazio lineala bada.

2) Baldin eta N M-ren azpimodulua bada, orduan $\pi : M \longrightarrow M/N$ aplikazioa non $\pi(x) = \overline{x}$ baita, modulu-epimorfismoa da.

3) Nabaria da identitate aplikazioa beti dela modulu baten automorfismoa.

6.19. Definizioa. Izan bedi $\varphi : M_1 \longrightarrow M_2$ modulu-homomorfismoa. Orduan, φ-ren *nukleoa* M_1-en azpimultzo hau da:

$$\ker \varphi = \{x \in M_1 \mid \varphi(x) = 0\}.$$

Bestela esanda, $\ker \varphi = \varphi^{-1}(0)$ dugu.

Adibidez, $\pi : M \longrightarrow M/N$ epimorfismo kanonikoa bada, orduan $\ker \pi = N$ dugu.

6.20. Teorema (Homomorfismoen propietateak)**.** *Izan bedi $\varphi : M_1 \longrightarrow M_2$ A-moduluen homomorfismoa. Orduan:*

(i) *$\varphi(ax + by) = a\varphi(x) + b\varphi(y)$, $a, b \in A$ eta $x, y \in M_1$ guztietarako. Bereziki, $\varphi(-x) = -\varphi(x)$.*
(ii) *$\varphi(0) = 0$.*
(iii) *N_1 M_1-en azpimodulua bada, orduan $\varphi(N_1)$ M_2-ren azpimodulua da. Bereziki,* $\operatorname{im} \varphi$ *M_2-ren azpimodulua da.*
(iv) *N_2 M_2-ren azpimodulua bada, orduan $\varphi^{-1}(N_2)$ M_1-en azpimodulua da. Bereziki,* $\ker \varphi$ *M_1-en azpimodulua da.*

Izan bitez M A-modulua, N M-ren azpimodulua eta $\pi : M \longrightarrow M/N$ epimorfismo kanonikoa. Orduan, L M-ren beste edozein azpimodulu bada,

$$\pi(L) = \{\overline{x} \mid x \in L\}$$

M/N-ren azpimodulua da. Korrespondentziaren teoremari begira, ohiko akatsa da $\pi(L) = L/N$ dela pentsatzea. Kontuan izan *L/N idatzi ahal izateko derrigorrezkoa dela $N \subseteq L$ izatea*. Beraz, oro har, ezin da $\pi(L) = L/N$ izan. Baina, korrespondentziaren teoremaren arabera, badago T M-ren azpimodulu bat non $\pi(L) = T/N$ baita. Zein da T hori? $L + N$, hain zuzen ere. Laburbilduz,

$$\pi(L) = \frac{L + N}{N}$$

dugu L azpimodulu guztietarako. Baldin eta $N \subseteq L$ bada, orduan $L + N = L$ dugu eta egiazkoa da hasieran planteatzen genuen berdintza: $\pi(L) = L/N$ dugu kasu horretan.

6.21. Teorema (Lehenengo isomorfismo-teorema)**.** *Izan bedi $\varphi : M_1 \longrightarrow M_2$ modulu-homomorfismoa. Orduan,*

$$\begin{array}{cccc} \overline{\varphi} : & M_1/\ker \varphi & \longrightarrow & \operatorname{im} \varphi \\ & \overline{x} & \longmapsto & \varphi(x) \end{array}$$

aplikazioa ondo definiturik dago eta isomorfismoa da. Beraz, isomorfismo hau dugu:

$$\frac{M_1}{\ker \varphi} \cong \operatorname{im} \varphi.$$

6.22. Teorema (Zatidura bikoitzaren teorema/Bigarren isomorfismo-teorema)**.** *Izan bitez M A-modulua, eta $N \subseteq L$ M-ren bi azpimodulu. Orduan,*

$$\frac{M/N}{L/N} \cong \frac{M}{L}.$$

6.23. Teorema (Hirugarren isomorfismo-teorema)**.** *Izan bitez M A-modulua, eta L eta N M-ren bi azpimodulu. Orduan,*

$$\frac{L+N}{N} \cong \frac{L}{L \cap N}.$$

6.4. Batura zuzenak

6.24. Definizioa. Izan bitez M modulua, eta L eta N M-ren bi azpimodulu. Orduan, $L+N$ batura *zuzena* dela esango dugu $L \cap N = \{0\}$ bada. Batura zuzena dela azpimarratu nahi badugu, $L \oplus N$ idatziko dugu $L+N$-ren ordez.

