Josef Eschgfäller

Geometria algebrica 1

Insiemi algebrici affini

Ferrara ◇ 2012

Josef Eschgfäller
Dipartimento di Matematica
Università di Ferrara

epubli GmbH - Verlagsgruppe Holtzbrinck
www.epubli.de

ISBN 978-3-8442-2802-1

Indice

I. INSIEMI ALGEBRICI AFFINI

1. Il teorema della base di Hilbert

Moduli finitamente generati. Anelli e moduli noetheriani. In un sottomodulo di un modulo noetheriano da ogni insieme generatore si può estrarre un sottoinsieme generatore finito. Coefficiente direttore di un polinomio. Teorema della base di Hilbert: Se A è noetheriano, anche $A[x]$ è noetheriano. Dimostrazione di Heidrun Sarges del teorema della base. Ogni immagine suriettiva di un modulo o di un anello noetheriano è noetheriana. Ogni insieme algebrico è intersezione di un numero finito di ipersuperfici. L'ideale generalizzato $\mathcal{J}(X)$. Esempi di anelli non noetheriani.

Situazione 1.1. Sia A un anello commutativo (cfr. oss. 1.20).

Quando non indicato diversamente, denotiamo con $x, x_1, x_2, \ldots$ indeterminate.

Definizione 1.2. Per un A-modulo M ed un sottoinsieme $E \subset M$ denotiamo con A_E il sottomodulo di M generato da E:

$$A\_E := \{a_1e_1 + \ldots + a_ke_k \mid e_1, \ldots, e_k \in E \text{ ed } a_1, \ldots, a_k \in A\}$$

con la convenzione $A\_\emptyset = 0$. Quando A è sottinteso, scriviamo talvolta anche semplicemente $\_E$.

Per $e_1, \ldots, e_m \in M$ scriviamo spesso $A\_(e_1, \ldots, e_m)$ invece di $A\_\{e_1, \ldots, e_m\}$.

Evidentemente $A\_(e_1, \ldots, e_m) = Ae_1 + \ldots + Ae_m$.

Definizione 1.3. Un A-modulo M si dice *finitamente generato*, se esiste un sottoinsieme *finito* $E \subset M$ tale che $M = A\_E$.

Definizione 1.4. Un A-modulo M si dice *noetheriano*, se ogni sottomodulo di M è finitamente generato.

L'anello A si dice *noetheriano*, se è noetheriano come modulo su se stesso. È chiaro che ciò equivale alla condizione che ogni ideale di A è finitamente generato. Infatti l'unico sottomodulo di A che non sia un ideale è A stesso. Ma $A = A\_1$ è sempre finitamente generato.

Osservazione 1.5. Ogni campo è noetheriano, essendo 0 il suo unico ideale. Ogni anello ad ideali principali è noetheriano, e quindi anche $\mathbb{Z}$ è un anello noetheriano.

Proposizione 1.6. *Per un A-modulo M sono equivalenti:*

(1) M è noetheriano.

(2) Per ogni catena non vuota $\mathcal{C}$ di sottomoduli di M si ha $\bigcup_{N \in \mathcal{C}} N \in \mathcal{C}$.

(3) Ogni insieme non vuoto di sottomoduli di M possiede un elemento massimale.

(4) Per ogni successione infinita ascendente

$$M_0 \subset M_1 \subset M_2 \subset \ldots$$

di sottomoduli di M esiste un $k \in \mathbb{N}$ tale che $M_i = M_k$ per ogni $i \geq k$.

(5) Per ogni successione infinita ascendente

$M_0 \subset M_1 \subset M_2 \subset \dots$

di sottomoduli finitamente generati di M *esiste un* $k \in \mathbb{N}$ *tale che* $M_i = M_k$ *per ogni* $i \geq k$.

Dimostrazione. (1) $\implies$ (2): Consideriamo una catena $\mathcal{C} \neq \emptyset$ di sottomoduli di M. Allora $P := \bigcup_{N \in \mathcal{C}} N$ è un sottomodulo di M. Per ipotesi P è finitamente generato. Perciò esistono $e_1, \dots, e_k \in P$ tali che $P = A_\smile(e_1, \dots, e_k)$. Siccome $\mathcal{C}$ è una catena, possiamo trovare un $N \in \mathcal{C}$ tale che $e_1, \dots, e_k \in N$. Ciò implica $P \subset N$. Siccome ovviamente $N \subset P$, abbiamo $P = N \in \mathcal{C}$.

(2) $\implies$ (3): Ciò segue dal lemma di Zorn.

(3) $\implies$ (4): Chiaro.

(4) $\implies$ (5): Chiaro.

(5) $\implies$ (1): Sia N un sottomodulo di M. Assumiamo, per assurdo, che N non sia finitamente generato. Scegliamo $e_1 \in N$. Per ipotesi $A_\smile(e_1) \neq N$, per cui esiste $e_2 \in N \setminus A_\smile(e_1)$. Ovviamente $A_\smile(e_1) \subsetneqq A_\smile(e_1, e_2)$. Per ipotesi $A_\smile(e_1, e_2) \neq N$, per cui esiste $e_3 \in N \setminus (A_\smile(e_1, e_2))$. Ovviamente $A_\smile(e_1, e_2) \subsetneqq A_\smile(e_1, e_2, e_3)$.

Continuando in questo modo otteniamo una successione infinita ascendente

$A_\smile(e_1) \subsetneqq A_\smile(e_1, e_2) \subsetneqq A_\smile(e_1, e_2, e_3) \subsetneqq \dots$

di sottomoduli finitamente generati di N, in contrasto con l'ipotesi.

Queste caratterizzazioni della noetherianità si usano continuamente!

Proposizione 1.7. *Sia* M *un* A*-modulo noetheriano. Allora per ogni sottoinsieme* $E \subset M$ *con* $E \neq \emptyset$ *esistono* $e_1, \dots, e_m \in E$ *tali che* $A_\smile E = A_\smile(e_1, \dots, e_m)$.

Dimostrazione. Sia, per assurdo, E un sottoinsieme non vuoto di M per il quale l'enunciato non sia vero. Sia $N := A_\smile E$.

Scegliamo $e_1 \in E$ in modo arbitrario e poniamo $E_1 := \{e_1\}$, $N_1 := A_\smile(e_1)$. Per ipotesi $N \neq N_1$, quindi $E \not\subset E_1$, cosicché possiamo scegliere un elemento $e_2 \in E \setminus E_1$; poniamo poi $E_2 := \{e_1, e_2\} = E_1 \cup \{e_2\}$ e $N_2 := A_\smile(e_1, e_2)$. Di nuovo troviamo $e_3 \in E \setminus E_2$ e possiamo porre $E_3 := E_2 \cup \{e_3\}$ e $N_3 := A_\smile(e_1, e_2, e_3)$.

Continuando in questo modo troviamo una successione ascendente infinita $N_1 \subsetneqq N_2 \subsetneqq N_3 \subsetneqq \dots$ di sottomoduli di M, in contrasto con il punto (4) della prop. 1.6.

Lemma 1.8. *Siano* M *un* A*-modulo noetheriano ed* $e_1, e_2, e_3, \dots$ *una successione infinita di elementi di* M. *Allora esistono* $\alpha \in \mathbb{N}$ *e* $c_1, \dots, c_\alpha \in A$ *tali che* $e_{\alpha+1} = c_1 e_1 + \dots + c_\alpha e_\alpha$.

Dimostrazione. È sufficiente considerare la successione di sottomoduli

$A_\smile(e_1) \subset A_\smile(e_1, e_2) \subset A_\smile(e_1, e_2, e_3) \subset \dots$

Definizione 1.9. Per un polinomio $f = a_0 x^n + a_1 x^{n-1} + \dots + a_n \in A[x]$ con $a_0 \neq 0$ poniamo $\operatorname{grado} f := n$ e $f\odot := a_0$.

Per il polinomio 0 poniamo $\operatorname{grado} 0 := -1$ (talvolta $-\infty$) e $0\odot := 0$.

Per ogni $f \in A[x]$ l'elemento $f\odot \in A$ si chiama il *coefficiente direttore* di f.

Per $n \in \mathbb{N}$ denotiamo inoltre con $A[x]_n$ l'insieme dei polinomi di grado n in $A[x]$ insieme al polinomio 0. Quindi $0 \in A[x]_n$ per ogni $n \in \mathbb{N}$.

Teorema 1.10 (teorema della base di Hilbert). *A sia noetheriano. Allora anche $A[x]$ è noetheriano.*

Dimostrazione. La dimostrazione seguente è del 1976 e dovuta a Heidrun Sarges.

Sia I un ideale *non* finitamente generato di $A[x]$. Allora $I \neq 0$ e quindi possiamo trovare un elemento $f_1 \in I \setminus 0$ che scegliamo di grado minimo.

Per ipotesi $A[x]_\smile(f_1) \neq I$, perciò possiamo trovare un elemento $f_2 \in I \setminus (A[x]_\smile(f_1))$ che scegliamo ancora di grado minimo.

Similmente, sfruttando sempre l'ipotesi che I non sia finitamente generato, per ogni $k \in \mathbb{N}+1$ possiamo trovare un polinomio $f_k \in I\setminus(A[x]_\smile(f_1,\ldots,f_{k-1}))$, ogni volta di grado minimo.

Per ogni $k \in \mathbb{N}+1$ siano $n_k := \operatorname{grado} f_k$ ed $a_k := f_k\odot$.

Siccome A è noetheriano, per il lemma 1.8 esiste un $\alpha \in \mathbb{N}$ tale che

$$a_{\alpha+1} = c_1a_1 + \ldots + c_\alpha a_\alpha$$

con $c_1,\ldots,c_\alpha \in A$. Osservando che $n_{k+1} \geq n_k$ per ogni k (perché ogni volta abbiamo scelto polinomi di grado minimo), possiamo formare il polinomio

$$f := f_{\alpha+1} - \sum_{k=1}^{\alpha} c_k f_k x^{n_{\alpha+1}-n_k}$$

Allora $f \in I \setminus (A[x]_\smile(f_1,\ldots,f_\alpha))$ e $\operatorname{grado} f < \operatorname{grado} f_{\alpha+1}$, in contrasto con la minimalità del grado di $f_{\alpha+1}$.

Corollario 1.11. *Sia A noetheriano. Allora $A[x_1,\ldots,x_n]$ è noetheriano.*

Corollario 1.12. *Sia K un campo. Allora $K[x_1,\ldots,x_n]$ è noetheriano.*

Corollario 1.13. *$\mathbb{Z}[x_1,\ldots,x_n]$ è noetheriano.*

Osservazione 1.14. $\varphi : M \longrightarrow N$ sia un omomorfismo suriettivo di A-moduli ed M sia noetheriano. Allora anche N è noetheriano.

Dimostrazione. Sia Q un sottomodulo di N. Allora $\varphi^{-1}(Q)$ è un sottomodulo di M e dalla suriettività di φ segue che $Q = \varphi\varphi^{-1}(Q)$. Per ipotesi esistono $e_1,\ldots,e_k \in M$ tali che $\varphi^{-1}(Q) = A_\smile(e_1,\ldots,e_k)$. È chiaro che allora $Q = A_\smile(\varphi(e_1),\ldots,\varphi(e_k))$.

Osservazione 1.15. $\varphi : A \longrightarrow B$ sia un omomorfismo suriettivo di anelli commutativi ed A sia noetheriano. Allora anche B è un anello noetheriano.

Dimostrazione. Ciò non segue direttamente dall'oss. 1.14, perché φ non è un omomorfismo di moduli, ma di anelli. Possiamo però usare essenzialmente la stessa dimostrazione.

Sia J un ideale di B. Allora $\varphi^{-1}(J)$ è un ideale di A (cfr. lemma 3.18). Per ipotesi esistono $e_1, \ldots, e_k \in A$ tali che $\varphi^{-1}(J) = A_{\smile}(e_1, \ldots, e_k)$. Allora J è generato da $\varphi(e_1), \ldots, \varphi(e_k)$.

Sia infatti $b \in J$. Allora esiste $a \in A$ con $b = \varphi(a)$. Perciò $a \in \varphi^{-1}(J)$, cosicché $a = c_1e_1 + \ldots + c_ke_k$ con $c_1, \ldots, c_k \in A$.

Ciò implica $b = \varphi(a) = \varphi(c_1)\varphi(e_1) + \ldots \varphi(c_k)\varphi(e_k)$.

Osservazione 1.16. Sia I un ideale di A. Se A è noetheriano, allora A/I è un anello noetheriano e anche noetheriano come A-modulo.

Osservazione 1.17. L'anello $A[x]$ sia noetheriano. Allora anche A stesso è noetheriano.

Dimostrazione. Siccome $A \cong A[x]/x$, ciò segue dall'oss. 1.16.

Nota 1.18. Siano K un campo ed $F \subset K[x_1, \ldots, x_n]$ un insieme qualsiasi di polinomi. Sia $I := K[x_1, \ldots, x_n]_{\smile}F$ l'ideale generalizzato generato da F. Per gli insiemi degli zeri vale allora $\mathrm{Zeri}(I) = \mathrm{Zeri}(F)$.

Per il teorema della base di Hilbert $K[x_1, \ldots, x_n]$ è noetheriano, perciò per il lemma 1.8 esistono $f_1, \ldots, f_m \in F$ tali che $I = K[x_1, \ldots, x_n]_{\smile}(f_1, \ldots, f_m)$ ed è chiaro che allora $\mathrm{Zeri}(F) = \mathrm{Zeri}(f_1, \ldots, f_m)$ è intersezione di un numero finito di ipersuperfici.

Definizione 1.19. Siano K un campo ed $F \subset K[x_1, \ldots, x_n]$ un insieme qualsiasi di polinomi. Come nella nota 1.18 usiamo la notazione

$$\mathrm{Zeri}(F) := \{\alpha \in K^n \mid f(\alpha) = 0 \text{ per ogni } f \in F\}$$

Solo raramente (come nel cap. 7) dovremo specificare n, ad esempio quando i polinomi di F sono considerati anche come elementi di $K[x_1, \ldots, x_{n+1}]$.
In tal caso scriviamo $\mathrm{Zeri}(F, \mathrm{in}\, K^n)$ risp. $\mathrm{Zeri}(F, \mathrm{in}\, K^{n+1})$.

Per $X \subset K^n$ sia

$$\mathcal{J}(X) := \{f \in K[x_1, \ldots, x_n] \mid f(\alpha) = 0 \text{ per ogni } \alpha \in X\}$$

È chiaro che $\mathcal{J}(X)$ è un ideale generalizzato di $K[x_1, \ldots, x_n]$.

Anche qui solo raramente dovremo specificare più precisamente
$\mathcal{J}(X, \mathrm{in}\, K[x_1, \ldots, x_n])$ risp. $\mathcal{J}(X, \mathrm{in}\, K[x_1, \ldots, x_{n+1}])$.

Osservazione 1.20. Un anello commutativo A contiene, per definizione, sempre un elemento neutro per la moltiplicazione, denotato con 1_A oppure semplicemente con 1. È ammesso il caso $1 = 0$; in tal caso tutto l'anello è uguale a 0. Un ideale di A è sempre $\neq A$ (cfr. def. 2.2), quindi l'anello 0 non contiene ideali. In un anello integro chiediamo $1 \neq 0$.

Un omomorfismo di anelli $A \longrightarrow B$ manda 1_A in 1_B.

Nelle situazioni all'inizio dei capitoli spesso specificheremo che $A \neq 0$.

Per l'applicazione $x \longmapsto \varphi(x)$ usiamo la notazione $\mathop{\bigcirc}\limits_x \varphi(x)$, introdotta in Eschgfäller [7331], come variante grafica del $\lambda x.\varphi(x)$ del λ-calcolo. La si ottiene in Latex con `\newcommand {\Fun} {\mathop{\bigcirc}\limits}`.

Nota 1.21. Diamo infine alcuni esempi di anelli non noetheriani.

(1) Sia A un anello commutativo $\neq 0$. Allora l'anello $B := A[x_1, x_2, \ldots]$ in un numero *infinito* di indeterminate non è noetheriano, perché esiste la catena infinita strettamente crescente di ideali $(x_1), (x_1, x_2), \ldots$

Se A è integro, però anche B è integro e quindi contenuto in un campo, quindi in un anello noetheriano. Ciò mostra che un sottoanello di un anello noetheriano non è necessario noetheriano.

(2) Sia A un anello commutativo noetheriano $\neq 0$. Allora $A[x, y]$ è noetheriano, ma non lo è il sottoanello $B := A[x, xy, xy^2, xy^3, \ldots]$. Anche qui, se A è integro, lo è anche B e quindi contenuto in un campo.

Cfr. Kemper [21951], p. 24.

(3) L'anello $C(\mathbb{R}, \mathbb{R})$ non è noetheriano. Basta considerare, per ogni $n \in \mathbb{N}$, l'ideale $I_n := \{f \in C(\mathbb{R}, \mathbb{R}) \mid f(x) = 0 \text{ per } x \geq n\}$.

(4) Siano A un anello commutativo $\neq 0$ ed X un insieme infinito. Scegliamo una successione infinita $x_1, x_2, \ldots$ di elementi distinti di X e definiamo $X_n := X \setminus \{x_1, \ldots, x_n\}$. Considerando poi gli ideali $I_n := \{f \in A^X \mid f_{|X_n} = 0\}$, vediamo che A^X non è noetheriano.

2. Operazioni elementari con gli ideali

Un ideale è un ideale generalizzato che non coincide con A. Un ideale generalizzato è un ideale se e solo se non contiene elementi invertibili. Somma $I + J$ e prodotto IJ di ideali. Legge modulare. Legge distributiva $(I + J)K = IK + JK$. $I + J = A$ implica $I^\alpha + J^\beta = A$.

Situazione 2.1. Sia A un anello commutativo.

Definizione 2.2. Un *ideale generalizzato* di A è un A-sottomodulo di A.

Un *ideale* di A è un ideale generalizzato di A che non coincide con A.

Osservazione 2.3. Sia I un ideale generalizzato di A. Allora sono equivalenti:

(1) $1 \in I$.

(2) I contiene un elemento invertibile di A.

(3) $I = A$.

Dimostrazione. (1) $\implies$ (2): Chiaro.

(2) $\implies$ (1): Sia $b \in I$ invertibile. Allora esiste $a \in A$ con $ab = 1$.
Ciò implica $1 \in I$.

(1) $\implies$ (3): Sia $a \in A$. Allora $a = a1 \in I$.

(3) $\implies$ (1): Chiaro.

Definizione 2.4. Siano I e J ideali generalizzati di A. Allora l'insieme

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

è un ideale generalizzato di A e si chiama la *somma* degli ideali generalizzati I e J. È immediato che

$$I + J = A_\smile(I \cup J).$$

Analogamente, per un insieme qualsiasi $\mathcal{I}$ di ideali generalizzati di A la loro somma $\sum\limits_{I\in\mathcal{I}} I := A_\smile \bigcup\limits_{I\in\mathcal{I}} I$ è definita come l'ideale generalizzato generato dalla loro unione.

Osservazione 2.5. L'intersezione di un insieme di ideali generalizzati di A è ancora un ideale generalizzato di A. Esso è un ideale tranne nel caso banale che tutti gli ideali generalizzati utilizzati nell'intersezione sono uguali ad A.

Definizione 2.6. Siano I e J ideali generalizzati di A. Allora l'insieme $IJ := A_\smile\{ab \mid a \in I, b \in J\}$ si chiama il prodotto di I e J.

Siccome per $a \in I$ e $b \in J$ si ha $ab \in I \cap J$, è chiaro che $IJ \subset I \cap J$. Ciò implica che IJ è un ideale se almeno uno dei due fattori è un ideale.

In particolare per ogni $n \in \mathbb{N} + 1$ è definita la potenza I^n e si ha $I^{n+1} \subset I^n$.

Osservazione 2.7. Nella teoria algebrica dei numeri l'operazione più importante per gli ideali è il prodotto IJ; infatti il concetto risale al tentativo

di ottenere, mediante l'introduzione di „numeri ideali“ (cioè proprio i nostri ideali), il teorema di decomposizione unica come prodotto di potenze di primi di ogni elemento negli anelli di numeri algebrici interi.

Nella geometria algebrica è invece più importante l'intersezione $I \cap J$.
Da Keller [1760], 112.

Osservazione 2.8. Siano $a_1, \ldots, a_m, b_1, \ldots, b_n \in A$.

Allora $A_\smile(a_1, \ldots, a_m) + A_\smile(b_1, \ldots, b_n) = A_\smile(a_1, \ldots, a_m, b_1, \ldots, b_n)$.

Osservazione 2.9. Siano I e J ideali generalizzati di A tali che $I + J = A$.

Allora $I \cap J = IJ$.

Dimostrazione. È sufficiente dimostrare che $I \cap J \subset IJ$.

Sia $a \in I \cap J$. Per ipotesi esistono $i \in I$ e $j \in J$ tali che $1 = i + j$. Allora $ai \in JI = IJ$ e $aj \in IJ$, cosicché $a = a(i + j) = ai + aj \in IJ$.

Osservazione 2.10. Siano I, J, K ideali generalizzati di A tali che $I \subset J$.

Allora $J \cap (I + K) = I + (J \cap K)$.

Questa regola si chiama *legge modulare*.

Dimostrazione. (1) Sia $j = i + k$ con $j \in J, i \in I$ e $k \in K$.
Allora $k = j - i \in J + I = J$ perché $I \subset J$.

Però $k \in K$, per cui $j = i + k \in I + (J \cap K)$.

(2) Sia $a = i + b$ con $i \in I$ e $b \in J \cap K$. Allora $a \in I + J \subset J$, ma anche $a \in I + K$.

Osservazione 2.11. Siano I, J, K ideali generalizzati di A.

Allora $(I + J) \cap (I + K) = I + ((I + J) \cap K)$.

Dimostrazione. (1) Sia $a = i + j = i' + k$ con $i, i' \in I$, $j \in J$ e $k \in K$.
Allora $k = i + j - i' \in (I + J) \cap K$, e quindi $a \in I + ((I + J) \cap K$.

(2) Sia $a = i + k$ con $i \in I$, $k \in K$ e $k = i' + j$ con $i' \in I$ e $j \in J$. Raccogliendo $a = (i + i') + j$ vediamo che $a \in I + J$, raccogliendo $a = i + (i' + j)$ vediamo che $a \in I + K$.

Osservazione 2.12. Siano $a_1, \ldots, a_m, b_1, \ldots, b_n \in A$ ed $I := A_\smile(a_1, \ldots, a_m)$, $J := A_\smile(b_1, \ldots, b_n)$.

Allora $IJ = A_\smile(a_1b_1, \ldots, a_1b_n, \ldots, a_mb_1, \ldots, a_mb_n)$.

Dimostrazione. Sia $a \in IJ$. Allora esistono $e_1, \ldots, e_k \in I$, $f_1, \ldots, f_k \in J$ e $c_1, \ldots, c_k \in A$ tali che $a = c_1e_1f_1 + \ldots + c_ke_kf_k$.

Ogni e_i è combinazione lineare di $a_1, \ldots, a_m$, ogni f_j combinazione lineare di $b_1, \ldots, b_n$, per cui evidentemente ogni e_if_j e con essi a stesso è combinazione lineare degli $a_\alpha b_\beta$.

Osservazione 2.13. Siano I, J, K ideali generalizzati di A.

Allora $(I + J)K = IK + JK$.

Dimostrazione. (1) Ogni elemento di $(I + J)K$ è combinazione lineare di elementi della forma $(i + j)k = ik + jk$ con $i \in I, j \in J, k \in K$ e appartiene quindi a $IK + JK$.

(2) È chiaro d'altra parte che $IK \subset (I+J)K$ e similmente $JK \subset (I+J)K$, per cui $IK + JK \subset (I + J)K$.

Osservazione 2.14. Siano I, J, K ideali generalizzati di A. Allora:

(1) $IJ + K \supset (I + K)(J + K)$.

(2) $I^\alpha + J \supset (I + J)^\alpha$ per ogni $\alpha \in \mathbb{N}$.

Dimostrazione. (1) Per l'oss. 2.13 abbiamo

$(I + K)(J + K) = IJ + IK + KJ + K^2 \subset IJ + K$.

(2) Per induzione abbiamo

$$\begin{aligned} I^\alpha + J = I^{\alpha-1}I + J &\supset (I^{\alpha-1} + J)(I + J) \supset (I + J)^{\alpha-1}(I + J) \\ &= (I + J)^\alpha \end{aligned}$$

Lemma 2.15. *Siano I, J ideali generalizzati di A con $I + J = A$.*
Allora $I^\alpha + J^\beta = A$ per ogni $\alpha, \beta \in \mathbb{N}$.

Dimostrazione. Per l'oss. 2.14 abbiamo

$I^\alpha + J^\beta \supset (I + J^\beta)^\alpha \supset ((I + J)^\beta)^\alpha = (A^\beta)^\alpha = A$

Proposizione 2.16. *Siano I, J ideali generalizzati di A con $I + J = A$.*
Sia $a \in A$ tale che $aJ \subset I$. Allora $a \in I$.

Dimostrazione. Per ipotesi esistono $i \in I$ e $j \in J$ tali che $1 = i + j$.
Perciò $a = a(i + j) = ai + aj \in I + I = I$.

3. Ideali primi e radicale

Un ideale P si dice primo, se $ab \in P$ implica $a \in P$ oppure $b \in P$. P è primo se e solo se A/P è integro. Ogni ideale è contenuto in un ideale massimale. Ciò implica in particolare che A possiede sempre un ideale massimale. $\mathfrak{m}$ è massimale se e solo se $A/\mathfrak{m}$ è un campo e se e solo se per ogni ideale $I \not\subset \mathfrak{m}$ si ha $I + \mathfrak{m} = A$. $\operatorname{Spec} A$ e $\operatorname{Max} A$. Ogni ideale primo contiene un ideale primo minimale. La controimmagine (rispetto a un omomorfismo di anelli) di un ideale è un ideale e la controimmagine di un ideale primo è primo. In genere invece la controimmagine di un ideale massimale non è più massimale (esempio $\mathbb{Z} \longrightarrow \mathbb{Q}$). Se φ è un omomorfismo di anelli e se P è un ideale primo tale che $P \supset \operatorname{Ker} \varphi$, allora anche $\varphi(P)$ è un ideale primo. Biiezione naturale tra gli ideali primi di A/I e gli ideali primi di A che contengono I. Un ideale è primo se e solo se il suo complemento è un sottomonoide (necessariamente puro) dell'anello. Per un sottoinsieme (spesso un sottomonoide puro) S di A sia $S^\sharp$ l'insieme degli ideali I con $I \cap S = \emptyset$. Gli ideali primi minimali coincidono con i sottomonoidi puri massimali. Il radicale $\sqrt{I}$ di I è definito come l'insieme di tutti gli elementi di cui una potenza appartiene ad I. Il radicale $\sqrt{0}$ coincide quindi con l'insieme degli elementi nilpotenti. Esso coincide anche con l'intersezione di tutti gli ideali primi di A. Similmente $\sqrt{I}$ è uguale all'intersezione di tutti gli ideali primi che contengono I. Un anello si dice ridotto se non possiede elementi nilpotenti $\neq 0$. L'anello $A/\sqrt{0}$ è sempre ridotto e, in un certo senso, l'anello ridotto più vicino ad A. $\sqrt{\sqrt{I}} = \sqrt{I}$. $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$. $\sqrt{I^\alpha J} = \sqrt{IJ}$. Un ideale generalizzato si dice radicale, se coincide con il proprio radicale. Ideali radicali di $\mathbb{Z}$. In un anello noetheriano esistono ideali primi $P_1, \ldots, P_n$ tali che $P_1 \cdots P_n = 0$. Il radicale di un anello noetheriano è nilpotente. Il radicale di Jacobson $\overset{\text{Jac}}{\sqrt{I}}$ è definito come l'intersezione di tutti gli ideali massimali che contengono I. Un anello si dice di Jacobson, se ogni ideale primo è intersezione di ideali massimali. In un anello di Jacobson per ogni ideale I si ha $\overset{\text{Jac}}{\sqrt{I}} = \sqrt{I}$.

Situazione 3.1. Sia A un anello commutativo $\neq 0$.

Definizione 3.2. Un *ideale primo* di A è un ideale P di A che soddisfa la seguente condizione:

Se $a, b \in A$ sono tali che $ab \in P$, allora $a \in P$ oppure $b \in P$.

Osservazione 3.3. Un ideale P di A è primo se e solo se l'anello A/P è un anello integro.

Lemma 3.4. *Sia P un ideale di A. Allora sono equivalenti:*

(1) P è primo.

(2) Se I e J sono ideali di A con $IJ \subset P$, allora $I \subset P$ oppure $J \subset P$.

(3) Se I e J sono ideali generalizzati di A con $IJ \subset P$, allora $I \subset P$ oppure $J \subset P$.

Dimostrazione. (1) $\implies$ (2): Siano I e J ideali di A con $IJ \subset P$. Assumiamo, per assurdo, che $I \not\subset P$ e $J \not\subset P$. Allora esistono $a \in I \setminus P$ e $b \in J \setminus P$. Ciò implica $ab \in IJ \subset P$ e quindi ad esempio $a \in P$, perché P è primo, in contrasto con l'ipotesi su a.

(2) $\implies$ (3): Se I e J sono ideali, l'enunciato segue dall'ipotesi (2). Altrimenti sia ad esempio $I = A$. Allora $J = AJ \subset P$.

(2) $\implies$ (1): Siano $a, b \in A$ tali che $ab \in P$. Siccome P è un ideale, ciò implica $Aa \cdot Ab \subset P$. Ma Aa e Ab sono ideali generalizzati di A, quindi per ipotesi ad esempio $Aa \subset P$ e ciò implica $a \in P$.

Proposizione 3.5. *Ogni ideale di A è contenuto in un ideale massimale.*

Dimostrazione. Ciò è una conseguenza facile del lemma di Zorn.

Corollario 3.6. *A contiene un ideale massimale.*

Dimostrazione. 0 è un ideale di A e contenuto in un ideale massimale per la prop. 3.5.

Proposizione 3.7. *A è un campo se e solo se non possiede ideali $\neq 0$.*

Dimostrazione. (1) A sia un campo. Sia I un ideale $\neq 0$ di A. Allora I contiene un elemento $\neq 0$, necessariamente invertibile perché A è un campo. Ciò non è possibile per l'oss. 2.3.

(2) Assumiamo che A non possieda ideali $\neq 0$. Sia $a \in A \setminus 0$. Allora $Aa = A$ e quindi $1 \in Aa$. Ciò significa che a è invertibile.

Corollario 3.8. *Sia $\mathfrak{m}$ un ideale di A. Allora $\mathfrak{m}$ è massimale se e solo se $A/\mathfrak{m}$ è un campo.*

Dimostrazione. Come sappiamo dall'algebra, gli ideali di $A/\mathfrak{m}$ corrispondono in modo naturale e biiettivo agli ideali di A che contengono $\mathfrak{m}$. L'enunciato segue quindi dalla prop. 3.7.

Corollario 3.9. *Ogni ideale massimale di A è primo.*

Dimostrazione. Sia $\mathfrak{m}$ un ideale massimale di A. Allora $A/\mathfrak{m}$ è un campo e quindi un anello integro, perciò $\mathfrak{m}$ è primo per l'oss. 3.3.

Corollario 3.10. *A contiene un ideale primo.*

Dimostrazione. Per il cor. 3.6 A contiene un ideale massimale che è primo per il cor. 3.9.

Lemma 3.11. *Siano S e T monoidi e $\varphi : S \longrightarrow T$ un omomorfismo di monoidi. Sia a un elemento invertibile di S.*

Allora φa è un elemento invertibile di T.

Dimostrazione. Per ipotesi esiste $u \in S$ tale che $au = 1_S$.

Perciò $1_T = \varphi 1_S = \varphi(au) = \varphi a \cdot \varphi b$.

Lemma 3.12. *(1) Siano B un anello commutativo $\neq 0$ e $\varphi : A \longrightarrow B$ un omomorfismo di anelli. Allora $\operatorname{Ker}\varphi$ è un ideale di A.*

(2) Siano K un campo e $\varphi : K \longrightarrow A$ un omomorfismo di anelli. Allora φ è iniettivo, per cui possiamo considerare K come un sottoanello di A.

Dimostrazione. (1) È chiaro che $\operatorname{Ker}\varphi \neq A$. Infatti $\varphi(1_A) = 1_B \neq 0$, per cui $1_A \notin \operatorname{Ker}\varphi$. È adesso immediato che $\operatorname{Ker}\varphi$ è un ideale generalizzato di A.

(2) Ciò è una conseguenza del lemma 3.11 e segue anche dal punto (1):

$\operatorname{Ker}\varphi$ è un ideale di K per l'oss. 3.11. Per la prop. 3.7 $\operatorname{Ker}\varphi = 0$.

Osservazione 3.13. Sia $\mathfrak{m}$ un ideale di A. Allora sono equivalenti:

(1) $\mathfrak{m}$ è massimale.

(2) Per ogni ideale I di A con $I \not\subset \mathfrak{m}$ si ha $I + \mathfrak{m} = A$.

(3) Per ogni $a \in A$ con $a \notin \mathfrak{m}$ si ha $Aa + \mathfrak{m} = A$.

Dimostrazione. (1) $\implies$ (2): Se $I \not\subset \mathfrak{m}$, allora $I + \mathfrak{m} \supsetneq \mathfrak{m}$ e quindi $I + \mathfrak{m} = A$, se $\mathfrak{m}$ è massimale.

(2) $\implies$ (3): Chiaro.

(3) $\implies$ (1): Sia I un ideale di A con $\mathfrak{m} \not\subset I$. Allora esiste $a \in I \setminus \mathfrak{m}$.
Per ipotesi $Aa + \mathfrak{m} = A$. Però $Aa + \mathfrak{m} \subset I + \mathfrak{m} \subset I \neq A$, una contraddizione.

Definizione 3.14. Poniamo

$\operatorname{Spec} A$:= insieme degli ideali primi di A.

$\operatorname{Max} A$:= insieme degli ideali massimali di A.

Definizione 3.15. Un *ideale primo minimale* di A è un ideale primo di A che non contiene nessun altro ideale primo.

Osservazione 3.16. Se A è integro, allora 0 è l'unico ideale primo minimale di A.

Proposizione 3.17. *Ogni ideale primo P di A contiene un ideale primo minimale.*

Dimostrazione. Consideriamo l'insieme $\operatorname{Spec} A$ ordinato per inclusione. Dal cor. 3.10 sappiamo che $\operatorname{Spec} A \neq \emptyset$.

Siano $\mathcal{C}$ una catena $\neq \emptyset$ di $\operatorname{Spec} A$ e $Q := \bigcap_{T \in \mathcal{C}} T$. Allora Q è un ideale di A contenuto in P.

Dobbiamo dimostrare che Q è primo:

Siano $a, b \in A$ tali che $ab \in Q$. Assumiamo, per assurdo, che $ab \notin Q$. Allora esistono $T_1, T_2 \in \mathcal{C}$ con $a \notin T_1$ e $b \notin T_2$. Siccome $\mathcal{C}$ è una catena, abbiamo ad esempio $T_1 \subset T_2$.

Allora $a, b \notin T_1$, mentre $ab \subset Q \subset T_1$. Ma ciò non è possibile, perché T_1 è primo.

Il lemma di Zorn implica l'enunciato.

Lemma 3.18. *Siano B un anello commutativo e $\varphi : A \longrightarrow B$ un omomorfismo di anelli. Allora:*

(1) Per ogni ideale J di B la preimmagine $\varphi^{-1}(J)$ è un ideale di A.

(2) Per ogni $Q \in \operatorname{Spec} B$ si ha $\varphi^{-1}(Q) \in \operatorname{Spec} A$.

Dimostrazione. (1) In primo luogo $1_A \notin \varphi^{-1}(J)$ perché $\varphi(1_A) = 1_B \notin J$.

Siano $a, b \in \varphi^{-1}(J)$ ed $r \in A$. Allora

$\varphi(a + b) = \varphi a + \varphi b \in J + J = J$ e

$\varphi(ra) = \varphi r \cdot \varphi a \in BJ = J$.

(2) Siano $a, b \in A$ tali che $ab \in \varphi^{-1}(Q)$.

Allora $\varphi a \cdot \varphi b = \varphi(ab) \in Q$.

Siccome Q è primo, ciò implica ad esempio $\varphi a \in Q$, cioè $a \in \varphi^{-1}(Q)$.

Osservazione 3.19. Nella situazione del lemma precedente non si può invece concludere che $\varphi^{-1}(\mathfrak{n}) \in \operatorname{Max} A$ per ogni $\mathfrak{n} \in \operatorname{Max} B$.

Siano ad esempio $A = \mathbb{Z}$, $B = \mathbb{Q}$, e $\varphi : \mathbb{Z} \longrightarrow \mathbb{Q}$ l'inclusione. Allora $0 \in \operatorname{Max} \mathbb{Q}$ per la prop. 3.7, ma $\varphi^{-1}(0) = 0 \notin \operatorname{Max} \mathbb{Z}$.

Questa osservazione è, insieme al lemma 3.18, una delle ragioni per cui nella geometria algebrica moderna si lavora con lo spettro primo e non solo con quello massimale; cfr. la discussione a pag. 40 in Görtz/ [21712].

Lemma 3.20. *Siano B un anello commutativo $\neq 0$ e $\varphi : A \longrightarrow B$ un omomorfismo suriettivo di anelli. Allora:*

(1) Se I è un ideale generalizzato di A, allora $\varphi(I)$ è un ideale generalizzato di B.

(2) Se I è un ideale di A tale che $I \supset \operatorname{Ker} \varphi$, allora $\varphi(I)$ è un ideale di B.

(3) Se $P \in \operatorname{Spec} A$ è tale che $P \supset \operatorname{Ker} \varphi$, allora $\varphi(P) \in \operatorname{Spec} B$.

Dimostrazione. (1) È chiaro che $\varphi(I)$ è un sottogruppo additivo di B. Siano $b \in \varphi(I)$ e $t \in B$. Allora esistono $a \in I$ ed $r \in A$ tali che $b = \varphi a$ e $t = \varphi r$. Siccome I è un ideale generalizzato di A, si ha $ra \in I$. Perciò $tb = \varphi r \cdot \varphi a = \varphi(ra) \in \varphi(I)$.

(2) Sia $1_B \in \varphi(I)$, ad esempio $1_B = \varphi a$ con $a \in I$. Siccome anche $\varphi(1_A) = 1_B$, abbiamo $1_A - a \in \operatorname{Ker} \varphi \subset I$ e ciò implica $1_A \in I$, una contraddizione.

(3) Siano $u, v \in B \setminus \varphi(P)$ tali che $uv \in \varphi(P)$, ad esempio $uv = \varphi p$ con $p \in P$.

Siccome φ è suriettivo, esistono $a, b \in A$ tali che $u = \varphi a$, $v = \varphi b$. Necessariamente $a, b \notin P$, perciò, essendo P primo, si ha $ab \notin P$.

Allora $\varphi p = uv = \varphi a \cdot \varphi b = \varphi(ab)$, per cui $ab - p \in \operatorname{Ker} \varphi \subset P$, cosicché $ab \in P$, una contraddizione.

Corollario 3.21. *Sia I un ideale di A.*

(1) Se $P \in \operatorname{Spec} A$ è tale che $P \supset I$, allora $P/I \in \operatorname{Spec} A/I$.

(2) Per ogni $Q \in \operatorname{Spec} A/I$ esiste esattamente un $P \in \operatorname{Spec} A$ con $P \supset I$ e tale che $Q = P/I$. Esplicitamente si ha $P = \{a \in A \mid a + I \in Q\}$.

Corollario 3.22. *Sia I un ideale di A. Allora esiste una biiezione naturale (compatibile con le operazioni insiemistiche)*

$$\begin{array}{rcl} \operatorname{Spec} A/I & \longleftrightarrow & \{P \in \operatorname{Spec} A \mid P \supset I\} \\ Q & \longmapsto & \{a \in A \mid a + I \in Q\} \\ P/I & \longleftarrow\!\shortmid & P \end{array}$$

Definizione 3.23. Un *sottomonoide* di A è un sottosemigruppo S di $(A, \cdot)$ tale che $1 \in S$. Il sottomonoide si dice *puro*, se $0 \notin S$.

Nella letteratura i sottomonoidi di A vengono anche detti *sistemi moltiplicativi*.

Proposizione 3.24. *Un ideale P di A è primo se e solo se $A \setminus P$ è un sottomonoide (necessariamente puro) di A.*

Dimostrazione. Ciò è immediato dalla def. 3.2.

Si noti che sicuramente $1 \in A \setminus P$.

Definizione 3.25. Sia S un sottoinsieme di A. Allora denotiamo con $S^{\#}$ l'insieme degli ideali I di A per i quali $I \cap S = \emptyset$.

In particolare $1^{\#}$ coincide con l'insieme di tutti gli ideali di A.

Osservazione 3.26. Sia S un sottoinsieme di A. Allora sono equivalenti:

(1) $S^{\#} = \emptyset$.

(2) $0 \notin S^{\#}$.

(3) $0 \in S$.

Dimostrazione. (1) $\implies$ (2): Chiaro.

(2) $\implies$ (3): Sia $0 \notin S^{\#}$. Allora $0 \cap S \neq \emptyset$ e quindi $0 \in S$.

(3) $\implies$ (1): Sia $0 \in S$. Siccome ogni ideale I di A contiene 0, si ha $I \cap S \neq \emptyset$, ovvero $I \notin S^{\#}$ e vediamo che $S^{\#} = \emptyset$.

Lemma 3.27. *Siano $a, b \in A$ ed I un ideale di A tale che $ab \in I$, $a \notin I$, $b \notin I$. Allora $Aa + I \neq A$.*

Dimostrazione. Altrimenti esistono $t \in A$ e $p \in I$ tali che $ta + p = 1$.
Ciò implica $tab + pb = b$, per cui $b \in I$, una contraddizione.

Proposizione 3.28. *Sia S un sottomonoide di A. Allora:*

(1) Ogni elemento di $S^{\#}$ è contenuto in un elemento massimale di $S^{\#}$ (il quale non sarà i.g. un ideale massimale, ma solo massimale tra gli elementi di $S^{\#}$).

(2) Ogni elemento massimale di $S^{\#}$ è un ideale primo.

In particolare vediamo che, se S è puro, allora $S^{\#}$ contiene un ideale primo.

Dimostrazione. Se $0 \in S$, allora $S^{\#} = \emptyset$ e i due enunciati sono banalmente veri. Assumiamo quindi che $0 \notin S$. Allora $S^{\#} \neq \emptyset$ per l'oss. 3.26.

(1) Sia $\mathcal{C}$ una catena $\neq \emptyset$ di $S^{\#}$. È chiaro che allora $J := \bigcup_{I \in \mathcal{C}} I$ è un ideale di A con $J \cap S = \emptyset$, per cui $J \in S^{\#}$.

Per il lemma di Zorn quindi ogni elemento di $S^{\#}$ è contenuto in un elemento massimale di $S^{\#}$.

(2) P sia un elemento massimale di $S^{\#}$. Siano $a, b \in A$ tali che $ab \in P$ ed $a, b \notin P$. Per il lemma 3.27 allora $Aa + P$ ed $Ab + P$ sono ideali di A e chiaramente $Aa + P \supsetneq P$, $Ab + P \supsetneq P$.

Per la massimalità di P perciò $Aa + P, Ab + P \notin S^{\#}$, per cui esistono $s \in S \cap (Aa + P)$ e $t \in S \cap (Ab + P)$.

Siccome S è un sottosemigruppo di A, ciò implica

$st \in S \cap (Aa + P)(Ab + P) \overset{2.13}{\subset} S \cap (Aab + P) \subset S \cap P$

e ciò non è possibile perché $P \in S^{\#}$.

Proposizione 3.29. *S sia un sottomonoide puro massimale di A.*

Allora $A \setminus S$ è un ideale primo minimale di A.

Dimostrazione. Per la prop. 3.24 è sufficiente dimostrare che $A \setminus S$ è un ideale di A. Certamente $A \setminus S \neq A$, perché $1 \in S$.

Inoltre $S^{\#} \neq \emptyset$ per l'oss. 3.26. Per la prop. 3.28 esiste perciò un ideale primo P di A con $P \in S^{\#}$.

Allora $A \setminus P$ è un sottomonoide puro di A con $S \subset A \setminus P$. Per la massimalità di S ciò implica $S = A \setminus P$ e vediamo che $A \setminus S = P$ è un ideale (primo) di A.

Lemma 3.30. *Ogni sottomonoide puro di A è contenuto in un sottomonoide puro massimale.*

Dimostrazione. Sia $\mathcal{C}$ una catena $\neq \emptyset$ di sottomonoidi puri di A. È chiaro allora che anche $\bigcup_{S \in \mathcal{C}} S$ è un sottomonoide puro, cosicché l'enunciato segue dal lemma di Zorn.

Proposizione 3.31. *Sia P un ideale primo minimale di A. Allora $A \setminus P$ è un sottomonoide puro massimale di A.*

Dimostrazione. Dalla prop. 3.24 sappiamo che $A \setminus P$ è un sottomonoide puro di A. Per il lemma 3.30 $A \setminus P$ è contenuto in un sottomonoide puro massimale di S.

Allora $A \setminus S \subset P$. Per la prop. 3.29 però $A \setminus S$ è un ideale primo (minimale) e ciò implica $A \setminus S = P$, perché per ipotesi P è minimale.

Corollario 3.32. *Gli ideali primi minimali di A coincidono con i complementi dei sottomonoidi puri massimali di A.*

Lemma 3.33. *Sia S un sottomonoide puro di A. Allora sono equivalenti:*

(1) S è un sottomonoide puro massimale di A.

(2) Per ogni $a \in A \setminus S$ esistono $s \in S$ e $k \in \mathbb{N}$ tali che $sa^k = 0$.

Dimostrazione. (1) $\implies$ (2): Siano $a \in A \setminus S$ e T il sottomonoide di A generato da S ed a. Allora $T = \{sa^k \mid s \in S, k \in \mathbb{N}\}$.

Siccome $a \notin S$, sicuramente $T \supsetneq S$. Per la massimalità di S però T non può essere puro, e ciò implica $0 \in T$.

(2) $\implies$ (1): Sia T un sottomonoide puro con $T \supsetneq S$. Allora esiste $a \in T \setminus S$. Per ipotesi esistono $s \in S$ e $k \in \mathbb{N}$ tali che $sa^k = 0$. Ma $sa^k \in T$, una contraddizione.

Corollario 3.34. *Sia P un ideale primo minimale di A. Allora per ogni $a \in P$ esistono $s \in A \setminus P$ e $k \in \mathbb{N}$ tali che $sa^k = 0$.*

Dimostrazione. Ciò è una conseguenza immediata del lemma 3.1 e del cor. 3.32.

Definizione 3.35. Per un ideale generalizzato I di A poniamo

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

$\sqrt{I}$ si chiama il *radicale* di I, mentre $\sqrt{0}$ si chiama anche il *radicale* di A.

Definizione 3.36. Un elemento $a \in A$ si dice *nilpotente*, se esiste $n \in \mathbb{N}$ tale che $a^n = 0$. Si osservi che allora necessariamente $n \geq 1$.

Per la def. 3.35 l'insieme degli elementi nilpotenti di A coincide con il radicale $\sqrt{0}$.

Proposizione 3.37. *Sia $a \in A$. Allora sono equivalenti:*

(1) a è nilpotente.

(2) a non appartiene a nessun sottomonoide puro di A.

(3) a non appartiene a nessun sottomonoide puro massimale di A.

Dimostrazione. (1) $\implies$ (2): Sia $n \in \mathbb{N}$ tale che $a^n = 0$ e sia S un sottomonoide di A con $a \in S$. Allora $0 = a^n \in S$ e quindi S non è puro.

(2) $\implies$ (3): Chiaro.

(3) $\implies$ (1): a non sia nilpotente. Allora $\{a^n \mid n \in \mathbb{N}\}$ è un sottomonoide puro di A il quale per il lemma 3.30 è contenuto in un sottomonoide puro massimale S a cui quindi a appartiene.

Teorema 3.38. *$\sqrt{0}$ coincide con l'intersezione di tutti gli ideali primi di A.*

Dimostrazione. Sia $\mathcal{S}_{\max}$ l'insieme di tutti i sottomonoidi puri massimali di A. Per la prop. 3.37

$$\sqrt{0} = A \setminus \bigcup_{S \in \mathcal{S}_{\max}} S = \bigcap_{S \in \mathcal{S}_{\max}} (A \setminus S)$$

L'intersezione a destra coincide però, per il cor. 3.32, con l'intersezione di tutti gli ideali primi minimali di A che a sua volta, per la prop. 3.17, è uguale all'intersezione di tutti gli ideali primi di A.

Corollario 3.39. *$\sqrt{0}$ è un ideale di A.*

Corollario 3.40. *Sia I un ideale di A. Allora $\sqrt{I}$ è uguale all'intersezione di tutti gli ideali primi di A che contengono I.*

Dimostrazione. Ciò segue dal teorema 3.38 tenendo conto del cor. 3.22.

Corollario 3.41. *Sia I un ideale di A. Allora $\sqrt{I}$ è un ideale di A.*

Definizione 3.42. Un anello commutativo si dice *ridotto*, se non possiede elementi nilpotenti $\neq 0$.

Ciò accade se e solo se $\sqrt{0} = 0$.

Proposizione 3.43. *L'anello $A/\sqrt{0}$ è ridotto.*

Dimostrazione. Per $a \in A$ denotiamo con $[a]$ la sua classe di equivalenza in $A/\sqrt{0}$.

Sia $[a]$ un elemento nilpotente di $A/\sqrt{0}$. Allora esiste un $n \in \mathbb{N}$ tale che $[a]^n = [a^n] = 0$, ovvero $a^n \in \sqrt{0}$. Ciò significa che esiste $k \in \mathbb{N}$ con $a^{nk} = 0$, cosicché $a \in \sqrt{0}$.

Osservazione 3.44. Sia I un ideale generalizzato di A. Allora $\sqrt{\sqrt{I}} = \sqrt{I}$.

Dimostrazione. È chiaro che $\sqrt{I} \subset \sqrt{\sqrt{I}}$.

Sia $a \in \sqrt{\sqrt{I}}$. Allora esiste un $n \in \mathbb{N}$ tale che $a^n \in \sqrt{I}$ e quindi esiste anche un $k \in \mathbb{N}$ con $a^{nk} = (a^n)^k \in I$, per cui $a \in \sqrt{I}$.

Lemma 3.45. *Siano I e J ideali generalizzati di A ed $\alpha \in \mathbb{N} + 1$. Allora:*

(1) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

(2) $\sqrt{I^\alpha} = \sqrt{I}$.

(3) $\sqrt{I^\alpha J} = \sqrt{IJ}$.

Dimostrazione. (1) È chiaro che $\sqrt{IJ} \subset \sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$.

Sia $a \in \sqrt{I} \cap \sqrt{J}$. Allora esistono $n, m \in \mathbb{N}$ tali che $a^n \in I$ e $a^m \in J$.
Ciò implica $a^{n+m} = a^n a^m \in IJ$.

(2) Segue da (1).

(3) $\sqrt{I^\alpha J} \overset{1}{=} \sqrt{I^\alpha} \cap \sqrt{J} \overset{2}{=} \sqrt{I} \cap \sqrt{J} \overset{1}{=} \sqrt{IJ}$.

Osservazione 3.46. Sia $P \in \operatorname{Spec} A$. Allora $\sqrt{P^\alpha} = P$ per ogni $\alpha \in \mathbb{N} + 1$.

Dimostrazione. Per il lemma 3.45 abbiamo $\sqrt{P^\alpha} = \sqrt{P}$.

$\sqrt{P} = P$ segue dal teorema 3.38 oppure direttamente dalla definizione del radicale.

Definizione 3.47. Un ideale generalizzato I di A si dice *radicale*, se $\sqrt{I} = I$.

Osservazione 3.48. Per l'oss. 3.46 ogni ideale primo è radicale così come, più in generale, ogni potenza di un ideale primo.

Nota 3.49. Gli ideali $\neq 0$ di $\mathbb{Z}$ sono esattamente gli insiemi della forma $m\mathbb{Z}$ con $m \in \mathbb{N} + 2$.

Gli ideali primi di $\mathbb{Z}$ sono esattamente gli insiemi della forma $p\mathbb{Z}$, dove p è un numero primo oppure $p = 0$.

Dimostrazione. Corsi di Algebra.

Esempio 3.50. Siano $p_1, \ldots, p_k$ numeri primi distinti ed $\alpha_1, \ldots, \alpha_k \in \mathbb{N} + 1$. Allora $\sqrt{p_1^{\alpha_1} \cdots p_k^{\alpha_k}\mathbb{Z}} = p_1 \cdots p_k\mathbb{Z}$.

Un ideale $\neq 0$ di $\mathbb{Z}$ è quindi radicale se e solo se è della forma $m\mathbb{Z}$ con $m \in \mathbb{N} + 2$ libero da quadrati.

L'ideale 0 è primo e quindi radicale per l'oss. 3.48.

Dimostrazione. Per l'oss. 2.12

$$p_1^{\alpha_1} \cdots p_k^{\alpha_k}\mathbb{Z} = (p_1\mathbb{Z})^{\alpha_1} \cdots (p_k\mathbb{Z})^{\alpha_k} \quad \text{e} \quad p_1 \cdots p_k\mathbb{Z} = (p_1\mathbb{Z}) \cdots (p_k\mathbb{Z})$$

cosicché l'enunciato segue dal lemma 3.45 e dall'oss. 3.46.

Definizione 3.51. Un ideale I di A si dice *nilpotente*, se esiste un $n \in \mathbb{N}$ tale che $I^n = 0$.

Lemma 3.52. *A sia noetheriano. Allora esistono ideali primi $P_1, \ldots, P_n$ di A tali che $P_1 \cdots P_n = 0$.*

Dimostrazione. Assumiamo, per assurdo, che l'enunciato non sia vero. Allora l'insieme $\mathcal{A}$ degli ideali di A, che non contengono un prodotto finito di ideali primi, contiene l'ideale 0 e quindi non è vuoto. Per la prop. 1.6 esiste un elemento massimale E di $\mathcal{A}$.

Allora però anche l'anello A/E è un controesempio e possiamo sostituire A con A/E, avendo adesso per la massimalità di E la seguente situazione:

(1) Un prodotto finito di ideali primi di A non è mai 0.

(2) In particolare 0 non è primo.

(3) Ogni ideale $\neq 0$ di A contiene un prodotto finito di ideali primi.

Per il punto (2) esistono ideali $I, J \neq 0$ tali che $IJ = 0$. Per il punto (3) esistono ideali primi $P_1, \ldots, P_m, Q_1, \ldots, Q_n$ tali che $P_1 \cdots P_m \subset I$ e $Q_1 \cdots Q_n \subset J$. Ma allora $0 = IJ \supset P_1 \cdots P_m Q_1 \cdots Q_n$ in contrasto con il punto (1).

Proposizione 3.53. *A sia noetheriano. Allora $\sqrt{0}$ è nilpotente.*

Dimostrazione. Per il lemma 3.52 esistono ideali primi $P_1, \ldots, P_n$ di A tali che $P_1 \cdots P_n = 0$.

Per il teorema 3.38 però $\sqrt{0} \subset P_i$ per ogni i e ciò implica $\sqrt{0}^n = 0$.

Un'altra dimostrazione si trova in 3518 Atiyah/, 7.15.

Definizione 3.54. Il *radicale di Jacobson* $\sqrt[\text{Jac}]{I}$ di un ideale I di A è definito come l'intersezione di tutti gli ideali massimali di A che contengono I.

Esso è quindi un ideale di A.

$\sqrt[\text{Jac}]{0}$ si chiama anche il radicale di Jacobson di A.

Definizione 3.55. A si chiama un *anello di Jacobson*, se ogni ideale primo di A è intersezione di ideali massimali.

Osservazione 3.56. A è un anello di Jacobson se e solo se per ogni ideale I di A si ha $\sqrt[\text{Jac}]{I} = \sqrt{I}$.

Proposizione 3.57. *Per $a \in A$ sono equivalenti:*

(1) $a \in \sqrt[\text{Jac}]{0}$.

(2) $1 - ab$ *è invertibile per ogni* $b \in A$.

Dimostrazione. (1) $\implies$ (2): Sia $1 - ab$ non invertibile. Allora esiste $\mathfrak{m} \in \operatorname{Max} A$ con $1 - ab \in \mathfrak{m}$.

Per ipotesi però $a \in \mathfrak{m}$ e quindi $ab \in \mathfrak{m}$. Ciò implica $1 \in \mathfrak{m}$, una contraddizione.

(2) $\implies$ (1): Assumiamo, per assurdo, che esista $\mathfrak{m} \in \operatorname{Max} A$ con $a \notin \mathfrak{m}$. Per l'oss. 3.13 allora $Aa + \mathfrak{m} = A$, per cui esistono $b \in A$ e $p \in \mathfrak{m}$ tali che $ab + p = 1$, ovvero $1 - ab \in \mathfrak{m}$. Ma allora $1 - ab$ non può essere invertibile.

4. Algebre commutative finitamente generate

Algebre commutative. Omomorfismo di struttura. Algebre finitamente generate. Il campo dei quozienti $\mathcal{K}(A)$ di un anello integro A. I tre diversi significati del termine finitamente generato. Una A-algebra commutativa è finitamente generata se e solo se è immagine omomorfa di un anello di polinomi $A[x_1, \ldots, x_n]$ e quindi isomorfa a un anello della forma $A[x_1, \ldots, x_n]/I$. Una A-algebra finitamente generata su un anello noetheriano è noetheriana. Omomorfismi di A-algebre.

Situazione 4.1. Sia A un anello commutativo.

Definizione 4.2. Una *A-algebra* commutativa è un anello commutativo B che è allo stesso tempo un A-modulo in modo tale che per $a \in A$ ed $u, v \in B$ si abbia $a(uv) = (au)v$.

In particolare si ha $av = a \cdot 1_B v = a1_B \cdot v$.

Si noti che si ha automaticamente $a(uv) = u(av)$.

Infatti $a(uv) = a(vu) = (av)u = u(av)$.

Nota 4.3. (1) Sia B una A-algebra commutativa. Allora possiamo definire un omomorfismo di anelli $\varphi : A \longrightarrow B$ ponendo $\varphi(a) := a1_B$.

Per $a \in A$ e $v \in B$ si ha allora $av = a1_B v = \varphi(a)v$.

φ si chiama l'*omomorfismo di struttura* della A-algebra B.

(2) Se viceversa φ è un anello commutativo e $\varphi : A \longrightarrow B$ è un omomorfismo di anelli, allora, ponendo $av := \varphi(a)v$ per $a \in A$ e $v \in B$, l'anello B diventa una A-algebra e si ha $a1_B = \varphi(a)1_B = \varphi(a)$.

Osservazione 4.4. Siano A un campo e B una A-algebra commutativa. Allora l'omomorfismo di struttura $\bigcirc\!\!\!\!\!\!\int_a a1_B : A \longrightarrow B$ è iniettivo, per cui possiamo considerare A in modo naturale come sottoanello di B.

Dimostrazione. Ciò segue dal lemma 3.12.

Osservazione 4.5. Siano B una A-algebra ed I un ideale generalizzato di B. Allora I è un sotto-A-modulo di B.

Dimostrazione. Siano $v \in I$ ed $a \in A$. Allora $av = a1_B \cdot v \in I$.

Definizione 4.6. Sia B una A-algebra commutativa. Una *sottoalgebra* (più precisamente sotto-A-algebra) di B è un sottoanello B_0 di B tale che per ogni $a \in A$ ed ogni $v \in B_0$ si abbia $av \in B_0$.

Definizione 4.7. Siano B una A-algebra commutativa ed $F \subset B$ un sottoinsieme.

La più piccola sottoalgebra di B che contiene F si chiama la sottoalgebra *generata* da F.

Essa coincide evidentemente con il sottoanello di B generato da F e l'insieme $A1_B = \{a1_B \mid a \in A\}$.

