Università degli Studi di Firenze
Facoltà di Scienze Matematiche, Fisiche e Naturali
C.d.L. in Matematica

Anno Accademico 2011-2012
Relazione finale per la Laurea Triennale

DIAGONALIZZAZIONE SU UN PID E APPLICAZIONI ALL'OMOLOGIA

Diagonalization over PIDs and applications in Homology

Candidato:
Luca Simi

Relatore:
Prof. Giorgio Ottaviani

Introduzione

L'obiettivo di questa relazione è quello di descrivere un procedimento automatizzato per determinare i gruppi di omologia simpliciale. Lo strumento fondamentale è la diagonalizzazione, che verrà presentata per matrici a valori in un PID. Una prima applicazione è il teorema di struttura per i moduli finitamente generati su un PID, che darà un significato più preciso al problema di determinare un gruppo di omologia. Nel corso dell'elaborato verrà dedotta la forma di Jordan in modo semplice a partire dai teoremi di struttura. L'ultima parte tratterà il problema centrale, presentando un algoritmo per determinare la struttura dei gruppi di omologia. Il problema verrà affrontato per i moduli finitamente generati su un PID.

1. Diagonalizzazione

Esistenza della forma canonica di Smith

Definizione 1.1 (forma canonica di Smith)**.** Siano R un anello commutativo, e $A \in R^{m,n}$. Si dice che A è in *forma canonica di Smith* se:

$$A = \left[\begin{array}{ccc|c} \alpha_1 & & & \\ & \ddots & & \\ & & \alpha_r & \\ \hline & & & \end{array}\right]$$

dove $(\alpha_r) \subseteq \ldots \subseteq (\alpha_1)$. Gli α_i, non nulli, sono detti *fattori invarianti* di A.

Proposizione 1.1. *Sia R un PID. È definita $\lambda : R \setminus \{0_R\} \to \mathbb{N}$ tale che $\lambda(r)$ è il numero di fattori irriducibili di r. Inoltre per ogni $a, b \in R \setminus \{0_R\}$ valgono le seguenti proprietà:*

1. $\lambda(ab) = \lambda(a) + \lambda(b)$
2. $\lambda(a) = 0 \iff a$ *è invertibile.*
3. *Se a divide b, e b non divide a:* $\lambda(a) < \lambda(b)$

Teorema 1.1 (Esistenza)**.** *Sia R un PID, e $A \in R^{m,n}$. Esistono due matrici $Q \in GL_m(R)$ e $P \in GL_n(R)$, tali che $A' = QAP^{-1}$ è in forma di Smith. L'algoritmo per trovare Q e P^{-1} è descritto nella dimostrazione.*

dim. Costruiamo un algoritmo iterativo che trasforma A in forma di Smith. Ad ogni passo dell'iterazione la matrice viene trasformata nella forma:

$$\left[\begin{array}{c|c} a & \\ \hline & B \end{array}\right]$$

dove a divide ogni elemento di B.

Primo passo:

- Primo caso: *A non è nulla.* Esistono i, j tali che $A_{i,j} \neq 0_R$ con $\lambda(A_{i,j})$ minimo. Permutando righe e colonne spostiamo $A_{i,j}$ in posizione $(1, 1)$. Andiamo avanti al secondo passo.

- Secondo caso: *A è nulla.* Non procediamo oltre.

Secondo passo:

- Primo caso: *$A_{1,1}$ divide tutti gli elementi della prima riga e della prima colonna.* Annulliamo gli $A_{i,1}$ per ogni $i > 1$ sommando alle righe opportuni multipli della prima. In modo analogo annulliamo gli $A_{1,j}$ per ogni $j > 1$. Andiamo al terzo passo.
- Secondo caso: *Almeno un elemento nella prima colonna non è multiplo di $A_{1,1}$.* Poniamo $\beta = \gcd(A_{1,1}, A_{i,1})$. Per l'identità di Bézout esistono $\sigma, \tau \in R$ tali che $\beta = \sigma A_{1,1} + \tau A_{i,1}$. Inoltre esistono $\alpha, \gamma \in R$ tali che $A_{1,1} = \alpha\beta$ e $A_{i,1} = \gamma\beta$. Sia:

$$L = \left[\begin{array}{ccccc|c} \sigma & & & & \tau & \\ & 1_R & & & & \\ & & \ddots & & & \\ & & & 1_R & & \\ -\gamma & & & & \alpha & \\ \hline & & & & & I_{m-i} \end{array}\right]$$

