

Lezione 1

Operazioni tra ideali. Radicale di un ideale.

Ricordiamo la seguente definizione:

Definizione 1.1 Si dice *anello* un insieme non vuoto A dotato di due operazioni, una somma $+$ ed un prodotto \cdot , tali che:

- $(A, +)$ sia un gruppo abeliano (detto *gruppo additivo* di A)
- il prodotto \cdot goda della proprietà associativa;
- valga la proprietà distributiva del prodotto \cdot rispetto alla somma $+$, ossia:

$$\forall a, b, c \in A, \quad a \cdot (b + c) = ab + ac \quad \text{e} \quad (b + c) \cdot a = ba + ca.$$

L'anello si dice *commutativo* se il prodotto \cdot gode della proprietà commutativa; si dice *unitario* se esiste l'elemento neutro del prodotto \cdot , che, solitamente, viene denotato con 1 , (o, per maggiore precisione, 1_A) e chiamato *unità*.

Si dice *sottoanello* dell'anello A ogni sottoinsieme B che è sottogruppo del gruppo additivo di A ed è chiuso rispetto al prodotto di A : in tal caso B è un anello.

Esempi 1.2 Sono anelli:

- l'insieme \mathbb{Z} dei numeri interi (anello commutativo unitario)
- l'insieme $n\mathbb{Z}$ dei multipli del numero naturale $n > 1$ (anello commutativo, non unitario)
- l'insieme $K[x]$ dei polinomi nell'indeterminata x a coefficienti nel campo K (anello commutativo unitario)
- l'insieme $M_n(K)$ delle matrici quadrate di ordine n a coefficienti in un campo K (anello unitario, non commutativo se $n > 1$.)

Tutti gli anelli del corso saranno **anelli commutativi unitari**.

Diamo ora una nozione che, come vedremo, svolge, nella teoria degli anelli, un ruolo analogo a quello del sottogruppo normale nella teoria dei gruppi.

Definizione 1.3 Dato un anello A , si dice *ideale* di A ogni sottoinsieme $I \subset A$ tale che:

- I è un sottogruppo del gruppo additivo di A
- $\forall a \in A, \forall x \in I, \quad ax \in I$.

Osservazioni 1.4

- Ogni anello è ideale di se stesso. Un ideale coincide con tutto l'anello se e solo se vi appartiene 1 . In ogni anello il sottoinsieme $\{0\}$ è un ideale.

- Ogni ideale è anche un sottoanello, ma non è vero il viceversa: \mathbf{Z} è un sottoanello di \mathbf{Q} , ma non è un ideale. Infatti, $\frac{1}{2} \cdot 1 \notin \mathbf{Z}$.

Esempio 1.5 a) Per ogni $n \in \mathbf{N}$, l'insieme $n\mathbf{Z}$ è un ideale di \mathbf{Z} . Poiché i sottogruppi di \mathbf{Z} sono tutti e soli i sottogruppi ciclici $n\mathbf{Z}$, segue che questi sono anche tutti i sottoanelli di \mathbf{Z} e, quindi, tutti e soli gli ideali di \mathbf{Z} .

b) L'insieme

$$(a) = \{ax \mid x \in A\}$$

è un ideale di A . Lo si chiama *ideale principale generato da a* (in A), ed è il più piccolo ideale di A contenente a .

La prossima proposizione illustra la profonda analogia tra sottogruppi normali ed ideali.

Proposizione 1.6 Sia I un ideale dell'anello A . Allora sul gruppo (additivo) quoziente A/I è definito, oltre alla somma

$$(a + I) + (b + I) = (a + b) + I$$

un prodotto

$$(a + I)(b + I) = ab + I,$$

e rispetto a tali operazioni A/I è un anello commutativo unitario, detto *anello quoziente (dell'anello A rispetto all'ideale I)*. L'unità moltiplicativa è $1 + I$.

Esempio 1.7 Per ogni intero $n \geq 2$, l'anello \mathbf{Z}_n degli interi modulo n coincide con l'anello quoziente $\mathbf{Z}/n\mathbf{Z}$.

È possibile definire operazioni tra ideali. La dimostrazione del seguente enunciato è un facile esercizio.