Definizione 4.8. Sia B una A-algebra commutativa. Da un polinomio $f \in A[x_1, \ldots, x_n]$ si ottiene un polinomio $f_B \in B[x_1, \ldots, x_n]$ sostituendo ogni coefficiente a di f con $a1_B$. Per $\alpha_1, \ldots, \alpha_n \in B$ è perciò definito

$f(\alpha_1, \ldots, \alpha_n) := f_B(\alpha_1, \ldots, \alpha_n)$

Definizione 4.9. Sia B una A-algebra commutativa. Per $\alpha_1, \ldots, \alpha_n \in B$ poniamo

$$A[\alpha_1, \ldots, \alpha_n] := \{f(\alpha_1, \ldots, \alpha_n) \mid f \in A[x_1, \ldots, x_n]\}$$

È immediata la verifica che $A[\alpha_1, \ldots, \alpha_n]$ coincide con la sotto-A-algebra generata da $\{\alpha_1, \ldots, \alpha_n\}$.

B si chiama una *A-algebra finitamente generata*, se esistono $\alpha_1, \ldots, \alpha_n \in B$ tali che $B = A[\alpha_1, \ldots, \alpha_n]$.

Definizione 4.10. Per un anello integro A denotiamo con $\mathcal{K}(A)$ il suo campo dei quozienti.

Nel caso che A sia sottoanello di un campo E, spesso identifichiamo tacitamente $\mathcal{K}(A)$ con il sottocampo $\left\{\frac{a}{b} \mid a \in A, b \in A \setminus 0\right\}$ di E.

Definizione 4.11. Siano E un campo e K un sottocampo di E.

Per $\alpha_1, \ldots, \alpha_n \in E$ allora $K(\alpha_1, \ldots, \alpha_n) := \mathcal{K}(K[\alpha_1, \ldots, \alpha_n])$ coincide con il più piccolo sottocampo di E che contiene K e l'insieme $\{\alpha_1, \ldots, \alpha_n\}$, come si dimostra facilmente. Cfr. Gabelli [21928], 111-112.

Nota 4.12. Nell'algebra commutativa il termine *finitamente generato* viene usato con tre diversi significati:

Assumiamo che B sia una A-algebra commutativa. Allora B è anche un A-modulo e può essere finitamente generata come A-modulo. Questa condizione è molto più forte della condizione che B sia finitamente generata come A-algebra.

Se A è un campo, B è uno spazio vettoriale su A e possiamo definire il *grado* $|B : A|$ di B su A come la dimensione di B su A; in tal caso B è finitamente generata come A-modulo se e solo se $|B : A| < \infty$.

Se infine sia A che B sono campi con A un sottocampo di B, allora B si chiama un campo finitamente generato su A se esistono $\alpha_1, \ldots, \alpha_n \in B$ tali che $B = A(\alpha_1, \ldots, \alpha_n)$.

Lemma 4.13. *Una A-algebra commutativa B è finitamente generata se e solo se esistono $n \in \mathbb{N}+1$ e un omomorfismo suriettivo di anelli $\theta : A[x_1, \ldots, x_n] \longrightarrow B$.*

In tal caso $B = A[\theta(x_1), \ldots, \theta(x_n)]$.

Dimostrazione. (1) B sia una A-algebra commutativa ed $\alpha_1, \ldots, \alpha_n \in B$ tali che $B = A[\alpha_1, \ldots, \alpha_n]$. Allora otteniamo un omomorfismo suriettivo di anelli $\theta : A[x_1, \ldots, x_n] \longrightarrow B$ ponendo $\theta(f) := f(\alpha_1, \ldots, \alpha_n)$ per ogni polinomio $f \in A[x_1, \ldots, x_n]$. In particolare si ha $\theta(x_i) = \alpha_i$ per ogni i.

(2) Sia viceversa dato un omomorfismo suriettivo $\theta : A[x_1, \ldots, x_n] \longrightarrow B$. Allora possiamo definire un omomorfismo $\varphi : A \longrightarrow B$ semplicemente ponendo $\varphi := \theta_{|A}$. Come nella nota 4.3 allora B diventa una A-algebra commutativa ed è chiaro che con $\alpha_i := \theta(x_i)$ per $i = 1, \ldots, n$ si ha $\theta(f) = f(\alpha_1, \ldots, \alpha_n)$ per ogni $f \in A[x_1, \ldots, x_n]$ e quindi $B = A[\alpha_1, \ldots, \alpha_n]$.

Corollario 4.14. *Una A-algebra commutativa B è finitamente generata se e solo se esistono $n \in \mathbb{N}+1$ e un ideale I di $A[x_1,\dots,x_n]$ tali che* $B \cong A[x_1,\dots,x_n]/I$.

Corollario 4.15. *Siano A noetheriano e B una A-algebra commutativa finitamente generata. Allora l'anello B è noetheriano.*

Dimostrazione. Per il lemma 4.13 esistono $n \in \mathbb{N}+1$ e un omomorfismo suriettivo di anelli $\theta : A[x_1,\dots,x_n] \longrightarrow B$.

Per il corollario 1.11 $A[x_1,\dots,x_n]$ è noetheriano, cosicché l'enunciato segue dall'oss. 1.15.

Definizione 4.16. Per un A-modulo M denotiamo con $|M : A|$ la minima cardinalità di un sistema di generatori di M su A.

Eventualmente qui si nasconde una piccola difficoltà insiemistica, che però non ci deve preoccupare.

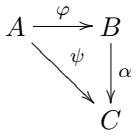
M è quindi finitamente generato come A-modulo se e solo se $|M : A| < \infty$. Se A è un campo, si ha semplicemente $|M : A| = \dim_A M$.

Definizione 4.17. Siano B e C A-algebre commutative. Un'applicazione $B \longrightarrow C$ si chiama un *omomorfismo* di A-algebre, se è allo stesso tempo un omomorfismo di anelli e un omomorfismo di A-moduli.

Osservazione 4.18. Siano B e C A-algebre commutative con gli omomorfismi di struttura φ e ψ ed $\alpha : B \longrightarrow C$ un'applicazione. Allora sono equivalenti:

(1) α è un omomorfismo di A-algebre.

(2) α è un omomorfismo di anelli che rende commutativo il diagramma



Dimostrazione. (1) $\implies$ (2): Per ogni $a \in A$ nell'ipotesi (1) si ha

$\alpha\varphi a = \alpha(a1_B) = a\alpha 1_B = a1_C = \psi a$

(2) $\implies$ (1): Per ogni $a \in A$ ed ogni $v \in B$ nell'ipotesi (2) si ha

$\alpha av = \alpha(\varphi a \cdot v) = \alpha\varphi a \cdot \alpha v = \psi a \cdot \alpha v = a\alpha v$

Definizione 4.19. Una A-algebra commutativa si dice *integra*, se è integra come anello, cioè se $A \neq 0$ e A non contiene zerodivisori $\neq 0$.

5. Lo schema di Ruffini nell'anello dei polinomi

Siano $f \in A[x]$ ed $\alpha \in A$. Allora esistono $g \in A[x]$ e $\beta \in A$ tali che $f = (x-\alpha)g+\beta$. Ovviamente $\beta = f(\alpha)$. Siano $f \in A[x_1, \ldots, x_n]$ ed $\alpha_1, \ldots, \alpha_n \in A$. Allora esistono $g_1 \in A[x_1, \ldots, x_n], g_2 \in A[x_2, \ldots, x_n], \ldots, g_n \in A[x_n]$ tali che $f = (x_1 - \alpha_1)g_1 + (x_2 - \alpha_2)g_2 + \ldots + (x_n - \alpha_n)g_n + f(\alpha_1, \ldots, \alpha_n)$. Se K è un campo, allora l'ideale $K[x_1, \ldots, x_n]\smile(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ è massimale.

Situazione 5.1. Sia A un anello commutativo.

Nota 5.2 (schema di Ruffini). Sia dato un polinomio

$f = a_0x^n + a_1x^{n-1} + \cdots + a_n \in A[x]$

Per $\alpha \in A$ vogliamo calcolare $f(\alpha)$.

Sia ad esempio $f = 3x^4 + 5x^3 + 6x^2 + 8x + 7$. Poniamo

$$\begin{aligned} b_0 &= 3 \\ b_1 = b_0\alpha + 5 &= 3\alpha + 5 \\ b_2 = b_1\alpha + 6 &= 3\alpha^2 + 5\alpha + 6 \\ b_3 = b_2\alpha + 8 &= 3\alpha^3 + 5\alpha^2 + 6\alpha + 8 \\ b_4 = b_3\alpha + 7 &= 3\alpha^4 + 5\alpha^3 + 6\alpha^2 + 8\alpha + 7 \end{aligned}$$

e vediamo che $b_4 = f(\alpha)$. Lo stesso si può fare nel caso generale:

$$\begin{aligned} b_0 &= a_0 \\ b_1 &= b_0\alpha + a_1 \\ &\cdots \\ b_k &= b_{k-1}\alpha + a_k \\ &\cdots \\ b_n &= b_{n-1}\alpha + a_n \end{aligned}$$

con $b_n = f(\alpha)$, come dimostriamo adesso. Consideriamo il polinomio

$g := b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-1}$.

Allora, usando che $\alpha b_k = b_{k+1} - a_{k+1}$ per $k = 0, \ldots, n-1$, abbiamo

$$\begin{aligned} \alpha g &= \alpha b_0x^{n-1} + \alpha b_1x^{n-2} + \cdots + \alpha b_{n-1} \\ &= (b_1 - a_1)x^{n-1} + (b_2 - a_2)x^{n-2} + \ldots \\ &\quad + (b_{n-1} - a_{n-1})x + b_n - a_n \\ &= (b_1x^{n-1} + b_2x^{n-2} + \cdots + b_{n-1}x + b_n) \\ &\quad - (a_1x^{n-1} + a_2x^{n-2} + \ldots a_{n-1}x + a_n) \\ &= x(g - b_0x^{n-1}) + b_n - (f - a_0x^n) \\ &= xg - b_0x^n + b_n - f + a_0x^n = xg + b_n - f \end{aligned}$$

quindi

$f = (x - \alpha)g + b_n$

e ciò implica $f(\alpha) = b_n$.

$b_0, \ldots, b_{n-1}$ sono perciò i coefficienti del quoziente nella divisione con resto di f per $x - \alpha$, mentre b_n è il resto, uguale a $f(\alpha)$.

Nota 5.3. Per il calcolo a mano lo schema di Ruffini nella situazione della nota 5.2 si può scrivere nella forma

	α
a_0	$b_0 = a_0$
a_1	$b_1 = \alpha b_0 + a_1$
a_2	$b_2 = \alpha b_1 + a_2$
a_3	$b_3 = \alpha b_2 + a_3$
$\ldots$	$\ldots$

Per $f = 3x^4 + 5x^3 + 6x^2 + 8x + 7$ ed $\alpha = 2$ abbiamo ad esempio

	2
3	3
5	11
6	28
8	64
7	135

per cui $f = (x - 2)(3x^3 + 11x^2 + 28x + 64) + 135$ ed $f(2) = 135$.

Corollario 5.4. *Siano $f \in A[x]$ ed $\alpha \in A$. Allora esistono $g \in A[x]$ e $\beta \in A$ tali che $f = (x - \alpha)g + \beta$.*

È chiaro inoltre che $\beta = f(\alpha)$.

Lemma 5.5. *Siano $f \in A[x_1, \ldots, x_n]$ ed $\alpha_1, \ldots, \alpha_n \in A$.*

Allora esistono $g_1 \in A[x_1, \ldots, x_n], g_2 \in A[x_2, \ldots, x_n], \ldots, g_n \in A[x_n]$ tali che

$$f = (x_1 - \alpha_1)g_1 + (x_2 - \alpha_2)g_2 + \ldots + (x_n - \alpha_n)g_n + f(\alpha_1, \ldots, \alpha_n)$$

Dimostrazione. Applicando il cor. 5.4 all'anello $A[x_2, \ldots, x_n]$ al posto di A troviamo $g_1 \in A[x_1, \ldots, x_n]$ e $h_1 \in A[x_2, \ldots, x_n]$ tali che $f = (x_1 - \alpha_1)g_1 + h_1$.

Adesso applichiamo il cor. 5.4 all'anello $A[x_3, \ldots, x_n]$ al posto di A, trovando $g_2 \in A[x_2, \ldots, x_n]$ e $h_2 \in A[x_3, \ldots, x_n]$ tali che $h_1 = (x_2 - \alpha_2)g_2 + h_2$, cosicché $f = (x_1 - \alpha_1)g_1 + (x_2 - \alpha_2)g_2 + h_2$.

Continuando in questo modo otteniamo l'enunciato.

Esempio 5.6. Siano $f = 5x^2y^2 + 3xy^2 + 7xy + 8x + 9y + 4 \in \mathbb{Z}[x, y]$ ed $\alpha = 1$, $\beta = 3$. Con il metodo del lemma 5.5 troviamo

	$\alpha = 1$
$5y^2$ $3y^2 + 7y + 8$ $9y + 4$	$5y^2$ $8y^2 + 7y + 8$ $8y^2 + 16y + 12$

per cui $f = (x-1)(5y^2x + 8y^2 + 7y + 8) + 8y^2 + 16y + 12$.

	$\beta = 3$
8 16 12	8 40 132

cosicché $f = (x-1)(5y^2x + 8y^2 + 7y + 8) + (y-3)(8y + 40) + 132$.

Proposizione 5.7. *Siano K un campo ed $\alpha_1, \ldots, \alpha_n \in K$.*

Allora l'ideale $K[x_1, \ldots, x_n]_\smile(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ è massimale.

Dimostrazione. Sia $\mathfrak{m} := K[x_1, \ldots, x_n]_\smile(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$.

Siano I un ideale di $K[x_1, \ldots, x_n]$ con $I \supset \mathfrak{m}$ ed $f \in I$.

Con il lemma 5.5 troviamo una rappresentazione

$$f = (x_1 - \alpha_1)g_1 + (x_2 - \alpha_2)g_2 + \ldots + (x_n - \alpha_n)g_n + \beta$$

con $g_1 \in K[x_1, \ldots, x_n]$, $g_2 \in K[x_2, \ldots, x_n]$, …, $g_n \in K[x_n]$ e $\beta \in K$.

Ciò implica $\beta \in I$. Perciò β non può essere invertibile. Siccome però K è un campo, necessariamente $\beta = 0$, per cui $f \in \mathfrak{m}$. Ciò mostra $I = \mathfrak{m}$.

6. L'anello A_f

Per f non nilpotente sia $S := \{f^n \mid n \in \mathbb{N}\}$. Un ideale H si dice S-saturo, se $a \in A, s \in S$ ed $as \in H$ implicano $a \in H$. $\Omega := \{a \in A \mid \exists s \in S \text{ con } as = 0\}$. $A_f := S^{-1}A := (A \times S)/\sim$, dove $(a,s) \sim (b,t)$, se $at - bs \in \Omega$. La classe di equivalenza di (a,s) viene denotata con $\frac{a_f}{s}$. A_f diventa un anello commutativo con le operazioni definite in modo naturale. L'applicazione $i_f := \bigcirc_a a_f : A \longrightarrow A_f$ è un omomorfismo, ma nel caso più generale non è iniettiva - il nucleo coincide con Ω. i_f è un isomorfismo se e solo se f è invertibile. Se A è integro, possiamo identificare A_f in modo naturale con il sottoanello $A\left[\frac{1}{f}\right]$ di $\mathcal{K}(A)$. Nel caso di un campo K possiamo quindi identificare $K[x_1, \ldots, x_n]_f$ con $K[x_1, \ldots, x_n, \frac{1}{f}]$. L'isomorfismo $A_f \cong A[x]/(fx - 1)$. Confronto con la costruzione algebrica dei numeri complessi.

Situazione 6.1. Siano A un anello commutativo, f un elemento *non nilpotente* di A ed $S := \{f^n \mid n \in \mathbb{N}\}$. L'ipotesi implica $A \neq 0$.

S è un sottomonoide puro di A.

Nota 6.2. Definiremo in un capitolo successivo la localizzazione rispetto a un qualsiasi sottomonoide puro di A. In questo capitolo ci limitiamo al caso del sottomonoide S definito nella situazione 6.1. Questo caso speciale è molto importante, non solo perché verrà utilizzato nella dimostrazione del teorema degli zeri di Hilbert, ma anche in una costruzione fondamentale della teoria degli schemi.

Molte delle definizioni e costruzioni di questo capitolo potranno essere usate tali e quali nel caso generale.

Definizione 6.3. Un ideale H di A si dice *S-saturo*, se vale l'implicazione

$a \in A, s \in S, as \in H \Longrightarrow a \in H$

Seguiamo in questa terminologia ad esempio Lam/ [21984]. Ideali e insiemi saturi vengono definiti in geometria algebrica in altri contesti in modo diverso.

Definizione 6.4. $\Omega := \Omega_S := \Omega_f := \{a \in A \mid \text{ esiste } s \in S \text{ con } as = 0\}$

si chiama l'*ideale di indeterminazione* di S. Esplicitamente si ha

$\Omega = \{a \in A \mid \text{ esiste } k \in \mathbb{N} \text{ con } af^k = 0\}$

Se f non è uno zerodivisore, si ha quindi $\Omega = 0$.

Osservazione 6.5. Ω è un ideale S-saturo di A.

Dimostrazione. (1) È chiaro che $0 \in \Omega$ e che $1 \notin \Omega$.

(2) Siano $a, b \in \Omega$, ad esempio $as = bt = 0$ con $s, t \in S$. Allora $ast = bst = 0$ e quindi $(a+b)st = 0$.

Siccome S è un sottosemigruppo di A, si ha $st \in S$.

(3) Siano $a \in \Omega$ e $b \in A$. Allora ad esempio $as = 0$ con $s \in S$, per cui $bas = 0$.

Ciò mostra che Ω è un ideale di A.

(4) Dimostriamo che Ω è S-saturo.

Siano $a \in A$ ed $s \in S$ con $as \in \Omega$. Allora esiste $t \in S$ con $ast = 0$. Ma ciò implica $a \in \Omega$, essendo $st \in S$.

Definizione 6.6. Sull'insieme $A \times S$ introduciamo la relazione

$$(a, s) \sim (b, t) : \iff at - bs \in \Omega$$

Lemma 6.7. *La relazione $\sim$ introdotta nella def. 6.6 è una relazione di equivalenza su $A \times S$.*

Dimostrazione. (1) Riflessività è simmetria di $\sim$ sono evidenti.

(2) Dimostriamo la transitività: Si abbia $(a, s) \sim (b, t) \sim (c, r)$.

Allora $at - bs \in \Omega$ e $br - ct \in \Omega$, per cui $atr - bsr \in \Omega$ e $bsr - cts \in \Omega$, cosicché $(ar - cs)t = atr - cts \in \Omega$.

Siccome Ω è S-saturo, ciò implica $ar - cs \in \Omega$ e quindi $(a, s) \sim (c, r)$.

Definizione 6.8. $S^{-1}A := A_f := (A \times S)/\sim$ si chiama la *localizzazione* di A in f (o rispetto al sottomonoide S).

Talvolta il termine localizzazione viene usato solo nel caso che S sia complemento di un ideale primo; allora nel caso generale $S^{-1}A$ si chiama l'anello delle *frazioni* rispetto ad S.

Definizione 6.9. Per $a \in A$ ed $s \in S$ denotiamo con a_f la classe di equivalenza di $(a, 1)$ in A_f, con $\dfrac{a_f}{s}$ la classe di equivalenza di (a, s).

Vedremo che questa notazione è legittima, perché gli elementi di S sono, come dimostreremo, invertibili in A_f.

Osservazione 6.10. Tenendo conto della definizione di S la def. 6.6 può essere riformulata più esplicitamente così: Per $m, n \in \mathbb{N}$ ed $a, b \in A$ si ha

$$\frac{a_f}{f^m} = \frac{b_f}{f^n} \iff \text{esiste un } k \in \mathbb{N} \text{ tale che } af^{n+k} = bf^{m+k}$$

Se f non è uno zerodivisore, si ha

$$\frac{a_f}{f^m} = \frac{b_f}{f^n} \iff af^n = bf^m$$

Osservazione 6.11. Siano $a, b \in A$. Allora

$$a_f = b_f \iff a - b \in \Omega$$

Più esplicitamente abbiamo

$$a_f = b_f \iff \text{esiste } k \in \mathbb{N} \text{ tale che } af^k = bf^k$$

Se f non è uno zerodivisore, si ha $a_f = b_f \iff a = b$.

Osservazione 6.12. Sia $a \in A$. Allora $a_f = 0 \iff a \in \Omega$.

Osservazione 6.13. $1_f \neq 0$.

Dimostrazione. Infatti $1 \notin \Omega$.

Osservazione 6.14. Siano $a, b, a', b' \in A$ ed $s, t, s', t' \in S$ tali che

$$\frac{a_f}{s} = \frac{a'_f}{s'} \text{ e } \frac{b_f}{t} = \frac{b'_f}{t'}$$

Allora

$$\frac{(at+bs)_f}{st} = \frac{(a't'+b's')_f}{s't'}$$

$$\frac{(ab)_f}{st} = \frac{(a'b')_f}{s't'}$$

Dimostrazione. (1) Per ipotesi $as' - a's, bt' - b't \in \Omega$.

(2) Moltiplicando il primo termine con tt' e il secondo con ss' otteniamo $as'tt' - a'stt', bt'ss' - b'tss' \in \Omega$, per cui $(at+bs)s't' - (a't'+b's')st \in \Omega$ e quindi

$$\frac{(at+bs)_f}{st} = \frac{(a't'+b's')_f}{s't'}$$

(3) Moltiplicando in (1) il primo termine con bt' e il secondo con $a's$ otteniamo $abs't' - a'bst', a'bst' - a'b'st \in \Omega$, per cui $abs't' - a'b'st \in \Omega$, e quindi

$$\frac{(ab)_f}{st} = \frac{(a'b')_f}{s't'}$$

Osservazione 6.15. Siano $a \in A$ ed $s, t \in S$. Allora

$$\frac{a_f}{s} = \frac{(at)_f}{st}$$

Proposizione 6.16. *Su A_f introduciamo le operazioni*

$$\frac{a_f}{s} + \frac{b_f}{t} := \frac{(at+bs)_f}{st}$$
$$\frac{a_f}{s}\frac{b_f}{t} := \frac{(ab)_f}{st}$$

Allora A_f diventa un anello commutativo in cui 0_f è l'elemento neutro dell'addizione e 1_f l'elemento neutro della moltiplicazione.

Dimostrazione. (1) Le operazioni sono ben definite per l'oss. 6.14.

(2) Si verifica facilmente che $(A_f, +)$ è un gruppo abeliano con elemento neutro 0_f e che $(A_f, \cdot)$ è un monoide commutativo con elemento neutro 1_f.

(3) Dimostriamo la legge di distributività: Usando l'oss. 6.15 per $a, b, c \in A$ ed $s, t, r \in S$ abbiamo

$$\left(\frac{a_f}{s} + \frac{b_f}{t}\right)\frac{c_f}{r} = \frac{(atc+bsc)_f}{str} = \frac{(actr+bcsr)_f}{str^2}$$
$$= \frac{(ac)_f}{sr} + \frac{(bc)_f}{tr} = \frac{a_f}{s}\frac{c_f}{r} + \frac{b_f}{t}\frac{c_f}{r}$$

Osservazione 6.17. Siano $a, b \in A$. Allora

$$(a+b)_f = a_f + b_f$$
$$(ab)_f = a_f b_f$$

Dimostrazione. $a_f + b_f = \dfrac{a_f}{1} + \dfrac{b_f}{1} = \dfrac{(a+b)_f}{1} = (a+b)_f$

$a_f b_f = \dfrac{a_f}{1}\dfrac{b_f}{1} = \dfrac{(ab)_f}{1} = (ab)_f$

Proposizione 6.18. *L'applicazione* $i_f := \bigcirc\limits_a a_f : A \longrightarrow A_f$ *è un omomorfismo di anelli con nucleo* Ω.

Dimostrazione. Ciò segue dalle oss. 6.17 e 6.12 e dalla prop. 6.16.

Corollario 6.19. *Se* f *non è uno zerodivisore, possiamo considerare* A *come sottoanello di* A_f *tramite l'omomorfismo* $i_f : A \longrightarrow A_f$.

Osservazione 6.20. f sia invertibile in A.

Allora per ogni $a \in A$ ed ogni $n \in \mathbb{N}$ si ha $\dfrac{a_f}{f^n} = (af^{-n})_f$.

In questo caso l'omomorfismo $i_f : A \longrightarrow A_f$ è un isomorfismo.

Dimostrazione. (1) Se f è invertibile, f non può essere uno zerodivisore, per cui $\Omega = 0$. L'omomorfismo i_f è quindi iniettivo.

(2) $a = (af^{-n})f^n$ implica $\dfrac{a_f}{f^n} = (af^{-n})_f$.

(3) Ciò significa però che $\dfrac{a_f}{f^n} = i_f(af^{-n})$, cosicché i_f è anche suriettivo.

Osservazione 6.21. L'applicazione $i_f : A \longrightarrow A_f$ è un isomorfismo se e solo se f è invertibile.

Dimostrazione. (1) Sia i_f un isomorfismo. Allora $\Omega = \operatorname{Ker} i_f = 0$.
Per la suriettività di i_f deve esistere un elemento $e \in A$ tale che $\dfrac{1_f}{f} = e_f$.
Cio implica $1 - fe \in \Omega = 0$, per cui f è invertibile.

(2) Abbiamo visto nell'oss. 6.20 che i_f è un isomorfismo, se f è invertibile.

Nota 6.22. A sia un anello integro. Allora l'applicazione

$$\begin{aligned} \varphi : A_f &\longrightarrow \mathcal{K}(A) \\ \frac{a_f}{s} &\longmapsto \frac{a}{s} \end{aligned}$$

è ben definita e costituisce un omomorfismo iniettivo di anelli che rende commutativo il diagramma

$$\begin{array}{ccc} A & \xrightarrow{i_f} & A_f \\ & \searrow^{j} & \downarrow{\scriptstyle \varphi} \\ & & \mathcal{K}(A) \end{array}$$

in cui j è l'inclusione canonica $\bigcirc\limits_a \dfrac{a}{1}$ di A nel suo campo dei quozienti.

Nel caso che A sia integro possiamo quindi identificare A_f con il sottoanello $\left\{ \dfrac{a}{s} \mid a \in A, s \in S \right\}$ di $\mathcal{K}(A)$, ottenendo semplicemente inclusioni

$A \subset A_f \subset \mathcal{K}(A)$. In particolare vediamo che anche A_f è un anello integro.

Dimostrazione. (1) Dimostriamo che φ è ben definito.

Osserviamo che $\Omega = 0$. Sia $\frac{a_f}{s} = \frac{b_f}{t}$. Allora $at = bs$ e ciò implica che $\frac{a}{s} = \frac{b}{t}$ in $\mathcal{K}(A)$.

(2) Dimostriamo che φ è iniettivo.

Sia $\frac{a}{s} = 0$ in $\mathcal{K}(A)$. Ciò implica però $a = 0$ e quindi $\frac{a_f}{s} = 0$.

(3) Per $a \in A$ abbiamo $\varphi(i_f(a)) = \varphi(a_f) = \frac{a}{1} = j(a)$.

(4) È infine una verifica immediata che φ è un omomorfismo di anelli.

Nota 6.23. Come nella nota 6.22 sia A un anello integro. Nel caso considerato in questo capitolo però $S = \{f^n \mid n \in \mathbb{N}\}$.

Perciò il sottoanello $\left\{\frac{a}{s} \mid a \in A, s \in S\right\} = \left\{\frac{a}{f^n} \mid a \in A, n \in \mathbb{N}\right\}$ coincide con il sottoanello $A\left[\frac{1}{f}\right]$ di $\mathcal{K}(A)$.

Se A è integro, possiamo quindi identificare A_f con $A\left[\frac{1}{f}\right]$, con quest'ultimo anello formato in $\mathcal{K}(A)$.

Esempio 6.24. Sia $b \in \mathbb{Z} \setminus 0$. Per la nota 6.23 possiamo identificare $\mathbb{Z}_b$ con il sottoanello $\left\{\frac{a}{b^k} \mid a \in \mathbb{Z}, k \in \mathbb{N}\right\}$ di $\mathbb{Q}$.

Corollario 6.25. *Siano K un campo ed $f \in K[x_1, \ldots, x_n]$ con $f \neq 0$.*

Allora $K[x_1, \ldots, x_n]_f$ può essere identificato con il sottoanello $K\left[x_1, \ldots, x_n, \frac{1}{f}\right]$ di $K(x_1, \ldots, x_n)$.

Osservazione 6.26. Per ogni $s \in S$ si ha $s_f \frac{1_f}{s} = 1_f$.

Dimostrazione. Infatti $s_f \frac{1_f}{s} = \frac{s_f}{s}$ ed è chiaro che l'ultima frazione coincide con 1_f (cfr. oss. 6.15).

Teorema 6.27. *Per ogni $s \in S$ l'elemento s_f è invertibile nell'anello A_f e si ha $(s_f)^{-1} = \frac{1_f}{s}$.*

Dimostrazione. Ciò è una conseguenza immediata dell'oss. 6.26.

Osservazione 6.28. L'oss. 6.26 e il teorema 6.27 giustificano anche la nostra notazione introdotta nella def. 6.9: Infatti per $a \in A$ ed $s \in S$ in A_f si ha $\frac{a_f}{s} = \frac{a_f 1_f}{s} = a_f (s_f)^{-1}$.

Lemma 6.29. *Definiamo un omomorfismo di A-algebre $\psi : A[x] \longrightarrow A_f$ ponendo, per $u = a_0 x^n + \ldots + a_n \in A[x]$,*

$$\psi(u) := u\left(\frac{1_f}{f}\right) = \frac{(a_0)_f}{f^n} + \frac{(a_1)_f}{f^{n-1}} + \ldots + (a_n)_f$$
$$= \frac{(a_0 + a_1 f + \ldots + a_n f^n)_f}{f^n}$$

Allora $\operatorname{Ker}\psi = A[x]_\smile(fx-1)$.

Dimostrazione. (1) È chiaro che ψ è un omomorfismo di A-algebre, ad es. usando l'idea della def. 4.8 considerando A_f come A-modulo, cosicché ψ diventa semplicemente l'operatore di evaluazione di un polinomio in $\frac{1_f}{f}$.

(2) È chiaro anche che $fx - 1 \in \operatorname{Ker}\psi$.

Infatti $\psi(fx-1) = \frac{(f-f)_f}{f} = 0$.

(3) Sia $u \in \operatorname{Ker}\psi$. Dimostriamo prima che esiste un $k \in \mathbb{N}$ tale che $f^k u \in A[x]_\smile(fx-1)$.

Con u come nell'enunciato abbiamo $(a_0 + a_1 f + \ldots + a_n f_n)_f = 0$, per cui esiste $m \in \mathbb{N}$ tale che

$$0 = f^m(a_0 + a_1 f + \ldots + a_n f^n) = a_0 f^m + a_1 f^{m+1} + \ldots + a_n f^{m+n} \quad (*)$$

Allora

$$f^{m+n}u = a_0 f^m f^n x^n + a_1 f^{m+1} f^{n-1} x^{n-1} + \ldots + a_{n-1} f^{m+n-1} fx + a_n f^{m+n}$$

e quindi $f^{m+n}u = v(fx)$ con

$$v := a_0 f^m x^n + a_1 f^{m+1} x^{n-1} + \ldots + a_{n-1} f^{m+n-1} x + a_n f^{m+n} \in A[x]$$

Per la relazione (*) abbiamo $v(1) = 0$, cosicché dalla nota 5.2 segue che esiste un polinomio $q \in A[x]$ tale che $v = (x-1)q$.

Allora però $f^{m+n}u = v(fx) = (fx-1)q(fx) \in A[x]_\smile(fx-1)$.

(4) Siano $u \in \operatorname{Ker}\psi$ ed m, n come al punto (3).

Con $k := m + n$ abbiamo allora $f^k u \in A[x]_\smile(fx-1) =: J$. Dobbiamo dimostrare che $u \in J$.

Però $1 = fx - (fx-1)$ e con $I := A[x]_\smile(f)$ abbiamo $A = I + J$.

Dal lemma 2.15 segue $A = I^k + J$.

Siccome $uf^k \in J$ implica $uI^k \subset J$ (per l'es. 2.12), dalla prop. 2.16 segue $u \in J$.

Proposizione 6.30. *L'omomorfismo ψ del lemma 6.29 induce un isomorfismo naturale di A-algebre*

$$A_f \cong A[x]/(fx-1)$$

Dimostrazione. Siccome $\operatorname{Ker}\psi = A[x]_\smile(fx-1)$, è sufficiente verificare che ψ è suriettivo.

Ma ciò è ovvio, perché per ogni $a \in A$ e per ogni $n \in \mathbb{N}$ abbiamo $\frac{a_f}{f^n} = \psi(ax^n)$. Cfr. Reid [16215], 86-87.

Esempio 6.31. Sia $b \in \mathbb{Z} \setminus 0$. Allora esistono isomorfismi naturali

$$\left\{ \frac{a}{b^k} \mid a \in \mathbb{Z}, k \in \mathbb{N} \right\} \cong \mathbb{Z}_b \cong \mathbb{Z}[x]/(bx-1)$$

Esempio 6.32. Siano K un campo e $f \in K[x_1, \ldots, x_n] \setminus 0$. Allora esiste un isomorfismo naturale di K-algebre

$$K[x_1, \ldots, x_n]_f \cong K[x_1, \ldots, x_{n+1}]/(fx_{n+1} - 1)$$

Nota 6.33. L'isomorfia $A_f \cong A[x]/(fx-1)$ nella prop. 6.30 è molto simile alla costruzione algebrica dei numeri complessi in cui si pone $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$, presenta però, nel caso generale, anche un'importante differenza.

(1) Lo scopo della costruzione di A_f è di poter calcolare con un'inversa (in un certo senso *„immaginaria“*) di f che potremmo (solo nell'ambito di questa nota) denotare con f^{-1}, ponendo $f^{-1} := x \mod (fx-1)$.

Allora $A[x]/(fx-1) = A[f^{-1}]$ e ogni elemento di $A[f^{-1}]$ è della forma $a_0(f^{-1})^n + a_1(f^{-1})^{n-1} + \ldots + a_n$ con $a_0, \ldots, a_n \in A$. Così come in $\mathbb{C}$, posto $i := x \mod (x^2+1)$, si calcola seconda la regola $i^2 + 1 = 0$, così in $A[f^{-1}]$ si calcola secondo la regola $f \cdot f^{-1} = 1$.

(2) Esiste però una differenza che rende un po' meno trasparente e meno facile da maneggiare la costruzione di A_f: Mentre possiamo considerare il campo dei numeri reali in modo naturale come sottocampo di $\mathbb{C}$, non posssiamo, nel caso generale, considerare A come sottoanello di A_f. Infatti l'omomorfismo $i_f : A \longrightarrow A_f$ della prop. 6.18 è iniettivo solo se $\Omega = 0$.

Quindi non possiamo identificare a con a_f; infatti si ha $a_f = b_f$ se e solo se $a - b \in \Omega$, come abbiamo già visto nell'oss. 6.11.

(3) Nel caso che A sia integro invece la situazione è addirittura più agevole di quanto lo sia nel caso dei numeri complessi. Infatti allora possiamo identificare l'elemento simbolico f^{-1} con il reciproco concreto $\frac{1}{f}$ calcolato nel campo dei quozienti $\mathcal{K}(A)$. In quel caso inoltre $\Omega = 0$, cosicché l'anello A è un sottoanello di A_f (cfr. nota 6.22).

7. Estensioni di campi

La notazione $E : K$. Grado (dimensione) di un'estensione. Elementi algebrici e trascendenti. Estensioni algebriche. Campi intermedi. $K[\alpha]$ e $K(\alpha)$. L'ideale primo $\mathcal{J}(\alpha)$. Il polinomio minimale di un elemento algebrico e sue caratterizzazioni. α è algebrico se e solo se $K[\alpha]$ è un campo (che in tal caso coincide con $K(\alpha)$). Se α è trascendente, si ha invece $K[\alpha] \cong K[x]$. Se α è algebrico e di grado n, allora gli elementi $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ sono tutti distinti e costituiscono una base di $K(\alpha)$. α è quindi algebrico se e solo $|K(\alpha) : K| < \infty$. Un'estensione di campi di dimensione finita è algebrica. Teorema della moltiplicazione dei gradi. L'estensione $E : K$ è di dimensione finita se e solo se può essere ottenuta tramite l'aggiunzione di un numero finito di elementi algebrici. Gli elementi algebrici costituiscono un campo. Se le estensioni $E : L$ ed $L : K$ sono algebriche, anche $E : K$ è algebrica. Campi algebricamente chiusi. K è algebricamente chiuso se e solo se non ammette estensioni algebriche non banali. Come questa proprietà verrà usata nella dimostrazione del teorema degli zeri.

Definizione 7.1. Un'*estensione di campi* è una coppia (E, K) di campi in cui K è un sottocampo di E. Invece di (E, K) scriviamo $E : K$ (pronunciato „E *su* K“), come d'uso nella letteratura.

Useremo continuamente che in questa situazione E è uno spazio vettoriale su K. La dimensione (possibilmente infinita) $\dim_K E = |E : K|$ (cfr. def. 4.16) si chiama anche il *grado* dell'estensione.

Situazione 7.2. Siano $E : K$ un'estensione di campi ed $\alpha, \beta, \ldots \in E$.

Definizione 7.3. α si dice *algebrico* su K, se esiste un polinomio $f \in K[x] \setminus 0$ tale che $f(\alpha) = 0$. α si dice *trascendente* su K, se α non è algebrico su K.

Poniamo $\mathrm{Alg}(E : K) := \{\alpha \in E \mid \alpha \text{ è algebrico su } K\}$.

Definizione 7.4. L'estensione $E : K$ si dice *algebrica* (ed E si dice algebrico su K) se ogni elemento di E è algebrico su K.

Definizione 7.5. Un *campo intermedio* di $E : K$ è un campo L che è sottocampo di E e contiene K. Insiemisticamente si ha quindi $K \subset L \subset E$.

Denotiamo con $\mathrm{Inter}(E : K)$ l'insieme dei campi intermedi di $E : K$.

Il concetto di campo intermedio è fondamentale nella teoria di Galois, nella quale si utilizza la teoria dei gruppi per descrivere $\mathrm{Inter}(E : K)$.

Nota 7.6. Dimostreremo nel teorema 7.26 che $\mathrm{Alg}(E : K)$ è un campo, cioè che, se α e β sono algebrici su K, allora anche $\alpha \pm \beta$, $\alpha\beta$, $\alpha\beta^{-1}$ (per $\beta \neq 0$) sono algebrici su K.

La dimostrazione non è immediata e richiede l'uso sistematico delle idee dell'algebra lineare.

Evidentemente $K \subset \mathrm{Alg}(E : K) \subset E$.

Osservazione 7.7. Le notazioni $K[\alpha]$ e $K(\alpha)$ sono già state introdotte nelle def. 4.9 e 4.11.

$K[\alpha]$ è il più piccolo sottoanello di E che contiene sia K che α.

$K(\alpha)$ è il più piccolo sottocampo di E che contiene sia K che α e quindi, come già osservato nella def. 4.11,

$$K(\alpha) = \mathcal{K}(K[\alpha]) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f, g \in K[x] \text{ con } g(\alpha) \neq 0 \right\}$$

Ricordiamo che invece (o come caso speciale)

$$K(x) = \mathcal{K}(K[x]) = \left\{ \frac{f}{g} \mid f, g \in K[x] \text{ con } g \neq 0 \right\}$$

Osservazione 7.8. Usiamo l'abbreviazione

$$\mathcal{J}(\alpha) := \mathcal{J}(\{\alpha\}, \text{in } K[x]) = \{f \in K[x] \mid f(\alpha) = 0\}$$

Attenzione: A differenza dalla situazione considerata nel capitolo 8 in genere α non è elemento di K e quindi non possiamo scrivere $\mathcal{J}(\alpha) = K[x]_\smile(x - \alpha)$.

Proposizione 7.9. *$\mathcal{J}(\alpha)$ è un ideale primo di $K[x]$.*

Dimostrazione. Immediata.

Osservazione 7.10. α è trascendente su K se e solo se $\mathcal{J}(\alpha) = 0$.

Proposizione 7.11. *Esistono solo due possibilità:*

(1) $\mathcal{J}(\alpha) = 0$ (e quindi α è trascendente su K).

(2) Esiste un polinomio irriducibile $f \in K[x]$ (che possiamo scegliere normato) tale che $\mathcal{J}(\alpha) = K[x]_\smile(f)$.

Nel secondo caso α è algebrico su K.

Dimostrazione. Ciò viene dimostrato nel corso di Algebra, usando il fatto che $K[x]$ è un anello ad ideali principali.

Nota 7.12. Sia $\alpha \in \text{Alg}(E : K)$. Come già osservato nella prop. 7.11, allora $\mathcal{J}(\alpha) = K[x]_\smile(f)$ per un polinomio irriducibile $f \in K[x]$.

Se f_1 è un altro polinomio con $\mathcal{J}(\alpha) = K[x]_\smile(f_1)$, allora $f = f_1 u$ per un polinomio u invertibile in $K[x]$. Ma allora u è una costante $\neq 0$ e vediamo che esiste un unico polinomio irriducibile *normato* in $K[x]$ che genera $\mathcal{J}(\alpha)$.

Questo polinomio si chiama il *polinomio minimale* di α e viene denotato con $\pi_{\alpha:K}$.

Proposizione 7.13. *Siano $\alpha \in \text{Alg}(E : K)$ ed $f \in K[x]$ un polinomio normato. Allora sono equivalenti:*

(1) $f = \pi_{\alpha:K}$.

(2) $\mathcal{J}(\alpha) = K[x]_\smile(f)$.

(3) f è irriducibile in $K[x]$ ed $f(\alpha) = 0$.

(4) $f(\alpha) = 0$ ed f possiede grado minimo tra gli elementi $\neq 0$ di $\mathcal{J}(\alpha)$.

Dimostrazione. Corso di Algebra. Facile.

Definizione 7.14. Sia $\alpha \in \text{Alg}(E : K)$. Allora il grado del polinomio $\pi_{\alpha:K}$ è detto anche grado di α su K e viene denotato con $|\alpha : K|$.

Quindi $|\alpha : K| = \text{grado}\, \pi_{\alpha:K}$.

Osservazione 7.15. L'applicazione $\theta_\alpha := \bigcirc_f f(\alpha) : K[x] \longrightarrow K[\alpha]$ è un omomorfismo suriettivo di anelli con $\operatorname{Ker}\theta_\alpha = \mathcal{J}(\alpha)$; cfr. lemma 4.13.

Abbiamo quindi un isomorfismo naturale $K[\alpha] \cong K[x]/\mathcal{J}(\alpha)$.

Teorema 7.16. *Sono equivalenti:*

(1) $\alpha \in \operatorname{Alg}(E : K)$.

(2) $K[\alpha]$ *è un campo.*

(3) $K[\alpha] = K(\alpha)$.

Dimostrazione. Usiamo l'isomorfismo $K[\alpha] \cong K[x]/\mathcal{J}(\alpha)$ dell'oss. 7.15.

(1) $\implies$ (2): Per ipotesi $\mathcal{J}(\alpha) \neq 0$. Sappiamo dalla prop. 7.9 che $\mathcal{J}(\alpha)$ è un ideale primo di $K[x]$ e dal corso di Algebra che ogni ideale primo $\neq 0$ di $K[x]$ è massimale. Perciò $K[x]/\mathcal{J}(\alpha)$ è un campo e quindi anche $K[\alpha]$ è un campo.

(2) $\implies$ (3): Per definizione (oss. 7.7) $K(\alpha) = \mathcal{K}(K[\alpha])$. Se $K[\alpha]$ è un campo, ciò implica $K(\alpha) = K[\alpha]$.

(3) $\implies$ (1): Se $K[\alpha] = K(\alpha)$, allora $\mathcal{J}(\alpha)$ deve essere un ideale massimale di $K[x]$ e quindi necessariamente $\mathcal{J}(\alpha) \neq 0$.

Proposizione 7.17. *Sono equivalenti:*

(1) α *è trascendente su* K.

(2) $K[\alpha] \cong K[x]$.

In questo caso $K(\alpha) \cong K(x)$.

Dimostrazione. (1) $\implies$ (2): Dall'oss. 7.15 abbiamo ancora $K[\alpha] \cong K[x]/\mathcal{J}(\alpha)$. Però se α è trascendente su K, allora $\mathcal{J}(\alpha) = 0$ e quindi $K[\alpha] \cong K[x]$.

(2) $\implies$ (1): Se viceversa $K[\alpha] \cong K[x]$, allora $K[\alpha]$ non può essere un campo e quindi α è trascendente per il teorema 7.16.

Se infine $K[\alpha] \cong K[x]$, allora anche

$$K(\alpha) = \mathcal{K}(K[\alpha]) \cong \mathcal{K}(K[x]) = K(x)$$

Teorema 7.18. *Siano* $\alpha \in \operatorname{Alg}(E : K)$ *ed* $n := |\alpha : K|$. *Allora:*

(1) Gli elementi $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ *sono tutti distinti e costituiscono una base di* $K(\alpha)$ *su* K.

(2) $|K(\alpha) : K| = n$.

(3) In particolare quindi $|K(\alpha) : K| < \infty$.

Dimostrazione. È sufficiente dimostrare il punto (1).

Per ipotesi $\pi_{\alpha:K} = x^n + a_1 x^{n-1} + \ldots + a_n$ con $a_1, \ldots, a_n \in K$.

Allora $\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0$ e quindi $\alpha^n = -(a_1\alpha^{n-1} + \ldots + a_n)$.
È chiaro che ciò implica che $1, \alpha, \ldots, \alpha^{n-1}$ generano $K[\alpha]$. Ma per il teorema 7.16 $K[\alpha] = K(\alpha)$.

Rimane quindi solo da dimostrare che gli elementi $1, \alpha, \ldots, \alpha^{n-1}$ sono linearmente indipendenti su K.

Sia $d_0 + d_1\alpha + \ldots + d_{n-1}\alpha^{n-1} = 0$ con $d_0, \ldots, d_{n-1} \in K$.

Allora $g := d_0 + d_1 x + \ldots + d_{n-1}x^{n-1} \in \mathcal{J}(\alpha)$.

Siccome $\operatorname{grado} g < n$, dalla prop. 7.13 segue $g = 0$.

Ma ciò significa che $d_0 = d_1 = \ldots = d_{n-1} = 0$.

Corollario 7.19. *Sono equivalenti:*

(1) $\alpha \in \operatorname{Alg}(E : K)$.

(2) $|K(\alpha) : K| < \infty$.

Dimostrazione. (1) $\implies$ (2): Teorema 7.18.

(2) $\implies$ (1): Sia $m := |K(\alpha) : K|$. Allora gli elementi $1, \alpha, \ldots, \alpha^m$ (tutti appartenenti a $K(\alpha)$) sono linearmente dipendenti, perciò esistono coefficienti $a_0, \ldots, a_m \in K$ non tutti nulli tali che $a_0 + a_1\alpha + \ldots + a_m\alpha^m = 0$.

Con $g := a_0 + a_1 x + \ldots + a_m x^m$ abbiamo allora trovato un elemento $\neq 0$ di $\mathcal{J}(\alpha)$.

Corollario 7.20. *Sono equivalenti:*

(1) α *è trascendente su* K.

(2) Gli elementi $1, \alpha, \alpha^2, \ldots$ *sono linearmente indipendenti su* K.

(3) $|K(\alpha) : K| = \infty$.

Corollario 7.21. E *contenga un elemento trascendente su* K.

Allora $|E : K| = \infty$.

Dimostrazione. Sia $\alpha \in E$ trascendente su K. Allora

$$|E : K| \geq |K(\alpha) : K| \overset{7.20}{=} \infty$$

Corollario 7.22. *Un'estensione di campi di dimensione finita è algebrica.*

Corollario 7.23. *Sia* $\alpha \in \operatorname{Alg}(E : K)$. *Allora l'estensione* $K(\alpha) : K$ *è algebrica.*

Dimostrazione. Per il cor. 7.19 $|K(\alpha) : K| < \infty$, cosicché l'enunciato segue dal cor. 7.22.

Proposizione 7.24 (teorema della moltiplicazione dei gradi).
Sia $L \in \operatorname{Inter}(E : K)$.

(1) Se $|L : K| < \infty$ *e* $|E : K| < \infty$, *allora* $|E : K| = |E : L||L : K|$.

In particolare in questo caso $|E : K| < \infty$.

(2) Sia $|E : K| < \infty$. *Allora* $|L : K| \leq |E : K|$ *e* $|E : L| \leq |E : K|$.

Dimostrazione. (1) $e_1, \ldots, e_r$ sia una base di $L : K$ e $d_1, \ldots, d_s$ una base di $E : L$. Si dimostra facilmente che gli rs elementi $e_i d_j$ per $1 \leq i \leq r$ e $1 \leq j \leq s$ sono tutti distinti e formano una base di $E : K$.

(2) Sia $|E : K| < \infty$. Ogni sistema di generatori per $E : K$ è anche un sistema di generatori per $E : L$, per cui $|E : L| \leq |E : K|$.

Ogni base di $L : K$ consiste di elementi di E linearmente indipendenti su K e ciò implica $|L : K| \leq |E : K|$.

Proposizione 7.25. *Sono equivalenti:*

(1) $|E : K| < \infty$.

(2) Esistono $\alpha_1, \ldots, \alpha_m \in \mathrm{Alg}(E : K)$ *tali che* $E = K(\alpha_1, \ldots, \alpha_m)$.

Dimostrazione. (1) $\implies$ (2): $\alpha_1, \ldots, \alpha_m$ sia una base di $E : K$. Ogni elemento di E è allora una combinazione lineare degli α_j con coefficienti in K e appartiene quindi a $K(\alpha_1, \ldots, \alpha_m)$.

(2) $\implies$ (1): Ponendo $L_0 := K$ e $L_i := K(\alpha_1, \ldots, \alpha_i) = L_{i-1}(\alpha_i)$ per $i = 1, \ldots, m$, abbiamo una catena di campi

$$L_0 \subset L_1 \subset \ldots L_{m-1} \subset L_m = E$$

Ogni α_i è per ipotesi algebrico su K e quindi anche su L_{i-1}. Dal teorema 7.18 segue $|L_i : L_{i-1}| = |L_{i-1}(\alpha_i) : L_{i-1}| < \infty$ per ogni i, cosicché per il teorema della moltiplicazione dei gradi si ha $|E : K| < \infty$.

Teorema 7.26. $\mathrm{Alg}(E : K)$ *è un campo.*

Dimostrazione. Dalla prop. 7.25 segue che per $\alpha, \beta \in \mathrm{Alg}(E : K)$ si ha $|K(\alpha, \beta) : K| < \infty$, cosicché dal cor. 7.22 segue che ogni elemento di $K(\alpha, \beta)$ è algebrico su K e quindi in particolare lo sono gli elementi $\alpha \pm \beta$, $\alpha\beta$ e $\alpha\beta^{-1}$ (per $\beta \neq 0$).

Teorema 7.27. *Sia* $L \in \mathrm{Inter}(E : K)$. *Le estensioni* $L : K$ *ed* $E : L$ *siano algebriche. Allora anche* $E : K$ *è algebrica.*

Dimostrazione. Siano $\alpha \in E$ e $\pi_{\alpha:L} = x^m + \rho_1 x^{m-1} + \ldots + \rho_m$. Allora α è algebrico su $K(\rho_1, \ldots, \rho_m)$!

Perciò $|K(\rho_1, \ldots, \rho_m, \alpha) : K(\rho_1, \ldots, \rho_m)| < \infty$.

Però $\rho_1, \ldots, \rho_m$ appartengono ad L e per ipotesi questi elementi sono algebrici su K. Dalla prop. 7.25 segue che $|K(\rho_1, \ldots, \rho_m) : K| < \infty$. Dal teorema della moltiplicazione dei gradi otteniamo adesso

$$\begin{aligned} |K(\alpha) : K| &\leq |K(\rho_1, \ldots, \rho_m, \alpha) : K| \\ &\leq |K(\rho_1, \ldots, \rho_m, \alpha) : K(\rho_1, \ldots, \rho_m)||K(\rho_1, \ldots, \rho_m : K| < \infty \end{aligned}$$

Definizione 7.28. Un campo K si dice *algebricamente chiuso*, se ogni polinomio non costante $f \in K[x]$ possiede una radice in K.

È chiaro che è sufficiente chiedere l'esistenza di una radice per ogni polinomio non costante irriducibile in $K[x]$.

Proposizione 7.29. *Per un campo* K *sono equivalenti:*

(1) K *è algebricamente chiuso.*

(2) Ogni polinomio irriducibile normato (e quindi non costante) in $K[x]$ *è della forma* $x - \alpha$ *con* $\alpha \in K$.

(3) Se $F : K$ *è un'estensione di campi algebrica, allora* $F = K$.

Dimostrazione. (1) $\implies$ (2): Sia $f \in K[x]$ irriducibile e normato. Per ipotesi esiste $\alpha \in K$ con $f(\alpha) = 0$.

Per il cor. 5.4 esiste $g \in K[x]$ tale che $f = (x - \alpha)g$. Ma g deve essere costante, altrimenti f non sarebbe irriducibile. Siccome f è normato, $g = 1$ e quindi $= x - \alpha$.

(2) $\implies$ (3): Siano $F : K$ un'estensione di campi algebrica ed $\alpha \in F$. Per ipotesi α è algebrico su K e per l'ipotesi (2) abbiamo $\pi_{\alpha:K} = x - \beta$ per qualche $\beta \in K$. Però $\alpha - \beta = \pi_{\alpha:K}(\alpha) = 0$, per cui $\alpha = \beta \in K$.

(3) $\implies$ (1): Sia $f \in K[x]$ un polinomio non costante. Possiamo assumere che f sia irriducibile e normato. Dal corso di Algebra sappiamo che esistono un'estensione di campi algebrica $F : K$ ed $\alpha \in F$ tali che $f(\alpha) = 0$ ed $F = K(\alpha)$. Per ipotesi però $F = K$ e ciò implica $\alpha \in K$.

Osservazione 7.30. Nelle dimostrazioni del teorema degli zeri, dato un ideale I di $K[x_1, \ldots, x_n]$, dimostreremo prima che esiste un campo E contenente K (o una sua copia isomorfa $\overline{K}$) come sottocampo tale che $\mathrm{Zeri}(I, \text{in } E^n) \neq \emptyset$. Ciò non sarà difficile.

Poi, e questa parte è molto meno facile, dimostreremo che l'estensione $E : K$ è algebrica. Se K è algebricamente chiuso, per la prop. 7.29 ciò implica $E = K$ (più precisamente $E = \overline{K}$), cosicché abbiamo effettivamente trovato radici di I in K^n.

8. Il principio di identificazione a posteriori

Come identificare un polinomio costante con il suo coefficiente costante. Sopra un anello integro A il grado del prodotto di due polinomi $\neq 0$ è la somma dei loro gradi e un polinomio è invertibile se e solo se è costante e invertibile in A.
K come sottoanello di $K[x_1, \ldots, x_n]/I$. La relazione magica $\overline{f} = f(\overline{x_1}, \ldots, \overline{x_n})$.
Per $f \in I$ si ha quindi $f(\overline{x_1}, \ldots, \overline{x_n}) = 0$.

Osservazione 8.1. Scopo di questo capitolo è di chiarire un meccanismo di identificazione che è ovvio da un lato, ma pone, se si vuole essere rigorosi, alcuni problemi di notazione. Una volta capito il principio però si può lavorare sempre con questa identificazione, semplificando notevolmente la scrittura. Lo spiegheremo in due situazioni diverse, prima nel caso quasi ovvio dell'identificazione di un polinomio costante con il proprio coefficiente costante, poi nel caso più delicato, ma ricorrente molto spesso in pratica, dell'immersione di un campo K in un'algebra polinomiale $K[\alpha_1, \ldots, \alpha_n]$.

Nota 8.2. Sia A un anello commutativo. Un polinomio nelle indeterminate $x_1, \ldots, x_n$ con coefficienti in A è, nella definizione più rigorosa, una coppia $f = ((x_1, \ldots, x_n), v)$ in cui $v \in A^{\mathbb{N}^n}$ è una multisuccessione nella quale solo per un numero finito di multiindici $(k_1, \ldots, k_n)$ il coefficiente $v(k_1, \ldots, k_n)$ è diverso da 0.

Simbolicamente si scrive allora $f = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^n} v(k_1, \ldots, k_n) x_1^{k_1} \cdots x_n^{k_n}$.
I calcoli vengono poi eseguiti come se le variabili x_j facessero parte di un anello commutativo di cui A è sottoanello. Con queste operazioni i polinomi formano un anello commutativo che denotiamo con $A[x_1, \ldots, x_n]$.

Naturalmente bisogna scegliere le indeterminate x_j in modo che siano completamente estranee agli altri oggetti che consideriamo. Realizzare ciò in modo formale è in verità un po' laborioso, ma significa semplicemente che le operazioni vengono effettuate direttamente sulla multisuccessione v e solo in un secondo momento si usano le variabili per denominare il polinomio ottenuto in modo più intuitivo. Nel caso $n = 1$ invece di x_1 useremo spesso l'indeterminata x.

Diamo questa parte adesso per scontata.

Definizione 8.3. Nella situazione della nota 8.2 il polinomio f si chiama *costante*, se $v(k_1, \ldots, k_n) = 0$ per ogni multiindice $(k_1, \ldots, k_n) \neq (0, \ldots, 0)$.

L'elemento $v(0, \ldots, 0)$ di A si chiama il *coefficiente costante* di f.

Nota 8.4. Sempre nella situazione della nota 8.2 possiamo considerare l'applicazione $j : A \longrightarrow A[x_1, \ldots, x_n]$ definita come l'applicazione che manda ogni elemento $a \in A$ nel polinomio costante (univocamente determinato) il cui coefficiente costante è uguale ad a.

È immediato che j è un omomorfismo iniettivo di anelli e ciò ci permette di identificare ogni polinomio costante con il suo coefficiente costante e di considerare uguali, *a posteriori*, l'anello di base A e il sottoanello dei polinomi costanti di $A[x_1, \ldots, x_n]$. In questo modo (tenendo presenti i non pochi passaggi di identificazione) possiamo da ora in avanti considerare A come sottoanello di $A[x_1, \ldots, x_n]$.

Lemma 8.5. *Siano A un anello integro ed $f, g \in A[x] \setminus 0$.*

Allora $\text{grado}\, fg = \text{grado}\, f + \text{grado}\, g$.

Dimostrazione. Immediata.

Corollario 8.6. *Siano A un anello integro ed $f \in A[x]$.*

Allora f è invertibile in $A[x]$ se e solo se f è costante ed invertibile in A.

Dimostrazione. (1) È chiaro che un polinomio costante invertibile in A è invertibile anche in $A[x]$.

(2) Sia $g \in A[x]$ tale che $fg = 1$. Allora $f, g \neq 0$ e dal lemma 8.5 segue $\text{grado}\, f + \text{grado}\, g = 0$. Ma ciò è possibile solo se $\text{grado}\, f = \text{grado}\, g = 0$, per cui f e g devono essere costanti $\neq 0$, l'una reciproca dell'altra.

Corollario 8.7. *Siano K un campo ed $f \in K[x_1, \ldots, x_n]$.*

Allora f è invertibile in $K[x_1, \ldots, x_n]$ se e solo se f è costante e $\neq 0$.

Dimostrazione. Ciò segue dal cor. 8.6 tramite induzione su n.

Nota 8.8. Siano K un campo ed I un ideale di $K[x_1, \ldots, x_n]$. Per $f \in K[x_1, \ldots, x_n]$ denotiamo con $\overline{f}$ la classe di f in $K[x_1, \ldots, x_n]/I$.