Adibidez, $\mathbb{Z}/12\mathbb{Z}$ talde abeldarra $\mathbb{Z}$-modulu gisa ikusten badugu, orduan $3\mathbb{Z}/12\mathbb{Z}$ eta $4\mathbb{Z}/12\mathbb{Z}$ azpimoduluen batura zuzena da, baina $3\mathbb{Z}/12\mathbb{Z}$ eta $2\mathbb{Z}/12\mathbb{Z}$-rena, berriz, ez ($6+12\mathbb{Z}$ elementu ez-nulu komuna baitute).

6.25. Teorema. *Izan bitez M modulua, eta L eta N M-ren bi azpimodulu. Orduan, baliokideak dira:*

(i) *L-ren eta N-ren batura zuzena da.*
(ii) *$L+N$-ren elementu bakoitza modu bakar batean idatz daiteke $\ell+n$ moduan, $\ell \in L$ eta $n \in N$ izanik.*

FROGA. (i) $\Rightarrow$ (ii). Izan bedi $x \in L+N$. Moduluen baturaren definizioaren arabera, $x = \ell+n$ moduan idatz daiteke. Deskonposizioaren bakartasuna ikusteko, demagun $x = \ell' + n'$ dela, $\ell' \in L$ eta $n' \in N$ izanik, eta ikus dezagun $\ell = \ell'$ eta $n = n'$ dela. Izan ere, $\ell + n = \ell' + n'$ denez, $\ell - \ell' = n' - n$ ondorioztatzen dugu. Elementu hori L-n eta N-n dago aldi berean, eta L-ren eta N-ren batura zuzena denez, 0 izan behar du. Beraz, $\ell - \ell' = n' - n = 0$ eta hemendik $\ell = \ell'$ eta $n = n'$, nahi bezala.

(ii) $\Rightarrow$ (i). Har dezagun $x \in L \cap N$ eta ikus dezagun $x = 0$ dela. Ohartu $x = x + 0$ eta $x = 0 + x$ x-ren bi deskonpozio direla L-ren elementu baten eta N-ren beste elementu baten batura gisa. Orduan, deskonposizioaren bakartasunak zuzenean $x = 0$ ematen digu. □

6.26. Teorema. *Izan bitez M modulua, eta L eta N M-ren bi azpimodulu. Orduan, L-ren eta N-ren batura zuzena bada, isomorfismo hau dugu:*

$$L \oplus N \cong L \times N.$$

FROGA. Definitu

$$\begin{array}{cccc} \varphi : & L \times N & \longrightarrow & L \oplus N \\ & (\ell, n) & \longmapsto & \ell + n. \end{array}$$

Orduan, erraz egiaztatzen da φ modulu-homomorfismoa dela. Gainera, φ supraiektiboa da. (Gogoratu $L \oplus N$ ikurra $L + N$ idazteko modu bat besterik ez dela.) Bestalde, aurreko teorema aplikatuz, φ injektiboa dela lortzen dugu. Hortaz, φ isomorfismoa da. □

Batura zuzenaren kontzeptua bi batugairen kasutik batugai kopuru orokor batera heda daiteke, eta aurrekoen antzeko emaitzak lortuko ditugu.

6.27. Definizioa. Izan bedi $\{N_i\}_{i \in I}$ azpimodulu-familia bat. Orduan, familia horretako azpimoduluen batura *zuzena* dela esango dugu,

$$N_i \cap \sum_{\substack{j \in I \\ j \neq i}} N_j = \{0\} \text{ bada, } i \in I \text{ guztietarako.}$$

Hala bada, eta batura zuzena dela azpimarratu nahi badugu, $\bigoplus_{i \in I} N_i$ idatziko dugu $\sum_{i \in I} N_i$-ren ordez.

