Schemi di Algebra 2

Giulio Del Corso

7 maggio 2016

Indice

Capitolo 1

Anelli e ideali

1.1 Anelli e ideali

Definizione 1.1.1. Un **anello** è un insieme munito di due operazioni, $(A, +, \cdots)$ con $(A, +)$ gruppo abeliano e distributivo ed associativo rispetto al $\cdot$

Definizione 1.1.2. Un **anello commutativo** è commutativo per l'operazione $\cdot$

Definizione 1.1.3. Un **anello commutativo con unità** è un anello per il quale $\exists\ 1 := Id_A$

> **Osservazione 1.1.1:** Lavoreremo quasi sempre con anelli commutativi con unità.
> Gli anelli non banali hanno $0 \neq 1$

Definizione 1.1.4. u è un'**unità** $\iff \exists a \in A \mid ua = 1_A$

> **Osservazione 1.1.2:** $A^* := \{u\ unit\} = \{invertibili\}$

Definizione 1.1.5. a si dice un **divisore di 0** se $\exists b \in A\ ;\ ab = 0$

> **Osservazione 1.1.3:** $D(A) := \{divisori\ di\ 0\ di\ A\}$

> **Osservazione 1.1.4:** Se A è fiinito, allora $A = A^* \cup D(A)$ con $A^* \cap D(A) = \emptyset$

Definizione 1.1.6. Un **dominio di integrità** è un anello A tale che $D(A) = 0$

Osservazione 1.1.5: In un dominio di integrità vale la legge di cancellazione:
$a \neq 0$; $ab = ac \implies b = c$

Definizione 1.1.7. Un elemento a si dice **nilpotente** se $\exists n \in \mathbb{N} \mid a^n = 0$

Osservazione 1.1.6: $N(A) := \{nilpotenti\}$; $N(A) \subseteq D(A)$

Definizione 1.1.8. Un anello si dice **ridotto** se $N(A) = (0)$

Definizione 1.1.9. Un elemento a si dice **idempotente** se $a^2 = a$

Definizione 1.1.10. $B \subseteq A$ è un **sottoanello** di A se è un anello con le operazioni indotte da A.

Definizione 1.1.11. Un **ideale** di un anello A è un sottogruppo rispetto al $+$ e vale la proprietà di assorbimento:
$a \in In \implies ax \in I \ \forall x \in A$

Osservazione 1.1.7: Un ideale si dice **proprio** se non è coincidente con l'anello A.

Osservazione 1.1.8: Ideale non implica sottoanello. Ogni sottoanello infatti possiede 1 mentre ogni ideale che possiede l'1 coincide con l'anello.

Definizione 1.1.12. Un **omomorfismo di anelli** è una $f : A \to B$ con A, B anelli tale che:
$f(a_1 + a_2) = f(a_1) + f(a_2)$
$f(a_1 a_2) = f(a_1) f(a_2)$
$f(1_A) = 1_B$

Osservazione 1.1.9: Dato $f : A \to B$ un omomorfismo di anelli:
$Ker(f) = \{a \in A \mid f(a) = 0\}$ è un ideale di A
$Im(f)$ è un sottoanello di B
f iniettivo $\iff Ker(f) = 0$
f surgettivo $\iff Im(f) = B$

1.2 Anelli a ideali principali e a fattorizzazione unica

Definizione 1.2.1. Dato un sottoinsieme $S \subseteq A$, l'**ideale generato da** S è:

$$(S) = \{\sum_i^k a_i s_i \ finite \ con \ a_i \in A \ ; \ s_i \in S\} \tag{1.1}$$

Definizione 1.2.2. Un ideale si dice **finitamente generato** se $I = (s_1, \cdots, s_n)$

Definizione 1.2.3. Un ideale si dice **principale** se è generato da un singolo elemento, $I = (a)$

> **Osservazione 1.2.1:** In $\mathbb{Z}$ tutti gli ideali sono principali.
> In $\mathbb{K}[x]$ tutti gli ideali sono principali.
> $\mathbb{Z}[x, y]$ non è un PID ma ogni ideale è finitamente generato.

Definizione 1.2.4. Un anello si dice un PID se ogni ideale è principale.

1.3 Operazioni su ideali di un anello commutativo unitario

Dato $\{I_h\}_{h \in H}$:
$\bigcap I_h$ è un ideale di A
$\sum_{h \in H} I_h$
$\prod_h I_h = \{\sum i_k i_j \ ; \ i_k \in I_k \ ; \ i_j \in I_j\}$
$(I : J) = \{a \in A \mid aJ \subseteq I\}$
$\sqrt{I}$

> **Osservazione 1.3.1:** $I : J \subseteq I \cap J$

1.4 Annullatore

Definizione 1.4.1. L'**annullatore** di un ideale è $(0 : J)$

1.5 Ideali coprimi

Definizione 1.5.1. Due ideali I, J si dicono **coprimi** se$I + J = A$.

Proposizione 1.5.1. *Se I, J sono due ideali coprimi allora $IJ = I \cap J$*

Il viceversa è falso:
$(x)(y) = (x) \cap (y)$ ma $(x, y) = (x) + (y) \neq \mathbb{K}[x, y]$

1.6 Ideale quoziente

Definizione 1.6.1. L'**anello quoziente** si definisce a partire da $f : A \to B$ omomorfismo di anelli ; $I \subseteq Ker(f)$; I ideale proprio di A.

$$\frac{A}{I} := \{a + I\} \tag{1.2}$$

Con operazioni date da:
$(a + I) + (b + I) = (a + b) + I$
$(a + I)(b + I) = ab + I$
E' un anello.

Sono notazioni equivalenti:
$a + I = b + I$
$a = b(I)$
$a - b \in I$

Metodi sul quoziente per verificare determinate proprietà:
I proprio $\iff \frac{A}{I} \neq (0)$
I primo $\iff \frac{A}{I}$ è un dominio
I massimale $\iff \frac{A}{I}$ è un campo
I primario $\iff$ in $\frac{A}{I}$ i divisori di 0 sono nilpotenti, ossia $Q(\frac{A}{I} \subseteq N(\frac{A}{I})$
I radicale $\iff \frac{A}{I}$ è privo di nilpotenti $\neq$, ossia $N(\frac{A}{I}) = (0)$

1.7 Ideali primi, massimali e irriducibili

Definizione 1.7.1. I ideale si dice **primo** se $ab \in I \implies a \in I$ o $b \in I$

> **Osservazione 1.7.1:** Tutti gli ideali generati da un primo sono primi.

Definizione 1.7.2. I ideale si dice **massimale** se $I \subseteq J \implies J = I$ oppure $J = A$

> **Osservazione 1.7.2:** A dominio infinito con $|A^*| < \infty \implies A$ possiede ∞ ideali massimali.

> **Osservazione 1.7.3:** A anello, $\exists$ sempre almeno un ideale massimale.

> **Osservazione 1.7.4:** Se I è un ideale di A proprio $\implies \exists M$ ideale massimale con $I \subseteq M$

Osservazione 1.7.5: a non invertibile $\implies \exists M$ ideale massimale tale che $a \in M$

Definizione 1.7.3. I ideale si dice **primario** se $ab \in I \implies a \in I$ oppure $b^n \in I$

Definizione 1.7.4. I ideale si dice **radicale** se $\sqrt{I} = I$

1.8 Nilradicale e radicale di Jacobson

Definizione 1.8.1. Il **radicale di Jacobson** è definito come:

$$J(A) := \bigcap_{M \ massimali \ di \ A} M \tag{1.3}$$

Proposizione 1.8.1. $a \in J(A) \iff \forall b \in A \ ; 1 - ab \in A^*$

Definizione 1.8.2. Il **Nilradicale** di un anello A è definito come:

$$N(A) = \sqrt{(0)} = \bigcap_{P \subset A \ primi} P \tag{1.4}$$

Proposizione 1.8.2. $\sqrt{I} = \bigcap_{I \subset P \subset A \ primi} P$

1.9 Estensioni e contrazioni di ideali

Definizione 1.9.1. Dato $f : A \to B$ omomorfismo di anelli, I ideale di A, J ideale di B, l'ideale contratto è definito come:

$$J^C := f^{-1}(J) = \{a \in A \mid f(a) \in J\} \tag{1.5}$$

Questo è sempre un ideale.

Dato I, $f(I)$ non è necessariamente un ideale ma è un sottoinsieme, quindi si prende:

$$I^e := (f(I)) = \{\sum b_j f(a_i) \mid a_i \in I\} \tag{1.6}$$

Questo si definisce l'**ideale esteso di** I.

Proposizione 1.9.1. *A dominio di integrità, allora:*
a primo $\implies$ a irriducibile

1.10 Ideale prodotto

Proposizione 1.10.1. *In $A \times B$; I ideale di A ; J ideale di B ; gli ideali sono tutti e soli della forma $I \times J$*

1.11 Teorema cinese del resto

Proposizione 1.11.1. *$P_1, \cdots, P_n$ primi ; $I \subseteq \bigcup_{i=1}^n P_i \implies \exists \bar{i}$ con $I \subseteq I_{\bar{i}}$ $I_1, \cdots, I_n$ ideali, P primo t.c. $\bigcap_{i=1}^n I_i \implies \exists \bar{i}$ con $I_{\bar{i}} \subseteq P$ tale che se $P = \bigcap I_i \implies P = I_{\bar{i}}$*

> **Osservazione 1.11.1:** A anello, $I_1, \cdots, I_n$ ideali con $(I_i, I_j) = 1$ allora $\forall a_1, \cdots, a_n \in A \exists a \in A \mid a \equiv a_i \ (I_i)$

In pratica:
Data una applicazione $f : A \rightarrow \frac{A}{I_1} \times \cdots \times \frac{A}{I_n}$ se gli I_i sono relativamente priimi, allora la mappa:
$f(a) \rightarrow f(\overline{a_1}, \cdots, \overline{a_n})$ è surgettiva (TCR).