Allora l'omomorfismo $\rho := \bigcirc_a \overline{a} : K \longrightarrow K[x_1, \ldots, x_n]/I$ è iniettivo. Ciò segue dall'oss. 4.4 oppure anche direttamente dal fatto che per $a, b \in K$ l'uguaglianza $\overline{a} = \overline{b}$ significa $a - b \in I$; la costante $a - b$ non può quindi essere invertibile in $K[x_1, \ldots, x_n]$ e quindi nemmeno in K e ciò implica $a = b$.

Possiamo quindi usare ρ per identificare gli elementi $\overline{a}$ per $a \in K$ con le costanti a stesse e considerare quindi anche stavolta uguali, *a posteriori*, il campo base K e l'insieme $\{\overline{a} \mid a \in K\}$ di $K[x_1, \ldots, x_n]/I$.

Quindi da ora in avanti possiamo considerare K come sottocampo dell'anello $K[x_1, \ldots, x_n]/I$ e scrivere ad esempio $f(\alpha_1, \ldots, \alpha_n)$ quando dovremmo scrivere, per $f \in K[x_1, \ldots, x_n]$, più precisamente $f(\overline{\alpha_1}, \ldots, \overline{\alpha_n})$.

Osservazione 8.9. Siano A un anello ed I un ideale di $A[x_1, \ldots, x_n]$. Per $f \in A[x_1, \ldots, x_n]$ come in precedenza denotiamo con $\overline{f}$ la classe di f in $A[x_1, \ldots, x_n]/I$.

Allora $\overline{f} = f(\overline{x_1}, \ldots, \overline{x_n})$.

Dimostrazione. Questa osservazione è quasi ovvia, ma fondamentale per tutta la teoria. Essa deriva semplicemente dal fatto che l'operazione $f \longmapsto \overline{f}$ è un omomorfismo di anelli, per cui per $f = \sum_{k_1, \ldots, k_n} a_{k_1 \ldots k_n} x_1^{k_1} \cdots x_n^{k_n}$ si ha

$$\overline{f} = \overline{\sum_{k_1, \ldots, k_n} a_{k_1 \ldots k_n} x_1^{k_1} \cdots x_n^{k_n}} = \sum_{k_1, \ldots, k_n} a_{k_1 \ldots k_n} \overline{x_1}^{k_1} \cdots \overline{x_n}^{k_n} = f(\overline{x_1}, \ldots, \overline{x_n})$$

Corollario 8.10. *Nella situazione e con la notazione dell'oss. 8.9 sia $f \in I$.*

Allora $f(\overline{x_1}, \ldots, \overline{x_n}) = 0$.

9. La forma astratta del teorema degli zeri

Con $\mathfrak{m} \in \operatorname{Max} K[x_1, \ldots, x_n]$ ed $E := K[x_1, \ldots, x_n]/\mathfrak{m}$ abbiamo sempre $(\overline{x_1}, \ldots, \overline{x_n}) \in \operatorname{Zeri}(\mathfrak{m}, \operatorname{in} E^n)$ e quindi $\operatorname{Zeri}(\mathfrak{m}, \operatorname{in} E^n) \neq \emptyset$. Se K è algebricamente chiuso e se riusciamo a dimostrare che l'estensione $E : K$ è algebrica, abbiamo dimostrato che $\operatorname{Zeri}(\mathfrak{m}, \operatorname{in} K^n) \neq \emptyset$. Un ideale massimale $\mathfrak{m}$ di $K[x_1, \ldots, x_n]$ non possiede più di uno zero in K^n. Se $\operatorname{Zeri}(\mathfrak{m}) \neq \emptyset$, allora $\mathcal{J}(\operatorname{Zeri}(\mathfrak{m})) = \mathfrak{m}$. Una formulazione ancora più concreta dell'idea della dimostrazione del teorema degli zeri: $K[x_1, \ldots, x_n]/\mathfrak{m} = K$ significa che esistono $\alpha_1, \ldots, \alpha_n \in K$ t.c. $x_i - \alpha_i \in \mathfrak{m}$ per ogni i e allora $\mathfrak{m} = \mathfrak{m}_{\alpha_1, \ldots, \alpha_n}$ e $\operatorname{Zeri}(\mathfrak{m}) = \{(\alpha_1, \ldots, \alpha_n)\}$.

Situazione 9.1. Sia K un campo.

Per un ideale massimale $\mathfrak{m}$ di $K[x_1, \ldots, x_n]$ denotiamo, come in precedenza, con $\overline{f}$ la classe di f in $K[x_1, \ldots, x_n]/\mathfrak{m}$.

Usiamo anche le notazioni della def. 1.19.

Nota 9.2. Siano $\mathfrak{m} \in \operatorname{Max} K[x_1, \ldots, x_n]$ ed $E := K[x_1, \ldots, x_n]/\mathfrak{m}$. Allora E è un campo di cui (con l'identificazione del capitolo 8) K è un sottocampo.

Per il cor. 8.10 $f(\overline{x_1}, \ldots, \overline{x_n}) = 0$ per ogni $f \in \mathfrak{m}$, cosicché

$(\overline{x_1}, \ldots, \overline{x_n}) \in \operatorname{Zeri}(\mathfrak{m}, \operatorname{in} E^n)$

Ciò implica in particolare che $\operatorname{Zeri}(\mathfrak{m}, \operatorname{in} E^n) \neq \emptyset$.

Assumiamo adesso di sapere che

(1) K è algebricamente chiuso;

(2) $E : K$ è un'estensione algebrica.

Per la prop. 7.29 allora $E = K$ e quindi troviamo che $\operatorname{Zeri}(\mathfrak{m}, \operatorname{in} K^n) \neq \emptyset$.

Osservazione 9.3. Siano I un ideale di $K[x_1, \ldots, x_n]$ ed $\mathfrak{m} \in \operatorname{Max} K[x_1, \ldots, x_n]$ tali che $I \subset \mathfrak{m}$.

Allora $\operatorname{Zeri}(\mathfrak{m}) \subset \operatorname{Zeri}(I)$.

Per dimostrare che $\operatorname{Zeri}(I) \neq \emptyset$ è quindi sufficiente dimostrare che $\operatorname{Zeri}(\mathfrak{m}) \neq \emptyset$.

Osservazione 9.4. La nota 9.2 può essere considerata come una forma astratta del teorema degli zeri. Nei casi concreti bisogna poi dimostrare il punto (2) di quella nota, cioè che l'estensione $E : K$ è algebrica, come faremo nei prossimi capitoli.

Nel resto di questo capitolo vogliamo ancora dimostrare che un ideale massimale di $K[x_1, \ldots, x_n]$ non possiede più di uno zero in K^n. Usiamo come sempre la notazione abbreviata $\operatorname{Zeri}(\mathfrak{m}) = \operatorname{Zeri}(\mathfrak{m}, \operatorname{in} K^n)$.

Definizione 9.5. Nel resto del capitolo per $\alpha_1, \ldots, \alpha_n \in K$ poniamo

$\mathfrak{m}_{\alpha_1, \ldots, \alpha_n} := K[x_1, \ldots, x_n]_\smile(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$

Dalla prop. 5.7 sappiamo che $\mathfrak{m}_{\alpha_1, \ldots, \alpha_n} \in \operatorname{Max} K[x_1, \ldots, x_n]$.

Lemma 9.6. *Siano $\alpha_1, \ldots, \alpha_n \in K$. Allora:*

(1) $\operatorname{Zeri}(\mathfrak{m}_{\alpha_1, \ldots, \alpha_n}) = \{(\alpha_1, \ldots, \alpha_n)\}$.

(2) $\mathcal{J}(\{(\alpha_1, \ldots, \alpha_n)\}) = \mathfrak{m}_{\alpha_1, \ldots, \alpha_n}$.

Dimostrazione. (1) Ciò è chiaro perché (come già osservato nella nota 1.18)

$\mathrm{Zeri}(\mathfrak{m}_{\alpha_1,\dots,\alpha_n}) = \mathrm{Zeri}(x_1 - \alpha_1, \dots, x_n - \alpha_n) = \{(\alpha_1, \dots, \alpha_n)\}$.

(2) È chiaro che $\mathfrak{m} := \mathfrak{m}_{\alpha_1,\dots,\alpha_n} \subset \mathcal{J}(\{(\alpha_1, \dots, \alpha_n)\}) := I$.

Siccome per la prop. 5.7 $\mathfrak{m}$ è massimale ed $I \neq K[x_1, \dots, x_n]$, ciò implica $I = \mathfrak{m}$.

Proposizione 9.7. *Sia* $\mathfrak{m} \in \mathrm{Max}\, K[x_1, \dots, x_n]$.

Se $\mathrm{Zeri}(\mathfrak{m}) \neq \emptyset$*, allora esistono* $\alpha_1, \dots, \alpha_n \in K$ *tali che*

$\mathfrak{m} = \mathfrak{m}_{\alpha_1,\dots,\alpha_n} = K[x_1, \dots, x_n]_{\smile}(x_1 - \alpha_1, \dots, x_n - \alpha_n)$

e quindi, per il lemma 9.6,

$\mathrm{Zeri}(\mathfrak{m}) = \{(\alpha_1, \dots, \alpha_n)\}$

e in più

$\mathfrak{m} = \mathcal{J}(\{(\alpha_1, \dots, \alpha_n)\})$

L'insieme degli zeri in K^n *di un ideale massimale di* $K[x_1, \dots, x_n]$ *è quindi vuoto oppure un insieme che consiste di un punto solo.*

Dimostrazione. Sia $\mathrm{Zeri}(\mathfrak{m}) \neq \emptyset$. Allora esistono $\alpha_1, \dots, \alpha_n \in K$ tali che $(\alpha_1, \dots, \alpha_n) \in \mathrm{Zeri}(\mathfrak{m})$.

Ciò implica $\mathfrak{m} \subset \mathfrak{m}_{\alpha_1,\dots,\alpha_n}$ e dalla massimalità di $\mathfrak{m}$ segue $\mathfrak{m} = \mathfrak{m}_{\alpha_1,\dots,\alpha_n}$.

L'enunciato segue adesso dal lemma 9.6.

Corollario 9.8. *Sia* $\mathfrak{m} \in \mathrm{Max}\, K[x_1, \dots, x_n]$ *e sia* $\mathrm{Zeri}(\mathfrak{m}) \neq \emptyset$.

Allora $\mathcal{J}(\mathrm{Zeri}(\mathfrak{m})) = \mathfrak{m}$.

Nota 9.9. Con le ultime considerazioni possiamo formulare l'idea della dimostrazione del teorema degli zeri in modo forse ancora più concreto:

Sia $\mathfrak{m} \in \mathrm{Max}\, K[x_1, \dots, x_n]$ e assumiamo di sapere che $K[x_1, \dots, x_n]/\mathfrak{m} = K$.

Ciò implica che esistono $\alpha_1, \dots, \alpha_n \in K$ con $x_1 - \alpha_1 \in \mathfrak{m}, \dots, x_n - \alpha_n \in \mathfrak{m}$. Allora però $\mathfrak{m}_{\alpha_1,\dots,\alpha_n} \subset \mathfrak{m}$ e da ciò segue $\mathfrak{m} = \mathfrak{m}_{\alpha_1,\dots,\alpha_n}$ perché $\mathfrak{m}_{\alpha_1,\dots,\alpha_n}$ è massimale, come sappiamo dalla prop. 5.7.

Pertanto $\mathrm{Zeri}(\mathfrak{m}) = \{(\alpha_1, \dots, \alpha_n)\}$.

10. Il teorema degli zeri per $|\mathbf{K}| > |\mathbb{N}|$

$|K[x_1, \ldots, x_n]/I : K| \leq |\mathbb{N}|$. Se t è trascendente su K, allora l'insieme $\{\frac{1}{t-a} \mid a \in K\}$ è linearmente indipendente su K. Perciò, se K non è numerabile ed $\mathfrak{m}$ è un ideale massimale di $K[x_1, \ldots, x_n]$, allora l'estensione di campi $K[x_1, \ldots, x_n]/\mathfrak{m} : K$ deve essere algebrica; essa coincide quindi con K se K è anche algebricamente chiuso. Dalla forma astratta del teorema degli zeri segue che, se K è un campo algebricamente chiuso non numerabile ed I un ideale di $K[x_1, \ldots, x_n]$, allora $(\mathrm{Zeri}(I) \neq \emptyset$. Vedremo nel prossimo capitolo che la condizione che K non sia numerabile non è necessaria.

Nota 10.1. La dimostrazione del teorema degli zeri per un campo non numerabile è molto più semplice di quella nel caso generale che vedremo nel prossimo capitolo.

Il caso semplice però è altrettanto istruttivo e sarebbe da solo sufficiente per tutte le applicazioni in cui il campo di base è il campo dei numeri complessi, essendo questo algebricamente chiuso e non numerabile.

Seguiamo l'esposizione in Perrin [21031], 15-16.

Osservazione 10.2. Siano A un anello commutativo ed M un A-modulo, N un sotto-A-modulo di M.

Siano G un sistema generatore di M su A e $\overline{G} := \{(g, \mathrm{in}\, M/N) \mid g \in G\}$. Allora $\overline{G}$ è un sistema generatore di M/N su A.

In particolare $|M/N : A| \leq |M : A|$.

Dimostrazione. Per ogni $v \in M$ denotiamo con $\overline{v} := (v, \mathrm{in}\, M/N)$ la sua classe di equivalenza in M/N.

Ogni elemento $y \in M/N$ è della forma $y = \overline{x}$ per qualche $x \in M$. Per ipotesi esistono $g_1, \ldots, g_m \in G$ ed $a_1, \ldots, a_m \in A$ tali che $x = a_1 g_1 + \ldots + a_m g_m$. Ciò implica $y = a_1 \overline{g_1} + \ldots + a_m \overline{g_m}$.

Corollario 10.3. *Siano K un campo ed I un ideale di $K[x_1, \ldots, x_n]$.*

Allora $|K[x_1, \ldots, x_n]/I : K| \leq |\mathbb{N}|$.

Dimostrazione. $K[x_1, \ldots, x_n]$ come spazio vettoriale su K è generato dai monomi $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Questi costituiscono un insieme numerabile cosicché l'enunciato segue dall'oss. 10.2.

Lemma 10.4. *Siano E un campo, K un sottocampo di E e $t \in E$ trascendente su K. Siano $f \in K[x_1, \ldots, x_{n+1}]$ ed $a_1, \ldots, a_n \in K$ tali che $f(a_1, \ldots, a_n, t) = 0$.*

Allora $f(a_1, \ldots, a_n, x_{n+1}) = 0$ e quindi $f(a_1, \ldots, a_n, \alpha) = 0$ per ogni $\alpha \in E$.

Dimostrazione. Per qualche $m \in \mathbb{N}$ possiamo scrivere $f = \sum_{k=0}^{m} g_k x_{n+1}^k$ con i polinomi $g_k \in K[x_1, \ldots, x_n]$ univocamente determinati. Allora $f(a_1, \ldots, a_n, x_{n+1}) = \sum_{k=0}^{m} g_k(a_1, \ldots, a_n) x_{n+1}^k$.

Per ipotesi abbiamo $\sum_{k=0}^{m} g_k(a_1, \ldots, a_n) t^k = 0$. Siccome t è trascendente su K, ciò implica $g_k(a_1, \ldots, a_n) = 0$ per ogni k.

Lemma 10.5. *Siano E un campo, K un sottocampo di E e $t \in E$ trascendente su K. Allora l'insieme $\left\{ \frac{1}{t-a} \mid a \in K \right\}$ è linearmente indipendente su K.*

Dimostrazione. Infatti, se $\frac{\lambda_1}{t-a_1} + \ldots + \frac{\lambda_m}{t-a_m} = 0$ con $a_1, \ldots, a_m, \lambda_1, \ldots, \lambda_m \in K$ e gli $a_1, \ldots, a_m$ tutti distinti, allora

$$\sum_{k=0}^{m} \lambda_k (t-a_1) \cdots \widehat{(t-a_k)} \cdots (t-a_m) = 0$$

Per il lemma 10.4 possiamo sostituire t con a_1, ottenendo

$$\lambda_1 (a_1 - a_2) \cdots (a_1 - a_m) = 0$$

e ciò significa $\lambda_1 = 0$. Nello stesso modo si vede che $\lambda_i = 0$ per $i = 2, \ldots, m$.

Corollario 10.6. *Siano K un campo algebricamente chiuso non numerabile ed E un campo che contiene K come sottocampo tale che $|E : K| \leq \mathbb{N}$.*

Allora $E = K$.

Dimostrazione. Siccome K è algebricamente chiuso, per la prop. 7.29 è sufficiente dimostrare che E è algebrico su K.

Ma E non può contenere un elemento t trascendente su K perché altrimenti, per il lemma 10.5, l'insieme non numerabile $\left\{ \frac{1}{t-a} \mid a \in K \right\}$ sarebbe linearmente indipendente su K, in contrasto con l'ipotesi sulla dimensione $|E : K|$.

Teorema 10.7 (teorema degli zeri per un campo non numerabile). *Siano K un campo algebricamente chiuso non numerabile ed I un ideale di $K[x_1, \ldots, x_n]$.*

Allora $\mathrm{Zeri}(I) \neq \emptyset$.

Dimostrazione. Sappiamo che I è contenuto in un ideale massimale $\mathfrak{m}$. Siccome $\mathrm{Zeri}(\mathfrak{m}) \subset \mathrm{Zeri}(I)$, è sufficiente dimostrare che $\mathrm{Zeri}(\mathfrak{m}) \neq \emptyset$.

L'anello $E := K[x_1, \ldots, x_n]/\mathfrak{m}$ è un campo. Come nei capitoli precedenti possiamo considerare K come sottocampo di E e dal cor. 10.3 sappiamo che $|E : K| \leq |\mathbb{N}|$.

Per il cor. 10.6 allora $E = K$. Dalla nota 9.2 (o in modo più concreto usando come nella nota 9.9 il fatto che l'uguaglianza $E = K$ implica che $\mathfrak{m} = \mathfrak{m}_\alpha$ per un punto $\alpha \in K^n$) segue che $\mathrm{Zeri}(\mathfrak{m}) \neq \emptyset$.

Nota 10.8. Attenzione: Il teorema 10.7 non implica il teorema fondamentale dell'algebra! Infatti nell'ipotesi dobbiamo supporre che K sia già algebricamente chiuso. Si tratta invece di una generalizzazione a più dimensioni: *Se il campo K è tale che ogni polinomio non costante in $K[x]$ possiede una radice in K (cioè se K è algebricamente chiuso), allora anche ogni ideale di $K[x_1, \ldots, x_n]$ ha radici in K^n*. La condizione che K non sia numerabile nel teorema 10.7 non è necessaria, come vedremo nel prossimo capitolo.

11. Il teorema degli zeri nel caso generale

Un'algebra polinomiale è, per definizione, un'algebra commutativa e finitamente generata. Un modulo finitamente generato su un anello commutativo noetheriano è noetheriano. Una sottoalgebra di codimensione finita di un'algebra polinomiale è anch'essa polinomiale. $K(x)$ non è un'algebra polinomiale. Lemma di Artin-Tate: Un'estensione di campi polinomiale è di dimensione finita e quindi algebrica. Un'estensione di campi $E : K$ è di grado finito se e solo se esistono $\alpha_1, \ldots, \alpha_n \in E$ tali che $E = K[\alpha_1, \ldots, \alpha_n]$. Teorema degli zeri: Se K è un campo algebricamente chiuso ed I è un ideale di $K[x_1, \ldots, x_n]$, allora $\mathrm{Zeri}(I) \neq \emptyset$.

Osservazione 11.1. Seguiamo Scheja/ [1589/2], 80-83.

Definizione 11.2 (non standard). Sia A un anello commutativo.
Una A-algebra *polinomiale* è una A-algebra commutativa e finitamente generata.

Un'estensione di campi $E : K$ si dice polinomiale, se E è una K-algebra polinomiale. Vedremo nel teorema 11.6 che questa condizione implica che l'estensione $E : K$ è di dimensione finita e quindi algebrica.

Osservazione 11.3. Siano A un anello commutativo noetheriano ed M un A-modulo finitamente generato. Allora M è noetheriano.

Dimostrazione. Ciò è immediato, se si tiene conto dei seguenti fatti noti:

(1) Ogni A-modulo è immagine omomorfa di un A-modulo libero.

(2) Siccome M è finitamente generato, il modulo libero può essere scelto della forma A^n con $n \in \mathbb{N} + 1$.

(3) La somma diretta di un numero finito di A-moduli noetheriani è noetheriana.

(4) Perciò, siccome A è noetheriano, anche A^n è un A-modulo noetheriano.

(5) Per l'oss. 1.14 quindi anche M è noetheriano.

Lemma 11.4. *Siano A un anello commutativo noetheriano, B una A-algebra polinomiale e T una sotto-A-algebra di codimensione finita di B, cioè tale che $|B : T| < \infty$.*

Allora anche T è una A-algebra polinomiale.

Dimostrazione. (1) Per ipotesi esistono $\alpha_1, \ldots, \alpha_n \in B$ ed $e_1, \ldots, e_m \in B$ tali che $B = A[\alpha_1, \ldots, \alpha_n] = T\smile(e_1, \ldots, e_m)$.

Per ogni i esiste quindi una rappresentazione $\alpha_i = \sum_{k=1}^{m} s_{ik}e_k$ con coefficienti $s_{ik} \in T$ e per ogni i, j esiste una rappresentazione $e_i e_j = \sum_{k=1}^{m} t_{ijk}e_k$ con coefficienti $t_{ijk} \in T$. Sia $C := A[s_{ik}, t_{ijk} \mid i, j \in \{1, \ldots, n\}, k \in \{1, \ldots, m\}]$.

Allora C è una sotto-A-algebra di T e quindi allo stesso tempo T è un C-modulo. Quest'ultimo fatto lo useremo subito.

(2) Consideriamo l'insieme $\widetilde{B} := C\smile(e_1, \ldots, e_m)$.

Siccome $C \subset T$, ovviamente $\widetilde{B} \subset B$.

Dalla rappresentazione degli α_i segue in un primo momento che $B \subset C[e_1, \ldots, e_m]$.

Dalla rappresentazione dei prodotti $e_i e_j$ segue però che $C[e_1, \ldots, e_m] \subset C_\smile(e_1, \ldots, e_m) = \widetilde{B}$.

Ciò implica $\widetilde{B} = B$ ovvero $B = C_\smile(e_1, \ldots, e_m)$.

(3) Per il cor. 4.15 C è un anello noetheriano.

(4) Per il punto (2) B è un C-modulo finitamente generato e quindi un C-modulo noetheriano per l'oss. 11.3.

Siccome T è un sotto-C-modulo di B, ciò implica che anche T è un C-modulo finitamente generato. Perciò esistono $f_1, \ldots, f_r \in T$ tali che $T = C_\smile(f_1, \ldots, f_r)$.

(5) Allora $T = A[s_{ik}, t_{ijk} \mid i, j, k]_\smile(f_1, \ldots, f_r) \subset A[s_{ik}, t_{ijk}, f_l \mid i, j, k, l] \subset T$.

Perciò $T = A[s_{ik}, t_{ijk}, f_l \mid i, j, k, l]$ è una A-algebra polinomiale.

Lemma 11.5. *Sia K un campo. Allora $K(x)$ non è una K-algebra polinomiale.*

Dimostrazione. Siano $\alpha_1, \ldots, \alpha_m \in K(x)$ tali che $K(x) = K[\alpha_1, \ldots, \alpha_m]$. Allora per ogni $i = 1, \ldots, m$ esiste una rappresentazione $\alpha_i = \dfrac{f_i}{g_i}$ con $f_i, g_i \in K[x]$ e $g_i \neq 0$. Raccogliendo i denominatori, possiamo assumere che i g_i siano tutti uguali, ad es. $g_i = g$ per ogni i.

g non può essere costante, perché altrimenti si avrebbe $\alpha_i \in K[x]$ per ogni i e quindi anche $K(x) = K[x]$.

Siccome $\dfrac{1}{g-1} \in K(x) = K\left[\dfrac{f_1}{g}, \ldots, \dfrac{f_m}{g}\right]$, devono esistere $h \in K[x]$ ed $r \in \mathbb{N}$ tali che $\dfrac{1}{g-1} = \dfrac{h}{g^r}$, ovvero $g^r = h \cdot (g-1)$. Ciò implica

$$1 + g + \ldots + g^{r-1} = \frac{g^r - 1}{g-1} = \frac{g^r}{g-1} - \frac{1}{g-1} = h - \frac{1}{g-1}$$

cosicché $\dfrac{1}{g-1} \in K[x]$ e ciò, essendo g non costante, non è possibile, come abbiamo visto nel cor. 8.7.

Teorema 11.6 (lemma di Artin-Tate). *Un'estensione di campi polinomiale è di dimensione finita e quindi algebrica.*

Dimostrazione. Sia $E : K$ un'estensione di campi polinomiale. Allora esistono $\alpha_1, \ldots, \alpha_n \in E$ tali che $E = K[\alpha_1, \ldots, \alpha_n]$.

(1) Ovviamente si ha anche $E = K(\alpha_1, \ldots, \alpha_n)$. Per $i = 1, \ldots, n$ poniamo $L_i := K(\alpha_1, \ldots, \alpha_i)$. Con $L_0 := K$ abbiamo allora una catena ascendente di campi intermedi

$$K = L_0 \subset L_1 \subset \ldots \subset L_n = E$$

(2) Per il teorema della moltiplicazione dei gradi è sufficiente dimostrare che $|L_i : L_{i-1}| < \infty$ per ogni $i = 1, \ldots, n$.

(3) Assumiamo che non sia così, cioè che esista un i tale che $|L_i : L_{i-1}| = \infty$, mentre $|L_j : L_{j-1}| < \infty$ per ogni $j > i$.

Ancora per il teorema della moltiplicazione dei gradi si ha $|E : L_i| < \infty$, cosicché dal lemma 11.4 segue che L_i è una K-algebra polinomiale.

(4) L_i è perciò anche una L_{i-1}-algebra polinomiale.

(5) D'altra parte per costruzione $L_i = L_{i-1}(\alpha_i)$ ed α_i deve essere trascendente su L_{i-1} perché altrimenti si avrebbe $|L_i : L_{i-1}| < \infty$.

Perciò $L_i \cong L_{i-1}(x)$ e possiamo applicare il lemma 11.5 (con L_{i-1} al posto di K), dal quale risulta che L_i non può essere una L_{i-1}-algebra polinomiale, in contrasto con il punto (4).

Corollario 11.7. *Sia $E : K$ un'estensione di campi. Allora sono equivalenti:*

(1) $|E : K| < \infty$.

(2) Esistono $\alpha_1, \ldots, \alpha_n \in \mathrm{Alg}(E : K)$ *tali che* $E = K(\alpha_1, \ldots, \alpha_n)$.

(3) Esistono $\alpha_1, \ldots, \alpha_n \in \mathrm{Alg}(E : K)$ *tali che* $E = K[\alpha_1, \ldots, \alpha_n]$.

(4) $E : K$ *è polinomiale, cioè esistono* $\alpha_1, \ldots, \alpha_n \in E$ *(a priori non necessariamente algebrici su* K*) tali che* $E = K[\alpha_1, \ldots, \alpha_n]$.

Dimostrazione. (1) $\implies$ (2): Prop. 7.25.

(2) $\implies$ (3): Per $i > 1$ naturalmente α_i è algebrico su $K(\alpha_1, \ldots, \alpha_{i-1})$, mentre α_1 è algebrico su K, cosicché per il teorema 7.16 abbiamo $E = K[\alpha_1, \ldots, \alpha_n]$.

(3) $\implies$ (4): Chiaro.

(4) $\implies$ (1): Teorema 11.6.

Osservazione 11.8. Il cor. 11.7 mostra che il teorema 11.6 è, nell'enunciato, semplicemente una generalizzazione della prop. 7.25 e del teorema 7.16 a più dimensioni.

La dimostrazione però non è ovvia e usa alcuni ragionamenti piuttosto profondi nei lemmi 11.4 e 11.5 e nella dimostrazione del teorema 11.6 stesso.

Teorema 11.9 (teorema degli zeri). *Siano K un campo algebricamente chiuso ed I un ideale di $K[x_1, \ldots, x_n]$.*

Allora $\mathrm{Zeri}(I) \neq \emptyset$.

Dimostrazione. Utilizziamo la stessa idea come nella dimostrazione del teorema 10.7.

Sappiamo che I è contenuto in un ideale massimale $\mathfrak{m}$. Siccome $\mathrm{Zeri}(\mathfrak{m}) \subset \mathrm{Zeri}(I)$, è sufficiente dimostrare che $\mathrm{Zeri}(\mathfrak{m}) \neq \emptyset$.

L'anello $E := K[x_1, \ldots, x_n]/\mathfrak{m}$ è un campo ed è ovviamente un'algebra polinomiale su K. Come in precedenza possiamo considerare K come sottocampo di E; dal teorema 11.6 sappiamo che l'estensione $E : K$ è algebrica.

Siccome K è algebricamente chiuso, ciò implica $E = K$. Dalla nota 9.2 segue che $\mathrm{Zeri}(\mathfrak{m}) \neq \emptyset$.

12. Il teorema del radicale

Trucco di Rabinovich: Per $f \in \mathcal{J}(\mathrm{Zeri}(I))$, l'ideale generato da $I \cup \{fx_{n+1} - 1\}$ non ha zeri e coincide quindi, se K è algebricamente chiuso, con $K[x_1, \ldots, x_{n+1}]$. Sempre nell'ipotesi che K sia algebricamente chiuso, si ha $\mathcal{J}(\mathrm{Zeri}(I)) = \sqrt{I}$.

Situazione 12.1. Siano K un campo ed I un ideale generalizzato di $K[x_1, \ldots, x_n]$.

Usiamo, come quasi sempre, le abbreviazioni $\mathrm{Zeri}(I) := \mathrm{Zeri}(I, \mathrm{in}\, K^n)$ e $\mathcal{J}(\mathrm{Zeri}(I)) := \mathcal{J}(\mathrm{Zeri}(I), \mathrm{in}\, K[x_1, \ldots, x_n])$.

Lemma 12.2 (trucco di Rabinovich). *Siano* $f \in \mathcal{J}(\mathrm{Zeri}(I))$ *ed* $M := K[x_1, \ldots, x_{n+1}]_\smile(I \cup \{fx_{n+1} - 1\})$.

Allora $\mathrm{Zeri}(M, \mathrm{in}\, K^{n+1}) = \emptyset$.

Dimostrazione. Sia $(\alpha_1, \ldots, \alpha_{n+1}) \in \mathrm{Zeri}(M, \mathrm{in}\, K^{n+1})$.

Allora $(\alpha_1, \ldots, \alpha_n) \in \mathrm{Zeri}(I)$ e $f(\alpha_1, \ldots, \alpha_n)\alpha_{n+1} = 1$.

La prima relazione implica però $f(\alpha_1, \ldots, \alpha_n) = 0$ e quindi otteniamo $0 = 1$, una contraddizione.

Corollario 12.3. *Siano* K *algebricamente chiuso ed* $f \in \mathcal{J}(\mathrm{Zeri}(I))$.

Allora $K[x_1, \ldots, x_{n+1}]_\smile(I \cup \{fx_{n+1} - 1\}) = K[x_1, \ldots, x_{n+1}]$.

Dimostrazione. Sia M l'ideale generalizzato alla sinistra nell'ultima riga dell'enunciato. Il lemma 12.2 implica $\mathrm{Zeri}(M, \mathrm{in}\, K^{n+1}) = \emptyset$.

Per il teorema 11.9 ciò è possibile solo se $M = K[x_1, \ldots, x_{n+1}]$.

Osservazione 12.4. $\mathrm{Zeri}(\sqrt{I}) = \mathrm{Zeri}(I)$ e quindi $\sqrt{I} \subset \mathcal{J}(\mathrm{Zeri}(I))$.

Dimostrazione. Siano $\alpha \in \mathrm{Zeri}(I)$ ed $f \in \sqrt{I}$. Allora esiste $k \in \mathbb{N}$ tale che $f^k \in I$. Ciò implica $f^k(\alpha) = 0$, per cui anche $f(\alpha) = 0$.

Teorema 12.5 (teorema del radicale). K *sia algebricamente chiuso.*

Allora $\mathcal{J}(\mathrm{Zeri}(I)) = \sqrt{I}$.

Dimostrazione. Per l'oss. 12.4 basta dimostrare che $\mathcal{J}(\mathrm{Zeri}(I)) \subset \sqrt{I}$.

Sia $f \in \mathcal{J}(\mathrm{Zeri}(I))$. Per il cor. 12.3 esistono $g_1, \ldots, g_m \in I$ e $p_1, \ldots, p_m, q \in K[x_1, \ldots, x_{n+1}]$ tali che

$$p_1 g_1 + \ldots + p_m g_m + (fx_{n+1} - 1)q = 1$$

Per la prop. 6.30 ciò implica che l'ideale generalizzato generato da $g_1, \ldots, g_m$ in $K[x_1, \ldots, x_n]_f$ è improprio, per cui esistono $h_1, \ldots, h_m \in K[x_1, \ldots, x_n]$ tali che (raccogliendo le potenze di f in un'unica potenza f^k) abbiamo

$$\frac{h_1 g_1 + \ldots + h_m g_m}{f^k} = 1 \text{ per qualche } k \in \mathbb{N}. \text{ Ma allora}$$

$f^k = h_1 g_1 + \ldots + h_m g_m \in I$ e ciò significa proprio $f \in \sqrt{I}$.

Osservazione 12.6. Il teorema del radicale è spesso anche detto *teorema degli zeri di Hilbert*, il teorema 11.9 *teorema debole degli zeri*.

13. K-algebre polinomiali sono anelli di Jacobson

Ogni immagine omomorfa di un'algebra polinomiale è polinomiale. Se A è una K-algebra polinomiale, allora per ogni $\mathfrak{m} \in \operatorname{Max} A$ l'estensione di campi $A/\mathfrak{m} : K$ è di grado finito. Una K-algebra integra di dimensione finita è un campo. La controimmagine di un ideale massimale di una K-algebra polinomiale è un ideale massimale. Se B è un'algebra polinomiale ed f è un elemento non nilpotente di B, allora anche B_f è un'algebra polinomiale. Ogni K-algebra polinomiale è un anello di Jacobson. Come si ottiene adesso il teorema del radicale.

Situazione 13.1. Sia K un campo.

Osservazione 13.2. Diamo in questo capitolo, in cui non usiamo i risultati del capitolo 12, una dimostrazione più astratta del teorema del radicale, in cui il trucco di Rabinovich (lemma 12.2) appare, nella prop. 13.8, in forma nascosta.

In questo approccio più teorico vedremo che il teorema del radicale è una conseguenza quasi immediata del cor. 9.8 e del fatto che ogni K-algebra polinomiale è un anello di Jacobson, un anello cioè in cui ogni ideale primo è intersezione di ideali massimali (def. 3.55).

Osservazione 13.3. Siano A un anello commutativo, B una A-algebra polinomiale ed I un ideale di B. Allora B/I è in modo naturale una A-algebra polinomiale.

Dimostrazione. Sia $\varphi : A \longrightarrow B$ l'omomorfismo di struttura di B. Allora la composizione $A \xrightarrow{\varphi} B \longrightarrow B/I$ di φ con la proiezione canonica fornisce una struttura di A-algebra commutativa su B/I.

Se $B = A[\alpha_1, \ldots, \alpha_n]$ e se con $\overline{\alpha_i}$ denotiamo la classe di equivalenza di α_i, allora si ha evidentemente $B/I = A[\overline{\alpha_1}, \ldots, \overline{\alpha_n}]$.

Corollario 13.4. *Siano A una K-algebra polinomiale ed $\mathfrak{m} \in \operatorname{Max} A$.*

Allora $|A/\mathfrak{m} : K| < \infty$.

Dimostrazione. Per l'oss. 13.3 $A/\mathfrak{m}$ è una K-algebra polinomiale. Essa è anche un campo, cosicché l'enunciato segue dal teorema 11.6.

Lemma 13.5. *Siano K un campo ed A una K-algebra integra con $|A : K| < \infty$. Allora A è un campo.*

Dimostrazione. Sia $a \in A, a \neq 0$. Siccome A è integra, l'applicazione K-lineare $L_a := \bigcirc_v av : A \longrightarrow A$ è iniettiva. Siccome $|A : K| < \infty$, essa è anche suriettiva. Ciò implica in particolare che esiste $b \in A$ tale che $L_a b = 1$ ovvero $ab = 1$. Perciò a è invertibile.

Proposizione 13.6. *Siano K un campo, A una K-algebra commutativa e B una K-algebra polinomiale. Siano $\varphi : A \longrightarrow B$ un omomorfismo di K-algebre ed $\mathfrak{n} \in \operatorname{Max} B$.*

Allora $\varphi^{-1}(\mathfrak{n}) \in \operatorname{Max} A$.

Dimostrazione. (1) Per il cor. 13.4 $|B/\mathfrak{n} : K| < \infty$.

(2) Sia $\mathfrak{m} := \varphi^{-1}(\mathfrak{n})$.

L'applicazione $\psi := \bigcirc_{a+\mathfrak{m}} \varphi a + \mathfrak{n} : A/\mathfrak{m} \longrightarrow B/\mathfrak{n}$ è ben definita e un omomorfismo di K-algebre. ψ è iniettivo perché $\psi(a+\mathfrak{m}) = 0$ significa $\varphi a + \mathfrak{n} = 0$, cioè $\varphi a \in \mathfrak{n}$, ovvero $a \in \mathfrak{m}$.

(3) $A/\mathfrak{m}$ è perciò come spazio vettoriale isomorfo a un sottospazio vettoriale di $B/\mathfrak{n}$, cosicché $|A/\mathfrak{m} : K| < \infty$.

(4) Dal lemma 3.18 sappiamo che $\mathfrak{m}$ è un ideale primo di A, per cui $A/\mathfrak{m}$ è integro. Ma allora dal lemma 13.5 segue che $A/\mathfrak{m}$ è un campo, cosicché $\mathfrak{m}$ deve essere un ideale massimale.

Osservazione 13.7. Siano A un anello commutativo, B una A-algebra polinomiale ed f un elemento non nilpotente di B. Allora anche B_f è una A-algebra polinomiale.

Dimostrazione. Usiamo l'oss. 13.3. Siano $\alpha_1, \ldots, \alpha_n \in B$ tali che $B = A[\alpha_1, \ldots, \alpha_n]$. Allora $B_f \overset{6.30}{\cong} B[x]/(fx-1) = A[\alpha_1, \ldots, \alpha_n, x]/(fx-1)$.

Proposizione 13.8. *Sia A una K-algebra polinomiale $\neq 0$.*

Allora $\sqrt{0} = \sqrt[\text{Jac}]{0}$.

Dimostrazione. (1) Ricordiamo che secondo la def. 3.35 $\sqrt{0}$ coincide con l'insieme degli elementi nilpotenti di A. Siccome $\sqrt{0} \subset \sqrt[\text{Jac}]{0}$, è sufficiente dimostrare che un elemento non nilpotente di A non è contenuto in $\sqrt[\text{Jac}]{0}$, cioè nell'intersezione di tutti gli ideali massimali di A.

(2) Sia f un elemento non nilpotente di A. Per il punto (1) è sufficiente trovare un ideale massimale di A che non contiene f.

Siccome f non è nilpotente, l'anello A_f è ben definito, quindi esiste $\mathfrak{n} \in \operatorname{Max} A_f$. Per l'oss. 13.7 anche A_f è una K-algebra polinomiale.

Per la prop. 13.6 $\mathfrak{m} := i_f^{-1}(\mathfrak{n}) \in \operatorname{Max} A$.

Ma $i_f(f)$ è invertibile in A_f, per cui $i_f(f) \notin \mathfrak{n}$, cosicché $f \notin \mathfrak{m}$.

Teorema 13.9. *Ogni K-algebra polinomiale $\neq 0$ è un anello di Jacobson.*

Dimostrazione. Siano A una K-algebra polinomiale ed I un ideale di A.

Per l'oss. 13.3 A/I è una K-algebra polinomiale. In essa si ha $\sqrt{0} = \sqrt[\text{Jac}]{0}$ per la prop. 13.8. Ciò significa proprio $\sqrt{I} = \sqrt[\text{Jac}]{I}$ in A e ciò implica l'enunciato.

Nota 13.10. Dal teorema 13.9 otteniamo una seconda dimostrazione del teorema del radicale (teorema 12.5), che non usa i risultati del capitolo 12.

(1) Sia I un ideale di $K[x_1, \ldots, x_n]$. Affinché $\mathcal{J}(\operatorname{Zeri}(I)) = \sqrt{I}$, per il teorema 13.9 è sufficiente che $\mathcal{J}(\operatorname{Zeri}(I)) \subset \mathfrak{m}$ per ogni $\mathfrak{m} \in \operatorname{Max} K[x_1, \ldots, x_n]$ per il quale $I \subset \mathfrak{m}$.

(2) Sia quindi $\mathfrak{m} \in \operatorname{Max} K[x_1, \ldots, x_n]$ con $I \subset \mathfrak{m}$.

(3) Assumiamo adesso che K sia algebricamente chiuso.

Per il teorema 11.9 $\operatorname{Zeri}(\mathfrak{m}) \neq \emptyset$, pertanto per il cor. 9.8 $\mathcal{J}(\operatorname{Zeri}(I)) \subset \mathcal{J}(\operatorname{Zeri}(\mathfrak{m})) = \mathfrak{m}$.

14. Insiemi algebrici affini

Insiemi algebrici affini. $\mathrm{Zeri}(I) \cup \mathrm{Zeri}(J) = \mathrm{Zeri}(I \cap J) = \mathrm{Zeri}(IJ)$; perciò l'unione di due insiemi algebrici è un insieme algebrico. $\mathrm{Zeri}(I) \cap \mathrm{Zeri}(J) = \mathrm{Zeri}(I + J)$; perciò l'intersezione di due insiemi algebrici è un insieme algebrico. $X \subset Y \Longrightarrow \mathcal{J}(Y) \subset \mathcal{J}(X)$. Per $\mathcal{X} \subset \mathcal{P}(K^n)$ si ha $\mathcal{J}(\bigcup_{X \in \mathcal{X}} X) = \bigcap_{X \in \mathcal{X}} \mathcal{J}(X)$. Lemma di Galois: $\mathcal{J}(\mathrm{Zeri}(\mathcal{J}(X))) = \mathcal{J}(X)$ e $\mathrm{Zeri}(\mathcal{J}(\mathrm{Zeri}(I))) = \mathrm{Zeri}(I)$. Se K è algebricamente chiuso, allora $\mathrm{Zeri}(I) \subset \mathrm{Zeri}(J) \iff \sqrt{J} \subset \sqrt{I}$. Ideali annullatori. Per un ideale generalizzato annullatore I si ha $I = \mathcal{J}(\mathrm{Zeri}(I))$ e per un insieme algebrico X si ha $X = \mathrm{Zeri}(\mathcal{J}(X))$. Due insiemi algebrici X ed Y coincidono quindi se e solo se $\mathcal{J}(X) = \mathcal{J}(Y)$ e due ideali generalizzati annullatori I e J coincidono se e solo se $\mathrm{Zeri}(I) = \mathrm{Zeri}(J)$. Biiezione canonica tra i sottoinsiemi algebrici di K^n e gli ideali generalizzati annullatori di $K[x_1, \ldots, x_n]$. Se K è algebricamente chiuso, allora I è annullatore se e solo se I è radicale e quindi si ottiene una biiezione canonica tra i sottoinsiemi algebrici di K^n e gli ideali generalizzati radicali di $K[x_1, \ldots, x_n]$. $\mathrm{Zeri}(\sum_{I \in \mathcal{I}} I) = \mathrm{Zeri}(\bigcup_{I \in \mathcal{I}} I) = \bigcap_{I \in \mathcal{I}} \mathrm{Zeri}(I)$. L'intersezione di una famiglia arbitraria di sottoinsiemi algebrici di K^n è quindi ancora un insieme algebrico. Possiamo perciò introdurre su K^n una topologia (detta di Zariski) i cui chiusi sono esattamente gli insiemi algebrici. In questa topologia K^n è uno spazio T_1, ma (tranne in casi banali) non uno spazio di Hausdorff. $\overline{X} = \mathrm{Zeri}(\mathcal{J}(X))$; la prima parte del lemma di Galois diventa quindi $\mathcal{J}(\overline{X}) = \mathcal{J}(X)$. $X \subset \overline{Y} \iff \mathcal{J}(Y) \subset \mathcal{J}(X)$, perciò se X ed Y sono algebrici, allora $X \subset Y \iff \mathcal{J}(Y) \subset \mathcal{J}(X)$. L'ideale generato da $x^2 + 1$ in $\mathbb{R}[x]$ è massimale, ma non possiede zeri e quindi non è un ideale annullatore. Se K è algebricamente chiuso, allora esistono una biiezione canonica tra i punti di K^n e gli ideali massimali di $K[x_1, \ldots, x_n]$ e, per un sottoinsieme algebrico X di K^n una biiezione canonica tra i punti di X e gli ideali massimali di $K[x_1, \ldots, x_n]$ che contengono $\mathcal{J}(X)$. L'ideale $\mathcal{J}(X)$ è massimale se e solo se X consiste di un solo punto. Ogni sottoinsieme finito di K^n è algebrico. I sottoinsiemi algebrici $\neq K$ di K coincidono con i sottoinsiemi finiti di K. Per un polinomio f l'applicazione $\bigcirc_{\alpha} f(\alpha) : K^n \longrightarrow K$ è continua rispetto alla topologia di Zariski. Se A è un anello integro ed S è un sottoinsieme infinito di A, allora $\mathcal{J}(S^n, \mathrm{in}\, A[x_1, \ldots, x_n]) = 0$. Se K è infinito, allora $\mathcal{J}(K^n) = 0$. In un campo finito K con q elementi si ha $\alpha^q = \alpha$ per ogni $\alpha \in K$ e quindi $(x_1^q - x_1) + \ldots + (x_n^q - x_n) \in \mathcal{J}(K^n)$. Un campo algebricamente chiuso K è infinito, cosicché $\mathcal{J}(K^n) = 0$. Se un ideale primo contiene un'intersezione di un numero finito di ideali, allora ne contiene il prodotto e quindi anche uno di quegli ideali. Se K è infinito, allora K^n non può essere rappresentato come unione di due chiusi $\neq K^n$, inoltre K^n non è uno spazio di Hausdorff nella topologia di Zariski e se X è un sottoinsieme algebrico $\neq K^n$, allora il complemento $K^n \setminus X$ è ancora un insieme infinito.

Situazione 14.1. Sia K un campo.

Definizione 14.2. Un sottoinsieme $X \subset K^n$ si dice *algebrico*, se esiste un insieme di polinomi $F \subset K[x_1, \ldots, x_n]$ tale che $X = \mathrm{Zeri}(F)$.

Abbiamo già osservato nella nota 1.18 che allora $X = \mathrm{Zeri}(I)$, dove I è l'ideale generalizzato generato da F in $K[x_1, \ldots, x_n]$.

Definizione 14.3. Un insieme *algebrico affine* (su K) è un sottoinsieme algebrico di K^n per qualche $n \in \mathbb{N} + 1$.

Osservazione 14.4. Siano I, J ideali generalizzati di $K[x_1, \ldots, x_n]$. Allora:

(1) $I \subset J \Longrightarrow \mathrm{Zeri}(J) \subset \mathrm{Zeri}(I)$.

(2) $I \subset \mathcal{J}(\mathrm{Zeri}(I))$.

Lemma 14.5. *Siano I, J ideali generalizzati di $K[x_1, \ldots, x_n]$. Allora:*

(1) $\mathrm{Zeri}(I) \cup \mathrm{Zeri}(J) = \mathrm{Zeri}(I \cap J) = \mathrm{Zeri}(IJ)$.

(2) $\mathrm{Zeri}(I) \cap \mathrm{Zeri}(J) = \mathrm{Zeri}(I + J)$.

Dimostrazione. (1) Abbiamo $IJ \subset I \cap J \subset I, J$ e quindi $\mathrm{Zeri}(I) \cup \mathrm{Zeri}(J) \subset \mathrm{Zeri}(I \cap J) \subset \mathrm{Zeri}(IJ)$ per l'oss. 13.4.

Sia $\alpha \in \mathrm{Zeri}(IJ)$, ma $\alpha \notin \mathrm{Zeri}(I) \cup \mathrm{Zeri}(J)$.

Allora esistono $f \in I$ e $g \in J$ tali che $f(\alpha) \neq 0$ e $g(\alpha) \neq 0$.

Ma $fg \in IJ$ e quindi $f(\alpha)g(\alpha) = 0$, una contraddizione.

(2) $I, J \subset I + J$ implica $\mathrm{Zeri}(I + J) \subset \mathrm{Zeri}(I) \cap \mathrm{Zeri}(J)$.

Siano $\alpha \in \mathrm{Zeri}(I) \cap \mathrm{Zeri}(J)$ ed $f \in I, g \in J$. Allora $f(\alpha) + g(\alpha) = 0$. Ciò mostra $\alpha \in \mathrm{Zeri}(I + J)$.

Corollario 14.6. *Siano $X, Y \subset K^n$ due insiemi algebrici.*

Allora $X \cup Y$ e $X \cap Y$ sono anch'essi insiemi algebrici.

Osservazione 14.7. Siano $X, Y \in K^n$. Allora:

(1) $X \subset Y \Longrightarrow \mathcal{J}(Y) \subset \mathcal{J}(X)$.

(2) $X \subset \mathrm{Zeri}(\mathcal{J}(X))$.

Lemma 14.8. *Sia $\mathcal{X}$ un insieme di sottoinsiemi di K^n.*

Allora $\mathcal{J}(\bigcup_{X \in \mathcal{X}} X) = \bigcap_{X \in \mathcal{X}} \mathcal{J}(X)$.

Dimostrazione. (1) È chiaro che $\mathcal{J}(\bigcup_{X \in \mathcal{X}} X) \subset \bigcap_{X \in \mathcal{X}} \mathcal{J}(X)$.

(2) Siano $f \in \bigcap_{X \in \mathcal{X}} \mathcal{J}(X)$ ed $\alpha \in \bigcup_{X \in \mathcal{X}} X$. Allora esiste un $X \in \mathcal{X}$ con $\alpha \in X$. Siccome $f \in \mathcal{J}(X)$, ciò implica $f(\alpha) = 0$.

Lemma 14.9 (lemma di Galois). *(1) Sia $X \subset K^n$.*

Allora $\mathcal{J}(\mathrm{Zeri}(\mathcal{J}(X))) = \mathcal{J}(X)$.

(2) Sia I un ideale generalizzato di $K[x_1, \ldots, x_n]$.

Allora $\mathrm{Zeri}(\mathcal{J}(\mathrm{Zeri}(I))) = \mathrm{Zeri}(I)$.

Dimostrazione. (1) Abbiamo $J(X) \subset \mathcal{J}(\mathrm{Zeri}(\mathcal{J}(X)))$ per l'oss. 14.4, ma anche $X \subset \mathrm{Zeri}(\mathcal{J}(X))$ e quindi $\mathcal{J}(\mathrm{Zeri}(\mathcal{J}(X))) \subset \mathcal{J}(X)$.

(2) Abbiamo $\mathrm{Zeri}(I) \subset \mathrm{Zeri}(\mathcal{J}(\mathrm{Zeri}(I)))$ per l'oss. 13.7, ma anche $I \subset \mathcal{J}(\mathrm{Zeri}(I))$ e quindi $\mathrm{Zeri}(\mathcal{J}(\mathrm{Zeri}(I))) \subset \mathrm{Zeri}(I)$.

Osservazione 14.10. Siano I, J ideali generalizzati di $K[x_1, \ldots, x_n]$. Allora

$$\mathrm{Zeri}(I) \subset \mathrm{Zeri}(J) \iff \mathcal{J}(\mathrm{Zeri}(J)) \subset \mathcal{J}(\mathrm{Zeri}(I))$$

Dimostrazione. L'implicazione $\Longrightarrow$ è chiara.

Sia invece $\mathcal{J}(\mathrm{Zeri}(J)) \subset \mathcal{J}(\mathrm{Zeri}(I))$. Allora

$$\mathrm{Zeri}(I) \overset{14.9}{=} \mathrm{Zeri}(\mathcal{J}(\mathrm{Zeri}(I))) \subset \mathrm{Zeri}(\mathcal{J}(\mathrm{Zeri}(J))) \overset{14.9}{=} \mathrm{Zeri}(J)$$

Corollario 14.11. *Siano I, J ideali generalizzati di $K[x_1, \ldots, x_n]$.*

Se K è algebricamente chiuso, allora

$$\mathrm{Zeri}(I) \subset \mathrm{Zeri}(J) \iff \sqrt{J} \subset \sqrt{I}$$

Definizione 14.12. Un ideale (generalizzato) di $K[x_1, \ldots, x_n]$ si chiama un ideale (generalizzato) *annullatore*, se esiste un sottoinsieme $X \subset K^n$ tale che $I = \mathcal{J}(X)$.

Lemma 14.13. *I sia un ideale generalizzato annullatore di $K[x_1, \ldots, x_n]$.*

Allora $I = \mathcal{J}(\mathrm{Zeri}(I))$.

Dimostrazione. Per ipotesi esiste $X \subset K^n$ con $I = \mathcal{J}(X)$. Dal lemma 14.9 abbiamo allora

$$I = \mathcal{J}(X) = \mathcal{J}(\mathrm{Zeri}(\mathcal{J}(X))) = \mathcal{J}(\mathrm{Zeri}(I))$$

Lemma 14.14. *Sia X un sottoinsieme algebrico di K^n.*

Allora $X = \mathrm{Zeri}(\mathcal{J}(X))$.

Dimostrazione. Per ipotesi esiste un ideale generalizzato I di $K[x_1, \ldots, x_n]$ tale che $X = \mathrm{Zeri}(I)$. Dal lemma 14.9 segue allora

$$X = \mathrm{Zeri}(I) = \mathrm{Zeri}(\mathcal{J}(\mathrm{Zeri}(I))) = \mathrm{Zeri}(\mathcal{J}(X))$$

Proposizione 14.15. *X ed Y siano sottoinsiemi algebrici di K^n tali che $\mathcal{J}(X) = \mathcal{J}(Y)$.*

Allora $X = Y$.

Dimostrazione. Per il lemma 14.14 abbiamo

$$X = \mathrm{Zeri}(\mathcal{J}(X)) = \mathrm{Zeri}(\mathcal{J}(Y)) = Y$$

Proposizione 14.16. *I e J siano ideali generalizzati annullatori di $K[x_1, \ldots, x_n]$ tali che $\mathrm{Zeri}(I) = \mathrm{Zeri}(J)$.*

Allora $I = J$.

Dimostrazione. Per il lemma 14.13 abbiamo

$$I = \mathcal{J}(\mathrm{Zeri}(I)) = \mathcal{J}(\mathrm{Zeri}(J)) = J$$

Proposizione 14.17. *Esiste una biiezione canonica*

$$\begin{array}{c} \{\textit{sottoinsiemi algebrici di } K^n\} \longleftrightarrow \{\textit{ideali generalizzati annullatori di } K[x_1, \ldots, x_n]\} \\ X \longmapsto \mathcal{J}(X) \\ \mathrm{Zeri}(I) \longmapsfrom I \end{array}$$

Dimostrazione. Le due applicazioni indicate sono l'una l'inversa dell'altra. Infatti utilizzando i lemmi 14.13 e 14.14 abbiamo, per un insieme algebrico X risp. per un ideale generalizzato annullatore I,

$$\begin{array}{c} \mathrm{Zeri}(\mathcal{J}(X)) = X \\ \mathcal{J}(\mathrm{Zeri}(I)) = I \end{array}$$

Osservazione 14.18. Sia I un ideale generalizzato di $K[x_1, \ldots, x_n]$.

(1) Se I è annullatore, allora I è radicale.

(2) Se I e radicale e K è algebricamente chiuso, allora I è annullatore.

Dimostrazione. Ricordiamo dalla def. 3.47 che I si chiama radicale, se $\sqrt{I} = I$.

(1) Sia I annullatore. Allora $I \overset{14.13}{=} \mathcal{J}(\mathrm{Zeri}(I)) \overset{12.4}{\supset} \sqrt{I} \supset I$, per cui $\sqrt{I} = I$.

(2) Sia $I = \sqrt{I}$. Se K è algebricamente chiuso, dal teorema 12.5 abbiamo $I = \mathcal{J}(\mathrm{Zeri}(I))$.

Corollario 14.19. *Sia K algebricamente chiuso. Allora la biiezione naturale della prop. 14.17 può essere espressa anche come biiezione*

$\{$*sottoinsiemi algebrici di* $K^n\} \longleftrightarrow \{$*ideali generalizzati radicali di* $K[x_1, \ldots, x_n]\}$

Osservazione 14.20. K^n e $\emptyset$ sono insiemi algebrici:

$\mathrm{Zeri}(K[x_1, \ldots, x_n]) = \emptyset$.

$\mathrm{Zeri}(0) = K^n$

Lemma 14.21. *Sia $\mathcal{I}$ un insieme di ideali generalizzati di $K[x_1, \ldots, x_n]$.*

Allora $\mathrm{Zeri}(\sum_{I \in \mathcal{I}} I) = \mathrm{Zeri}(\bigcup_{I \in \mathcal{I}} I) = \bigcap_{I \in \mathcal{I}} \mathrm{Zeri}(I)$

Dimostrazione. Si ha evidentemente $\mathrm{Zeri}(\sum_{I \in \mathcal{I}} I) \subset \mathrm{Zeri}(\bigcup_{I \in \mathcal{I}} I) \subset \bigcap_{I \in \mathcal{I}} \mathrm{Zeri}(I)$.

Sia $\alpha \in \bigcap_{I \in \mathcal{I}} \mathrm{Zeri}(I)$. Sia $\varphi \in \sum_{I \in \mathcal{I}} I$. Allora esistono $I_1, \ldots, I_k \in \mathcal{I}$ ed $f_1 \in I_1, \ldots, f_k \in I_k$ tali che $\varphi = f_1 + \ldots + f_k$.

Ciò implica $\varphi(\alpha) = f_1(\alpha) + \ldots + f_k(\alpha) = 0$.

Si potrebbe anche ragionare direttamente con l'uguaglianza $\mathrm{Zeri}(\bigcup_{I \in \mathcal{I}} I) = \bigcap_{I \in \mathcal{I}} \mathrm{Zeri}(I)$ e usare poi che $\sum_{I \in \mathcal{I}}$ è l'ideale generalizzato generato da $\bigcup_{I \in \mathcal{I}} I$.

Il lemma generalizza il punto (2) del lemma 14.5.

Corollario 14.22. *L'intersezione di una famiglia arbitraria di sottoinsiemi algebrici di K^n è ancora un insieme algebrico.*

Nota 14.23. (1) $\emptyset$ è un sottoinsieme algebrico di K^n per l'oss. 14.20.

(2) K^n è un sottoinsieme algebrico di K^n per l'oss. 14.20.

(3) L'unione di due sottoinsiemi algebrici di K^n è un sottoinsieme algebrico per il cor. 14.6.

(4) Un'intersezione arbitraria di sottoinsiemi algebrici di K^n è un sottoinsieme algebrico per il cor. 14.22.

Possiamo quindi introdurre su K^n una topologia i cui chiusi sono esattamente gli insiemi algebrici.

Questa topologia è detta *topologia di Zariski* su K^n.

Attenzione: Per $K = \mathbb{R}$ o $K = \mathbb{C}$ la topologia di Zariski è molto meno fine della topologia euclidea!

Osservazione 14.24. Usiamo nel seguito le notazioni del capitolo 9, scrivendo però $\alpha = (\alpha_1, \ldots, \alpha_n)$ e quindi $\mathfrak{m}_\alpha$ per l'ideale massimale $K[x_1, \ldots, x_n]\_(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$.

Definizione 14.25. Uno spazio topologico si dice T_1, se ogni suo punto è chiuso.

Proposizione 14.26. *K^n è uno spazio T_1 nella topologia di Zariski.*

Dimostrazione. Ogni punto di K^n è chiuso; infatti per $\alpha \in K^n$ abbiamo $\{\alpha\} = \mathrm{Zeri}(\mathfrak{m}_\alpha)$.