  L è invertibile: $\det(L)\beta = \sigma\alpha\beta + \tau\gamma\beta = \sigma A_{1,1} + \tau A_{i,1} = \beta$, pertanto $\det(L) = 1_R$. Per le proprietà di λ abbiamo $\lambda(\beta) < \lambda(A_{1,1})$: $A_{1,1}$ non divide $A_{i,1}$, quindi β divide $A_{1,1}$, ma $A_{1,1}$ non divide β. Sostituendo A con LA il nuovo elemento in posizione $(1,1)$ è β. Torniamo al primo passo.
- Terzo caso: *Almeno un elemento nella prima riga non è multiplo di $A_{1,1}$.* Procediamo analogamente al caso precedente.

Terzo passo:

- Primo caso: *$A_{i,j}$ è multiplo di $A_{1,1}$ per ogni $i, j > 1$.* Sia B la matrice ottenuta da A eliminando prima riga e prima colonna. Il passo iterativo termina.
- Secondo caso: *Esistono $i > 1, j > 1$ tali che $A_{1,1}$ non divide $A_{i,j}$.* Sommiamo la j-esima colonna alla prima. Torniamo indietro al secondo passo.

Termine: Ogni volta che il flusso dell'algoritmo dal secondo passo si sposta al primo, o dal terzo al secondo, il valore $\lambda(A_{1,1})$ diminuisce. Se non termina prima, il valore minimo di $\lambda(A_{1,1})$ è 1. In tal caso $A_{1,1}$ è diventato invertibile e la procedura termina. Per diagonalizzare una matrice proseguiamo lavorando nello stesso modo su B.

Divisibilità: Escludendo il caso in cui $A = 0$, ogni volta che dal passo 3 torniamo al passo 1 ($A_{1,1}$ divide gli $A_{i,j}$ per ogni $i, j > 1$) proseguiamo modificando la nuova matrice A con prodotti destri e sinistri, al termine dei quali i nuovi $A_{i,j}$ saranno ancora multipli dello stesso fattore, quindi $\alpha_i \mid \alpha_{i+1}$ per ogni i.

□

Caratterizzazione dei fattori invarianti delle matrici

Definizione 1.2 (Equivalenza tra matrici)**.** Sia R un anello commutativo. Due matrici $A, B \in R^{m,n}$ si dicono *equivalenti* se esistono $Q \in GL_m(R)$ e $P \in GL_n(R)$ tali che $B = QAP^{-1}$.

Definizione 1.3 (Rango di una matrice)**.** Sia R un anello commutativo e $A \in R^{m,n}$. Si definisce *rango* di A il massimo intero r per cui A possiede un minore di ordine r non nullo. Si indica con $\mathrm{rk}(A)$.

Definizione 1.4 (Fattori determinanti)**.** Sia R un anello commutativo e $A \in R^{m,n}$. Per $1 \leq k \leq \mathrm{rk}(A)$ si dice *fattore determinante* di ordine k il massimo comun divisore dei minori di ordine k di A. Si indica con $d_k(A)$.

Proposizione 1.2. *Sia R un anello commutativo e $A \in R^{m,n}$.*

1. *Per $1 \leq k \leq \mathrm{rk}(A)$ abbiamo $d_k(A) \neq 0_R$.*
2. *Per $1 \leq k < \mathrm{rk}(A)$ abbiamo $d_k(A) \mid d_{k+1}(A)$.*

Proposizione 1.3. *Sia R un anello commutativo. Siano $Q \in R^{m,m}$ e $A \in R^{m,n}$. Allora $\mathrm{rk}(QA) \leq \mathrm{rk}(A)$.*

dim. I minori di ordine k di QA sono combinazioni lineari dei minori di ordine k di A, quindi se questi ultimi sono tutti nulli, ogni minore di ordine k di QA è nullo. Poichè i minori di QA di ordine superiore a k sono combinazioni lineari di quelli di ordine k il rango di QA può al massimo eguagliare quello di A. □

Proposizione 1.4. *Sia R un anello commutativo e $A, B \in R^{m,n}$ matrici equivalenti. Allora $\mathrm{rk}(A) = \mathrm{rk}(B) = r$. Se inoltre R è un PID per $1 \leq k \leq r$ si ha che $d_k(A)$ e $d_k(B)$ sono associati.*