1.12 Anello dei polinomi $A[x]$

Dato $f(x) \in A[x]$
f è un'unita $\iff a_0 \in A^*$ e $a_i \in N(A) \ \forall i \geq 1$
f è nilpotente $\iff a_i \in N(A) \ \forall i$
f divisore di 0 $\iff \exists c \in A \ ; \ c \neq 0 \ ; \ cf = 0$

Proposizione 1.12.1. *a nilpotente $\rightarrow 1 + a$ invertibile*

Proposizione 1.12.2. *I primario $\iff I[x]$ primo.*

Proposizione 1.12.3. *I primario $\iff I[x]$ è primario.*

Attenzione:
Queste proprietà non valgono per estensioni in generale. La primalità si conserva per contrazione mentre la massimalità no.

Capitolo 2

Polinomi in piu' variabili

Estendiamo il concetto di divisione euclidea ai polinomi multivariabili. Nel caso specifico degli ideali monomiali sarà particolarmente facile determinare se un elemento appartiene all'ideale, in generale questi saranno i primi passi verso le basi di Grobner.

2.1 Ordinamento monomiale

Lemma 1. *$(\mathbb{N}^n, \geq)$ è un buon ordine $\iff$ ogni catena discendente è stazionaria.*

Definizione 2.1.1. Un **ordinamento monomiale** è una relazione d'ordine su $\mathbb{N}^n$ che rispetta le seguenti prorpietà:

1. è un buon ordine
2. $\forall \alpha, \beta, \gamma \in \mathbb{N}^n \; \alpha < \beta \implies \alpha + \gamma < \beta + \gamma$

Algoritmi di uso frequente:

Ordinamento lessicografico:
$\alpha \geq \beta \implies$ il primo termine non nullo di $\alpha - \beta$ è maggiore di 0.

Ordinamento totale lex:
Detto $|\alpha| = a_1 + \cdots + a_n$
$\alpha \geq \beta \implies |\alpha| \geq |\beta| \vee \alpha \geq \beta$ per l'ordinamento lessicografico.

Ordinamento reverse lex:
Detto $|\alpha| = a_1 + \cdots + a_n$
$\alpha \geq \beta \implies |\alpha| \geq |\beta| \vee |\alpha| = |\beta|$ e l'ultimo termine non 0 in $\alpha - \beta$ è $<$ di 0

2.2 Algoritmo di divisione per polinomi in $\mathbb{K}[x_1, \cdots, x_n]$

Definizione 2.2.1. Sia $f \in \mathbb{K}[x_1, \cdots, x_n]$, $f = \sum_\alpha c_\alpha x^\alpha$, dove $c_\alpha \in \mathbb{K}$, fissato un ordinamento monomiale, definiamo:

1. Il **multigrado di un polinomio** è $deg(f) := max\{\alpha | c_\alpha \neq 0\}$
2. Il **coefficiente direttore** è $lc(f) = c_\alpha$ dove $\alpha = deg(f)$
3. Il **termine di testa** è $lt(f) = c_\alpha x^\alpha$, dove $\alpha = deg(f)$
4. Il **monomio di testa** è $lm(f) = x^\alpha$, dove $\alpha = deg(f)$

Teorema 1. *Consideriamo $R = \mathbb{K}[x_1, \cdots, x_n]$ con un fissato ordinamento monomiale, siano $p, f_1, \cdots, f_k \in R \implies \exists\ a_1, \cdots, a_k \in R\ \exists r \in R$ t.c.*

$$p = \sum_{i=1}^{k} a_i f_i + r \tag{2.1}$$

Dove $\forall i\ deg(p) \geq deg(a_i f_i)$
$r = 0 \vee r = \sum r_\alpha x^\alpha$ in modo tale che $\forall \alpha\ x^\alpha \notin (lt(f_1) \cdots lt(f_k))$

Lo pesudocodice dell'algoritmo è:

$p \leftarrow f$
$r \leftarrow 0$
while $p \neq 0$ **do**
$i \leftarrow 1$
$diviso \leftarrow false$
while $i \leq k$ et $diviso == false$ **do**
if $lt(f_i) | lt(p)$ **then**
$c_i \leftarrow \frac{lt(p)}{lt(f_i)}$
$p \leftarrow p - c_i f_i$
$diviso \leftarrow true$
$a_i \leftarrow a_i + c_i$
else $i++$
end if
end while
if $diviso == false$ **then**
$r \leftarrow r + lt(p)$
$p \leftarrow p - lt(p)$
end if
end while

Osservazione 2.2.1: L'algoritmo descritto non garantisce l'unicità del resto. Necessitiamo di determinati f_i che rendano efficace l'algoritmo.
Dato un ideale I possiamo associare l'ideale $lt(I) := (\{lt(f)|f \in I\})$. $lt(I)$ è per definizione monomiale, dunque esistono dei polinomi $g_1, \cdots, g_k$ tali che $lt(I) = (lt(g_1), \cdots, lt(g_k))$

Teorema 2. *Sia I un ideale di $\mathbb{K}[x_1, \cdots, x_n]$ e siano $g_1, \cdots, g_k \in I$ tali che $lt(I) = (lt(g_1), \cdots, lt(g_k))$. Allora:*

1. $I = (g_1, \cdots, g_k)$
2. $f \in I \iff$ *il resto della divisione di f per $\{g_i | i \in \{1, \cdots, k\}\}$ è 0*

Corollario 1: Ogni ideale di $\mathbb{K}[x_1, \cdots, x_n]$ è finitamente generato.

2.3 Ideali monomiali

Definizione 2.3.1. $I \subseteq \mathbb{K}[x_1, \cdots, x_n]$ si dice **monomiale** se $\exists A \subseteq \mathbb{N}^n$ tale che $I = (x^\alpha | \alpha \in A)$

Determinare se un polinomio appartiene ad un ideale monomiale è particolarmente semplice, infatti:

Proposizione 2.3.1. *Sia I un ideale monomiale, $I = (x^\alpha | \alpha \subseteq \mathbb{N}^n)$, sia $f = \sum_\gamma c_\gamma x^\gamma$*

, allora:

$$f \in I \iff \forall \gamma \ , \ c_\gamma x^\gamma \in I \tag{2.2}$$

Vogliamo scrivere una corrispondenza fra monomi e vettori $a \in \mathbb{N}^n$ dei gradi delle variabili; gli ideali a quel punto sono equivalenti a certi sottoinsiemi di $\mathbb{N}^n$

Definizione 2.3.2. $A \subseteq \mathbb{N}^n$ si dice **E-sottoinsieme** se $A \neq 0$ e se vale:

$$x \in A \implies \forall \in \mathbb{N}^n \ x + \gamma \in A \tag{2.3}$$

2.4 Frontiera di un ideale monomiale

Definizione 2.4.1. $F \subseteq A$, con A E-sottoinsieme, si dice una **frontiera** di A se:

$$\forall \alpha \in A \ \exists f \in F \ \exists \gamma \in \mathbb{N}^n | \alpha = f + \gamma \tag{2.4}$$

Lemma 2. *Sia A un E-sottoinsieme di $\mathbb{N}^n$ e $\pi : \mathbb{N}^n \to \mathbb{N}^{n-1}$ la proiezione su $n-1$ componenti. Allora $\pi(A)$ è un E-sottoinsieme di $\mathbb{N}^{n-1}$*

2.5 Lemma di Dickson

Lemma 3 (Dickson). *Ogni E-sottoinsieme ammette una frontiera finita.*

Corollario 2: Ogni ideale monomiale è finitamente generato.

2.6 Proprietà degli ideali monomiali

Vogliamo caratterizzare le frontiere di un E-sottoinsieme. Se esiste una frontiera minimale allora, mediante la corrispondenza vista prima, esisterebbe un insieme di generatori non ridondanti di un ideale monomiale.