Proposizione 14.27. *Nella topologia di Zariski per $X \subset K^n$ si ha $\overline{X} = \mathrm{Zeri}(\mathcal{J}(X))$.*

Dimostrazione. $\mathrm{Zeri}(\mathcal{J}(X))$ è un chiuso che contiene X.

Perciò è sufficiente dimostrare che $\mathrm{Zeri}(\mathcal{J}(X))$ è il più piccolo chiuso che contiene X. Sia Y un chiuso con $X \subset Y$.

Allora $\mathrm{Zeri}(\mathcal{J}(X)) \subset \mathrm{Zeri}(\mathcal{J}(Y)) \overset{14.14}{=} Y$.

Osservazione 14.28. Sia $X \subset K^n$. Allora $\mathcal{J}(\overline{X}) = \mathcal{J}(X)$.

Dimostrazione. Con la prop. 14.27 ciò è una riformulazione del punto (1) del lemma 14.9.

Corollario 14.29. *Siano $X, Y \subset K^n$. Allora*

$X \subset \overline{Y} \iff \mathcal{J}(Y) \subset \mathcal{J}(X)$

Dimostrazione. (1) Sia $X \subset \overline{Y}$. Allora $\mathcal{J}(Y) \overset{14.28}{=} \mathcal{J}(\overline{Y}) \subset \mathcal{J}(X)$.

(2) Sia $\mathcal{J}(Y) \subset \mathcal{J}(X)$. Allora

$X \subset \overline{X} = \mathrm{Zeri}(\mathcal{J}(X)) \subset \mathrm{Zeri}(\mathcal{J}(Y)) = \overline{Y}$

Corollario 14.30. *Siano X, Y sottoinsiemi algebrici di K^n. Allora*

$X \subset Y \iff \mathcal{J}(Y) \subset \mathcal{J}(X)$

Osservazione 14.31. Se K non è algebricamente chiuso, un ideale massimale di $K[x_1, \ldots, x_n]$ non è necessariamente un ideale annullatore.

Un esempio è l'ideale $\mathfrak{m} := \mathbb{R}[x]\_(x^2 + 1)$ che è massimale perché $\mathbb{R}[x]/\mathfrak{m} \cong \mathbb{C}$ è un campo, ma non possiede zeri.

Proposizione 14.32. *Sia K algebricamente chiuso. Allora esiste una biiezione naturale*

$$\begin{aligned} K^n &\longleftrightarrow \mathrm{Max}\, K[x_1, \ldots, x_n] \\ \alpha &\longmapsto \mathfrak{m}_\alpha \\ \mathrm{Zeri}(\mathfrak{m}) &\longmapsfrom \mathfrak{m} \end{aligned}$$

Dimostrazione. Ciò segue dalla prop. 14.17 oppure direttamente dal fatto che le due applicazioni indicate sono una l'inversa dell'altra, come abbiamo visto nel capitolo 9:

(1) $\mathrm{Zeri}(\mathfrak{m}_\alpha) = \{\alpha\}$ per il lemma 9.6. Qui non si usa l'ipotesi che K sia algebricamente chiuso.

(2) Sia $\mathfrak{m} \in \operatorname{Max} K[x_1, \ldots, x_n]$. Per il teorema degli zeri $\mathrm{Zeri}(\mathfrak{m}) \neq \emptyset$, perciò $\mathfrak{m} = \mathfrak{m}_\alpha$ ed $\alpha = \mathrm{Zeri}(\mathfrak{m})$ per un unico punto $\alpha \in K^n$, come abbiamo visto nella prop. 9.7.

Proposizione 14.33. *Siano K algebricamente chiuso ed X un sottoinsieme algebrico di K^n. Allora la biiezione della prop. 14.32 induce una biiezione naturale*

$$X \longleftrightarrow \{\mathfrak{m} \in \operatorname{Max} K[x_1, \ldots, x_n] \mid \mathfrak{m} \supset \mathcal{J}(X)\}$$

Dimostrazione. Per $\alpha \in K^n$abbiamo $\alpha \in X \iff \mathcal{J}(X) \subset \mathfrak{m}_\alpha$ per il cor. 14.30, cosicché l'enunciato segue dalla prop. 14.32.

Osservazione 14.34. Sia $X \subset K^n$. Allora $\mathcal{J}(X) = \bigcap_{\alpha \in X} \mathfrak{m}_\alpha$.

Dimostrazione. Siccome $X = \bigcup_{\alpha \in X} \{\alpha\}$, ciò segue dal lemma 14.8.

Proposizione 14.35. *Sia $X \subset K^n$. Allora sono equivalenti:*

(1) X consiste di un solo punto.

(2) $\mathcal{J}(X) \in \operatorname{Max} K[x_1, \ldots, x_n]$.

Dimostrazione. (1) $\implies$ (2): Sia $X = \{\alpha\}$ per un $\alpha \in K^n$.

Allora $\mathcal{J}(X) \overset{9.6}{=} \mathfrak{m}_\alpha$ è massimale per la prop. 5.7.

(2) $\implies$ (1): Sia $\mathcal{J}(X) =: \mathfrak{m}$ un ideale massimale. Allora $X \neq \emptyset$ e $X \subset \mathrm{Zeri}(\mathfrak{m})$. Ciò implica $\mathrm{Zeri}(\mathfrak{m}) \neq \emptyset$, e per la prop. 9.7 esiste $\alpha \in K^n$ con $\mathfrak{m} = \mathfrak{m}_\alpha$ ed $\mathrm{Zeri}(\mathfrak{m}) = \{\alpha\}$. Da ciò segue evidentemente che anche $X = \{\alpha\}$.

Osservazione 14.36. Ogni sottoinsieme finito di K^n è algebrico.

Dimostrazione. (1) $\emptyset$ è algebrico per l'oss. 14.20.

(2) Dalla prop. 14.26 sappiamo che ogni punto di K^n è algebrico. L'enunciato segue dal cor. 14.6.

Proposizione 14.37. *I sottoinsiemi algebrici $\neq K$ di K coincidono con i sottoinsiemi finiti di K.*

Dimostrazione. (1) Per l'oss. 14.36 ogni sottoinsieme finito di K è algebrico.

(2) Sia X un sottoinsieme algebrico di K. Allora esiste un ideale I di $K[x]$ tale che $X = \mathrm{Zeri}(I)$. Però K è un anello ad ideali principali, per cui esiste $f \in K[x]$ con $I = K[x]_\smile f$. Perciò $X = \mathrm{Zeri}(f)$.

Per $f = 0$ otteniamo $X = K$, altrimenti f possiede solo un numero finito di zeri. X è proprio l'insieme di questi zeri e quindi finito.

Proposizione 14.38. *Sia $f \in K[x_1, \ldots, x_n]$. Allora l'applicazione indotta $f_{\text{app}} := \bigcirc_{\alpha} f(\alpha) : K^n \longrightarrow K$ è continua rispetto alle topologie di Zariski su K^n e K.*

Dimostrazione. Dobbiamo dimostrare che la controimmagine di ogni chiuso B di K è chiuso in K^n. Ciò è chiaro per $B = \emptyset$ oppure $B = K$.

Altrimenti per la prop. 14.37 $B = \{\lambda_1, \ldots, \lambda_m\}$ con $\lambda_1, \ldots, \lambda_m$.

Allora $f_{\text{app}}^{-1}(B) = \bigcup_{k=1}^{m} f_{\text{app}}^{-1}(\lambda_k)$, per cui è sufficiente dimostrare che per ogni $\lambda \in K$ la fibra $f_{\text{app}}^{-1}(\lambda)$ è chiusa in K^n.

Ma $f_{\text{app}}^{-1}(\lambda) = \{\alpha \in K^n \mid f(\alpha) = \lambda\} = (f - \lambda = 0)$ è chiuso (cioè algebrico), perché per $\lambda \in K$ anche $f - \lambda \in K[x_1, \ldots, x_n]$.

Proposizione 14.39. *Siano A un anello integro ed S un sottoinsieme infinito di A. Allora $\mathcal{J}(S^n, \text{in } A[x_1, \ldots, x_n]) = 0$.*

Concretamente ciò significa che un polinomio che si annulla su S^n è uguale al polinomio costante zero.

Dimostrazione. Testi di Algebra, ad es. Gabelli [21928], pag. 49.

Corollario 14.40. *K sia infinito. Allora:*

(1) $\mathcal{J}(K^n) = 0$.

(2) Se I è un ideale generalizzato di $K[x_1, \ldots, x_n]$ tale che $\text{Zeri}(I) = K^n$, allora $I = 0$.

Dimostrazione. (1) Segue dalla prop. 14.39.

(2) L'ipotesi implica $I \subset \mathcal{J}(\text{Zeri}(I)) = \mathcal{J}(K^n) = 0$.

Nota 14.41. Sia K un campo finito con q elementi.

Allora $\alpha^q = \alpha$ per ogni $\alpha \in K$.

Dimostrazione. Infatti $(K \setminus 0, \cdot)$ è un gruppo finito con $q - 1$ elementi, per cui $\alpha^{q-1} = 1$ e quindi anche $\alpha^q = \alpha$ per ogni $\alpha \in K \setminus 0$. L'ultima equazione vale però anche per $\alpha = 0$.

Corollario 14.42. *Sia K un campo finito con q elementi.*

Allora $\{x_1^q - x_1, \ldots, x_n^q - x_n\} \subset \mathcal{J}(K^n)$, per cui $\mathcal{J}(K^n) \neq 0$.

Osservazione 14.43. Un campo algebricamente chiuso è infinito.

Dimostrazione. Ciò segue dal fatto che la chiusura algebrica di un campo finito è infinito (e numerabile); cfr. Gabelli [21928], pag. 186.

Corollario 14.44. *K sia algebricamente chiuso. Allora $\mathcal{J}(K^n) = 0$.*

Lemma 14.45. *Siano A un anello commutativo, $P \in \text{Spec } A$ ed $I_1, \ldots, I_m$ ideali generalizzati di A.*

(1) Se $I_1 \cap \ldots \cap I_m \subset P$, allora esiste un j tale che $I_j \subset P$.

(2) Se $I_1 \cap \ldots \cap I_m = P$, allora esiste un j tale che $I_j = P$.

Dimostrazione. (1) L'ipotesi implica $I_1 I_2 \cdots I_m \subset P$, cosicché l'enunciato segue dal lemma 3.4.

(2) Ciò segue dal punto (1), perché l'ipotesi (2) implica $P \subset I_j$ per ogni j.

Lemma 14.46. *K sia infinito.*

(1) Siano X, Y chiusi di K^n, entrambi $\neq K^n$. Allora $X \cup Y \neq K^n$.

(2) Siano U, V aperti $\neq \emptyset$ di K^n. Allora $U \cap V \neq \emptyset$.

Dimostrazione. (1) Sia $X \cup Y = K^n$. Allora $\mathcal{J}(X) \cap \mathcal{J}(Y) \overset{14.8}{=} \mathcal{J}(X \cup Y) = \mathcal{J}(K^n) \overset{14.40}{=} 0$. Ma ciò non è possibile, perché l'ideale 0 nell'anello integro $K[x_1, \ldots, x_n]$ è primo e l'ipotesi implica che $\mathcal{J}(X), \mathcal{J}(Y) \neq 0$, contraddicendo il lemma 14.45.

(2) Segue da (1).

Corollario 14.47. *K sia infinito. Allora K^n non è uno spazio di Hausdorff nella topologia di Zariski.*

Dimostrazione. Siccome ovviamente K^n possiede almeno due punti (ne possiede un numero infinito), l'enunciato segue dal lemma 14.46.

Corollario 14.48. *K sia infinito ed X un sottoinsieme algebrico di K^n con $X \neq K^n$. Allora $K^n \setminus X$ è un insieme infinito.*

Dimostrazione. Se $Y := K^n \setminus X$ fosse finito, Y sarebbe un chiuso $\neq K^n$ per l'oss. 14.36; inoltre $K^n = X \cup Y$, in contrasto con il lemma 14.46.

Corollario 14.49. *K sia infinito.*

Allora K^n non è unione di un numero finito di ipersuperfici.

In particolare K^n non è unione di un numero finito di iperpiani.

Osservazione 14.50. I ragionamenti negli ultimi risultati possono essere formulati nel linguaggio della topologia generale, come faremo nei prossimi due capitoli.

15. Spazi topologici irriducibili

Sia X uno spazio topologico $\neq \emptyset$. X si dice irriducibile, se non è unione di due chiusi $\neq X$. Un sottoinsieme $Z \neq \emptyset$ di X è irriducibile se e solo se ogni volta che $Z \subset A \cup B$ con chiusi A, B si ha $Z \subset A$ oppure $Z \subset B$. X è irriducibile $\iff$ l'intersezione di due aperti $\neq \emptyset$ non è vuota $\iff$ ogni aperto $\neq \emptyset$ di X è denso $\iff$ ogni aperto $\neq \emptyset$ è irriducibile. Uno spazio irriducibile con più di due punti non è di Hausdorff. X è irriducibile se e solo se ogni aperto (e quindi in particolare X stesso) è connesso. Z è irriducibile se e solo se $\overline{Z}$ è irriducibile. Se X contiene un sottoinsieme irriducibile denso, allora X è irriducibile. Per $A \subset Y \subset X$ la chiusura di A in Y è data da $Y \cap \overline{A}$ ed A è denso in Y se e solo se $\overline{A} = \overline{Y}$. Se U è un aperto di X, allora esiste una biiezione naturale tra i chiusi irriducibili di U e i chiusi irriducibili Z di X con $Z \cap U \neq \emptyset$. L'immagine continua di un insieme irriducibile è irriducibile. Un sottoinsieme irriducibile massimale si chiama una componente irriducibile. Ogni componente irriducibile è chiusa. L'unione di una catena non vuota di insiemi irriducibili è irriducibile. Ogni sottoinsieme irriducibile è contenuto in una componente irriducibile. Ogni componente connessa di X (e quindi anche X stesso) è unione (in genere non disgiunta) di componenti irriducibili di X. Se X possiede un ricoprimento aperto concatenato, i cui elementi sono tutti irriducibili, allora X è irriducibile. Se $Z \subset X$ è irriducibile ed U è un aperto irriducibile con $Z \cap U \neq \emptyset$, allora $Z \cup U$ è irriducibile. Se un aperto irriducibile interseca una componente irriducibile, allora è contenuto in quella componente. Se $X = Z_1 \cup \ldots \cup Z_n$ con gli Z_k tutti irriducibili, allora ogni componente connessa coincide con uno degli $\overline{Z_k}$; in particolare X possiede solo un numero finito di componenti irriducibili. Se gli Z_k sono chiusi e non comparabili (rispetto all'inclusione insiemistica), allora essi sono esattamente le componenti irriducibili di X. Se X è connesso e unione di un numero finito di aperti irriducibili, allora X è irriducibile. Come si trovano le componenti irriducibili di un sottoinsieme. Sia K un campo. Un chiuso di K^n è irriducibile se e solo se $\mathcal{J}(X)$ è un ideale primo. Se K è infinito, allora K^n è irriducibile. Se K è algebricamente chiuso, allora si ha una biiezione naturale tra i chiusi irriducibili di K^n e gli ideali primi di $K[x_1, \ldots, x_n]$.

Situazione 15.1. Siano X sia uno spazio topologico e K un campo.

Definizione 15.2. X si dice *irriducibile*, se $X \neq \emptyset$ e X non può essere rappresentato come unione di due sottoinsiemi chiusi $\neq X$.

Lemma 15.3. *Sia Z un sottoinsieme $\neq \emptyset$ di X. Allora sono equivalenti:*

(1) Z è irriducibile.

(2) Se A e B sono chiusi di X con $Z \subset A \cup B$, allora $Z \subset A$ oppure $Z \subset B$.

Dimostrazione. (1) $\implies$ (2): Z sia irriducibile e A, B chiusi di X tali che $Z \subset A \cup B$. Allora $Z = (A \cap Z) \cup (B \cap Z)$. Siccome $A \cap Z$ e $B \cap Z$ sono chiusi in Z, l'ipotesi implica che ad esempio $Z = A \cap Z$, ovvero $Z \subset A$.

(2) $\implies$ (1): Siano A', B' chiusi di Z con $Z = A' \cup B'$. Allora esistono chiusi A, B di X con $A' = A \cap Z$, $B' = B \cap Z$.

Ciò implica $Z = (A \cap Z) \cup (B \cap Z) \subset A \cup B$ e per ipotesi si ha ad esempio $Z \subset A$, cioè $A' = A \cap Z = Z$.

Lemma 15.4. *Sia $X \neq \emptyset$. Allora sono equivalenti:*

(1) X è irriducibile.

(2) Se U e V sono aperti $\neq \emptyset$ di X, allora $U \cap V \neq \emptyset$.

(3) Ogni aperto $\neq \emptyset$ di X è denso in X.

(4) Ogni aperto $\neq \emptyset$ di X è irriducibile.

Dimostrazione. (1) $\iff$ (2): Chiaro, usando le regole di De Morgan.

(2) $\iff$ (3): Infatti un sottoinsieme U (non necessariamente aperto) di X è denso in X se e solo se $U \cap V \neq \emptyset$ per ogni aperto $V \neq \emptyset$ di X.

(2) $\implies$ (4): Usiamo il lemma 15.3. Siano U un aperto $\neq \emptyset$ di X ed A, B chiusi di X con $U \subset A \cup B$. Assumiamo, per assurdo, che $U \not\subset A$ e $U \not\subset B$. Allora gli aperti $U \setminus A$ e $U \setminus B$ sono $\neq \emptyset$, quindi per ipotesi $U \setminus (A \cup B) = (U \setminus A) \cap (U \setminus B) \neq \emptyset$, e ciò è impossibile perché $U \subset A \cup B$.

(4) $\implies$ (1): Chiaro.

Corollario 15.5. *X sia irriducibile e contenga almeno due punti. Allora X non è uno spazio di Hausdorff.*

Dimostrazione. Ciò segue dal punto (2) del lemma 15.4.

Definizione 15.6. Uno spazio topologico si dice *connesso*, se non è unione di due aperti disgiunti e $\neq \emptyset$.

Lemma 15.7. *Sia $X \neq \emptyset$. Allora sono equivalenti:*

(1) X è irriducibile.

(2) Ogni aperto di X è connesso.

Dimostrazione. (1) $\implies$ (2): Siano U un aperto di X e V, W aperti $\neq \emptyset$ di U tali che $U = V \cup W$ e $V \cap W = \emptyset$.

Ma V e W sono aperti anche in X e quindi per il lemma 15.4 si deve invece avere $V \cap W \neq \emptyset$.

(2) $\implies$ (1): Dimostriamo che è soddisfatta la condizione (2) del lemma 15.4. Siano U, V aperti $\neq \emptyset$ di X con $U \cap V = \emptyset$. Allora $U \cup V$ è un aperto non connesso di X, in contrasto con l'ipotesi.

Corollario 15.8. *X sia irriducibile. Allora ogni aperto $\neq \emptyset$ di X è denso, irriducibile e connesso. In particolare X stesso è connesso.*

Proposizione 15.9. *Sia $Z \subset X$. Allora sono equivalenti:*

(1) Z è irriducibile.

(2) $\overline{Z}$ è irriducibile.

Dimostrazione. (1) $\implies$ (2): Siccome $Z \neq \emptyset$, anche $\overline{Z} \neq \emptyset$.

Siano A, B chiusi di X con $\overline{Z} \subset A \cup B$. Allora anche $Z \subset A \cup B$, quindi per il lemma 15.3 ad esempio $Z \subset A$. Ciò implica $\overline{Z} \subset \overline{A} = A$.

(2) $\implies$ (1): Siccome $\overline{Z} \neq \emptyset$, anche $Z \neq \emptyset$.

Siano A, B chiusi di X con $Z \subset A \cup B$. Allora $\overline{Z} \subset \overline{A \cup B} = A \cup B$, quindi per ipotesi ad esempio $\overline{Z} \subset A$. Ciò implica $Z \subset A$.

Corollario 15.10. *X contenga un sottoinsieme irriducibile denso.*

Allora X è irriducibile.

Osservazione 15.11. Sia $A \subset Y \subset X$. Allora:

(1) La chiusura di A in Y è data da $Y \cap \overline{A}$.

(2) A è denso in Y se e solo se $\overline{A} = \overline{Y}$.

Dimostrazione. (1) Ad esempio Engelking [715], pag. 66.

(2) Sia A denso in Y. Per il punto (1) ciò significa $Y = Y \cap \overline{A}$, per cui $\overline{A} \subset \overline{Y} = \overline{Y \cap \overline{A}} \subset \overline{\overline{A}} = \overline{A}$.

Sia invece $\overline{A} = \overline{Y}$. Allora $Y \cap \overline{A} = Y \cap \overline{Y} = Y$.

Osservazione 15.12. Siano Z un sottoinsieme irriducibile di X ed U un aperto di X tale che $Z \cap U \neq \emptyset$.

Allora $\overline{Z \cap U} = \overline{Z}$.

Dimostrazione. $Z \cap U$ è un aperto $\neq \emptyset$ di Z e quindi denso in Z per il lemma 15.4. Per l'oss. 15.11 si ha $\overline{Z \cap U} = \overline{Z}$.

Proposizione 15.13. *Sia U un aperto di X. Allora esiste una biiezione*

$$\begin{array}{rcl} \{\textit{chiusi irriducibili di } U\} & \longleftrightarrow & \{\textit{chiusi irriducibili } Z \textit{ di } X \textit{ con } Z \cap U \neq \emptyset\} \\ A & \longmapsto & \overline{A} \\ Z \cap U & \longleftarrow\!\shortmid & Z \end{array}$$

Dimostrazione. (1) Sia A un chiuso irriducibile di U. Allora $\overline{A}$ è un chiuso irriducibile di X per la prop. 15.9, inoltre $\overline{A} \cap U = A \neq \emptyset$ per l'oss. 15.11.

(2) Sia Z un chiuso irriducibile di X con $Z \cap U \neq \emptyset$. Allora $Z \cap U$ è aperto in Z e perciò irriducibile per il lemma 15.4.

Inoltre $Z \cap U$ è chiuso in U e per l'oss. 15.12 si ha $\overline{Z \cap U} = \overline{Z} = Z$.

Proposizione 15.14. *Siano Y uno spazio topologico e $f : X \longrightarrow Y$ un'applicazione continua. Sia $Z \subset X$ irriducibile.*

Allora $f(Z)$ è irriducibile.

Dimostrazione. Siano A, B chiusi di Y con $f(Z) \subset A \cup B$.

Allora $Z \subset f^{-1}(f(Z)) \subset f^{-1}(A) \cup f^{-1}(B)$. Siccome gli ultimi due insiemi sono chiusi, per ipotesi ad esempio $Z \subset f^{-1}(A)$ e quindi $f(Z) \subset A$.

Corollario 15.15. *Sia Y uno spazio topologico omeomorfo ad X.*

Se X è irriducibile, anche Y è irriducibile.

Definizione 15.16. Un sottoinsieme irriducibile massimale di X si chiama una *componente irriducibile* di X.

Osservazione 15.17. Ogni componente irriducibile di X è chiusa.

Dimostrazione. Ciò è una conseguenza immediata della prop. 15.9.

Lemma 15.18. *Sia $\mathcal{C}$ una catena non vuota di sottoinsiemi irriducibili di X. Allora $\bigcup_{C \in \mathcal{C}} C$ è irriducibile.*

Dimostrazione. Sia $Z := \bigcup_{C \in \mathcal{C}} C$. Allora $Z \neq \emptyset$.

Siano A, B chiusi di X con $Z \subset A \cup B$. Assumiamo, per assurdo, che $Z \not\subset A$ e $Z \not\subset B$. Allora esistono $x, y \in Z$ tali che $x \notin A$ e $y \notin B$.

Siccome $\mathcal{C}$ è una catena, esiste $C \in \mathcal{C}$ tale che $x, y \in C$. Però C è irriducibile e naturalmente $C \subset A \cup B$, quindi per esempio $C \subset A$. Ciò implica $x \in A$, una contraddizione.

Proposizione 15.19. *Ogni sottoinsieme irriducibile di X è contenuto in una componente irriducibile di X.*

Dimostrazione. Ciò segue dal lemma di Zorn, usando il lemma 15.18.

Corollario 15.20. *Sia $X \neq \emptyset$. Allora X è unione (i.g. non disgiunta) di componenti irriducibili di X.*

Dimostrazione. Ogni punto di X è un insieme irriducibile. Pertanto l'enunciato segue dalla prop. 15.19.

L'unione i.g. non è disgiunta, come mostra l'esempio 15.36.

Corollario 15.21. *Sia $X \neq \emptyset$. Allora ogni componente connessa di X è unione di componenti irriducibili di X.*

Dimostrazione. Siccome ogni componente irriducibile C di X è connessa e queste ultime sono a due a due disgiunte, C deve essere contenuta in una ed una sola componente connessa di X. L'enunciato segue dal cor. 15.20.

Osservazione 15.22. Sia U un aperto di X. La biiezione della prop. 15.13 induce una biiezione tra l'insieme delle componenti irriducibili di U e le componenti irriducibili Z di X per le quali $Z \cap U \neq \emptyset$.

Lemma 15.23. *Sia $n \in \mathbb{N} + 1$ e siano dati aperti $U_0, \ldots, U_n$ di X tali che $U_i \cap U_{i+1} \neq \emptyset$ per $i = 0, \ldots, n-1$. Per ogni i con $0 < i < n$ l'insieme U_i sia irriducibile.*

Allora $U_0 \cap U_1 \cap \ldots \cap U_n \neq \emptyset$.

Dimostrazione. L'enunciato è banale per $n = 1$. Sia $n \geq 2$.

$U_0 \cap U_1$ e $U_1 \cap U_2$ sono aperti $\neq \emptyset$ dell'insieme irriducibile U_1, perciò $U_0 \cap U_1 \cap U_2$ è un aperto $\neq \emptyset$ dell'insieme irriducibile U_2, così come $U_2 \cap U_3$. Perciò $U_0 \cap U_1 \cap U_2 \cap U_3 \neq \emptyset$.

Di nuovo questo è un aperto $\neq \emptyset$ dell'insieme irriducibile U_3, così come $U_3 \cap U_4$. Perciò $U_0 \cap U_1 \cap U_2 \cap U_3 \cap U_4 \neq \emptyset$. E così via.

Definizione 15.24. Un insieme $\mathcal{R}$ di sottoinsiemi di X si dice *concatenato*, se per ogni $A, B \in \mathcal{R}$ esistono $n \in \mathbb{N} + 1$ e $C_0, \ldots, C_n \in \mathcal{R}$ tali che $C_0 = A$, $C_n = B$ e $C_i \cap C_{i+1} \neq \emptyset$ per $i = 0, \ldots, n-1$.

In particolare $\mathcal{R}$ è concatenato, se $A \cap B \neq \emptyset$ per ogni $A, B \in \mathcal{R}$.

Proposizione 15.25. *$\mathcal{R}$ sia un ricoprimento aperto concatenato di X. Ogni elemento di $\mathcal{R}$ sia irriducibile.*

Allora X è irriducibile.

Dimostrazione. Per il cor. 15.10 è sufficiente dimostrare che ogni elemento di $\mathcal{R}$ è denso in X.

Siano $U \in \mathcal{R}$ e W un aperto $\neq \emptyset$ di X. Dimostriamo che $U \cap W \neq \emptyset$.
Sia $V \in \mathcal{R}$ tale che $V \cap W \neq \emptyset$.

Per ipotesi esistono $C_0, \ldots, C_n \in \mathcal{R}$ tali che $C_0 = U$, $C_{n-1} = V$, $C_n = W$ e $C_i \cap C_{i+1} \neq \emptyset$ per $i = 0, \ldots, n-1$. Dal lemma 15.23 segue $C_0 \cap \ldots \cap C_n \neq \emptyset$. Ma questa intersezione è contenuta in $U \cap W$.

Corollario 15.26. *$\mathcal{R}$ sia un ricoprimento aperto di X tale che $U \cap V \neq \emptyset$ per ogni $U, V \in \mathcal{R}$. Ogni elemento di $\mathcal{R}$ sia irriducibile.*

Allora X è irriducibile.

Corollario 15.27. *Sia $n \in \mathbb{N} + 1$ e siano dati aperti irriducibili $U_0, \ldots, U_n$ di X tali che $U_i \cap U_{i+1} \neq \emptyset$ per $i = 0, \ldots, n-1$. Sia $X = U_0 \cup \ldots \cup U_n$.*

Allora X è irriducibile.

Dimostrazione. Per la prop. 15.25 è sufficiente dimostrare che il ricoprimento $\{U_0, \ldots, U_n\}$ è concatenato.

Sia $0 \leq i < j \leq n$. Allora $U_i \cap U_{i+1} \neq \emptyset, \ldots, U_{j-1} \cap U_j \neq \emptyset$.

Lemma 15.28. *Siano Z un sottoinsieme irriducibile di X ed U un aperto irriducibile di X tale che $Z \cap U \neq \emptyset$.*

Allora $Z \cup U$ è irriducibile.

Dimostrazione. Per il cor. 15.10 è sufficiente dimostrare che U è denso in $Z \cup U$. Per il lemma 15.12 abbiamo $\overline{Z \cap U} = \overline{Z}$, perciò

$$\overline{Z \cup U} = \overline{Z} \cup \overline{U} = \overline{Z \cap U} \cup \overline{U} = \overline{U}$$

cosicché dall'oss. 15.11 segue che U è denso in $Z \cup U$.

Corollario 15.29. *Siano Z una componente irriducibile di X ed U un aperto irriducibile di X tale che $Z \cap U \neq \emptyset$.*

Allora $U \subset Z$.

Dimostrazione. Per il lemma 15.28 $Z \cup U$ è ancora irriducibile.

Dalla massimalità di Z segue $Z \cup U = Z$, ovvero $U \subset Z$.

Lemma 15.30. *Sia $X = Z_1 \cup \ldots \cup Z_n$ con gli Z_k tutti irriducibili. Allora ogni componente irriducibile di X coincide con uno degli insiemi $\overline{Z_k}$.*

L'ipotesi implica quindi in particolare che X possiede solo un numero finito di componenti irriducibili.

Dimostrazione. In primo luogo si ha $X = \overline{Z_1} \cup \ldots \cup \overline{Z_n}$.

Sia C una componente irriducibile di X. Per il lemma 15.3 esiste un k tale che $C \subset \overline{Z_k}$. Siccome anche $\overline{Z_k}$ è irriducibile, dalla massimalità di C segue $C = \overline{Z_k}$.

Corollario 15.31. *(1) Sia $X = Z_1 \cup \ldots \cup Z_m$ con gli Z_k tutti irriducibili e chiusi e tali che $Z_i \not\subset Z_k$ per $i \neq k$. Allora $Z_1, \ldots, Z_m$ sono esattamente le componenti irriducibili di X.*

(2) Sia $X = Z_1 \cup \ldots \cup Z_m = Y_1 \cup \ldots \cup Y_n$ con gli Z_k, Y_j tutti irriducibili e chiusi e tali che $Z_i \not\subset Z_k$ per ogn $i \neq k$ e $Y_i \not\subset Y_k$ per ogni $i \neq k$.

Allora $m = n$ e gli Y_j coincidono, a parte la numerazione, con gli Z_k.

Proposizione 15.32. *Sia $X = U_1 \cup \ldots \cup U_n$ con gli U_k aperti irriducibili. X sia connesso.*

Allora X è irriducibile.

Dimostrazione. Seguiamo Görtz/ [21712], p. 14.

Per il lemma 15.30 X possiede solo un numero finito di componenti irriducibili, ad esempio $X_1, \ldots, X_m$ con gli X_j tutti distinti. Assumiamo, per assurdo, che X non sia irriducibile. Allora necessariamente $m \geq 2$.

Siccome X è connesso, si deve avere $X_1 \cap (X_2 \cup \ldots \cup X_m) \neq \emptyset$. Quindi si ha ad esempio $X_1 \cap X_2 \neq \emptyset$, con $X_1 \neq X_2$.

L'ipotesi implica inoltre che esiste un k con $X_1 \cap X_2 \cap U_k \neq \emptyset$.

Dal cor. 15.29 si ha allora $U_k \subset X_1 \cap X_2$ e ciò implica $\overline{U_k} = \overline{X_1} = X_1$ e $\overline{U_k} = \overline{X_2} = X_2$, sicché $X_1 = X_2$, una contraddizione.

Proposizione 15.33. *Sia $Y \subset X$. Y possieda solo un numero finito di componenti irriducibili. Queste siano $Y_1, \ldots, Y_m$, tutte distinte. Allora:*

(1) $\overline{Y_i} \not\subset \overline{Y_j}$ per $i \neq j$.

(2) Le componenti irriducibili di $\overline{Y}$ sono esattamente gli insiemi $\overline{Y_1}, \ldots, \overline{Y_m}$.

Dimostrazione. (1) Sia $\overline{Y_i} \subset \overline{Y_j}$. Siccome gli Y_k sono chiusi di Y, dall'oss. 15.11 abbiamo $Y_i = Y \cap \overline{Y_i} \subset Y \cap \overline{Y_j} = Y_j$, in contrasto con l'ipotesi che gli Y_k siano tutti distinti e quindi anche inconfrontabili rispetto all'inclusione insiemistica.

(2) Siccome $\overline{Y} = \overline{Y_1} \cup \ldots \cup \overline{Y_m}$, l'enunciato segue adesso dal cor. 15.31.

Teorema 15.34. *Sia $X \subset K^n$. Allora sono equivalenti:*

(1) X è irriducibile.

(2) $\mathcal{J}(X)$ è un ideale primo.

Dimostrazione. (1) $\implies$ (2): L'ideale generalizzato $\mathcal{J}(X)$ è un ideale, perché $X \neq \emptyset$. Siano $f, g \in K[x_1, \ldots, x_n]$ tali che $fg \in \mathcal{J}(X)$.

Allora $X \subset \mathrm{Zeri}(fg) = \mathrm{Zeri}(f) \cup \mathrm{Zeri}(g)$. Siccome X è irriducibile, ciò implica che ad esempio $X \subset \mathrm{Zeri}(f)$ e quindi $f \in \mathcal{J}(X)$.

(2) $\implies$ (1): Se $\mathcal{J}(X)$ è un ideale primo, necessariamente $X \neq \emptyset$.

Siano A, B chiusi di K^n con $X \subset A \cup B$.

Allora $\mathcal{J}(A) \cap \mathcal{J}(B) = \mathcal{J}(A \cup B) \subset \mathcal{J}(X)$ e quindi ad esempio $\mathcal{J}(A) \subset \mathcal{J}(X)$ per il lemma 14.45.

Il cor. 14.29 implica $X \subset \overline{A} = A$.

Corollario 15.35. *Sia K infinito. Allora K^n è irriducibile.*

Dimostrazione. Ciò è stato dimostrato nel lemma 14.46 e segue anche dal teorema 15.34, perché $\mathcal{J}(K^n) = 0$ è un ideale primo.

Esempio 15.36. Sia $X := \mathrm{Zeri}(xy) \subset K^2$. Allora $X = \mathrm{Zeri}(x) \cup \mathrm{Zeri}(y)$.

Se K è infinito, gli insiemi $\mathrm{Zeri}(x)$ e $\mathrm{Zeri}(y)$ sono irriducibili (ad esempio per la prop. 15.14, se li consideriamo come ottenuti tramite proiezioni $K^2 \longrightarrow K^2$) e chiusi, sicché il cor. 15.31 implica che essi coincidono con le componenti connesse di X.

Però $\mathrm{Zeri}(x) \cap \mathrm{Zeri}(y) = \{(0,0)\} \neq \emptyset$.

Corollario 15.37. *Sia K algebricamente chiuso. La biiezione della prop. 14.17 induce allora una biiezione naturale*

$$\begin{aligned} \{\textit{chiusi irriducibili di } K^n\} &\longleftrightarrow \operatorname{Spec} K[x_1, \ldots, x_n] \\ X &\longmapsto \mathcal{J}(X) \\ \mathrm{Zeri}(P) &\longleftarrow\!\shortmid P \end{aligned}$$

Dimostrazione. Prop. 14.17 e teorema 15.34.

16. Spazi topologici noetheriani

Sia X uno spazio topologico. X si dice noetheriano, se ogni successione discendente di chiusi (o equivalentemente ogni successione ascendente di aperti) diventa stazionaria. X è noetheriano se e solo se ogni catena non vuota di chiusi contiene la propria intersezione (o ogni catena non vuota di aperti contiene la propria unione) e se e solo se ogni ogni insieme non vuoto di chiusi contiene un elemento minimale (o ogni insieme non vuoto di aperti contiene un elemento massimale). Ogni sottospazio di uno spazio noetheriano è noetheriano. Un'unione finita di spazi noetheriani è uno spazio noetheriano. Uno spazio noetheriano è compatto. X è noetheriano se e solo se ogni sottoinsieme di X è compatto e se e solo se ogni aperto di X è compatto. Uno spazio noetheriano possiede solo un numero finito di componenti irriducibili (e quindi anche solo un numero finito di componenti connesse). Uno spazio noetheriano infinito non è di Hausdorff. Sia K un campo. K^n è noetheriano nella topologia di Zariski. Ogni sottoinsieme algebrico di K^n è unione di un numero finito di insiemi algebrici irriducibili non comparabili insiemisticamente e questi sono univocamente determinati. Se K è algebricamente chiuso, allora ogni ideale radicale di $K[x_1, \ldots, x_n]$ è intersezione di un numero finito di ideali primi non comparabili insiemisticamente e questi sono univocamente determinati.

Situazione 16.1. Siano X uno spazio topologico e K un campo.

Definizione 16.2. X si dice *noetheriano*, se per ogni successione infinita discendente $A_0 \supset A_1 \supset A_2 \supset \ldots$ di chiusi di X esiste un $k \in \mathbb{N}$ tale che $A_i = A_k$ per ogni $i \geq k$.

Proposizione 16.3. *Sono equivalenti:*

(1) X è noetheriano.

(2) Per ogni successione infinita ascendente $U_0 \subset U_1 \subset U_2 \subset \ldots$ di aperti di X esiste un $k \in \mathbb{N}$ tale che $U_i = U_k$ per ogni $i \geq k$.

(3) Per ogni catena non vuota $\mathcal{C}$ di chiusi di X si ha $\bigcap_{A \in \mathcal{C}} A \in \mathcal{C}$.

(4) Per ogni catena non vuota $\mathcal{C}$ di aperti di X si ha $\bigcup_{U \in \mathcal{C}} U \in \mathcal{C}$.

(5) Ogni insieme non vuoto di chiusi di X possiede un elemento minimale.

(6) Ogni insieme non vuoto di aperti di X possiede un elemento massimale.

Dimostrazione. (1) $\iff$ (2): Chiaro.

(1) $\implies$ (3): Siano $\mathcal{C}$ una catena non vuota di chiusi e $B := \bigcap_{A \in \mathcal{C}} A \notin \mathcal{C}$. Scegliamo $A_1 \in \mathcal{C}$. Allora $A_1 \neq B$. Ciò significa che esiste $A_2 \in \mathcal{C}$ tale che $A_2 \subsetneqq A_1$ (qui usiamo che $\mathcal{C}$ è una catena). Ma anche $A_2 \neq B$.

Perciò esiste $A_3 \in \mathcal{C}$ tale che $A_3 \subsetneqq A_2$, ecc. Per ipotesi non possiamo continuare all'infinito in questo modo e ciò mostra che la premessa $B \notin \mathcal{C}$ non si può verificare.

(3) $\iff$ (4): Chiaro.

(3) $\implies$ (5): Ciò segue dal lemma di Zorn.

(5) $\iff$ (6): Chiaro.

(5) $\implies$ (1): Chiaro.

Osservazione 16.4. Siano X noetheriano ed $Y \subset X$.

Allora Y è noetheriano.

Dimostrazione. Sia $\mathcal{A}$ un insieme non vuoto di chiusi di Y.
Allora l'insieme $\{\overline{A} \mid A \in \mathcal{A}\}$ possiede un elemento minimale $\overline{B}$ con $B \in \mathcal{A}$.

Ciò implica $B \overset{15.11}{=} \overline{B} \cap Y \subset \overline{A} \cap Y = A$ per ogni $A \in \mathcal{A}$.

Lemma 16.5. *Sia $X = X_1 \cup \ldots \cup X_m$ con gli X_j tutti noetheriani.*

Allora X è noetheriano.

Dimostrazione. Sia $A_0 \supset A_1 \supset A_2 \supset \ldots$ una catena infinita discendente di chiusi di X. Per ogni j allora $A_0 \cap X_j \supset A_1 \cap X_j \supset A_2 \cap X_j \supset \ldots$ è una catena infinita discendente di chiusi di X_j, perciò esiste un indice k_j tale che $A_i \cap X_j = A_{k_j} \cap X_j$ per ogni $i \geq k_j$.

Se poniamo $k := \max(k_1, \ldots, k_m)$, abbiamo quindi $A_i \cap X_j = A_k \cap X_j$ per ogni j e ogni $i \geq k$.

Per $i \geq k$ abbiamo perciò $A_i = \bigcup_{j=1}^{m} (A_i \cap X_j) = \bigcup_{j=1}^{m} (A_k \cap X_j) = A_k$.

Lemma 16.6. *Sia X noetheriano. Allora X è compatto.*

Dimostrazione. Siano $\mathcal{R}$ un ricoprimento aperto di X ed $\mathcal{F}$ l'insieme delle unioni finite di elementi di $\mathcal{R}$. Ogni elemento di $\mathcal{F}$ è aperto, perciò $\mathcal{F}$ contiene un elemento massimale U. Dimostriamo che $U = X$.

Altrimenti esistono $x \in X \setminus U$ e per esso un elemento $V \in \mathcal{R}$ con $x \in V$, cosicché $U \cup V \supsetneq U$. Ma ovviamente anche $U \cup V \in \mathcal{F}$, in contrasto con la massimalità di U.

Proposizione 16.7. *Sono equivalenti:*

(1) X è noetheriano.

(2) Ogni sottoinsieme di X è compatto.

(3) Ogni aperto di X è compatto.

Dimostrazione. (1) $\implies$ (2): Sia $A \subset X$. Per l'oss. 15.4 A è noetheriano e quindi compatto per il lemma 15.6.

(2) $\implies$ (3): Chiaro.

(3) $\implies$ (1): Sia $\mathcal{C}$ una catena non vuota di aperti di X. Poniamo $W := \bigcup_{U \in \mathcal{C}} .$
Allora W è un aperto di X e $\mathcal{C}$ è un ricoprimento aperto di W.

Per ipotesi esistono $U_1, \ldots, U_m \in \mathcal{C}$ tali che $W = U_1 \cup \ldots \cup U_m$. Siccome $\mathcal{C}$ è una catena, si ha ad esempio $W = U_1 \in \mathcal{C}$.

Proposizione 16.8. *X sia noetheriano. Allora X possiede solo un numero finito di componenti irriducibili.*

Dimostrazione. Seguiamo Görtz/ [21712], p. 15.

Per il lemma 15.30 è sufficiente dimostrare che X può essere rappresentato come unione di un numero finito di sottoinsiemi irriducibili.

Dimostriamo invece (come enunciato più forte) che ogni sottoinsieme chiuso $\neq \emptyset$ di X è unione di un numero finito di sottoinsiemi irriducibili.

Sia quindi $\mathcal{L}$ l'insieme dei sottoinsiemi chiusi $\neq \emptyset$ di X che non sono unione di un numero finito di sottoinsiemi irriducibili. Assumiamo, per assurdo, che $\mathcal{L} \neq \emptyset$.

Siccome X è noetheriano, $\mathcal{L}$ possiede un elemento minimale Z. Allora Z non può essere irriducibile, perciò esistono chiusi A, B di Z tali che $Z = A \cup B$ con $A, B \subsetneqq Z$ e perciò $A, B \neq \emptyset$. Siccome Z è chiuso, A e B sono chiusi anche in X. La minimalità di Z implica $A, B \notin \mathcal{L}$.

Entrambi sono perciò unioni di un numero finito di sottoinsiemi irriducibili e quindi lo stesso vale per Z, una contraddizione.

Corollario 16.9. *X sia noetheriano. Allora X possiede solo un numero finito di componenti connesse.*

Osservazione 16.10. X sia noetheriano. Se X è di Hausdorff, allora X è finito.

Dimostrazione. Per la prop.16.8 X è unione di un numero finito di sottospazi irriducibili $Z_1, \ldots, Z_m$. Se X è di Hausdorff, ogni Z_j è di Hausdorff e consiste quindi, per il cor. 15.5, di un punto solo.

Proposizione 16.11. *K^n è uno spazio noetheriano nella topologia di Zariski.*

Dimostrazione. Per la prop. 14.17 esiste una biiezione canonica tra l'insieme dei chiusi di K^n e l'insieme degli ideali generalizzati di $K[x_1, \ldots, x_n]$. Questa biiezione è compatibile con l'inclusione insiemistica per la prop. 14.15 e il cor. 14.30.

Siccome l'anello $K[x_1, \ldots, x_n]$ è noetheriano per il teorema della base di Hilbert, si ottiene direttamente la validità della condizione nella def. 16.2.

Teorema 16.12. *Sia $X \subset K^n$ un insieme algebrico. Allora esistono insiemi algebrici irriducibili $X_1, \ldots, X_m \subset K^n$ tali che $X = X_1 \cup \ldots \cup X_m$ con $X_i \not\subset X_j$ per $i \neq j$.*

Gli insiemi X_j sono (a parte la numerazione) univocamente determinati.

Dimostrazione. Ciò segue dalle prop. 16.11 e 16.8, tenendo conto del cor. 15.31.

Corollario 16.13. *K sia algebricamente chiuso. Sia I un ideale radicale di $K[x_1, \ldots, x_n]$. Allora I può essere rappresentato come intersezione $P_1 \cap \ldots \cap P_m$ di ideali primi tali che $P_i \not\subset P_j$ per $i \neq j$ e (a parte la numerazione) univocamente determinati da questa condizione.*

Dimostrazione. Ciò è una conseguenza diretta del teorema 16.12 e del corollario 14.19.

17. Anelli locali

Un anello commutativo A si dice locale, se possiede un unico ideale massimale $\mathfrak{m}$; il campo $A/\mathfrak{m}$ si chiama campo residuo di A. Ogni campo è un anello locale. A è locale se e solo se gli elementi non invertibili formano un ideale (che in tal caso è proprio l'unico ideale massimale). Se $(A, \mathfrak{m})$ è locale, per ogni $r \in \mathfrak{m}$ l'elemento $1 + r$ è invertibile. Un omomorfismo $(A, \mathfrak{m}) \longrightarrow (B, \mathfrak{n})$ si dice locale, se $\varphi(\mathfrak{m}) \subset \mathfrak{n}$. In tal caso $\varphi^{-1}(\mathfrak{n}) = \mathfrak{m}$. Ogni immagine omomorfa di un anello locale è un anello locale. Un ideale Q di A si dice primario, se $ab \in Q$ con $a \notin Q$ implica $b \in \sqrt{Q}$. Ogni ideale primo è primario. Il radicale di un ideale primario è primo. Q si dice P-primario, se Q è primario e $\sqrt{Q} = P$. Un'intersezione finita di ideali P-primari è un ideale P-primario. La controimmagine del radicale di un ideale è il radicale della controimmagine dell'ideale. La controimmagine di un ideale P-primario è un ideale $\varphi^{-1}(P)$ primario. Una potenza di un ideale primo non è necessariamente un ideale primario. Esempi. Invece la potenza di un ideale massimale $\mathfrak{m}$ è un ideale $\mathfrak{m}$-primario. Infatti ogni ideale, il cui radicale è un ideale massimale, è primario.

Situazione 17.1. Sia A un anello commutativo $\neq 0$.

Definizione 17.2. L'anello A si dice *locale*, se possiede un unico ideale massimale.

Osservazione 17.3. Sia A un anello locale con ideale massimale $\mathfrak{m}$. Allora $k := A/\mathfrak{m}$ è un campo.

Perciò in tal caso si usa spesso la dizione „sia $(A, \mathfrak{m})$ un anello locale“ oppure „sia $(A, \mathfrak{m}, k)$ un anello locale“.

Definizione 17.4. Sia $(A, \mathfrak{m})$ un anello locale. Allora il campo $A/\mathfrak{m}$ si chiama il *campo residuo* di A.

Esempio 17.5. (1) Ogni campo è un anello locale.

(2) Siano p un numero primo, $\in \mathbb{N} + 1$ ed $A := \mathbb{Z}/p^m$. Allora A possiede un unico ideale primo $(p\mathbb{Z}/p^m)$ ed è quindi in particolare locale con campo residuo $\mathbb{Z}/p^m/p\mathbb{Z}/p^m \cong \mathbb{Z}/p$. Per $m \geq 2$ però A non è un campo.

Lemma 17.6. *Le seguenti condizioni sono equivalenti:*

(1) A è locale.

(2) L'insieme degli elementi non invertibili di A è un ideale.

(3) La somma di due elementi non invertibili di A non è invertibile.

(4) Se $a, b \in A$ sono tali che $a + b = 1$, allora almeno uno degli elementi a e b è invertibile.

Dimostrazione. (1) $\implies$ (2): Sia $\mathfrak{m}$ l'unico ideale massimale di A. Siano a e b elementi non invertibili di A. Allora Aa e Ab sono ideali di A e quindi entrambi contenuti in $\mathfrak{m}$. Ciò implica $a + b \in \mathfrak{m}$ e $ca \in \mathfrak{m}$ per ogni $c \in A$, per cui gli elementi $a + b$ e ca non possono essere invertibili.

(2) $\implies$ (3) $\iff$ (4): Chiaro.

(3) $\implies$ (1): Sia $\mathfrak{m}$ l'insieme degli elementi non invertibili di A. Per $a, b \in \mathfrak{m}$ l'ipotesi (3) implica allora $a+b \in \mathfrak{m}$. Inoltre è chiaro che $ca \in \mathfrak{m}$ per ogni $c \in A$. Pertanto $\mathfrak{m}$ è un ideale di A.

Sia ora I un ideale di A. Allora gli elementi di I sono tutti non invertibili, quindi si ha $I \subset \mathfrak{m}$.

Corollario 17.7. *Sia $(A, \mathfrak{m})$ un anello locale. Allora ogni elemento di $A \setminus \mathfrak{m}$ è invertibile (mentre naturalmente tutti gli elementi di $\mathfrak{m}$ sono non invertibili).*

Proposizione 17.8. *Sia $(A, \mathfrak{m})$ un anello locale. Allora per ogni $r \in \mathfrak{m}$ l'elemento $1 + r$ è invertibile.*

Dimostrazione. È chiaro che per $r \in \mathfrak{m}$ si ha $1 + r \notin \mathfrak{m}$. L'enunciato segue perciò dal cor. 17.7. È anche contenuto nella prop. 3.57.

Proposizione 17.9. *Sia $\mathfrak{m}$ un ideale massimale di A tale che $1 + r$ è invertibile per ogni $r \in \mathfrak{m}$.*

Allora $\mathfrak{m}$ è l'unico ideale massimale di A.

Dimostrazione. Sia a un elemento non invertibile di A. Dimostriamo che $a \in \mathfrak{m}$. Assumiamo, per assurdo, che $a \notin \mathfrak{m}$. Allora $Aa + \mathfrak{m} = A$, per cui esistono $b \in A$ ed $r \in \mathfrak{m}$ tali che $ab + r = 1$. Per ipotesi $ab = 1 - r$ è invertibile, ma ciò implicherebbe che anche a è invertibile in contrasto con le assunzioni.

Osservazione 17.10. Sia $(A, \mathfrak{m})$ un anello locale. Allora $\mathfrak{m}$ coincide con il radicale di Jacobson di A.

Definizione 17.11. Siano $(A, \mathfrak{m})$ e $(B, \mathfrak{n})$ anelli locali. Un omomorfismo di anelli $\varphi : A \longrightarrow B$ si dice *locale*, se $\varphi(\mathfrak{m}) \subset \mathfrak{n}$.

Osservazione 17.12. Siano $(A, \mathfrak{m})$ e $(B, \mathfrak{n})$ anelli locali e $\varphi : A \longrightarrow B$ un omomorfismo locale. Allora:

(1) $\varphi^{-1}(\mathfrak{n}) = \mathfrak{m}$.

(2) φ induce un omomorfismo (necessariamente iniettivo)
$\overline{\varphi} := \bigcirc\limits_{a+\mathfrak{m}} \varphi a + \mathfrak{n} : A/\mathfrak{m} \longrightarrow B/\mathfrak{n}$.

(3) Se φ è suriettivo, anche $\overline{\varphi}$ è suriettivo e quindi un isomorfismo.
In questo caso si ha inoltre $\varphi(\mathfrak{m}) = \mathfrak{n}$.

Dimostrazione. (1) Per ipotesi $\varphi(\mathfrak{m}) \subset \mathfrak{n}$. Ciò implica $\mathfrak{m} \subset \varphi^{-1}(\mathfrak{n})$.
Ma $\varphi^{-1}(\mathfrak{n})$ è un ideale di A per il lemma 3.18 e deve quindi coincidere con $\mathfrak{m}$, perché $\mathfrak{m}$ è massimale.

(2) L'applicazione $\bigcirc\limits_{a+\mathfrak{m}} \varphi a + \mathfrak{n}$ è ben definita ed è chiaro che si tratta di un omomorfismo.

(3) Siano φ suriettivo e $b + \mathfrak{n} \in B/\mathfrak{n}$. Allora esiste $a \in A$ tale che $b = \varphi a$, sicché $b + \mathfrak{n} = \overline{\varphi}(a + \mathfrak{m})$.

Infine, per la suriettività di φ si ha $\varphi(\mathfrak{m}) = \varphi(\varphi^{-1}(\mathfrak{n})) = \mathfrak{n}$.

Esempio 17.13. Siano $(A, \mathfrak{m})$ un anello locale ed I un ideale di A. Allora A/I è un anello locale con ideale massimale $\mathfrak{m}/I$.

La proiezione canonica $\pi : A \longrightarrow A/I$ è un omomorfismo locale, perché $\varphi(\mathfrak{m}) = \mathfrak{m}/I$, perciò dall'oss. 17.12 segue che π induce un isomorfismo naturale (e ovvio) $\overline{\pi} : A/\mathfrak{m} \longrightarrow A/I/\mathfrak{m}/I$ dei campi residui.

Definizione 17.14. Un ideale Q di A si dice *primario*, se è soddisfatta la seguente condizione:

Se $a, b \in A$ sono tali che $ab \in Q$ ed $a \notin Q$, allora $b \in \sqrt{Q}$.

Osservazione 17.15. Ogni ideale primo è primario.

Osservazione 17.16. Un ideale Q di A è primario se e solo se ogni zero-divisore di A/Q è nilpotente.

Proposizione 17.17. *Sia Q un ideale primario di A. Allora il suo radicale $\sqrt{Q}$ è primo ed è quindi il più piccolo ideale primo che contiene Q.*

Dimostrazione. Siano $a, b \in A$ tali che $ab \in \sqrt{Q}$. Allora esiste $n \in \mathbb{N}$ tale che $a^n b^n = (ab)^n \in Q$. Sia $a \notin \sqrt{Q}$. Allora $a^n \notin Q$. Siccome Q è primario, ciò implica $b^n \in \sqrt{Q}$, ovvero $b \in \sqrt{\sqrt{Q}} = \sqrt{Q}$.

Definizione 17.18. Sia $P \in \operatorname{Spec} A$. Un ideale *$P$-primario* è un ideale primario il cui radicale coincide con P.

Osservazione 17.19. Siano $P \in \operatorname{Spec} A$ e Q un ideale P-primario. Sia Q_1 un ideale di A con $Q \subset Q_1 \subset P$.

Allora anche Q_1 è P-primario.

Dimostrazione. (1) In primo luogo si ha $P = \sqrt{Q} \subset \sqrt{Q_1} \subset \sqrt{P} = P$, per cui $\sqrt{Q_1} = P$.

(2) Siano $a, b \in A$ con $ab \in Q_1$, ma $a \notin Q_1$. Allora $a \notin Q$ e quindi $b \in P$.

Questa osservazione, di cui la dimostrazione è immediata, viene spesso usata.

Lemma 17.20. *Siano $P \in \operatorname{Spec} A$ e $Q_1, \ldots, Q_n$ ideali P-primari.*

Allora anche $Q_1 \cap \ldots \cap Q_n$ è P-primario.

Dimostrazione. Sia $Q := Q_1 \cap \ldots \cap Q_n$.

(1) Per il lemma 3.45 $\sqrt{Q} = P$.

(2) Siano $a, b \in A$ tali che $ab \in Q$ ed $a \notin Q$. Allora $a \notin Q_i$ per qualche $i \in \{1, \ldots, n\}$, mentre naturalmente $ab \in Q_i$, per cui $b \in \sqrt{Q_i} = P$.

Osservazione 17.21. Siano B un anello commutativo, $\varphi : A \longrightarrow B$ un omomorfismo di anelli ed I un ideale generalizzato di B.

Allora $\sqrt{\varphi^{-1}(I)} = \varphi^{-1}(\sqrt{I})$.

Dimostrazione. (1) Sia $a \in \sqrt{\varphi^{-1}(I)}$. Allora esiste $n \in \mathbb{N}$ con $a^n \in \varphi^{-1}(I)$, ovvero $(\varphi a)^n = \varphi a^n \in I$ e quindi $\varphi a \in \sqrt{I}$, per cui $a \in \varphi^{-1}(\sqrt{I})$.

(2) Sia $\varphi a \in \sqrt{I}$. Allora esiste $n \in \mathbb{N}$ con $\varphi a^n = (\varphi a)^n \in I$, per cui $a^n \in \varphi^{-1}(I)$ e quindi $a \in \sqrt{\varphi^{-1}(I)}$.

Osservazione 17.22. Siano B un anello commutativo, $\varphi : A \longrightarrow B$ un omomorfismo di anelli, $P \in \operatorname{Spec} B$ e Q un ideale P-primario di B. Allora $\varphi^{-1}(Q)$ è un ideale $\varphi^{-1}(P)$-primario di A.

Dimostrazione. (1) $\varphi^{-1}(Q)$ è un ideale per il lemma 3.18.

(2) Siano $a, b \in A$ tali che $ab \in \varphi^{-1}(Q)$ ed $a \notin \varphi^{-1}(Q)$. Allora $\varphi a \cdot \varphi b \in Q$ e $\varphi a \notin Q$, per cui esiste $n \in \mathbb{N}$ tale che $\varphi b^n = (\varphi b)^n \in Q$, cosicché $b^n \in \varphi^{-1}(Q)$.

(3) Per l'oss. 17.21 si ha infine $\sqrt{\varphi^{-1}(Q)} = \varphi^{-1}(\sqrt{Q}) = \varphi^{-1}(P)$.

Osservazione 17.23. Siano I un ideale di A e $P \in \operatorname{Spec} A$ tali che $P^n \subset I \subset P$ per qualche $n \in \mathbb{N}$.

Allora $\sqrt{I} = P$.

Dimostrazione. Per ipotesi si ha $\sqrt{P^n} \subset \sqrt{I} \subset \sqrt{P}$. Dal lemma 3.45 segue che $\sqrt{P^n} = \sqrt{P} = P$, per cui $\sqrt{I} = P$.

Nota 17.24. (1) Se il radicale $\sqrt{I}$ di un ideale I è primo, ciò non implica che I sia primario (esempio 17.25).

(2) Infatti nemmeno una potenza di un ideale primo è necessariamente un ideale primario (esempio 17.26).

(3) Se invece il radicale $\sqrt{I}$ di un ideale I è un ideale massimale, allora I è primario (prop. 17.27).

(4) Ogni potenza di un ideale massimale è quindi un ideale primario (cor. 17.29).

Esempio 17.25. Siano K un campo e $I := K[x, y]_{\smile}(x^2, xy)$. Allora:

(1) $P := K[x, y]_{\smile}(x)$ è un ideale primo con $P^2 \subset I \subset P$.

(2) Perciò $\sqrt{I} = P$ è primo.