Teorema 1.2 (Essenziale unicità dei fattori invarianti)**.** *Sia R un PID e $A \in R^{m,n}$. La forma canonica di Smith di A è definita a meno di fattori invarianti associati.*

dim. Siano $A', A'' \in R^{m,n}$ due forme diagonali di Smith di A. Dal momento che A' e A'' sono equivalenti abbiamo $\mathrm{rk}(A') = \mathrm{rk}(A'') = r$ e $d_k(A') = d_k(A'')$ per $1 \leq k \leq r$. Dall'uguaglianza dei ranghi possiamo affermare che il numero di fattori invarianti è lo stesso. Chiamando α_i i fattori invarianti di A' e β_i quelli di A'' è facile calcolare $d_k(A')$ e $d_k(A'')$:

$$d_k(A') = \prod_{i=1}^{k} \alpha_i \ , \ d_k(A'') = \prod_{i=1}^{k} \beta_i$$

Da cui otteniamo $d_{k+1}(A') = d_k(A')\alpha_{k+1}$, $d_{k+1}(A'') = d_k(A'')\beta_{k+1}$. Possiamo quindi affermare che α_k e β_k sono associati per $1 \leq k \leq r$. □

2. Teoremi di struttura

Relazioni e matrici di presentazione

Definizione 2.1. Siano V un R-modulo e $v_1, \ldots, v_m \in V$. Una *relazione* sugli elementi $v_1, \ldots, v_m$ è un'equazione del tipo $r_1v_1 + \ldots + r_mv_m = 0$ e $[r_1, \ldots, r_m]^T$ viene detto *vettore di relazione*.

Definizione 2.2. Sia V un R-modulo generato da $v_1, \ldots, v_m$. L'insieme dei vettori di relazione forma un sottomodulo $V^{(1)} \subseteq R^m$. Un *insieme completo di relazioni* è una base per $V^{(1)}$.

Definizione 2.3. Sia $\phi : W \to W'$ un morfismo di R-moduli. Si dice *cokernel* di ϕ l'R-modulo quoziente $W'/\mathrm{Im}(\phi)$. Nel caso di $\phi : R^n \to R^m$, se A è la matrice associata a ϕ il cokernel di ϕ si scrive come R^m/AR^n. Un R-isomorfismo $R^m/AR^n \to V$ si dice *presentazione* di V e la matrice A si dice *matrice di presentazione* per V.

Proposizione 2.1. *Sia R un PID. Siano V un R-modulo libero di rango m e W un R-sottomodulo di V. Esistono una base $\{v_1, \ldots, v_m\}$ di V e una base $\{w_1, \ldots, w_n\}$ di W tali che:*

1. *$n \leq m$.*
2. *Per ogni $i \leq n$ esiste $\alpha_i \in R$ tale che $w_i = \alpha_i v_i$.*
3. *$(\alpha_n) \subseteq \ldots \subseteq (\alpha_1)$.*

Proposizione 2.2. *Ogni R-modulo finitamente generato ha una presentazione.*

dim. Sia V un R-modulo generato da $v_1, \ldots, v_m$. È definito il morfismo suriettivo $f : R^m \to V$ che manda $(r_1, \ldots, r_m)$ in $r_1 v_1 + \ldots + r_m v_m$. Sia $W = \ker(f)$. Per il teorema di omomorfismo R^m/W è isomorfo a V. W è libero, con n generatori e $n \leq m$. Siano $w_1, \ldots, w_n \in W$ una base per W. Definiamo $g : R^n \to W$ come prima è stata definita f. Il morfismo $\phi : R^n \to R^m$, ottenuto componendo g con l'inclusione $W \to R^m$ può essere descritto da una matrice $A \in R^{m,n}$ in termini di moltiplicazione a sinistra. $\phi(R^n) = AR^n = W$. Quindi V è isomorfo a R^m/AR^n e A è una matrice di presentazione per V. Le colonne di A generano W, quindi formano un insieme completo di relazioni. □

Proposizione 2.3. *Sia V un R-modulo e $A \in R^{m,n}$ una sua matrice di presentazione. Le seguenti matrici A' sono matrici di presentazione per V.*