Proposizione 2.6.1. *Dato un A un E-sottoinsieme, esiste un'unica frontiera di cardinalità minimale di A.*

Proposizione 2.6.2. *Siani I, J due ideali monomiali, $I = (m_1, ..., m_k)$. Allora:*

a) $I \cap J$ *è monomiale*

b) Se $m_k = uv$*, con* $(u, v) = 1 \implies (I, u) \cap (I, v)$

2.7 Caratterizzazione degli ideali monomiali irriducibili, radicali, primi e primari

Lemma 4. *Sia I un ideale tale che* $\sqrt{I}$ *è massimale* $\implies$ *I è primario.*

Proposizione 2.7.1. *Sia* $I = (m_1, \cdots, m_k)$ *un ideale monomiale con una base minimale.*

1) I è primo $\iff \forall i\ \exists x_{j_i}$ *t.c.* $m_i = x_{j_i}$

2) I è radicale $\iff \forall i\ m_i = x_{i_1}, \cdots, x_{i_k}$ *con* $i_k \neq i_h$ *se* $h \neq k$

3) I è primario $\iff I = (x_{i_1}^{\alpha_1}, \cdots, x_{i_k}^{\alpha_k}, m_1, \cdots, m_s =$ *con* $m_i \in \mathbb{K}[x_{i_1}, \cdots, x_{i_k}]$

Capitolo 3

Basi di Grobner

3.1 Basi di Grobner

Definizione 3.1.1. $(g_1, \cdots, g_k)$ si dice una **base di Grobner** di I se $g_i \in I\ \forall i$ e $lt(I) = (lt(g_1), \cdots, lt(g_k))$

Il resto della divisione di un polinomio f per una base di Grobner G si indica con $\overline{f}^G$

Definizione 3.1.2. Una base di Grobner si dice **minimale** se:

1. $(lt(g_1), \cdots, lt(g_k))$ è la frontiera di cardinalità minimale di $lt(I)$
2. $\forall i = 1, \cdots, k\ lc(g_i) = 1$

Definizione 3.1.3. Una base di Grobner è detta **ridotta** se è minimale e inoltre:
$\forall i = 1, \cdots, k\ \overline{g_i}^{G-\{g_i\}} = g_i$

Teorema 3. *Sia I un ideale di $\mathbb{K}[x_1, \cdots, x_n]$. Allora I ammette un'unica base di Grobner ridotta.*

Definizione 3.1.4. Siano f, g polinomi di $\mathbb{K}[x_1, \cdots, x_n]$, siano $\alpha = deg(f)$ e $\beta = deg(g)$.
Detto $\gamma \in \mathbb{N}^n$ il vettore di componenti $\gamma_i = max(\alpha_i, \beta_i)$ definiamo l'**S-polinomio** fra f e g come:

$$S(f, g) = \frac{x^\gamma}{lt(f)} f - \frac{x^\gamma}{lt(g)} g \tag{3.1}$$

Teorema 4. *Sia $I = (g_1, \cdots, g_k)$ un ideale di $\mathbb{K}[x_1, \cdots, x_n]$.*
$\{g_1, \cdots, g_k\}$ è una base di Grobner $\iff \forall i = 1, \cdots, k\ \forall j \neq i\ \overline{S(g_i, g_j)}^G = 0$

3.2 Algoritmo di Buchberger

$F \leftarrow f_1, \cdots, f_k$
$G \leftarrow F$
$G' \leftarrow \emptyset$
while $G \neq G'$ **do**
$G' \leftarrow G$
for $i = 1\ ;\ i \leq \#G\ ;\ i{+}{+}$ **do**
for $j = 1\ ;\ j \leq \#G\ ;\ j{+}{+}$ **do**
$s \leftarrow \overline{S(f_i, f_j)}$
if $s \neq 0$ **then**
$G \leftarrow G \cup \{s\}$
end if
end for
end for
end while

Lemma 5. *Ogni catena ascendente di ideali di* $\mathbb{K}[x_1 \cdots, x_n]$ *è stazionaria.*

Proposizione 3.2.1. *L'algoritmo di Buchberger termina ed è corretto.*

3.3 Proprietà di eliminazione dell'ordinamento lessicografico

Definizione 3.3.1. Sia I un ideale di $\mathbb{K}[x_1, \cdots, x_n]$.
Definiamo il **k-esimo ideale di eliminazione** come:

$$I_k := I \cap \mathbb{K}[x_{k+1}, \cdots, x_n] \tag{3.2}$$

Teorema 5. *Sia G una base di Grobner di un ideale I rispetto all'ordinamento lessicografico $x_1 > x_2 > \cdots > x_n$.*
Sia $G_k = G \cap \mathbb{K}[x_{k+1}, \cdots, x_n]$.
Allora G_k è una base di Grobner di I_k.

3.4 Risultante

Definizione 3.4.1. Sia R un dominio di integrità e siano $f, g \in R[x]$

$$\begin{aligned} f &= a_m x^m + \cdots + a_0 \\ g &= b_n x^n + \cdots + b_0 \end{aligned} \tag{3.3}$$

La **matrice di Sylvester** associata è:

$$Syl(f,g) = \begin{pmatrix} a_m & \cdots & a_0 & & & \\ & \ddots & & & \ddots & \\ & & a_m & & \cdots & a_0 \\ b_n & \cdots & b_1 & b_0 & & \\ & \ddots & & & \ddots & \\ & & b_n & & \cdots & b_0 \end{pmatrix} \tag{3.4}$$

Il **risultante** di f, g è:

$$Ris(f,g) = det(Syl(f,g)) \tag{3.5}$$

Proposizione 3.4.1. *Siano $f, g \in R[x]$ e $a, b \in R$. Allora:*

1. $Ris(f,g) = (-1)^{mn} Ris(g,f)$
2. $Ris(af,g) = a^m Ris(f,g)$ *e* $Ris(f,ag) = a^n Ris(f,g)$

Teorema 6. *Sia R un dominio, $g \in R[x]$ un polinomio di grado $n > 0$. Allora:*

$$Ris_x(f_m(x,y), g(x)) = g(y_m) Ris_x(f_{m-1}(x,y), g(x)) \tag{3.6}$$

Corollario 3: Siano $f, g \in \mathbb{K}[x]$. Allora:

$$Ris(f,g) = 0 \iff \exists \alpha \in \overline{\mathbb{K}} \ t.c. \ f(\alpha) = g(\alpha) = 0 \tag{3.7}$$

Corollario 4: Siano $f, g \in R[x]$, sia a_m il coefficiente direttore di f e siano z_i le radici di f.

$$Ris(f,g) = a_m^n \prod g(z_i) \tag{3.8}$$

Corollario 5: Siano R un dominio, $f, h_1, h_2 \in R[x]$.

$$Ris(f, h_1 h_2) = Ris(f, h_1) Ris(f, h_2) \tag{3.9}$$

Corollario 6: Siano R un dominio, $f, h, g \in R[x]$.

$$Ris(f, hf + p) = a_n^{N - deg(p)} Ris(f, p) \tag{3.10}$$

Dove $N = \deg hf$

Proposizione 3.4.2. *Siano $f, g \in R[x]$, allora:*

$$Ris(f,g) = Af + Bg \tag{3.11}$$

Dove $\deg A < \deg g$ *e* $\deg B < \deg f$

Lemma 6. *Sia $\phi : R[x] \to R[x]$ un omomorfismo di R-moduli e siano $f, g \in R[x]$ due polinomi tali che* $\deg f = \deg \phi f$ *e* $\deg g = \deg \phi g$. *Allora:*

$$\phi(Ris(f,g)) = Ris(\phi f, \phi g) \tag{3.12}$$

3.5 Teoremi di estensione

Definizione 3.5.1. Sia $I \subseteq \mathbb{K}[x_1, \cdots, x_n]$ un ideale, la **varietà affine** di I è:

$$\mathbb{V}(I) := \{\alpha \in \mathbb{K}^n \mid f(\alpha) = 0 \ \forall f \in I\} \tag{3.13}$$

Data una varietà affine V, definiamo:

$$\mathbb{I}(V) := \{f \in \mathbb{K}[x] \mid f(\alpha) = 0 \ \forall \alpha \in V\} \tag{3.14}$$

Proposizione 3.5.1. *Siano I, J ideali e V, W varietà affini. Allora:*

1. $I \subseteq J \implies \mathbb{V}(J) \subseteq \mathbb{V}(I)$
2. $\mathbb{V}(\mathbb{I}(\mathbb{V}(I))) = \mathbb{V}(I)$
3. $V \subseteq W \iff \mathbb{I}(W) \subseteq \mathbb{I}(V)$
4. $\mathbb{V}(I + J) = \mathbb{V}(I) \cap \mathbb{V}(J)$
5. $\mathbb{V}(IJ) = \mathbb{V}(I) \cup \mathbb{V}(J)$
6. $\mathbb{V}(I \cap J) = \mathbb{V}(I) \cup \mathbb{V}(J)$

Corollario 7: Siano V, W varietà affini, allora $V \cap W$ e $V \cup W$ sono varietà affini.