(3) I non è però un ideale primario.

Dimostrazione. Dobbiamo solo dimostrare il punto (3). Ciò è però evidente, perché $xy \in I$ ed $x \notin I$, mentre $y \notin \sqrt{I} = P$.

Esempio 17.26. Siano K un campo ed $A := K[x, y, z]/(xy - z^2)$. Siano $\overline{x}, \overline{y}, \overline{z}$ le classi di x, y, z in A e $P := A_{\smile}(\overline{x}, \overline{z})$. Allora:

(1) P è primo.

(2) P^2 non è primario.

Dimostrazione. (1) $A/P \cong K[y]$ è integro.

(2) $\overline{x}\overline{y} = \overline{z}^2 \in P^2$, ma $\overline{x} \notin P^2$ e $\overline{y} \notin \sqrt{P^2} = P$.

Proposizione 17.27. *Sia Q un ideale di A tale che $\sqrt{Q}$ è massimale. Allora:*

(1) $\sqrt{Q}$ è l'unico ideale primo che contiene Q.

(2) A/Q è un anello locale con ideale massimale $\sqrt{Q}/Q$.

(3) Q è primario.

Dimostrazione. (1) Ciò segue dal cor. 3.40.

(2) Chiaro, tenendo conto di (1).

(3) Siano $a, b \in A$ tali che $ab \in Q$ con $b \notin \sqrt{Q}$. Dal punto (2) e dal cor. 17.7 segue che b è invertibile in A/Q. Perciò esistono $c \in A$ e $q \in Q$ tali che $1 = bc + q$. Ma allora $a = abc + aq \in Q + Q = Q$.

Corollario 17.28. *Siano Q un ideale di A ed $\mathfrak{m} \in \operatorname{Max} A$ tali che $\mathfrak{m}^n \subset Q \subset \mathfrak{m}$ per qualche $n \in \mathbb{N}$. Allora:*

(1) $\sqrt{Q} = \mathfrak{m}$.

(2) Q è $\mathfrak{m}$-primario.

Dimostrazione. (1) Ciò segue dall'oss. 17.23.

(2) Prop. 17.27.

Corollario 17.29. *Sia $\mathfrak{m} \in \operatorname{Max} A$. Allora $\mathfrak{m}^n$ è primario per ogni $n \in \mathbb{N} + 1$.*

Nota 17.30. Anelli locali sono onnipresenti nell'algebra commutativa. Infatti, come vedremo, per ogni ideale primo P la localizzazione A_P è un anello locale con ideale massimale PA_P.

18. Il lemma di Nakayama

Il lemma di Nakayama è un risultato tecnico che viene usato molto spesso per dimostrare che un modulo si annulla o che due moduli sono uguali. Per la dimostrazione si usa il trucco del determinante, applicando la regola di Cramer astratta - $T_{\mathrm{ad}}T = TT_{\mathrm{ad}} = (\det T)\cdot\delta$ - all'anello $A[\varphi]$, dove φ è un endomorfismo del modulo M considerato, ottenendo una generalizzazione del teorema di Cayley-Hamilton: Se il modulo M è finitamente generato, I è un ideale generalizzato e φ un endomorfismo di M con $\varphi M \subset IM$, allora φ è zero di un polinomio monico con coefficienti in I. Anche nel seguito sia M finitamente generato (questa ipotesi è necessaria per la validità dei risultati). Se I è un ideale generalizzato con $IM = M$, allora esiste $t \in 1 + I$ tale che $tM = 0$. Da ciò si deduce che un endomorfismo suriettivo di un modulo finitamente generato è anche iniettivo. Lemma di Nakayama: Se I è un ideale contenuto nel radicale di Jacobson di A e se $IM = M$, allora $M = 0$ (oppure, diversamente formulato, se $M \neq 0$, allora $IM \neq M$). Da ciò si ottiene un criterio di uguaglianza: Se N è un sottomodulo di M e I è un ideale contenuto nel radicale di Jacobson di A tale che $M = N + IM$, allora $M = N$. Quindi se in un anello locale $(A, \mathfrak{m})$ si ha $M = N + \mathfrak{m}M$, allora $M = N$. Sempre nell'ipotesi che M sia finitamente generato ed I un ideale contenuto nel radicale di Jacobson di A, se $v_1 + IM, \ldots, v_n + IM$ generano M/IM, allora $v_1, \ldots, v_n$ generano M. Perciò se $(A, \mathfrak{m}, k)$ è un anello locale e $v_1 + \mathfrak{m}M, \ldots, v_n + \mathfrak{m}M$ generano il k-spazio vettoriale $M/\mathfrak{m}M$, allora $v_1, \ldots, v_n$ generano M. Se $A = (A, \mathfrak{m}, k)$ è locale, N è un A-modulo finitamente generato e se $\varphi : M \longrightarrow N$ un omomorfismo tale che l'applicazione k-lineare indotta $\overline{\varphi} : M/\mathfrak{m}M \longrightarrow N/\mathfrak{m}N$ è suriettiva, allora anche φ è suriettivo.

Situazione 18.1. Siano A un anello commutativo $\neq 0$ ed M un A-modulo.

Nota 18.2. Per una matrice $T \in A_n^n$ definiamo il determinante $\det T \in A$ e la matrice aggiunta $T_{\mathrm{ad}} \in A_n^n$ come d'uso nei corsi di Algebra lineare. Si ha la relazione fondamentale (regola di Cramer astratta)

$$T_{\mathrm{ad}}T = TT_{\mathrm{ad}} = (\det T)\cdot\delta$$

dove, come sempre, con δ indichiamo la matrice identica.

Nota 18.3. Se $\varphi : M \longrightarrow M$ è un endomorfismo, allora possiamo considerare l'anello $A[\varphi]$ generato in $\operatorname{End} M$ da φ e dalle moltiplicazioni $a\,\mathrm{id}_M = \bigcirc\!\!\!\!\!\!\int_x ax$ per $a \in A$. È chiaro che $A[\varphi]$ è un anello commutativo e che l'applicazione $\bigcirc\!\!\!\!\!\!\int_a a\,\mathrm{id}_M : A \longrightarrow A[\varphi]$ è un omomorfismo di anelli.

Attenzione: Questo omomorfismo in genere non è iniettivo; il suo nucleo è l'insieme $\{a \in A \mid aM = 0\}$.

Nota 18.4. Sia $\varphi : M \longrightarrow M$ un endomorfismo. Allora possiamo considerare M come $A[\varphi]$-modulo in modo ovvio: Ogni elemento di $A[\varphi]$ è della forma $\psi = a_0\varphi^m + a_1\varphi^{m-1} + \ldots + a_{m-1}\varphi + a_m\,\mathrm{id}_M$ con $a_0, \ldots, a_m \in M$, cosicché per $x \in M$ abbiamo $\psi x = a_0\varphi^m x + a_1\varphi^{m-1}x + \ldots + a_{m-1}\varphi x + a_m x$.

Nota 18.5. (1) Per ogni $n \in \mathbb{N}+1$ anche M^n è un A-modulo, quindi anche un A_n^n-modulo. Per $v_1, \ldots, v_n \in M$ e $T \in A_n^n$ si ha semplicemente

$$T\begin{pmatrix} v^1 \\ \vdots \\ v^n \end{pmatrix} = \begin{pmatrix} w^1 \\ \vdots \\ w^n \end{pmatrix}$$

con $w^i = \sum_{k=1}^{m} T_k^i v^k$ per ogni $i = 1, \ldots, n$. Per $n = 2$ si ha ad esempio

$$\begin{pmatrix} T_1^1 & T_2^1 \\ T_1^2 & T_2^2 \end{pmatrix} \begin{pmatrix} v^1 \\ v^2 \end{pmatrix} = \begin{pmatrix} T_1^1 v^1 + T_2^1 v^2 \\ T_1^2 v^1 + T_2^2 v^2 \end{pmatrix}$$

Per $S, T \in A_n^n$ si ha $(ST)v = S(Tv)$ per ogni $v \in M^n$.

(2) Se $\varphi : M \longrightarrow M$ è un endomorfismo, essendo l'anello $A[\varphi]$ commutativo, la costruzione nel punto (1) può essere applicata con $A[\varphi]$ al posto di A.

Osservazione 18.6. Siano $v \in M^n$ e $T \in A_n^n$ tali che $Tv = 0$.

Allora $(\det T)v = 0$.

Dimostrazione. Per la nota 18.2 abbiamo $(\det T)v = T_{\mathrm{ad}} T v = 0$.

Teorema 18.7. *M sia finitamente generato come A-modulo. Siano I un ideale generalizzato di A e $\varphi : M \longrightarrow M$ un endomorfismo tali che $\varphi M \subset IM$.*

Allora esistono $a_1, \ldots, a_n \in I$ tali che $\varphi^n + a_1 \varphi^{n-1} + \ldots + a_{n-1}\varphi + a_n \,\mathrm{id}_M = 0$.

Dimostrazione. Sia $\{v^1, \ldots, v^n\}$ un sistema di generatori di M.

Sia $v := \begin{pmatrix} v^1 \\ \vdots \\ v^n \end{pmatrix} \in M^n$.

Per ipotesi esiste una matrice $T \in I_n^n$ (cioè una matrice $n \times n$ con coefficienti in I) tale che $\varphi v^i = \sum_{k=1}^{n} T_k^i v^k$ per ogni i, ovvero $\begin{pmatrix} \varphi & & \\ 0 & \ddots & 0 \\ & & \varphi \end{pmatrix} v = Tv$.

Sia $S := \begin{pmatrix} \varphi & & \\ 0 & \ddots & 0 \\ & & \varphi \end{pmatrix} - T$. Allora $S \in (A[\varphi])_n^n$ e si ha $Sv = 0$.
Dall'oss. 18.6 segue $(\det S)v = 0$. Siccome $v^1, \ldots, v^n$ generano M, ciò implica $\det S = 0$. Si osservi che $\det S \in A[\varphi]$.

Ma è chiaro che $\det S$ è un polinomio monico in φ con coefficienti in I.

Nota 18.8. Il teorema 18.7 non è altro che una generalizzazione (importante) del teorema di Cayley-Hamilton dell'algebra lineare. Per convincersi di ciò è sufficiente esaminare la dimostrazione nel caso che M sia libero con base ordinata $v = (v_1, \ldots, v_n)$ ed $I = A$.

Allora nella dimostrazione del teorema 18.7 T è la matrice di φ rispetto alla base v e $\det S$ è proprio il polinomio caratteristico di φ.

Corollario 18.9. *M sia finitamente generato come A-modulo. Sia I un ideale generalizzato di A tale che $IM = M$.*

Allora esiste $t \in 1 + I$ tale che $tM = 0$.

Dimostrazione. Per ipotesi $\mathrm{id}_M M = M = IM$. Per il teorema 18.7 esistono $a_1, \ldots, a_n \in I$ tali che $\mathrm{id}_M^n + a_1 \,\mathrm{id}_M^{n-1} + \ldots + a_{n-1} \,\mathrm{id}_M + a_n \,\mathrm{id}_M = 0$.

Ma ciò significa proprio che per $t := 1 + a_1 + \ldots + a_n$ si ha $t \in 1 + I$ e $tv = 0$ per ogni $v \in M$.

Proposizione 18.10. *Siano M finitamente generato come A-modulo e $\psi : M \longrightarrow M$ un endomorfismo suriettivo. Allora ψ è anche iniettivo e quindi un isomorfismo.*

Dimostrazione. M è finitamente generato anche come $A[\psi]$-modulo. Applichiamo il cor. 18.9 con $A[\psi]$ al posto di A e con $I := A[\psi]\psi$.

La suriettività di ψ implica $IM = M$, cosicché per il cor. 18.9 esiste $p \in I$ tale che $\mathrm{id}_M + p = 0$.

p è però della forma $f(\psi)\psi$ con $f \in A[x]$. Perciò abbiamo $\mathrm{id}_M = -f(\psi)\psi$.

Ciò implica che $-f(\psi)$ è un'inversa di ψ.

Questa dimostrazione, dovuta a Vasconcelos, si trova ad es. in Matsumura [2460], pag. 9, e Eisenbud [11998], pagg. 120-121.

Teorema 18.11 (lemma di Nakayama). *Siano M finitamente generato come A-modulo e I un ideale di A contenuto nel radicale di Jacobson di A tale che $IM = M$.*

Allora $M = 0$.

Dimostrazione. Per il cor. 18.9 esiste $t \in 1 + I$ tale che $tM = 0$.

Per la prop. 3.57 però t è invertibile e ciò implica $M = t^{-1}tM = 0$.

Corollario 18.12. *Siano M finitamente generato come A-modulo ed N un sottomodulo di M. Sia I un ideale di A contenuto nel radicale di Jacobson di A tale che $M = N + IM$.*

Allora $M = N$.

Dimostrazione. Possiamo applicare il teorema 18.11 al modulo M/N, anch'esso finitamente generato come A-modulo.

Infatti l'ipotesi implica $I(M/N) = (IM + N)/N = M/N$ e dal lemma di Nakayama otteniamo $M/N = 0$, ovvero $M = N$.

Corollario 18.13. *A sia locale con ideale massimale $\mathfrak{m}$. Siano M finitamente generato come A-modulo ed N un sottomodulo di M tale che $M = N + \mathfrak{m}M$.*

Allora $M = N$.

Dimostrazione. In un anello locale il radicale di Jacobson coincide con l'ideale massimale.

Osservazione 18.14. Sia I un ideale generalizzato di A. Allora:

(1) M/IM è in modo naturale un A/I-modulo, se per $x \in M$ ed $a \in A$ poniamo $(a + I)(x + IM) := ax + IM$.

(2) M/IM è naturalmente anche un A-modulo.

(3) Siano $v_1, \ldots, v_n \in M$. Allora gli elementi $v_1 + IM, \ldots, v_n + IM$ generano M/IM come A/I-modulo se e solo se essi generano M/IM come A-modulo.

Proposizione 18.15. *M sia finitamente generato come A-modulo ed I un ideale di A contenuto nel radicale di Jacobson di A.*

Gli elementi $v_1, \ldots, v_n$ siano tali che $v_1 + IM, \ldots, v_n + IM$ generano M/IM come A-modulo (o equivalentemente come A/I-modulo).

Allora $v_1, \ldots, v_n$ generano M come A-modulo.

Dimostrazione. Siano $N := A\_(v_1, \ldots, v_n)$ e $P := M/N$.

L'ipotesi implica che per ogni $x \in M$ esiste $y \in N$ con $x - y \in IM$, sicché $N + IM = M$. Perciò $P/IP = \dfrac{M/N}{(N+IM)/N} = \dfrac{M/N}{M/N} = 0$ e quindi $P = IP$.

Dal teorema 18.11 segue $P = 0$ e ciò significa $M = N$.

Osservazione 18.16. $A = (A, \mathfrak{m}, k)$ sia locale. Allora $M/\mathfrak{m}M$ è uno spazio vettoriale su k.

Corollario 18.17. *$A = (A, \mathfrak{m}, k)$ sia locale. Siano M finitamente generato come A-modulo e $v_1, \ldots, v_n$ elementi di M tali che $v_1 + \mathfrak{m}M, \ldots, v_n + \mathfrak{m}M$ generano il k-spazio vettoriale $M/\mathfrak{m}M$.*

Allora $v_1, \ldots, v_n$ generano M come A-modulo.

Corollario 18.18. *$A = (A, \mathfrak{m}, k)$ sia locale. Siano N un A-modulo finitamente generato e $\varphi : M \longrightarrow N$ un omomorfismo.*

Siccome $\varphi(\mathfrak{m}M) \subset \mathfrak{m}N$, possiamo definire un'applicazione k-lineare $\overline{\varphi} := \bigcirc_{x+\mathfrak{m}M} \varphi x + \mathfrak{m}N : M/\mathfrak{m}M \longrightarrow N/\mathfrak{m}N$.

Se $\overline{\varphi}$ è suriettivo, anche φ è suriettivo.

Dimostrazione. Per l'oss. 10.2 anche $N/\mathfrak{m}M$ è finitamente generato su A e quindi per l'oss. 18.14 $N/\mathfrak{m}M$ è uno spazio vettoriale su k.

Per la suriettività di $\overline{\varphi}$ esistono $v_1, \ldots, v_n \in M$ tali che $\varphi v_1 + \mathfrak{m}N, \ldots, v_n + \mathfrak{m}N$ generano $N/\mathfrak{m}N$ su k.

Per il cor. 18.17 $\varphi v_1, \ldots, \varphi v_n$ generano N su A. È chiaro che ciò implica la suriettività di φ.

Nota 18.19. Nel cor. 18.17 e quindi anche nella prop. 18.15 l'ipotesi che M sia finitamente generato è necessaria. Un esempio si trova in Reid [16215], pag. 44.

I cor. 18.17 e 18.18 (e con essi il lemma di Nakayama da cui derivano) sono molto importanti, perché permettono di ricondurre lo studio dei moduli finitamente generati su un anello locale $A = (A, \mathfrak{m}, k)$ alla teoria degli spazi vettoriali (di dimensione finita) su k.

19. Anelli di frazioni: Il caso generale

S sia un sottomonoide puro di A. Ideali S-saturi. L'ideale di indeterminazione Ω è S-saturo. $S^{-1}A := (A \times S)/\sim$ con $(a,s) \sim (b,t) :\iff ta - sb \in \Omega$. Notazioni a_S e $\frac{a_S}{s}$. Addizione e moltiplicazione in $S^{-1}A$. L'omomorfismo $i_S := \bigcap_a a_S : A \longrightarrow S^{-1}A$; il suo nucleo è Ω. Caso, in cui S non contiene zerodivisori, ad esempio, quando A è integro. In quest'ultima ipotesi possiamo considerare $S^{-1}A$ come sottoanello del campo $\mathcal{K}(A)$. Ogni elemento di S diventa invertibile in $S^{-1}A$. Proprietà universale di $S^{-1}A$ rispetto ad omomorfismi di anelli φ per i quali ogni elemento di $\varphi(S)$ è invertibile. Estensione $S^{-1}I$ di un ideale I di A e contrazione $S^*J = i_S^{-1}(J)$ di un ideale J di $S^{-1}A$. La contrazione di un ideale primo è un ideale primo. $S^*S^{-1}I = \{a \in A \mid \text{ esiste } s \in S \text{ con } sa \in I\}$. L'estensione di un ideale primo P con $P \cap S = \emptyset$ è un ideale primo. $S^*S^{-1}I = I$ se e solo se I è S-saturo. Biiezione tra gli ideali generalizzati S-saturi di A e gli ideali generalizzati di $S^{-1}A$. Se A è noetheriano, anche $S^{-1}A$ è noetheriano. Estensione di ideali primari. Un ideale generalizzato H è S-saturo se e solo se $(a,s) \sim (h,t)$ con $h \in H$ implica $a \in H$. Biiezione tra gli ideali primi P di A con $P \cap S = \emptyset$ e gli ideali primi di $S^{-1}A$. Omomorfismo canonico $S^{-1}A \longrightarrow T^{-1}A$ per $S \subset T$. $\sqrt{S^{-1}I} = S^{-1}\sqrt{I}$.

Situazione 19.1. Siano A un anello commutativo ed S un sottomonoide puro di A. L'ipotesi implica $A \neq 0$.

Ripetiamo in questo capitolo molti dei concetti già visti nel capitolo 6, dove abbiamo trattato il caso speciale in cui $S = \{f^n \mid n \in \mathbb{N}\}$ con $f \in A$ non nilpotente.

Definizione 19.2. Un ideale generalizzato H di S si dice *S-saturo*, se vale l'implicazione

$$a \in A, s \in S, sa \in H \Longrightarrow a \in H$$

Definizione 19.3. $\Omega := \Omega_S := \{a \in A \mid \text{ esiste } s \in S \text{ con } sa = 0\}$ si chiama l'*ideale di indeterminazione* di S.

Osservazione 19.4. Ω è un ideale S-saturo di A.

Dimostrazione. Uguale a quella dell'oss. 6.5, in cui di S si usa solo che è un sottomonoide puro di A.

Definizione 19.5. Sull'insieme $A \times S$ introduciamo la relazione

$$(a,s) \sim (b,t) :\iff ta - sb \in \Omega$$

Lemma 19.6. *La relazione $\sim$ introdotta nella def. 19. 5 è una relazione di equivalenza su $A \times S$.*

Dimostrazione. Uguale a quella del lemma 6.7.

Definizione 19.7. $S^{-1}A := (A \times S)/\sim$ si chiama la *localizzazione* di A rispetto al sottomonoide puro S.

Definizione 19.8. Per $a \in A$ ed $s \in S$ denotiamo con a_S la classe di equivalenza di $(a,1)$ in $S^{-1}A$, con $\dfrac{a_S}{s}$ la classe di equivalenza di (a,s).

Vedremo che questa notazione è legittima, perché gli elementi di S sono, come dimostreremo, invertibili in $S^{-1}A$.

Osservazione 19.9. La def. 19.5 può essere riformulata così: Per $a, b \in A$ ed $s, t \in S$ si ha

$$\frac{a_S}{s} = \frac{b_S}{t} \iff \text{esiste } u \in S \text{ tale che } u(ta - sb) = 0$$

Se S non contiene zerodivisori, si ha

$$\frac{a_S}{s} = \frac{b_S}{t} \iff ta = sb$$

Osservazione 19.10. Siano $a, b \in A$. Allora

$$a_S = b_S \iff a - b \in \Omega$$

Se S non contiene zerodivisori, allora $a_S = b_S \iff a = b$.

Osservazione 19.11. Sia $a \in A$. Allora $a_S = 0 \iff a \in \Omega$.

Osservazione 19.12. $1_S \neq 0$.

Dimostrazione. Infatti $1 \notin \Omega$.

Osservazione 19.13. Siano $a, b, a', b' \in A$ ed $s, t, s', t' \in S$ tali che

$$\frac{a_S}{s} = \frac{a'_S}{s'} \text{ e } \frac{b_S}{t} = \frac{b'_S}{t'}$$

Allora

$$\frac{(ta + sb)_S}{st} = \frac{(t'a' + s'b')_S}{s't'}$$

$$\frac{(ab)_S}{st} = \frac{(a'b')_S}{s't'}$$

Dimostrazione. (1) Per ipotesi $s'a - sa', t'b - tb' \in \Omega$.

(2) Moltiplicando il primo termine con tt' e il secondo con ss' otteniamo $tt's'a - tt'sa', ss't'b - ss'tb' \in \Omega$, per cui $t's'(ta + sb) - ts(t'a' + s'b') \in \Omega$ e quindi

$$\frac{(ta + sb)_S}{st} = \frac{(t'a' + s'b')_S}{s't'}$$

(3) Moltiplicando in (1) il primo termine per $t'b$ e il secondo con sa' otteniamo $t's'ab - t'sa'b, st'a'b - sta'b' \in \Omega$, per cui $t's'ab - sta'b' \in \Omega$, e quindi

$$\frac{(ab)_S}{st} = \frac{(a'b')_S}{s't'}$$

Osservazione 19.14. Siano $a \in A$ ed $s, t \in S$. Allora $\frac{a_S}{s} = \frac{(ta)_S}{ts}$.

Proposizione 19.15. *Su $S^{-1}A$ introduciamo le operazioni*

$$\frac{a_S}{s} + \frac{b_S}{t} := \frac{(ta + sb)_S}{st}$$

$$\frac{a_S}{s}\frac{b_S}{t} := \frac{(ab)_S}{st}$$

Allora $S^{-1}A$ diventa un anello commutativo in cui 0_S è l'elemento neutro dell'addizione e 1_S è l'elemento neutro della moltiplicazione.

Dimostrazione. (1) Le operazioni sono ben definite per l'oss. 19.13.

(2) Si verifica facilmente che $(S^{-1}A, +)$ è un gruppo abeliano con elemento neutro 0_S e che $(S^{-1}A, \cdot)$ è un monoide commutativo con elemento neutro 1_S.

(3) Dimostriamo la legge di distributività: Usando l'oss. 19.14
per $a, b, c \in A$ ed $s, t, r \in S$ abbiamo

$$\left(\frac{a_S}{s} + \frac{b_S}{t}\right)\frac{c_S}{r} = \frac{(tac + sbc)_S}{str} = \frac{(rtac + rsbc)_S}{str^2}$$
$$= \frac{(ac)_S}{sr} + \frac{(bc)_S}{tr} = \frac{a_S}{s}\frac{c_S}{r} + \frac{b_S}{t}\frac{c_S}{r}$$

Osservazione 19.16. Siano $a, b \in A$. Allora

$(a + b)_S = a_S + b_S$

$(ab)_S = a_S b_S$

Dimostrazione. (1) Infatti

$$a_S + b_S = \frac{a_S}{1} + \frac{b_S}{1} = \frac{(a+b)_S}{1} = (a + b)_S$$

(2) Similmente

$$a_S b_S = \frac{a_S}{1}\frac{b_S}{1} = \frac{(ab)_S}{1} = (ab)_S$$

Proposizione 19.17. *L'applicazione $i_S := \bigcirc_a a_S : A \longrightarrow S^{-1}A$ è un omomorfismo di anelli con nucleo Ω.*

Dimostrazione. Ciò segue dalle oss. 19.16 e 19.11 e dalla prop. 19.15.

Corollario 19.18. *Se S non contiene zerodivisori, possiamo considerare A come sottoanello di $S^{-1}A$ tramite l'omomorfismo $i_S : A \longrightarrow S^{-1}A$.*

Osservazione 19.19. Gli elementi di S siano invertibili in A.
Allora per ogni $a \in A$ ed ogni $s \in S$ si ha $\frac{a_S}{s} = (s^{-1}a)_S$.

Dimostrazione. $a = ss^{-1}a$ implica $\frac{a_S}{s} = (s^{-1}a)_S$.

Osservazione 19.20. L'applicazione $i_S : A \longrightarrow S^{-1}A$ è un isomorfismo se e solo se ogni elemento di S è invertibile in A.

Dimostrazione. (1) Sia i_S un isomorfismo. Allora $\Omega = \operatorname{Ker} i_S = 0$. Per la suriettività di i_S, dato $s \in S$, deve esistere $e \in A$ tale che $\frac{1_S}{s} = e_S$.

Ciò significa che $1 - es \in \Omega = 0$, per cui s è invertibile.

(2) Ogni elemento di S sia invertibile. Ciò implica che S non contiene zerodivisori. Dall'oss. 19.11 segue che $\operatorname{Ker} i_S = \Omega = 0$, pertanto i_S è iniettivo.

Sia ora $\frac{a_S}{s} \in S^{-1}A$. Dall'oss. 19.19 segue che $\frac{a_S}{s} = (s^{-1}a)_S = i_S(s^{-1}a)$, e vediamo che i_S è suriettivo.

Nota 19.21. A sia un anello integro. Allora l'applicazione

$$\begin{array}{rcl} \varphi : S^{-1}A & \longrightarrow & \mathcal{K}(A) \\ \frac{a_S}{s} & \longmapsto & \frac{a}{s} \end{array}$$

è ben definita e costituisce un omomorfismo di anelli che rende commutativo il diagramma

$$\begin{array}{ccc} A & \xrightarrow{i_S} & S^{-1}A \\ & \searrow^{j} & \downarrow{\scriptstyle \varphi} \\ & & \mathcal{K}(A) \end{array}$$

in cui j è l'inclusione $\bigcirc_a \frac{a}{1}$ di A nel suo campo dei quozienti.

Quando A è integro, possiamo quindi identificare $S^{-1}A$ con il sottoanello $\left\{\frac{a}{s} \mid a \in A, s \in S\right\}$ di $\mathcal{K}(A)$. In tal caso perciò anche l'anello $S^{-1}A$ è integro.

Dimostrazione. (1) Dimostriamo che φ è ben definito.

Osserviamo che $\Omega = 0$. Sia $\frac{a_S}{s} = \frac{b_S}{t}$. Allora $ta - sb = 0$ e ciò implica che $\frac{a}{s} = \frac{b}{t}$ in $\mathcal{K}(A)$.

(2) Dimostriamo che φ è iniettivo.

Sia $\frac{a}{s} = 0$ in $\mathcal{K}(A)$. Ciò implica però $a = 0$ e quindi $\frac{a_S}{s} = 0$.

(3) Per $a \in A$ abbiamo $\varphi(i_S(a)) = \varphi(a_S) = \frac{a}{1} = j(a)$.

(4) Si verifica facilmente che φ è un omomorfismo di anelli.

Osservazione 19.22. Per ogni $s \in S$ si ha $s_S \frac{1_S}{s} = 1_S$.

Dimostrazione. Infatti $s_S \frac{1_S}{s} = \frac{s_S}{s}$ ed è chiaro che l'ultima frazione coincide con 1_S (cfr. oss. 19.14).

Teorema 19.23. *Per ogni $s \in S$ l'elemento s_S è invertibile nell'anello $S^{-1}A$ e si ha $(s_S)^{-1} = \frac{1_S}{s}$.*

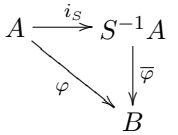
Dimostrazione. Ciò è una conseguenza immediata dell'oss. 19.22.

Osservazione 19.24. L'oss. 19.22 e il teorema 19.23 giustificano la nostra notazione introdotta nella def. 19.8. Infatti, per $a \in A$ ed $s \in S$ in $S^{-1}A$ si ha

$$\frac{a_S}{s} = \frac{1_S a_S}{s} = (s_S)^{-1} a_S$$

Teorema 19.25. *Siano B un anello commutativo e $\varphi : A \longrightarrow B$ un omomorfismo di anelli tale che ogni elemento di $\varphi(S)$ sia invertibile in B.*

Allora esiste un unico omomorfismo di anelli $\overline{\varphi} : S^{-1}A \longrightarrow B$ *che rende commutativo il diagramma*



Per $a \in A$ *ed* $s \in S$ *si ha* $\overline{\varphi}\Big(\dfrac{a_S}{s}\Big) = (\varphi s)^{-1}\varphi a$.

Dimostrazione. (1) Se $\overline{\varphi}$ esiste, per $a \in A$ ed $s \in S$ dall'uguaglianza $\dfrac{a_S}{s}s_S = a_S$ valida in $S^{-1}A$ dobbiamo avere $\overline{\varphi}\Big(\dfrac{a_S}{s}\Big)\overline{\varphi}s_S = \overline{\varphi}a_S$ ovvero $\overline{\varphi}\Big(\dfrac{a_S}{s}\Big)\varphi s = \varphi a$. D'altra parte ogni elemento di $\varphi(S)$ è invertibile in B, quindi $\overline{\varphi}\Big(\dfrac{a_S}{s}\Big) = (\varphi s)^{-1}\varphi a$.

(2) Dobbiamo ancora dimostrare che in questo modo l'applicazione $\overline{\varphi}$ è ben definita.

Sia $\dfrac{a_S}{s} = \dfrac{b_S}{t}$ con $a, b \in A$ ed $s, t \in S$. Allora esiste $u \in S$ con $u(ta - sb) = 0$. Ciò implica $\varphi u(\varphi t\varphi a - \varphi s\varphi b) = 0$ e, siccome φu è invertibile, si ha $\varphi t\varphi a = \varphi s\varphi b$. Ma anche φs e φt sono invertibili, per cui $(\varphi s)^{-1}\varphi a = (\varphi t)^{-1}\varphi b$.

(3) È chiaro adesso che $\overline{\varphi}$ è un omomorfismo di anelli.

(4) Per $a \in A$ abbiamo infine $\overline{\varphi}a_S = \overline{\varphi}\Big(\dfrac{a_S}{1}\Big) = (\varphi 1)^{-1}\varphi a = \varphi a$, cosicché $\overline{\varphi}$ rende commutativo il diagramma.

Definizione 19.26. Per un sottoinsieme $E \subset A$ sia

$$S^{-1}E := \Big\{\frac{e_S}{s} \mid e \in E, s \in S\Big\}$$

Osservazione 19.27. Nella situazione del teorema 19.25 si ha

$$\operatorname{Ker}\overline{\varphi} = S^{-1}\operatorname{Ker}\varphi$$

Dimostrazione. Infatti $\overline{\varphi}\Big(\dfrac{a_S}{s}\Big) = 0 \iff (\varphi s)^{-1}\varphi a = 0 \iff \varphi a = 0$.

Lemma 19.28. *Sia* I *un ideale generalizzato di* A. *Allora:*

(1) $S^{-1}I$ *è un ideale generalizzato di* $S^{-1}A$.

(2) $S^{-1}I$ *è un ideale di* $S^{-1}A$ *se e solo se* $I \cap S = \emptyset$.

Dimostrazione. (1) Siano $a, b \in I$ ed $s, t \in S$.

Allora $\dfrac{a_S}{s} + \dfrac{b_S}{t} = \dfrac{(ta + sb)_S}{st} \in S^{-1}I$.

Inoltre per $c \in A$ ed $r \in S$ si ha $\dfrac{c_S}{r}\dfrac{a_S}{s} = \dfrac{(ca)_S}{rs} \in S^{-1}I$

(2a) Sia $I \cap S \neq \emptyset$, ad esempio $s \in I \cap S$. Allora $1_S = \dfrac{s_S}{s} \in S^{-1}I$.

(2b) Sia $S^{-1}I = S^{-1}A$. Allora esistono $a \in I$ ed $s \in S$ tali che $\dfrac{a_S}{s} = 1_S$. Ciò significa che esiste $u \in S$ con $u(a - s) = 0$ quindi $us = ua \in S \cap I$.

Definizione 19.29. Per un ideale generalizzato J di $S^{-1}A$ usiamo la notazione

$$S^*J := i_S^{-1}(J) = \{a \in A \mid a_S \in J\}$$

S^*J si chiama la *contrazione* di J ad A.

Osservazione 19.30. (1) Sia J un ideale di $S^{-1}A$.

Allora S^*J è un ideale di A.

(2) Sia $Q \in \operatorname{Spec} S^{-1}A$. Allora $S^*Q \in \operatorname{Spec} A$.

Dimostrazione. Siccome i_S è un omomorfismo di anelli, l'enunciato segue dal lemma 3.18.

Lemma 19.31. *Sia J un ideale generalizzato di $S^{-1}A$.*

Allora $S^{-1}S^*J = J$.

Dimostrazione. (1) Sia $q \in S^{-1}S^*J$. Allora esistono $e \in S^*J$ ed $s \in S$ tali che $q = \dfrac{e_S}{s} = (s_S)^{-1}e_S$. Per ipotesi J è un ideale generalizzato di $S^{-1}A$ ed $e_S \in J$, perciò $q \in J$.

(2) Sia $q \in J$, ad esempio $q = \dfrac{a_S}{s}$ con $a \in A$ ed $s \in S$. Allora $a_S = qs_S \in J$ e quindi $a \in S^*J$. Da ciò segue direttamente che $q \in S^{-1}S^*J$.

Lemma 19.32. *Sia I un ideale generalizzato di A. Allora*

$$S^*S^{-1}I = \{a \in A \mid \textit{ esiste } s \in S \textit{ con } sa \in I\}$$

Dimostrazione. (1) Sia $a \in S^*S^{-1}I$. Ciò significa $a_S \in S^{-1}I$, perciò esistono $b \in I$ ed $s \in S$ con $a_S = \dfrac{b_S}{s}$, ovvero $sa_S = b_S$. Pertanto esiste $t \in S$ con $tsa = tb \in I$.

(2) Siano $a \in A$ ed $s \in S$ con $sa \in I$. Allora $a_S = \dfrac{(sa)_S}{s} \in S^{-1}I$ e quindi $a \in S^*S^{-1}I$.

Proposizione 19.33. *Sia $P \in \operatorname{Spec} A$ tale che $P \cap S = \emptyset$.*

Allora $S^{-1}P \in \operatorname{Spec} S^{-1}A$.

Dimostrazione. (1) Per il lemma 19.28 $S^{-1}P$ è un ideale di $S^{-1}A$.

(2) Siano $u, v \in S^{-1}A$ tali che $uv \in S^{-1}P$. Allora esistono $a, b \in A$, $p \in P$ ed $s, t, x \in S$ tali che $u = \dfrac{a_S}{s}$, $v = \dfrac{b_S}{t}$ e $uv = \dfrac{(ab)_S}{st} = \dfrac{p_S}{x}$, cosicché esiste $y \in S$ con $y(xab - pst) = 0$. Ciò significa che $abxy = psty \in P$, cosicché necessariamente $ab \in P$, cioè $a \in P$ oppure $b \in P$.

Se ad esempio $a \in P$, allora $u = \dfrac{a_S}{s} \in S^{-1}P$.

Corollario 19.34. *Per un ideale generalizzato I di A sono equivalenti:*

(1) $S^*S^{-1}I = I$.

(2) I è S-saturo.

Dimostrazione. (1) $\implies$ (2): Per il lemma 19.32 I coincide con l'insieme $\{a \in A \mid \text{ esiste } s \in S \text{ con } sa \in I\}$, quindi la tesi segue direttamente dalla def. 19.2.

(2) $\implies$ (1): Sia $a \in S^*S^{-1}I$. Allora, ancora per il lemma 19.32, esiste $s \in S$ tale che $sa \in I$, quindi, poiché I è S-saturo, $a \in I$.

Teorema 19.35. *Esiste una biiezione canonica*

$$\{\textit{ideali generalizzati } S\textit{-saturi di } A\} \longleftrightarrow \{\textit{ideali generalizzati di } S^{-1}A\}$$
$$I \longmapsto S^{-1}I$$
$$S^*J \longmapsfrom J$$

Dimostrazione. (1) Per ogni ideale generalizzato J di $S^{-1}A$, S^*J è S-saturo, come si vede dal cor. 19.34: $S^*S^{-1}S^*J \overset{19.31}{=} S^*J$.

(2) Le due applicazioni indicate sono perciò ben definite e una l'inversa dell'altra, come segue dal lemma 19.31 e dal cor. 19.34.

Osservazione 19.36. Siano I un ideale generalizzato di A ed $e_1, \ldots, e_m \in A$ tali che $I = A_\smile(e_1, \ldots, e_m)$.

Allora $S^{-1}I = (S^{-1}A)_\smile((e_1)_S, \ldots, (e_m)_S)$.

Dimostrazione. (1) Sia $x \in S^{-1}I$. Allora $x = \dfrac{b_S}{s}$ per qualche $b \in I$ ed $a \in S$. Esistono dunque $a_1, \ldots, a_m \in A$ tali che $b = a_1e_1 + \ldots + a_me_m$. Da ciò segue che

$$\begin{aligned} x &= \frac{(a_1e_1 + \ldots + a_me_m)_S}{s} \\ &= \frac{(a_1e_1)_S}{s} + \ldots + \frac{(a_me_m)_S}{s} \\ &= \frac{(a_1)_S}{s}(e_1)_S + \ldots + \frac{(a_m)_S}{s}(e_m)_S \in (S^{-1}A)_\smile((e_1)_S, \ldots, (e_m)_S) \end{aligned}$$

(2) Sia $x \in (S^{-1}A)_\smile((e_1)_S, \ldots, (e_m)_S)$. Allora esistono $a_1, \ldots, a_m \in A$ e $s_1, \ldots, s_m \in S$ tali che

$$\begin{aligned} x &= \frac{(a_1)_S}{s_1}(e_1)_S + \ldots + \frac{(a_m)_S}{s_m}(e_m)_S \\ &= \frac{(s_2 \cdots s_m a_1 e_1 + \ldots + s_1 \cdots s_{m-1} a_m e_m)_S}{s_1 \cdots s_m} \in S^{-1}I \end{aligned}$$

Corollario 19.37. *Se A è noetheriano, anche $S^{-1}A$ è noetheriano.*

Osservazione 19.38. Per un ideale generalizzato I di A sono equivalenti:

(1) $S^*S^{-1}I = A$.

(2) $S^{-1}I = S^{-1}A$.

(3) $I \cap S \neq \emptyset$.

Dimostrazione. (1) $\implies$ (2): Dal lemma 19.31 abbiamo $S^{-1}A = S^{-1}S^*S^{-1}I = S^{-1}I$.

(2) $\implies$ (1): Nell'ipotesi (2) si ha $S^*S^{-1}I = S^*S^{-1}A = i_S^{-1}(S^{-1}A) = A$.

(2) $\iff$ (3): Segue direttamente dal lemma 19.28.

Osservazione 19.39. Sia I un ideale di A tale che $S \cap I = \emptyset$.

Allora $S \cap \sqrt{I} = \emptyset$.

Dimostrazione. Sia $s \in S \cap \sqrt{I}$. Allora esiste $n \in \mathbb{N}$ con $s^n \in I$. Però $s^n \in S$ e quindi $s^n \in S \cap I$, una contraddizione.

Lemma 19.40. *Sia Q un ideale primario di A tale che $S \cap Q = \emptyset$.*

Allora Q è S-saturo.

Dimostrazione. Siano $a \in A$ ed $s \in S$ tali che $sa \in Q$. Per l'oss. 19.39 $s \notin \sqrt{Q}$, perciò $a \in Q$.

Corollario 19.41. *Sia $P \in \operatorname{Spec} A \cap S^\sharp$, cioè $P \in \operatorname{Spec} A$ e $P \cap S = \emptyset$.*

Allora P è S-saturo.

Osservazione 19.42. I sia un ideale S-saturo di A.

Allora $I \cap S = \emptyset$, cioè $I \in S^\sharp$.

Dimostrazione. Sia $s \in I \cap S$. Allora $s = s1 \in I$ e quindi $1 \in I$, una contraddizione.

Corollario 19.43. *Per un ideale primario Q di A sono equivalenti:*

(1) $S \cap Q = \emptyset$.

(2) Q è S-saturo.

(3) $S^*S^{-1}Q = Q$.

Dimostrazione. (1) $\implies$ (2): Lemma 19.40.

(2) $\implies$ (3): Cor. 19.34.

(3) $\implies$ (1): Oss. 19.38.

Lemma 19.44. *Per un ideale generalizzato H di A sono equivalenti:*

(1) H è S-saturo.

(2) Se $a \in A, h \in H$ ed $s, t \in S$ sono tali che $(a, s) \sim (h, t)$, allora $a \in H$.

(3) Se $a \in A$ ed $s \in S$ sono tali che $\dfrac{a_S}{s} \in S^{-1}H$, allora $a \in H$.

Dimostrazione. (1) $\implies$ (2): Siano a, h, s, t come nell'ipotesi del punto (2). Allora esiste $u \in S$ tale che $uta = ush \in H$. Siccome H è S-saturo, ciò implica $a \in H$.

(2) $\iff$ (3): Si ha $(a, s) \sim (h, t)$ con $h \in H$ ed $s, t \in S$ se e solo se $\dfrac{a_S}{s} \in S^{-1}H$.

(2) $\Longrightarrow$ (1): Siano $a \in A$ ed $s \in S$ tali che $sa =: h \in H$. Allora $(a,1) \sim (h,s)$ e l'ipotesi implica $a \in H$.

Corollario 19.45. *Sia Q un ideale primario (ad esempio un ideale primo) di A con $Q \cap S = \emptyset$. Siano $a \in A$ ed $s \in S$ tali che $\frac{a_S}{s} \in S^{-1}Q$.*

Allora $a \in Q$.

Dimostrazione. Per il lemma 19.40 Q è S-saturo. L'enunciato segue dal lemma 19.44.

Teorema 19.46. *La biiezione del teorema 19.35 induce una biiezione* $(\operatorname{Spec} A) \cap S^\sharp \longleftrightarrow \operatorname{Spec} S^{-1}A$.

Proposizione 19.47. *Sia T un sottomonoide puro di A con $S \subset T$. Allora esiste un unico omomorfismo $i_{S,T} : S^{-1}A \longrightarrow T^{-1}A$ che rende commutativo il diagramma*

$$\begin{array}{ccc} A & \xrightarrow{i_S} & S^{-1}A \\ & \searrow^{i_T} & \downarrow{\scriptstyle i_{S,T}} \\ & & T^{-1}A \end{array}$$

$i_{S,T}$ è dato da $i_{S,T}\left(\frac{a_S}{s}\right) := \frac{a_T}{s}$.

Dimostrazione. Applichiamo il teorema 19.25 al caso $B = T^{-1}A$ e $\varphi = i_T$. Allora

$$i_{S,T}\left(\frac{a_S}{s}\right) = \overline{i_T}\left(\frac{a_S}{s}\right) = (i_T(s))^{-1} i_T(a) = \frac{1_S}{s} a_T = \frac{a_T}{s}$$

Proposizione 19.48. *Sia I un ideale generalizzato di A.*

Allora $\sqrt{S^{-1}I} = S^{-1}\sqrt{I}$.

Dimostrazione. (1) Siano $a \in A, s \in S$ ed $n \in \mathbb{N}$ tali che $\left(\frac{a_S}{s}\right)^n \in S^{-1}I$. Allora esistono $b \in I$ e $t \in T$ tali che $\left(\frac{a_S}{s}\right)^n = \frac{b_S}{t}$ e quindi esiste $u \in S$ con $uta^n = usb \in I$.

Ciò implica $(uta)^n \in I$, per cui $uta \in \sqrt{I}$. Dal lemma 19.32 segue $a \in S^* S^{-1}\sqrt{I}$. Ma allora $\frac{a_S}{s} \in S^{-1}S^*S^{-1}\sqrt{I} \overset{19.31}{=} S^{-1}\sqrt{I}$.

(2) Sia $q \in S^{-1}\sqrt{I}$. Allora esistono $a \in \sqrt{I}$ ed $s \in S$ tali che $q = \frac{a_S}{s}$. Sia ad esempio $a^n \in I$. Allora $q^n = \frac{(a^n)_S}{s^n} \in S^{-1}I$, quindi $q \in \sqrt{S^{-1}I}$.

20. Moduli di frazioni

Siano S un sottomonoide puro di A ed M un A-modulo. Sottomoduli S-saturi. $\Omega_{S,M} := \{x \in M \mid \text{ esiste } s \in S \text{ con } sx = 0\}$ è un sottomodulo S-saturo. $S^{-1}M := (M \times S)/\sim$, dove $(x,s) \sim (y,t) \iff tx - sy \in \Omega_{S,M}$. Notazioni x_S e x_S/s per le classi di equivalenza. $S^{-1}M$ è un $S^{-1}A$-modulo (e quindi anche un A-modulo). Per un ideale generalizzato S-saturo I di A le due definizioni (19.26 e 20.7) coincidono; ma anche quando I non è S-saturo, esse sono equivalenti in un modo naturale. L'omomorfismo canonico $\underset{x}{\bigcirc} x_S : M \longrightarrow S^{-1}M$. Estensione di un omomorfismo $\varphi : M \longrightarrow N$ a un omomorfismo $S^{-1}\varphi : S^{-1}M \longrightarrow S^{-1}N$. Una successione $M_1 \xrightarrow{\varphi} M \xrightarrow{\psi} M_2$ di omomorfismi di moduli su un anello si dice *esatta*, se $\operatorname{Ker}\psi = \operatorname{Im}\varphi$. In tal caso anche la successione $S^{-1}M_1 \xrightarrow{S^{-1}\varphi} S^{-1}M \xrightarrow{S^{-1}\psi} S^{-1}M_2$ è esatta. Se in particolare $\varphi : M \longrightarrow N$ è iniettivo, anche $S^{-1}\varphi$ è iniettivo, e se φ è suriettivo, anche $S^{-1}\varphi$ è suriettivo. N, N_1 e N_2 siano sottomoduli di M. Allora $S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N)$, inoltre $S^{-1}(N_1 + N_2) = S^{-1}N_1 + S^{-1}N_2$ e $S^{-1}(N_1 \cap N_2) = S^{-1}N_1 \cap S^{-1}N_2$.

Situazione 20.1. Siano A un anello commutativo ed S un sottomonoide puro di A. L'ipotesi implica $A \neq 0$. $M, N, \ldots$ siano A-moduli.

Definizione 20.2. Un sottomodulo H di M si chiama un sottomodulo S-*saturo* di M, se vale l'implicazione

$$x \in M, s \in S, sx \in H \Longrightarrow x \in H$$

Definizione 20.3. $\Omega_{S,M} := \{x \in M \mid \text{ esiste } s \in S \text{ con } sx = 0\}$.

Osservazione 20.4. $\Omega_{S,M}$ è un sottomodulo S-saturo di M.

Dimostrazione. (1) Siano $x, y \in \Omega_{S,M}$. Allora esistono $s, t \in S$ tali che $sx = 0$ e $ty = 0$. Siccome S è un sottomonoide di A, si ha allora $st \in S$. Inoltre $stx = 0$ e $sty = 0$ e quindi $st(x + y) = 0$, perciò $x + y \in \Omega_{S,M}$.

(2) Siano $x \in \Omega_{S,M}$ ed $a \in A$. Allora $sx = 0$ per qualche $s \in S$, per cui $sax = asx = 0$ e vediamo che $\Omega_{S,M}$ è un sottomodulo di M.

(3) Siano $x \in M$ ed $s \in S$ tali che $sx \in \Omega_{S,M}$. Allora esiste $t \in S$ tale che $tsx = 0$ e poiché $ts \in S$ ciò implica $x \in \Omega_{S,M}$.

Definizione 20.5. Sull'insieme $M \times S$ introduciamo la relazione

$$(x,s) \sim (y,t) :\Longleftrightarrow tx - sy \in \Omega_{S,M}$$

Lemma 20.6. *La relazione $\sim$ introdotta nella def. 20.5 è una relazione di equivalenza su $M \times S$.*

Dimostrazione. (1) Riflessività e simmetria di $\sim$ sono evidenti.

(2) Dimostriamo la transitività: Si abbia $(x,s) \sim (y,t) \sim (z,u)$. Allora $tx - sy \in \Omega_{S,M}$ e $uy - tz \in \Omega_{S,M}$, per cui $tux - suy \in \Omega_{S,M}$ e $usy - tsz \in \Omega_{S,M}$. Quindi $t(ux - sz) = tux - tsz \in \Omega_{S,M}$ e dall'oss. 20.4 segue $ux - sz \in \Omega_{S,M}$ e quindi $(x,s) \sim (z,u)$.

Definizione 20.7. $S^{-1}M := (M \times S)/\sim$ si chiama la *localizzazione* di M rispetto al sottomonoide S (oppure il *modulo di frazioni* di M rispetto ad S).

Definizione 20.8. Per $x \in M$ ed $s \in S$ denotiamo con x_S la classe di equivalenza di $(x,1)$ in $S^{-1}M$, con $\dfrac{x_S}{s}$ la classe di equivalenza di (x,s).

Osservazione 20.9. Siano $x, y \in M$. Allora $x_S = y_S \iff x - y \in \Omega_{S,M}$.

In particolare $x_S = 0 \iff x \in \Omega_{S,M}$.

Osservazione 20.10. (1) Siano $x, y, x', y' \in M$ ed $s, t, s', t' \in S$ tali che

$$\frac{x_S}{s} = \frac{x'_S}{s'} \text{ e } \frac{y_S}{t} = \frac{y'_S}{t'}.$$

Allora $\dfrac{(tx+sy)_S}{st} = \dfrac{(t'x'+s'y')_S}{s't'}$.

(2) Siano $x, x' \in M$, $a, a' \in A$ ed $s, t, s', t' \in S$ tali che

$$\frac{x_S}{s} = \frac{x'_S}{s'} \text{ e } \frac{a_S}{t} = \frac{a'_S}{t'}$$

Allora $\dfrac{(ax)_S}{st} = \dfrac{a'x'}{s't'}$.

Dimostrazione. Uguale a quella dell'oss. 6.14 risp. dell'oss. 19.13.

Proposizione 20.11. *Su $S^{-1}M$ definiamo le operazioni*

$$\frac{x_S}{s} + \frac{y_S}{t} := \frac{(tx+sy)_S}{st}$$

$$\frac{a_S}{s}\frac{x_S}{t} := \frac{(ax)_S}{st}$$

Allora $S^{-1}M$ diventa un $S^{-1}A$-modulo (e quindi anche un A-modulo), in cui 0_S è l'elemento neutro dell'addizione.

Dimostrazione. (1) Le operazioni sono ben definite per l'oss. 20.10.

(2) Si verifica facilmente che $(S^{-1}M, +)$ è un gruppo abeliano con elemento neutro 0_S ed è chiaro che $1_S\dfrac{x_S}{s} = \dfrac{x_S}{s}$ per ogni $x \in M, s \in S$.

(3) La distributività si dimostra come nella prop. 19.15.

Nota 20.12. Sia I un ideale generalizzato di A (cioè un sottomodulo di A). Allora possiamo definire $S^{-1}I$ come nella def. 20.7 oppure come nella def. 19.26.

(1) Se I è S-saturo, *i due insiemi coincidono* per il lemma 19.44.

(2) È immediato però che anche nel caso generale le due definizioni sono equivalenti: Denotiamo infatti con $\sim_{20.7}$ l'equivalenza della def. 20.7 e con $[\,]_{20.7}$ le classi di equivalenza corrispondenti e con $(S^{-1}I)_{20.7}$ il modulo di frazioni. L'indice 19.26 sia usato in modo analogo.

Allora per $a \in I$ ed $s \in S$ la classe $[(a,s)]_{19.26}$ si distingue da $[(a,s)]_{20.7}$ solo perché contiene anche coppie (b,t) con $b \in A$ e $t \in S$, dove non necessariamente $b \in I$.

(i) Possiamo però definire un'applicazione

$\psi : (S^{-1}I)_{20.7} \longrightarrow (S^{-1}I)_{19.26}$ con $[(a,s)]_{20.7} \longmapsto [(a,s)]_{19.26}$

Per $b \in I$ e $t \in S$ infatti

$(a,s) \sim_{20.7} (b,t) \iff$ esiste $u \in S$ con $u(ta - sb) = 0 \iff (a,s) \sim_{19.26} (b,t)$

per cui l'applicazione ψ è ben definita e iniettiva.

(ii) Ogni elemento di $(S^{-1}I)_{19.26}$ è della forma $z = [(a,s)]_{19.26}$ con $a \in I$ ed $s \in S$ e quindi $z = \psi([(a,s)]_{20.7})$. Perciò ψ è suriettiva.

(iii) È chiaro infine che ψ è un omomorfismo di A-moduli.

Nel seguito quindi non distinguiamo più tra le due definizioni.

Osservazione 20.13. Siano $x, y \in M$ ed $a \in A$. Allora

$(x+y)_S = x_S + y_S$ e $(ax)_S = a_S x_S$.

Dimostrazione. Ciò segue direttamente dalla prop. 20.11 utilizzando lo stesso ragionamento come nell'oss. 19.16.

Proposizione 20.14. *L'applicazione* $i_{S,M} := \bigcirc_x x_S : M \longrightarrow S^{-1}M$ *è un omomorfismo di* A*-moduli con nucleo* $\Omega_{S,M}$.

Dimostrazione. (1) Dall'oss. 20.13 segue che $i_{S,M}$ è un omomorfismo di gruppi abeliani.

(2) Siano $a \in A$ ed $x \in M$. Allora

$i_{S,M}(ax) = (ax)_S \overset{20.13}{=} a_S x_S = a x_S = a i_{S,M}(x)$

(3) Dall'oss. 20.9 abbiamo $\operatorname{Ker} i_{S,M} = \Omega_{S,M}$.

Proposizione 20.15. *Sia* $\varphi : M \longrightarrow N$ *un omomorfismo di* A*-moduli. Allora esiste un unico omomorfismo* $S^{-1}\varphi$ *di* $S^{-1}A$*-moduli* $S^{-1}M \longrightarrow S^{-1}N$ *che rende commutativo il diagramma (di* A*-moduli)*

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ {\scriptstyle i_{S,M}}\downarrow & & \downarrow{\scriptstyle i_{S,N}} \\ S^{-1}M & \xrightarrow{S^{-1}\varphi} & S^{-1}N \end{array}$$

$S^{-1}\varphi$ è dato da $(S^{-1}\varphi)\dfrac{x_S}{s} = \dfrac{(\varphi x)_S}{s}$.

Dimostrazione. (1) La costruzione del diagramma implica che per $x \in M$ dobbiamo avere $(S^{-1}\varphi)(x_S) = (\varphi x)_S$. Siccome $S^{-1}\varphi$ deve essere un omomorfismo di $S^{-1}A$-moduli, per $s \in S$ dobbiamo avere

$$(S^{-1}\varphi)\frac{x_S}{s} = \frac{1_S}{s}(S^{-1}\varphi)(x_S) = \frac{1_S}{s}(\varphi x)_S = \frac{(\varphi x)_S}{s}$$

(2) Dimostriamo che $S^{-1}\varphi$ in questo modo è ben definito.

Siano $\dfrac{x_S}{s} = \dfrac{y_S}{t}$, dove $s, t \in S$ ed $x, y \in M$. Allora esiste $u \in S$ tale che $u(tx - sy) = 0$. Ma ciò implica $u(t\varphi x - s\varphi y) = 0$.

(3) È immediato adesso che $S^{-1}\varphi$ è un omomorfismo di $S^{-1}A$-moduli.

Definizione 20.16. Una successione $M_1 \xrightarrow{\varphi} M \xrightarrow{\psi} M_2$ di omomorfismi di moduli su un anello si dice *esatta*, se $\operatorname{Ker}\psi = \operatorname{Im}\varphi$.

Teorema 20.17. *La successione $M_1 \xrightarrow{\varphi} M \xrightarrow{\psi} M_2$ di A-moduli sia esatta.*

Allora anche la successione $S^{-1}M_1 \xrightarrow{S^{-1}\varphi} S^{-1}M \xrightarrow{S^{-1}\psi} S^{-1}M_2$ è esatta.

Dimostrazione. (1) Siano $x \in M_1$ ed $s \in S$. Allora

$$(S^{-1}\psi)(S^{-1}\varphi)\frac{x_S}{s} = (S^{-1}\psi)\frac{(\varphi x)_S}{s} = \frac{(\psi(\varphi x))_S}{s} = \frac{0_S}{s} = 0$$

Perciò $\operatorname{Im}\varphi \subset \operatorname{Ker}\psi$.

(2) Siano $x \in M$ ed $s \in S$ tali che $(S^{-1}\psi)\dfrac{x_S}{s} = 0$. Ciò significa che $\dfrac{(\psi x)_S}{s} = 0$. Pertanto esiste $t \in S$ tale che $0 = t\psi x = \psi tx$. Per ipotesi esiste $y \in M_1$ tale che $tx = \varphi y$. Allora $x_S = \dfrac{(\varphi y)_S}{t}$, per cui $\dfrac{x_S}{s} = \dfrac{(\varphi y)_S}{st} = (S^{-1}\varphi)\dfrac{y_S}{st}$.

Ciò mostra $\operatorname{Ker}\psi \subset \operatorname{Im}\varphi$.

Corollario 20.18. *$\varphi : M \longrightarrow N$ sia un omomorfismo di A-moduli.*

(1) Se φ è iniettivo, allora anche $S^{-1}\varphi : S^{-1}M \longrightarrow S^{-1}N$ è iniettivo.

(2) Se φ è suriettivo, allora anche $S^{-1}\varphi : S^{-1}M \longrightarrow S^{-1}N$ è suriettivo.

Osservazione 20.19. Siano N un sottomodulo di M ed $i : N \longrightarrow M$ l'inclusione.

Per il cor. 20.18 l'omomorfismo $S^{-1}i : S^{-1}N \longrightarrow S^{-1}M$ è iniettivo e ci permette di considerare $S^{-1}N$ come sottomodulo di $S^{-1}M$.

Osservazione 20.20. Sia N un sottomodulo di M. Dalla successione esatta

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

otteniamo allora una successione esatta

$$0 \longrightarrow S^{-1}N \longrightarrow S^{-1}M \longrightarrow S^{-1}(M/N) \longrightarrow 0$$

che ci fornisce un isomorfismo $S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N)$.

Proposizione 20.21. *Siano N_1 ed N_2 sottomoduli di M. Allora:*

(1) $S^{-1}(N_1 + N_2) = S^{-1}N_1 + S^{-1}N_2$.

(2) $S^{-1}(N_1 \cap N_2) = S^{-1}N_1 \cap S^{-1}N_2$.

