# Algebra 2

Riccardo Zanotto

13 aprile 2017

## Indice

# 1 Anelli e ideali

## 1.1 Definizioni

**Definizione 1.1** (Anello)**.** Un insieme $A$ è detto *anello* se è dotato di due operazioni $(A, +, \cdot)$ tali che

- $(A, +)$ è un gruppo commutativo, con elemento neutro $0_A$
- $\cdot$ è associativo
- Esiste un elemento $1 \in A$ tale che $1 \cdot a = a \cdot 1 = a \forall a \in A$
- $\forall x, y, z \in A$ vale $x \cdot (x + z) = xy + xz$ e $(y + z) \cdot x = yx + zx$

Inoltre se il prodotto è commutativo, $A$ è detto *anello commutativo*

**Osservazione.** In generale $0 \neq 1$, altrimenti $A = 0$ è l'anello banale, poiché $a = a \cdot 1 = a \cdot 0 = 0$

**Esempio.**

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ con le operazioni usuali sono anelli commutativi
- Le matrici $n \times n$ sono un anello non commutativo

**Definizione 1.2** (Unità)**.** Un elemento $a \in A$ si dice *unità* se $\exists b \in A$ tale che $ab = 1$.
Si indica con $A^*$ l'insieme delle unità, o elementi invertibili.

**Definizione 1.3** (Divisore di 0)**.** Un elemento $a \in A$ si dice *divisore di* 0 se $\exists b \in A$ tale che $ab = 0$.
Si indica con $\mathcal{D}(A)$ l'insieme dei divisori di 0.
Se $D(A) = 0$, allora l'anello è detto *dominio.*

**Definizione 1.4** (Nilpotente)**.** Un elemento $a \in A$ si dice *nilpotente* se $\exists n \in \mathbb{N}$ tale che $a^n = 0$.
Si indica con $N(A)$ l'insieme degli elementi nilpotenti, che è detto nilradicale.
Se $N(A) = 0$, l'anello $A$ è detto *ridotto.*

**Esempio.** Prendiamo $A = \mathbb{Z}/n\mathbb{Z}$ con $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Allora i nilpotenti sono tutti e soli gli elementi del tipo $p_1^{b_1} \cdots p_k^{b_k}$ cpn $b_i > 0$. I divisori di 0 sono gli $m$ tali che $\gcd(m, n) > 1$.

**Proposizione 1.1.** *La somma di un nilpotente ed un invertibile è ancora invertibile.*

*Dimostrazione.*
Detto $a \in A^*$ e $b \in N(A)$, consideriamo $a^{-1}(a + b) = 1 - x$ e osserviamo che $x$ è ancora nilpotente.
Detto $n$ l'indice di nilpotenza di $x$, vale $(1-x)(1+x+\cdots+x^{n-1}) = 1-x^n = 1$ cioè $1 - x$ è invertibile; ma allora anche $a(1 - x) = a + b$ è invertibile. $\square$

Consideriamo ora dei sottoinsiemi particolari di un anello, che saranno fondamentali nello studio delle proprietà degli anelli, in quanto corrispettivi della nozione di sottogruppo.

**Definizione 1.5** (Ideale)**.** Un sottoinsieme $I \subset A$ di un anello è detto *ideale* se è un sottogruppo di $(A, +)$ ed è chiuso rispetto alla moltiplicazione per elementi di $A$, ovvero $x \in A, i \in I \implies xi \in I$.

**Esempio.**

- In $\mathbb{Z}$ un ideale è formato ad esempio da tutti i multipli di 5.
- In $\mathbb{Z}[x]$ tutti i polinomi che non hanno termine noto formano un ideale.

Osserviamo che se $S \subset A$, è facile costruire un ideale $I$ che contenga $S$; in particolare $(S) = \left\{ \sum_{i=1}^{k} a_i s_i \mid a_i \in A, s_i \in S \right\}$ si dice *ideale generato da $S$*.
Se $S$ è finito, allora $(S)$ è *finitamente generato*.

**Definizione 1.6** (Principale)**.** Un ideale $I \subset A$ è detto *principale* se $\exists a \in A$ per cui $I = (a)$.

**Definizione 1.7** (Primo)**.** Un ideale $I \subset A$ è detto *primo* se $ab \in I \implies a \in I \vee b \in I$.
L'insieme di tutti gli ideali primi $Spec(A)$ è detto *spettro* di $A$.

