ALGEBRA I: MODULI

1. Generalità sugli A-moduli

Il concetto di A-modulo generalizza quello di spazio vettoriale su un campo $\mathbb{K}$

Definizione 1.1. Sia A un anello commutativo con unità. Un A-modulo è un insieme M dotato di un'operazione di somma $+ : M \times M \to M$ e di prodotto per uno scalare $\cdot : A \times M \to M$ tali che:

- $(M, +)$ è un gruppo abeliano;
- le operazioni $+$ e $\cdot$ soddisfano:
  - $(a + b) \cdot m = a \cdot m + b \cdot m$,
  - $a \cdot (m + n) = a \cdot m + a \cdot n$,
  - $(ab) \cdot m = a \cdot (b \cdot m)$,
  - $1_A \cdot m = m$;

  per ogni scelta di $a, b \in A, m, n \in M$.

Almeno inizialmente, indicheremo con $0_A, 1_A$ lo zero e l'unità nell'anello A e con 0_M l'elemento neutro del gruppo abeliano $(M, +)$.

Osservazione 1.2. È facile mostrare che $0_A \cdot m = a \cdot 0_M = 0_M$ per ogni scelta di $m \in M, a \in A$. In effetti, poiché $0_A \cdot m = (0_A + 0_A) \cdot m = 0_A \cdot m + 0_A \cdot m$, è sufficiente sommare ad entrambi i membri l'inverso additivo di $0_A \cdot m$ per ottenere $0_M = 0_A \cdot m$. Allo stesso modo, da $a \cdot 0_M + a \cdot 0_M = a \cdot (0_M + 0_M) = a \cdot 0_M$ segue $a \cdot 0_M = 0_M$.

Inoltre, $(-1_A) \cdot m$ è uguale all'inverso additivo di $m \in M$, che indichiamo con $-m$. In effetti:

$$0_M = 0_A \cdot m = (1_A + (-1_A)) \cdot m = 1_A \cdot m + (-1_A) \cdot m = m + (-1_A) \cdot m.$$

Dall'unicità dell'inverso segue che: $(-1_A) \cdot m = -m$. In seguito eviteremo di aggiungere gli indici A ed M per distinguere gli elementi neutri nell'anello e nel modulo, ottenendo quindi le più leggibili proprietà $0 \cdot m = 0, 1 \cdot m = m, (-1) \cdot m = -m$.

Tutte le manipolazioni valide negli spazi vettoriali continuano ad essere valide anche negli A-moduli, tranne quelle che coinvolgono la semplificazione (per divisione) degli scalari.

Esempi 1.3.

(1) Se $\mathbb{K}$ è un campo, il concetto di $\mathbb{K}$-modulo è equivalente a quello di spazio vettoriale su $\mathbb{K}$.
(2) Ogni gruppo abeliano $(\Gamma, +)$ possiede una struttura di $\mathbb{Z}$-modulo definita da:

$$ha = \begin{cases} \underbrace{a + \cdots + a}_{h \text{ volte}} & \text{se } h > 0 \\ 0 & \text{se } h = 0 \\ -\underbrace{(a + \cdots + a)}_{-h \text{ volte}} & \text{se } h < 0 \end{cases}.$$

Di conseguenza, il concetto di $\mathbb{Z}$-modulo è equivalente a quello di gruppo abeliano. *[Controllate per esercizio che la struttura di sopra definisce uno $\mathbb{Z}$-modulo, e spiegate per quale motivo sia l'unica compatibile con l'operazione di gruppo!]*

(3) Le operazioni di somma e prodotto in un anello A definiscono una struttura di A-modulo su A stesso.
(4) Sia A^n il prodotto cartesiano di n copie di A. Allora le operazioni definite da

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n), \qquad a \cdot (a_1, \ldots, a_n) = (aa_1, \ldots, aa_n)$$

forniscono una struttura di A-modulo su A^n.

1.1. Omomorfismi e sottomoduli.

Definizione 1.4. Sia M un A-modulo. Un sottoinsieme (non vuoto) $N \subseteq M$ è un *sottomodulo* se:

- N è un sottogruppo abeliano di M.
- $an \in N$ ogni volta che $a \in A, n \in N$.

Esempi 1.5.

(1) Sia $\mathbb{K}$ un campo. Abbiamo già visto come un $\mathbb{K}$-modulo sia semplicemente uno spazio vettoriale su $\mathbb{K}$. Se V è un $\mathbb{K}$-modulo, i sotto $\mathbb{K}$-moduli di V sono semplicemente i sottospazi vettoriali di V.
(2) $\{0\}$ ed M sono sempre sottomoduli di ogni A-modulo M: sono detti *sottomoduli banali*.
(3) Gli A-sottomoduli dell'A-modulo A sono semplicemente gli ideali di A.

Definizione 1.6. Un'applicazione tra A-moduli $f : M \to N$ si dice *applicazione A-lineare*, o anche *A-omomorfismo* o *omomorfismo di A-moduli* se:

- $f(m + m') = f(m) + f(m')$,
- $f(a \cdot m) = a \cdot f(m)$,

per ogni scelta di $a \in A, m, m' \in M$.

Osservazione 1.7. Segue immediatamente dalla definizione che, se f è un A-omomorfismo, allora:

$$f(0) = f(0 \cdot m) = 0 \cdot f(m) = 0, \qquad f(-m) = f((-1) \cdot m) = (-1) \cdot f(m) = -f(m).$$

Proposizione 1.8. *Sia $f : M \to N$ un A-omomorfismo. Allora l'immagine*

$$f(M) = \operatorname{Im} f = \{n \in N \mid n = f(m) \text{ per qualche } m \in M\}$$

e il nucleo

$$\ker f = \{m \in M \mid f(m) = 0\}$$

sono sottomoduli di N e di M rispettivamente. L'omomorfismo f è suriettivo se e solo se $f(M) = N$ ed è iniettivo se e solo se $\ker f = (0)$.

Dimostrazione. Come al solito. È lasciata per esercizio. □

Un A-omomorfismo iniettivo e suriettivo si dice *A-isomorfismo*. L'inverso di un A-isomorfismo è ancora A-lineare ed è quindi esso stesso un A-isomorfismo.

1.2. **Moduli quoziente e teorema di omomorfismo.** Siano M, N A-moduli, $N \subseteq M$ sottomodulo. Allora

$$m \sim_N m' \iff m' - m \in N$$

definisce su M una relazione di equivalenza (controllatelo per esercizio!) e quindi un insieme quoziente $M/\sim_N$.