Dimostrazione. (1) Siano $x \in N_1, y \in N_2$ ed $s, t \in S$. Allora $\dfrac{x_S}{s} + \dfrac{y_S}{t} = \dfrac{tx_S + sy_S}{st}$ e ciò mostra che $S^{-1}N_1 + S^{-1}N_2 \subset S^{-1}(N_1 + N_2)$.

L'inclusione in senso opposto è ovvia.

(2) Anche qui è sufficiente dimostrare che $S^{-1}N_1 \cap S^{-1}N_2 \subset S^{-1}(N_1 \cap N_2)$:

Siano $x \in N_1, y \in N_2$ ed $s, t \in S$ tali che $\dfrac{x_S}{s} = \dfrac{y_S}{t}$. Allora esiste $u \in S$ con $utx = usy =: p$.

In particolare $p \in N_1 \cap N_2$, quindi $\dfrac{x_S}{s} = \dfrac{(utx)_S}{uts} = \dfrac{p_S}{uts} \in S^{-1}(N_1 \cap N_2)$.

21. Localizzazione in un ideale primo

Sia P un ideale primo di A. La localizzazione in P è la localizzazione rispetto al sottomonoide puro $A \setminus P$. $(A \setminus P)^{-1}P = PA_P$. Sia $s \in A \setminus P$. Allora $\frac{a_P}{s}$ è invertibile in $A_P \iff a \notin P \iff \frac{a_P}{s} \notin PA_P$. Perciò A_P è un anello locale con ideale massimale PA_P. Gli ideali primi di A_P corrispondono in modo biiettivo e naturale agli ideali primi di A contenuti in P. Ogni elemento di un ideale primo minimale è uno zerodivisore; la dimostrazione è un primo esempio come attraverso la localizzazione si possono ottenere proposizioni, nel cui enunciato non appare il concetto di localizzazione. Isomorfia naturale $A_P/PA_P \cong \mathcal{K}(A/P)$ attraverso l'applicazione $\frac{a_P}{s} + PA_P \longmapsto \frac{a+P}{s+P}$. $\operatorname{Ann}(X) := \{a \in A \mid aX = 0\}$. Per un A-modulo finitamente generato M si ha $M_P \neq 0 \iff \operatorname{Ann}(M) \subset P$; l'implicazione $\implies$ vale anche senza l'ipotesi che M sia finitamente generato. Spesso attraverso lo studio (cosiddetto locale) delle localizzazioni si possono dimostrare proprietà globali: Per un A-modulo M si ha $M = 0 \iff M_P = 0$ per ogni $P \in \operatorname{Spec} A \iff M_\mathfrak{m} = 0$ per ogni $\mathfrak{m} \in \operatorname{Max} A$. Per $f \in A \setminus P$ possiamo formare la localizzazione A_f, perché f non è nilpotente, ottenendo un omomorfismo $A_f \longrightarrow A_P$. La totalità di questi omomorfismi permette di ricostruire A_P tramite la rappresentazione $A_P = \varinjlim_{f \in A \setminus P} A_f$ (senza dimostrazione).

Situazione 21.1. Siano A un anello commutativo e $P \in \operatorname{Spec} A$.
L'ipotesi implica $A \neq 0$.

Osservazione 21.2. $A \setminus P$ è un sottomonoide puro di A.

Definizione 21.3. Per un A-modulo M poniamo $M_P := (A \setminus P)^{-1}M$ e in particolare $A_P := (A \setminus P)^{-1}A$.

Per $x \in M$ risp. $a \in A$ ed $s \in A \setminus P$ poniamo $x_P := x_{A\setminus P}$ risp. $a_P := a_{A\setminus P}$, $\frac{x_P}{s} := \frac{x_{A\setminus P}}{s}$, $\frac{a_P}{s} := \frac{a_{A\setminus P}}{s}$.

Similmente con $i_P : A \longrightarrow A_P$ denotiamo l'omomorfismo canonico $i_{A\setminus P}$.

Queste notazioni sono comunemente usate e non ambigue, perché, essendo $0 \in P$, P non è mai un sottomonoide puro di A.

Osservazione 21.4. $PA_P = (A \setminus P)^{-1}P = P_P$.

Dimostrazione. Basta osservare che tramite l'omomorfismo canonico $A \longrightarrow A_P$ per $a \in A$ e $p \in P$ si ha $pa_P = p_P a_P = (pa)_P$ e che $PA = P$, perché P è un ideale.

Osservazione 21.5. P è $(A \setminus P)$-saturo.

Dimostrazione. Ovviamente $P \cap (A \setminus P) = \emptyset$, quindi l'enunciato segue dal cor. 19.41 (o direttamente dalla definizione di ideale primo).

Lemma 21.6. *Siano $a \in A$ ed $s \in A \setminus P$. Allora sono equivalenti:*

(1) $\frac{a_P}{s} \in PA_P$.

(2) $a \in P$.

Dimostrazione. Per l'oss. 21.5 P è $(A\setminus P)$-saturo, cosicché l'enunciato segue dal cor. 19.45 e dall'oss. 21.4.

Lemma 21.7. *Siano $a \in A$ ed $s \in A \setminus P$. Allora sono equivalenti:*

(1) $\frac{a_P}{s}$ è invertibile in A_P.

(2) $a \notin P$.

(3) $\frac{a_P}{s} \notin PA_P$.

(4) $\frac{a_P}{s} + PA_P \neq 0$.

Dimostrazione. (1) $\implies$ (2): Sia $\frac{a_S}{s}\frac{b_S}{t} = 1_S$ con $b \in A, t \in A \setminus P$. Allora esiste $u \in A \setminus P$ tale che $uab = ust \in A \setminus P$. Necessariamente si ha $a \notin P$.

(2) $\implies$ (1): Se $a \notin P$, allora $\frac{a_S}{s}\frac{s_S}{a} = 1_S$ in A_P.

(2) $\iff$ (3): Segue direttamente dal lemma 21.6.

(3) $\iff$ (4): Chiaro.

Teorema 21.8. *A_P è un anello locale con ideale massimale PA_P.*

Dimostrazione. Per il lemma 21.7 l'insieme degli elementi non invertibili di A_P coincide con l'ideale PA_P. Per il lemma 17.6 A_P è un anello locale il cui ideale massimale è uguale a PA_P per il cor. 17.7.

Osservazione 21.9. $(A \setminus P)^\sharp$ è l'insieme degli ideali di A contenuti in P.

Dimostrazione. Infatti per un ideale I di A si ha

$$I \in (A \setminus P)^\sharp \iff I \cap (A \setminus P) = \emptyset \iff I \subset P$$

Teorema 21.10. *La biiezione del teorema 19.35 induce una biiezione naturale*

$$\begin{aligned} \{Q \in \operatorname{Spec} A \mid Q \subset P\} &\longleftrightarrow \operatorname{Spec} A_P \\ Q &\longmapsto QA_P \\ i_P^{-1}(N) &\longmapsto\!\shortmid\ N \end{aligned}$$

Dimostrazione. Teorema 19.46.

Proposizione 21.11. *P sia un ideale primo minimale. Allora:*

(1) PA_P è l'unico ideale primo di A_P.

(2) Ogni elemento di P è uno zerodivisore.

Dimostrazione. Seguiamo Brüske/ [1224], p.26.

(1) Per il teorema 21.10 PA_P è un ideale primo minimale di A_P e per il teorema 21.8 è anche l'unico ideale massimale. È chiaro che ciò implica che non ci possono essere altri ideali primi di A_P.

(2) Sia $a \in P$. Vogliamo dimostrare che a è uno zerodivisore. Possiamo assumere che $a \neq 0$. Il punto (1) implica che in A_P si ha $\sqrt{0} = PA_P$, perciò esiste $n \in \mathbb{N} + 1$ tale che $a_P^n = 0$. Scegliamo n in modo minimale, cosicché

$a_P^{n-1} \neq 0$. Allora esiste $s \in A \setminus P$ tale che $sa^n = 0$. Per ipotesi su n si ha $sa^{n-1} \neq 0$, perché altrimenti si avrebbe $a_P^{n-1} = 0$.

Osservazione 21.12. Siano $a, b \in A$ ed $s, t \in A \setminus P$. Allora sono equivalenti:

(1) $\dfrac{a_P}{s} + PA_P = \dfrac{b_P}{t} + PA_P$.

(2) $ta - sb \in P$.

(3) $\dfrac{a+P}{s+P} = \dfrac{b+P}{t+P}$ in $\mathcal{K}(A/P)$.

Dimostrazione. (1) $\iff$ (2): Si ha

$$\frac{a_P}{s} + PA_P = \frac{b_P}{t} + PA_P \iff \frac{(ta-sb)_P}{st} \in PA_P \overset{21.7}{\iff} ta - sb \in P$$

(2) $\implies$ (3): Sia $ta - sb \in P$. Allora

$$\frac{a+P}{s+P} = \frac{b+P}{t+P} = \frac{ta-sb+P}{st+P} = 0 \quad \text{in } \mathcal{K}(A/P).$$

(3) $\implies$ (2): Sia $\dfrac{a+P}{s+P} = \dfrac{b+P}{t+P}$. Allora $\dfrac{ta-sb+P}{st+P} = 0$ in $\mathcal{K}(A/P)$ e ciò significa proprio che $ta - sb \in P$.

Proposizione 21.13. $A_P/PA_P \cong \mathcal{K}(A/P)$.

Esplicitamente si ha l'isomorfismo $\dfrac{a_P}{s} + PA_P \longmapsto \dfrac{a+P}{s+P}$.

Dimostrazione. L'applicazione indicata è ben definita e un isomorfismo per l'oss. 21.12.

Definizione 21.14. Per un A-modulo M e un sottoinsieme $X \subset M$ poniamo

$$\operatorname{Ann}(X) := \{a \in A \mid aX = 0\}$$

In particolare abbiamo così definito l'annullatore $\operatorname{Ann}(M)$ di tutto il modulo M e l'annullatore $\operatorname{Ann}(x)$ di un singolo elemento $x \in M$.

Osservazione 21.15. Siano M un A-modulo ed $X \subset M$. Allora $\operatorname{Ann}(X)$ è un ideale generalizzato di A e un ideale di A se e solo se X contiene un elemento $\neq 0$.

Dimostrazione. Chiaro. Se $x \in M$ ed $x \neq 0$, allora $1x \neq 0$, quindi $\operatorname{Ann}(X) \neq A$.

Osservazione 21.16. Sia M un A-modulo. Allora valgono le implicazioni:

(1) $M_P \neq 0 \implies \operatorname{Ann}(M) \subset P$.

(2) $\operatorname{Ann}(M) \subset P$ ed M finitamente generato $\implies M_P \neq 0$.

Dimostrazione. (1) Siano $x \in M$ ed $s \in A \setminus P$ tali che $\dfrac{x_S}{s} \neq 0$. Allora $tx \neq 0$ per ogni $t \in A \setminus P$.

Ciò significa $\operatorname{Ann}(M) \cap (A \setminus P) = \emptyset$, ossia $\operatorname{Ann}(M) \subset P$.

(2) Sia $\operatorname{Ann}(M) \subset P$. Per ipotesi esistono $e_1, \ldots, e_m \in M$ tali che $M = A\langle e_1, \ldots, e_m \rangle$.

Sia $M_P = 0$. Allora $(e_1)_P = \ldots = (e_m)_P = 0$. Ciò significa che esistono $s_1, \ldots, s_m \in A \setminus P$ tali che $s_1 e_1 = \ldots = s_m e_m = 0$ e quindi anche $te_i = 0$ per ogni i, se poniamo $t := s_1 \cdots s_m \in A \setminus P$.

Ma ciò implica $t \in \operatorname{Ann}(M)$ e quindi $t \in P$, una contraddizione.

Teorema 21.17. *Per un A-modulo M sono equivalenti:*

(1) $M = 0$.

(2) $M_P = 0$ *per ogni* $P \in \operatorname{Spec} A$.

(3) $M_{\mathfrak{m}} = 0$ *per ogni* $\mathfrak{m} \in \operatorname{Max} A$.

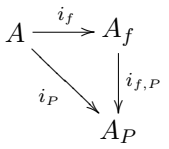
Dimostrazione. (1) $\implies$ (2) $\implies$ (3): Chiaro.

(2) Assumiamo, per assurdo, che $M \neq 0$. Sia $x \in M$ con $x \neq 0$.

Allora $\operatorname{Ann}(x) = \operatorname{Ann}(Ax)$ è un ideale e quindi contenuto in un ideale massimale $\mathfrak{m}$. Siccome l'A-modulo Ax è finitamente generato, dall'oss. 21.16 segue $(Ax)_{\mathfrak{m}} \neq 0$ e quindi anche $M_{\mathfrak{m}} \neq 0$ (ciò è ovvio e segue anche dal cor. 20.18), una contraddizione.

Nota 21.18. Sia $f \in A \setminus P$. Allora f non è nilpotente per il teorema 3.38, perciò possiamo formare il sottomonoide puro $S := \{f^n \mid n \in \mathbb{N}\}$ e la localizzazione $A_f = S^{-1}A$.

Per la prop. 19.47 esiste un unico omomorfismo di anelli $i_{f,P} : A_f \longrightarrow A_P$ che rende commutativo il diagramma



dato da $i_{f,P}\left(\dfrac{a_f}{f^n}\right) = \dfrac{a_P}{f^n}$.

Si può dimostrare che la totalità di queste informazioni permette di ricostruire A_P, nel senso che

$$A_P = \varinjlim_{f \in A \setminus P} A_f$$

utilizzando il concetto di limite induttivo che forse tratteremo piu avanti nell'ambito della teoria dei fasci; cfr. Görtz/ [21712], pag. 553, e Atiyah/ [3518], es. 3.23.

22. Applicazioni polinomiali tra insiemi affini

I prossimi capitoli, apparentemente complicati, non contengono risultati veramente profondi, ma piuttosto riformulazioni sotto diversi punti di vista e con notazioni adeguate di concetti legati agli insiemi algebrici affini. Sia K un campo. Useremo da ora in avanti l'abbreviazione $K[n] := K[x_1, \dots, x_n]$. Composizione di polinomi per sostituzione: $g(f_1, \dots, f_m)$. L'applicazione $(f_1, \dots, f_m)_{K^n \longrightarrow K^m} := \bigcirc_\alpha (f_1(\alpha), \dots, f_m(\alpha))$. Costruzione controvariante dell'omomorfismo di K-algebre $(f_1, \dots, f_m)^{K[m] \longrightarrow K[n]} := \bigcirc_g g(f_1, \dots, f_m)$. Se J è un ideale di $K[m]$, allora si ha $\varphi^{-1}(\mathrm{Zeri}(J)) = \mathrm{Zeri}((f_1, \dots, f_m)^{K[m] \longrightarrow K[n]}(J))$. Applicazioni polinomiali $K^n \longrightarrow K^m$. Esse sono continue nella topologia di Zariski. La topologia di Zariski su K^n non coincide con la topologia prodotto. L'insieme $\mathcal{O}(X, Y)$ delle applicazioni polinomiali $(f_1, \dots, f_m)_{X \longrightarrow Y}$. La composizione di applicazioni polinomiali è polinomiale.

Situazione 22.1. Sia K un campo.

In alcuni esempi assumiamo che K abbia caratteristica 0.

Definizione 22.2. Per brevità nel seguito per $n \in \mathbb{N} + 1$ per un anello commutativo A (in particolare per $A = K$) utilizzeremo spesso la notazione $A[n] := A[x_1, \dots, x_n]$.

Essa naturalmente non deve essere confusa con la notazione usata nella def. 4.9 o nell'oss. 7.7.

Osservazione 22.3. Siano $g \in K[m]$ ed $f_1, \dots, f_m \in K[n]$. Se sostituiamo in g ogni x_i con f_i, otteniamo l'elemento $g(f_1, \dots, f_m) \in K[n]$.

Ciò è in accordo con la def. 4.8, usando il fatto che $K[n]$ è una K-algebra commutativa.

Osservazione 22.4. Nella situazione dell'oss. 22.3 per $\alpha \in K^n$ si ha

$$g(f_1, \dots, f_m)(\alpha) = g(f_1(\alpha), \dots, f_m(\alpha))$$

Dimostrazione. Ciò è evidente se scriviamo $g(f_1, \dots, f_m)$ nella forma $g(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))$. Cfr. es. 22.5.

Esempio 22.5. Siano $g = x^2 + 4x + 3$, $f = 2x^3 + 7x + 5$. Allora

$$g(f) = (2x^3 + 7x + 5)^2 + 4(2x^3 + 7x + 5) + 3$$

e per $\alpha \in K$ si ha

$$g(f)(\alpha) = (2\alpha^3 + 7\alpha + 5)^2 + 4(2\alpha^3 + 7\alpha + 5) + 3 = g(f(\alpha))$$

Esempio 22.6. Siano $g = x_1^3 + 3x_1x_2 + 6x_1 + 5$, $f_1 = x_1x_3 + x_2 + 4$, $f_2 = x_2^3 + 4x_1x_2x_3 + x_2^2 + x_1 + 1$.

Allora $g(f_1, f_2) = (x_1x_3 + x_2 + 4)^3 + 3(x_1x_3 + x_2 + 4)(x_2^3 + 4x_1x_2x_3 + x_2^2 + x_1 + 1) + 6(x_1x_3 + x_2 + 4) + 5 \in K[x_1, x_2, x_3]$.

Osservazione 22.7. Alcune delle notazioni in questo capitolo sono un po' complicate e spesso nei testi le varie costruzioni vengono identificate. D'altra parte forse è utile all'inizio usare notazioni precise, anche se più impegnative nella scrittura.

Definizione 22.8. Per $f \in K[n]$ con $f_{K^n \longrightarrow K}$ denotiamo l'applicazione $\bigcirc\limits_{\alpha} f(\alpha) : K^n \longrightarrow K$.

Nella prop. 14.38 abbiamo scritto f_{app} invece di $f_{K^n \longrightarrow K}$.

Più in generale per $f_1, \ldots, f_m \in K[n]$ definiamo l'applicazione $(f_1, \ldots, f_m)_{K^n \longrightarrow K^m} := \bigcirc\limits_{\alpha}(f_1(\alpha), \ldots, f_m(\alpha)) : K^n \longrightarrow K^m$.

Definizione 22.9. Per $f_1, \ldots, f_m \in K[n]$ introduciamo l'applicazione

$$\begin{aligned}(f_1, \ldots, f_m)^{K[m] \longrightarrow K[n]} : K[m] &\longrightarrow K[n] \\ g &\longmapsto g(f_1, \ldots, f_m)\end{aligned}$$

Per l'oss. 22.3 questa applicazione è ben definita e si verifica facilmente che essa è un omomorfismo di K-algebre.

Abbiamo posto la sigla $K[m] \longrightarrow K[n]$ in alto per indicare che essa descrive un'operazione *controvariante*.

Esempio 22.10. (1) I polinomi $f_1 := x^2+5, f_2 := x^4+3x+2 \in K[x]$ definiscono l'applicazione

$$\begin{aligned}(f_1, f_2)^{K[x_1,x_2] \longrightarrow K[x]} : K[x_1, x_2] &\longrightarrow K[x] \\ g &\longmapsto g(x^2+5, x^4+3x+2)\end{aligned}$$

(2) I polinomi $f_1 = x_1x_2x_3 + 4, f_2 = x_1x_2 + x_2x_3 + x_1x_3 + 3x_1 + 5 \in K[3]$ definiscono l'applicazione

$$\begin{aligned}(f_1, f_2)^{K[2] \longrightarrow K[3]} : K[2] &\longrightarrow K[3] \\ g &\longmapsto g(x_1x_2x_3 + 4, x_1x_2 + x_2x_3 + x_1x_3 + 3x_1 + 5)\end{aligned}$$

Lemma 22.11. *Siano $f_1, \ldots, f_m \in K[n]$ e $\varphi := (f_1, \ldots, f_m)_{K^n \longrightarrow K^m}$. Sia J un ideale generalizzato di $K[m]$. Allora*

$$\varphi^{-1}(\text{Zeri}(J)) = \text{Zeri}((f_1, \ldots, f_m)^{K[m] \longrightarrow K[n]}(J))$$

Dimostrazione. Per $\alpha \in K^n$ sono equivalenti:

$\alpha \in \varphi^{-1}(\text{Zeri}(J))$.

$(f_1(\alpha), \ldots, f_m(\alpha)) \in \text{Zeri}(J)$.

$g(f_1(\alpha), \ldots, f_m(\alpha)) = 0$ per ogni $g \in J$.

$((f_1, \ldots, f_m)^{K[m] \longrightarrow K[n]}(g))(\alpha) = 0$ per ogni $g \in J$.

$h(\alpha) = 0$ per ogni $h \in (f_1, \ldots, f_m)^{K[m] \longrightarrow K[n]}(J)$.

Osservazione 22.12. Nella situazione del lemma 22.11 siano $h_1, \ldots, h_k \in K[m]$ tali che $J = K[m]_{\smile}(h_1, \ldots, h_k)$. Allora

$$\varphi^{-1}(\text{Zeri}(J)) = \text{Zeri}(h_1(f_1, \ldots, f_m), \ldots, h_k(f_1, \ldots, f_m))$$

Dimostrazione. È chiaro che l'insieme alla destra contiene $\text{Zeri}((f_1, \ldots, f_m)^{K[m] \longrightarrow K[n]}(J))$.

Sia viceversa $\alpha \in K^m$ tale che $h_i(f_1, \ldots, f_m)(\alpha) = 0$ per ogni i e sia $u = p_1h_1 + \ldots + p_kh_k \in J$. Allora

$$u(f_1, \ldots, f_m)(\alpha) \overset{22.4}{=} \sum_{i=1}^{k} p_i(f_1, \ldots, f_m)(\alpha) \cdot h_i(f_1, \ldots, f_m)(\alpha) = 0$$

Esempio 22.13. Siano $f := x^2$ e $\varphi := f_{K \longrightarrow K} = \bigcirc_{\alpha} \alpha^2 : K \longrightarrow K$. Sia J un ideale generalizzato di $K[x]$. Siccome $K[x]$ è un anello ad ideali principali, esiste $h \in K[x]$ tale che $J = K[x]_{\smile} h$.

Allora $\mathrm{Zeri}(J) = \mathrm{Zeri}(h)$ e per il lemma 22.11 abbiamo

$$\varphi^{-1}(\mathrm{Zeri}(h)) \overset{22.12}{=} \mathrm{Zeri}(f^{K[x] \longrightarrow K[x]}(h)) = \mathrm{Zeri}(h(x^2))$$

Se per esempio $h = (x-1)(x-4)$ e quindi $\mathrm{Zeri}(h) = \{1, 4\}$, allora

$$\begin{aligned} \varphi^{-1}(\mathrm{Zeri}(h)) &= \mathrm{Zeri}((x^2-1)(x^2-4)) \\ &= \mathrm{Zeri}((x-1)(x+1)(x-2)(x+2)) = \{1, -1, 2, -2\} \end{aligned}$$

Definizione 22.14. Un'applicazione $\varphi : K^n \longrightarrow K^m$ si dice *polinomiale*, se esistono polinomi $f_1, \ldots, f_m \in K[n]$ tali che $\varphi = (f_1, \ldots, f_m)_{K^n \longrightarrow K^m}$.

Proposizione 22.15. *Sia $\varphi : K^n \longrightarrow K^m$ un'applicazione polinomiale.*

Allora φ è continua nella topologia di Zariski di K^n risp. K^m.

Dimostrazione. Il lemma 22.11 implica che per ogni chiuso Y di K^m la controimmagine $\varphi^{-1}(Y)$ è un chiuso di K^n.

Osservazione 22.16. Per la dimostrazione della prop. 22.15 non possiamo usare la prop. 14.38 perché, come vedremo adesso, la topologia di Zariski su K^n (o K^m) non coincide con la topologia prodotto (tranne in casi banali).

Nota 22.17. Sia K infinito. Denotiamo con $\Delta := (x_1 = x_2) = \{(t, t) \mid t \in K\}$ la diagonale di K^2. Allora $K^2 \setminus \Delta$ è un aperto di K^2 nella topologia di Zariski, ma non contiene nessun insieme della forma $U \times V$, con U e V aperti non vuoti di K.

Ciò mostra che la topologia di Zariski su K^2 non coincide con la topologia prodotto definita dalla topologia di Zariski su K.

Dimostrazione. Assumiamo, per assurdo, che U e V siano aperti non vuoti di K con $U \times V \subset K^2 \setminus \Delta$.

Allora sicuramente $U, V \neq K$, quindi per la prop. 14.37 esistono sottoinsiemi finiti F, G di K tali che $U = K \setminus F$, $V = K \setminus G$.

Siccome K è infinito, l'insieme $K \setminus (F \cup G)$ è anch'esso infinito e quindi non vuoto, per cui possiamo trovare un elemento $t \in K \setminus (F \cup G)$. Allora $(t, t) \in (U \times V) \cap \Delta$, una contraddizione.

Definizione 22.18. Siano $X \subset K^n$ ed $Y \subset K^m$ (supporremo quasi sempre che X ed Y siano chiusi non vuoti) e siano $f_1, \ldots, f_m \in K[n]$ tali che $(f_1(\alpha), \ldots, f_m(\alpha)) \in Y$ per ogni $\alpha \in X$. Allora possiamo definire l'applicazione

$$\begin{aligned} (f_1, \ldots, f_m)_{X \longrightarrow Y} : X &\longrightarrow Y \\ \alpha &\longmapsto (f_1(\alpha), \ldots, f_m(\alpha)) \end{aligned}$$

Nel caso speciale $X = K^n$, $Y = K^m$ questa notazione è in accordo con quella introdotta nella def. 22.8.

Definizione 22.19. Siano $X \subset K^n$ ed $Y \subset K^m$. Un'applicazione $\varphi : X \longrightarrow Y$ si chiama *polinomiale*, se esistono polinomi $f_1, \ldots, f_m \in K[n]$ tali che $\varphi = (f_1, \ldots, f_m)_{X \longrightarrow Y}$.

Nel caso speciale $X = K^n, Y = K^m$ ciò è in accordo con la def. 22.14.

$\mathcal{O}(X, Y)$ sia l'insieme delle applicazioni polinomiali $X \longrightarrow Y$.

Proposizione 22.20. *Siano $X \subset K^n$, $Y \subset K^m$, $Z \subset K^p$ e $\varphi \in \mathcal{O}(X, Y)$, $\psi \in \mathcal{O}(Y, Z)$. Allora $\psi \circ \varphi \in \mathcal{O}(X, Z)$.*

Più precisamente, se $\varphi = (f_1, \ldots, f_m)_{X \longrightarrow Y}$ e $\psi = (g_1, \ldots, g_p)_{Y \longrightarrow Z}$ con $f_1, \ldots, f_m \in K[n]$ e $g_1, \ldots, g_p \in K[m]$, allora

$$\psi \circ \varphi = (g_1(f_1, \ldots, f_m), \ldots, g_p(f_1, \ldots, f_m))_{X \longrightarrow Z}$$

Dimostrazione. Per $\alpha \in X$ abbiamo

$$\begin{aligned} \psi(\varphi(\alpha)) &= \psi(f_1(\alpha), \ldots, f_m(\alpha)) \\ &= (g_1(f_1(\alpha), \ldots, f_m(\alpha)), \ldots, g_p(f_1(\alpha), \ldots, f_m(\alpha))) \end{aligned}$$

e usando l'oss. 22.4 vediamo che con $h_j := g_j(f_1, \ldots, f_m) \in K[n]$ per $j = 1, \ldots, p$ abbiamo $\psi \circ \varphi = (h_1, \ldots, h_p)_{X \longrightarrow Z}$.

Osservazione 22.21. Siano $X \subset K^n$, $Y \subset K^m$ ed $f_1, \ldots, f_m, f'_1, \ldots, f'_m$ polinomi appartenenti a $K[n]$. Allora sono equivalenti:

(1) $(f_1, \ldots, f_m)_{X \longrightarrow Y} = (f'_1, \ldots, f'_m)_{X \longrightarrow Y}$.

(2) $f_i - f'_i \in \mathcal{J}(X)$ per ogni $i = 1, \ldots, m$.

Dimostrazione. Infatti (1) e (2) sono entrambi equivalenti alla condizione che $f_i(\alpha) = f'_i(\alpha)$ per ogni $\alpha \in X$ ed ogni $i = 1, \ldots, m$.

23. L'anello $\mathcal{O}(\mathbf{X}) \cong \Gamma(\mathbf{X})$ delle funzioni polinomiali

La K-algebra K^X. La sotto-K-algebra $\mathcal{O}(X) := \mathcal{O}(X,K) = \{f_{X\longrightarrow K} \mid f \in K[n]\}$ delle funzioni polinomiali si chiama l'anello delle funzioni polinomiali su X. $f_{X\longrightarrow K} = g_{X\longrightarrow K} \iff f - g \in \mathcal{J}(X) \iff f_{\overline{X}\longrightarrow K} = g_{\overline{X}\longrightarrow K}$. Isomorfia naturale $\Gamma(X) := K[n]/\mathcal{J}(X) \cong \mathcal{O}(X)$. $\mathcal{O}(X)$ separa i punti di X. Se $\varphi, \psi : X \longrightarrow Y$ sono due applicazioni tali che $\eta \circ \varphi = \eta \circ \psi$ per ogni $\eta \in \mathcal{O}(Y)$, allora $\varphi = \psi$. Un'applicazione $\varphi : X \longrightarrow Y$ appartiene a $\mathcal{O}(X,Y)$ se e solo se $\eta \circ \varphi \in \mathcal{O}(X)$ per ogni $\eta \in \mathcal{O}(Y)$. Le coordinate $\pi_i^X := (x_i)_{X\longrightarrow K}$. Per ogni $f \in K[n]$ si ha $f_{X\longrightarrow K} = f(\pi_1^X, \ldots, \pi_n^X)$. Ciò implica $\mathcal{O}(X) = K[\pi_1^X, \ldots, \pi_n^X]$ - per questa ragione $\mathcal{O}(X)$ si chiama anche l'anello delle coordinate di X.

Situazione 23.1. Sia K un campo.

Definizione 23.2. Per insiemi X, Y denotiamo, come d'uso comune, con Y^X l'insieme delle applicazioni $X \longrightarrow Y$.

Osservazione 23.3. Sia X un insieme. Allora K^X è una K-algebra con le operazioni

$$\begin{aligned} \varphi + \psi &:= \bigcirc_\alpha \varphi(\alpha) + \psi(\alpha) \\ \varphi \cdot \psi &:= \bigcirc_\alpha \varphi(\alpha)\psi(\alpha) \\ a\varphi &:= \bigcirc_\alpha a\varphi(\alpha) \end{aligned}$$

per $\varphi, \psi \in K^X$ ed $a \in K$.

Definizione 23.4. Per un sottoinsieme $X \subset K^n$ sia $\mathcal{O}(X) := \mathcal{O}(X,K)$ l'insieme delle funzioni polinomiali $X \longrightarrow K$. Quindi

$$\mathcal{O}(X) = \{f_{X\longrightarrow K} \mid f \in K[n]\}$$

Anche qui spesso chiederemo che X sia un insieme algebrico.

Osservazione 23.5. Siano $X \subset K^n$ ed $f, g \in K[n]$, $a \in K$. Allora

$$\begin{aligned} f_{X\longrightarrow K} + g_{X\longrightarrow K} &= (f+g)_{X\longrightarrow K} \\ f_{X\longrightarrow K} g_{X\longrightarrow K} &= (fg)_{X\longrightarrow K} \\ af_{X\longrightarrow K} &= (af)_{X\longrightarrow K} \end{aligned}$$

Dimostrazione. Per ogni $\alpha \in X$ abbiamo $\varphi(\alpha) = f(\alpha)$, $\psi(\alpha) = g(\alpha)$, e quindi

$$\begin{aligned} (\varphi + \psi)(\alpha) &= \varphi(\alpha) + \psi(\alpha) = f(\alpha) + g(\alpha) = (f+g)(\alpha) \\ (\varphi\psi)(\alpha) &= \varphi(\alpha)\psi(\alpha) = f(\alpha)g(\alpha) = (fg)(\alpha) \\ (a\varphi)(\alpha) &= a\varphi(\alpha) = af(\alpha) = (af)(\alpha) \end{aligned}$$

per cui $\varphi + \psi = (f+g)_{X\longrightarrow K}$, $\varphi\psi = (fg)_{X\longrightarrow K}$, $a\varphi = (af)_{X\longrightarrow K}$.

Proposizione 23.6. *Sia $X \subset K^n$.*

Allora $\mathcal{O}(X)$ è una sotto-K-algebra di K^X.

Dimostrazione. L'enunciato segue dall'oss. 23.5.

Osservazione 23.7. Siano $X \subset K^n$ ed $f, g \in K[n]$. Allora

$$f_{X \longrightarrow K} = g_{X \longrightarrow K} \iff f - g \in \mathcal{J}(X)$$

Dimostrazione. I seguenti enunciati sono equivalenti:

(1) $f_{X \longrightarrow K} = g_{X \longrightarrow K}$.

(2) $f(\alpha) = g(\alpha)$ per ogni $\alpha \in X$.

(3) $(f - g)(\alpha) = 0$ per ogni $\alpha \in X$.

(4) $f - g \in \mathcal{J}(X)$.

Corollario 23.8. *Siano $X \subset K^n$ ed $f, g \in K[n]$ tali che $f_{X \longrightarrow K} = g_{X \longrightarrow K}$.*

Allora $f_{\overline{X} \longrightarrow K} = g_{\overline{X} \longrightarrow K}$.

Dimostrazione. Dall'oss. 14.28 sappiamo che $\mathcal{J}(X) = \mathcal{J}(\overline{X})$. L'enunciato segue dall'oss. 23.7.

Definizione 23.9. $\Gamma(X) := K[n]/\mathcal{J}(X)$.

Nota 23.10. Per $X \subset K^n$ l'applicazione

$$\begin{aligned} K[n] &\longrightarrow \mathcal{O}(X) \\ f &\longmapsto f_{X \longrightarrow K} \end{aligned}$$

è per definizione suriettiva e, come si vede dall'oss. 23.5, un omomorfismo di K-algebre (cioè un omomorfismo di anelli che è allo stesso tempo K-lineare), il cui nucleo è uguale a $\mathcal{J}(X)$. Otteniamo così un isomorfismo naturale

$$\begin{aligned} \Gamma(X) &\longrightarrow \mathcal{O}(X) \\ f + \mathcal{J}(X) &\longmapsto f_{X \longrightarrow K} \end{aligned}$$

Definizione 23.11. Sia $X \subset K^n$. La K-algebra $\mathcal{O}(X)$ si chiama *l'anello delle funzioni polinomiali* su X e può, per la nota 23.10, essere identificata con la K-algebra $\Gamma(X)$.

Osservazione 23.12. Nelle ultime considerazioni non abbiamo supposto che l'insieme $X \subset K^n$ sia algebrico. Solo quando vogliamo ricostruire X dall'algebra $\mathcal{O}(X)$ in modo univoco, dobbiamo supporre che X sia algebrico.

Nota 23.13. Sia $X \subset K^n$. Allora per $i \in \{1, \ldots, n\}$ la funzione $(x_i)_{X \longrightarrow K}$ appartiene a $\mathcal{O}(X)$ ed è semplicemente la proiezione sull'i-esima coordinata.

Siano adesso $Y \subset K^m$ e $\varphi : X \longrightarrow Y$ un'applicazione (non necessariamente polinomiale). Allora per $i \in \{1, \ldots, m\}$ la funzione $\varphi_i := (x_i)_{Y \longrightarrow K} \circ \varphi : X \longrightarrow K$ è la i-esima componente dell'applicazione φ.

Se ad esempio con $K = \mathbb{R}$, $X = \mathbb{R} \times (0, \infty)$, $Y = [0, 1] \times [-1, 1]$, l'applicazione φ è data da $\varphi(x, y) := (\cos^2(x + y), \sin \log y)$, allora $\varphi_1 = \bigcirc\limits_{(x,y)} \cos^2(x + y)$, $\varphi_2 = \bigcirc\limits_{(x,y)} \sin \log y$.

È chiaro che due applicazioni $\varphi, \psi : X \longrightarrow Y$ coincidono se e solo se $\varphi_i = \psi_i$ per ogni $i = 1, \ldots, m$ e quindi se e solo se $(x_i)_{Y \longrightarrow K} \circ \varphi = (x_i)_{Y \longrightarrow K} \circ \psi$ per ogni $i = 1, \ldots, m$.

Proposizione 23.14. *Sia $X \subset K^n$. Allora $\mathcal{O}(X)$ separa i punti di X.*

In altre parole, se $\alpha, \beta \in X$ sono tali che $\alpha \neq \beta$, allora esiste $\theta \in \mathcal{O}(X)$ con $\theta(\alpha) \neq \theta(\beta)$.

Dimostrazione. Ciò è dovuto al fatto che le proiezioni $(x_i)_{X \longrightarrow K}$ separano i punti di X: Sia ad esempio $\alpha_1 \neq \beta_1$.

Allora per $\theta := (x_1)_{X \longrightarrow K}$ si ha $\theta(\alpha) = \alpha_1 \neq \beta_1 = \theta(\beta)$.

Lemma 23.15. *Siano $X \subset K^n, Y \subset K^m$ e $\varphi, \psi : X \longrightarrow Y$ due applicazioni. Allora sono equivalenti:*

(1) $\varphi = \psi$.

(2) $\eta \circ \varphi = \eta \circ \psi$ per ogni $\eta \in \mathcal{O}(Y)$.

(3) $(x_i)_{Y \longrightarrow K} \circ \varphi = (x_i)_{Y \longrightarrow K} \circ \psi$ per ogni $i = 1, \ldots, m$.

Dimostrazione. (1) $\implies$ (2) $\implies$ (3): Chiaro.

(3) $\implies$ (2): Nota 23.13.

Teorema 23.16. *Siano $X \subset K^n, Y \subset K^m$ e $\varphi = (\varphi_1, \ldots, \varphi_m) : X \longrightarrow Y$ un'applicazione. Allora sono equivalenti:*

(1) $\varphi \in \mathcal{O}(X)$.

(2) $\eta \circ \varphi \in \mathcal{O}(X)$ per ogni $\eta \in \mathcal{O}(Y)$.

(3) $\varphi_i \in \mathcal{O}(X)$ per ogni $i = 1, \ldots, m$.

Dimostrazione. (1) $\implies$ (2): Prop. 2.20.

(2) $\implies$ (3): Chiaro, perché $\varphi_i = (x_i)_{Y \longrightarrow K} \circ \varphi$.

(3) $\implies$ (1): L'ipotesi (3) implica che per ogni $i = 1, \ldots, m$ esiste $f_i \in K[n]$ tale che $\varphi_i = (f_i)_{X \longrightarrow K}$.

Ma allora per ogni $\alpha \in X$ si ha

$$\varphi(\alpha) = (\varphi_1(\alpha), \ldots, \varphi_m(\alpha)) = (f_1(\alpha), \ldots, f_m(\alpha))$$

e quindi $\varphi = (f_1, \ldots, f_m)_{X \longrightarrow Y} \in \mathcal{O}(X, Y)$.

Osservazione 23.17. Vediamo in questo modo un primo esempio (quasi ovvio, ma fondamentale) di come mediante lo studio della K-algebra $\mathcal{O}(X)$ si possano descrivere proprietà dell'insieme algebrico X: Un'applicazione $\varphi : X \longrightarrow Y$ è polinomiale se e solo se per ogni $\eta \in \mathcal{O}(Y)$ la composizione $\eta \circ \varphi$ appartiene a $\mathcal{O}(X)$.

Questa condizione verrà, adeguatamente riformulata, presa come base per definire morfismi tra varietà algebriche nel caso generale.

Osservazione 23.18. Introduciamo adesso una notazione che rende ancora più concreto il significato dell'algebra $\mathcal{O}(X)$ e della prop. 22.20.

Definizione 23.19. Per $X \subset K^n$ ed $i = 1, \ldots, n$ sia $\pi_i^X := (x_i)_{X \longrightarrow K}$. Come già osservato nella nota 23.13, la funzione π_i^X è semplicemente la proiezione sull'i-esima coordinata (e in un linguaggio astratto essa stessa è chiamata i-esima *coordinata*).

Nota 23.20. Siano $X \subset K^n$ e $\theta_1, \ldots, \theta_m \in \mathcal{O}(X)$. Per $g \in K[m]$ possiamo allora formare la funzione $g(\theta_1, \ldots, \theta_m) \in \mathcal{O}(X)$ calcolata come in 8.2: Infatti g può essere scritto in modo univoco nella forma

$$g = \sum_{(k_1,\ldots,k_m)\in\mathbb{N}^m} a_{k_1\ldots k_m} x_1^{k_1} \cdots x_m^{k_m}$$

con i coefficienti $a_{k_1\ldots k_m} \in K$, cosicché

$$g(\theta_1, \ldots, \theta_m) = \sum_{(k_1,\ldots,k_m)\in\mathbb{N}^m} a_{k_1\ldots k_m} \theta_1^{k_1} \cdots \theta_m^{k_m}$$

Da questa rappresentazione è immediato che per $\alpha \in X$ si ha

$$(g(\theta_1, \ldots, \theta_m))(\alpha) = g(\theta_1(\alpha), \ldots, \theta_m(\alpha))$$

Proposizione 23.21. *Siano $X \subset K^n$ ed $f \in K[n]$. Allora*

$$f_{X\longrightarrow K} = f(\pi_1^X, \ldots, \pi_n^X)$$

Dimostrazione. Per $\alpha \in X$ abbiamo

$$f_{X\longrightarrow K}(\alpha) = f(\alpha_1, \ldots, \alpha_n) = f(\pi_1^X(\alpha), \ldots, \pi_n^X(\alpha)) \overset{23.20}{=} (f(\pi_1^X, \ldots, \pi_n^X))(\alpha)$$

Osservazione 23.22. La prop. 23.21 esprime semplicemente il fatto ovvio che, se per esempio $f = 3x_1x_2x_3^2 + 2x_1x_3 + 5x_2 + 6$, allora (si osservi che $1_{\mathcal{O}(X)}$ è l'applicazione costante $\bigcirc_\alpha 1 : X \longrightarrow K$)

$$\begin{aligned} f_{X\longrightarrow K} &= 3\pi_1^X\pi_2^X(\pi_3^X)^2 + 2\pi_1^X\pi_3^X + 5\pi_2^X + 6 \cdot 1_{\mathcal{O}(X)} \\ &= \bigcirc_{(x,y,z)} 3xyz^2 + 2xz + 5y + 6 \end{aligned}$$

Essa ha però alcune importanti conseguenze, come vedremo adesso.

Nota 23.23. $\mathcal{O}(X) = K[\pi_1^X, \ldots, \pi_n^X]$.

Per questa ragione $\mathcal{O}(X)$ è detto anche anello (o algebra) delle coordinate di X (cfr. def. 23.19) o, più correttamente, anello (o algebra) generato dalle coordinate di X.

24. La biiezione tra $\mathcal{O}(\mathbf{X},\mathbf{Y})$ e $\mathrm{Hom}_{\mathbf{K}\text{-algebre}}(\mathcal{O}(\mathbf{Y}),\mathcal{O}(\mathbf{X}))$

Per ogni $\varphi \in \mathcal{O}(X,Y)$ possiamo definire un omomorfismo $\varphi^{\mathcal{O}} := \bigcirc_{\eta} \eta \circ \varphi : \mathcal{O}(Y) \longrightarrow \mathcal{O}(X)$. Se $\varphi = (f_1,\ldots,f_m)_{X\longrightarrow Y}$, allora per $g \in K[m]$ si ha $\varphi^{\mathcal{O}}(g_{Y\longrightarrow K}) = (g(f_1,\ldots,f_m))_{X\longrightarrow K}$. Se B è una K-algebra commutativa ed $u : \mathcal{O}(Y) \longrightarrow B$ è un omomorfismo, allora u è univocamente determinato dai valori $u(\pi_1^Y),\ldots,u(\pi_m^Y)$ e per $g \in K[m]$ si ha $u(g_{Y\longrightarrow K}) = g(u(\pi_1^Y),\ldots,u(\pi_m^Y))$. Se Y è chiuso e se $u : \mathcal{O}(Y) \longrightarrow \mathcal{O}(X)$ è un omomorfismo, allora esiste, univocamente determinata, un'applicazione $\varphi \in \mathcal{O}(X,Y)$ tale che $u = \varphi^{\mathcal{O}}$. Per $\alpha \in X$ si ha $\varphi(\alpha) = (u(\pi_1^Y)(\alpha),\ldots,u(\pi_m^Y)(\alpha))$. In questa situazione poniamo $u_{X\longrightarrow Y} := \varphi$. Si ha quindi $(u_{X\longrightarrow Y})^{\mathcal{O}} = u$ e da ciò facilmente $(\varphi^{\mathcal{O}})_{X\longrightarrow Y} = \varphi$. Sempre nell'ipotesi che Y sia chiuso si ha una biiezione naturale $\mathcal{O}(X,Y) \longleftrightarrow \mathrm{Hom}_{K\text{-algebre}}(\mathcal{O}(Y),\mathcal{O}(X))$.

$u_{X\longrightarrow Y} = v_{X\longrightarrow Y}$ implica $u = v$. $(\psi\circ\varphi)^{\mathcal{O}} = \varphi^{\mathcal{O}} \circ \psi^{\mathcal{O}}$ e $(u\circ v)_{X\longrightarrow Z} = v_{Y\longrightarrow Z} \circ u_{X\longrightarrow Y}$. $\varphi : X \longrightarrow Y$ è un isomorfismo se e solo se $\varphi^{\mathcal{O}}$ è un isomorfismo di K-algebre. In particolare vediamo che gli insiemi X ed Y sono isomorfi se e solo se le K-algebre $\mathcal{O}(X)$ ed $\mathcal{O}(Y)$ sono isomorfe. Questi risultati possono essere immediatamente tradotti in risultati equivalenti per le K-algebre $\Gamma(X) = K[n]/\mathcal{J}(X)$. Se m è dispari, l'ideale generato da $y^2 - x^m$ in $K[x,y]$ è primo. L'applicazione $\bigcirc_{\alpha}(\alpha^2,\alpha^3) : K \longrightarrow (y^2 = x^3)$ è polinomiale e biiettiva, ma non è un isomorfismo.

Riformulazione in veste algebrica di alcune costruzioni viste nel capitolo.

Situazione 24.1. Sia K un campo.

Definizione 24.2. Siano $X \subset K^n, Y \subset K^m$ e $\varphi \in \mathcal{O}(X,Y)$. Allora otteniamo un'applicazione

$$\begin{aligned}\varphi^{\mathcal{O}} : \mathcal{O}(Y) &\longrightarrow \mathcal{O}(X)\\ \eta &\longmapsto \eta\circ\varphi\end{aligned}$$

ben definita per la prop. 22.20 ed è chiaro che si tratta di un omomorfismo di K-algebre.

Proposizione 24.3. *Siano $X \subset K^n, Y \subset K^m$ e $\varphi,\psi \in \mathcal{O}(X,Y)$ tali che $\varphi^{\mathcal{O}} = \psi^{\mathcal{O}}$. Allora $\varphi = \psi$.*

Dimostrazione. Ciò segue dal lemma 23.15.

Lemma 24.4. *Siano $X \subset K^n, Y \subset K^m$ e $\varphi = (\varphi_1,\ldots,\varphi_m) \in \mathcal{O}(X,Y)$. Per $i = 1,\ldots,m$ sia $\varphi_i = (f_i)_{X\longrightarrow K}$ con $f_i \in K[n]$. Sia $g \in K[m]$. Allora*

$$\varphi^{\mathcal{O}}(g_{Y\longrightarrow K}) \overset{25.2}{=} g_{Y\longrightarrow K}\circ\varphi = g(\varphi_1,\ldots,\varphi_m) = (g(f_1,\ldots,f_m))_{X\longrightarrow K}$$

Dimostrazione. Infatti (come nella dimostrazione della prop. 22.20) per $\alpha \in X$ abbiamo

$$g_{Y\longrightarrow K}(\varphi(\alpha)) = g(\varphi_1(\alpha),\ldots,\varphi_m(\alpha)) \overset{23.20}{=} (g(\varphi_1,\ldots,\varphi_m))(\alpha)$$

e anche

$$\begin{aligned}g_{Y\longrightarrow K}(\varphi(\alpha)) = g(\varphi_1(\alpha),\ldots,\varphi_m(\alpha)) &= g(f_1(\alpha),\ldots,f_m(\alpha))\\ &\overset{22.4}{=} (g(f_1,\ldots,f_m))(\alpha)\end{aligned}$$

La seconda parte è in verità un caso speciale della prop. 22.20.

Osservazione 24.5. Siano $X \subset K^n, Y \subset K^m$ e $\varphi = (\varphi_1, \ldots, \varphi_m) \in \mathcal{O}(X,Y)$. Per ogni $i = 1, \ldots, m$ allora

$$\varphi^{\mathcal{O}}(\pi_i^Y) = \varphi_i$$

Notiamo che se $\varphi_i = (f_i)_{X \longrightarrow K}$ con $f_i \in K[n]$, allora $\varphi_i = f_i(\pi_1^X, \ldots, \pi_n^X)$ per la prop. 23.21.

Dimostrazione. Infatti $\varphi^{\mathcal{O}}(\pi_i^Y) = \pi_i^Y \circ \varphi = \varphi_i$.

Lemma 24.6. *Siano B una K-algebra commutativa, $Y \subset K^m$ ed $u : \mathcal{O}(Y) \longrightarrow B$ un omomorfismo di K-algebre.*

Allora u è univocamente determinato dai valori $u(\pi_1^Y), \ldots, u(\pi_m^Y)$. Infatti per $g \in K[m]$ si ha

$$u(g_{Y \longrightarrow K}) = g(u(\pi_1^Y), \ldots, u(\pi_m^Y))$$

Dimostrazione. Usando l'ipotesi che u sia un omomorfismo di K-algebre dalla prop. 23.21 otteniamo

$$u(g_{Y \longrightarrow K}) = u(g(\pi_1^Y, \ldots, \pi_m^Y)) = g(u(\pi_1^Y), \ldots, u(\pi_m^Y))$$

Se ad esempio $g = x_1x_2 + 4x_3^2 + 5$, allora

$$\begin{aligned} u(g_{Y \longrightarrow K}) &= u(\pi_1^Y \pi_2^Y + 4(\pi_3^Y)^2 + 5 \cdot 1_{\mathcal{O}(Y)}) \\ &= u(\pi_1^Y)u(\pi_2^Y) + 4(u(\pi_3^Y))^2 + 5 \cdot 1_B = g(u(\pi_1^Y), u(\pi_2^Y), u(\pi_3^Y)) \end{aligned}$$

Proposizione 24.7. *Siano $X \subset K^n, Y \subset K^m$ ed $u : \mathcal{O}(Y) \longrightarrow \mathcal{O}(X)$ un omomorfismo di K-algebre. Y sia chiuso in K^m.*

Per ogni $i = 1, \ldots, m$ abbiamo allora $u(\pi_i^Y) \in \mathcal{O}(X)$, per cui possiamo scegliere $f_i \in K[n]$ in modo tale che $u(\pi_i^Y) = (f_i)_{X \longrightarrow K}$. Allora:

(1) Per ogni $\alpha \in X$ si ha $f_1(\alpha), \ldots, f_m(\alpha)) \in Y$.

(2) Perciò è definita l'applicazione $\varphi := (f_1, \ldots, f_m)_{X \longrightarrow Y} \in \mathcal{O}(X,Y)$.

(3) $u = \varphi^{\mathcal{O}}$.

Dimostrazione. (1) Sia $\alpha \in X$. Siccome Y è chiuso, per dimostrare che $(f_1(\alpha), \ldots, f_m(\alpha)) \in X$ è sufficiente dimostrare che $g(f_1(\alpha), \ldots, f_m(\alpha)) = 0$ per ogni $g \in \mathcal{J}(Y)$.

Per $i = 1, \ldots, m$ poniamo $\theta_i := (f_i)_{X \longrightarrow K} \in \mathcal{O}(X)$.

Per $g \in K[m]$ abbiamo adesso $g_{Y \longrightarrow K} = 0$ e perciò

$$\begin{aligned} g(f_1(\alpha), \ldots, f_m(\alpha)) &= g(\theta_1(\alpha), \ldots, \theta_m(\alpha)) \overset{23.20}{=} (g(\theta_1, \ldots, \theta_m))(\alpha) \\ &= g(u(\pi_1^Y), \ldots, u(\pi_m^Y))(\alpha) \overset{24.6}{=} u(g_{Y \longrightarrow K})(\alpha) = u(0)(\alpha) = 0(\alpha) = 0 \end{aligned}$$

(2) Non necessita di dimostrazione.

(3) Per il lemma 24.6 è sufficiente dimostrare che $\theta_i = \varphi^{\mathcal{O}}(\pi_i^Y)$ per ogni $i = 1, \ldots, m$.

Ma per ogni i abbiamo $\varphi^{\mathcal{O}}(\pi_i^Y) = \pi_i^Y \circ \varphi = (f_i)_{X \longrightarrow K} = \theta_i$.

Teorema 24.8. *Siano $X \subset K^n, Y \subset K^m$ ed Y chiuso. Sia $u : \mathcal{O}(Y) \longrightarrow \mathcal{O}(X)$ un omomorfismo di K-algebre.*

Allora esiste un'applicazione $\varphi \in \mathcal{O}(X, Y)$, univocamente determinata, tale che $u = \varphi^{\mathcal{O}}$.

Per $\alpha \in X$ si ha $\varphi(\alpha) = (u(\pi_1^Y)(\alpha), \ldots, u(\pi_m^Y)(\alpha))$.

Dimostrazione. Esistenza e unicità di φ seguono dalle prop. 24.7 e 24.3.

Definizione 24.9. Nella situazione del teorema 24.8 poniamo $u_{X \longrightarrow Y} := \varphi$.

Per definizione abbiamo quindi $\quad (u_{X \longrightarrow Y})^{\mathcal{O}} = u$.

Osservazione 24.10. Siano U e V insiemi e $\sigma : U \longrightarrow V$, $\tau : V \longrightarrow U$ due applicazioni tali che $\tau\sigma = \mathrm{id}_U$. La τ sia iniettiva.

Allora τ è biiettiva e si ha $\sigma = \tau^{-1}$.

Dimostrazione. Infatti dalla relazione $\tau\sigma = \mathrm{id}_U$ segue che τ è suriettiva.

Corollario 24.11. *Siano $X \subset K^n, Y \subset K^m$ ed Y chiuso. Sia $\varphi \in \mathcal{O}(X, Y)$.*

Allora $(\varphi^{\mathcal{O}})_{X \longrightarrow Y} = \varphi$.

Dimostrazione. (1) Sia $\psi := (\varphi^{\mathcal{O}})_{X \longrightarrow Y}$. Allora

$$\psi^{\mathcal{O}} = ((\varphi^{\mathcal{O}})_{X \longrightarrow Y})^{\mathcal{O}} \overset{24.9}{=} \varphi^{\mathcal{O}}$$

e dalla prop. 24.3 segue $\varphi = \psi$.

(2) Il corollario può essere anche considerato come una conseguenza dell'oss. 24.10.

Infatti con $U := \mathrm{Hom}_{K\text{-algebre}}(\mathcal{O}(Y), \mathcal{O}(X))$, $V := \mathcal{O}(X, Y)$, $\sigma := \bigcirc\!\!\!\!\!\!\int_u u_{X \longrightarrow Y}$, $\tau := \bigcirc\!\!\!\!\!\!\int_\varphi \varphi^{\mathcal{O}}$ con la def. 24.9 abbiamo $\tau\sigma = \mathrm{id}_U$, mentre dalla prop. 24.3 sappiamo che l'applicazione τ è iniettiva.

L'oss. 24.10 implica che τ è biiettiva e $\sigma = \tau^{-1}$.

Corollario 24.12. *Siano $X \subset K^n, Y \subset K^m$ ed Y chiuso. Allora esiste una biiezione*

$$\begin{aligned} \mathcal{O}(X, Y) &\longrightarrow \mathrm{Hom}_{K\text{-algebre}}(\mathcal{O}(Y), \mathcal{O}(X)) \\ \varphi &\longmapsto \varphi^{\mathcal{O}} \\ u_{X \longrightarrow Y} &\longmapsfrom u \end{aligned}$$

Più esplicitamente le biiezioni possono essere scritte nella forma

$$\begin{aligned} \varphi &\longmapsto \bigcirc\!\!\!\!\!\!\int_\eta \eta \circ \varphi \\ \bigcirc\!\!\!\!\!\!\int_\alpha (u(\pi_1^Y)(\alpha), \ldots, u(\pi_m^Y)(\alpha)) &\longmapsfrom u \end{aligned}$$

Corollario 24.13. *Se nelle ipotesi del cor. 24.12 u e v sono omomorfismi di K-algebre $\mathcal{O}(Y) \longrightarrow \mathcal{O}(X)$ tali che $u_{X \longrightarrow Y} = v_{X \longrightarrow Y}$, allora $u = v$.*

Proposizione 24.14. *Siano $X \subset K^n$, $Y \subset K^m$, $Z \subset K^p$ e $\varphi \in \mathcal{O}(X,Y)$, $\psi \in \mathcal{O}(Y,Z)$. Allora*

$$(\psi \circ \varphi)^{\mathcal{O}} = \varphi^{\mathcal{O}} \circ \psi^{\mathcal{O}}$$

Dimostrazione. Dalla prop. 22.20 sappiamo che $\psi \circ \varphi \in \mathcal{O}(X,Z)$.
Per $\zeta \in \mathcal{O}(Z)$ abbiamo

$$(\psi \circ \varphi)^{\mathcal{O}}(\zeta) = \zeta \circ \psi \circ \varphi = \varphi^{\mathcal{O}}(\zeta \circ \psi) = \varphi^{\mathcal{O}}(\psi^{\mathcal{O}}(\zeta))$$

Osservazione 24.15. Sia $X \subset K^n$. Allora:

(1) $\mathrm{id}_X \in \mathcal{O}(X,X)$.

(2) $\mathrm{id}_X^{\mathcal{O}} = \mathrm{id}_{\mathcal{O}(X)}$.

(3) Se X è chiuso, allora $(\mathrm{id}_{\mathcal{O}(X)})_{X \longrightarrow X} = \mathrm{id}_X$.

Proposizione 24.16. *Siano $X \subset K^n$, $Y \subset K^m$, $Z \subset K^p$ ed Y, Z chiusi.*

Siano $u : \mathcal{O}(Y) \longrightarrow \mathcal{O}(X)$ e $v : \mathcal{O}(Z) \longrightarrow \mathcal{O}(Y)$ omomorfismi di K-algebre. Allora

$$(u \circ v)_{X \longrightarrow Z} = v_{Y \longrightarrow Z} \circ u_{X \longrightarrow Y}$$

Dimostrazione. Usando le formule nella def. 24.9 e nel cor. 24.11 abbiamo

$$\begin{aligned}(u \circ v)_{X \longrightarrow Z} &= ((u_{X \longrightarrow Y})^{\mathcal{O}} \circ (v_{Y \longrightarrow Z})^{\mathcal{O}})_{X \longrightarrow Z} \\ &\overset{24.14}{=} ((v_{Y \longrightarrow Z} \circ u_{X \longrightarrow Y})^{\mathcal{O}})_{X \longrightarrow Z} = v_{Y \longrightarrow Z} \circ u_{X \longrightarrow Y}\end{aligned}$$

Definizione 24.17. Siano $X \subset K^n$ ed $Y \subset K^m$. Un *isomorfismo* da X in Y è un'applicazione $\varphi : X \longrightarrow Y$ che soddisfa le seguenti condizioni:

(1) $\varphi \in \mathcal{O}(X,Y)$.

(2) φ è biiettiva.

(3) $\varphi^{-1} \in \mathcal{O}(Y,X)$.

Se esiste un isomorfismo da X in Y, allora diciamo che gli insiemi X ed Y sono *isomorfi* e scriviamo $X \cong Y$. È chiaro che questa relazione è riflessiva, simmetrica e transitiva.

Applicheremo anche questa definizione quasi sempre nel caso che X ed Y siano insiemi algebrici.