Proposizione 1.8 Siano I, J ideali di un anello A . Allora

- $I \cap J$ è un ideale di A ;
- $I + J = \{x + y \mid x \in I, y \in J\}$ è un ideale di A contenente I e J ;
- $IJ = \left\{ \sum_{i=1}^n x_i y_i \mid x_i \in I, y_i \in J, n \in \mathbf{N} \right\}$ è un ideale di A contenuto in I e in J .

Esercizio 1.9* Siano I, J, K ideali dell'anello A .

- Provare che $I(J + K) = IJ + IK$.
- Dire se, in generale, $I \cap (J + K) = I \cap J + I \cap K$. In caso negativo, aggiungere opportune ipotesi.
- Provare che se $I = (a)$ e $J = (b)$, allora $IJ = (ab)$.

Osservazione 1.10 Le operazioni definite nella Proposizione 1.8, naturalmente, si possono estendere ad un qualunque insieme finito non vuoto di ideali, e godono della proprietà associativa. In particolare:

- Dati $a_1, \dots, a_r \in A$, si dice *ideale generato da a_1, \dots, a_r* l'ideale somma

$$(a_1) + \cdots + (a_r),$$

che, per semplicità, viene anche indicato con (a_1, \dots, a_r) . Non è difficile dimostrare che è il più piccolo ideale di A contenente a_1, \dots, a_r , e si ha

$$(a_1, \dots, a_r) = \left\{ \sum_{i=1}^r a_i x_i \mid x_i \in A \text{ per ogni } i = 1, \dots, r \right\}.$$

L'insieme dei generatori, naturalmente, non è univocamente determinato. Ad esempio, è possibile sostituire ogni elemento con la somma dello stesso elemento e di una combinazione lineare degli altri generatori a coefficienti in A . Ad esempio, nell'anello $A = K[x, y]$ (dove K è un campo), si ha

$$(x, y) = (x + y, y) = (x + xy + y^2, y)$$

che è l'ideale di A formato dai polinomi del tipo $f(x, y) = xg(x, y) + yh(x, y)$, ossia, dai polinomi che hanno il termine noto nullo.

b) Ogni ideale I dell'anello A può essere sommato a se stesso, oppure moltiplicato con se stesso, un numero n di volte, per ogni intero positivo n . Mentre, però,

$$\underbrace{I + \cdots + I}_{n \text{ volte}} = I$$

e quindi il "multiplo" di un ideale è un concetto poco significativo, diversa è la situazione della *potenza*. Si ha, infatti,

$$\underbrace{I \cdots I}_{n \text{ volte}} = I^n \subset I,$$

e, in generale, l'inclusione è stretta. Più precisamente, si ha la seguente catena discendente di ideali:

$$I \supset I^2 \supset I^3 \supset I^4 \supset \cdots$$

Un esempio di catena strettamente discendente è la seguente catena di ideali di \mathbf{Z} :

$$(2) \supset (4) \supset (8) \supset (16) \supset \cdots$$

Esempio 1.11 Sia A un PID, e siano $a_1, \dots, a_r \in A$ non nulli. Allora, come noto,

$$\sum_{i=1}^r (a_i) = (\text{MCD}(a_1, \dots, a_r))$$

$$\prod_{i=1}^r (a_i) = \left(\prod_{i=1}^r a_i \right)$$

$$\bigcap_{i=1}^r (a_i) = (\text{mcm}(a_1, \dots, a_r))$$

In particolare, si ha $\prod_{i=1}^r (a_i) = \bigcap_{i=1}^r (a_i)$ se e solo se gli elementi a_1, \dots, a_r sono a due a due coprimi. Ciò si verifica se $(a_i) + (a_j) = A$ per ogni coppia di indici distinti i, j . La prossima proposizione ci mostra che ciò non è vero solo in un PID, bensì in un qualunque anello.

Proposizione 1.12 Siano I_1, \dots, I_r ideali dell'anello A . Allora $I_1 \cdots I_r \subset I_1 \cap \cdots \cap I_r$, e vale $I_1 \cdots I_r = I_1 \cap \cdots \cap I_r$ se $I_i + I_j = A$, per ogni coppia di indici distinti i e j (in tal caso gli ideali si dicono *a due a due coprimi*).