Esercizio: Verificate che le operazioni $[m]+[m'] = [m+m']$ e $a[m] = [am]$ sono ben definite sulle classi di equivalenza e che soddisfano gli assiomi di A-modulo.

Definizione 1.9. L'insieme $M/\sim_N$ dotato della struttura di A-modulo appena descritta si dice *modulo quoziente*, e si indica con M/N.

La proiezione al quoziente $\pi : M \to M/N$ è un omomorfismo suriettivo di A-moduli, il cui nucleo coincide con N.

Teorema 1.10. *Sia $f : M \to M'$ un omomorfismo di A-moduli, $N \subseteq M$ un sottomodulo contenuto in* $\ker f$*. Se indichiamo con $\pi : M \to M/N$ la proiezione al quoziente, allora esiste un unico A-omomorfismo $F : M/N \to M'$ tale che $f = F \circ \pi$. F ed f hanno la stessa immagine: in particolare, F è suriettivo se e solo se f è suriettivo; inoltre F è iniettivo se e solo se* $\ker f = N$.

Dimostrazione. La solita. Anche questa per esercizio. □

Quello appena visto è il cosiddetto teorema di omomorfismo, che si presenta analogo in molteplici contesti algebrici. Ha le solite conseguenze, che si dimostrano come da tradizione.

Teorema 1.11. *Se $f : M \to N$ è un omomorfismo di A-moduli, allora $f(M)$ è isomorfo al quoziente $M/\ker f$.*

Dimostrazione. L'applicazione $F : M/\ker f \to N$ è iniettiva, e la sua immagine coincide con $f(M) \subseteq N$. Pertanto F definisce un isomorfismo di $M/\ker f$ con $f(M)$. □

Se $N, N' \subseteq M$ sono sottomoduli, anche $N \cap N'$ e $N + N' = \{n + n' \mid n \in N, n' \in N'\}$ sono sottomoduli di M (esercizio!).

Teorema 1.12. *$(N + N')/N'$ è isomorfo a $N/(N \cap N')$.*

Dimostrazione. Sia $\pi : M \to M/N'$ la proiezione al quoziente. Allora $\pi|_N : N \to M/N'$ è un A-omomorfismo la cui immagine coincide con $(N + N')/N'$, ed il cui nucleo è $N \cap N'$. Per il risultato precedente $(N + N')/N' = \operatorname{Im} \pi|_N \simeq N/\ker \pi|_N = N/(N \cap N')$. □

Infine

Teorema 1.13. *Sia M un A-modulo, siano $N_0 \subseteq N \subseteq M$ sottomoduli. Allora: $M/N \simeq (M/N_0)/(N/N_0)$.*

Dimostrazione. Come al solito. □

1.3. **Somma diretta di A-moduli.** Se M, N sono A-moduli, le operazioni:

$$(m, n) + (m', n') = (m + m', n + n'), \qquad a \cdot (m, n) = (am, an)$$

definiscono sul prodotto cartesiano $M \times N$ una struttura di A-modulo detta *somma diretta* di M ed N, che si indica con $M \oplus N$. La somma diretta si può fare anche di tre o più A-moduli, e persino di una famiglia infinita di A-moduli. In questo caso la definizione è:

Definizione 1.14. Sia $\{M_i\}_{i \in I}$ una famiglia di A-moduli. L'insieme:

$$\bigoplus_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i,\ m_i \neq 0 \text{ solo per un numero finito di indici}\}.$$

è un A-modulo rispetto alle operazioni di $+$ e $\cdot$ definite componente per componente, detto *somma diretta* degli $\{M_i\}_{i \in I}$.

Osservazione 1.15. Analogamente alla definizione appena data, si può definire anche su

$$\prod_{i\in I} M_i = \{(m_i)_{i\in I} \mid m_i \in M_i\}.$$

una struttura di A-modulo, che è detta *prodotto diretto* degli $\{M_i\}_{i\in I}$. Il prodotto diretto di A-moduli è generalmente più grande della somma diretta. Ad ogni modo, somma diretta e prodotto diretto di un numero *finito* di A-moduli coincidono.

Esempio 1.16. $A^n = \bigoplus_{i=1}^n A = \underbrace{A \oplus A \oplus \cdots \oplus A}_{n \text{ volte}}$

Il risultato che segue ci servirà più tardi.

Lemma 1.17. *Siano M, N A-moduli, $M' \subseteq M, N' \subseteq N$ sottomoduli. Allora $N \oplus N'$ è un sottomodulo di $M \oplus M'$ e*

$$(M \oplus N)/(M' \oplus N') \simeq M/M' \oplus N/N'.$$

Dimostrazione. Che $M' \oplus N'$ sia un sottomodulo di $M \oplus N$ è chiaro. L'omomorfismo $\pi : M \oplus N \to M/M' \oplus N/N'$ dato da $\pi(m, n) = ([m]_{M'}, [n]_{N'})$ è suriettivo, ed il suo nucleo coincide con $M' \oplus N'$. Ora basta utilizzare il Teorema 1.11. □

2. Dipendenza ed indipendenza lineare negli A-moduli

Siano $m_1, \ldots, m_n$ elementi di un A-modulo M. Si dice combinazione A-lineare di $m_1, \ldots, m_n$ ogni espressione del tipo $a_1m_1 + \cdots + a_nm_n, a_i \in A$. Se $X \subseteq M$ è un sottoinsieme (anche infinito) di elementi di M, una combinazione lineare di elementi di X è ogni espressione: $a_1m_1 + \cdots + a_nm_n \in X, \quad a_i \in A$. È importante osservare che le combinazioni lineari sono sempre *finite*, perché non sapremmo sommare infiniti termini distinti, a meno di invocare strutture ulteriori (topologia, convergenza, ecc ...) che non abbiamo. Sappiamo sommare due elementi e quindi anche un insieme finito di elementi, ripetendo ricorsivamente l'operazione di somma.

Definizione 2.1. Sia M un A-modulo, $X \subseteq M$ un sottoinsieme. Il sottomodulo di M generato da X è il più piccolo sottomodulo di M che contenga X, e si indica con $\langle X \rangle$.

L'intersezione di sottomoduli di M è ancora un sottomodulo, e quindi:

$$\langle X \rangle = \bigcap_{\substack{N \subseteq M \text{ sottomodulo} \\ X \subseteq N}} N,$$

il che garantisce l'esistenza del sottomodulo generato da $X \subseteq M$. È importante osservare che se m appartiene ad un sottomodulo N, anche i suoi multipli am, $a \in A$, stanno in N. Allo stesso modo, se $m_1, \ldots, m_n \in N$, allora $a_1m_1 + \cdots + a_nm_n \in N$ per ogni scelta di $a_i \in A$. Sappiamo dalla definizione che $X \subseteq \langle X \rangle$, e quindi $\langle X \rangle$ deve contenere ogni combinazione lineare di elementi di X.