Proposizione 24.18. *Siano $X \subset K^n$ ed $Y \subset K^m$ insiemi algebrici. Allora:*

(1) Se $\varphi : X \longrightarrow Y$ è un isomorfismo, allora $\varphi^{\mathcal{O}} : \mathcal{O}(Y) \longrightarrow \mathcal{O}(X)$ è un isomorfismo di K-algebre.

(2) Se invece $u : \mathcal{O}(Y) \longrightarrow \mathcal{O}(X)$ è un isomorfismo di K-algebre, allora $u_{X \longrightarrow Y} : X \longrightarrow Y$ è un isomorfismo.

(3) In particolare vediamo che X ed Y sono isomorfi se e solo se le K-algebre $\mathcal{O}(X)$ e $\mathcal{O}(Y)$ sono isomorfe.

Dimostrazione. (1) Sia $\psi := \varphi^{-1}$. Allora $\varphi \circ \psi = \mathrm{id}_Y$ e $\psi \circ \varphi = \mathrm{id}_X$ e quindi, per le oss. 24.14 e 24.15,

$$\psi^{\mathcal{O}} \circ \varphi^{\mathcal{O}} = \mathrm{id}_Y^{\mathcal{O}} = \mathrm{id}_{\mathcal{O}(Y)}$$
$$\varphi^{\mathcal{O}} \circ \psi^{\mathcal{O}} = \mathrm{id}_X^{\mathcal{O}} = \mathrm{id}_{\mathcal{O}(X)}$$

(2) Sia $v = u^{-1}$. Allora $v \circ u = \mathrm{id}_{\mathcal{O}(Y)}$ e $u \circ v = \mathrm{id}_{\mathcal{O}(X)}$ e quindi, per le oss. 24.16 e 24.15,

$$u_{X \longrightarrow Y} \circ v_{Y \longrightarrow X} = (\mathrm{id}_{\mathcal{O}(Y)})_{Y \longrightarrow Y} = \mathrm{id}_Y$$
$$v_{Y \longrightarrow X} \circ u_{X \longrightarrow Y} = (\mathrm{id}_{\mathcal{O}(X)})_{X \longrightarrow X} = \mathrm{id}_X$$

Proposizione 24.19. *Siano $X \subset K^n, Y \subset K^m$ ed $u : \mathcal{O}(Y) \longrightarrow \mathcal{O}(X)$ un omomorfismo di K-algebre. Allora possiamo definire un omomorfismo di K-algebre $u^{\Gamma(Y) \longrightarrow \Gamma(X)} : \Gamma(Y) \longrightarrow \Gamma(X)$ tramite il diagramma commutativo*

$$\begin{array}{ccc} \mathcal{O}(Y) & \xrightarrow{\quad u \quad} & \mathcal{O}(X) \\ {\scriptstyle \bigcirc}_{g+\mathcal{J}(Y)} \; g_{Y \longrightarrow K} \uparrow & & \downarrow {\scriptstyle \bigcirc}_{h_{X \longrightarrow K}} \; h+\mathcal{J}(X) \\ \Gamma(Y) & \xrightarrow{u^{\Gamma(Y) \longrightarrow \Gamma(X)}} & \Gamma(X) \end{array}$$

Più esplicitamente, se per $i = 1, \ldots, m$ scegliamo $f_i \in K[n]$ in modo tale che $u(\pi_i^Y) = (f_i)_{X \longrightarrow K}$, allora per $g \in K[m]$ abbiamo

$$u^{\Gamma(Y) \longrightarrow \Gamma(X)}(g + \mathcal{J}(Y)) = g(f_1, \ldots, f_m) + \mathcal{J}(X)$$

Dimostrazione. (1) Le due frecce verticali sono ben definite e isomorfismi per la nota 23.10. Perciò anche l'omomorfismo $u^{\Gamma(Y) \longrightarrow \Gamma(X)}$ è ben definito.

(2) Per $g \in K[m]$ abbiamo

$$\begin{aligned} u(g + \mathcal{J}(Y)) = u(g_{Y \longrightarrow K}) &\overset{24.6}{=} g((f_1)_{X \longrightarrow K}, \ldots, (f_m)_{X \longrightarrow K}) \\ &\overset{24.4}{=} (g(f_1, \ldots, f_m))_{X \longrightarrow K} \end{aligned}$$

Applicando la seconda freccia verticale si ottiene l'enunciato.

Definizione 24.20. Siano $X \subset K^n, Y \subset K^m$ e $\varphi \in \mathcal{O}(X, Y)$. Allora poniamo

$$\varphi^{\Gamma} := (\varphi^{\mathcal{O}})^{\Gamma(Y) \longrightarrow \Gamma(X)}$$

Se $\varphi = (f_1, \ldots, f_m)_{X \longrightarrow K}$ con $f_1, \ldots, f_m \in K[n]$, allora per $g \in K[m]$ si ha

$$\varphi^{\Gamma}(g + \mathcal{J}(Y)) = g(f_1, \ldots, f_m) + \mathcal{J}(X)$$

Osservazione 24.21. Tramite la prop. 24.19 tutti i risultati ottenuti in questo capitolo per $\mathcal{O}(X)$ ed $\mathcal{O}(Y)$ possono essere tradotti in enunciati equivalenti per $\Gamma(X)$ e $\Gamma(Y)$.

Osservazione 24.22. Siano A un anello integro ed $f \in A \setminus 0$.

(1) Se l'ideale Af è primo, allora f è irriducibile.

(2) Se A è un dominio a fattorizzazione unica (come $K[n]$) ed f è irriducibile, allora l'ideale Af è primo.

Dimostrazione. Facile, ad esempio Dummit/Foote [16966], p. 284 e 286.

Nota 24.23. Per ogni $m \in 2\mathbb{N}+1$ l'ideale generato da $x_2^2 - x_1^m$ in $K[2]$ è primo.

Dimostrazione. Lavoriamo con le variabili x ed y invece di x_1 e x_2. Per l'oss. 24.22 è sufficiente dimostrare che il polinomio $y^2 - x^m$ è irriducibile in $K[x, y]$.

Siano $g, h \in K[x, y]$ tali che $gh = y^2 - x^m$.

Il grado in y di g ed h deve essere ≤ 2 (perché l'anello $K[x]$ è integro), perciò possiamo scrivere

$$g = A + By + Cy^2$$
$$h = D + Ey + Fy^2$$

con $A, \ldots, F \in K[x]$.

(1) Sia $C \neq 0$. Allora necessariamente $E = F = 0$ e quindi

$$y^2 - x^m = AD + BDy + CDy^2$$

Ciò implica $AD = -x^m$, $BD = 0$, $CD = 1$, per cui D è una costante $\neq 0$, cosicché $g = -x^m/D + y^2/D = (y^2 - x^m)/D$, $h = D \in K$. La fattorizzazione $y^2 - x^m = gh$ è perciò banale.

(2) Sia $F \neq 0$. Allora ragioniamo come nel caso (1).

(3) Sia $C = F = 0$. Allora $gh = AD + (AE + BD)y + BEy^2$.

Perciò $AD = -x^m$, $AE + BD = 0$ e $BE = 1$.

Allora B ed E sono costanti $\neq 0$ e ciò implica che A e D possiedono (rispetto ad x) lo stesso grado. Ma ciò non è possibile, perché per ipotesi il grado di $AD = -x^m$ è dispari.

Esempio 24.24. Sia P l'ideale generato da $x_2^2 - x_1^3$ in $K[2]$. Il campo K sia algebricamente chiuso (e quindi infinito). Per la nota 24.23 l'ideale P è primo e quindi radicale.

Se poniamo $Y := \mathrm{Zeri}(P)$, allora per il teorema degli zeri $\mathcal{J}(Y) = P$.

Perciò $\Gamma(Y) = K[2]/P$. Siccome K è infinito, invece $\mathcal{J}(K) = 0$, cosicché $\Gamma(K) = K[1]$.

Consideriamo l'applicazione

$$\begin{aligned} \varphi : K &\longrightarrow Y \\ \alpha &\longmapsto (\alpha^2, \alpha^3) \end{aligned}$$

Siccome $(\alpha^3)^2 - (\alpha^2)^3 = 0$, questa applicazione è ben definita ed ovviamente polinomiale, infatti $\varphi = (x_1^2, x_2^3)_{K \longrightarrow Y}$.

φ è per definizione suriettiva, ma è anche iniettiva, perché possiede l'inversa $\psi : Y \longrightarrow K$ data da $\psi(0, 0) := 0$ e $\psi(s, t) := t/s$ per $s \neq 0$.

φ non è però un isomorfismo.

Per dimostrare ciò consideriamo l'omomorfismo $u := \varphi^\Gamma$. Dalla formula esplicita nella def. 24.20 abbiamo

$$u(g + P) = g(x_1^2, x_1^3) \quad \text{per ogni } g \in K[2]$$

ed è chiaro che ciò implica che l'elemento x_1 di $\Gamma(K) = K[x_1]$ non appartiene all'immagine di u, per cui u non è suriettivo.

Dalla prop. 24.18 segue che φ non è un isomorfismo.

Ciò è in accordo con quanto si intuisce dalla forma dell'inversa $\varphi^{-1} = \psi$ che evidentemente non è un'applicazione polinomiale.

Osservazione 24.25. Nell'ultima parte del capitolo facciamo vedere brevemente come gli omomorfismi $\Gamma(Y) \longrightarrow \Gamma(X)$ si possano ottenere direttamente in modo algebrico senza passare attraverso gli omomorfismi $\mathcal{O}(Y) \longrightarrow \mathcal{O}(X)$. Naturalmente si tratta soltanto di una riformulazione di quanto già visto.

Proposizione 24.26. *Siano B una K-algebra commutativa ed $f_1, \ldots, f_m \in B$ scelti in modo arbitrario.*

Allora esiste un unico omomorfismo di K-algebre $u : K[m] \longrightarrow B$ tale che $u(x_i) = f_i$ per ogni $i = 1, \ldots, m$ e si ha $u(g) = g(f_1, \ldots, f_m)$ per ogni $g \in K[m]$.

Dimostrazione. Sia $g \in K[m]$. Allora (come nella nota 8.2) possiamo scrivere g in modo unico nella forma $g = \sum_{(k_1,\ldots,k_m)\in\mathbb{N}^m} a_{k_1\ldots k_m} x_1^{k_1} \cdots x_m^{k_m}$ con i coefficienti $a_{k_1\ldots k_m} \in K$.

Se $u : K[m] \longrightarrow B$ è un omomorfismo di K-algebre con $u(x_i) = f_i$ per ogni i, allora necessariamente

$$\begin{aligned} u(g) &= \sum_{(k_1,\ldots,k_m)\in\mathbb{N}^m} a_{k_1\ldots k_m} u(x_1^{k_1}) \cdots u(x_m^{k_m}) \\ &= \sum_{(k_1,\ldots,k_m)\in\mathbb{N}^m} a_{k_1\ldots k_m} f_1^{k_1} \cdots f_m^{k_m} = g(f_1, \ldots, f_m) \end{aligned}$$

Si verifica facilmente che definendo u in questo modo si ottiene veramente un omomorfismo di K-algebre. Cfr. lemma 24.6.

Osservazione 24.27. Nella prop. 24.26 l'espressione $g(f_1, \ldots, f_m)$ è calcolata come nella def. 4.8.

Nel caso $B = K[n]$ si ottiene lo stesso risultato come nell'oss. 22.3.

Proposizione 24.28. *(1) Siano $f_1, \ldots, f_m \in K[n]$ ed $u := (f_1, \ldots, f_m)^{K[m]\longrightarrow K[n]}$. Per ogni $i = 1, \ldots m$ allora $u(x_i) = f_i$.*

(2) Sia viceversa $u : K[m] \longrightarrow K[n]$ un omomorfismo di K-algebre. Se per $i = 1, \ldots, m$ poniamo $f_i := u(x_i)$, allora $u = (f_1, \ldots, f_m)^{K[m]\longrightarrow K[n]}$.

Dimostrazione. (1) Conseguenza immediata della definizione (cfr. def. 22.9).

(2) Ciò segue dalla prop. 24.26.

Lemma 24.29. *Siano I un ideale di $K[n]$, J un ideale di $K[m]$ ed $u : K[m]/J \longrightarrow K[n]/I$ un omomorfismo di K-algebre.*

Per ogni $i = 1, \ldots, m$ scegliamo un polinomio $f_i \in K[n]$ tale che $u(x_i + J) = f_i + I$. Allora con $v := (f_1, \ldots, f_m)^{K[m]\longrightarrow K[n]}$ otteniamo un diagramma commutativo

$$\begin{array}{ccc} K[m] & \xrightarrow{v} & K[n] \\ \downarrow{\scriptstyle \pi_J} & & \downarrow{\scriptstyle \pi_I} \\ K[m]/J & \xrightarrow{u} & K[n]/I \end{array}$$

in cui con π_I e π_J abbiamo denotato le proiezioni canoniche. Per ogni $g \in K[m]$ abbiamo quindi $u(g + J) = g(f_1, \ldots, f_m) + I$.

Dimostrazione. Il diagramma esprime semplicemente il modo in cui abbiamo scelto v. Per $i = 1, \ldots, m$ abbiamo

$$\pi_I(v(x_i)) = \pi_I(f_i) = f_i + I = u(x_i + J) = u(\pi_J(x_i))$$

Dalla prop. 24.26 segue che $\pi_I \circ v = u \circ \pi_J$.

Corollario 24.30. *Siano $X \subset K^n$ e $Y \subset K^m$ ed $u : \Gamma(Y) \longrightarrow \Gamma(X)$ un omomorfismo di K-algebre.*

Per ogni $i = 1, \ldots, m$ scegliamo un polinomio $f_i \in K[n]$ tale che $u(x_i + \mathcal{J}(Y)) = f_i + \mathcal{J}(X)$. Allora per ogni $g \in K[m]$ abbiamo

$$u(g + \mathcal{J}(Y)) = g(f_1, \ldots, f_m) + \mathcal{J}(X)$$

25. Proprietà intrinseche di applicazioni polinomiali

Se K è algebricamente chiuso ed $X \subset K^n$ è algebrico, allora esiste una biiezione $X \longleftrightarrow \operatorname{Max}\Gamma(X)$ e quindi anche una biiezione $X \longleftrightarrow \operatorname{Max}\mathcal{O}(X)$. $\mathcal{J}(\alpha, \operatorname{in}\mathcal{O}(X)) := \{\theta \in \mathcal{O}(X) \mid \theta(\alpha) = 0\}$. Per $\varphi \in \mathcal{O}(X,Y)$ abbiamo allora $\mathcal{J}(\varphi(\alpha), \operatorname{in}\mathcal{O}(Y)) = (\varphi^{\mathcal{O}})^{-1}(\mathcal{J}(\alpha, \operatorname{in}\mathcal{O}(X)))$. Per $Y \subset X$ sia $\mathcal{J}(Y, \operatorname{in}\mathcal{O}(X)) := \{\theta \in \mathcal{O}(X) \mid \theta_{|Y} = 0\} = \{f_{X \longrightarrow K} \mid f \in \mathcal{J}(Y)\}$. Se K è algebricamente chiuso, allora si ha una biiezione tra i chiusi di X e gli ideali generalizzati radicali di $\mathcal{O}(X)$. Per $Y \subset X \subset K^n$ esiste un isomorfismo naturale $\mathcal{O}(Y) \cong \mathcal{O}(X)/\mathcal{J}(Y, \operatorname{in}\mathcal{O}(X))$. Notazione generale $f_{A \longrightarrow B}$. Gli insiemi della forma $(\theta \neq 0)$ per $\theta \in \mathcal{O}(X)$ formano una base per gli aperti di X. $\varphi : X \longrightarrow Y$ è detta densa (o dominante), se $\overline{\varphi(X)} = Y$. $\varphi \in \mathcal{O}(X,Y)$ è densa se e solo se $\varphi^{\mathcal{O}}$ è iniettivo. $\operatorname{Ker}\varphi^{\mathcal{O}} = \mathcal{J}(\varphi(X), \operatorname{in}\mathcal{O}(Y))$. Se $\varphi \in \mathcal{O}(X,Y)$ e B è un chiuso di Y, allora $\varphi^{-1}(B) = \operatorname{Zeri}(\varphi^{\mathcal{O}}(\mathcal{J}(B, \operatorname{in}\mathcal{O}(Y))))$. $\varphi \in \mathcal{O}(X,Y)$ si chiama un'immersione chiusa, se $\varphi(X)$ è chiuso in Y e l'applicazione $\varphi_{X \longrightarrow \varphi(X)}$ è un isomorfismo. Assumiamo che K sia algebricamente chiuso e che gli insiemi $X \subset K^n$ e $Y \subset K^m$ siano algebrici. Allora $\varphi^{\mathcal{O}}$ è suriettivo se e solo se φ è un'immersione chiusa.

Situazione 25.1. Sia K un campo.

Teorema 25.2. *Siano K algebricamente chiuso e X un sottoinsieme algebrico di K^n.*

(1) Dalla prop. 14.33 otteniamo una biiezione naturale

$$\begin{array}{rcl} X & \longleftrightarrow & \operatorname{Max}\Gamma(X) \\ \alpha & \longmapsto & \mathfrak{m}_\alpha/\mathcal{J}(X) \\ \operatorname{Zeri}(\pi^{-1}(\mathfrak{n})) & \longleftarrow\!\shortmid & \mathfrak{n} \end{array}$$

dove $\pi : K[n] \longrightarrow \Gamma(X)$ è la proiezione naturale.

(2) Per $\alpha \in X$ e $f \in K[n]$ si ha

$$f + \mathcal{J}(X) \in \mathfrak{m}_\alpha/\mathcal{J}(X) \iff f(\alpha) = 0$$

Dimostrazione. (1) Ciò è una conseguenza immediata della prop. 14.33, usando la biiezione naturale

$$\{\mathfrak{m} \in \operatorname{Max} K[n] \mid \mathfrak{m} \supset \mathcal{J}(X)\} \longleftrightarrow \operatorname{Max}\Gamma(X)$$

(2) Per $\alpha \in X$ si ha $\mathcal{J}(X) \subset \mathfrak{m}_\alpha$ e quindi

$$f + \mathcal{J}(X) \in \mathfrak{m}_\alpha/\mathcal{J}(X) \iff f \in \mathfrak{m}_\alpha \iff f(\alpha) = 0$$

Corollario 25.3. *Siano K algebricamente chiuso e X un sottoinsieme algebrico di K^n. Allora la biiezione del teorema 25.2 si traduce in una biiezione naturale*

$$\begin{array}{rcl} X & \longleftrightarrow & \operatorname{Max}\mathcal{O}(X) \\ \alpha & \longmapsto & \{\theta \in \mathcal{O}(X) \mid \theta(\alpha) = 0\} \end{array}$$

Dimostrazione. Ciò segue dall'isomorfismo $\mathcal{O}(X) \cong K[n]/\mathcal{J}(X)$ e dal teorema 25.2.

Definizione 25.4. Sia $X \subset K^n$.

(1) Per $\alpha \in X$ poniamo $\mathcal{J}(\alpha, \operatorname{in}\mathcal{O}(X)) := \{\theta \in \mathcal{O}(X) \mid \theta(\alpha) = 0\}$.

Se K è algebricamente chiuso e X è un sottoinsieme algebrico di K^n, otteniamo quindi una biiezione $X \longleftrightarrow \operatorname{Max}\mathcal{O}(X)$ data da $\alpha \longmapsto \mathcal{J}(\alpha, \operatorname{in}\mathcal{O}(X))$.

(2) Per $\mathfrak{n} \in \operatorname{Max}\Gamma(X)$ poniamo

$$(\mathfrak{n}, \operatorname{in}\mathcal{O}(X)) := \{f_{X\longrightarrow K} \mid f \in K[n] \text{ e } f + \mathcal{J}(X) \in \mathfrak{n}\}$$

Per $X \subset K^n$ ed $\alpha \in X$ abbiamo

$$\mathcal{J}(\alpha, \operatorname{in}\mathcal{O}(X)) = (\mathfrak{m}_\alpha/\mathcal{J}(X), \operatorname{in}\mathcal{O}(X)) = \mathcal{O}(X)_\smile(\pi_1^X - \alpha_1, \ldots, \pi_n^X - \alpha_n)$$

Proposizione 25.5. *Siano $X \subset K^n$, $Y \subset K^m$. Assumiamo che $\varphi \in \mathcal{O}(X, Y)$ e $\alpha \in X$. Allora:*

(1) $\mathcal{J}(\varphi(\alpha), \operatorname{in}\mathcal{O}(Y)) = (\varphi^{\mathcal{O}})^{-1}(\mathcal{J}(\alpha, \operatorname{in}\mathcal{O}(X)))$.

(2) $\mathfrak{m}_{\varphi(\alpha)}/\mathcal{J}(Y) = (\varphi^{\Gamma})^{-1}(\mathfrak{m}_\alpha/\mathcal{J}(X))$.

Dimostrazione. (1) Per $\eta \in \mathcal{O}(Y)$ sono equivalenti:

$\eta \in (\varphi^{\mathcal{O}})^{-1}(\mathcal{J}(\alpha, \operatorname{in}\mathcal{O}(X)))$.

$(\varphi^{\mathcal{O}})(\eta) \in \mathcal{J}(\alpha, \operatorname{in}\mathcal{O}(X))$.

$\eta \circ \varphi \in \mathcal{J}(\alpha, \operatorname{in}\mathcal{O}(X))$.

$\eta(\varphi(\alpha)) = 0$.

$\eta \in \mathcal{J}(\varphi(\alpha), \operatorname{in}\mathcal{O}(Y))$.

(2) Ciò segue da (1), usando le isomorfie $\mathcal{O}(X) \cong \Gamma(X)$ e $\mathcal{O}(Y) \cong \Gamma(Y)$.

L'enunciato può essere dimostrato anche in modo diretto:

Sia $g \in K[n]$. Allora, supponendo che $\varphi = (f_1, \ldots, f_m)_{X\longrightarrow Y}$, le seguenti affermazioni sono equivalenti:

$g + \mathcal{J}(Y) \in (\varphi^{\Gamma})^{-1}(\mathfrak{m}_\alpha/\mathcal{J}(X))$.

$g(f_1, \ldots, f_m) + \mathcal{J}(X) \in \mathfrak{m}_\alpha/\mathcal{J}(X)$.

$g(f_1, \ldots, f_m) \in \mathfrak{m}_\alpha$.

$g(f_1(\alpha), \ldots, f_m(\alpha)) = 0$.

$g(\varphi(\alpha)) = 0$.

$g \in \mathfrak{m}_{\varphi(\alpha)}$.

$g + \mathcal{J}(Y) \in \mathfrak{m}_{\varphi(\alpha)}/\mathcal{J}(Y)$.

Definizione 25.6. Sia $Y \subset X \subset K^n$. Generalizzando la def. 25.4 poniamo

$$\mathcal{J}(Y, \operatorname{in}\mathcal{O}(X)) := \{\theta \in \mathcal{O}(X) \mid \theta_{|Y} = 0\} = \{f_{X\longrightarrow K} \mid f \in \mathcal{J}(Y)\}$$

È chiaro che $\mathcal{J}(Y, \operatorname{in}\mathcal{O}(X))$ è un ideale generalizzato radicale di $\mathcal{O}(X)$ e un ideale se $Y \neq \emptyset$. D'altra parte $\mathcal{J}(X, \operatorname{in}\mathcal{O}(X)) = 0$.

Nota 25.7. Sia $X \subset K^n$.

(1) Per ogni ideale generalizzato I di $\mathcal{O}(X)$ l'insieme

$$\operatorname{Zeri}(I) = \{\alpha \in X \mid \theta(\alpha) = 0 \text{ per ogni } \theta \in I\}$$

è chiuso in X.

(2) Per $Y \subset X$ si ha $\overline{Y} \cap X = \operatorname{Zeri}(\mathcal{J}(Y, \operatorname{in}\mathcal{O}(X)))$.

(3) Se K è algebricamente chiuso e gli insiemi X and Y sono algebrici, allora le costruzioni nella def. 25.6 ed in (1) sono l'una inversa all'altra. Otteniamo così (in queste ipotesi più restrittive) una biiezione naturale

$$\begin{array}{rcl} \{\text{sottoinsiemi chiusi di } X\} & \longleftrightarrow & \{\text{ideali generalizzati radicali di } \mathcal{O}(X)\} \\ Y & \longmapsto & \mathcal{J}(Y, \text{in}\,\mathcal{O}(X)) \\ \text{Zeri}(I) & \longleftarrow\!\shortmid & I \end{array}$$

Dimostrazione. Facile, usando il cor. 14.19. Cfr. Bump [16216], p. 14.

Il punto (2) è una conseguenza diretta della prop. 14.27 e verrà dimostrato nel lemma 25.16.

Osservazione 25.8. Sia $Y \subset X \subset K^n$. Dalla def. 25.6 vediamo che nell'isomorfismo naturale

$$\begin{array}{rcl} \mathcal{O}(X) & \longrightarrow & \Gamma(X) = K[n]/\mathcal{J}(X) \\ f_{X \longrightarrow K} & \longmapsto & f + \mathcal{J}(X) \end{array}$$

della nota 23.10 gli elementi di $\mathcal{J}(Y, \text{in}\,\mathcal{O}(X))$ corrispondono biiettivamente agli elementi di $\mathcal{J}(Y)/\mathcal{J}(X)$:

$\mathcal{J}(Y, \text{in}\,\mathcal{O}(X)) \longleftrightarrow \mathcal{J}(Y)/\mathcal{J}(X)$

Ciò dà luogo ad isomorfismi naturali

$$\mathcal{O}(X)/\mathcal{J}(Y, \text{in}\,\mathcal{O}(X)) \cong \frac{K[n]/\mathcal{J}(X)}{\mathcal{J}(Y)/\mathcal{J}(X)} \cong K[n]/\mathcal{J}(Y) = \Gamma(Y) \cong \mathcal{O}(Y)$$

In particulare e più esplicitamente abbiamo un isomorfismo

$$\begin{array}{rcl} \mathcal{O}(X)/\mathcal{J}(Y, \text{in}\,\mathcal{O}(X)) & \longrightarrow & \mathcal{O}(Y) \\ f_{X \longrightarrow K} + \mathcal{J}(Y, \text{in}\,\mathcal{O}(X)) & \longmapsto & f_{Y \longrightarrow K} \end{array}$$

Definizione 25.9. Siano X, Y insiemi, $f : X \longrightarrow Y$ una funzione ed $A \subset X$, $B \subset Y$ tali che $f(A) \subset B$.

Allora possiamo definire l'applicazione $f_{A \longrightarrow B} := \bigcirc_a f(a) : A \longrightarrow B$.

Questa notazione è definita in un contesto diverso da quello delle def. 22.18 e 24.9 e non è in contrasto con esse.

In particulare è sempre definita l'applicazione $f_{X \longrightarrow f(X)}$. La restrizione $f_{|A}$ diventa $f_{A \longrightarrow Y}$.

Osservazione 25.10. Sia $X \subset K^n$. Allora gli insiemi $(f \neq 0) \cap X$ con $f \in K[n]$ formano una base per gli aperti di X.

Ciò significa che per ogni insieme $U \subset X$ che è aperto in X ed ogni $\alpha \in U$ esiste $f \in K[n]$ tale che $\alpha \in (f \neq 0) \cap X \subset U$.

Dimostrazione. Siano U aperto in X ed $\alpha \in U$. Allora esiste un aperto $W \subset K^n$ tale che $U = W \cap X$.

$K^n \setminus W$ è chiuso in K^n, quindi per la nota 1.18 esistono $f_1, \ldots, f_m \in K[n]$ tali che $K^n \setminus W = \text{Zeri}(f_1, \ldots, f_m)$.

L'ipotesi $\alpha \in U$ implica che per esempio $f_1(\alpha) \neq 0$; inoltre $\alpha \in X$.
Osservando che $(f_1 \neq 0) \subset W$ otteniamo $\alpha \in (f_1 \neq 0) \cap X \subset W \cap X = U$.

Osservazione 25.11. Sia $X \subset K^n$.

(1) Sia $f \in K[n]$. Con $\theta := f_{X \longrightarrow K} \in \mathcal{O}(X)$ abbiamo $(f \neq 0) \cap X = (\theta \neq 0)$.

(2) Sia $\theta \in \mathcal{O}(X)$. Allora esiste $f \in K[n]$ con $\theta = f_{X \longrightarrow K}$ e quindi ancora $(\theta \neq 0) = (f \neq 0) \cap X$.

Ciò mostra che gli insiemi della forma $(f \neq 0) \cap X$ con $f \in K[n]$ coincidono con gli insiemi della forma $(\theta \neq 0)$ con $\theta \in \mathcal{O}(X)$.

Corollario 25.12. *Sia $X \subset K^n$. Allora gli insiemi $(\theta \neq 0)$ con $\theta \in \mathcal{O}(X)$ formano una base per gli aperti di X.*

Definizione 25.13. Un'applicazione $\varphi : X \longrightarrow Y$ tra spazi topologici è detta *densa* (o, in geometria algebrica, *dominante*), se $\overline{\varphi(X)} = Y$.

Proposizione 25.14. *Siano $X \subset K^n, Y \subset K^m$ e $\varphi \in \mathcal{O}(X, Y)$. Allora sono equivalenti:*

(1) φ è densa.

(2) L'omomorfismo $\varphi^{\mathcal{O}}$ è iniettivo.

Dimostrazione. (1) $\implies$ (2): Sia $\eta \in \operatorname{Ker} \varphi^{\mathcal{O}}$. Allora $\eta \circ \varphi = 0$.

Assumiamo che $\eta \neq 0$. Ciò significa che $(\eta \neq 0) \neq \emptyset$.

Per la prop. 22.15 l'insieme $(\eta \neq 0)$ è aperto, perciò l'ipotesi che φ sia densa implica l'esistenza di un $\alpha \in X$ con $\varphi(\alpha) \in (\eta \neq 0)$, cioè $\eta(\varphi(\alpha)) \neq 0$.

Ma ciò è impossibile, perché $\eta \circ \varphi = 0$.

(2) $\implies$ (1): Per l'oss. 25.11 è sufficiente dimostrare che per ogni $\eta \in \mathcal{O}(Y)$ con $\eta \neq 0$ esiste un $\alpha \in X$ tale che $\varphi(\alpha) \in (\eta \neq 0)$, cioè $\eta(\varphi(\alpha)) \neq 0$.

Ma siccome per ipotesi $\varphi^{\mathcal{O}}$ è iniettivo, per $\eta \neq 0$ si ha $\eta \circ \varphi \neq 0$ e ciò significa che esiste un $\alpha \in X$ con $\eta(\varphi(\alpha)) \neq 0$.

Lemma 25.15. *Siano $X \subset K^n$, $Y \subset K^m$ e $\varphi \in \mathcal{O}(X, Y)$. Se l'omomorfismo $\varphi^{\mathcal{O}}$ è suriettivo , allora φ è iniettiva.*

Dimostrazione. Siano $\alpha, \beta \in X$ ed $\alpha \neq \beta$. Per la prop. 23.14 esiste $\theta \in \mathcal{O}(X)$ tale che $\theta(\alpha) \neq \theta(\beta)$. Per ipotesi l'omomorfismo $\varphi^{\mathcal{O}}$ è suriettivo, perciò esiste $\eta \in \mathcal{O}(Y)$ con $\theta = \eta \circ \varphi$.

Ma allora $\eta(\varphi(\alpha)) = \theta(\alpha) \neq \theta(\beta) = \eta(\varphi(\beta))$ e ciò è possibile sole se $\varphi(\alpha) \neq \varphi(\beta)$.

Lemma 25.16. *Sia $Y \subset X \subset K^n$. Allora $\overline{Y} \cap X = \operatorname{Zeri}(\mathcal{J}(Y, \operatorname{in} \mathcal{O}(X)))$.*

Dimostrazione. Chiaramente $Y \subset \operatorname{Zeri}(\mathcal{J}(Y, \operatorname{in} \mathcal{O}(X)))$. $\operatorname{Zeri}(\mathcal{J}(Y, \operatorname{in} \mathcal{O}(X)))$ è chiuso in X (ciò segue dalla prop. 22.15), perciò $\overline{Y} \cap X \subset \operatorname{Zeri}(\mathcal{J}(Y, \operatorname{in} \mathcal{O}(X)))$.

Assumiamo viceversa che $\alpha \in \operatorname{Zeri}(\mathcal{J}(Y, \operatorname{in} \mathcal{O}(X)))$, ma $\alpha \notin \overline{Y}$.

Per la prop. 14.27 esiste $f \in \mathcal{J}(Y)$ tale che $f(\alpha) \neq 0$.
Poniamo $\theta := f_{X \longrightarrow K}$. Allora $\theta \in \mathcal{O}(X)$ e, siccome $f \in \mathcal{J}(Y)$, abbiamo $\theta_{Y \longrightarrow K} = 0$, cioè $\theta \in \mathcal{J}(Y, \operatorname{in} \mathcal{O}(X))$ e perciò $f(\alpha) = \theta(\alpha) = 0$.

Questo lemma è semplicemente una trascrizione della prop. 14.27.

Corollario 25.17. *Sia $\alpha \in X \subset K^n$. Allora $\{\alpha\} = \mathrm{Zeri}(\mathcal{J}(\alpha, \mathrm{in}\,\mathcal{O}(X)))$.*

Osservazione 25.18. Sia $Y \subset X \subset K^n$.

Allora $\mathcal{J}(Y, \mathrm{in}\,\mathcal{O}(X)) = \mathcal{J}(\overline{Y} \cap X, \mathrm{in}\,\mathcal{O}(X))$.

Dimostrazione. È chiaro che $\mathcal{J}(\overline{Y} \cap X, \mathrm{in}\,\mathcal{O}(X)) \subset \mathcal{J}(Y, \mathrm{in}\,\mathcal{O}(X))$.

Dal lemma 25.16 segue però che ogni elemento di $\mathcal{J}(Y, \mathrm{in}\,\mathcal{O}(X))$ si annulla su $\overline{Y} \cap X$ e ciò significa $\mathcal{J}(Y, \mathrm{in}\,\mathcal{O}(X)) \subset \mathcal{J}(\overline{Y} \cap X, \mathrm{in}\,\mathcal{O}(X))$.

Osservazione 25.19. Siano $X \subset K^n$, $Y \subset K^m$ e $\varphi \in \mathcal{O}(X, Y)$. Allora

$$\mathrm{Ker}\,\varphi^{\mathcal{O}} = \mathcal{J}(\varphi(X), \mathrm{in}\,\mathcal{O}(Y)) \overset{25.18}{=} \mathcal{J}(\overline{\varphi(X)} \cap Y, \mathrm{in}\,\mathcal{O}(Y))$$

Dimostrazione. Per $\eta \in \mathcal{O}(Y)$ sono equivalenti:

$\eta \in \mathrm{Ker}\,\varphi^{\mathcal{O}}$.

$\eta \circ \varphi = 0$.

$\eta(\varphi(\alpha)) = 0$ per o gni $\alpha \in X$.

$\eta_{\varphi(X) \longrightarrow K} = 0$.

$\eta \in \mathcal{J}(\varphi(X), \mathrm{in}\,\mathcal{O}(Y))$.

Osservazione 25.20. Siano $X \subset K^n$, $Y \subset K^m$ e $\varphi \in \mathcal{O}(X, Y)$.
Se B è chiuso in Y, allora

$$\varphi^{-1}(B) = \mathrm{Zeri}(\varphi^{\mathcal{O}}(\mathcal{J}(B, \mathrm{in}\,\mathcal{O}(Y))))$$

Dimostrazione. Siccome B è chiuso in Y, abbiamo $B = \overline{B} \cap Y$ per l'oss. 15.11.

Per $\alpha \in X$ sono equivalenti:

$\alpha \in \varphi^{-1}(B)$.

$\varphi(\alpha) \in B = \overline{B} \cap Y$.

$\varphi(\alpha) \in \mathrm{Zeri}(\mathcal{J}(B, \mathrm{in}\,\mathcal{O}(Y)))$ per il lemma 25.16.

$\eta(\varphi(\alpha)) = 0$ per ogni $\eta \in \mathcal{J}(B, \mathrm{in}\,\mathcal{O}(Y))$.

$\theta(\alpha) = 0$ per ogni $\theta \in \varphi^{\mathcal{O}}(\mathcal{J}(B, \mathrm{in}\,\mathcal{O}(Y)))$.

Corollario 25.21. *Siano $X \subset K^n$, $Y \subset K^m$ e $\varphi \in \mathcal{O}(X, Y)$. Assumiamo inoltre che K sia algebricamente chiuso e che l'omomorfismo $\varphi^{\mathcal{O}}$ sia suriettivo.*

Allora $\varphi(X)$ è chiuso in Y, cioè $\overline{\varphi(X)} \cap Y = \varphi(X)$.

Dimostrazione. Sia $\beta \in \overline{\varphi(X)} \cap Y$. Dobbiamo dimostrare che $\varphi^{-1}(\beta) \neq \emptyset$.

Per l'oss. 25.20 abbiamo $\varphi^{-1}(\beta) = \mathrm{Zeri}(\varphi^{\mathcal{O}}(\mathcal{J}(\beta, \mathrm{in}\,\mathcal{O}(Y))))$.

Dalle oss. 25.18 e 25.19 otteniamo

$$\mathrm{Ker}\,\varphi^{\mathcal{O}} = \mathcal{J}(\varphi(X), \mathrm{in}\,\mathcal{O}(Y)) = \mathcal{J}(\overline{\varphi(X)} \cap Y, \mathrm{in}\,\mathcal{O}(Y)) \subset \mathcal{J}(\beta, \mathrm{in}\,\mathcal{O}(Y))$$

Siccome $\varphi^{\mathcal{O}}$ è suriettivo, dal lemma 3.20 sappiamo che $\varphi^{\mathcal{O}}(\mathcal{J}(\beta, \mathrm{in}\,\mathcal{O}(Y)))$ è un ideale di $\mathcal{O}(X)$.

Siccome K è algebricamente chiuso, il teorema degli zeri (teorema 11.9) implica $\varphi^{-1}(\beta) \neq \emptyset$.

Osservazione 25.22. Siano $Y \subset X \subset K^n$ e $i : Y \longrightarrow X$ l'inclusione.

Allora l'omomorfismo $i^{\mathcal{O}}$ è suriettivo.

Dimostrazione. Sia $\eta \in \mathcal{O}(Y)$. Allora esiste $f \in K[n]$ tale che $\eta = f_{Y \longrightarrow K}$. Ma allora $f_{X \longrightarrow K} \in \mathcal{O}(X)$ e $\eta = f_{X \longrightarrow K} \circ i = i^{\mathcal{O}}(f_{X \longrightarrow K})$.

Osservazione 25.23. Siano $X \subset K^n$ e $Y \subset K^m$ insiemi algebrici e $\varphi \in \mathcal{O}(X, Y)$. Inoltre siano $\varphi(X)$ chiuso e $\varphi_{X \longrightarrow \varphi(X)}$ un isomorfismo.

Allora l'omomorfismo $\varphi^{\mathcal{O}}$ è suriettivo.

Dimostrazione. Considerando la composizione $\varphi : X \longrightarrow \varphi(X) \xrightarrow{i} Y$, dove i è l'inclusione, dall'oss. 24.14 abbiamo

$$\varphi^{\mathcal{O}} = i^{\mathcal{O}} \circ (\varphi_{X \longrightarrow \varphi(X)})^{\mathcal{O}}$$

Il primo fattore è suriettivo per l'oss. 25.22 e il secondo è un isomorfismo per la prop. 24.18. Perciò $\varphi^{\mathcal{O}}$ è suriettivo.

Teorema 25.24. *Siano $X \subset K^n$ e $Y \subset K^m$ insiemi algebrici e $\varphi \in \mathcal{O}(X, Y)$. Assumiamo inoltre che K sia algebricamente chiuso. Allora sono equivalenti:*

(1) L'omomorfismo $\varphi^{\mathcal{O}}$ è suriettivo.

(2) $\varphi(X)$ è chiuso e l'applicazione $\varphi_{X \longrightarrow \varphi(X)}$ è un isomorfismo.

Dimostrazione. (1) $\implies$ (2): Per il lemma 25.25 φ è iniettivo e dal cor. 25.21 sappiamo che $\overline{\varphi(X)} = \overline{\varphi(X)} \cap Y = \varphi(X)$.

Dall'oss. 25.8 abbiamo isomorfismi

$$\begin{array}{ccccc} \mathcal{O}(\varphi(X)) & \longrightarrow & \mathcal{O}(Y)/\mathcal{J}(\varphi(X), \operatorname{in} \mathcal{O}(Y)) & \longrightarrow & \mathcal{O}(X) \\ f_{\varphi(X) \longrightarrow K} & \longmapsto & [f_{Y \longrightarrow K}] & \longmapsto & f_{Y \longrightarrow K} \circ \varphi \end{array}$$

dove il secondo isomorfismo è l'isomorfismo canonico indotto dall'omomorfismo suriettivo $\varphi^{\mathcal{O}}$, il cui nucleo è $\mathcal{J}(\varphi(X), \operatorname{in} \mathcal{O}(Y))$, come abbiamo visto nell'oss. 25.19.

L'applicazione $f_{\varphi(X) \longrightarrow K} \longmapsto f_{Y \longrightarrow K} \circ \varphi$ coincide però con l'omomorfismo $(\varphi_{X \longrightarrow \varphi(X)})^{\mathcal{O}}$ che è un isomorfismo. Per la prop. 24.18 l'applicazione $\varphi_{X \longrightarrow \varphi(X)}$ è un isomorfismo.

Si noti che per poter applicare la prop. 24.18 abbiamo dovuto assumere che X ed Y siano insiemi algebrici.

(2) $\implies$ (1): Oss. 25.23.

Definizione 25.25. Siano $X \subset K^n$, $Y \subset K^m$ e $\varphi \in \mathcal{O}(X, Y)$.

φ si chiama un'*immersione chiusa*, se $\varphi(X)$ è chiuso in Y e l'applicazione $\varphi_{X \longrightarrow \varphi(X)}$ è un isomorfismo.

26. K-algebre polinomiali ridotte

$X \subset K^n$ è irriducibile se e solo se $\mathcal{O}(X)$ è un anello integro. Un ideale I di un anello commutativo A è radicale se e solo se A/I è ridotto. $\mathcal{J}(X)$ è radicale per ogni $X \subset K^n$. Per un sottoinsieme $X \subset K^n$ la K-algebra $\mathcal{O}(X)$ è polinomiale e ridotta. Se K è algebricamente chiuso, le K-algebre polinomiali ridotte coincidono (a meno di isomorfia) con le K-algebre della forma $\mathcal{O}(X)$ con $X \subset K^n$; l'insieme X può essere scelto algebrico. Sempre nell'ipotesi che K sia algebricamente chiuso, le K-algebre polinomiali integre coincidono (a meno di isomorfia) con le K-algebre della forma $\mathcal{O}(X)$, dove X è un sottoinsieme irriducibile di K^n che può essere scelto algebrico.

Situazione 26.1. Sia K un campo.

Osservazione 26.2. Sia $X \subset K^n$. Le K-algebre $\Gamma(X)$ e $\mathcal{O}(X)$ sono isomorfe per la nota 23.10, per cui ogni enunciato su una delle due si traduce immediatamente in un enunciato equivalente per l'altra. Perciò in questo capitolo di natura prevalentemente algebrica, mentre negli enunciati parleremo piuttosto di $\mathcal{O}(X)$, nelle dimostrazioni lavoreremo spesso con $\Gamma(X)$.

Molti autori infatti non distinguono tra $\Gamma(X)$ e $\mathcal{O}(X)$, semplificando la notazione. Si noti però che $\Gamma(X) = \Gamma(\overline{X})$, mentre si ha solo un isomorfismo naturale $\mathcal{O}(X) \cong \mathcal{O}(\overline{X})$.

Proposizione 26.3. *Sia $X \subset K^n$. Allora sono equivalenti:*

(1) X è irriducibile.

(2) $\mathcal{O}(X)$ è un anello integro.

Dimostrazione. Ricordiamo che per definizione un insieme irriducibile è non vuoto. Dal teorema 15.34 sappiamo che X è irriducibile se e solo se $\mathcal{J}(X)$ è un ideale primo.

Siccome $\mathcal{O}(X) \cong \Gamma(X) = K[n]/\mathcal{J}(X)$, otteniamo l'enunciato.

Osservazione 26.4. Ricordiamo dalla def. 3.42 che un anello commutativo (ad esempio una K-algebra commutativa) si dice *ridotto*, se non possiede elementi nilpotenti $\neq 0$.

Osservazione 26.5. Siano A un anello commutativo ed I un ideale di A. Allora sono equivalenti:

(1) I è radicale.

(2) A/I è ridotto.

Dimostrazione. Per $a \in A$ denotiamo con $[a]$ la sua classe di equivalenza in A/I.

(1) $\implies$ (2): Supponiamo che I sia radiale. Siano $a \in A$ e $k \in \mathbb{N}$ tali che $[a]^k = 0$. Però $[a]^k = [a^k]$, per cui $a^k \in I$, ossia $a \in \sqrt{I} = I$, per cui $[a] = 0$.

(2) $\implies$ (1): Supponiamo che A/I sia ridotto. Sia $a \in \sqrt{I}$, ad esempio $a^k \in I$ per un $k \in \mathbb{N}$. Ciò significa che $[a]^k = [a^k] = 0$, cosicché per ipotesi $[a] = 0$, ovvero $a \in I$.

Osservazione 26.6. Sia $X \subset K^n$. Allora l'ideale generalizzato $\mathcal{J}(X)$ è radicale.

Dimostrazione. Ciò segue dall'oss. 14.18 e può essere anche dimostrato direttamente (ricalcando la dimostrazione dell'oss. 12.4):

Sia $f \in \sqrt{\mathcal{J}(X)}$, ad esempio $f^k \in \mathcal{J}(X)$ per un $k \in \mathbb{N}$. Il caso $X = \emptyset$ è banale, perché allora $\mathcal{J}(X) = K[n]$ è sicuramente radicale.

Per $X \neq \emptyset$ necessariamente $k \geq 1$ e se $\alpha \in X$, allora $(f(\alpha))^k = f^k(\alpha) = 0$ e quindi anche $f(\alpha) = 0$, e vediamo che $f \in \mathcal{J}(X)$.

Osservazione 26.7. Sia $X \subset K^n$. Allora la K-algebra $\mathcal{O}(X)$ è polinomiale.

Dimostrazione. Ricordiamo dalla def. 11.2 che una K-algebra è (per definizione) polinomiale se e solo se è una K-algebra commutativa e finitamente generata.

È chiaro che $\mathcal{O}(X)$ è commutativa. Essa è anche finitamente generata, come si vede dal cor. 4.14, essendo $\mathcal{O}(X) \cong \Gamma(X) = K[n]/\mathcal{J}(X)$.

Corollario 26.8. *Sia $X \subset K^n$. Allora la K-algebra polinomiale $\Gamma(X)$ è ridotta.*

Dimostrazione. Per l'oss. 26.6 l'ideale $\mathcal{J}(X)$ è radicale, quindi la K-algebra $\mathcal{O}(X) \cong \Gamma(X) = K[n]/\mathcal{J}(X)$ è ridotta per l'oss. 26.5.

Teorema 26.9. *Siano K algebricamente chiuso ed A una K-algebra polinomiale ridotta.*

Allora esiste un insieme $X \subset K^n$ tale che $A \cong \mathcal{O}(X)$.

L'isomorfia è un'isomorfia di K-algebre.

Dimostrazione. Il caso $A = 0$ è banale. Sia $A \neq 0$.

Per il cor. 4.14 l'ipotesi che A sia polinomiale significa che esistono $n \in \mathbb{N} + 1$ e un ideale I di $K[n]$ tali che $A \cong K[n]/I$.

L'ipotesi che A sia ridotta, per l'oss. 26.5 implica che $\sqrt{I} = I$.

Sia $X := \mathrm{Zeri}(I)$. Dal teorema 12.5 sappiamo che $X \neq \emptyset$ e $\mathcal{J}(X) = \sqrt{I} = I$. In questo modo abbiamo $A \cong K[n]/I = K[n]/\mathcal{J}(X) = \Gamma(X) \cong \mathcal{O}(X)$.

Corollario 26.10. *Siano K algebricamente chiuso ed A una K-algebra commutativa. Allora sono equivalenti:*

(1) A è polinomiale e ridotta.

(2) Esiste $X \subset K^n$ tale che $A \cong \mathcal{O}(X)$.

(3) Esiste $X \subset K^n$ algebrico tale che $A \cong \mathcal{O}(X)$.

Le isomorfie sono isomorfie di K-algebre.

Dimostrazione. (1) $\implies$ (2): Teorema 26.9.

(2) $\implies$ (1): Cor. 26.8.

L'equivalenza (2) $\iff$ (3) è ovvia, perché per un sottoinsieme $X \subset K^n$ si ha $\mathcal{J}(X) = \mathcal{J}(\overline{X})$ per la prop. 14.27 e quindi $\mathcal{O}(X) \cong \Gamma(X) = \Gamma(\overline{X}) \cong \mathcal{O}(\overline{X})$.

Corollario 26.11. *Siano K algebricamente chiuso ed A una K-algebra commutativa. Allora sono equivalenti:*

(1) A è polinomiale e integra.

(2) Esiste un insieme irriducibile $X \subset K^n$ tale che $A \cong \mathcal{O}(X)$.

(3) Esiste un insieme algebrico irriducibile $X \subset K^n$ tale che $A \cong \mathcal{O}(X)$.

Le isomorfie sono isomorfie di K-algebre.

Dimostrazione. L'enunciato segue dal cor. 26.10, tenendo conto della prop. 26.3.

Osservazione 26.12. Siano K algebricamente chiuso ed A una K-algebra polinomiale. Allora $A/\sqrt{0}$ è una K-algebra polinomiale ridotta e può quindi esssere interpretata come un'algebra $\mathcal{O}(X)$ per qualche insieme algebrico affine X.

27. Una stima per la dimensione di $\mathrm{A[x]}$

Per $n \in \mathbb{N}+2$ le varietà affini K e K^n non sono isomorfe. L'ideale $I[x]$. Isomorfia naturale $A[x]/I[x] \cong (A/I)[x]$. $P[x]$ è primo se e solo se P è primo. In tal caso anche $xA[x]+P[x]$ è un ideale primo di $A[x]$. Catene di Krull e dimensione di Krull di un anello commutativo. Se K è un campo, allora $\dim K[x] = 1$. Se $(P_0, \ldots, P_n)$ è una catena di Krull di A, allora $(P_0[x], \ldots, P_n[x], xA[x] + P_n[x])$ è una catena di Krull di $A[x]$. Perciò $\dim A[x] \geq 1 + \dim A$. L'ideale di eliminazione $J \cap A$. Isomorfia naturale $(S^{-1}A)[x] \cong S^{-1}(A[x])$. Se (Q_1, Q_2) è una catena di Krull di $A[x]$ tale che $Q_2 \cap A = 0$, allora $Q_1 = 0$. Se (Q_0, Q_1, Q_2) è una catena di Krull di $A[x]$, allora $Q_0 \cap A \neq Q_2 \cap A$. Perciò $1 + \dim A \leq \dim A[x] \leq 1 + 2\dim A$. Se $\dim A < \infty$, anche $\dim A[x] < \infty$ e per $n > m$ si ha $\dim A[n] > \dim A[m]$. Per $n \neq m$ le varietà affini K^n e K^m non sono isomorfe. Ogni endomorfismo suriettivo di un anello noetheriano è un isomorfismo. Se A è noetheriano e se esiste un omomorfismo suriettivo $A[m] \longrightarrow A[n]$, allora $m \geq n$. Se A è noetheriano e $n \neq m$, allora gli anelli $A[n]$ e $A[m]$ non sono isomorfi.

Situazione 27.1. Sia A un anello commutativo $\neq 0$.

Proposizione 27.2. *Sia K un campo. Allora per $n \in \mathbb{N}+2$ le varietà affini K e K^n non sono isomorfe.*

Dimostrazione. (1) Per $|K| < \infty$ ciò segue immediatamente dal fatto che le cardinalità $|K|$ e $|K^n| = |K|^n$ non sono uguali.

(2) Sia $|K| = \infty$. Allora $\Gamma(K^n) = K[n]$ e $\Gamma(K) = K[1]$.

È noto però dai corsi di Algebra che $K[1]$ è un anello ad ideali principali, mentre non lo è $K[n]$ (nella nostra ipotesi che $n \geq 2$). Le K-algebre $K[1]$ e $K[n]$ non possono perciò essere isomorfe e quindi, per la prop. 24.18, non lo sono nemmeno le varietà affini K e K^n.

Nota 27.3. La dimostrazione della prop. 27.2 nel caso che K sia finito è banale. Ma anch'essa usa un principio generale: Per dimostrare che due strutture matematiche non sono isomorfe, dimostriamo che per esse un'*invariante* non coincide, di cui sappiamo che è uguale per strutture isomorfe. La più semplice di queste invarianti è la cardinalita che nel caso di insiemi finiti permette spesso una rapida prima classificazione.

Simile come idea, ma molto più potente è versatile, è il concetto di *dimensione* che viene utilizzato (e definito in modi diversi) in molti campi della matematica e che introdurremo adesso nel caso degli anelli commutativi.

Osservazione 27.4. Nella prop. 27.2 anche per $|K| = \infty$ si sarebbe potuto evitare l'utilizzo della prop. 24.18. Infatti la diagonale $\{(\alpha, \ldots, \alpha) \mid \alpha \in K\}$ in K^n è un sottoinsieme chiuso infinito e distinto da K^n per $n \geq 2$. Nella topologia di Zariski gli spazi topologici K e K^n non possono perciò essere omeomorfi. Siccome un isomorfismo è anche un omeomorfismo (per la prop. 22.15), le varietà affini K e K^n non sono isomorfe.

Definizione 27.5. Sia I un ideale generalizzato di A. Allora con

$$I[x] := \{a_0 + a_1 x + \ldots + a_m x^m \mid a_0, \ldots, a_m \in I\}$$

denotiamo l'insieme dei polinomi nell'indeterminata x i cui coefficienti appartengono tutti ad I.

È chiaro che $I[x]$ è un ideale generalizzato di $A[x]$.

Osservazione 27.6. Sia I un ideale generalizzato di A.

Allora $I[x] = A[x]_{\smile}I$.

Dimostrazione. (1) Sia $f \in I[x]$, ad es. $f = a_0 + a_1x + \ldots + a_mx^m$ con $a_0, \ldots, a_m \in I$. È chiaro che allora $f \in A[x]_{\smile}I$.

(2) Sia $f \in A[x]_{\smile}I$. Allora esistono $a_1, \ldots, a_k \in I$ e $g_1, \ldots, g_k \in A[x]$ tali che $f = a_1g_1 + \ldots + a_kg_k$.

Siccome I è un ideale generalizzato di A, per ogni j i coefficienti di a_jg_j appartengono ad I ed espandendo i g_j vediamo che $f \in I[x]$.

Osservazione 27.7. (1) Se I e J sono ideali generalizzati di A con $I \neq J$, allora $I[x] \neq J[x]$.

(2) Se I è un ideale di A, allora $I[x]$ è un ideale di $A[x]$.

Dimostrazione. (1) Sia ad es. $a \in I \setminus J$. Allora si ha anche $a \in I[x] \setminus J[x]$.

(2) Per ipotesi si ha $I \neq A$, cosicché il punto (1) implica $I[x] \neq A[x]$.

Osservazione 27.8. Sia I un ideale generalizzato di A.

Allora $I[x] \cap A = I$.

Dimostrazione. (1) È chiaro che $I \subset I[x] \cap A$.

(2) Sia $f = a_0 + a_1x + \ldots + a_mx^m \in I[x] \cap A$. Allora necessariamente $a_1, \ldots, a_m = 0$ ed $a_0 \in I$, quindi $f = a_0 \in I$.

Proposizione 27.9. *Siano I un ideale generalizzato di A e $\psi : A[x] \longrightarrow (A/I)[x]$ l'applicazione che trasforma un polinomio $f = a_0 + a_1x + \ldots + a_mx^m$ nel polinomio $(a_0 + I) + (a_1 + I)x + \ldots + (a_m + I)x^m =: f \mod I \in (A/I)[x]$.*

Allora ψ è un omomorfismo di anelli suriettivo e si ha $\operatorname{Ker}\psi = I[x]$. Otteniamo quindi un isomorfismo naturale

$$\begin{aligned} A[x]/I[x] &\longrightarrow (A/I)[x] \\ f + I[x] &\longmapsto f \mod I \end{aligned}$$

Dimostrazione. È immediato che ψ è un omomorfismo di anelli suriettivo.

Le altre affermazioni sono a questo punto evidenti. Cfr. Dummit/Foote [16966], p. 296, oppure Reiffen/Scheja/Vetter [1799], p. 160-161.

Proposizione 27.10. *Sia P un ideale generalizzato di A. Allora sono equivalenti:*

(1) P è primo (come ideale di A).

(2) $P[x]$ è primo (come ideale di $A[x]$).

Dimostrazione. Per la prop. 27.9 sono equivalenti:

P è primo.

A/P è integro.

$(A/P)[x]$ è integro.

$A[x]/P[x]$ è integro.

$P[x]$ è primo.

Osservazione 27.11. Non è difficile dimostrare la prop. 27.10 direttamente, senza appello alla prop. 27.9:

Siano $f, g \in A[x]$ tali che $fg \in P[x]$. Assumiamo che $f, g \notin P[x]$. Allora possiamo scrivere $f = \sum_{k=0}^{\infty} a_k x^k$ e $g = \sum_{k=0}^{\infty} b_k x^k$ con $a_k = b_k = 0$ per $k >> 0$ e per ipotesi esistono $p, q \in \mathbb{N}$ tali che $a_p \notin P$, $b_q \notin P$, mentre $a_i \in P$ per ogni $i < p$, $b_j \in P$ per ogni $j < q$.

Il coefficiente c_{p+q} di x^{p+q} in fg è allora uguale a una somma di termini della forma $a_i b_j$ con $i + j = p + q$. Si ha o $i = p, j = q$ oppure $i < p$ oppure $j < q$. Negli ultimi due casi però $a_i b_j \in P$, mentre $a_p b_q \notin P$. Ma allora anche $c_{p+q} \notin P$, una contraddizione all'ipotesi che $fg \in P[x]$.

Lemma 27.12. *(1) Siano I un ideale di A, $a \in A \setminus I$ ed $u \in A[x]$.*

Allora $a + xu \notin xA[x] + I[x]$.

(2) Sia I un ideale di A. Allora $xA[x] + I[x]$ è un ideale di $A[x]$.

(3) Sia P un ideale primo di A. Allora $xA[x] + P[x]$ è un ideale primo di $A[x]$.

Dimostrazione. (1) Siano $v \in A[x]$ e $w \in I[x]$ tali che $a+xu = xv+w$. Allora possiamo scrivere w nella forma $w = b+xf$ con $b \in I$ ed $f \in I[x]$. Ciò implica però $a + xu = xv + b + xf$ e quindi $a = b \in I$, una contraddizione.

(2) Dal punto (1) per $u = 0$ (o direttamente) si vede che $1 \notin xA[x] + I[x]$.

(3) Siano $M := xA[x] + P[x]$ ed $f, g \in A[x] \setminus M$.

Possiamo scrivere $f = a+xu, g = b+xv$ con $a, b \in A$ ed $u, v \in A[x]$. L'ipotesi $f, g \notin M$ implica $a, b \notin P$ e quindi $ab \notin P$, perché P è primo.

Dal punto (1) segue che $fg = ab + x(av + bu + xuv) \notin M$.

Definizione 27.13. (1) Una *catena di Krull* di A è una sequenze finita $(P_0, \ldots, P_k)$ di ideali primi di A tale che $P_0 \subsetneqq P_1 \subsetneqq \ldots \subsetneqq P_k$.

k si chiama allora l'*altezza* della catena.

(2) Se in A esistono catene di Krull di altezza arbitraria, allora diciamo che A possiede dimensione infinita e scriviamo $\dim A = \infty$.