Bereziki, $N_1, \ldots, N_r$ azpimodulu-familia *finitua* bada, orduan horien batura zuzena da baldin eta soilik baldin

$$N_i \cap (N_1 + \cdots + N_{i-1} + N_{i+1} + \cdots + N_r) = \{0\} \text{ bada } i = 1, \ldots, r \text{ guztietarako.}$$

6.28. Teorema. *Izan bitez M modulua eta $\{N_i\}_{i \in I}$ M-ren azpimoduluen familia bat. Orduan, baliokideak dira:*

(i) $\sum_{i \in I} N_i$ *batura zuzena da.*
(ii) $\sum_{i \in I} N_i$ *baturako elementu bakoitza modu bakar batean idatz daiteke* $\sum_{i \in I} x_i$ *moduan,* $x_i \in N_i$ *izanik, eta* x_i *guztiak* 0 *izanik, kopuru finitu bat izan ezik.*

Familia finitu baten batura zuzena den kasuan,

$$N_1 \oplus N_2 \oplus \cdots \oplus N_r \cong N_1 \times N_2 \times \cdots \times N_r$$

isomorfismoa dugu. Bestalde, familia infinitua den kasuan, $\bigoplus_{i \in I} N_i$ batura zuzena ez da $\prod_{i \in I} N_i$ biderkadura cartesiarrarekin isomorfoa. Bai da isomorfoa, ordea, biderkadura cartesiarraren azpimodulu batekin: osagai guztiak, kopuru finitu bat izan ezik, nuluak diren tuplek osatutako azpimoduluarekin, alegia.

6.5. Modulu askeak

6.29. Definizioa. Izan bitez M A-modulua eta $\{x_i\}_{i \in I}$ M-ren elementuen familia bat. Orduan:

(i) Familia hori *askea* edo *linealki independentea* dela esango dugu baldintza hau betetzen bada:

$$\sum_{i\in I} a_i x_i = 0,\ a_i \in A \text{ izanik} \quad \Longrightarrow \quad a_i = 0\ i \in I \text{ guztietarako.}$$

Bestela, familia hori *lotua* edo *linealki dependentea* dela esango dugu.

(ii) Familia hori *M-ren oinarria* dela esango dugu linealki independentea bada eta M-ren sistema sortzailea bada.

6.30. Adibidea. Izan bedi A eraztuna, eta ikus dezagun A A-modulu gisa. Orduan, $x \in A$ elementu bakar bat linealki independentea da baldin eta soilik baldin $x \neq 0$ bada eta x zeroren zatitzailea ez bada. Bestalde, $x, y \in A$ bi edozein elementu ez dira inoiz linealki independenteak. Izan ere, $x, y \neq 0$ dela pentsa dezakegu, eta orduan $yx - xy = 0$ erlazioak dependentzia lineala frogatzen du.

Oro har, M modulu batean x elementu bat linealki dependentea da baldin eta soilik baldin existitzen bada $a \in A$, $a \neq 0$, non $ax = 0$ baita. Badakigu hori bektore-espazioetan ezinezkoa dela $x \neq 0$ bada, baina moduluetan gerta daitekeela. Hori dela eta, hurrengo definizioa ematen dugu.

6.31. Definizioa. Izan bitez M A-modulua eta $x \in M$. Existitzen bada $a \in A$, $a \neq 0$, halakoa non $ax = 0$ baita, orduan x M-ren *bihurdura-elementu* bat dela esango dugu.

6.32. Adibideak. 1) Izan bedi G talde abeldarra, $\mathbb{Z}$-modulu gisa ikusita. Orduan, bihurdura-elementuak G-ren ordena finituko elementuak dira.

2) Izan bedi A eraztuna, A-modulu gisa ikusita. Orduan, bihurdura-elementuak (0 neutroaz aparte) A-ren zeroren zatitzaileak dira.

