Operazioni con gli ideali

Sia A un anello (commutativo, unitario). Se I e J sono due ideali di A, si definisce $I+J$ come il pipiccolo ideale che contiene sia I, sia J. Si verifica che vale:

$$I+J = \{a+b \mid a \in I,\ b \in J\}$$

Analogamente si può definire la somma (finita) di un insieme di ideali $(I_k)_{k\in K}$.

Se $(I_k)_{k\in K}$ è una qualunque famiglia di ideali, si verifica che $\cap_{k\in K} I_k$ è un ideale.

Se I e J sono due ideali di A, si definisce il loro prodotto $I \cdot J$ come il più piccolo ideale che contiene I e J. Vale: $IJ \subseteq I \cap J$, ma in generale l'inclusione è stretta. Se I_k ($k \in \{1,\dots,n\}$) è una famiglia finita di ideali, il prodotto $I_1 \cdot I_2 \cdots I_k$ è l'ideale generato dai prodotti $x_1 \cdot x_2 \cdots x_k$ con $x_j \in I_j$. In particolare, per ogni n si può definire la potenza n-ima I^n di un ideale. Inoltre si pone $I^0 = (0)$.

Vale: $I \cdot (J_1 + J_2) = IJ_1 + IJ_2$. (Si prova verificando la doppia inclusione).

Def. Due ideali I, J di A si dicono coprimi se $I + J = (1)$.

Siano I_k ($k = \{1,\dots,n\}$) ideali di A e sia

$$\phi : A \longrightarrow A/I_1 \times A/I_2 \times \cdots \times A/I_n$$

data da: $\phi(a) = ([a]_{I_1},\dots,[a]_{I_n})$.

Proposizione 1 *Valgono le seguenti condizioni:*

- *Se I_j e I_k sono coprimi se $j \neq k$, allora:*

$$\prod_k I_k = \bigcap_k I_k$$

- *ϕ è suriettiva se e solo se I_j e I_k sono coprimi se $j \neq k$.*
- *ϕ è iniettiva se e solo se $\bigcap_k I_k = (0)$.*

Proposizione 2 *Valgono le seguenti condizioni:*

1. *Siano $\mathcal{P}_1,\dots,\mathcal{P}_n$ ideali primi di A e sia I un ideale di A tale che $I \subseteq \bigcup \mathcal{P}_i$. Allora esiste un indice k tale che $I \subseteq \mathcal{P}_k$.*
2. *Siano $I_1,\dots,I_n$ ideali di A e sia $\mathcal{P}$ un ideale primo di A tale che $\bigcap I_k \subseteq \mathcal{P}$. Allora esite un j tale che $I_j \subseteq \mathcal{P}$. Se, in particolare, $\mathcal{P} = \bigcap I_k$, allora esiste un j tale che $I_j = \mathcal{P}$.*

Dim.: Per il punto 1). Procediamo per induzione su n mostrando che vale la seguente affermazione:

$$\text{Se } I \not\subseteq \mathcal{P}_i \ \ \forall\, i, \quad \text{allora} \quad I \not\subseteq \bigcup_i \mathcal{P}_i$$

Se $n = 1$ l'affermazione è banale. Vediamo che $n - 1 \Rightarrow n$. Supponiamo quindi che $I \nsubseteq \mathcal{P}_i \quad \forall\ i$. Fissato $k \in \{1, \dots, n\}$, per ipotesi induttiva abbiamo che $I \nsubseteq \bigcup_{i \neq k} \mathcal{P}_i$, quindi per ogni k esiste $x_k \in I_k \setminus \bigcup_{i \neq k} \mathcal{P}_i$. Se per qualche k accade che $x_k \notin \mathcal{P}_k$, allora x_k è un elemento di I che non sta in nessun $\mathcal{P}_i$ e la tesi è provata. Supponiamo allora che $x_k \in \mathcal{P}_k$ per ogni k. Consideriamo l'elemento:

$$y = x_2 x_3 \cdots x_n + x_1 x_3 \cdots x_n + \cdots + x_1 x_2 \cdots x_{n-1}$$