**Definizione 1.8** (Primario)**.** Un ideale $I \subset A$ è detto *primario* se $ab \in I \implies a \in I \vee b^n \in I$ per qualche $n \in \mathbb{N}$.

**Definizione 1.9** (Massimale)**.** Un ideale $I \subset A$ è detto *massimale* se $I \neq A$ e non esiste nessun ideale $J \neq A$ tale che $I \subset J$.

Esempi, esempi, esempi!!!

**Esercizio 1.1.** Se ogni ideale di $A$ è primo, allora $A$ è un campo.

## 1.2 Prime proprietà

Vediamo ora alcune proprietà degli ideali, che saranno gli oggetti più studiati. Iniziamo col vedere che questi oggetti esistono realmente.

**Proposizione 1.2.** *Sia $A$ un anello non banale. Allora esiste sempre un ideale massimale $\mathfrak{m} \subset A$.*

*Dimostrazione.*
Sia $\Sigma = \{I \mid I \subsetneq A\}$ ordinato con l'inclusione. Osserviamo che $(0) \in \Sigma$.
Prendiamo una catena $\{I_j\}_{j \in J}$ e consideriamo $I = \bigcup_{j \in J} I_j$; dimostriamo che $I$ è un ideale.
Infatti se $x, y \in I$ vuol dire che $x \in I_h$ e $y \in I_k$ per qualche indice; supponiamo senza perdita di generalità che $I_h \subset I_k$. Allora $x \in I_k$, perciò $x + y \in I_k \subset I$.
La verifica che $ai \in I \forall a \in A, i \in I$ è banale.
Inoltre $I$ è proprio, poiché $1 \notin I_j \forall j$, per cui $1 \not\ni I$. Perciò $I$ è un maggiorante della catena che avevamo considerato. Concludiamo usando il lemma di Zorn su $\Sigma$, perciò esiste un ideale massimale. $\square$

**Osservazione.** Dato un elemento $a \notin A^*$, si dimostra che esiste un massimale $\mathfrak{m}$ con $a \in \mathfrak{m}$, prendendo $\Sigma = \{I \mid I \subsetneq A, a \in I\}$.

**Proposizione 1.3.** *Dato un anello $A$, il nilradicale si può esprimere come* $N(A) = \bigcap\limits_{P \text{ primi}} P$.

*Dimostrazione.*

$\subset$ Dato $a \in N(A)$, allora $a^n = 0 \in P$ per ogni ideale $P$. Ma se $P$ è primo, $0 = a^n = a \cdot a^{n-1}$, per cui o $a \in P$, o $a^{n-1} \in P$. Procedendo così ottengo in ogni caso che $a \in P$.

$\supset$ Dato un $a \notin N(A)$, voglio trovare un $P$ primo per cui $a \notin P$.
Sia $\Sigma = \left\{I \text{ ideale proprio} | a^n \notin I \forall n \in \mathbb{N}\right\}$ ordinato con l'inclusione.
Data una catena $\{I_j\}_{j \in J}$, considero $I = \bigcup_{j \in J} I_j$ e vale ovviamente $a^n \notin I$.
Inoltre $\Sigma \neq \emptyset$ poiché essendo $a$ non nilpotente, $(0) \in \Sigma$.
Per il lemma di Zorn, esiste allora un elemento $P \in \Sigma$ massimale; osserviamo che $P$ è un ideale, e voglio mostrare che è primo.
Siano $x, y \notin P$. Allora $(P, x) = P + (x) \supsetneq P$, per cui $(P, x) \notin \Sigma$, ovvero $a^n \in P + (x)$; analogamente $a^m \in P + (y)$.
Questo vuol dire che $a^n = kx + p_1, a^m = hy + p_2$, perciò $a^{m+n} = khxy + p_1hy + p_2kx + p_1p_2 \in P + (xy)$, per cui $P + (xy) \notin \Sigma$.
Ma allora $xy \notin P$, altrimenti $P + (xy) = P \in \Sigma$.

□

Costruiamo ora alcune operazioni tra ideali che risulteranno utili in seguito...