Dimostrazione: L'inclusione segue dalla Proposizione 1.8 c) per induzione. Per provare la seconda parte dell'enunciato, procediamo per induzione su $r \geq 2$. Per la base dell'induzione, supponiamo che $I_1 + I_2 = A$. Allora esistono $a_1 \in I_1, a_2 \in I_2$ tali che si abbia $a_1 + a_2 = 1$. Sia $a \in I_1 \cap I_2$. Allora $a = a(a_1 + a_2) = aa_1 + aa_2 \in I_2 I_1 + I_1 I_2 = I_1 I_2$, per cui $I_1 \cap I_2 \subset I_1 I_2$, come volevasi. Sia ora $r > 2$ e supponiamo la tesi vera per $r-1$. Allora per ogni coppia di indici $i, j \in \{1, \dots, r-2\}$ si ha che $I_i + I_j = A$, e, inoltre, in virtù dell'Esercizio 1.9 a) e della Proposizione 1.8 c),

$$A = (I_i + I_{r-1})(I_i + I_r) = I_i^2 + I_{r-1}I_i + I_i I_r + I_{r-1}I_r \subset I_i + I_{r-1}I_r, \quad \text{per cui} \quad A = I_i + I_{r-1}I_r.$$

Dunque l'ipotesi induttiva si applica agli ideali $I_1, \dots, I_{r-2}, I_{r-1}I_r$, e pertanto, tenendo anche conto della base dell'induzione, applicata a I_{r-1}, I_r ,

$$I_1 \cap \cdots \cap I_{r-2} \cap I_{r-1} \cap I_r = I_1 \cap \cdots \cap I_{r-2} \cap I_{r-1}I_r = I_1 \cdots I_{r-2} I_{r-1} I_r.$$

Osservazione 1.13 L'implicazione contenuta nella Proposizione 1.12 non può essere rovesciata, ossia si può avere l'uguaglianza tra il prodotto e l'intersezione di ideali senza che gli ideali siano a due a due coprimi. Ad esempio, nell'anello dei polinomi $A = K[x, y]$, ove K è un campo, si ha che $(x)(y) = (x) \cap (y)$, mentre $(x) + (y) \neq A$. In generale, se A è un UFD, e $a_1, \dots, a_r \in A$ sono elementi a due a due coprimi, allora si ha sempre che $\prod_{i=1}^r (a_i) = \bigcap_{i=1}^r (a_i)$ (infatti, un elemento di A è multiplo di tutti gli a_i se e solo se è multiplo del prodotto di questi ultimi).

Prima di enunciare il prossimo risultato, ricordiamo che agli anelli (come ai gruppi) si applicano nozioni come gli omomorfismi, costruzioni come il prodotto diretto e la somma diretta, e proprietà

come i teoremi di isomorfismo e di corrispondenza. Nel seguito le utilizzeremo senza richiamarle preliminarmente.

Proposizione 1.14 Siano I_1, \dots, I_r ideali dell'anello A . Allora l'applicazione

$$\begin{aligned} \varphi : A &\rightarrow A/I_1 \times \dots \times A/I_r = \prod_{i=1}^r A/I_i \\ a &\mapsto (a + I_1, \dots, a + I_r) = (a + I_i)_{i=1, \dots, r} \end{aligned}$$

è un omomorfismo di anelli tale che $\text{Ker } \varphi = \bigcap_{i=1}^r I_i$. Inoltre φ è suriettivo se e solo se I_1, \dots, I_r sono a due a due coprimi.

Dimostrazione: La prima affermazione è ovvia. Proviamo la seconda. Se φ è suriettivo, allora, in particolare, esiste $a \in A$ tale che $\varphi(a) = (a + I_1, a + I_2, \dots, a + I_r) = (1 + I_1, I_2, \dots, I_r)$. Quindi

$$1 - a \in I_1 \quad \text{e} \quad a \in I_i \quad \text{per ogni } i = 2, \dots, r.$$

Segue che, per ogni $i = 2, \dots, r$, si ha $1 = (1 - a) + a \in I_1 + I_i$, e quindi $A = I_1 + I_i$, ossia I_1 e I_i sono coprimi. Analogamente si prova che, per ogni coppia di indici distinti i e j , gli ideali I_i e I_j sono coprimi. Viceversa, supponiamo che sia vera quest'ultima affermazione. Allora, per ogni $i = 2, \dots, r$, $I_1 + I_i = A$. Quindi per ogni $i = 2, \dots, r$ esistono $a_i \in I_1$ e $b_i \in I_i$ tali che $a_i + b_i = 1$. Sia $b = \prod_{i=2}^r b_i$.