1. *$A' = QAP^{-1}$, per ogni $Q \in GL_m(R)$ e $P \in GL_n(R)$.*
2. *A' ottenuta da A rimuovendo una colonna nulla.*
3. *A' ottenuta da A rimuovendo i-esima riga e j-esima colonna se la j-esima colonna di A è $u\boldsymbol{e_i}$ con $u \in R$ invertibile.*

<u>**Teoremi di struttura**</u>

Definizione 2.4 (Fattori invarianti dei moduli)**.** Siano R un PID e V un R-modulo finitamente generato. Se esistono $v_1, \ldots, v_m \in V$ non nulli tali che $V = Rv_1 \oplus \ldots \oplus Rv_m$ e $\mathrm{ann}(v_m) \subseteq \ldots \subseteq \mathrm{ann}(v_1)$. Ponendo $\mathrm{ann}(v_i) = (\alpha_i)$, gli α_i sono detti *fattori invarianti* di V e $Rv_1 \oplus \ldots \oplus Rv_m$ viene detta *decomposizione in fattori invarianti* di V.

Teorema 2.1 (Teorema di struttura - Decomposizione in fattori invarianti)**.** *Siano R un PID e V un R-modulo finitamente generato. Allora V ammette una decomposizione in fattori invarianti.*

dim. Sia A una matrice di presentazione. La sua forma di Smith presenta ancora V, siano α_i i suoi fattori invarianti. Eliminiamo le colonne nulle. Rimuoviamo anche le righe e le colonne i-esime ogni volta che α_i è invertibile. La matrice così modificata avrà m righe e k colonne, con $m \geq k$, e ogni elemento diagonale soddisferà le condizioni richieste. Essendo ancora una matrice di presentazione, deduciamo che V è generato da m elementi $v_1, \ldots, v_m$, dei quali i primi k soddisfano le relazioni $\alpha_i v_i = 0$. Proviamo $V = Rv_1 \oplus \ldots \oplus Rv_m$. È evidente che $V = Rv_1 + \ldots + Rv_m$. Sia $z_1 + \ldots + z_k + w = 0_V$ con $z_j \in Rv_j$ e $w \in Rv_{k+1} + \ldots + Rv_m$. Ogni elemento z_j può essere scritto come $r_j v_j$ per qualche $r_j \in R$, w può essere scritto come $r_{k+1}v_{k+1} + \ldots + r_m v_m$. La relazione diventa $r_1 v_1 + \ldots + r_m v_m = 0_V$. Dato che le colonne di A formano un insieme completo di relazioni il vettore $[r_1, \ldots, r_m]^t$ è combinazione lineare delle colonne, pertanto gli elementi r_j per ogni $j > k$ sono tutti nulli. Per quanto riguarda i precedenti, ogni r_j è multiplo di α_j per $1 \leq j \leq$, e $r_j = s_j \alpha_j$ per qualche $s_j \in R$. Abbiamo $z_j = s_j \alpha_j v_j = 0$ per $1 \leq j \leq k$. Inoltre, per la stessa ragione, $\mathrm{ann}(v_j) = \alpha_j$. □

Teorema 2.2 (Teorema cinese dei resti)**.** *Sia R un PID e siano $d_1, \ldots, d_k \in R$ elementi a due a due coprimi. Sia $d = d_1 \ldots d_k$. L'anello quoziente R/dR è isomorfo a $R/d_1R \times \ldots \times R/d_kR$ mediante il morfismo di anelli $f : R/dR \to R/d_1R \times \ldots \times R/d_kR$ tale che $f(r + dR) = (r + d_1R, \ldots, r + d_kR)$.*

Teorema 2.3 (Teorema di struttura - Decomposizione in ciclici primari)**.** *Sia R un PID e V un R-modulo finitamente generato. Esistono $v_1, \ldots, v_m \in V$ tali che $V = Rv_1 \oplus \ldots \oplus Rv_k \oplus \ldots \oplus Rv_m$ tali che* $\mathrm{ann}(v_1)$ *è potenza di un primo per $1 \leq i \leq k$ e* $\mathrm{ann}(v_i) = 0$ *per $i > k$.*