- Data una famiglia arbitraria di ideali $\{I_j\}_{j \in J}$, allora $\bigcap I_j$ è un ideale.
- Dati due ideali $I_1, I_2$, si definisce la somma $I_1 + I_2 = (I_1, I_2) = \{i_1 + i_2 \mid i_1 \in I_1, i_2 \in I_2\}$, ovvero l'ideale generato da $I_1 \cup I_2$.
  In generale $\sum I_j = (\bigcup I_j)$.
- Dati due ideali $I_1, I_2$, si definisce il prodotto $I_1 \cdot I_2 =$
  $= \left\{\sum x_j^{(1)} x_j^{(2)} \mid x_j^{(1)} \in I_1, x_j^{(2)} \in I_2\right\}$
- Dati due ideali $I, J$, si definisce $I : J = \{a \in A \mid aJ \subset I\}$
- Dato un ideale $I$, si definisce radicale $\sqrt{I} = \{a \in A \mid \exists n \in \mathbb{N} a^n \in I\}$

Per quest'ultima operazione non è banale il fatto che si ottenga un altro ideale, ma si può dimostrare nella seguente

**Proposizione 1.4.** *Dato un ideale $I$, il suo radicale $\sqrt{I}$ è un ideale.*

*Dimostrazione.*
Vediamo intanto che se $a \in \sqrt{I}$, allora $a^n \in I$ per un qualche $n$, per cui $(ka)^n = k^n a^n \in I \forall k \in A$, cioè $ka \in \sqrt{I}$.
Siano ora $a, b \in I$, cioè $a^n \in I$ e $b^m \in I$ per certi interi. Dimostriamo che

$(a+b)^{n+m} \in I$.

$$\begin{aligned}(a+b)^{m+n} &= \sum_{k=0}^{m+n} \binom{n+m}{k} a^k b^{m+n-k} \\ &= \sum_{k=0}^{n} \binom{n+m}{k} a^k b^{m+n-k} + \sum_{k=n+1}^{m+n} \binom{n+m}{k} a^k b^{m+n-k}\end{aligned}$$

Osserviamo che nella prima sommatoria $m+n-k \geq m$, per cui possiamo raccogliere $b^m$; analogamente nella seconda $k \geq n$, per cui raccogliamo $a^n$. Ma allora abbiamo una combinazione lineare di $a^n$ e $b^m$ che stanno entrambi in $I$, per cui tutta la somma sta in $I$. □

Definiamo ora un ideale particolare:

**Definizione 1.10** (Radicale di Jacobson)**.** $J(A) = \bigcap_{\mathfrak{m} \subset A} \mathfrak{m}$

**Proposizione 1.5.** $x \in J(A) \iff \forall y \in A \;\; 1 - xy \in A^*$

*Dimostrazione.*

- $\Longleftarrow$ Se $x \notin J(A)$, allora $\exists \mathfrak{m}$ massimale tale che $x \notin \mathfrak{m}$, perciò l'ideale $(\mathfrak{m}, x) \supset \mathfrak{m}$ conincide con tutto l'anello $A$.
  Allora $A \ni 1 = m + xy$ con $m \in \mathfrak{m}$ e $y \in A$, ovvero $1 - xy \in \mathfrak{m}$ da cui $1 - xy \in A^*$, perché altrimenti $\mathfrak{m} = A$.

- $\Longrightarrow$ Se $\alpha = 1 - xy \notin A^*$, allora esiste un $\mathfrak{m}$ ideale massimale tale che $\alpha \in \mathfrak{m}$. Ma allora $x \notin \mathfrak{m}, y \notin \mathfrak{m}$, altrimenti si avrebbe $1 \in \mathfrak{m}$ e perciò $\mathfrak{m} = A$. Dunque $x \notin J(A) \subset \mathfrak{m}$.

□

**Definizione 1.11** (Anello locale)**.** Dato un anello $A$, se esiste un unico ideale $\mathfrak{m}$ massimale, allora $A$ è detto *locale* e di solito si indica con $(A, \mathfrak{m})$

**Esempio.** L'anello $\mathbb{Z}/p^n\mathbb{Z}$ è locale: gli unici ideali propri sono $(p^i)$ con $i = 1, .., n-1$ e in particolare l'unico ideale massimale è $(p)$

**Definizione 1.12.** Dato un anello $A$ e due ideali $I, J \subset A$, si dice che $I$ e $J$ sono *comassimali* o *coprimi* se $I + J = A$