Proposizione 2.2. *$\langle X \rangle$ coincide con l'insieme delle combinazioni lineari degli elementi di X.*

Dimostrazione. Basta far vedere che l'insieme delle combinazioni lineari è chiuso rispetto alla somma e al prodotto per elementi di A. □

Se $M = \langle X \rangle$, con $X \subseteq M$, diremo che *X è un insieme di generatori per M*. Un A-modulo M si dice *finitamente generato* se possiede un insieme finito di generatori, cioè se esistono $m_1, \ldots, m_n \in M$ tali che ogni elemento di M si esprima come $a_1m_1 + \cdots + a_nm_n$ per una scelta oppurtuna di $a_1, \ldots, a_n \in A$. Da questo momento in poi darò le definizioni solo nel caso finito, poiché saremo principalmente interessati ai moduli finitamente generati.

Definizione 2.3. Sia M un A-modulo. Gli elementi $m_1, \ldots, m_n \in M$ si dicono

- *A-liberi* o *linearmente indipendenti su A* se
$$a_1m_1 + \cdots + a_nm_n = 0 \Longrightarrow a_1 = a_2 = \cdots = a_n = 0,$$
cioè se l'unica combinazione lineare nulla è quella a coefficienti tutti nulli;
- *generatori* di M se per ogni elemento $m \in M$ esistono $a_1, \ldots, a_n$ tali che $m = a_1m_1 + \cdots + a_nm_n$;
- una *A-base* di M se sono generatori A-liberi di M.

Gli elementi $m_1, \ldots, m_n$ sono *linearmente dipendenti* se non sono linearmente indipendenti. Se $m_1, \ldots, m_n$ sono A-liberi si dice che $\{m_1, \ldots, m_n\}$ è un insieme *libero* o *A-libero*, o semplicemente *A-linearmente indipendente*. L'insieme vuoto è sempre libero.

Per ogni scelta di $m_1, \ldots m_n \in M$ possiamo costruire l'applicazione $f : A^n \to M$ definita da $f(a_1, \ldots, a_n) = a_1m_1 + \cdots + a_nm_n$. Se $\underline{a} = (a_1, \ldots, a_n)$ e $\underline{a}' = (a'_1, \ldots, a'_n)$ allora $\underline{a} + \underline{a}' = (a_1 + a'_1, \ldots, a_n + a'_n)$, e:

$$\begin{aligned} f(\underline{a} + \underline{a}') &= (a_1 + a'_1)m_1 + \cdots + (a_n + a'_n)m_n \\ &= a_1m_1 + a'_1m_1 + \cdots + a_nm_n + a'_nm_n \\ &= (a_1m_1 + \cdots + a_nm_n) + (a'_1m_1 + \cdots + a'_nm_n) \\ &= f(\underline{a}) + f(\underline{a}'). \end{aligned}$$

In modo simile si mostra che $f(c\underline{a}) = cf(\underline{a})$, e dunque f è A-lineare.

Proposizione 2.4. *L'omomorfismo di A-moduli $A^n \ni (a_1, \dots, a_n) \mapsto a_1 m_1 + \cdots + a_n m_n \in M$ è:*

- *iniettivo se e solo se $m_1, \dots, m_n$ sono linearmente indipendenti;*
- *suriettivo se e solo se $m_1, \dots, m_n$ generano M;*
- *un isomorfismo se e solo se $m_1, \dots, m_n$ sono una base di M.*

Dimostrazione. E' una riformulazione delle definizioni. □

Questo mostra che un A-modulo che possiede una base con n elementi è isomorfo ad A^n. Gli A-moduli che possiedono una base sono detti *liberi*. Se M è un A-modulo libero ed $m_1, \dots, m_n \in M$ costituiscono una sua base, allora l'inversa della $f : A^n \to M$ costruita sopra è l'A-omomorfismo che associa a ciascun $m \in M$ le sue "coordinate" nella base $m_1, \dots, m_n$. È importante osservare come ogni isomorfismo $f : A^n \to M$ sia costruibile a partire da una base.

Lemma 2.5. *Sia $f : A^n \to M$ un omomorfismo di A-moduli. Se poniamo $m_1 = f(1, 0, \dots, 0)$, $m_2 = f(0, 1, 0, \dots, 0), \dots$, $m_n = f(0, \dots, 0, 1)$, allora $f(a_1, \dots, a_n) = a_1 m_1 + \cdots + a_n m_n$.*

Dimostrazione. Poiché $(a_1, \dots, a_n) = a_1(1, 0, \dots, 0) + \cdots + a_n(0, \dots, 0, 1)$, allora $f(a_1, \dots, a_n) = a_1 f(1, 0, \dots, 0) + \cdots + a_n f(0, \dots, 0, 1) = a_1 m_1 + \cdots + a_n m_n$. □

Proposizione 2.6. *Sia $f : A^n \to M$ un isomorfismo di A-moduli. Allora $m_1 = f(1, 0, \dots, 0)$, $m_2 = f(0, 1, 0, \dots, 0), \dots$, $m_n = f(0, \dots, 0, 1)$ sono una base di M.*

Dimostrazione. Segue dal lemma precedente e dalla Proposizione 2.4. □

In conclusione, gli isomorfismi $A^n \to M$ sono in corrispondenza biunivoca con le basi di M e gli isomorfismi $M \to A^n$ sono tutti e soli quelli che calcolano le coordinate degli elementi di M in qualche base. Prima di passare avanti, osserviamo come ad ogni A-omomorfismo $T : A^m \to A^n$ si possa associare una matrice $n \times m$ — che indicheremo con $[T]$ — a coefficienti in A, tale che:

$$T(a_1, \dots, a_n) = (b_1, \dots, b_n) \text{ se e solo se } [T] \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

Tale matrice $[T]$ è quella che ha per colonne le immagini $T(1, 0, \dots, 0), \dots, T(0, \dots 0, 1)$ degli elementi della *base canonica* di A^n. Alla composizione di applicazioni corrisponde, ovviamente, il prodotto righe per colonne di matrici:

$$[T \circ S] = [T] \cdot [S]$$

3. Determinante di matrici a valori in un anello commutativo con unità

Avete già incontrato il concetto di determinante di una matrice $n \times n$ a coefficienti in un campo. Sapete che se $M = (m_{ij})_{i,j=1,\dots,n}$ è una matrice a coefficienti in un campo $\mathbb{K}$, il suo determinante è definito da:

$$\det M = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot m_{1\sigma_1}, m_{2\sigma_2}, \dots, m_{n\sigma_n}.$$