Allora

$$b + I_1 = \prod_{i=2}^r [(1 - a_i) + I_1] = 1 + I_1 \quad \text{e} \quad b + I_i = b_i \prod_{j \neq i} b_j + I_i = I_i \quad \text{per ogni } i = 2, \dots, r.$$

Quindi

$$\varphi(b) = (1 + I_1, I_2, \dots, I_r).$$

Analogamente si prova che $(I_1, \dots, 1 + I_i, \dots, I_r) \in \text{Im } \varphi$ per ogni $i = 2, \dots, r$. Ciò basta per concludere che φ è surgettivo.

Dalle Proposizioni 1.12 e 1.14 segue, in virtù del teorema fondamentale di omomorfismo per anelli:

Corollario 1.15 Siano I_1, \dots, I_r ideali dell'anello A , a due a due coprimi. Allora

$$A / \prod_{i=1}^r I_i = A / \bigcap_{i=1}^r I_i \cong \prod_{i=1}^r A / I_i.$$

Osservazione 1.16 Il Teorema Cinese del Resto, noto dal corso di Algebra 1, è una conseguenza del Corollario 1.15.

Il prossimo esercizio utilizza la nozione di A -modulo, che verrà introdotta nella Lezione 3.

Esercizio 1.17 Siano I, J ideali dell'anello A . Allora si ha una *sequenza esatta corta* di omomorfismi di A -moduli:

$$0 \rightarrow A/I \cap J \xrightarrow{f} A/I \times A/J \xrightarrow{g} A/I + J \rightarrow 0,$$

ossia esistono omomorfismi di A -moduli $A/I \cap J \xrightarrow{f} A/I \times A/J$, iniettivo e $A/I \times A/J \xrightarrow{g} A/I + J$, suriettivo, tali che $\text{Im } f = \text{Ker } g$.

Svolgimento: Con la notazione della Proposizione 1.14, l'omomorfismo $A \xrightarrow{\varphi} A/I \times A/J$ induce, in virtù del teorema fondamentale di omomorfismo per anelli, un omomorfismo iniettivo

$$\begin{aligned} A/I \cap J &\xrightarrow{f=\varphi^*} A/I \times A/J \\ a + I \cap J &\mapsto (a + I, a + J) \end{aligned}$$

Definiamo l'applicazione

$$\begin{aligned} A/I \times A/J &\xrightarrow{g} A/I + J \\ (a + I, b + J) &\mapsto (a - b) + I + J \end{aligned}$$

Questo è un omomorfismo di A -moduli ben definito, ed è evidentemente suriettivo. Inoltre si ha che, per ogni $a \in A$, $g((a + I, a + J)) = I + J$, per cui $\text{Im } f \subset \text{Ker } g$. Per provare l'altra inclusione, supponiamo che $g((a + I, b + J)) = I + J$, cioè che $a - b \in I + J$. Esistono allora $x \in I$ e $y \in J$ tali che $a - b = x + y$. Pertanto, $a + I = a - x + I$, e $b + J = a - x - y + J = a - x + J$. Quindi $(a + I, b + J) = (a - x + I, a - x + J) = f(a - x + I \cap J)$. Ciò prova che $\text{Ker } g \subset \text{Im } f$.