6.33. Lema. *Izan bitez M A-modulua eta $x \in M$. Orduan, x ez bada bihurdura-elementua, $Ax \cong A$ isomorfismoa dugu.*

FROGA. Berehala egiaztatzen da $\varphi : A \longrightarrow Ax$ aplikazioa, non $\varphi(a) = ax$ baita, modulu-isomorfismoa dela. □

6.34. Teorema. *Izan bitez M A-modulua eta $\{x_i\}_{i\in I}$ M-ren elementuen familia bat. Orduan, baliokideak dira:*

(i) *$\{x_i\}_{i\in I}$ M-ren oinarria da.*

(ii) *M-ren elementu bakoitza modu bakar batean idatz daiteke $\sum_{i\in I} a_i x_i$ moduan, $a_i \in A$ izanik, eta a_i guztiak 0 izanik, kopuru finitu bat izan ezik.*

(iii) *$M = \bigoplus_{i\in I} Ax_i$, eta x_i bakoitza ez da bihurdura-elementua.*

(iv) *M A-rekin isomorfoak diren azpimoduluen batura zuzena da.*

FROGA. Berehalakoa da. □

Konparatu azken atala bektore-espazioen kasuarekin: V bektore-espazioa bada K gorputzaren gainean, eta $\dim V = n$ bada, orduan $V \cong K^n$ isomorfismoa dugu. (Gogoratu bi bektore-espazio isomorfoak direla baldin eta soilik baldin dimentsio bera badute.)

6.35. Definizioa. Izan bedi M A-modulua. Orduan:

(i) M *modulu askea* dela esango dugu oinarri bat baldin badu.
(ii) M *bihurduragabea* dela esango dugu haren bihurdura-elementu bakarra 0 bada.

6.36. Adibideak. 1) Izan bedi A eraztuna. Orduan, A^n A-modulu askea da $n \geq 1$ guztietarako: *oinarri kanonikoa* dugu bertan, $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, \ldots, 0)$, $\ldots$, $e_n = (0, \ldots, 0, 1)$ bektoreek osatutakoa. Bereziki, A bera askea da A-modulu gisa, $\{1\}$ oinarriarekin.

2) Izan bitez A integritate-domeinua eta $\mathfrak{a} = (a)$ A-ren ideal nagusia. Orduan, $\mathfrak{a}$ A-modulu askea da, eta $\{a\}$ A-ren oinarri bat da.

6.37. Korolarioa. *Izan bedi M A-modulua, A integritate-domeinua izanik. Orduan, M askea bada, bihurduragabea da.*

FROGA. Demagun $\{x_i\}_{i \in I}$ M-ren oinarria dela, eta izan bedi $x \in M$ bihurdura-elementua. Beraz, existitzen da $a \in A$, $a \neq 0$, halakoa non $ax = 0$ baita. Idatz dezagun $x = \sum_{i \in I} a_i x_i$. Orduan, $0 = \sum_{i \in I} a a_i x_i$ dugu eta, $\{x_i\}_{i \in I}$ linealki independentea denez, $a a_i = 0$ dugu $i \in I$ guztietarako. Orain, A integritate domeinua denez, $a_i = 0$ dugu $i \in I$ guztietarako. Beraz, $x = 0$ dela ondorioztatzen dugu. $\square$

Bestela esanda, A integritate-domeinu baten gainean, modulu batek bihurdura-elementu ez-nulu bat badu, orduan ez da modulu askea. Horren ondorioz, hurrengo adibidea lortzen dugu.

6.38. Adibidea. Izan bedi G talde abeldar finitu ez-tribiala, $\mathbb{Z}$-modulu gisa ikusita. Orduan, G ez da modulu askea.

Hala ere, 6.37 korolarioaren alderantzizkoa ez da betetzen: gerta daiteke modulu bat bihurduragabea izatea integritate-domeinu baten gainean eta, hala ere, ez izatea modulu askea.