Teorema 7 (Teorema di Estensione). *Sia $\mathbb{K}$ un campo algebricamente chiuso.*
Sia $I = (f_1, \cdots, f_k)$ un ideale di $\mathbb{K}[x_1, \cdots, x_n]$.
Siano $g_i(x_2, \cdots, x_n) = lt(f_i)$ con $f_i \in \mathbb{K}[x_2, \cdots, x_n][x_1]$. Allora:

$$\forall a = (a_2, \cdots, a_n) \in (\mathbb{V}(I_1) \ \mathbb{V}(g_1, \cdots, g_k)) \ \exists b \in \mathbb{K} \ t.c. \ (b, a_2, \cdots, a_n) \in \mathbb{V}(I) \tag{3.15}$$

3.6 Teorema degli 0 di Hilbert

Teorema 8 (Forma debole). *Sia $\mathbb{K}$ un campo algebricamente chiuso, sia $A = \mathbb{K}[x_1, x_2, \cdots, x_]$ e sia I un ideale di A, allora:*

$$\mathbb{V}(I) = \emptyset \iff I = A \tag{3.16}$$

Teorema 9 (Forma forte). *Sia $\mathbb{K}$ un campo algebricamente chiuso, sia $A = \mathbb{K}[x_1, x_2, \cdots, x_]$ e sia I un ideale di A, allora:*

$$\sqrt{I} = \mathbb{I}(\mathbb{V}(I)) \tag{3.17}$$

Corollario 8: Sia $\mathbb{K}$ un campo algebricamente chiusto e siano $f_1, \cdots, f_k \in \mathbb{K}[x_1, \cdots, x_n]$. Allora il sistema polinomiale:

$$\begin{cases} f_1 = 0 \\ \cdots \\ f_k = 0 \end{cases} \tag{3.18}$$

ha soluzioni $\iff 1 \notin (f_1, \cdots, f_k)$

Corollario 9: $f \in \sqrt{I} \iff (1 - tf, I)\mathbb{K}[t, x] = (1)$

Lemma 7. *Sia $a = (a_1, \cdots, a_n) \in \mathbb{K}^n$. Allora $\mathbb{M} = (x_1 - a_1, \cdots, x_n - a_n)$ è un ideale massimale.*

Proposizione 3.6.1. *Sia $\mathbb{K}$ un campo algebricamente chiuso. Allora $\mathbb{M}$ è un ideale massimale $\iff$ esiste $a \in \mathbb{K}^n$ tale che $\mathbb{M} = (x_1 - a_1, \cdots, x_n - a_n)$*

3.7 Corrispondenza ideali varietà affini

Definizione 3.7.1. Sia S un sottoinsieme di $\mathbb{K}^n$ $\overline{S} = \mathbb{V}(\mathbb{I}(S))$ è la chiusura di Zariski di S

Lemma 8. *La chiusura di Zariski è la più piccola varietà affine che contiene S.*

Proposizione 3.7.1. *Sia I un ideale, sia $V = \mathbb{V}(I)$ e sia:*

$$\pi_k : \mathbb{K}^n \to \mathbb{K}^{n-k} \quad (a_1, \cdots, a_n) \to (a_{n-k+1}, \cdots, a_n) \tag{3.19}$$

Allora $\overline{\pi_k(V)} = \mathbb{V}(I_k)$

Lemma 9. *Siano V, W varietà affini e sia $V \subseteq W$. Allora:*

$$W = V \cup (\overline{W \backslash V}) \tag{3.20}$$

Proposizione 3.7.2. *Ogni catena discendente di varietà affini è stazionaria.*

Definizione 3.7.2. Una varietà V si dice **irriducibile** se, date V_1, V_2 varietà:

$$V = V_1 \cup V_2 \implies (V_1 = V) \vee (V_2 = V) \tag{3.21}$$

Proposizione 3.7.3. *Una varietà V è irriducibile $\iff$ $\mathbb{I}(V)$ è un ideale primo.*

Teorema 10. *Sia V una varietà affine.*
Allora esistono $V_1, \cdots, V_n$ varietà irriducibili tali che $V = \bigcup_{i=1}^n V_i$

Proposizione 3.7.4. *Sia V una varietà affine e sia $V = \bigcup_{i=1}^n V_i$ una sua decomposizione in varietà irriducibili.*
Se $\forall i = 1, \cdots, n$ $\forall j \neq i$ $V_i \not\subseteq V_j$ allora la decomposizione è unica.

3.8 Ideali 0 dimensionali e basi di Grobner

Definizione 3.8.1. Una mappa $\phi : \mathbb{K}^n \to \mathbb{K}^m$ si dice **polinomiale*** se esistono $f_1, \cdots, f_m \in \mathbb{K}[x]$ tali che $\phi(a) = (f_1(a), \cdots, f_m(a))$

> **Osservazione 3.8.1:** Siano $\phi, \psi : \mathbb{K}^n \to \mathbb{K}^m$ mappe polinomiali tali che $\forall a \in V \ \phi(a) = \psi(a)$. Allora:
> $(\phi - \psi)(a) = 0$ e dunque $\phi - \psi \in \mathbb{I}(V)$

Definizione 3.8.2. L'anello $\mathbb{K}[V] := \frac{\mathbb{K}[x]}{\mathbb{I}(V)}$ è detto **anello delle coordinate di V**

Ricerchiamo dei rappresentanti privilegiati per le classi di resto:

Proposizione 3.8.1. *Sia $\mathbb{K}[x_1, \cdots, x_n]$, sia $\leq$ un ordinamento monomiale su A e sia I un ideale di A. Allora:*

1. *$\forall f \in A$ esiste un unico $\overline{f}$ tale che $f \simeq \overline{f}(\mod I)$ e $\overline{f} = \sum c_\beta x^\beta$, dove $x^\beta \notin lt(I)$*
2. *$\{x^\alpha \mid x^\alpha \notin lt(I)\}$ è una base di $\frac{A}{I}$ come $\mathbb{K}$-spazio vettoriale.*

Teorema 11. *Sia $\mathbb{K}$ un campo algebricamente chiuso, sia $A = \mathbb{K}[x_1, \cdots, x_n]$, sia $\leq$ un ordinamento monomiale su A e sia I un ideale di A. Sono equivalenti:*

1. $\#\mathbb{V}(I) < \infty$
2. *$\forall i = 1, \cdots, n \ \exists m_i \in \mathbb{N}$ t.c. $x_i^{m_i} \in lt(I)$*
3. *Data $(G, \leq)$ una base di Grobner di I $\forall i \ \exists h \in \mathbb{N}$; $\exists g_k \in G$ t.c. $lt(g_k) \mid x_i^h$*
4. $\dim_{\mathbb{K}} \frac{A}{I} < \infty$

Proposizione 3.8.2. *Sia mathbbK un campo algebricamente chiuso, sia I un ideale radicale di $\mathbb{K}[x_1, \cdots, x_n]$.*
Supponiamo che $\#\mathbb{V}(I) = s$. Allora:

$$dim \frac{\mathbb{K}[x]}{I} = s \tag{3.22}$$

Lemma 10. *Sia $I = (f, g)$ un ideale di $\mathbb{C}[x, y]$. Allora:*

$$Ris(f, g) \neq 0 \implies \#\mathbb{V}(f, g) < \infty \tag{3.23}$$

Capitolo 4

Moduli: Proprieta' di base e forme normali

4.1 Moduli su di un anello commutativo unitario

Definizione 4.1.1. Sia A un anello. M si dice un **A-modulo** se $(M, +)$ è un gruppo abeliano munito di una funzione:

$$f : A \times M \to M \ ; \ (a, m) \to am \tag{4.1}$$

Che rispetta le seguenti proprietà:
$(a + b)m = am + bn$
$a(m + n) = am + an$
$abm = a(bm)$
$1_A m = m$

> **Osservazione 4.1.1:** Se A è un campo, gli A-moduli sono tutti A-spazi vettoriali.
> I moduli sono una generalizzazione degli spazi vettoriali.

4.2 Sottomoduli e quozienti

Definizione 4.2.1. $N \subseteq M$ è un **sottomodulo** se è un sottogruppo additivo di M chiuso rispetto alle operazioni.
Equivalente: $\forall a \in A \ \forall n \in N \ an \in N$

> **Osservazione 4.2.1:** I sottomoduli di A come A-modulo sono tutti e soli gli ideali di A.
> Preso I ideale di A, l'insieme $IM = \{\sum a_i m_i | a_i \in I \ m_i \in M\}$ è un sottomodulo di M.

Definizione 4.2.2. L'**ideale quoziente** si definisce come:

$$(M : N) := \{a \in A \mid aN \subseteq M\} \tag{4.2}$$

Osservazione 4.2.2: L'ideale quoziente è un ideale di A.
Per $M = 0$ definiamo l'**annullatore** di N come $Ann(N) = (0 : N)$

4.3 Omomorfismi di moduli

Definizione 4.3.1. Siano M, N degli A-moduli, $f : M \to N$ è un **omomorfismo di A-moduli** se:

$$\begin{aligned} f(m+n) &= f(m) + f(n) \\ f(am) &= af(m) \end{aligned} \tag{4.3}$$

Osservazione 4.3.1: Dato un omomorfismo, sono sottomoduli:
$\ker f = \{m \in M | f(m) = 0\}$
$Imf = \{n \in N | \exists m \in M \ t.c. \ f(m) = n\}$

Proposizione 4.3.1. *Sia M un A-modulo. Allora* $\hom_A(A, M) \simeq M$

4.4 Somma diretta e prodotto di moduli

Definizione 4.4.1. Data una famiglia di moduli $\{M_i \mid i \in I\}$ il **modulo somma** è dato da:

$$\sum_{i \in I} M_i := \Big\{ \sum_i m_i \mid m_i \neq 0 \ per \ un \ numero \ finito \ di \ indici \ e \ m_i \in M_i \Big\} \tag{4.4}$$

Definizione 4.4.2. Data una famiglia di moduli $\{M_i \mid i \in I\}$ il **modulo somma diretta** è dato da:

$$\bigoplus_{i \in I} M_i := \big\{(m_i)_{i \in I} \mid m_i \neq 0 \ per \ un \ numero \ finito \ di \ indici \ e \ m_i \in M_i\big\} \tag{4.5}$$

Definizione 4.4.3. Data una famiglia di moduli $\{M_i \mid i \in I\}$ il **modulo prodotto diretto** è dato da:

$$\prod_{i \in I} M_i := \big\{(m_i)_{i \in I} \mid m_i \in M_i\big\} \tag{4.6}$$

Proposizione 4.4.1. *Sia M_i una famiglia di A-moduli ed N un A-modulo. Supponiamo che esista $\forall i$ un omomorfismo $\phi_i : M_i \to N$.*

Detto $M = \bigotimes M_i$ si ha allora che esiste un omomorfismo $\phi : M \to N$ che fa commutare i diagrammi (j è l'inclusione canonica):

$$\begin{array}{ccc} M_i & \xrightarrow{j} & M \\ \phi_i \downarrow & \swarrow \phi & \\ N & & \end{array}$$

Proposizione 4.4.2. *Sia M_i una famiglia di A-moduli ed N un A-modulo. Supponiamo che esista $\forall i$ un omomorfismo $\phi_i : N \to M_i$.*
Detto $M = \prod M_i$ si ha allora che esiste un omomorfismo $\phi : N \to M$ che fa commutare i diagrammi:

$$\begin{array}{ccc} M & \xrightarrow{\pi_i} & M_i \\ \phi \uparrow & \nearrow \phi_i & \\ N & & \end{array}$$

> **Osservazione 4.4.1:** Dato M un A-modulo e I un ideale non possiamo sempre mure M della struttura di $\frac{A}{I}$-modulo.
> Se $I \subseteq Ann(M)$ questo è possibile in quanto $(a + I)m = am$ è ben definita e non dipende dal rappresentate.