Dove S_n è l'insieme (anzi: il gruppo) delle permutazioni su n elementi e $\operatorname{sgn}(\sigma)$ è il segno della permutazione σ. Il determinante soddisfa $\det \mathrm{Id} = 1, \det MN = (\det M)(\det N)$, è multilineare sia come funzione delle righe che delle colonne della matrice usata come argomento, ed è alternante per scambi di righe e/o di colonne. Avete inoltre appreso la procedura di calcolo per la matrice inversa di M, quando esiste: cioè esattamente quando $\det M \neq 0$. Non ripercorrerò le relative dimostrazioni, ma mi limiterò a motivare come, a partire da questi enunciati, si possano ottenere affermazioni simili anche per matrici a coefficienti in un anello commutativo con unità qualsiasi, che sia o meno un campo o un dominio d'integrità. La prima osservazione importante da fare è che possiamo utilizzare il campo di nostra preferenza. Abbiamo già visto in precedenza come costruire, a partire da un dominio d'integrità D un campo che lo contenga, detto "campo delle frazioni" $\mathbb{K} = \mathbb{K}_D$. Per matrici a coefficienti in $\mathbb{K}$, e quindi in particolare per matrici a coefficienti in D, tutte le affermazioni continueranno ad essere valide. È importante notare che la formula per il determinante è data come una somma di prodotti, e quindi non richiede mai la necessità di calcolare inversi. L'anello che ci interessa considerare è quello

$$D = \mathbb{Z}[x_{11}, x_{12}, \dots, x_{1n}, x_{21}, \dots, x_{2n}, \dots, x_{n1}, \dots, x_{nn}, y_{11}, \dots, y_{nn}],$$

dei polinomi a coefficienti in $\mathbb{Z}$ nelle $2n^2$ variabili $x_{ij}, y_{ij}, 1 \leq i, j \leq n$. Questo è certamente un dominio di integrità e possiede un campo della frazioni — per la cronaca $\mathbb{K}_D$ si indica con $\mathbb{Q}(x_{11}, \dots, x_{nn}, y_{11}, \dots, y_{nn})$. Poiché $\det(MN) = (\det M)(\det N)$ vale per matrici a coefficienti in $\mathbb{K}_D$, vale anche per matrici a coefficienti in D. Ad esempio, vale per le due matrici:

$$M = \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \dots & x_{nn} \end{pmatrix}, N = \begin{pmatrix} y_{11} & \dots & y_{1n} \\ \vdots & & \vdots \\ y_{n1} & \dots & y_{nn} \end{pmatrix}, \text{ che sono a coefficienti in } D.$$

Questo ci dice che l'identità $\det(MN) = \det M \det N$ è vera in termini delle espressioni polinomiali in x_{ij}, y_{ij} *prima* di utilizzare la conoscenza del valore che possiamo attribuire ai coefficienti delle matrici. In altre parole, la formula di Binet $\det(MN) = \det M \det N$ vale per matrici a coefficienti indeterminati. Se A è un anello commutativo, e M, N

sono matrici a coefficienti in A, basta calcolare l'identità polinomiale di Binet in $x_{ij} = m_{ij}, y_{ij} = n_{ij}$ per ottenerla per le matrici "concrete", $M = (m_{ij}), N = (n_{ij})$ che abbiamo bisogno di considerare.

Nel calcolo del determinante ci sono solo somme di prodotti e non abbiamo mai bisogno di "uscire" dalll'anello $\mathbb{Z}[x_{11}, \dots, x_{nn}, y_{11}, \dots, y_{nn}]$ per poter descrivere l'identità, che può poi essere calcolata per ogni scelta di elementi in un anello commutativo. Tutte le proprietà di multilinearità e alternanza seguono alla stessa maniera. Più delicato è l'algoritmo di calcolo della matrice inversa, che richiede prima il calcolo dei minori $(n-1) \times (n-1)$ della matrice M — i cosidetti "complementi algebrici" — e poi la divisione per $\det M$. Effettivamente, quando A non è un campo, non è detto che $\det M$, anche se diverso da 0, sia invertibile.

Lemma 3.1. *Siano M, N matrici $n \times n$ a coefficienti in un anello commutativo con unità A tali che $MN = NM = \mathrm{Id}$. Allora $\det M$ e $\det N$ sono elementi invertibili di A.*

Dimostrazione. Per la formula di Binet $\det(M)\det(N) = \det(MN) = \det \mathrm{Id} = 1$. □

Questo dimostra che una matrice $M \in \mathrm{Mat}_{n\times n}(A)$ che voglia avere la speranza di essere invertibile deve avere $\det(M) \in A^\times$.

Teorema 3.2. *$M \in \mathrm{Mat}_{n\times n}(A)$ è invertibile in $M \in \mathrm{Mat}_{n\times n}(A)$ se e solo se $\det(M) \in A^\times$.*

Dimostrazione. Una delle due implicazioni è già stata mostrata nel lemma precedente. Viceversa, supponiamo che $\det(M) \in A^\times$. Sia $X = (x_{ij})_{i,j=1,\dots,n}$ la matrice $n \times n$ a coefficienti in $D = \mathbb{Z}[x_{11}, \dots, x_{nn}]$. Il calcolo della sua inversa in $\mathbb{K}_D$ è possibile ($\det X$ è un polinomio non nullo in D) ma richiede l'inversione di $\det X$; tuttavia vi è un'identità per matrici a coefficienti in $\mathbb{K}_D$ che non richiede l'inversione di elementi. Se X^C è la matrice dei complementi algebrici di X (cioè la matrice matrice il cui coefficiente X^C_{ij} è $(-1)^{i+j}$ moltiplicato per il determinante della matrice che si ottiene rimuovendo da X la i-esima colonna e la j-esima riga), allora:

$$X^C \cdot X = (\det X)\,\mathrm{Id} = X \cdot X^C$$

Poichè il calcolo di X^C e $\det X$ richiede solo somme di prodotti, otteniamo una formula *universale*, cioè a coefficienti indeterminati, che può essere "specializzata" agli elementi di qualsiasi anello commutativo con unità. Ora, se $M \in \mathrm{Mat}_{n\times n}(A)$, allora $M^C \cdot M = (\det M)\,\mathrm{Id} = M \cdot M^C$. E se $\det M$ è invertibile in A, allora moltiplicando l'identità precedente per $(\det M)^{-1}$ si ottiene $(\det M)^{-1} \cdot M^C \cdot M = \mathrm{Id} = M \cdot M^C \cdot (\det M)^{-1}$. In conclusione, abbiamo trovato un'inversa $(\det M)^{-1} M^C$ della matrice M non appena $\det M \in A^\times$. □