Osservazione 1.18 Quando I e J sono coprimi, l'Esercizio 1.17 fornisce una sequenza esatta corta

$$0 \rightarrow A/I \cap J \xrightarrow{f} A/I \times A/J \longrightarrow 0,$$

e quindi un isomorfismo $A/I \times A/J \cong A/I \cap J$, in accordo con il Corollario 1.15. Osserviamo, inoltre, che lo stesso esercizio non si estende banalmente al caso in cui gli ideali sono più di due. Consideriamo, ad esempio, gli ideali $I_1 = 6\mathbf{Z}$, $I_2 = 10\mathbf{Z}$, $I_3 = 15\mathbf{Z}$ dell'anello $A = \mathbf{Z}$. Allora

$$\begin{aligned} A/I_1 \cap I_2 \cap I_3 &= \mathbf{Z}/30\mathbf{Z}, & A/I_1 \times A/I_2 \times A/I_3 &= \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/10\mathbf{Z} \times \mathbf{Z}/15\mathbf{Z}, \\ A/I_1 + I_2 + I_3 &= \mathbf{Z}/6\mathbf{Z} + 10\mathbf{Z} + 15\mathbf{Z} = \mathbf{Z}/\mathbf{Z} = \{0\}. \end{aligned}$$

Ma non esiste una sequenza esatta $0 \rightarrow \mathbf{Z}/30\mathbf{Z} \xrightarrow{f} \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/10\mathbf{Z} \times \mathbf{Z}/15\mathbf{Z} \rightarrow 0$, perché i due anelli, avendo ordini finiti distinti (30 e 900 rispettivamente), non possono essere isomorfi.

Abbiamo definito sopra il prodotto e la potenza di ideali. È possibile, entro certi limiti, definire le corrispondenti "operazioni inverse", ossia il *quoziente* ed il *radicale*.

Definizione 1.19 Siano I, J ideali di un anello A . Si dice *quoziente di I rispetto a J* l'insieme

$$I : J = \{a \in A \mid ax \in I \text{ per ogni } x \in J\}$$

Se I è l'ideale nullo, l'insieme è

$$0 : J = \{a \in A \mid ax = 0 \text{ per ogni } x \in J\}$$

e lo si dice *annullatore di J* , denotato anche con $\text{Ann}(J)$. Se, inoltre $J = (x)$, l'insieme è

$$0 : x = \{a \in A \mid ax = 0\},$$

e si chiama *annullatore di x* , indicato dal simbolo $\text{Ann}(x)$.

È immediato verificare la seguente

Proposizione 1.20 Dati gli ideali I, J dell'anello A , $I : J$ è un ideale di A contenente I .

Per altre proprietà del quoziente di ideali si rimanda a [AM], Esercizio 1.12.

Esempi 1.21

a) Sia A un UFD, e siano $a, b \in A$ non nulli. Allora si ha:

$$(a) : (b) = \left(\frac{a}{\text{MCD}(a, b)} \right).$$

b) L'unione $D = \bigcup_{\substack{x \in A \\ x \neq 0}} \text{Ann}(x)$ è l'insieme dei divisori dello zero dell'anello A (ossia degli elementi non nulli di A che violano la legge di annullamento del prodotto).

Definizione 1.22 Sia I un ideale dell'anello A . Si dice *radicale di I* l'insieme

$$\sqrt{I} = \{a \in A \mid a^n \in I \text{ per qualche } n \in \mathbf{N}^*\}.$$

Se I è l'ideale nullo, l'insieme è

$$\sqrt{0} = \{a \in A \mid a^n = 0 \text{ per qualche } n \in \mathbf{N}^*\}$$

e viene detto *nilradicale di A* : è l'insieme degli elementi nilpotenti di A . Se $I = \sqrt{I}$, l'ideale I si dice *ideale radicale* o anche *ideale ridotto*.

Proposizione 1.23 Sia I un ideale dell'anello A . Allora \sqrt{I} è un ideale di A contenente I .

Dimostrazione: La relazione di inclusione $I \subset \sqrt{I}$ è ovvia. Quindi \sqrt{I} è non vuoto. Siano $a, b \in \sqrt{I}$, con $a^n \in I, b^m \in I$ per opportuni $n, m \in \mathbf{N}^*$. Allora, naturalmente, $a^r, b^s \in I$ per ogni $r \geq n, s \geq m$. Proviamo che $a - b \in \sqrt{I}$. Sia $N = n + m$. Si ha:

$$(a - b)^N = \sum_{i=0}^N (-1)^{N-i} \binom{N}{i} a^i b^{N-i},$$

dove, per ogni $i = 0, \dots, N$,

$$\begin{cases} \text{se } i < n, \text{ allora } N - i > m, \text{ e quindi } b^{N-i} \in I \\ \text{se } i \geq n, \text{ allora } a^i \in I \end{cases}$$

Quindi, in ogni caso, $a^i b^{N-i} \in I$. Segue che $(a - b)^N \in I$, per cui, come volevasi, $a - b \in \sqrt{I}$. Ciò prova che \sqrt{I} è un sottogruppo additivo di A . Inoltre, per ogni $a \in A, x \in \sqrt{I}$, se $x^n \in I$, allora

$$(ax)^n = a^n x^n \in I,$$

e pertanto $ax \in \sqrt{I}$.