Fissiamo k. Tutti gli addendi di y, tranne il k-imo, sono multipli di x_k, quindi stanno in $\mathcal{P}_k$. Se esistesse un k tale che $y \in \mathcal{P}_k$, allora l'addendo di y dato da $x_1 \cdots x_{k-1} \cdot x_{k+1} \cdots x_n$ si otterrebbe come differenza di elementi di $\mathcal{P}_k$ e quindi starebbe in $\mathcal{P}_k$. Poiché $\mathcal{P}_k$ è primo, uno dei fattori, diciamo x_j con $j \neq k$, starebbe in $\mathcal{P}_k$, contro l'ipotesi da cui si è partiti.
Vediamo il punto 2). Supponiamo che, per ogni k, $I_k \nsubseteq \mathcal{P}$. Quindi costruiamo degli elementi $x_k \in I_k$ con $x_k \notin \mathcal{P}$. Sia $y = \prod_k x_k$. Allora $y \in \prod I_k \subseteq \bigcap I_k \subseteq \mathcal{P}$. Ma, essendo $\mathcal{P}$ primo, qualcuno degli x_k deve stare in $\mathcal{P}$. Pertanto deve esistere j tale che $I_j \subseteq \mathcal{P}$. Se, in particolare, $\mathcal{P} = \bigcap I_k$ allora $\mathcal{P}$ è anche contenuto in ciascun ideale I_k, quindi $\mathcal{P} = I_k$.

Siano I, J ideali di A. Si definisce $I : J$ l'ideale:

$$\{a \in A \mid aJ \subseteq I\}$$

(si verifica che effettivamente è un ideale). Ad esempio $(0) : I = \mathrm{Ann}(I)$.
Se $x \in A$, si definisce $\mathrm{Ann}(x) = (0) : (x) = \{a \in A \mid ax = 0\}$. Sia poi:

$$D = \{a \in A \mid a \text{ è un divisore dello zero}\}$$

Si vede subito che vale:

$$D = \bigcup_{x \neq 0} \mathrm{Ann}(x)$$

Ad esempio in $K[x, y]$ (con K campo), vale $(x^2 y, xy^2) : (x) = (xy, y^2)$.
Def. Sia $I \subseteq A$ un ideale. Si chiama *radicale di I* l'insieme:

$$\sqrt{I} = \{a \in A \mid \text{esiste } n \in \mathbb{N} \text{ tale che } a^n \in I\}$$

Un ideale I di A si chiama radicale se vale $I = \sqrt{I}$.
Se I è un ideale, $\sqrt{I}$ è un ideale. Sia $\pi : A \longrightarrow A/I$ l'epimorfismo canonico. Vale:

$$\sqrt{I} = \pi^{-1}\left(\mathcal{N}_{A/I}\right)$$

(dove $\mathcal{N}_{A/I}$ è il nilradicale di A/I). Ricordando che $\mathcal{N}_{A/I} = \bigcap_{\mathcal{P}} \mathcal{P}$, ($\mathcal{P}$ primo) e ricordando che l'epimorfismo canonico π fa corrispondere ideali primi di A/I con ideali primi di A che contengono I, si ha:

$$\sqrt{I} = \bigcap_{\mathcal{P} \supseteq I} \mathcal{P} \quad (\mathcal{P} \text{ primo})$$

Alcune proprietà (di facile verifica) del radicale:
$I \subseteq \sqrt{I}$, $\sqrt{\sqrt{I}} = \sqrt{I}$, $\sqrt{I \cdot J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Più in generale, si può definire, dato un qualunqe insieme $E \subseteq A$ l'insieme $\sqrt{E} = \{a \in A \mid \text{esiste } n \in \mathbb{N} \text{ tale che } a^n \in E\}$. In questo caso $\sqrt{E}$ non è necessariamente un ideale. Vale: se E_l $(l \in L)$ è una famiglia qualunque di sottoinsiemi, allora

$$\sqrt{\bigcup_{l \in L} E_l} = \bigcup_{l \in L} \sqrt{E_l}$$

Proposizione 3 *Vale:*

$$D = \bigcup_{x \neq 0} \sqrt{\mathrm{Ann}(x)}$$

Dim.: Si ha: $D = \sqrt{D} = \sqrt{\bigcup_{x \neq 0} \mathrm{Ann}(x)} = \bigcup_{x \neq 0} \sqrt{\mathrm{Ann}(x)}$.