**Proposizione 1.6.** *Siano $I, J \subset A$ due ideali comassimali, allora $I \cap J = IJ$*

*Dimostrazione.*
Osserviamo intanto che l'inclusione $I \cap J \supset IJ$ è vera sempre.
Dimostriamo allora che se $\alpha \in I \cap J$, allora $\alpha \in IJ$. Infatti essendo $I, J$ comassimali esistono $i \in I, j \in J$ tali che $1 = i + j$.
Ma allora $\alpha = \alpha \cdot 1 = \alpha \cdot i + \alpha \cdot j$ ed entrambi i termini appartengono all'ideale $IJ$. □

**Osservazione.** Il viceversa non è in generale vero: se consideriamo come anello $K[x, y]$ e prendiamo gli ideali $(x), (y)$, vale chiaramente $(x) \cap (y) = (xy)$, ma ad esempio nell'ideale $(x) + (y)$ non troviamo le costanti.

**Esempio.** Su $\mathbb{Z}$, osserviamo che $(a) + (b) = (\gcd(a, b))$ mentre $(a) \cap (b) = (\operatorname{lcm}(a, b))$. Vediamo poi che se $\gcd(a, b) = 1$ allora $\operatorname{lcm}(a, b) = a \cdot b$, che è esattamente la proposizione.

**Lemma 1.7** (di scansamento)**.**

*a) Siano $A$ un anello, $P$ un ideale primo, $I_1, \dots, I_n$ ideali. Vale*

$$\bigcap I_i \subset P \Longrightarrow \exists j \mid I_j \subset P$$

*Inoltre se $\bigcap I_i = P$ vale anche $I_j = P$.*

*b) Siano $A$ un anello, $I \subset A$ un ideale, $P_1, \dots, P_n$ ideali primi. Vale*

$$I \subset \bigcup P_i \Longrightarrow \exists j \mid I \subset P_j$$

*Dimostrazione.*

a) Dimostriamo che $\forall i \;\; I_i \not\subset P \Longrightarrow \bigcap I_i \not\subset P$.
L'ipotesi ci fornisce allora per ogni $i$ un elemento $x_i \in I_i$ e $x_i \notin P$.
Ma allora $x_1 \cdots x_n \in \prod I_i \subset \bigcap I_i$, ma $x_1 \cdots x_n \notin P$ poiché prodotto di elementi che non stanno in un ideale primo.
Infine se $P = \bigcap I_i$, allora $I_i \supset \bigcap I_i = P$, e in particolare $P \subset I_j$, dove $I_j$ è l'ideale tale che $I_j \subset P$ che abbiamo appena dimostrato esistere, da cui $P = I_j$.

b) Dimostriamo per induzione su $n$ che $\forall i \;\; I \not\subset P_i \Longrightarrow I \not\subset \bigcup P_i$.
Il caso $n = 1$ è banale, dimostriamo il passo induttivo $n - 1 \to n$.
Per ipotesi induttiva vale che $I \not\subset \bigcup_{i \neq k} P_i \quad \forall k$, ovvero $\exists x_k \in I$ per cui $x_k \notin \bigcup_{i \neq k} P_i$.
Osserviamo che se per un qualche $k$, $x_k \notin P_k$, allora la tesi segue poiché $\bigcup P_i = P_k \cup \bigcup_{i \neq k} P_i$.
Supponendo per assurdo $x_i \in P_i \quad \forall i$, consideriamo $\alpha = \displaystyle\sum_{i=1}^{n} \prod_{j \neq i} x_j = x_2 \cdots x_n + x_1 x_3 \cdots x_n + \cdots + x_1 \cdots x_{n-1}$.
Chiaramente $\alpha \in I$; inoltre $P_i \ni \alpha - x_i(\dots) = \prod_{j \neq i} x_j \notin P_i$ perché prodotto di fattori che non stanno in $P_i$. Assurdo.

□

## 1.3 Quozienti e omomorfismi

Cominciamo ad entrare nel vivo della teoria degli anelli, e vediamo quali sono le relazioni che sussistono tra anelli diversi, e qual è la struttura e l'utilità degli anelli quozienti.

**Definizione 1.13** (Omomorfismo)**.** Dati due anelli $A, B$, una funzione $f : A \to B$ si dice *omomorfismo di anelli* se valgono le seguenti proprietà:

- $f(a + b) = f(a) + f(b)$
- $f(ab) = f(a)f(b)$

- $f(1_A) = 1_B$

**Osservazione.** Esiste un unico omomorfismo di anelli $f : \mathbb{Z} \to \mathbb{Z}$, ed è l'identità. Infatti $\mathbb{Z}$ è un gruppo ciclico e fissando l'immagine di 1 si fissa l'omomoerfismo.