4.5 Moduli liberi e rango

Definizione 4.5.1. Un insieme $S = \{s_1, \cdots, s_k\}$ si dice **libero** se:

$$\sum_{i=1}^{k} a_i s_i = 0 \implies a_i = 0 \ \forall i = 1, \cdots, k \tag{4.7}$$

Definizione 4.5.2. Un insieme di generatori libero si dice una **base**

Teorema 12. *Sia M un A-modulo libero. Allora tutte le basi hanno la stessa cardinalità **(rango)***

4.6 Moduli finitamente generati

Definizione 4.6.1. Sia $S \subseteq M$, il **sottomodulo generato da S** è definito come:

$$\langle S \rangle = \{\sum a_i s_i | a_i \in A \ s_i \in S\} \tag{4.8}$$

Se $\#S = 1$ e $\langle S \rangle = M$ allora M si dice **ciclico**.
Se $\#S < \infty$ e $\langle S \rangle = M$ allora M si dice **finitamente generato**.

4.7 Teorema di Hamilton - Cayley

Teorema 13 (Hamilton - Cayley). *Sia M un A-modulo finitamente generato e sia I un ideale di A.*
Sia ϕ un endomorfismo di M tale che $\phi(M) \subseteq IM$
Allora esistono $a_0, \cdots, a_{n-1} \in I$ tali che:

$$\phi^n + \sum_{i=0}^{n-1} a_i \phi^i \equiv 0 \tag{4.9}$$

4.8 Lemma di Nakayama

Lemma 11 (Lemma di Nakayama - I forma). *Sia M un A-modulo finitamente generato e sia I un ideale tale che $M = IM$.*
Allora esiste un elemento $a \in A$ tale che $a \equiv 1(I)$ e $aM = 0$

Lemma 12 (Lemma di Nakayama - II forma). *Sia M un A-modulo finitamente generato e sia $I \subseteq Jacobson(A)$ un ideale di A tale che $IM = M$.*
Allora $M = 0$.

Lemma 13 (Lemma di Nakayama - III forma). *Sia M un modulo finitamente generato, sia N un suo sottomodulo e sia $I \subseteq Jacobson(A)$ un ideale di A.*
Se $M = N + IM \implies M = N$

Alcune conseguenze del Lemma di Nakayama sono le seguenti:

Lemma 14. *Sia $(A, \mathbb{M})$ un anello locale e sia M un A-modulo finitamente generato. Sia $\overline{m_1}, \cdots, \overline{m_k}$ una base di $\frac{M}{\mathbb{M}M}$.*
Allora, comunque presi $m_1, \cdots, m_k \in M$ tali che $\pi(m_i) = \overline{m_i}$ si ha che $M = \langle m_1, \cdots, m_k \rangle$

Proposizione 4.8.1. *Sia $(A, \mathbb{M})$ un anello locale e sia M un A-modulo finitamente generato.*
Allora ogni insieme di generatori minimale ha la stessa cardinalità.

Proposizione 4.8.2. *Sia M un A-modulo finitamente generato e sia f un endomorfismo surgettivo. Allora f è un isomorfismo.*

> **Osservazione 4.8.1:** In uno spazio vettoriale ogni endomorfismo surgettivo o iniettivo è un isomorfismo, fra i moduli non è detto.

4.9 Moduli su PID e loro struttura

Diversamente dagli spazi vettoriali i sottomoduli di un modulo libero non sono necessariariamente liberi.

Teorema 14. *Sia A un PID, sia M un A-modulo libero finitamente generato e sia N un suo sottomodulo non banale.*
Allora N è libero.

Osservazione 4.9.1: $Rank(N) \leq Rank(M)$

Corollario 10: Sia A un PID:
P proiettivo $\iff$ P libero

Corollario 11: Sia A un PID:
N sottomodulo di M, M finitamente generato $\implies$ N finitamente generato

4.10 Forma normale di Smith e di Hermite

Sia M un A-modulo finitamente generato con A PID. M è allora quoziente di un modulo libero finitamente generato:

$$0 \to \ker f \to^i A^n \to^f M \tag{4.10}$$

$\ker f$ è libero, sia allora $v_1, \cdots, v_m$ una base di $\ker f$
Considerata l'applicazione:

$$\psi : A^m \to A^n \quad e_i \to v_i \tag{4.11}$$

Si ha che $\ker f = Im(f)$ e dunque $M \simeq Coker(\psi)$

Per classificare i moduli finitamente generati su di un PID basta studiare le applicazioni tra moduli liberi e i loro Coker.

Fissate due base B_1, B_2 di $A^m; A^n$ si ha che un qualsiasi omomorfismo fra questi può essere rappresentato da una matrice:

$$M_{ij} = ([f(b_i)^{(m)}]_{B^n}) \tag{4.12}$$

Definizione 4.10.1. Siano $X, Y \in M(n, m, A)$. X e Y si dicono **equivalenti** se esistono due matrici $S \in GL(n, A)$ e $T \in GL(m, A)$ tali che $X = SYT$

Proposizione 4.10.1. *Sia $X \in M(n,m,A)$ con A un PID. Allora X è equivalente ad una matrice D in forma diagonale.*

Definizione 4.10.2. Una matrice diagonale D si dice in **forma di Smith** se $d_{11} \mid d_{22} \mid \cdots \mid d_{nn}$

Proposizione 4.10.2. *Sia D una matrice in forma diagonale. Allora D è equivalente ad una matrice $\overline{D}$ in forma di Smith.*

Corollario 12: La forma di Smith è unica a meno di associati.

Non abbiamo ancora dimostrato che questa forma è indipendente dalla scelta dell'omomorfismo di A-moduli scelto.

Lemma 15. *Supponiamo che M si scriva come somma diretta*

$$M = \frac{A}{J_1} \oplus \frac{A}{J_2} \tag{4.13}$$

dove J_1 ; J_2 sono ideali di A. Sia I un ideale di A. Allora:

$$\frac{M}{IM} \simeq \frac{A}{J_1 + I} \oplus \frac{A}{J_2 + I} \tag{4.14}$$

Lemma 16. *Sia $M = \frac{A}{J}$ e sia $a \in A$. Allora $aM \simeq \frac{A}{(J:a)}$*

Lemma 17. *Sia B un anello e sia $f : B^n \to B^m$ un omomorfismo surgettivo con $m > n \implies B = (0)$*

Teorema 15. *Sia A un anello. Supponiamo che esistano due catene di ideali*

$$\begin{array}{c} I_n \subseteq \cdots \subseteq I_2 \subseteq I_1 \\ J_m \subseteq \cdots \subseteq J_2 \subseteq J_1 \end{array} \tag{4.15}$$

con $m > n$ e supponiamo che

$$M \simeq \bigoplus_{k=1}^{n} \frac{A}{I_k} \simeq \bigoplus_{k=1}^{m} \frac{A}{J_k} \tag{4.16}$$

Allora $J_1 = J_2 = \cdots = J_{m-n} = A$ e $\forall i = 1, \cdots, n$ $J_{m-n+i} = I_i$

Capitolo 5

Moduli: Successioni, moduli proiettivi e prodotto tensoriale

5.1 Successioni esatte

Definizione 5.1.1. Sia $\{M_i\}$ una famiglia di A- moduli.
Supponiamo che $\forall i \in I$ sia definito un omomorfismo di A-moduli
$\phi_i : M_{i-1} \to M_i$
La successione:
$\cdots \to M_{i-1} \to^{\phi_i} M_i \to^{\phi_{i+1}} M_{i+1} \to \cdots$
Si dice **esatta in** M_i se $Im(\phi_i) = Ker(\phi_{i+1})$.
Si dice **esatta** se è esatta in ogni M_i.