Corollario 3.3. *Se $M \in \mathrm{Mat}_{m\times n}(A), N \in \mathrm{Mat}_{n\times m}(A), MN = \mathrm{Id}_m, NM = \mathrm{Id}_n$, allora $m = n$ e $\det(M), \det(N) \in A^\times$. In particolare, un A-omomorfismo $f : A^m \to A^n$ può essere invertibile se e solo se $m = n$, e in questo caso la sua invertibilità è equivalente all'invertibilità del determinante della sua matrice.*

Dimostrazione. Sia $m \neq n$. A meno di scambiare le due matrici, possiamo suppore che $m > n$. Allora:

$$(M|0)\begin{pmatrix} N \\ \hline 0 \end{pmatrix} = (MN) = \mathrm{Id}_n\,.$$

Ma questo è impossibile poiché $\det(M|0) = 0$. In effetti, moltiplicando per 0 una delle colonne nulle, il determinante viene moltiplicato per 0 e quindi diventa 0. Ma la matrice resta la stessa. □

4. Basi di moduli liberi

In algebra lineare vale il seguente risultato:

Proposizione 4.1. *Sia V uno spazio vettoriale su $\mathbb{K}$. Da ogni sottoinsieme di $\mathbb{K}$-generatori di V si può estrarre una $\mathbb{K}$-base; inoltre, ogni insieme di elementi $\mathbb{K}$-linearmente indipendenti di V si può completare una base.*

In particolare, tutti gli elementi non nulli di uno spazio vettoriale possono far parte di una base. Sono tutti "equivalenti", insomma. La situazione è diversa per gli A-moduli, come andiamo a mostrare con esempi.

Lemma 4.2. *Nell'A-modulo A, due elementi, comunque siano presi, sono sempre linearmente dipendenti.*

Dimostrazione. dati $a, b \in A$, si ha $b \cdot a + (-a) \cdot b = 0$, che è una relazione di dipendenza lineare non appena $a, b \neq 0$. Se $a = b = 0$, ogni $h \cdot a + k \cdot b$ è uguale a 0, e quindi si ha ancora dipendenza lineare. □

Esempi 4.3.

(1) Se $A = \mathbb{Z}$, $M = \mathbb{Z}$, allora $\{2\}$ è un insieme libero che non può essere completato ad una base. In effetti, se $a \cdot = 0$, allora $a = 0$, quindi $\{2\}$ è linearmente indipendente. $\{2\}$ genera tutto il sottomodulo dei pari e quindi non genera tutto $\mathbb{Z}$. In ogni caso, se aggiungiamo anche solo un elemento a $\{2\}$ ottieniamo, per il lemma, un insieme non libero.
(2) Se $A = \mathbb{Z}, M = \mathbb{Z}$, allora $\{2, 3\}$ è un insieme di generatori di M dal quale non si estrae alcuna base. L'insieme $\{2, 3\}$ è un insieme di generatori di $\mathbb{Z}$ poiché $2 \cdot 2 - 1 \cdot 3 = 1$ e quindi $2h \cdot 2 - h \cdot 3 = h$. In ogni caso $\{2, 3\}$ non è una base per il lemma, e nessuno dei sottoinsiemi propri $\{2\}, \{3\}, \emptyset$ è un insieme di generatori.

Abbiamo bisogno di un criterio per stabilire se un insieme $\{m_1, \cdots, m_h\}$ di elementi di A^n sia una base. Sappiamo già che h deve essere uguale ad n, poiché l'applicazione:

$$A^h \xrightarrow{f} A^n$$
$$(a_1, \cdots, a_h) \mapsto a_1 m_1 + \cdots + a_h m_h$$

deve essere un isomorfismo se $\{m_1, \ldots, m_h\}$ è una base.

Proposizione 4.4. *$\{m_1, \ldots, m_n\} \subseteq A^n$ è una A-base se e solo se la matrice che ha per colonne le coordinate degli elementi $m_1, \ldots, m_n$ è invertibile in A.*

Dimostrazione. $m_1, \ldots, m_n$ è una base se e solo se l'A-omomorfismo $A^n \ni (a_1, \ldots, a_n) \mapsto a_1 m_1 + \cdots + a_n m_n \in A^n$ è invertibile. Questo accade se e solo se la matrice associata ha determinante invertibile. È facile osservare che le colonne di tale matrice sono le coordinate degli elementi $m_1, \ldots, m_n$. □

Corollario 4.5. *Se $d \in A$ è un elemento non invertibile tale che $d | a_1, \ldots, a_n$, allora $(a_1, \ldots, a_n)$ non appartiene a nessuna base di A^n.*

Dimostrazione. Ogni matrice che abbia una colonna uguale a $(a_1, \ldots, a_n)$ ha determinante multiplo di d, e quindi non invertibile. □

Daremo una caratterizzazione degli elementi che si completano ad una base di A^n, nel caso in cui A sia un dominio a ideali principali.

4.1. **Moduli liberi in domini a ideali principali.** Sia D un dominio a ideali principali. Il mio obiettivo è quello di dimostrare la seguente

Proposizione 4.6. *L'elemento $(a_1, \ldots, a_n) \in D^n$ appartiene a qualche base di D^n se e solo se* $\mathrm{MCD}(a_1, \ldots, a_n) = 1$.

Prima di passare alla dimostrazione, cerchiamo di capire i casi $n = 1, 2$.

Esempi 4.7.

(1) $\{a\}$ è una base di $D \iff a$ è invertibile in D.
In effetti, il sottomodulo di D generato da a è l'ideale (a), che è uguale a $D \iff a$ è invertibile.
(2) $(a, b) \in D^2$ si completa ad una base di $D^2 \iff \mathrm{MCD}(a, b) = 1$.
In effetti, se $\mathrm{MCD}(a, b) = 1$, allora esistono $h, k \in D$ tali che $ha + kb = 1$. Ma allora:

$$\det \begin{pmatrix} a & -k \\ b & h \end{pmatrix} = 1,$$

e quindi $\{(a, b), (-k, h)\}$ è una base di D^2.

Abbiamo già visto che se $\mathrm{MCD}(a, b) = d \neq 1$ e quindi non invertibile, allora (a, b) non appartiene a nessuna base.