**Definizione 1.14.** Si chiama *nucleo* dell'omomorfismo l'ideale $ker(f) = \{a \in A \mid f(a) = 0\}$.
Si dice *immagine* dell'omomorfismo il sottoanello $Im(f) = \{b \in B \mid \exists a \in A\ f(a) = b\}$

Come per i gruppi, possiamo definire una relazione d'equivalenza su $A$:
Fissato un ideale $I$, diciamo che $a \equiv b \pmod{I}$ se $a - b \in I$.
Le classi di equivalenza sono i laterali, che sono della forma $a + I$; l'insieme dei laterali è detto quoziente e si indica con $A/I$.

**Proposizione 1.8.** *Il quoziente $A/I$ ha una struttura di anello con le operazioni indotte da $A$:*

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

Possiamo allora definire un'importante mappa, la proiezione al quoziente:

$$\begin{aligned} \Pi : A &\to A/I \\ a &\mapsto a + I \end{aligned}$$

In particolare osserviamo che se $J \subset A$ è un ideale di $A$, allora $\Pi(J) = J/I$ è un ideale di $A/I$. Perciò vale la seguente

**Proposizione 1.9.** *Esiste una corrispondenza biunivoca tra gli ideali di $A/I$ e gli ideali $A \supset J \supset I$. Tale bigezione è data da $\Pi^{-1}(L) = \{b \in A \mid \Pi(b) \in L\}$*

Vi sono inoltre i fondamentali teoremi di omomorfismo, analoghi a quelli sui gruppi

**Teorema 1.10.**

*1) Sia $f : A \to B$ un omomorfismo. Allora $A/ker(f) \cong Im(f)$*

*2) Data una catena di ideali $I \subset J \subset A$ vale*

$$\frac{A/I}{J/I} \cong A/J$$

*Dimostrazione.*

1) Chiamiamo $I = ker(f)$; sia $\varphi : A/I \to Im(f)$ definita da $\varphi(a+I) = f(a)$.
Si osserva banalmente che $\varphi$ è un omomorfismo.
Supponiamo che $\varphi(a + I) = \varphi(b + I)$, ma allora $f(a) = f(b)$ ovvero $f(a - b) = 0$ e $a - b \in I$; quindi $\varphi$ è iniettiva.
Inoltre è chiaramente surgettiva, perciò è un isomorfismo.

2) Definiamo $f : A/I \to A/J$ come $f([b]_I) = [b]_J$, ed è una buona definizione in quanto se $[b_1]_I = [b_2]_I$ allora $b_1 - b_2 \in I \subset J$. Vediamo subito che è surgettiva.
Per il punto 1), basta dimostrare che $ker(f) = J/I$; ma questo si vede subito in quanto $f([b]_I) = 0 \iff b \in J$, perciò $ker(f) = \{j + I \mid j \in J\} = J/I$.

$\square$

Osserviamo ora che ci sono delle ben precise relazioni tra le proprietà dell'ideale $I$ e quelle dell'anello quoziente $A/I$. In particolare vale

**Proposizione 1.11.**

- *l'ideale $I$ è massimale $\iff$ $A/I$ è un campo*
- *l'ideale $I$ è primo $\iff$ $A/I$ è un dominio*
- *l'ideale $I$ coincide con $\sqrt{I}$ $\iff$ $A/I$ è ridotto*
- *l'ideale $I$ è primario $\iff$ $N(A/I) = D(A/I)$*

**Teorema 1.12** (cinese del resto)**.** *Sia $A$ un anello e $I_1, \dots, I_n$ ideali a coppie coprimi. Allora vale ${}^{A}\!/_{I_1 \times \dots \times I_n} \cong A/I_1 \times \dots \times A/I_n$*