Esempio 1.24 Sia A un UFD, e sia $a \in A$ un elemento non nullo e non invertibile di fattorizzazione

$$a = \prod_{i=1}^s p_i^{\alpha_i},$$

ove i p_i sono primi a due a due non associati (diremo: distinti) e gli esponenti α_i sono tutti interi positivi. Allora

$$\sqrt{(a)} = \left(\prod_{i=1}^s p_i \right).$$

Indicheremo, nel seguito, con a^{rid} il prodotto dei divisori primi (distinti) di a . Rispetto a questa notazione, si ha dunque

$$\sqrt{(a)} = (a^{\text{rid}}).$$

Abbiamo così stabilito il

Corollario 1.25 Se A è un UFD, e $a \in A$ è il prodotto di primi a due a due distinti, allora (a) è un ideale radicale. Ciò vale, in particolare, se a è irriducibile.

Esempio 1.26 Nell'anello di polinomi $K[x, y, z]$, il radicale dell'ideale $I = (x^2 y^3 z^5)$ è $\sqrt{I} = (xyz)$.

Studiamo ora il comportamento del radicale rispetto alle operazioni di intersezione, prodotto e somma di ideali:

Esercizio 1.27 Siano I, J ideali di un anello A . Provare che:

- a) se $I \subset J$, allora $\sqrt{I} \subset \sqrt{J}$;
- b) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$;
- c) $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

Svolgimento:

- a) Questa affermazione è immediata conseguenza della Definizione 1.22.
- b) Le inclusioni $\sqrt{IJ} \subset \sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$ sono di immediata verifica: la prima segue da a) alla luce della Proposizione 1.8 c), la seconda è diretta conseguenza della Definizione 1.22. Resta da provare che $\sqrt{I} \cap \sqrt{J} \subset \sqrt{IJ}$. Sia $a \in \sqrt{I} \cap \sqrt{J}$, con $a^n \in I, a^m \in J$. Allora $a^{n+m} \in IJ$, e quindi $a \in \sqrt{IJ}$.
- c) L'inclusione $\sqrt{I+J} \subset \sqrt{\sqrt{I} + \sqrt{J}}$ si deduce facilmente da a). Proviamo l'altra. Sia $a \in \sqrt{\sqrt{I} + \sqrt{J}}$, con $a^n \in \sqrt{I} + \sqrt{J}$, diciamo $a^n = x + y$, ove $x \in \sqrt{I}, y \in \sqrt{J}$. Sia $x^r \in I, y^s \in J$. Allora è facile vedere, come nella dimostrazione della Proposizione 1.23, che

$$(a^n)^{r+s} \in I + J.$$

Segue che $a \in \sqrt{I+J}$, come volevasi.

Osservazione 1.28 L'uguaglianza b) dell'Esercizio 1.27 si rivelerà fondamentale ai fini delle applicazioni dell'algebra commutativa alla geometria.

Intanto vale la pena di approfondire l'uguaglianza c). Ci potremmo chiedere perché, in generale, non valga

$$\sqrt{I+J} = \sqrt{I} + \sqrt{J}. \quad (1)$$

Escludendo i casi banali, ci limiteremo a considerare gli ideali diversi da (0) e A . Proviamo, anzitutto, che la (1) è sempre vera in un PID. Infatti, se A è un PID, allora, per tutti gli $a, b \in A$ non nulli e non invertibili si ha, in base a quanto stabilito negli Esempi 1.11 e 1.24,

$$\sqrt{(a) + (b)} = \sqrt{(\text{MCD}(a, b))} = (\text{MCD}(a, b))^{\text{rid}} \stackrel{(*)}{=} (\text{MCD}(a^{\text{rid}}, b^{\text{rid}})) = (a^{\text{rid}}) + (b^{\text{rid}}) = \sqrt{(a)} + \sqrt{(b)}$$

Si noti che l'uguaglianza (*) deriva da un semplice fatto aritmetico: le quantità a destra e a sinistra si possono entrambe descrivere come il prodotto dei fattori primi distinti comuni ad a e b .