Lemma 4.8. *Sia $\underline{a} = (a_1, a_2, \ldots, a_n) \in D^n$. Allora esiste una base di D^n nella quale le coordinate di $\underline{a}$ sono $(d, a_3, a_4, \ldots, a_n, 0)$, dove $d = \mathrm{MCD}(a_1, a_2)$. Equivalentemente, esiste un D-omomorfismo invertibile $\phi : D^n \to D^n$ tale che: $\phi(a_1, \ldots, a_n) = (d, a_3, \ldots, a_n, 0)$.*

Dimostrazione. Sia $d = \mathrm{MCD}(a_1, a_2)$. Allora $a_1 = db_1, a_2 = db_2$ con $\mathrm{MCD}(b_1, b_2) = 1$. Si ha quindi $hb_1 + kb_2 = 1$, per un'oppurtuna scelta di $h, k \in D$. Consideriamo i vettori $m_1 = (b_1, b_2, 0, \ldots, 0), m_2 = (-k, h, 0, \ldots, 0), m_3 = (0, 0, 1, 0, \ldots, 0), \ldots, m_n = (0, \ldots, 0, 1)$. Sono sicuramente una base poiché:

$$\det \left(\begin{array}{cc|c} b_1 & -k & 0 \\ b_2 & h & \\ \hline 0 & & I_{n-2} \end{array} \right) = \det \begin{pmatrix} b_1 & -k \\ b_2 & h \end{pmatrix} = 1.$$

e in questa base $(a_1, \ldots, a_n)$ si esprime come:

$$(a_1, a_2, a_3, \ldots, a_n) = d(b_1, b_2, 0, \ldots, 0) + (0, 0, a_3, a_4, \ldots, a_n) = dm_1 + 0 \cdot m_2 + a_3 m_3 + \cdots + a_n m_n$$

Chiaramente, anche $m_1, m_3, \ldots, m_n, m_2$ è una base di D^n, nella quale le coordinate di $\underline{a} = (a_1, a_2, \ldots, a_3)$ sono $(d, a_3, a_4, \ldots, a_n, 0)$. □

Proposizione 4.9. *Sia $\underline{a} = (a_1, a_2, \ldots, a_n) \in D^n, d = \mathrm{MCD}(a_1, \ldots, a_n)$. Allora esiste una base di D^n in cui le coordinate di $\underline{a}$ sono $(d, 0, \ldots, 0)$. Equivalentemente, esiste $\phi : D^n \to D^n$ invertibile tale che $\phi(a_1, \ldots, a_n) = (d, 0 \ldots, 0)$.*

Dimostrazione. Applicando il lemma precedente $n - 1$ volte, si trovano A-omomorfismi invertibili $\phi_1, \phi_2 \ldots, \phi_n$ tali che:

$$(a_1, \ldots, a_n) \overset{\phi_1}{\mapsto} (\mathrm{MCD}(a_1, a_2), a_3, \ldots, a_n, 0) \overset{\phi_2}{\mapsto} (\mathrm{MCD}(a_1, a_2, a_3), a_4, \ldots, a_n, 0, 0) \overset{\phi_3}{\mapsto} \cdots \overset{\phi_{n-1}}{\mapsto} (\mathrm{MCD}(a_1, \ldots, a_n), 0, \ldots, 0).$$

La composizione $\phi_{n-1} \circ \phi_{n-2} \circ \cdots \circ \phi_2 \circ \phi_1$ è ancora un A-omomorfismo invertibile. □

Teorema 4.10. *$\underline{a} = (a_1, \ldots, a_n) \in D^n$ appartiene ad una base di $D^n \iff \mathrm{MCD}(a_1, \ldots, a_n) = 1$.*

Dimostrazione. $\Rightarrow$: lo abbiamo già visto nel Corollario 4.5.
$\Leftarrow$: Se $\mathrm{MCD}(a_1, \ldots, a_n) = 1$, allora esiste una base in cui le coordinate di $\underline{a}$ sono $(1, 0, \ldots, 0)$, cioè una base della quale è il primo elemento. □

Nel caso $D = \mathbb{Z}, \mathrm{MCD}(a_1, \dots, a_n)$ misura quanti punti si vedono tra $(a_1, \dots, a_n)$ e l'origine. I vettori che appartengono a basi di D^n sono tutti e soli quelli che vedono l'origine.

Nel seguito, chiamerò $\mathrm{MCD}(a_1, \dots, a_n)$ la "lunghezza" dell'elemento $(a_1, \dots, a_n)$, e la indicherò con $\ell(a_1, \dots, a_n)$. È importante osservare che $\ell(a_1, \dots, a_n)$ è un elemento di D definito a meno di moltiplicazione per un invertibile. La dimostrazione precedente rende chiaro che la lunghezza è indipendente dalla base nella quale sono calcolate le coordinate. Si noti che 1 è la lunghezza minima, mentre 0 è quella massima (!).

5. La funzione lunghezza e le sue proprietà

Se $\underline{a} = (a_1, \dots, a_n) \in D^n$, dove D è un dominio ad ideali principali, poniamo $\ell(\underline{a}) = \mathrm{MCD}(a_1, a_2, \dots, a_n)$. L'applicazione ℓ associa ad ogni n-upla un elemento definito a meno di invertibili (cioè un elemento dell'insieme quoziente $D/\sim$ ottenuto da D considerando la relazione di equivalenza $\sim$ di essere uguali a meno di invertibili).

Lemma 5.1. *$\ell(a_1, \dots, a_n) \mid a_1$. Inoltre $\ell(a_1, \dots, a_n) = a_1 \iff a_1$ divide tutti gli a_i*

Dimostrazione. Sono ovvie proprietà del MCD. □

Dirò che un elemento $\underline{a} \in N$ ha lunghezza minimale

Vi ricordo che in un insieme parzialmente ordinato $(X, \leq)$ un elemento $x \in X$ è minimale se $y \in X, y \leq x \Rightarrow x = y$, ed è minimo se $x \leq y \quad \forall y \in X$. Ogni elemento minimo è anche minimale, ma il viceversa è generalmente falso.