*Dimostrazione.*
Consideriamo l'omomorfismo di proiezione $\varphi : A \to A/I_1 \times \dots \times A/I_n$ che manda $a$ in $([a]_{I_1}, \dots, [a]_{I_n})$. Dimostriamo che è surgettiva.
Prendiamo $(a_1, \dots, a_n) \in A/I_1 \times \dots \times A/I_n$; poiché gli ideali sono a coppie comassimali, $\forall i, j$ esistono $\alpha_i^{(j)} \in I_i, \alpha_j^{(i)} \in I_j$ tali che $\alpha_i^{(j)} + \alpha_j^{(i)} = 1$.
Costruiamo $L_i = \prod_{j \neq i} a_j^{(i)}$ e poi $a = \sum a_i L_i$.
Allora vediamo che $\varphi(a) = (a_1, \dots, a_n)$, poiché $L_i \equiv 0 \pmod{I_j}$ se $j \neq i$, mentre $L_i \equiv \prod(1 - \alpha_i^{(j)}) \equiv 1 \pmod{I_i}$.
Osserviamo che $\ker \varphi = \bigcap I_i$. Dimostriamo che $\bigcap I_i = \prod I_i$; per induzione, basta che $(I_n, \prod_{i \leq n-1} I_i) = (1)$.
Ma allora prendiamo $L_n \in \prod_{i \leq n-1} I_i$ e vediamo che vale $L_n \equiv 1 \pmod{I_n}$. $\square$

**Osservazione.** Se come anello consideriamo $\mathbb{R}[x]$ e come ideali quelli generati da polinomi di primo grado $I_i = (x - a_i)$, vediamo che gli $L_i$ sono proprio i polinomi interpolanti di Lagrange.

## 1.4 Ideali contratti ed estesi

Siano $A, B$ due anelli e $f : A \to B$ un omomorfismo. Prendiamo poi $I \subset A$ e $J \subset B$ ideali.

**Definizione 1.15.**

- L'ideale contratto di $J$ è $J^c = f^{-1}(J) = \{a \in A \mid f(a) \in J\}$
- L'ideale esteso di $I$ è $I^e = (f(I)) = \{\sum b_i f(a_i) \mid a_i \in I\}$ cioè l'ideale generato dall'immagine di $I$

Vale la seguente proprietà

**Proposizione 1.13.**

1. *$J^c$ è un ideale $\forall J \subset B$ ideale.*
2. *se $f$ è surgettiva, allora $f(I)$ è un ideale.*

*Dimostrazione.*

1. Siano $a, b \in J^c$, allora $f(a), f(b) \in J$; ma allora $J \ni f(a)+f(b) = f(a+b)$ cioè $a+b \in J^c$. Inoltre se $c \in A$, $J \ni f(c)f(a) = f(ca)$ cioè $ca \in J^c$
2. Vale banalmente $f(I) \subset (f(I))$; prendiamo ora $b \in I^e$ ovvero $b = \sum b_i f(a_i)$. Poiché $f$ è surgettiva, esistono $c_i \in A$ tali che $b_i = f(c_i)$ $\forall i$. Allora $b = f\left(\sum c_i a_i\right) \in f(I)$.

□

**Esercizio 1.2.** Valgono le uguaglianze $I^{ece} = I$ e $J^{cec} = J$

**Proposizione 1.14.** *La contrazione di un ideale primo è primo.*

*Dimostrazione.*
Sia $J \subset B$ un ideale primo; supponiamo $ab \in J^c$, ovvero $f(ab) \in J$. Ciò vuol dire $f(a)f(b) \in J$, ed essendo primo abbiamo $f(a) \in J$ oppure $f(b) \in J$, cioè $a \in J^c$ o $b \in J^c$ □

## 1.5 Esercizi svolti

**Problema 1.1.** Se $A$ è un anello finito, allora $A = D(A) \cup A^*$

**Problema 1.2.** Dato un anello $A$ e un ideale $I \subset A$ tale che $\forall x \notin I \;\; x \in A^*$, dimostrare che $A$ è locale e $I$ è il suo massimale.

**Problema 1.3.** Dato un anello $A$ in cui ogni ideale primo è principale, allora ogni ideale è principale ($A$ è un PIR).