6.39. Adibidea. Izan bedi K gorputza. Orduan, (X, Y) $K[X, Y]$-ren ideala denez, $K[X, Y]$-modulua da. Modulu hori bihurduragabea da, $K[X, Y]$ integritate-domeinua delako, baina ez da askea. Izan ere, alde batetik (X, Y)-ren sistema sortzaile batek (eta, beraz, oinarri batek) gutxienez bi elementu behar ditu, elementu horiek ideal gisa ere sortuko baitute (X, Y). Baina, lehenago ikusi dugun bezala, $K[X, Y]$-ko bi edozein elementu linealki dependenteak dira $K[X, Y]$-ren gainean. Beraz, (X, Y)-k ezin du oinarririk izan. Bide batez, adibide honek erakusten du modulu aske baten azpimodulu batek ez duela zertan askea izan: $K[X, Y]$ askea da, baina (X, Y) ez da.

6.40. Teorema. *Izan bedi M modulu askea. Orduan, M-ren oinarri guztiek kardinal bera dute.*

FROGA. Aukeratu $\{x_i\}_{i\in I}$ M-ren oinarri bat. Izan bedi $\mathfrak{m}$ A-ren ideal maximala, eta jarri
$$N = \mathfrak{m}M = \{\sum_{i=1}^{n} a_i x_i \mid a_i \in \mathfrak{m},\ x_i \in M, n \in \mathbb{N}\}.$$
Orduan, garbi dago N M-ren azpimodulua dela. Gainera, M/N zatidura A-modulua $\mathfrak{m}$-ko elementu guztiek anulatzen dute eta, hortaz, $A/\mathfrak{m}$-modulua ere bada. Kontuan hartzen badugu $A/\mathfrak{m}$ gorputza dela, orduan M/N bektore-espazioa da. Orain, erraz frogatzen da $\{x_i\}_{i\in I}$ M-ren oinarria dela baldin eta soilik baldin $\{x_i + N\}_{i\in I}$ M/N-ren oinarria bada $A/\mathfrak{m}$-ren gaineko bektore-espazio gisa. Horrek frogatzen du M-ren oinarri guztiek kardinal bera dutela, bektore-espazioetan hala gertatzen delako. $\square$

6.41. Definizioa. Izan bedi M modulu askea. Orduan, M-ren *heina*, $\operatorname{rk} M$ ikurraren bitartez adierazten duguna, M-ren oinarri baten (edozeinen) kardinala da.

Hala ere, kontuz ibili behar da ez pentsatzeko bektore-espazioen propietate guztiak modulu askeetara hedatzen direnik.

Izan bedi M modulu askea, $\operatorname{rk} M = n < \infty$ izanik. Orduan, $\{x_1, \dots, x_n\} \subseteq M$ linealki independentea bada, ez du zertan M-ren oinarria izan. Adibidez, $\mathbb{Z}^2$ askea da $\mathbb{Z}$-modulu gisa ikusita, eta $\operatorname{rk} \mathbb{Z}^2 = 2$ dugu. Orduan, $\{(2,0),(0,1)\}$ linealki independentea da, baina ez da $\mathbb{Z}^2$-ren oinarria.

Modulu aske batean, ezin da oro har ziurtatu sistema linealki independente bat oinarri bateraino luza daitekeenik. Adibidez, $\{(2,0)\}$ linealki independentea da $\mathbb{Z}^2$-n, baina ezin da luzatu $\mathbb{Z}^2$-ren oinarri bateraino.

Modulu aske batean, ezin da oro har ziurtatu sistema sortzaile baten barruan oinarri bat aurki daitekeenik. Adibidez, $\{(2,0),(3,0),(0,1)\}$ $\mathbb{Z}^2$-ren sistema sortzailea da, baina horren bi elementuko edozein azpimultzo ez da sistema sortzailea (beraz, oinarria ere ez da).

Modulu aske batean, ezin da oro har ziurtatu azpimodulu batek osagarri bat izango duenik. Hau da, $N \leq M$ bada, ezin dugu baieztatu $L \leq M$ egongo denik non $M = L \oplus N$ baita. Adibidez, $\langle(2,0)\rangle$ azpimoduluak ez du osagarririk $\mathbb{Z}^2$-n.