Proposizione 5.2. *Se $N \subseteq D^n$ è un sottomodulo e $(d, 0, \dots, 0) \in N$ è un suo elemento di lunghezza minimale, allora per ogni $(a_1, \dots, a_n) \in N$, d divide tutti gli a_i.*

Dimostrazione. Innanzitutto, mostriamo che d divide a_1.
Se $d_1 = \mathrm{MCD}(d, a_1)$, allora esistono $h, k \in D$ tali che $d_1 = hd + ka_1$, per l'identità di Bézout. Allora $\underline{b} = h(d, 0, \dots, 0) + k(a_1, \dots, a_n)$ è un elemento di N, poiché combinazione lineare di elementi di N. Inoltre il suo primo coefficiente è d_1 e quindi, per il lemma precedente, $\ell(\underline{b}) \leq d_1 \leq d = \ell(d, 0, \dots, 0)$. Per la minimalità della lunghezza di $d, 0, \dots, 0)$, deve essere $\ell(\underline{b}) = d$ e quindi $d = \mathrm{MCD}(d, a_1)$. In altre parole, d divide a_1. Mostriamo adesso che d divide anche gli altri coefficienti a_i. Poiché $(a_1, \dots, a_n) \in N$, abbiamo già mostrato che $d \mid a_1$ e quindi che $a - 1 = hd$. Allora anche $\underline{c} = (a_1, \dots, a_n) - (h-1)(d, 0, \dots 0) = (d, a_2, \dots, a_n)$ è un elemento di N, e $\ell(\underline{c}) \leq d$, poiché d è il suo primo coefficiente. Per la minimalità della lunghezza di $d, 0, \dots, 0)$ deve essere $\ell(\underline{c}) = d$; ma allora d divide $a_2, \dots, a_n$. □

Osservazione 5.3. nelle ipotesi della proposizione precedente, abbiamo mostrato che la lunghezza di $(d, 0, \dots, 0)$ è in realtà minimo, poiché se $(a_1, \dots, a_n) \in N$, allora d divide ogni a_i e anche il loro $\mathrm{MCD} = \ell(a_1, \dots n)$. Di conseguenza $d \leq \ell(\underline{n})$ per ogni $\underline{n} \in N$.

Corollario 5.4. *Sia $N \subseteq D^{n+1} = D \oplus D^n$ un sottomodulo, e supponiamo che un elemento della forma $(d, 0, \dots, 0)$ sia in N, e abbia lunghezza minimale tra gli elementi di N. Allora esiste un sottomodulo $N' \subseteq D^n$ tale che $N = (d) \oplus N' \subseteq D \oplus D^n = D^{n+1}$.*

Dimostrazione. Sia $N' = \{a_1, \dots, a_n) \in D^n \mid (0, a_1, \dots, a_n) \in N\}$. Se $(a_0, a_1, \dots, a_n) \in N$ abbiamo visto che d divide a_0. Ma allora, se $a_0 = dh$ si ha:

$$(a_0, a_1, \dots, a_n) = h(d, 0, \dots, 0) + (0, a_1, \dots, a_n),$$

e $(0, a_1, \dots, a_n) \in N$ poiché è la differenza di elementi in N. Di conseguenza $(a_1, \dots, a_n) \in N$. In conclusione, $(a_0, a_1, \dots, a_n) \in (d) \oplus N'$ per ogni scelta di $(a_0, \dots, a_n) \in N$, cioè $N \subseteq (d) \oplus N'$. L'altra inclusione è ovvia. □

6. Classificazione dei moduli finitamente generati su domini a ideali principali

Teorema 6.1. *Sia D un dominio a ideali principali, e M un D-modulo finitamente generato, Allora esistono $d_1 | d_2 | \dots | d_n$ in D tali che:*

$$M \simeq {}^{D}\!/_{(d_1)} \oplus {}^{D}\!/_{(d_2)} \oplus \cdots \oplus {}^{D}\!/_{(d_n)}.$$

Dimostrazione. Siamo $m_1, \dots, m_n \in M$ generatori. Possiamo costruire un omomorfismo suriettivo $D^n \overset{f}{\twoheadrightarrow} M$ Per il teorema di omomorfismo, $M \simeq {}^{D^n}\!/_{\ker f}$, dove $\ker f$ è un sottomodulo. A meno di un isomorfismo di $D^n, \ker f$ è della forma $(d_1) \oplus (d_2) \oplus \cdots \oplus (d_n)$ con $d_1 | d_2 | \dots | d_n$, e quindi:

$$\begin{aligned} {}^{D}\!/_{\ker f} &\simeq {}^{D^N}\!/_{(d_1) \oplus (d_2) \oplus \cdots \oplus (d_n)} \\ &= {}^{D \oplus D \oplus \cdots \oplus D}\!/_{(d_1) \oplus (d_2) \oplus \cdots \oplus (d_n)} \\ &= {}^{D}\!/_{(d_1)} \oplus {}^{D}\!/_{(d_2)} \oplus \cdots \oplus {}^{D}\!/_{(d_n)}. \end{aligned}$$

Se d_i è invertibile, $(d_1) = D$, ${}^{D}\!/_{D} = (0)$ può essere rimosso dalla somma diretta. □

Osservazione 6.2. I moduli ${}^{D}\!/_{(d_1)}$ sono D-moduli ciclici, e si può quindi dire che i moduli finitamente generati sono tutti somma diretta di moduli ciclici.

7. Invarianti di moduli finitamente generati su PID

Sia D un dominio a ideali principali. Abbiamo appena visto che ogni D-modulo finitamente generato M è isomorfo ad una somma diretta

$$M \simeq D/(d_1) \oplus D/(d_2) \oplus \cdots \oplus D/(d_n).$$

per un'opportuna scelta di elementi $d_1|d_2|\ldots|d_n \in D$. E' in principio possibile che M ammetta due scelte diverse dei d_i, ma questo in realtà non accade, ed è quello che dimostriamo in questo paragrafo.

Lemma 7.1. *Siano $N \subset M$ due D-moduli. Se $m_1, \ldots, m_k$ generano il D-modulo M, allora le corrispondenti proiezioni $\overline{m_1}, \ldots, \overline{m_k}$ generano il quoziente M/N.*

Dimostrazione. Immediato. □

Proposizione 7.2. *Siano $d_1|d_2|\ldots|d_n$ elementi non invertibili di D. Allora ogni insieme di generatori del D-modulo $M = D/(d_1) \oplus D/(d_2) \oplus \cdots \oplus D/(d_n)$ contiene almeno n elementi. In particolare, n è il minimo numero di generatori del D-modulo M.*

Dimostrazione. Sia p un divisore irriducibile di d_1, così che $K = D/(p)$ sia un campo. Allora $(p) \supset (d_i)$ per ogni $i = 1, \ldots, n$; in particolare

$$(p) \oplus (p) \oplus \cdots \oplus (p) \supset (d_1) \oplus \cdots \oplus (d_n).$$

Questo mostra che $K^n \simeq D^{\oplus n}/(p)^{\oplus n}$ è un quoziente di M.