Caratterizzazione dei fattori invarianti dei moduli

Proposizione 2.4 (Il numero dei fattori invarianti è unico)**.** *Siano R un PID e V un R-modulo finitamente generato. Siano $v_1, \ldots, v_m, w_1, \ldots, w_n \in V$ tali che $V = Rv_1 \oplus \ldots \oplus Rv_m = Rw_1 \oplus \ldots \oplus Rw_n$. Siano* $\mathrm{ann}(v_i) = (\alpha_i)$ *e* $\mathrm{ann}(w_j) = (\beta_j)$*, con $\alpha_i, \beta_j \in R$ non invertibili. Sia inoltre $(\alpha_m) \subseteq \ldots \subseteq (\alpha_1)$ e $(\beta_n) \subseteq \ldots \subseteq (\beta_1)$. Allora $m = n$.*

dim. In quanto insiemi di generatori possiamo scrivere $v_i = \sum_{l=1}^{m} r_{i,l} w_l$ e $w_l = \sum_{j=1}^{n} s_{l,j} v_j$ con $r_{i,l}, s_{l,j} \in R$. Supponiamo $m < n$. Siano $A, B \in R^{n,n}$ con $A_{i,l} = r_{i,l}$ per $1 \leq l \leq m$, $A_{i,l} = 0_R$ altrimenti, analogamente sia $B_{l,j} = s_{l,j}$ per $1 \leq l \leq m$, $B_{l,j} = 0_R$ altrimenti. Abbiamo $v_i = \sum_{l=1}^{m} r_{i,l} \left(\sum_{j=1}^{n} s_{l,j} v_j \right) = \sum_{j=1}^{n} \left(\sum_{l=1}^{m} r_{i,l} s_{l,j} \right) v_j$. Osserviamo che $(AB)_{i,j} = \sum_{l=1}^{m} r_{i,l} s_{l,j}$. Dalla somma diretta abbiamo che α_j divide $(AB)_{i,j}$ se $i \neq j$ e α_i divide $\sum_{l=1}^{m} r_{i,l} s_{l,j} - 1_R$ se $i = j$. Inoltre α_1 divide ogni α_i, pertanto la matrice AB ha la seguente forma:

$$AB = \begin{bmatrix} h_{1,1}\alpha_1 + 1_R & \cdots & h_{1,n}\alpha_1 \\ \vdots & \ddots & \vdots \\ h_{n,1}\alpha_1 & \cdots & h_{n,n}\alpha_1 + 1_R \end{bmatrix}$$

Con $h_{i,j} \in R$. Abbiamo $\det(AB) = \det(A)\det(B) = 0_R$ perchè A e B hanno almeno una riga o una colonna nulla. Sviluppando il determinante abbiamo che $\det(AB) = h\alpha_1 + 1_R$ per qualche $h \in R$, quindi $h\alpha_1 + 1_R = 0_R$. Questo significa che α_1 è invertibile e $Rv_1 = 0$, che è assurdo. □

Proposizione 2.5 (Caratterizzazione dei fattori invarianti - Essenziale unicità)**.** *Siano R un PID e V un R-modulo finitamente generato. Siano $v_1, \dots, v_m \in V$ tali che $V = Rv_1 \oplus \dots \oplus Rv_m$. Sia* $\operatorname{ann}(v_i) = (\alpha_i)$ *con $\alpha_i \in R$ non invertibili. Sia inoltre $(\alpha_m) \subseteq \dots \subseteq (\alpha_1)$. Allora $\alpha_i = \gcd\{s \in R$ tale che sV ha al più $m - i$ fattori invarianti $\}$.*

dim. Sia $s \in R$, allora:

$$sV = sRv_1 \oplus \dots \oplus sRv_m = Rsv_1 \oplus \dots \oplus Rsv_m \cong R/(d_1) \times \dots \times R/(d_m)$$

dove $(d_i) = \operatorname{ann}(sv_i)$. Se $(rs)v_i = 0$ allora $rs \in (\alpha_i)$, quindi $\operatorname{ann}(sv_i) = \alpha_i / \gcd(\alpha_i, s)$. Quindi $(d_i) = (\alpha_i / \gcd(\alpha_i, s))$ e vale ancora $(d_m) \subseteq \dots \subseteq (d_1)$. I d_i invertibili corrispondono esattamente a componenti $R(sv_i)$ nulle, che rimuoviamo. Il numero di generatori rimossi è almeno i, perchè sicuramente rimuoviamo i primi i generatori, quindi sV ha al più $m-i$ fattori invarianti. □

3. Forma canonica di Jordan

Applicazioni lineari e moduli

Osservazione. Applicazioni lineari tra F-spazi vettoriali e $F[t]$-moduli sono concetti equivalenti:

- Sia V uno spazio vettoriale su un campo F e $T : V \to V$ un'applicazione lineare. Possiamo definire su V una struttura di $F[t]$-modulo: per ogni $f(t) = a_n t^n + \dots + a_1 t + a_0 \in F[t], v \in V$ poniamo $f(t)v = a_n T^n(v) + \dots a_1 T(v) + a_0$.
- Sia V è un $F[t]$-modulo. Possiamo assegnare su V una struttura di spazio vettoriale su F restringendo il prodotto per scalari ai polinomi costanti. Inoltre è definito l'operatore lineare $T : V \to V$ tale che $T(v) = tv$.