**Problema 1.4.** $D(A)$ è unione di ideali primi; inoltre $D(A) = \bigcup \sqrt{\mathrm{Ann}(a)}$

**Problema 1.5.** Se $\sqrt{I}$ è massimale, allora $I$ è primario.

# 2 Anelli di polinomi

## 2.1 Polinomi in una variabile

Sia $A$ un anello e consideriamo l'anello di polinomi $A[x]$.
Prendiamo il morfismo di inclusione $i : A \hookrightarrow A[x]$, siano $I \subset A, J \subset A[x]$ e studiamo $I^e, J^c$. Si vede subito che vale

**Proposizione 2.1.**

- $J^c = J \cup A$
- $I^e = I[x]$

Vale inoltre la importante

**Proposizione 2.2.** *Dato $I \subset A$ ideale,* $A[x]\diagup_{I[x]} \cong \left(A\diagup_I\right)[x]$

*Dimostrazione.*
Consideriamo $\varphi : A[x] \to \left(A\diagup_I\right)[x]$ tale che $\varphi\left(\sum a_i x^i\right) = \sum \pi(a_i)x^i$ dove $\pi$ è la proiezione al quoziente.
È chiaramente surgettiva; inoltre $ker\varphi$ è esattamente $I[x]$, perciò il risultato segue dal primo teorema di omomorfismo. □

**Corollario.** *Se $I \subset A$ è primo, allora $I^e = I[x]$ è primo in $A[x]$*

Infatti, se $A/I$ è dominio, anche $\left(A\diagup_I\right)[x]$ è dominio; ma questo è esattamente $A[x]\diagup_{I[x]}$, perciò $I[x]$ è primo.

Detto $R = A[x]$ con $A$ anello, cerchiamo di identificare $N(R), D(R)$ e $R^*$.

**Proposizione 2.3.** *Sia $f = \sum a_i x^i \in R$. Allora*

1. $f \in R^* \iff a_0 \in A^*$ *e* $a_1, \ldots, a_n \in N(A)$
2. $f \in N(R) \iff a_i \in N(A)\ \forall i$
3. $f \in D(R) \iff \exists a \in A$ *tale che* $af = 0$

*Dimostrazione.*

2, $\Leftarrow$ Detti $m_i$ gli indici di nilpotenza di $a_i$, si vede facilmente che $f^{m_1+\cdots+m_n+1} = 0$

1, $\Leftarrow$ Usando la freccia appena dimostrata di 2, sappiamo che $g(x) = a_1x + \cdots + a_nx^n \in N(R)$; ma allora $f = a_0 + g$ è somma di un invertibile e un nilpotente, quindi è ancora invertibile.

1, $\Rightarrow$ Sia $g = \sum b_i x^i$ di grado $m$ tale che $fg = 1$; guardando il termine noto sappiamo $a_0b_0 = 1$ perciò $a_0$ e $b_0$ sono invertibili.
Considerando poi i termini di grado maggiore abbiamo $0 = a_nb_m$ e $0 = a_nb_{m-1} + a_{n-1}b_m$, da cui moltiplicando la seconda per $a_n$ otteniamo $a_n^2b_{m-1} = 0$. Continuando così ricaviamo $a_n^{r+1}b_{m-r} = 0$; se prendiamo $r = m$ abbiamo $a_n^{m+1}b_0 = 0$ ed essendo $b_0$ invertibile, abbiamo $a_n$ nilpotente.
Riapplichiamo ora questo ragionamento a $f - a_nx^n$ che è ancora invertibile.

2, $\Rightarrow$ Se $f$ è nilpotente, anche $xf \in N(R)$; ma allora $1 + xf \in R^*$ e per la 1 si deve avere $a_0, \ldots, a_n \in N(A)$.

□

## 2.2 Ideali monomiali

Prendiamo ora un campo $k$ e consideriamo l'anello $A = k[x_1, \dots, x_n]$.
Diamo una notazione per rendere le scritture più compatte: chiamiamo $X = (x_1, \dots, x_n)$ e se $\alpha = (a_1, \dots, a_n)$ allora $X^\alpha$ indica il monomio $x_1^{a_1} \cdots x_n^{a_n}$.
In generale un $f \in k[X]$ si scrive come $f = \sum c_\alpha X^\alpha$ con $c_\alpha \in k$, e la somma è finita.