Proposizione 5.1.1. $0 \to M \to^f N$ *è esatta* $\iff$ f *è iniettiva*

Proposizione 5.1.2. $M \to^f N \to 0$ *è esatta* $\iff$ f *è surgettiva*

5.2 Funtori Hom(-,N) e Hom(M,-)

Dato $f \in Hom(M,N)$ e $h \in Hom(N,P)$ possiamo definire per composizione:

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, dashed, "f^*(h)"'] & N \arrow[dl, "h"] \\ P & \end{tikzcd}$$

La funzione $f^*(h)$

Risulta definito il seguente omomorfismo:

$$f^* : Hom(N,P) \to Hom(M,P) \quad h \to f_*(h) = h \circ f \tag{5.1}$$

Dato $f \in Hom(M, N)$ e $h \in Hom(N, P)$ possiamo definire per composizione:

$$\begin{tikzcd} M \arrow[r, "f"] & N \\ P \arrow[u, "h"] \arrow[ur, dashed, "f_*(h)"'] & \end{tikzcd}$$

La funzione $f^*(h)$

Risulta definito il seguente omomorfismo:

$$f_* : Hom(P, M) \to Hom(P, N) \quad h \to f_*(h) = f \circ h \tag{5.2}$$

Proposizione 5.2.1. *La successione:*

$$M_1 \to^f M \to^g M_2 \to 0 \tag{5.3}$$

è esatta $\iff$ *la successione:*

$$0 \to Hom(M_2, N) \to^{g^*} Hom(M, N) \to^{f^*} Hom(M_1, N) \tag{5.4}$$

è esatta per ogni A-modulo N

5.3 Successioni che spezzano

Definizione 5.3.1. Si dice che una successione esatta:
$0 \to M \to^\alpha N \to^\beta P \to 0$ **spezza** se esiste $f : M \oplus P \to N$ isomorfismo che fa commutare il seguente diagramma:

$$\begin{tikzcd} & & M \oplus P \arrow[d, "f"'] \arrow[drr, "\pi_P"] & & & \\ 0 \arrow[r] & M \arrow[ur, "i_M"] \arrow[r, "\alpha"'] & N \arrow[rr, "\beta"'] & & P \arrow[r] & 0 \end{tikzcd}$$

Proposizione 5.3.1. *Consideriamo una successione esatta:*

$$0 \to M \to^\alpha N \to^\beta P \to 0 \tag{5.5}$$

Sono equivalenti:

1. *La successione spezza*

2. *Esiste un omomorfismo $r : N \to M$ tale che $r \circ \alpha = Id_M$*

3. *Esiste un omomorfismo $s : P \to N$ tale che $\beta \circ s = Id_P$*

Teorema 16 (Lemma del serpente)**.** *Consideriamo due successioni esatte e degli omomorfismi $\alpha; \beta; \gamma$ che fanno coomutare il seguente diagramma:*

$$\begin{tikzcd}
 & M \arrow[r, "f"] \arrow[d, "\alpha"'] & N \arrow[r, "g"] \arrow[d, "\beta"'] & P \arrow[r] \arrow[d, "\gamma"'] & 0 \\
0 \arrow[r] & M' \arrow[r, "f'"'] & N' \arrow[r, "g'"'] & P' &
\end{tikzcd}$$

Esiste allora una successione esatta come indicata dalla linea tratteggiata:

$$\begin{tikzcd}
 & Ker(\alpha) \arrow[r, "\overline{f}"] \arrow[d] & Ker(\beta) \arrow[r, "\overline{g}"] \arrow[d] & Ker(\gamma) \arrow[d] \arrow[dddll, dashed] & \\
 & M \arrow[r, "f"] \arrow[d] & N \arrow[r, "g"] \arrow[d] & P \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M' \arrow[r, "f'"'] \arrow[d] & N' \arrow[r, "g'"'] \arrow[d] & P' \arrow[d] & \\
 & Coker(\alpha) \arrow[r, "\overline{f'}"'] & Coker(\beta) \arrow[r, "\overline{g'}"'] & Coker(\gamma) &
\end{tikzcd}$$

Osservazione 5.3.1: Se f è iniettiva allora anche $\overline{f}$ è iniettiva.
Se g' è surgettiva allora anche $\overline{g'}$

Corollario 13 (Lemma dei Cinque)**:** Consideriamo il diagramma:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "\alpha"'] & N \arrow[r, "g"] \arrow[d, dashed, "\beta"'] & P \arrow[r] \arrow[d, "\gamma"'] & 0 \\
0 \arrow[r] & M' \arrow[r, "f'"'] & N' \arrow[r, "g'"'] & P' \arrow[r] & 0
\end{tikzcd}$$

Se due dei tre omomorfismi $\alpha; \beta; \gamma$ sono isomorfismi, allora lo è anche il terzo.

5.4 Moduli proiettivi

Definizione 5.4.1. Un A-modulo si dice **proiettivo** se per ogni $f : P \to N$ e $h : M \to N$ surgettiva esiste $\overline{f}$ che fa commutare il seguente diagramma:

$$\begin{tikzcd} M \arrow[d, "h"'] & P \arrow[l, "\overline{f}"'] \arrow[dl, "f"] \\ N & \end{tikzcd}$$

Lemma 18. *Sia P un modulo libero.*
Allora P è proiettivo.

Proposizione 5.4.1. *Sono fati equivalenti:*

1. *P proiettivo*
2. *Ogni successione esatta $0 \to M \to N \to P \to 0$ spezza*
3. *P è addendo diretto di un modulo libero*
4. *Il funtore $F : M \to Hom_A(P, M)$ è esatto, cioè manda successioni esatte corte in successioni esatte corte.*

Proposizione 5.4.2. *Sia $M = \oplus_{i \in I} M_i$.*
Allora M è proiettivo $\iff$ M_i è proiettivo $\forall i$

Proposizione 5.4.3. *P è proiettivo $\iff$ P è addendo diretto di ogni modulo di cui è quoziente.*

5.5 Prodotto tensoriale

Definizione 5.5.1. Siano M, N, P A-moduli, $f : M \times N \to P$ si dice **bilineare** se:
$f(m_1 + m_2, n_1 + n_2) = f(m_1, n_1) + f(m_1, n_2) + f(m_2, n_1) + f(m_2, n_2)$
$f(am, bn) = abf(m, n)$

Dato $M \times N$ consideriamo il modulo libero generato dagli elementi di $M \times N$, $A^{M \times N} = C$
Sia D il sottomodulo di C generato dagli elementi della forma:
$(m_1 + m_2, n) - (m_1, n) - (m_2, n)$
$(m, n_1 + n_2) - (m, n_1) - (m, n_2)$
$a(m - n) - (am, n)$
$a(m, n) - (m, an)$

Definizione 5.5.2. Definiamo il **prodotto tensore** tra M e N come $M \otimes N = \frac{C}{D}$

Osservazione 5.5.1: Poiché C è generato dalle coppie $(m, n) \in M \otimes N$, si ha che $\overline{(m, n)} = m \otimes n$ è un insieme di generatori per $M \otimes_A N$

Lemma 19. *1.* $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$

2. $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$

3. $a(m \otimes n) = am \otimes n = m \otimes (an)$

Corollario 14: $g : M \times N \to M \otimes_A N$ con $(m, n) \to m \otimes n$ è una mappa bilineare.

Caratterizziamo ora il prodotto tensoriale in termini categoriali, fissiamo M, N due A-moduli. Consideriamo la categoria C nella quale gli oggeti sono i prodotti bilineari $f : M \times N \to P$ dove P è un qualsiasi A-modulo e le quale i morfismi sono le mappe che fanno commutare il seguente diagramma:

$$\begin{tikzcd} M \times N \arrow[r, "g"] \arrow[d, "f"'] & P_1 \arrow[dl, "\overline{g}"] \\ P_2 & \end{tikzcd}$$

Si ha che in questa categoria il prodotto tensore è un oggetto universale.

Proposizione 5.5.1. *Siano M, N, P A-moduli e sia $f : M \times N \to P$ una mappa bilineare. Allora:*
$\exists! \overline{f} : M \otimes_A N \to P$ omomorfismo di A-moduli che fa commutare il diagramma:

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "g"'] & P \\ M \otimes_A N \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

Proposizione 5.5.2. *$M \otimes_A N$ è l'unico A-modulo che soddisfa la proprietà universale della proposizione precedente.*

Corollario 15: Siano $u : M \to M'$; $v : N \to N'$ omomorfismi di A-moduli. Allora:
$\exists! \phi : M \otimes_A N \to M' \otimes_A N'$ con $m \otimes n \to u(m) \otimes v(n)$

Proposizione 5.5.3. *Siano M, N, P A-moduli:*

1. $A \otimes_A M \simeq M$

2. $M \otimes_A N \simeq N \otimes_A M$

3. $(M \otimes_A N) \otimes_A P \simeq M \otimes_A (N \otimes_A P)$

4. $(M \oplus_A N) \otimes_A P \simeq (M \otimes_A P) \oplus (N \otimes_A P)$

Caratterizziamo a meno di isomorfismo i prodotti tensoriali più semplici:

Corollario 16: $A^n \otimes_A A^m \simeq A^{mn}$

Proposizione 5.5.4. *Sia A un anello e siano I, J ideali di A. Allora:*

$$\frac{A}{I} \otimes_A \frac{A}{J} \simeq \frac{A}{I+J} \tag{5.6}$$

Determiniamo come si comporta il prodotto tensore con le successioni esatte:

Teorema 17. *Siano M, N, P A-moduli:*

$$Bil(M \times N, P) \simeq Hom_A(M \otimes_A N, P) \simeq Hom_A(M, Hom_A(N, P)) \tag{5.7}$$

Corollario 17: $M' \to^f M \to^g M'' \to 0$ è esatta
$\forall N$ A-modulo $M' \otimes N \to^{f \otimes id} M \otimes N \to^{g \otimes id} M'' \otimes N \to 0$ è esatta.