Forma canonica razionale

Osservazione. Sia V uno spazio vettoriale di dimensione finita e $T : V \to V$ un'applicazione lineare. Allora V con la struttura indotta di $F[t]$-modulo è un modulo di torsione.

Proposizione 3.1 (Forma canonica razionale)**.** *Sia V uno spazio vettoriale di dimensione n su un campo F. Sia $T : V \to V$ un'applicazione lineare. Esiste una base su V in cui la matrice associata a T è composta da blocchi della seguente forma:*

$$\left[\begin{array}{ccc|c} & & & -c_0 \\ \hline 1 & & & -c_1 \\ & \ddots & & \vdots \\ & & 1 & -c_{n-1} \end{array}\right]$$

dim. L'operatore T induce su V una struttura di $F[t]$-modulo. Avendo dimensione finita come spazio vettoriale, diventa un $F[t]$-modulo di torsione, decomponendo: $V = W_1 \oplus \dots \oplus W_n$ con W_i ciclici di torsione. Per ogni i, W_i è $F[t]$-isomorfo al quoziente $F[t]/(f_i(t))$, con $f_i(t) \in F[t]$ monico di grado $r_i = \dim(W_i)$. Inoltre W_i e $F[t]/(f_i(t))$ sono isomorfi come spazi vettoriali.

Sia $w_{i,0} = 1_F + (f_i(t))$, generatore di $F[t]/(f_i(t))$ come $F[t]$-modulo. Gli elementi $w_{i,k} = t^k w_{i,0}$ per $0 \leq k < r_i$ sono una base di $F[t]/(f_i(t))$ come spazio vettoriale su F. Pertanto $\{w_{i,k}$ t.c. $1 \leq i \leq n$ e $0 \leq k \leq r_i\ \}$ è una base di $F[t]/(f_1(t)) \oplus \ldots \oplus F[t]/(f_n(t))$. Se $f_i(t) = t^n + a_{i,r_i-1}t^{n-1} + \ldots + a_{i,1}t + a_{i,0}$ valgono le relazioni $w_{i,k+1} = tw_{i,0}$ per $0 \leq k < n-1$ e $w_n = -a_0 w_1 \ldots - a_{n-1} w_{n-1}$. L'operatore T come $F[t]$-morfismo corrisponde alla moltiplicazione per t sulla base, quindi ha la forma cercata. □

Forma canonica di Jordan

Teorema 3.1 (Forma canonica di Jordan)**.** *Sia V uno spazio vettoriale su $\mathbb{C}$ di dimensione finita. Sia $T : V \to V$ un'applicazione lineare. Esiste una base su V in cui la matrice associata a T è composta da blocchi della seguente forma (blocchi di Jordan):*

$$\begin{bmatrix} \lambda & & & \\ 1 & \ddots & & \\ & \ddots & \lambda & \\ & & 1 & \lambda \end{bmatrix}$$

dim. Decomponiamo V nella somma diretta di $\mathbb{C}[t]$-sottomoduli ciclici primari. Ogni $\mathbb{C}[t]$-modulo ciclico primario è isomorfo a $\mathbb{C}[t]/((t-\lambda)^n)$ per qualche n. Definendo w_0 come un generatore di $\mathbb{C}[t]/((t-\lambda)^n)$, gli elementi $w_i = (t-\lambda)^i w_0$ sono una base di $\mathbb{C}[t]/((t-\lambda)^n)$. In questo caso valgono $w_{i+1} = (t-\lambda)w_i$ per $0 \leq i < n-1$ e $(t-\lambda)w_{n-1} = 0$. La matrice corrispondente è un blocco di Jordan. □

4. Omologia

Definizione 4.1. Un *complesso di catene* è una successione

$$\cdots \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} \cdots \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_1} C_0 \longrightarrow 0$$

di R-moduli C_i e di R-morfismi $\partial_i : C_i \to C_{i-1}$, chiamati *operatori bordo*, con la proprietà $\partial_i \circ \partial_{i+1} = 0$.