Se $m_1, \ldots, m_k$ è un insieme di generatori D-lineari di M, le corrispondenti proiezioni $\overline{m_1}, \ldots, \overline{m_k}$ generano il D-modulo K^n. Ad ogni modo, ogni D-combinazione lineare in K^n è in realtà una K-combinazione lineare e quindi i k elementi che abbiamo elencato generano K^n come K-spazio vettoriale. Ma allora $k \geq n$ segue dai soliti ragionamenti di algebra lineare.

L'ultima affermazione segue dal fatto che $([1], [0], \ldots, [0]), \ldots, ([0], \ldots, [0], [1])$ è un insieme di esattamente n generatori D-lineari di M. □

Se M è un D-modulo e $a \in D$, allora la moltiplicazione per a è un endomorfismo D-lineare $M \to M$. La sua immagine $a.M$ è quindi un sottomodulo di M.

Lemma 7.3. *Siano $a, d \in D$, con d non invertibile. Allora*

$$a.D/(d) = (a, d)/(d) \simeq D/(d/\operatorname{MCD}(a, d)).$$

In particolare, $a.D/(d) = 0$ esattamente quando $a \in (d)$.

Dimostrazione. Sia $m = \operatorname{MCD}(a, d)$. Per l'identità di Bézout, esistono $h, k \in D$ tali che $m = ha + kd$. Allora $[m] = [ha + kd] = h[a]$ in $D/(d)$ e quindi $[m] \in a.D/(d)$. Viceversa, poiché m divide a, si ha $[a] \in m.D/(d)$. Questo mostra che $a.D/(d) = m.D/(d)$ o equivalentemente

$$a.D/(d) = m.D/(d) = (a, d)/d.$$

Poiché m divide d, scriviamo $d = mb$, dove $b = d/\operatorname{MCD}(a, d) \in D$. L'applicazione $f : D \to D/(d)$ definita da $x \mapsto [mx]$ è un omomorfismo di D-moduli e la sua immagine $(m)/(d)$ è quindi isomorfa a $D/\ker f$. Si vede subito che $\ker f = (b)$ e quindi $(m)/(d)$ è isomorfo a $D/(b)$.

In conclusione, $a.D/(d)$ è il D-modulo banale esattamente quando b è invertibile in D, cioè quando $\operatorname{MCD}(a, d) = d$ o equivalentemente $a \in (d)$. □

Corollario 7.4. *Siano $d_1|d_2|\ldots|d_n$ elementi non invertibili di D, $M = D/(d_1) \oplus D/(d_2) \oplus \cdots \oplus D/(d_n)$. Se $a \in D$, il D-modulo $a.M$ possiede un insieme di generatori con meno di n elementi esattamente quando $a \in (d_1)$.*

Dimostrazione. Per il Lemma precedente, si ha

$$a.M = a.D/(d_1) \oplus a.D/(d_2) \oplus \cdots \oplus a.D/(d_n),$$

e quindi un insieme di generatori del D-modulo $a.M$ possiede sempre almeno n elementi, a meno che $a.D/(d_i) = 0$ per qualche i. Questo accade quando $a \in (d_i)$ per qualche i, nel qual caso inevitabilmente $a \in (d_1)$. □

Teorema 7.5. *Siano $d_1|d_2|\ldots|d_n$ elementi non invertibili di D, $M = D/(d_1) \oplus D/(d_2) \oplus \cdots \oplus D/(d_n)$.*

Allora gli elementi non invertibili[1] $d_1, \ldots, d_n \in D$ sono univocamente determinati, a meno di associati, da M.

Dimostrazione. Per induzione su n. Se $n = 1$, allora $M = D/(d) \neq \{0\}$ è generato da $[1]$. Inoltre (d) coicide con l'*annullatore* $\operatorname{Ann} M := \{a \in D \mid a.M = \{0\}\}$ di M. Pertanto d è il generatore di $\operatorname{Ann} M$, ed è quindi univocamente determinato a meno di associati.

Sia ora $n > 1$. Allora n è la minima cardinalità di un insieme di generatori del D-modulo M, mentre d_1 genera l'ideale

$$\{a \in D \mid a.M \text{ ammette un insieme di generatori con meno di } n \text{ elementi}\},$$

ed è quindi univocamente determinato a meno di associati.

Inoltre $M/d_1.M$ è isomorfo a

$$D/(d_1/d_1) \oplus D/(d_2/d_1) \oplus \cdots \oplus D/(d_n/d_1).$$

[1] nonché il loro numero!

Il numero di addendi non nulli coincide allora con il numero di d_i non associati a d_1, mentre i rimanenti quozienti d_i/d_1 sono determinati, a meno di associati, da $M/d_1.M$. □

8. Forme canoniche di endomorfismi e Teorema di Cayley-Hamilton

Da scrivere.

9. Un controesempio

L'anello $D = \mathbb{C}[x, y]$ è un dominio a fattorizzazione unica, ma i suoi ideali non sono tutti principali. Ad esempio, l'ideale $I = (x, y)$ non è principale in quanto un suo generatore dovrebbe dividere sia x che y, e gli unici tali elementi sono le costanti non nullo, che generano tutto D; tuttavia, I è propriamente contenuto in D, in quanto contiene tutti e soli gli elementi i polinomi di termine noto nullo.

L'ideale I è un D-modulo finitamente generato — è per definizione generato dagli elementi x, y. Vogliamo convincerci del fatto che I non è isomorfo a nessun D-modulo della forma $D/I_1 \oplus D/I_2 \oplus \dots D/I_n$, dove $I_1 \supsetneq I_2 \supsetneq \cdots \supsetneq I_n$ sono ideali propri di D.

Intanto, il minimo numero di generatori D-lineari di I è due, poiché I non è un ideale principale ma è generato da due elementi. Questo mostra che un eventuale isomorfismo obbligherebbe $n = 2$. Ora, se $I \simeq D/I_1 \oplus D/I_2$, allora I sarebbe somma diretta di due suoi D-sottomoduli $J_1, J_2 \subset I$ non nulli; poiché $I \subset D$, tali sottomoduli sarebbero ideali non banali di D ad intersezione nulla. Ma allora $xy = 0$ per ogni scelta di $x \in J_1, y \in J_2$, il che è impossibile dal momento che D è un dominio d'integrità.

Questo mostra che l'enunciato del Teorema di classificazione dei moduli finitamente generati su domini a ideali principali non può valere per anelli più generali, nemmeno se si tratta di domini a fattorizzazione unica.

Dipartimento di Matematica, Università degli studi di Roma – "La Sapienza"
E-mail address: dandrea@mat.uniroma1.it