**Definizione 2.1.** Un ideale $I \subset A$ è detto *monomiale* se $\exists E \in \mathbb{N}^n$ tale che $I = (X^\alpha, \alpha \in E)$

**Proposizione 2.4.** *Dato un ideale $I$ monomiale, $f = \sum c_\beta X^\beta \in I$ se e solo se $X^\beta \in I \ \forall \beta$*

*Dimostrazione.*
Una freccia è ovvia. Se invece $f \in I$, allora $f = \sum_{\alpha \in E} P_\alpha(X) X^\alpha$ con $P_\alpha(X) = \sum d_{\gamma,\alpha} X^\gamma$ con i $d \in k$. Quindi $\sum c_\beta X^\beta = f = \sum d_{\gamma,\alpha} X^{\alpha+\gamma}$, perciò ogni $X^\beta$ è della forma $X^{\alpha+\gamma}$ ovvero $X^\beta \in I$ □

Osserviamo che agli ideali monomiali corrispondono in maniera ovvia certi sottoinsiemi di $\mathbb{N}^n$ grazie alla mappa $X^\alpha \mapsto (a_1, \dots, a_n)$.

**Definizione 2.2.** Un sottoinsieme non vuoto $E \subset \mathbb{N}^n$ si dice $\mathcal{E}$-sottoinsieme se $\forall \alpha \in E, \forall \beta \in \mathbb{N}^n$ anche $\alpha + \beta$ sta in $E$.
$F \subset E$ si dice *frontiera* di $E$ se $\forall \alpha \in E \ \ \exists \gamma \in F, \beta \in \mathbb{N}^n$ tali che $\alpha = \gamma + \beta$

**Lemma 2.5** (Dickson)**.** *Ogni $\mathcal{E}$-sottoinsieme $E$ ha una frontiera finita.*

*Dimostrazione.*
Facciamo una induzione su $n$.
Se $n = 1$, allora $E \subset \mathbb{N}$; ma poiché $\mathbb{N}$ è ben ordinato, la frontiera è semplicemente $\min(E)$.
Passo induttivo $n \Rightarrow n + 1$: $E \subset \mathbb{N}^{n+1}$.
Consideriamo la proiezione $\Pi : \mathbb{N}^{n+1} \to \mathbb{N}^n$ che ignora l'ultima coordinata. Allora $\Pi(E)$ è ancora un $\mathcal{E}$-sottoinsieme: infatti $\Pi(\alpha) + \gamma = \Pi(\alpha + (\gamma, 0))$.
Per ipotesi induttiva $\Pi(E)$ ha una frontiera finita $\hat{F} = \{\hat{\gamma}_1, \dots, \hat{\gamma}_k\}$. Siano $\gamma_i \in E$ tali che $\Pi(\gamma_i) = \hat{\gamma}_i$, e $\tilde{F} = \{\gamma_i\}$.
Prendiamo $\bar{a}$ il massimo delle componenti $n+1$-esime dei $\gamma_i$, e per ogni $a < \bar{a}$ poniamo $E_a = E \cap \left(\mathbb{N}^n \times \{a\}\right)$.
Si vede che $\Pi(E_a)$ è ancora un $\mathcal{E}$-sottoinsieme di $\mathbb{N}^n$ e quindi ha frontiera finita $\hat{F}_a = \{\gamma_{a,1}, \dots, \gamma_{a,k_a}\}$; rimontiamo questo insieme in $E$: $F_a = \{(\gamma_{a,i}, a) \mid i = 1, \dots, k_a\}$.
Allora la frontiera di $E$ è $F = \tilde{F} \cup \left(\bigcup_{a<\bar{a}} F_a\right)$.
Sia infatti $\alpha = (a_1, \dots, a_n, a_{n+1}) \in E$; se $a_{n+1} \geq \bar{a}$, allora esiste un $\beta \in \tilde{F}$ tale che $\alpha - \beta \in \mathbb{N}^{n+1}$; se $a_{n+1} < \bar{a}$, allora $\alpha \in E_{a_{n+1}}$ per cui $\exists \gamma \in F_{a_{n+1}}$ per cui $\alpha - \gamma \in \mathbb{N}^{n+1}$. □

**Corollario.** *Ogni ideale monomiale è finitamente generato*

**Proposizione 2.6.** *Dato un $\mathcal{E}$-sottoinsieme $E \subset \mathbb{N}^n$, esiste un'unica frontiera di cardinalità minima.*

Operazioni, caratterizzazione...

## 2.3 Riduzione di polinomi

Ordinamento
Riduzione
Alg divisione

## 2.4 Basi di Gröbner

Caratterizzazione
Alg Buchberger
Eliminazione
0-dimensionale

## 2.5 Risoluzione dei sistemi di equazioni polinomiali

Varietà affine
Risultante
Estensione
Nullstellensatz

# 3 Moduli