Proposizione 4 *Due ideali I e J di A sono coprimi, se e solo se $\sqrt{I}$ e $\sqrt{J}$ sono coprimi.*

Dim.: Se I e J sono coprimi, $\sqrt{I}$ e $\sqrt{J}$ sono anche coprimi, banalmente. Siano $\sqrt{I}$ e $\sqrt{J}$ coprimi. Allora esistono $m, n \in \mathbb{N}$ e $a, b \in A$, tali che $a^m \in I$, $b^n \in J$ e $a^m + b^n = 1$. Sia $r \in \mathbb{N}$. Sviluppando $(a^m + b^n)^r = 1$ con il binomio di Newton si vede che, se r è sufficientemente grande, ogni addendo di $(a^m + b^n)^r$ sta in I o in J e quindi $I + J = (1)$.

Estensione e contrazione

Sia $f : A \longrightarrow B$ un omomorfismo tra due anelli A e B. Sia $I \subseteq A$ un ideale di A. In generale, $f(I)$ non è un ideale di B. Si definisce $I^e = (f(I))$ (l'ideale generato da $f(I)$). I^e si dice l'ideale I *esteso*. Se $J \subseteq B$ è un ideale, allora $f^{-1}(J)$ è un ideale di A, si indica con J^c e si dice l'ideale J *contratto*. Se J è primo, J^c è primo (non vale analoga proprietà per le estensioni).

Proposizione 5 *Valgono le seguenti proprietà:*

- $I \subseteq I^{ec}$, $J \supseteq J^{ec}$;
- $J^c = J^{cec}$, $I^e = I^{ece}$

Le dimostrazioni sono facili verifiche.

Lemma di Nakayama

Ricordare che, se U è una matrice quadrata di ordine n (con entrate in un campo) si può definire la matrice aggiunta U' di U. La matrice aggiunta risulta essere definita come la trasposta della matrice dei cofattori e ha la proprietà che $U \cdot U' = U' \cdot U = \det(U) I_n$. Si noti inoltre che $\det(U)$ è definito sommando opportuni prodotti di entrate di U, quindi per definire il determinante di una matrice non serve che i coefficienti stiano in un campo, ma è sufficiente che stiano in un anello. Analogamente ciascuna delle entrate della matrice aggiunta U' è definita sommando opportuni prodotti di alcune entrate di U, quindi anche

U' può essere definita in un qualunque anello. Se quindi U è una matrice con entrate in un anello B qualunque, si può costruire una matrice U' con entrate in B tale che valga: $U \cdot U' = U' \cdot U = \det(U) I_n$.

Proposizione 6 *Sia A un anello commutativo unitario e sia M un A-modulo finitamente generato. Sia $I \subseteq A$ un ideale e sia $\phi : M \longrightarrow M$ un endomorfismo di M tale che $\phi(M) \subseteq IM$ (dove IM indica il sottomodulo di M generato da elementi della forma am con $a \in I$, $m \in M$). Allora esiste un polinomio $f(x) \in A[x]$ monico, con gli altri coefficienti in I, tale che $\phi(f) = 0$.*

Dim.: Sia $x_1, \ldots, x_n$ un sistema di generatori di M come A-modulo. Poiché $\phi(x_i) \in IM$, esistono $a_{ji} \in I$ tali che

$$\phi(x_i) = \sum_{j=1}^{n} a_{ji} x_j.$$

Pertanto vale: $\phi(x_i) - a_{1i}x_1 - \cdots - a_{ni}x_n = 0$ e, introducendo l'omomorfismo identità $\mathbf{1}_M$ e la delta di Kronecker δ_{ji}, si può scrivere:

$$\sum_{j=1}^{n} (\delta_{ji}\phi - a_{ji}\mathbf{1}_M)(x_j) = 0.$$

$\delta_{ji}\phi - \mathbf{1}_M$ è un endomorfismo di M e quindi può essere pensato come un elemento dell'anello (non commutativo) $B = \mathrm{End}(M)$ degli endomorfismo di M. Si consideri allora la matrice: $U = (\delta_{ji}\phi - \mathbf{1}_M)_{ji}$. La relazione scritta sopra dice che $U \cdot {}^t(x_1, \ldots, x_n) = 0$. Sia U' è la matrice aggiunta di U, pertanto si ha che $U'U \cdot {}^t(x_1, \ldots, x_n) = 0$, quindi $\det(U)(x_i) = 0$ per ogni $i = 1, \ldots, n$, pertanto $\det(U)(x_i)$ è l'endomorfismo nullo. Sviluppando il determinante si ottiene un polinomio a coefficienti in A di grado n monico che si annulla su ϕ.

Corollario 7 *Sia M un A-modulo finitamente generato e sia $I \subseteq A$ un ideale tale che $IM = M$. Allora esiste $t \in A$, $t \equiv 1$ modulo I, tale che $tM = 0$.*

Dim.: Prendiamo, nella proposizione di sopra, $\phi = \mathbf{1}_M$ (cioè l'identità). Sia $f(x) \in A[x]$ il polinomio che si annulla sull'endomorfismo ϕ della proposizione precedente. Se $f(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0$, allora $\mathbf{1}_M^n + \alpha_{n-1}\mathbf{1}_M^{n-1} + \cdots + \alpha_0 \mathbf{1}_M = 0$ cioè $m + \alpha_{n-1}m + \ldots + \alpha_0 m = 0$ per ogni $m \in M$, quindi $(1 + \alpha_{n-1} + \ldots + \alpha_0)m = 0$ per ogni $m \in M$, pertanto, se si prende $t = 1 + \alpha_{n-1} + \ldots + \alpha_0$, si ottiene che $t \equiv 1$ modulo I e $tM = 0$.

Teorema 8 *(Lemma di Nakayama) Sia M un A-modulo finitamente generato e sia $I \subseteq A$ un ideale tale che $I \subseteq \mathcal{J}(I)$ (dove $\mathcal{J}(I)$ è il radicale di Jacobson di A). Se $IM = M$, allora $M = 0$.*

Dim.: Per il risultato precedente, esiste $t \in A$ tale che $tM = 0$ e $1-t \in I$. Quindi $1 - t \in J(A)$, ma allora, per una proprietà vista del radicale di Jacobson, t è invertibile, quindi $M = 0$.

Si può vedere anche un'altra dimostrazione del lemma di Nakayama:
Sia $x_1, \dots, x_n$ un sistema di generatori di M e sia minimale, nel senso che tutti gli x_i sono necessari per ottenere gli elementi di M. Poiché $IM = M$, abbiamo in particolare che $x_1 \in IM$, quindi x_1 è combinazione lineare di $x_1, \dots, x_n$ con coefficienti in I, quindi $x_1 = a_1 x_1 + \cdots + a_n x_n$ (con $a_i \in I$). Pertanto vale: $(1 - a_1)x_1 = a_2 x_2 + \cdots + a_n x_n$. Ma $a_1 \in \mathcal{J}(A)$ e quindi $1 - (1 - a_1)$ è invertibile. Ma allora x_1 è un generatore superfluo.

Corollario 9 *Sia M un A-modulo finitamente generato, $N \subseteq M$ un sottomodulo e sia $M = IM + N$, con $I \subseteq J(A)$. Allora $M = N$.*

Dim.: Vale $M/N = (IM + N)/N = IM/N$ e ci si riconduce al lemma di Nakayama.

Sia $(A, \mathcal{M}, k)$ un anello locale. Sia M un A-modulo finitamente generato. Allora $M/\mathcal{M}M$ è un k spazio vettoriale di dimensione finita. Vale:

Proposizione 10 *Siano $x_1, \dots, x_n$ elementi di M tali che $[x_1], \dots, [x_n]$ formano una base di $M/\mathcal{M}M$. Allora gli $x_1, \dots, x_n$ generano M.*

Dim.: Sia $N = \langle x_1, \dots, x_n \rangle$. Poiché $[x_1], \dots, [x_n]$ generano $M/\mathcal{M}M$, allora $M = \mathcal{M}M + N$ e quindi $M = N$.