Osservazione. $\partial_i \circ \partial_{i+1} = 0$ e $\mathrm{Im}(\partial_{n+1}) \subseteq \ker(\partial_n)$ sono equivalenti.

Definizione 4.2. Si definisce *n-esimo R-modulo di omologia* il quoziente

$$H_n = \ker(\partial_n)/\mathrm{Im}(\partial_{n+1}).$$

Notazione. Se C_n e C_{n-1} hanno generatori, cioè se sono entrambi non nulli, è definita la matrice associata a ∂_n, scritta nelle basi assegnate, che indichiamo con D_n.

Osservazione. Se R è un PID e C_{n+1}, C_n, C_{n-1} sono R-moduli finitamente generati e non nulli, è possibile determinare H_n con un procedimento automatico:

1. *Determiniamo una base opportuna per* $\ker(\partial_n)$*:*
   C_n è un R-modulo libero (diciamo di rango k), quindi gli elementi di $\ker(\partial_n)$, nella base assegnata di C_n, sono caratterizzati da $D_n[r_1, \ldots, r_k]^T = [0_R, \ldots, 0_R]^T$, sistema che, in generale, può essere complicato da risolvere. Indicando con $D'_n = QD_nP^{-1}$ la forma di Smith di D_n e con $d_1, \ldots d_s$ i suoi fattori invarianti, il sistema diventa semplice:

   $$D'_n[r'_1, \ldots, r'_k]^T = [d_1r'_1, \ldots, d_sr'_s, 0_R, \ldots, 0_R]^T = [0_R, \ldots, 0_R]^T$$

   L'equazione $d_jr'_j = 0_R$, ammette, come unica soluzione $r'_j = 0_R$. Abbiamo $r'_j = 0_R$ per le prime s coordinate e per le rimanenti non abbiamo vincoli: $0_Rr'_j = 0_R$ è comunque vera, indipendentemente da r'_j. Quindi $\ker(\partial_n)$ è generato dagli ultimi $k - s$ elementi della nuova base di C_n. Questi, scritti nella vecchia base di C_n, sono le ultime $k - s$ colonne della matrice P^{-1}. Abbiamo $QD_nP^{-1}[r'_1, \ldots, r'_k]^T = [0_R, \ldots, 0_R]^T$, quindi $D_nP^{-1}[r'_1, \ldots, r'_k]^T = Q^{-1}[0_r, \ldots, 0_R]^T = [0_r, \ldots, 0_R]^T$. Dall'invertibilità di P abbiamo $[r_1, \ldots, r_k]^T = P^{-1}[r'_1, \ldots, r'_k]^T$

2. *Determiniamo una base per* $\mathrm{Im}(\partial_{n+1})$*:*
   La matrice PD_{n+1} descrive ∂_{n+1} nella nuova base di C_n. Dato che $\mathrm{Im}(\partial_{n+1}) \subseteq \ker(\partial_n)$ le colonne di PD_{n+1} sono elementi di $\ker(\partial_n)$ (che è generato dagli ultimi $k-s$ elementi della nuova base di C_n), quindi le prime s righe di PD_{n+1} sono nulle. Sia B la matrice ottenuta da PD_{n+1} rimuovendo le prime s righe. B descrive l'applicazione $\partial_{n+1} : C_{n+1} \to \ker(\partial_n)$. Sia B' ottenuta diagonalizzando B. Le colonne non nulle costituiscono i generatori di $\mathrm{Im}(\partial_{n+1})$, scritti nella base di $\ker(\partial_n)$. Sono generatori indipendenti, perchè multipli non nulli di elementi della base di $\ker(\partial_n)$.