Lemma 20. *Sia A un anello, I un ideale di A e M un A-modulo. Allora: $\frac{A}{I} \otimes_A M$ si può munire della struttura di $\frac{A}{P}I$-modulo.*

Proposizione 5.5.5. *Sia M un A-modulo, P un B-modulo e N un A e B modulo. Allora:*

$$(M \otimes_A N) \otimes_B P \simeq M \otimes_A (N \otimes_B P) \tag{5.8}$$

Lemma 21. *Sia A un anello, I un ideale di A e sia M un A-modulo. Allora:*

$$\frac{A}{I} \otimes_A M \simeq \frac{M}{IM} \tag{5.9}$$

Proposizione 5.5.6. *Sia A un anello locale, siano M, N A-moduli finitamente generati. Allora:*

$$M \otimes_A N = 0 \implies (M = 0) \vee (N = 0) \tag{5.10}$$

5.6 Moduli piatti

Sono l'equivalente dei moduli proiettivi per i prodotti tensori.

Definizione 5.6.1. Un A-modulo si dice piatto se per ogni successione esatta corta vale:

$$0 \to M' \to^{f} M \to^{g} M'' \to 0 \ \ esatta \tag{5.11}$$

$$0 \to N \otimes_A M' \to^{id \otimes f} N \otimes_A M \to^{id \otimes g} N \to_A M'' \to 0 \ \ esatta \tag{5.12}$$

Lemma 22. *N_1, N_2 A-moduli. Allora:*
$N_1 \oplus N_2$ è piatto $\iff$ N_1, N_2 sono piatti.

Proposizione 5.6.1. *Sia M un A-modulo libero.*
Allora M è piatto.

Proposizione 5.6.2. *Sia M un A-modulo proiettivo.*
Allora M è piatto.

Capitolo 6

Moduli: Anelli locali e di frazioni

6.1 Anelli locali e semilocali

Definizione 6.1.1. Un anello di A si dice **locale** se $\exists!$ ideale massimale in A.
Un anello si dice invece semilocale se ne ha un numero finito.

> **Esempio:** $\mathbb{Z}_8$ è un anello locale con ideale massimale (2)
> $\frac{\mathbb{Z}[x,y]}{(x^2,y^2)}$ è un anello locale con unico anello massimale (x, y)

Proposizione 6.1.1. *In un anello locale, se a non appartiene ad m* $\implies a \in A^*$

Proposizione 6.1.2. *A anello, M ideale,* $\forall a \notin M$ *se* $a \in A^* \implies A$ *è un anello locale ed M è il suo unico ideale massimale.*

Proposizione 6.1.3. *A anello, M ideale massimale ed ogni elemento* $1+m$ *invertibile* $(m \in M) \implies$ *A locale ed M il suo unico ideale massimale.*

6.2 Anello delle frazioni

Definizione 6.2.1. Sia A un anello. Un sottoinsieme $S \subseteq A$ si dice **moltiplicativamente chiuso** se:

1. $\in S$
2. $s, t \in S \implies st \in S$

Definizione 6.2.2. Dato un sottoinsieme moltiplicativamente chiuso di A, possiamo definire l'**anello delle frazioni** $A \times S$ con la relazione:

$$(a, s) \sim (b, t) \iff \exists u \in S \text{ t.c. } u(at - bs)00 \tag{6.1}$$

Come $S^{-1}A := \frac{A \times S}{\sim}$ con le operazioni definite come:
$\frac{a}{s} + \frac{b}{t} = \frac{at+sb}{st}$
$\frac{a}{s} + \frac{b}{t} = \frac{ab}{st}$

Lemma 23. $\sim$ *è una relazione di equivalenza.*

Proposizione 6.2.1. $S^{-1}A$ *è un anello con le operazioni sopra introdotte.*

Lemma 24. $S^{-1}A = 0 \iff 0 \in S$

Osservazione 6.2.1: Esiste un omomorfismo canonico $f : A \to S^{-1}A$ con $a \to \frac{a}{1}$

Lemma 25. f *è iniettiva* $\iff S \cap D(A) = \emptyset$

Caratterizzazione mediante proprietà universale dell'anello delle frazioni:
Fissato un anello A e un suo sottoinsieme moltiplicativamente chiuso S definiamo C come la categoria in cui gli oggetti sono gli anelli e i morfismo sono gli omomorfismi di anelli $f : A \to B$ tali che $f(S) \subseteq B^*$
$S^{-1}A$ risulta essere universale in tale categoria, ossia:

Proposizione 6.2.2. *Sia S un sottoinsieme moltiplicativamente chiuso di un anello A e sia $f : A \to S^{-1}A$ l'omomorfismo canonico.*
Sia $\phi : A \to B$ un omomorfismo di anelli tale che $\phi(S) \subseteq B^*$
Allora $\exists! h : S^{-1}A \to B$ che fa commutare il seguente diagramma:

$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[d, "f"'] & B \\ S^{-1}A \arrow[ur, "h"'] & \end{tikzcd}$$

Proposizione 6.2.3. *Sia $\phi : A \to B$*

1. $\phi(S) \subseteq B^*$
2. $\phi(a) = 0 \implies \exists s \in S \text{ t.c. } as = 0$
3. $\forall b \in B\ \exists a \in A\ \exists s \in S \text{ t.c. } b = \phi(a)\phi(s)^{-1}$

6.3 Localizzazione di anelli e moduli

Sia $P \in Spec(A)$; $S = \frac{A}{P}$ è allora un sottoinsieme moltiplicativamente chiuso.
Definiamo $A_p := S^{-1}A$

Lemma 26. *A_p è un anello locale, con ideale massimale $M = \{\frac{a}{s} \mid a \in P\}$*

6.4 Ideali degli anelli localizzati

Proposizione 6.4.1.

1. *Ogni ideale di $S^{-1}A$ è l'estensione di un ideale di A*
2. *$\forall I$ ideale di A allora $I^{ec} = \bigcup_{s\in S}(I : s)$*
3. *I è un ideale contratto $\iff \forall s \in S$ $s + I \notin D(\frac{A}{I}$*
4. *$\{P \in Spec(A) \mid P \cap S = \emptyset\}$ è in corrispondenza biunivoca con $Spec(S^{-1}A)$*

6.5 Moduli di frazioni

Possiamo generalizzare questo concetto ai moduli definendo la relazione di equivalenza su $M \times S$

Lemma 27. *Siano M, N degli A-moduli e sia $\phi : M \to N$ un omomorfismo di A-moduli $\implies$ ϕ induce un omomorfismo di $S^{-1}A$ moduli.*
$s^{-1}\phi : S^{-1}M \to S^{-1}N$
$\frac{m}{s} \to \frac{\phi(m)}{s}$

> **Corollario 18:** Siamo M, N, P A-moduli, $\phi : M \to N$ e $\psi : N \to P$ omomorfismi di A-moduli $\implies$ $s^{-1}(\psi \circ \phi) = s^{-1}\psi \circ s^{-1}\phi$

Proposizione 6.5.1. *Sia $M \to^{\phi} N \to^{\psi} P$ una successione esatta di A-moduli e sia S un sottoinsieme moltiplicativamente chiuso. Allora la successione:*
$S^{-1}M \to^{s^1\phi} S^{-1}N \to^{s^{-1}\psi} S^{-1}P$
è esatta.

> **Corollario 19:** M, N A-moduli, $N \subset M$ $\implies$ $S^{-1}N \hookrightarrow S^{-1}M$ in modo canonico.

Proposizione 6.5.2 (Operazioni fra sottomoduli)**.** *M, N, P A-moduli. $M, N \subset P$*

1. *$S^{-1}(M + N) = S^{-1}M + S^{-1}N$*

2. $S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N$
3. $S^{-1}(\frac{P}{M}) = \frac{S^{-1}P}{S^{-1}M}$

Proposizione 6.5.3 (Rapporto fra moduli e prodotto tensore). $S^{-1}M \simeq S^{-1}A \otimes_A M$

6.6 Moduli piatti

Proposizione 6.6.1. *$S^{-1}A$ è un A-modulo piatto.*

Proposizione 6.6.2. *Siano M, N A-moduli, $S \subseteq A$ un sottoinsieme moltiplicativamente chiuso, allora:*
$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \simeq S^1(M \otimes_A N)$

> **Corollario 20:** $M_P \otimes_A N_p \simeq (M \otimes N)_P$

> **Corollario 21:** $S^{-1}(M \oplus N) \simeq S^{-1}M \oplus S^{-1}N$

6.7 Proprietà locali

Le proprietà locali sono fondamentali nella teoria delle localizzazioni.