In particolare abbiamo stabilito che $\sqrt{(a, b)} = (a^{\text{rid}}, b^{\text{rid}})$. Con un facile ragionamento induttivo si dimostra che, se A è un PID, dati $a_1, \dots, a_r \in A$, si ha:

$$\sqrt{(a_1, \dots, a_r)} = (a_1^{\text{rid}}, \dots, a_r^{\text{rid}}) \quad (= (\text{MCD}(a_1^{\text{rid}}, \dots, a_r^{\text{rid}}))).$$

Questa proprietà può sembrare un po' ridondante in un anello in cui tutti gli ideali sono principali. In effetti, la sua importanza si avverte non appena ci viene assegnato, in un PID, un ideale tramite un insieme di più generatori. Dal punto di vista pratico, è più semplice prima ridurre i generatori, e poi calcolare il massimo comune divisore degli elementi ridotti, piuttosto che calcolare prima il massimo comune divisore dei generatori di partenza, e poi ridurlo.

La (1) non è però sempre vera in un anello che non è un PID, ad esempio in $K[x, y]$, dove K è un campo. Infatti, si ha

$$\sqrt{(x^2 + y) + (y)} = \sqrt{(x^2 + y, y)} = \sqrt{(x^2, y)} = (x, y),$$

dove l'ultima uguaglianza si prova facilmente: l'inclusione $\sqrt{(x^2, y)} \supset (x, y)$ è ovvia, perché $x, y \in \sqrt{(x^2, y)}$. Per provare l'altra, supponiamo che $f(x, y) \in \sqrt{(x^2, y)}$, diciamo $f(x, y)^n \in (x^2, y)$, $f(x, y)^n = x^2 g(x, y) + yh(x, y)$. Allora il termine noto di $f(x, y)$ è 0, quindi $f(x, y) \in (x, y)$, per cui $\sqrt{(x^2, y)} \subset (x, y)$.

Invece, in virtù del Corollario 1.25,

$$\sqrt{(x^2 + y) + (y)} = (x^2 + y) + (y) = (x^2, y) \neq (x, y).$$

Esercizio 1.29* Provare che, nell'anello $K[x, y, z]$,

$$\sqrt{(xy, yz + xz)} = (xy, yz, xz)$$

L'Esercizio 1.29 può essere svolto con calcoli diretti, che devono essere sviluppati *ad hoc*, e sono più complessi di quelli visti sopra. Notiamo, in particolare, che l'identità c) dell'Esercizio 1.27 non ci è affatto utile: applicata al primo membro, ci restituisce la stessa espressione di partenza. Più avanti conosceremo metodi molto più rapidi basati sulla controparte geometrica degli anelli di polinomi, ossia le cosiddette *varietà algebriche*, che sono sottoinsiemi dello spazio n -dimensionale K^n costituiti dai punti le cui coordinate sono soluzioni di un sistema di equazioni polinomiali. Il passaggio fondamentale nella nuova tecnica risolutiva per l'Esercizio 1.29 sarà, infatti, considerare i valori in cui si annullano determinati polinomi.

Osservazione 1.30 Occorre non cadere nella facile suggestione del simbolo \sqrt{I} : esso non si comporta, formalmente, come una radice quadrata: l'abbiamo visto, nell'Esercizio 1.27 c), per quanto riguarda la somma. La parte b) dello stesso esercizio potrebbe, invece, far credere che siano rispettate le regole per la radice del prodotto. La smentita viene dalla considerazione della potenza n -esima di un ideale. Infatti si ha, per ogni ideale I di un anello A , ed ogni intero positivo n ,

$$\begin{aligned}\sqrt{I^n} &= \sqrt{I} \\ \sqrt{\sqrt{I}} &= \sqrt{I}\end{aligned}$$

La facile verifica di queste identità è lasciata al lettore.