3. *Decomponiamo* H_n*:*
   Abbiamo determinato una base di $\ker(\partial_n)$ e una base di $\mathrm{Im}(\partial_{n+1})$ costituita da multipli della prima. In generale se V è generato dalla base $(v_1, \ldots, v_n)$ e W dalla base $(d_1v_1, \ldots, d_mv_m)$ con $m \leq n$, il quoziente V/W è generato da $(v_1+W, \ldots, v_n+W)$, quindi $V/W = R(v_1+W)+\ldots+R(v_n+W)$. Sia $(r_1v_1 + W) + \ldots + (r_nv_n + W) = W$, cioè $r_1v_1 + \ldots + r_nv_n \in W$. Pertanto ogni r_i è multiplo di d_i e $r_iv_i + W = W$. Concludiamo in questo modo $V/W = R(v_1 + W) \oplus \ldots \oplus R(v_n + W)$, che è isomorfo a $R/(d_1) \oplus \ldots \oplus R/(d_m) \oplus R^{n-m}$. In questo modo abbiamo decomposto H_n (il numero di righe nulle in B' è uguale al numero di generatori della parte libera di H_n).

La procedura descritta funziona quando C_{n+1}, C_n, C_{n-1} sono finitamente generati e non nulli. In caso contrario almeno una matrice tra D_{n+1} e D_n non è definita (dovrebbe avere una dimensione nulla). Tuttavia possiamo usare i ragionamenti già fatti per adattare l'algoritmo. Supponiamo che C_n sia diverso da 0 (altrimenti $H_n = 0$). Analizziamo adesso i casi possibili per C_{n+1} e C_{n-1}:

1. $0 \longrightarrow C_n \xrightarrow{\partial_n} C_{n-1}$:
   In questo caso H_n è isomorfo a $\ker(\partial_n)$, che è libero. Per calcolare il numero di generatori è sufficiente diagonalizzare D_n, e contare le colonne nulle (al passo 1 della procedura abbiamo fatto proprio questo).

2. $C_{n+1} \xrightarrow{\partial_{n+1}} C_n \longrightarrow 0$:
   In questo caso $H_n = C_n/\mathrm{Im}(\partial_{n+1})$. Sia D'_{n+1} ottenuta diagonalizzando D_{n+1}. In questo modo abbiamo determiniamo due nuove basi, una di C_{n+1} e una di C_n, in cui l'operatore ∂_{n+1} possiede forma diagonale. Il gruppo $\mathrm{Im}(\partial_{n+1})$ è libero ed è generato dalle colonne non nulle di D'_{n+1}. La torsione è descritta dai fattori invarianti di D'_{n+1}. Per calcolare la dimensione della parte libera basta contare il numero di righe nulle (è analogo al passo 2, lavorando su D_{n+1} invece che su PD_{n+1}).

3. $0 \longrightarrow C_n \longrightarrow 0$:
   In questo caso $H_n \cong C_n$.

Teorema 4.1. *Data la successione* $C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1}$. *La seguente procedura consente di determinare la decomposizione in fattori invarianti di* H_n*:*

- Se $C_n = 0$:
  $H_n = 0$.
- Se $C_n \neq 0$:
  - Se $C_{n+1} \neq 0$ e $C_{n-1} \neq 0$:
    1. *Sia* D'_n *la forma di Smith di* D_n*:* $D'_n = QD_nP^{-1}$ *con* P *e* Q *invertibili.*
    2. *Se* D'_n *ha esattamente* s *fattori invarianti sia* B *ottenuta rimuovendo le prime* s *righe a* PD_{n+1}.
    3. *Sia* B' *la forma di Smith di* B*:* H_n *ha come torsione la somma diretta dei ciclici i cui annullatori sono i fattori invarianti di* B'*. La sua parte libera ha rango uguale al numero di righe nulle in* B'.
  - Se $C_{n+1} = 0$ e $C_{n-1} \neq 0$:
    1. *Sia* D'_n *la forma di Smith di* D_n*:* H_n *è libero e il suo rango è il numero di colonne nulle di* D'_n.
  - Se $C_{n+1} \neq 0$ e $C_{n-1} = 0$:
    1. *Sia* D'_{n+1} *la forma di Smith di* D_{n+1}*:* H_n *ha come torsione la somma diretta dei ciclici i cui annullatori sono i fattori invarianti di* D'_{n+1}*. La sua parte libera ha rango uguale al numero di righe nulle di* D'_{n+1}.
  - Se $C_{n+1} = 0$ e $C_{n-1} = 0$:
    1. $H_n \cong C_n$.

Riferimenti bibliografici

[1] M. ARTIN, Algebra, capitolo 12

[2] N. JACOBSON, Basic Algebra I, capitolo 3

[3] A. HATCHER, Algebraic Topology, capitolo 2

[4] WIKIPEDIA, Smith normal form, http://en.wikipedia.org/wiki/Smith_normal_form