Definizione 6.7.1. Sia M un A-modulo. Una proprietà P si dice locale se: M soddisfa $\mathbb{P} \iff M_P$ soddisfa $\mathbb{P}$ $\forall P \in Spec(A)$

Proposizione 6.7.1. *Sia M un A-modulo. Sono equivalenti:*

1. $M = 0$
2. $M_P = 0$ $\forall P \in Spec(A)$
3. $M_{\mathbb{M}}$ $\forall \mathbb{M} \in SpecM(A)$

> **Corollario 22:** Sia $\phi : M \to N$ un omomorfismo di A-moduli. Sono equivalenti:

1. ϕ iniettivo
2. $\phi_P : M_P \to N_P$ iniettivo $\forall P \in Spec(A)$
3. $\phi_{\mathbb{M}} : N_{\mathbb{M}}$ iniettivo $\forall \mathbb{M} \in SpecM(A)$

> **Corollario 23:** Sia $\phi : M \to N$ un omomorfismo di A-moduli. Sono equivalenti:

1. ϕ surgettivo

2. ϕ_P :; $M_P \to N_P$ surgettivo $\forall P \in Spec(A)$
3. $\phi_{\mathbb{M}} : M_{\mathbb{M}} \to N_{\mathbb{M}}$ surgettivo $\forall \mathbb{M} \in SpecM(A)$

Corollario 24: Sono fatti equivalenti:

1. M piatto
2. M_P piatto $\forall P \in Spec(A)$
3. $M_{\mathbb{M}}$ piatto $\forall \mathbb{M} \in SpecM(A)$

Lemma 28. *Sia A un anello e sia S un suo sottoinsieme moltiplicativamente chiuso e sia I un ideale di A. Allora:*
$S^{-1}\sqrt{I} = \sqrt{S^{-1}I}$

Proposizione 6.7.2. *Sono fati equivalenti:*

1. *M ridotto*
2. *M_P ridotto $\forall P \in Spec(A)$*
3. *$M_{\mathbb{M}}$ ridotto $\forall \mathbb{M} \in SpecM(A)$*

L'essere un dominio non è una proprietà locale.
L'essere un anello noetheriano non è una proprietà locale.

Capitolo 7

Moduli: Moduli Noetheriani e Artiniani

7.1 Anelli e moduli noetheriani

Definizione 7.1.1. Un A-modulo M si dice **modulo noetheriano** se ogni catena ascendente di sottomoduli è stazionaria.

Proposizione 7.1.1. *Sia* $(\sum, \geq)$ *un insieme parzialmente ordinato.*
Sono equivalenti:

1. *Ogni catena ascendente di* $\sum$ *è stazionaria.*
2. *Ogni sottoinsieme non vuoto di* $\sum$ *ammette un elemento massimale.*

> **Esempio:** $\mathbb{Z}$ è uno $\mathbb{Z}$-modulo noetheriano, $\mathbb{K}[x_1, x_2, \cdots]$ non lo è.

Proposizione 7.1.2. *Sia* M *un* A*-modulo.*
M *è noetheriano* $\iff \forall N \subseteq M$ N *è finitamente generato.*

Proposizione 7.1.3. *Siano* M, N, P *degli* A*-moduli e sia:*
$0 \to N \to^f M \to^g P \to 0$
Una successione esatta. Vale allora:
M *è noetheriano* $\iff$ N, P *sono noetheriani*

> **Corollario 25:** Sia $M = \bigotimes_{i=1}^{n} M_i$; allora:
> M è noetheriano $\iff$ M_i noetheriano $\forall i$

Definizione 7.1.2. Un anello A si dice **anello noetheriano** se è noetheriano come modulo di se stesso.

> **Osservazione 7.1.1:** I sottomoduli di un modulo noetheriano sono gli ideali.

Corollario 26: Sia A un anello noetheriano e sia M un A- modulo. Allora:
M è finitamente generato $\iff$ M è noetheriano

Corollario 27: Sia A un anello noetheriano e sia I un ideale di A. Allora $\frac{A}{I}$ è noetheriano.

Corollario 28: Sia A un anello e sia M un A-modulo noetheriano. Allora $\frac{A}{Ann(M)}$ è noetheriano.

Proposizione 7.1.4. *A anello noetheriano, S sottoinsieme moltiplicativamente chiuso.*
Allora S^-1A è noetheriano.

7.2 Teorema della base di Hilbert

Teorema 18 (Teorema della base di Hilbert)**.** *Sia A un anello noetheriano. Allora $A[x]$ è noetheriano.*

7.3 Ideali irriducibili e primari

Inseriamo gli strumenti di base per determinare una decompoisizione di un ideale in un anello noetheriano come intersezione di ideali primari.

Proposizione 7.3.1. *Sia A un anello noetheriano. Allora:*
I è irriducibile $\iff$ I è primario

Proposizione 7.3.2. *Sia A un anello noetheriano e sia I un ideale di A. Allora:*
$\exists Q_1, \cdots, Q_n$ *irriducibili t.c.* $I = \bigcap_{i=1}^n Q_i$

7.4 Decomposizione di un ideale come intersezione di ideali primari

Definizione 7.4.1. Sia I un ideale di A. Una **decomposizione primaria** di I è una scrittura $I = \bigcap_{i=1}^n Q_i$ dove ogni Q_i è un ideale primario.

Definizione 7.4.2. Una decomposizione primaria si dice **minimale** se $\bigcap_{j\neq i} Q_j \not\subset Q_i$ e se, detti $P_i = \sqrt{Q_i}$ si ha $P_i \neq P_j \ \forall i \neq j$

Lemma 29. *Siano Q_1, Q_2 ideali P-primari e sia $Q = Q_1 \cap Q_2$.*
Allora Q è P-primario.

Lemma 30. *Sia A un anello noetheriano e sia I un ideale di A.*
Allora $\exists m \in \mathbb{N}$ tale che $(\sqrt{I})^m \subseteq I$

Lemma 31. *Sia Q un ideale P-primario e sia $a \in A$.*

1. $a \in Q \implies (Q : a) = A$
2. $a \notin Q \implies (Q : a)$ *è P-primario*
3. $a \notin P \implies (Q : a) = Q$

Teorema 19 (Unicità della decomposizione primaria)**.** *Sia $I = \bigcap Q_i$ una decomposizione primaria minimale di I.*

1. $\{P_i \mid \sqrt{Q_i} = P_i\} = \{\sqrt{(I : a)} \mid \sqrt{(I : a)}\ e'\ primo\}$
2. *Se A è noetheriano* $\{P_i \mid \sqrt{Q_i} = P_i\} = \{(I : a) \mid (I : a)\ e'\ primo\}$

> **Corollario 29:** I primi P_i di una decomposizione minimale sono indipendenti dalla decomposizione scelta.

Definizione 7.4.3. Sia $I = \bigcap Q_i$. Gli ideali P_i si dicono **primi associati** di I.
I P_i si dicono **minimali** se sono minimali tra i primi associati, altrimenti si dicono **immersi**.

Lemma 32. *I primi associati minimali sono minimali nell'insieme dei primi che contengono I.*

Proposizione 7.4.1. *Sia $I = \bigcap Q_i$ una decomposizione primaria minimale. Allora:*
$\bigcup P_i = \{a \in A \mid (I : a) \neq I\}$

Vogliamo caratterizzare gli ideali primari di una decomposizione:

Teorema 20. *Sia $A \subseteq A$ un sottoinsieme moltiplicativamente chiuso e sia A un ideale P-primario.*

1. *Se $S \cap P \neq \emptyset$ allora $S^{-1}Q = S^{-1}A$*
2. *Se $S \cap P = \emptyset$ allora $S^{-1}Q$ è $S^{-1}P$-primario e $(S^{-1}Q)^c = Q$*

Proposizione 7.4.2. *Sia $S \subseteq A$ un sottoinsieme moltiplicativamente chiuso, sia $I = \bigcap_{i=1}^m Q_i \ \bigcap\ \bigcap_{i=m+1}^n Q_i$ una decomposizione primaria minimale. Supponiamo che:*

1. $S \cap P_i = \emptyset\ \forall i = 1, \cdots, m$
2. $S \cap P_i \neq \emptyset\ \forall i = m+1, \cdots, n$

Allora $(S^{-1}I)^C = \bigcap_{i=1}^m Q_i$

7.5 Anelli e moduli artiniani

Definizione 7.5.1. M si dice artiniano se ogni catena discendente di sottomoduli è stazionaria.

> **Osservazione 7.5.1:** Un quoziente e un sottomodulo di un modulo artiniano sono artinani.

Proposizione 7.5.1. *Sia A un anello artiniano.*
Allora ogni primo è massimale.

Proposizione 7.5.2. *Sia A un anello artiniano.*
Allora A ha finiti massimali.

7.6 Dimensione di un anello

Definizione 7.6.1. Sia A un anello:

$$\dim A := \max\{\textit{lunghezze di catene di primi}\} \tag{7.1}$$

Definizione 7.6.2. Sia I un ideale:

$$\dim I := \dim \frac{A}{I} \tag{7.2}$$

> **Osservazione 7.6.1:** Se $\mathbb{K}$ è un campo $\implies \dim \mathbb{K} = 0$.

> **Osservazione 7.6.2:** Se $\mathbb{K}$ è un PID $\implies \dim \mathbb{K} = 1$.

7.7 Caratterizzazione anelli noetheriani e artiniani

Lemma 33. *Sia A un anello artiniano.*
Allora $\exists n \in \mathbb{N}$ tale che $N(A)^n = 0$

Teorema 21. *A è artiniano $\iff$ A è prodotto diretto finito di anelli locali artiniani.*

Lemma 34. *Sia A un anello nel quale esistono $M_1, \cdots, M_n$ ideai massimali tali che $M_1 \cdots M_n = (0)$. Allora:*
A è artiniano $\iff$ A è noetheriano

Teorema 22. *A è artiniano $\iff$ (A è noetheriano) $\wedge$ ($\dim A = 0$)*