Se $A = 0$ (questo è l'unico caso in cui non esistono catene di Krull in A), allora poniamo $\dim A := -\infty$.

Altrimenti la *dimensione* (di Krull) di A è definita come l'altezza massima di una catena di Krull di A.

(3) Per un ideale primo $P \in \operatorname{Spec} A$ definiamo l'*altezza* mediante

$$\operatorname{alt} P := \dim A_P$$

Essa coincide, per il teorema 21.10, con il sup (possibilmente infinito) delle altezze di catene di Krull terminanti in P.

Osservazione 27.14. È chiaro che anelli commutativi isomorfi possiedono la stessa dimensione.

Osservazione 27.15. Sia A integro. Allora $\dim A = 0$ se e solo se A è un campo.

Si noti però che ad esempio anche $\dim \mathbb{Z}/m = 0$ per ogni $m \in \mathbb{N} + 2$.

Osservazione 27.16. (1) Sia A un anello ad ideali principali. Se A è un campo, allora $\dim A = 0$. Altrimenti $\dim A = 1$.

(2) Sia K un campo. Allora $\dim K[x] = 1$.

Dimostrazione. (1) È noto dal corso di Algebra che in un anello ad ideali principali ogni ideale primo $\neq 0$ è massimale.

(2) Ciò segue da (1), perché $K[x]$ è un anello ad ideali principali, ma non è un campo.

Lemma 27.17. *Sia* $(P_0, \ldots, P_n)$ *una catena di Krull di* A.

Allora $(P_0[x], \ldots, P_n[x], xA[x] + P_n[x])$ *è una catena di Krull di* $A[x]$.

Dimostrazione. (1) Dalla prop. 27.10 e dal lemma 27.12 segue che gli ideali nella seconda sequenza sono tutti primi. Dall'oss. 27.7 sappiamo che $P_0[x] \subsetneqq \ldots \subsetneqq P_n[x]$.

(2) È chiaro che $P_n[x] \subset xA[x] + P_n[x]$. Questa inclusione è stretta perché $x \notin P_n[x]$.

Corollario 27.18. $\dim A[x] \geq 1 + \dim A$.

Osservazione 27.19. Sia J un ideale generalizzato di $A[x]$. Allora:

(1) $J \cap A$ è un ideale generalizzato di A.

(2) Se J è un ideale di $A[x]$, allora $J \cap A$ è un ideale di A.

(3) Se J è un ideale primo di $A[x]$, allora $J \cap A$ è un ideale primo di A.

Dimostrazione. Sia $i : A \longrightarrow A[x]$ l'inclusione. Allora $i^{-1}(J) = \{a \in A \mid a \in J\} = J \cap A$. L'enunciato segue perciò dal lemma 3.18.

Definizione 27.20. Sia J un ideale di $A[x]$. Allora $J \cap A$ si chiama l'*ideale di eliminazione* di J (rispetto all'indeterminata x).

Si noti che $J \cap A$ consiste semplicemente dei polinomi costanti (rispetto all'indeterminata x) appartenenti a J. In particolare si ha $J \cap A = 0$ se e solo se J non contiene polinomi costanti $\neq 0$.

La terminologia è dovuta al fatto che quando A è a sua volta un anello di polinomi, ad es. $A = F[y_1, \ldots, y_m]$, dove F è un anello commutativo ed $y_1, \ldots, y_m$ sono indeterminate (diverse da x), allora $J \cap A$ consiste esattamente dei polinomi in $A[y_1, \ldots, y_m, x]$ in cui l'indeterminata x non appare („è stata eliminata", cfr. Kreuzer/Robbiano [16994], p. 195).

Osservazione 27.21. Sia Q un ideale primo di $A[x]$ tale che $Q \cap A = 0$.

Allora l'anello A è integro.

Dimostrazione. Per l'oss. 27.19 $Q \cap A$ è un ideale primo di A. Se $Q \cap A = 0$, ciò implica che A è integro.

Una dimostrazione diretta è altrettanto semplice: Siano $a, b \in A$ tali che $ab = 0$. Allora $ab \in Q$ (in $A[x]$) e quindi ad esempio $a \in Q$. Allora però $a \in Q \cap A = 0$ e quindi $a = 0$.

Proposizione 27.22. *Sia S un sottomonoide puro di A. Allora l'applicazione*

$$\tau : (S^{-1}A)[x] \longrightarrow S^{-1}(A[x]) \quad \textit{data da} \quad \sum_{k=0}^{n} \frac{(a_k)_S}{s} x^k \longmapsto \frac{\left(\sum_{k=0}^{n} a_k x^k\right)_S}{s}$$

è ben definita e un isomorfismo.

Dimostrazione. (1) Osserviamo prima che ogni elemento $\sum_{k=0}^{n} \frac{(a_k)_S}{s_k} x^k$ di $(S^{-1}A)[x]$ può essere scritto nella forma $\sum_{k=0}^{n} \frac{(a_k)_S}{s} x^k$, semplicemente raccogliendo i denominatori.

(2) È una verifica immediata adesso che l'applicazione τ è ben definita e un omomorfismo.

(3) È evidente che τ è suriettivo.

(4) Dimostriamo l'iniettività. Sia $\frac{\left(\sum_{k=0}^{n} a_k x^k\right)_S}{s} = 0$. Allora esiste $t \in S$ tale che $t \sum_{k=0}^{n} a_k x^k = 0$. Ciò significa $t a_k = 0$ e quindi $(a_k)_S = 0$ per ogni k.

Cfr. Scheja/Storch [1589], 2. volume, p. 21.

Corollario 27.23. *Sia A un anello integro. Allora esiste un isomorfismo naturale $\mathcal{K}(A)[x] \cong (A \setminus 0)^{-1}(A[x])$.*

Lemma 27.24. *Sia (Q_1, Q_2) una catena di Krull di $A[x]$ tale che $Q_2 \cap A = 0$.*

Allora $Q_1 = 0$.

Dimostrazione. Dal lemma 27.21 segue che A è un anello integro. Perciò l'insieme $S := A \setminus 0$ è un sottomonoide puro di A. Per il cor. 27.23 abbiamo un isomorfismo naturale $\mathcal{K}(A)[x] \cong S^{-1}(A[x])$.

L'ipotesi $Q_2 \cap A = 0$ implica però $Q_2 \cap S = \emptyset$. Assumiamo adesso, per assurdo, che $Q_1 \neq 0$. Allora $(0, Q_1, Q_2)$ è una catena di Krull di $A[x]$ e siccome $0 \cap S = \emptyset$, dal teorema 19.46 otteniamo una catena di Krull $(0, S^{-1}Q_1, S^{-1}Q_2)$ in $S^{-1}(A[x])$.

Quest'ultimo anello però è isomorfo a $\mathcal{K}(A)[x]$ ed ha quindi dimensione 1 per l'oss. 27.16 e perciò non può contenere una catena di Krull di altezza 2.

Corollario 27.25. *Sia $Q \in \operatorname{Spec} A[x]$ tale che $Q \neq 0$ e $Q \cap A = 0$.*

Allora $\operatorname{alt} Q = 1$.

Osservazione 27.26. Sia J un ideale generalizzato di $A[x]$.

Allora $(J \cap A)[x] \subset J$.

Dimostrazione. Siano $a_0, \ldots, a_m \in J \cap A$. Siccome J è un ideale generalizzato di $A[x]$, ciò implica $a_0, a_1 x, \ldots, a_m x^m \in J$ e quindi anche $a_0 + a_1 x + \ldots + a_m x^m \in J$.

Lemma 27.27. *Sia* (Q_0, Q_1, Q_2) *una catena di Krull di* $A[x]$.

Allora $Q_0 \cap A \neq Q_2 \cap A$.

Dimostrazione. Assumiamo, per assurdo, che $Q_0 \cap A = Q_2 \cap A$.

Per l'oss. 27.19 $P_0 := Q_0 \cap A$ è un ideale primo di A. Sia $A' := A/P_0$. Poniamo inoltre

$Q_1' := \{f \mod P_0 \mid f \in Q_1\} \subset A'[x]$

$Q_2' := \{f \mod P_0 \mid f \in Q_2\} \subset A'[x]$

dove l'espressione $f \mod P_0$ è definita come nella prop. 27.9.

Se $\theta : A[x]/P_0[x] \longrightarrow A'[x]$ è l'isomorfismo di quella proposizione, abbiamo quindi $Q_1' = \theta(Q_1)$ e $Q_2' = \theta(Q_2)$. Da ciò segue che (Q_1', Q_2') è una catena di Krull di $A'[x]$.

Inoltre $Q_2' \cap A' = \{a \mod P_0 \mid a \in Q_2 \cap A = P_0\} = 0$.

Per il lemma 27.24 quindi $Q_1' = 0$ e ciò significa che $f \mod P_0 = 0$ per ogni $f \in Q_1$, ovvero $Q_1 \subset P_0[x]$.

Usando l'oss. 27.26 abbiamo $Q_1 \subset (Q_0 \cap A)[x] \subset Q_0$, una contraddizione.

Proposizione 27.28. $1 + \dim A \leq \dim A[x] \leq 1 + 2 \dim A$.

Dimostrazione. (1) La prima disuguaglianza è già stata stabilita nel cor. 27.18.

(2) Se $\dim A = \infty$, l'enunciato è banalmente vero.

(3) Assumiamo quindi che $\dim A < \infty$. Data una catena di Krull di $A[x]$, la possiamo scrivere nella forma $(Q_{01}, \ldots, Q_{0m_0}, Q_{11}, \ldots, Q_{1m_1}, \ldots, Q_{k1}, \ldots, Q_{km_k})$, dove per ogni i fissato le intersezioni $P_i := Q_{ij} \cap A$ per $j = 1, \ldots, m_i$ sono tutte uguali, mentre gli ideali P_i sono tutti distinti.

L'altezza h della catena è uguale ad $h = m_0 + \ldots + m_k - 1$ e dal lemma 27.27 segue $h \leq 2(k+1) - 1 = 2k + 1$.

Necessariamente però $k \leq \dim A$, per cui $h \leq 1 + 2 \dim A$. Ciò mostra che $\dim A[x] \leq 1 + 2 \dim A$.

Corollario 27.29. *Se* $\dim A < \infty$*, allora anche* $\dim A[x] < \infty$.

Corollario 27.30. *Siano* $n, m \in \mathbb{N}$ *con* $n > m$ *e sia* $\dim A < \infty$.

Allora $\dim A[n] > \dim A[m]$.

Gli anelli $A[n]$ *ed* $A[m]$ *non sono quindi isomorfi.*

Dimostrazione. Per il cor. 27.18 abbiamo $\dim A[n] \geq \dim A[m] + (n - m)$.

Per il cor. 27.29 $\dim A[m] < \infty$ e quindi $\dim A[n] > \dim A[m]$.

Corollario 27.31. *Sia* K *un campo e siano* $n, m \in \mathbb{N}$ *con* $n \neq m$*. Allora le varietà affini* K^n *e* K^m *non sono isomorfe.*

Dimostrazione. (1) Per $|K| < \infty$ ciò è evidente perche $|K^n| \neq |K^m|$.

(2) Se $|K| = \infty$, allora gli anelli $\Gamma(K^n) = K[n]$ e $\Gamma(K^m) = K[m]$ non sono isomorfi e quindi anche le varietà K^n e K^m non possono essere isomorfe.

Osservazione 27.32. Facciamo adesso vedere che è possibile arrivare alla conclusione del cor. 27.31 per una via diretta che non necessita del concetto di dimensione, importantissimo comunque in situazioni più complesse, come abbiamo già osservato nella nota 27.3.

Lemma 27.33. *Se A è noetheriano, allora ogni endomorfismo (di anelli) suriettivo di A è iniettivo e quindi un isomorfismo.*

Dimostrazione. Siano $u : A \longrightarrow A$ un endomorfismo suriettivo ed $a \in \operatorname{Ker} u$ con $a \neq 0$.

Sia $n \in \mathbb{N}+1$. Siccome anche u^n è suriettivo, esiste $b \in A$ tale che $u^n(b) = a$. Allora $u^{n+1}(b) = 0$, mentre per ipotesi $u^n(b) = a \neq 0$.

Siccome $\operatorname{Ker} u^n \subset \operatorname{Ker} u^{n+1}$, abbiamo quindi $\operatorname{Ker} u^n \subsetneqq \operatorname{Ker} u^{n+1}$. In questo modo otteniamo una catena infinita $\operatorname{Ker} u \subsetneqq \operatorname{Ker} u^2 \subsetneqq \dots$ in contrasto con l'ipotesi che A sia noetheriano.

Proposizione 27.34. *Siano A noetheriano ed $n, m \in \mathbb{N}$. Se esiste un omomorfismo suriettivo di anelli $A[m] \longrightarrow A[n]$, allora $m \geq n$.*

Dimostrazione. Assumiamo, per assurdo, che $m < n$. Sia $\pi : A[n] \longrightarrow A[m]$ la proiezione naturale indotta dall'isomorfia $A[m] \cong A[n]/(x_{m+1}, \dots, x_n)$ (o, più direttamente, determinata da $x_i \longmapsto x_i$ per $i \leq m$ e $x_i \longmapsto 0$ per $i = m+1, \dots, n$, seconda la prop. 24.26 che rimane valida anche quando K è solo un anello commutativo e non necessariamente un campo).

Sia $v : A[m] \longrightarrow A[n]$ un omomorfismo suriettivo.

Allora $v \circ \pi : A[n] \longrightarrow A[n]$ è un endomorfismo suriettivo e non iniettivo dell'anello noetheriano $A[n]$, in contrasto con il lemma 27.3.

Corollario 27.35. *Siano $n, m \in \mathbb{N}$ con $n \neq m$. Se A è noetheriano, allora gli anelli $A[n]$ e $A[m]$ non sono isomorfi.*

28. Primi esempi

Un insieme si dice localmente chiuso se è intersezione di un chiuso e di un aperto, e costruibile se è unione di un numero finito di insiemi localmente chiusi. Per un teorema di Chevalley l'immagine di un sottoinsieme algebrico di K^n tramite un'applicazione polinomiale è costruibile; in genere invece non è più algebrico, come mostra la proiezione di un'iperbole. Se $\operatorname{car} K \neq 2$ e se in K esiste un elemento i tale che $i^2 = -1$, allora cerchio e iperbole, cioè gli insiemi $\operatorname{Zeri}(x^2+y^2-1)$ e $\operatorname{Zeri}(xy-1)$, sono isomorfi. Se K è algebricamente chiuso, allora un sottoinsieme $X \subset K^n$ è connesso se e solo se $\mathcal{O}(X)$ non contiene idempotenti $\neq 0, 1$. Se $n \in \mathbb{N}+2$ ed $h \in K[n-1]$, allora il grafico $\operatorname{Zeri}(x_n - h)$ è isomorfo a K^{n-1}; se K è infinito, allora $\mathcal{J}(\operatorname{Zeri}(x_n - h)) = K[n]\frown(x_n - h)$ e quindi il polinomio $x_n - h$ è irriducibile. Le varietà affini $X := \operatorname{Zeri}(xy-1)$ e K non sono isomorfe: se K è finito, ciò segue dal fatto che $|\operatorname{Zeri}(xy-1)| = |K| - 1$, se K invece è infinito, si dimostra che la K-algebra $\Gamma(X)$ contiene un elemento invertibile che non appartiene a K. Il polinomio $xy-1$ è irriducibile: infatti le K-algebre $K[x,y]/(xy-1)$ e $K[x]_x$ sono isomorfe e di $K[x]_x$ sappiamo che è un anello integro. D'altra parte, se $2 < |K| < \infty$, allora $\operatorname{Zeri}(xy-1)$ non è irriducibile e quindi il suo ideale non può essere uguale a $K[x,y]\frown(xy-1)$. Un'applicazione qualsiasi definita su un sottoinsieme finito di K^n è polinomiale; ciò implica in particolare che due insiemi affini finiti sono isomorfi se e solo se hanno lo stesso numero di elementi. Infatti si dimostra facilmente che per X finito la funzione caratteristica di ogni elemento di X è polinomiale, poi si usa la formula $\varphi = \sum_{\alpha \in X} \varphi(\alpha)\chi_\alpha$ valida per ogni applicazione $\varphi : X \longrightarrow K^m$. Se K è infinito ed X un sottoinsieme finito di K^n, allora le funzioni caratteristiche dei punti di X si possono ottenere mediante un'applicazione lineare $K^n \longrightarrow K$ che separa i punti di X (di cui cioè la restrizione ad X è iniettiva); nella dimostrazione si usa essenzialmente che K^n non è unione di un numero finito di iperpiani. Se K è finito e possiede q elementi, possiamo invece per ogni $\alpha = (\alpha_1, \ldots, \alpha_n) \in K^n$ rappresentare la funzione caratteristica di α tramite il polinomio $\prod_{1 \leq i \leq n} (1 - (x_i - \alpha_i)^{q-1})$. Applicando questa formula nel caso particolare di una funzione booleana $\varphi : 2^n \longrightarrow 2$, otteniamo la forma normale disgiuntiva di φ. Per $X \subset K^n$ la K-algebra $\mathcal{O}(X)$ è di dimensione finita su K se e solo se l'insieme X è finito. Se K è algebricamente chiuso ed $f \in K[n]$ è un polinomio non costante con $n \geq 2$, allora gli insiemi $\operatorname{Zeri}(f)$ e $K^n \setminus \operatorname{Zeri}(f)$ sono entrambi infiniti. Il criterio di Eisenstein ci permette di dimostrare che per $n \geq 3, \operatorname{car} K = 0, d_1, \ldots, d_n \in \mathbb{N}+1$ ed $a_1, \ldots, a_n \in K \setminus 0$ il polinomio $a_1 x_1^{d_1} + \ldots + a_n x_n^{d_n}$ è irriducibile. L'ipotesi $n \geq 3$ qui è necessaria; si può comunque dimostrare che per $d, e \in \mathbb{N}+1$ con $\operatorname{mcd}(d,e) = 1$ ed $a, b \in K \setminus 0$ il polinomio $ax^d + by^e$ è irriducibile. Il quoziente di ideali $I : J = \{a \in A \mid aJ \subset I\}$ geometricamente corrisponde alla differenza insiemistica: Se K è algebricamente chiuso ed I e J sono due ideali generalizzati di $K[n]$, allora, posto $X := \operatorname{Zeri}(I)$ ed $Y := \operatorname{Zeri}(J)$, si ha $\overline{X \setminus Y} = \operatorname{Zeri}(\sqrt{I} : J)$. Il foglio di Cartesio $y^2 = x^3 + x^2$.

Situazione 28.1. Sia K un campo. Usiamo spesso le indeterminate $x := x_1$, $y := x_2$, $z = x_3$.

Definizione 28.2. Un sottoinsieme Y di uno spazio topologico X si dice

(1) *localmente chiuso*, se è intersezione di un chiuso e di un aperto di X;

(2) *costruibile*, se è unione di un numero finito di sottoinsiemi localmente chiusi di X.

Nota 28.3. L'immagine di un sottoinsieme algebrico $X \subset K^n$ mediante un'applicazione polinomiale i.g. non è più un insieme algebrico.

Consideriamo ad esempio $X := \operatorname{Zeri}(xy-1) \subset K^2$ e la proiezione $\pi_1 = (x_1)_{X \longrightarrow K} : K^2 \longrightarrow K$.

Siccome per ogni $\alpha \in K \setminus 0$ esiste $\beta \in K$ con $\alpha\beta = 1$ (perché K è un campo), mentre sicuramente $0 \notin \pi_1(X)$, vediamo che $\pi_1(X) = K \setminus 0$. Questo insieme non è algebrico se K è un campo infinito.

Nel caso generale per un'applicazione polinomiale $\varphi : K^n \longrightarrow K^m$ e un sottoinsieme algebrico $X \subset K^n$ non è facile verificare se l'immagine $\varphi(X)$ è algebrica. Per un teorema di Chevalley essa è costruibile, se K è algebricamente chiuso.

Cfr. le dimostrazioni in Fieseler/Kaup [19875], p. 96-97, Mumford [22023], p. 51, Patil/Storch [22111], p. 108, Eisenbud [11998], p. 315, Kemper [21951], p. 144, e la discussione in Hartshorne [1470], p. 94, Cox/Little/O'Shea [22312], p. 126-127, 262-263, Brodmann [1026], p. 292.

Lemma 28.4. *Sia $\varphi : K^n \longrightarrow K^n$ un isomorfismo di insiemi algebrici affini e sia X un chiuso di K^n. Allora:*

(1) $\varphi(X)$ è un chiuso di K^n.

(2) Se $h_1, \ldots, h_k \in K[n]$ sono tali che $\mathcal{J}(X) = K[n]_\smile(h_1, \ldots, h_k)$ e se
$\varphi^{-1} = (g_1, \ldots, g_n)_{K^n \longrightarrow K^n}$ *con $g_1, \ldots, g_n \in K[n]$, allora*
$\varphi(X) = \mathrm{Zeri}(h_1(g_1, \ldots, g_n), \ldots, h_k(g_1, \ldots, g_n))$.

Dimostrazione. (1) φ è in particolare un omeomorfismo rispetto alla topologia di Zariski e quindi trasforma chiusi in chiusi. L'enunciato segue anche dal punto (2).

(2) Ciò è una conseguenza immediata dell'oss. 22.12, osservando che $X = \mathrm{Zeri}(\mathcal{J}(X))$, perché X è chiuso, e quindi

$$\varphi(X) = (\varphi^{-1})^{-1}(\mathrm{Zeri}(\mathcal{J}(X))) = (\varphi^{-1})^{-1}(\mathrm{Zeri}(K[n]_\smile(h_1, \ldots, h_k)))$$

Esempio 28.5. Siano $\mathrm{car}\, K \neq 2$ ed $i \in K$ tale che $i^2 = -1$ (un tale elemento esiste sicuramente se K è algebricamente chiuso).

Consideriamo l'applicazione $\varphi := (x + iy, x - iy)_{K^2 \longrightarrow K^2}$. Allora $\varphi^{-1} = \left(\dfrac{x+y}{2}, \dfrac{x-y}{2i}\right)_{K^2 \longrightarrow K^2}$ e vediamo che φ è un isomorfismo.
Sia $X := \mathrm{Zeri}(x^2 + y^2 - 1)$.

Per il lemma 28.4 abbiamo $\varphi(X) = \mathrm{Zeri}\left(\left(\dfrac{x+y}{2}\right)^2 + \left(\dfrac{x-y}{2i}\right)^2 - 1\right)$.

Però $\left(\dfrac{x+y}{2}\right)^2 + \left(\dfrac{x-y}{2i}\right)^2 = \dfrac{x^2 + 2xy + y^2}{4} - \dfrac{x^2 - 2xy + y^2}{4} = xy$, per cui $\varphi(X) = \mathrm{Zeri}(xy - 1)$. Otteniamo così un isomorfismo

$$\varphi_{X \longrightarrow \varphi(X)} : \mathrm{Zeri}(x^2 + y^2 - 1) \longrightarrow \mathrm{Zeri}(xy - 1)$$

Si noti che l'ipotesi che esista l'elemento i è necessaria, come mostra il caso $K = \mathbb{R}$. Cfr. Ueno [21931], vol. 1, p. 14.

Lemma 28.6. *Siano X un insieme e $\theta \in K^X$. Allora:*

(1) θ è idempotente se e solo se θ assume solo i valori 0 e 1.

(2) Se θ è idempotente, allora $X = \mathrm{Zeri}(\theta) \sqcup \mathrm{Zeri}(1 - \theta)$.

Dimostrazione. (1) Chiaro, perché in un campo gli unici elementi idempotenti sono 0 e 1.

(2) Dal punto (1) segue che $\mathrm{Zeri}(1-\theta) = X \setminus \mathrm{Zeri}(\theta)$.

Corollario 28.7. *Sia $X \subset K^n$. Se l'anello $\mathcal{O}(X)$ contiene un idempotente $\neq 0, 1$, allora X non è connesso.*

Dimostrazione. Sia θ un idempotente di $\mathcal{O}(X)$. Se $\theta \neq 0, 1$, allora $\mathrm{Zeri}(\theta) \neq X$ e $\mathrm{Zeri}(1-\theta) \neq X$. Gli insiemi $\mathrm{Zeri}(\theta)$ e $\mathrm{Zeri}(1-\theta)$ sono chiusi di X, per cui l'enunicato segue dal lemma 28.6.

Osservazione 28.8. Siano A un anello commutativo ed $a, b \in A$ tali che $a + b = 1$.

Se in più $ab = 0$, allora gli elementi a e b sono idempotenti.

Dimostrazione. Infatti $a^2 = a(1-b) = a - ab = a$ e similmente $b^2 = b$.

Proposizione 28.9. *Siano K algebricamente chiuso ed $X \subset K^n$ un sottoinsieme algebrico. Allora sono equivalenti:*

(1) X è connesso.

(2) $\mathcal{O}(X)$ non contiene elementi idempotenti $\neq 0, 1$.

Dimostrazione. (1) $\implies$ (2): Cor. 28.8.

(2) $\implies$ (1): Siano A, B sottoinsiemi chiusi di X con $X = A \cup B$ ed $A \cap B = \emptyset$. Siano $I := \mathcal{J}(A)$ e $J := \mathcal{J}(B)$. Allora

$$\emptyset = A \cap B = \overline{A} \cap \overline{B} = \mathrm{Zeri}(I) \cap \mathrm{Zeri}(J) \overset{14.5}{=} \mathrm{Zeri}(I + J)$$

Siccome K è algebricamente chiuso, dal teorema degli zeri otteniamo $I + J = K[n]$. Perciò esistono $f \in I$ e $g \in J$ tali che $f + g = 1$.

Siano $\theta := f_{X \longrightarrow K}$ ed $\eta := g_{X \longrightarrow K}$. Allora $\theta\eta \in \mathcal{O}(X)$ e $\theta + \eta = 1$.

D'altra parte però $\theta_{|A} = 0$ ed $\eta_{|B} = 0$, cosicché da $X = A \cup B$ abbiamo $\theta\eta = 0$. Dall'oss. 28.8 segue che θ ed η sono idempotenti.

L'ipotesi (2) implica che ad esempio $\theta = 1$ ed $\eta = 0$ e da ciò segue $A = \emptyset$.

Cfr. Perrin [21031], p. 24. L'ipotesi che X sia algebrico in verità non è necessaria, come si vede facilmente.

Lemma 28.10. *K sia infinito. Siano $n \geq 2$ ed $h \in K[n-1]$.*

Allora $\mathcal{J}(\mathrm{Zeri}(x_n - h)) = K[n]_{\smile}(x_n - h)$.

Dimostrazione. Sia $f \in \mathcal{J}(\mathrm{Zeri}(x_n - h))$.

Allora $f(\alpha_1, \ldots, \alpha_{n-1}, h(\alpha_1, \ldots, \alpha_{n-1})) = 0$ per ogni $\alpha = (\alpha_1, \ldots, \alpha_{n-1})$ appartenente a K^{n-1} e quindi $f(x_1, \ldots, x_{n-1}, h) = 0$, perché K è infinito. Dallo schema di Ruffini applicato all'anello $K[n-1]$ otteniamo

$$f = (x_n - h)g + r \text{ con } g \in K[n] \text{ ed } r \in K[n-1]$$

Ma allora $0 = f(x_1, \ldots, x_{n-1}, h) = r$ implica $f = (x_n - h)g$.

Esempio 28.11. Siano $n \geq 2$, $h \in K[n-1]$ ed $X := \mathrm{Zeri}(x_n - h) \subset K^n$ il grafico di $h_{K^{n-1} \longrightarrow K}$. Allora l'applicazione $\varphi := \bigcirc_{\alpha}(\alpha_1, \ldots, \alpha_{n-1}) : X \longrightarrow K^{n-1}$

è polinomiale e l'applicazione $\psi := \bigcirc_{(\alpha_1,\ldots,\alpha_{n-1})} (\alpha_1, \ldots, \alpha_{n-1}, h(\alpha_1, \ldots, \alpha_{n-1})) : K^{n-1} \longrightarrow X$, anch'essa polinomiale, è ben definita e l'inversa di φ.

L'insieme algebrico X è quindi isomorfo a K^{n-1}. Se K è infinito, l'insieme X è perciò irriducibile e dal teorema 15.34 segue, usando il lemma 28.10, che il polinomio $x_n - h$ è irriducibile.

Sempre nell'ipotesi che K sia infinito e posto $P := K[n]_\smile(x_n - h)$, gli isomorfismi di K-algebre $\varphi^\Gamma : K[n-1] \longrightarrow K[n]/P$ e $\psi^\Gamma : K[n]/P \longrightarrow K[n-1]$ sono dati da $\varphi^\Gamma(g) = g + P$ per $g \in K[n-1]$ risp. $\psi^\Gamma(f + P) = f(x_1, \ldots, x_{n-1}, h)$ per $f \in K[n]$. Infatti si ha allora

$$\begin{aligned}\varphi^\Gamma(\psi^\Gamma(f + P) &= \varphi^\Gamma(f(x_1, \ldots, x_{n-1}, h)) = f(x_1, \ldots, x_{n-1}, h) + P \\ &= f(x_1, \ldots, x_n) + P = f + P\end{aligned}$$

$$\psi^\Gamma(\varphi^\Gamma(g)) = \psi^\Gamma(g + P) = g$$

perché in $g + P$ il polinomio g è considerato come elemento di $K[n]$.

Osservazione 28.12. Dimostreremo adesso che le varietà affini K e $\mathrm{Zeri}(xy - 1)$ non sono isomorfe.

Osservazione 28.13. $\mathrm{Zeri}(xy - 1) = \left\{ \left(\alpha, \frac{1}{\alpha}\right) \mid \alpha \in K \setminus 0 \right\}$.

Osservazione 28.14. K sia finito. Allora $|\mathrm{Zeri}(xy - 1)| = |K| - 1$ e quindi le varietà affini K e $\mathrm{Zeri}(xy - 1)$ non sono isomorfe.

Osservazione 28.15. Sia A una K-algebra. Per il lemma 3.12 possiamo assumere che K sia un sottoanello di A. Se A contiene un elemento invertibile che non appartiene a K, allora per $n \in \mathbb{N} + 1$ le K-algebre $K[n]$ ed A non possono essere isomorfe.

Dimostrazione. Sia $u : A \longrightarrow K[n]$ un isomorfismo di K-algebre e sia $e \in A$ un elemento invertibile con $e \notin K$. Allora anche $f := u(e)$ è invertibile.

Per il cor. 8.7 allora $f \in K$ e quindi, siccome u è un isomorfismo di K-algebre, $e = u^{-1}(f) = f \in K$, una contraddizione.

Osservazione 28.16. Siano $|K| > 2$ ed $\alpha \in K$. Allora $x - \alpha \notin \mathcal{J}(\mathrm{Zeri}(xy - 1))$.

Dimostrazione. Altrimenti si avrebbe

$$\mathrm{Zeri}(xy - 1) \overset{14.9}{=} \mathrm{Zeri}(\mathcal{J}(\mathrm{Zeri}(xy - 1))) \subset \mathrm{Zeri}(x - \alpha)$$

Siccome $(1, 1) \in \mathrm{Zeri}(xy - 1)$, allora necessariamente $\alpha = 1$.

Per ipotesi esiste però un elemento $\beta \in K$ con $\beta \neq 0, 1$. Ma allora $\left(\beta, \frac{1}{\beta}\right)$ appartiene a $\mathrm{Zeri}(xy - 1)$ e non a $\mathrm{Zeri}(x - 1)$.

Osservazione 28.17. Per $K = \{0, 1\}$ invece $\mathrm{Zeri}(xy - 1) = \{(1, 1)\}$.

Proposizione 28.18. *Le varietà affini K e $\mathrm{Zeri}(xy - 1)$ non sono isomorfe.*

Dimostrazione. (1) Per $|K| < \infty$ ciò segue dall'oss. 28.14.

(2) Sia K infinito e sia $I := \mathcal{J}(\mathrm{Zeri}(xy-1))$. Siccome $xy-1 \in I$, l'elemento $x \bmod I$ è invertibile in $\Gamma(X) = K[x,y]/I$.

Siccome K è infinito, si ha però $\Gamma(K) = K[x]$, quindi per l'oss. 28.15 è sufficiente dimostrare che $x \bmod I \notin K$, cioè che non esiste $\alpha \in K$ tale che $x - \alpha \in I$. Ciò è stato dimostrato nell'oss. 28.16.

Osservazione 28.19. Il polinomio $xy-1$ è irriducibile.

Dimostrazione. Per la prop. 6.30 le K-algebre $K[x,y]/(xy-1)$ e $K[x]_x$ sono isomorfe.

$K[x]_x$ è però un anello integro per la nota 6.22 (o la nota 19.21).

Nota 28.20. Sia $2 < |K| < \infty$. Allora per l'oss. 28.14 l'insieme $\mathrm{Zeri}(xy-1)$ è un insieme finito con almeno due punti e non può quindi essere irriducibile.

Insieme con l'oss. 28.19 ciò mostra che per un ideale primo P di $K[n]$ l'insieme $\mathrm{Zeri}(P)$ non è necessariamente irriducibile. Per il teorema 15.34 in tal caso $\mathcal{J}(\mathrm{Zeri}(P))$ non può coincidere con P.

In particolare vediamo che per $2 < |K| < \infty$ si ha
$\mathcal{J}(\mathrm{Zeri}(xy-1)) \neq K[x,y]_{\smile}(xy-1)$.

Questo esempio e altri in questo capitolo mostrano che, almeno con gli strumenti che abbiamo sviluppato finora, solo su un campo algebricamente chiuso possiamo descrivere fedelmente concetti geometrici tramite concetti algebrici. La teoria degli schemi supera questa difficoltà e permette di applicare gli strumenti dell'algebra e della teoria delle categorie anche a varietà definite su campi non algebricamente chiusi.

Osservazione 28.21. Vogliamo adesso dimostrare che un'applicazione qualsiasi definita su un sottoinsieme finito di K^n è polinomiale. Ciò implica in particolare che due insiemi affini finiti sono isomorfi se e solo se hanno lo stesso numero di elementi.

Osservazione 28.22. Siano I un ideale di $K[n]$ ed $\alpha \in K^n \setminus \mathrm{Zeri}(I)$.

Allora esiste $f \in I$ tale che $f(\alpha) = 1$.

Dimostrazione. L'ipotesi implica che esiste $g \in I$ tale che $g(\alpha) \neq 0$.

Con $f := \dfrac{1}{g(\alpha)} g$ allora si ha $f \in I$ ed $f(\alpha) = 1$.

Lemma 28.23. *Siano X un sottoinsieme finito di K^n ed $\alpha \in X$.*

Denotiamo con $\chi_\alpha : X \longrightarrow K$ la funzione caratteristica di α in X con valori in K, cioè la funzione definita da

$$\chi_\alpha(\beta) := \begin{cases} 1 & \textit{se } \beta = \alpha \\ 0 & \textit{altrimenti} \end{cases}$$

Allora $\chi_\alpha \in \mathcal{O}(X)$.

Più esplicitamente ciò significa che esiste $f \in K[n]$ tale che per $\beta \in X$ si ha

$$f(\beta) := \begin{cases} 1 & \textit{se } \beta = \alpha \\ 0 & \textit{altrimenti} \end{cases}$$

Dimostrazione. L'insieme $X \setminus \alpha$ è anch'esso finito e quindi algebrico per l'oss. 14.36. Perciò esiste un ideale I di $K[x]$ tale che $X \setminus \alpha = \mathrm{Zeri}(I)$.

Per l'oss. 28.22 possiamo trovare un $f \in I$ tale che $f(\alpha) = 1$. Ma allora $f_{X \longrightarrow K} = \chi_\alpha$.

Teorema 28.24. *Sia X un sottoinsieme finito di K^n. Allora ogni applicazione $\varphi : X \longrightarrow K^m$ è polinomiale.*

Dimostrazione. Per ogni $\alpha \in X$ definiamo la funzione caratteristica χ_α come nel lemma 28.23. Per lo stesso lemma χ_α è una funzione polinomiale.

Per un'applicazione qualsiasi $\varphi : X \longrightarrow K^m$ abbiamo adesso $\varphi = \sum_{\alpha \in X} \varphi(\alpha)\chi_\alpha$ e ciò mostra che φ è polinomiale.

Corollario 28.25. *Due insiemi finiti $X \subset K^n$ ed $Y \subset K^m$ sono isomorfi se e solo se possiedono lo stesso numero di elementi.*

Dimostrazione. (1) È chiaro che insiemi isomorfi devono avere lo stesso numero di elementi.

(2) Sia $|X| = |Y|$. Possiamo assumere $X, Y \neq \emptyset$. Allora esiste una biiezione $\varphi : X \longrightarrow Y$. Per il teorema 28.24 le applicazioni φ e φ^{-1} sono polinomiali.

Osservazione 28.26. Quando nella dimostrazione del teorema 28.24 per ogni $\alpha \in X$ per la costruzione di χ_α ci appelliamo al lemma 28.23, ciò implica che per ogni α dobbiamo trovare un ideale I_α di $K[n]$ tale che $X \setminus \alpha = \mathrm{Zeri}(I_\alpha)$.

In teoria ciò non è difficile, ad esempio ponendo $I_\alpha := \bigcap_{\beta \in X \setminus \alpha} \mathfrak{m}_\beta$ oppure $I_\alpha := \prod_{\beta \in X \setminus \alpha} \mathfrak{m}_\beta$, usando i lemmi 9.6 e 14.5, ma costituisce un considerevole impegno nel calcolo, per cui adesso presenteremo tecniche più efficienti per rappresentare la funzione caratteristica.

Lemma 28.27. *K sia infinito ed X un sottoinsieme finito di K^n.*

Allora esiste un'applicazione lineare $\varphi : K^n \longrightarrow K$ che separa i punti di X, cioè tale che per $\alpha, \beta \in X$ con $\alpha \neq \beta$ si abbia $\varphi(\alpha) \neq \varphi(\beta)$.

Dimostrazione. Sia $X = \{\alpha_1, \ldots, \alpha_m\}$ con gli α_j tutti distinti. Scriviamo ogni α_j come vettore colonna $\alpha_j = \begin{pmatrix} {\alpha_j}^1 \\ \vdots \\ {\alpha_j}^n \end{pmatrix}$. Un'applicazione lineare $\varphi : K^n \longrightarrow K$ può essere rappresentata da un vettore riga $(\lambda_1, \ldots, \lambda_n)$ che possiamo considerare ancora come un elemento di K^n.

L'uguaglianza $\varphi(\alpha_j) = \varphi(\alpha_k)$ significa allora

$$\lambda_1 \alpha_j^1 + \ldots + \lambda_n \alpha_j^n = \lambda_1 \alpha_k^1 + \ldots + \lambda_n \alpha_k^n$$

ovvero

$$(\alpha_j^1 - \alpha_k^1)\lambda_1 + \ldots + (\alpha_j^n - \alpha_k^n)\lambda_n = 0$$

ed è quindi equivalente alla condizione $(\lambda_1, \ldots, \lambda_n) \in \mathrm{Zeri}(f_{jk})$ con $f_{jk} := (\alpha_j^1 - \alpha_k^1)x_1 + \ldots + (\alpha_j^n - \alpha_k^n)x_n$.

Perciò φ separa i punti di X se e solo se

$$(\lambda_1, \ldots, \lambda_n) \notin \bigcup_{j<k} \mathrm{Zeri}(f_{jk}) \overset{14.5}{=} \mathrm{Zeri}(\prod_{j<k} f_{jk}).$$

Per ipotesi gli f_{jk} sono tutti $\neq 0$, per cui anche $g := \prod_{j<k} f_{jk} \neq 0$.

Dal cor. 14.40 segue $\mathrm{Zeri}(g) \neq K^n$ perché per ipotesi K è infinito.

Si noti che per ogni $j < k$ l'insieme $\mathrm{Zeri}(f_{jk})$ è un iperpiano per l'origine, per cui $\mathrm{Zeri}(g)$ è unione di un insieme finito di iperpiani passanti per l'origine; cfr. cor. 14.49.

Esempio 28.28. Sia $X = \left\{ \begin{pmatrix} 7 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 8 \end{pmatrix} \right\} \subset \mathbb{Q}^2$.

Allora l'applicazione lineare $\varphi_{\lambda\mu} := \bigcirc_{(\alpha,\beta)} \lambda\alpha + \mu\beta : \mathbb{Q}^2 \longrightarrow \mathbb{Q}$ separa i punti di X se e solo se

$$(\lambda, \mu) \notin \mathrm{Zeri}((4x+3y)(6x+3y)(4x-3y)(2x)(-6y)(-2x-6y))$$

Osservazione 28.29. Quando nella situazione del lemma 28.27 esiste un i tale che le i-esime coordinate degli elementi di X sono tutte distinte, si può naturalmente scegliere direttamente $\varphi = \pi_i^X = (x_i)_{X \longrightarrow K}$.

Nota 28.30. Siano K infinito, X un sottoinsieme finito di K^n ed $\alpha \in X$. Calcoliamo la funzione caratteristica 28.23 seguendo Cox/Little/O'Shea [18321], p. 43, 46. Per il lemma 28.27 esiste un'applicazione lineare $\varphi : K^n \longrightarrow K$ che separa i punti di X. φ è polinomiale, perciò esiste $g \in K[n]$ con $\varphi = g_{K^n \longrightarrow K}$ (siccome K è infinito, g è univocamente determinato e della forma $g = \lambda_1 x_1 + \ldots + \lambda_n x_n$ con $\lambda_1, \ldots, \lambda_n \in K$). Sia $X' := X \setminus \alpha$. Allora possiamo formare il polinomio

$$f := \prod_{\beta \in X'} \frac{g - \varphi(\beta)}{\varphi(\alpha) - \varphi(\beta)} = \prod_{\beta \in X'} \frac{g - g(\beta)}{g(\alpha) - g(\beta)}$$

Siccome $\varphi(\alpha) \neq \varphi(\beta)$ per ogni $\beta \in X'$, il polinomio f è ben definito. Inoltre evidentemente $f(\alpha) = 1$ ed $f(\beta) = 0$ per $\beta \in X'$.

Esempio 28.31. Consideriamo ancora l'insieme $X \subset \mathbb{Q}^2$ dell'es. 28.28.
Sia $\alpha := \begin{pmatrix} 7 \\ 5 \end{pmatrix}$. L'applicazione lineare $(x-y)_{\mathbb{Q}^2 \longrightarrow \mathbb{Q}}$ separa i punti di X, per cui nella nota 28.30 possiamo porre

$$f := \frac{x-y-1}{2-1} \cdot \frac{x-y+1}{2+1} \cdot \frac{x-y+5}{2+5} = (x-y-1)(x-y+1)(x-y+5)/21$$

Esempio 28.32. Siano $X := \left\{ \alpha := \begin{pmatrix} 7 \\ 5 \end{pmatrix}, \beta := \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \gamma := \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\}$ ed
$Y := \left\{ \alpha' := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \beta' := \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \gamma' := \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$, considerati come sottoinsiemi di $\mathbb{Q}^2$. La biezione $\varphi : X \longrightarrow Y$ sia definita da $\alpha \longmapsto \alpha'$, $\beta \longmapsto \beta'$, $\gamma \longmapsto \gamma'$.

L'applicazione $x_{\mathbb{Q}^2 \longrightarrow \mathbb{Q}}$ separa i punti di X (cfr. oss. 28.29) e con il metodo della nota 28.30 troviamo, con notazioni autoesplicative e identificando funzioni e polinomi,

$$\chi_\alpha = \frac{x-3}{7-3}\cdot\frac{x-1}{7-1} = (x-3)(x-1)/24$$
$$\chi_\beta = \frac{x-7}{3-7}\cdot\frac{x-1}{3-1} = -(x-7)(x-1)/8$$
$$\chi_\gamma = \frac{x-7}{1-7}\cdot\frac{x-3}{1-3} = (x-7)(x-3)/12$$

Perciò

$$\varphi = (\varphi_1, \varphi_2) = \frac{(x-3)(x-1)}{24}\begin{pmatrix}1\\0\end{pmatrix} - \frac{(x-7)(x-1)}{8}\begin{pmatrix}0\\1\end{pmatrix} + \frac{(x-7)(x-3)}{12}\begin{pmatrix}1\\1\end{pmatrix}$$

per cui

$$\begin{aligned}\varphi_1 &= \frac{(x-3)(x-1)}{24} + \frac{(x-7)(x-3)}{12} = \frac{(x-3)(x-1+2x-14)}{24}\\ &= \frac{(x-3)(3x-15)}{24} = \frac{x^2-8x+15}{8}\\ \varphi_2 &= \frac{-(x-7)(x-1)}{8} + \frac{(x-7)(x-3)}{12} = \frac{x-7}{24}(-3x+3+2x-6)\\ &= \frac{x-7}{24}(-x-3) = \frac{-x^2+4x+21}{24}\end{aligned}$$

Per separare i punti di Y usiamo $(x-y)_{\mathbb{Q}^2\longrightarrow\mathbb{Q}}$, ottenendo similmente

$$\chi_{\alpha'} = \frac{x-y+1}{1+1}\cdot\frac{x-y-0}{1-0} = (x-y+1)(x-y)/2$$
$$\chi_{\beta'} = \frac{x-y-1}{-1-1}\cdot\frac{x-y-0}{-1-0} = (x-y-1)(x-y)/2$$
$$\chi_{\gamma'} = \frac{x-y-1}{0-1}\cdot\frac{x-y+1}{0+1} = -(x-y-1)(x-y+1)$$

Perciò

$$\begin{aligned}\varphi^{-1} = (\psi_1, \psi_2) = \frac{(x-y+1)(x-y)}{2}\begin{pmatrix}7\\5\end{pmatrix} + \frac{(x-y-1)(x-y)}{2}\begin{pmatrix}3\\2\end{pmatrix}\\ - (x-y-1)(x-y+1)\begin{pmatrix}1\\2\end{pmatrix}\end{aligned}$$

per cui

$$\begin{aligned}\psi_1 &= \frac{7(x-y+1)(x-y)+3(x-y-1)(x-y)-2(x-y-1)(x-y+1)}{2}\\ &= 4x^2-8xy+4y^2+2x-2y+1\\ \psi_2 &= \frac{5(x-y+1)(x-y)+2(x-y-1)(x-y)-4(x-y-1)(x-y+1)}{2}\\ &= \frac{3x^2-6xy+3y^2+3x-3y+4}{2}\end{aligned}$$

Lemma 28.33. *K sia finito con $|K| = q$ ed $\alpha = (\alpha_1, \ldots, \alpha_n) \in K^n$.*
Sia $f_\alpha := \prod_{1 \le i \le n} (1 - (x_i - \alpha_i)^{q-1})$.

Allora per ogni $\beta \in K^n$ si ha

$$f_\alpha(\beta) = \begin{cases} 1 & \text{se } \beta = \alpha \\ 0 & \text{altrimenti} \end{cases}$$

Dimostrazione. È chiaro che $f_\alpha(\alpha) = 1$. Sia $\beta \neq \alpha$.

Allora esiste un indice i tale che $\alpha_i \neq \beta_i$. Per la nota 14.41 ciò implica $(\alpha_i - \beta_i)^{q-1} = 1$, quindi uno dei fattori in $f_\alpha(\beta)$ si annulla, cosicché necessariamente $f_\alpha(\beta) = 0$.

Nota 28.34. Una *funzione booleana* è una funzione $\varphi : 2^n \longrightarrow 2$, dove con $2 = \{0, 1\}$ denotiamo il campo con 2 elementi. Per il lemma 28.33 la rappresentazione $\varphi = \sum_{\alpha \in 2^n} \varphi(\alpha)\chi_\alpha$, che abbiamo usato nella dimostrazione del teorema 28.24, può essere scritta nella forma $\varphi = f_{2^n \longrightarrow 2}$ con

$$f = \sum_{\alpha \in 2^n} \varphi(\alpha) \prod_{i=1}^{n} (1 + x_i + \alpha_i)$$

Si noti in primo luogo che, essendo i valori $\varphi(\alpha)$ tutti o uguali a 1 o a 0, dobbiamo sommare solo su quegli α nei quali la funzione φ assume il valore 1, per cui, posto $\operatorname{supp} \varphi := \{\alpha \in 2^n \mid \varphi(\alpha) = 1\}$, abbiamo

$$f = \sum_{\alpha \in \operatorname{supp} \varphi} \prod_{i=1}^{n} (1 + x_i + \alpha_i)$$

Se, come d'uso nella teoria delle funzioni booleane, poniamo $\overline{x_i} := 1 + x_i$, con una notazione abbreviata possiamo scrivere

$$f = \sum_{\alpha \in \operatorname{supp} \varphi} \prod_{\alpha_i = 1} x_i \prod_{\alpha_j = 0} \overline{x_j}$$

Questa è esattamente la *forma normale disgiuntiva* della funzione φ. Essa può essere anche scritta nella forma

$$\varphi = \bigvee_{\alpha \in \operatorname{supp} \varphi} \left(\prod_{\alpha_i = 1} x_i \prod_{\alpha_j = 0} \overline{x_j} \right)_{2^n \longrightarrow 2}$$

se con $\bigvee$ denotiamo la formazione del massimo. Infatti i sommandi sono funzioni caratteristiche di elementi distinti e quindi per ogni α al massimo uno di essi è diverso da 0.

Esempio 28.35. Consideriamo la funzione booleana $\varphi : 2^3 \longrightarrow 2$ data dalla tabella

α_1	α_2	α_3	$\varphi(\alpha)$
0	0	0	1
0	0	1	0
0	1	0	1
1	0	0	0
0	1	1	1
1	0	1	1
1	1	0	0
1	1	1	0

Allora φ è rappresentata dal polinomio

$$\begin{aligned} f &= \overline{x_1}\,\overline{x_2}\,\overline{x_3} + \overline{x_1}x_2\overline{x_3} + \overline{x_1}x_2x_3 + x_1\overline{x_2}x_3 \\ &= (1+x_1)(1+x_2)(1+x_3) + (1+x_1)x_2(1+x_3) + (1+x_1)x_2x_3 + x_1(1+x_2)x_3 \\ &= 1 + x_1 + x_3 + x_2x_3 \end{aligned}$$

Osservazione 28.36. La forma normale disgiuntiva di una funzione booleana (e quindi anche il polinomio che abbiamo costruito nella nota 28.34) è in un certo senso una rappresentazione tautologica: essa non è altro che un elenco dei punti in cui la funzione assume il valore 1 e quindi non contiene informazioni che non siano anche immediate dalla tabella della funzione. In particolare la forma normale disgiuntiva non rispecchia direttamente proprietà particolari della funzione (ad esempio proprietà aritmetiche o di simmetria) se non nella stessa misura della tabella. Nonostante ciò essa ha una notevole importanza perché esprime il contenuto della tabella mediante una *formula* che succcessivamente può essere combinata con altre formule o elaborata con le tecniche della teoria classica delle funzioni booleane oppure con gli strumenti dell'algebra commutativa.

Osservazione 28.37. Dal punto di vista numerico l'interpolazione polinomiale multivariata è piuttosto intricata e ancora oggetto della ricerca; si cfr. de Boor [22529], Gasca/Sauer [22352], Ballico [22351], Stetter [18343], p. 404-408.

Interessanti sono anche le tecniche sviluppate nell'ambito dell'*Algebraic Oil Project* (cfr. ad es. Baciu/Kreuzer [22675], Heldt/Kreuzer/Pokutta/Poulisse [20478, 22676] e Kreuzer/Poulisse/Robbiano [22678].) che probabilmente possono essere applicate in molti altri campi, ad esempio nella modellazione matematica di sistemi biologici o nell'interpretazione di dati clinici.

Osservazione 28.38. Sia X un sottoinsieme di K^n. Allora $\mathcal{O}(X)$ è un sottospazio vettoriale di K^X.

Se X è finito, per il teorema 28.24 $\mathcal{O}(X) = K^X$ e quindi in tal caso si ha $\dim_K \mathcal{O}(X) = |X| < \infty$.

Proposizione 28.39. *Sia X un sottoinsieme di K^n.*

Allora $\dim_K \mathcal{O}(X) < \infty$ se e solo se X è finito.

Dimostrazione. Per l'oss. 28.38 dobbiamo dimostrare solo l'implicazione in una direzione. Sia $\dim_K \mathcal{O}(X) < \infty$. Assumiamo, per assurdo, che l'insieme X sia infinito.

Allora possiamo scegliere un sottoinsieme finito $Y \subset X$ tale che si abbia $|Y| > \dim_K \mathcal{O}(X)$.

Per l'oss. 25.22 l'inclusione $i : Y \longrightarrow X$ induce un omomorfismo suriettivo di K-algebre $\mathcal{O}(X) \longrightarrow \mathcal{O}(Y)$ che è in particolare anche un'applicazione K-lineare suriettiva. Ciò implica $\dim_K \mathcal{O}(X) \geq \dim_K \mathcal{O}(Y) \overset{28.38}{=} |Y|$, in contrasto alle ipotesi.

Osservazione 28.40. Siano $n \geq 2$, K algebricamente chiuso ed $f \in K[n]$.

Allora $K[n]_\smile f$ non è un ideale massimale di $K[n]$.

Dimostrazione. Sia $I := K[n]_\smile f$.

(1) Se f è costante, allora $I = 0$ oppure $I = K[n]$, come segue dal cor. 8.6.

(2) Sia f non costante. L'ideale I sia massimale. Per il teorema degli zeri esiste $\alpha = (\alpha_1, \ldots, \alpha_n) \in K^n$ tale che $I = \mathfrak{m}_\alpha$.

Ciò implica che esiste $e_1 \in K[n]$ tale che $x_1 - \alpha_1 = e_1 f$. Per il lemma 8.5 allora f non dipende da $x_2, \ldots, x_n$.

Similmente però esiste $e_2 \in K[n]$ tale che $x_2 - \alpha_2 = e_2 f$ e quindi f non dipende da $x_1, x_3, \ldots, x_n$. Ma ciò implica che f è costante, una contraddizione.

Proposizione 28.41. *Siano $n \geq 2$, K algebricamente chiuso ed $f \in K[n]$ un polinomio non costante.*

Allora gli insiemi $\mathrm{Zeri}(f)$ e $K^n \setminus \mathrm{Zeri}(f)$ sono entrambi infiniti.

Dimostrazione. (1) Siccome sicuramente $\mathrm{Zeri}(f) \neq K^n$, per il cor. 14.48 è sufficiente dimostrare che $\mathrm{Zeri}(f)$ è infinito.

(2) Siccome l'anello $K[n]$ è fattoriale, l'ipotesi su f implica che esistono polinomi irriducibili $g_1, \ldots, g_m \in K[n]$ e $k_1, \ldots, k_m \in \mathbb{N} + 1$ tali che $f = g_1^{k_1} \cdots g_m^{k_m}$. Allora $\mathrm{Zeri}(f) = \mathrm{Zeri}(g_1) \cup \ldots \cup \mathrm{Zeri}(g_m)$, per cui possiamo assumere che f stesso sia irriducibile.

Sia $P := K[n]_\smile f$. Allora p è un ideale primo. Assumiamo, per assurdo, che $\mathrm{Zeri}(f) = \mathrm{Zeri}(P)$ sia finito. Ma questo insieme è irriducibile e quindi deve allora consistere di un solo punto α. Dal teorema degli zeri segue

$$P = \mathcal{J}(\mathrm{Zeri}(P)) = \mathcal{J}(\{\alpha\}) = \mathfrak{m}_\alpha$$

in contrasto con l'oss. 28.40.

Lemma 28.42. *Siano A un anello integro e $g, h \in A[x]$ tali che $gh = ax^n$ con $a \in A \setminus 0$ ed $n \in \mathbb{N}$.*

Allora esistono $b, c \in A$ ed $m \in \mathbb{N}$ tali che $g = bx^m$, $h = cx^{n-m}$, $a = bc$.

Dimostrazione. L'ipotesi implica che g ed h sono $\neq 0$. Perciò possiamo scrivere $g = b_k x^k + \ldots$, $h = c_i x^i + \ldots$, dove i termini indicati con $\ldots$ hanno grado maggiore di k risp. i.

Ma allora il termine di grado minimo di gh è uguale a $b_k c_i x^{k+i}$ e ciò implica l'enunciato.

Proposizione 28.43 (criterio di Eisenstein). *Siano A un anello integro, $P \in \operatorname{Spec} A$ ed $f = a_0x^n + \ldots + a_n \in A[x]$ con $n \geq 1$ un polinomio i cui coefficienti soddisfano le seguenti condizioni:*

(1) $a_0 \notin P$.

(2) $a_1, \ldots, a_n \in P$.

(3) $a_n \notin P^2$.

Allora non esistono polinomi non costanti $g, h \in A[x]$ con $f = gh$.

Dimostrazione. Seguiamo Scheja/Storch [1589], vol. 2, p. 180.

Il punto (1) implica in particolare che $a_0 \neq 0$ e $\operatorname{grado} f = n$.

Assumiamo, per assurdo, che g ed h siano polinomi non costanti in $A[x]$ tali che $f = gh$. Per $e \in A[x]$ denotiamo con $\overline{e}$ l'immagine di e nell'omomorfismo canonico $A[x] \longrightarrow (A/P)[x]$ della prop. 27.9.

Allora $\overline{f} = \overline{g}\overline{h}$. L'ipotesi (2) implica però che $\overline{f} = \overline{a_0}x^n$ e dall'ipotesi (1) segue che $\overline{a_0} \neq 0$.

Siccome l'anello A/P è integro, possiamo applicare il lemma 28.42. Perciò esistono $b, c \in A$ ed $m \in \mathbb{N}$ tali che $\overline{g} = \overline{b}x^m$, $\overline{h} = \overline{c}x^{n-m}$ ed $\overline{a_0} = \overline{b}\overline{c}$.

Osserviamo adesso che necessariamente $m = \operatorname{grado} g$ ed $n - m = \operatorname{grado} h$, perché altrimenti il massimo coefficiente di g o h apparterebbe a P e quindi anche $a_0 \in P$, in contrasto con l'ipotesi (1).

Perciò $m > 0$ ed $n - m > 0$ perché i polinomi g ed h non sono costanti. Ciò implica però che i coefficienti costanti di g e di h appartengono a P, per cui $a_n \in P^2$ in contrasto con l'ipotesi (3).

Esempio 28.44. Sia $\operatorname{car} K = 0$ e siano $n \in \mathbb{N} + 3, d_1, \ldots, d_n \in \mathbb{N} + 1$ ed $a_1, \ldots, a_n \in K \setminus 0$.

Allora il polinomio $a_1x_1^{d_1} + \ldots + a_nx_n^{d_n}$ è irriducibile.

Si noti che l'ipotesi $n \geq 3$ è necessaria, come mostra l'esempio $x^2 - y^2 = (x - y)(x + y)$.

Dimostrazione. Seguiamo Scheja/Storch 1589], vol. 2, p. 181.

(1) Siano $f := a_1x_1^{d_1} + \ldots + a_nx_n^{d_n}$ e $g := a_2x_2^{d_2} + \ldots + a_nx_n^{d_n} \in A$ con $A := K[x_2, \ldots, x_n]$.

(2) Siccome A è fattoriale e g è $\neq 0$ e non invertibile in A, esiste un elemento primo $p \in A$ tale che $p|g$ in A e quindi $g \in Ap := P$, un ideale primo di A.

(3) Assumiamo di aver dimostrato che $p^2 \nmid g$ in A, cioè che $g \notin P^2$.

(4) Siccome sicuramente $a_1 \notin P$, possiamo applicare il criterio di Eisenstein al polinomio $f = a_1x_1^{d_1} + g \in A[x_1]$. Siano quindi $u, v \in K[n]$ tali che $f = uv$. Dal criterio di Eisenstein segue che ad esempio u è costante rispetto ad x_1, ovvero $u \in K[x_2, \ldots, x_n]$.

Ma se allora $v = h_0x_1^m + \ldots + h_m$ con $h_i \in K[x_2, \ldots, x_n]$ per ogni i, necessariamente $h_ou = a_1 \in K$. Ciò implica in particolare che u deve essere costante, cioè $u \in K$.

(5) Dobbiamo ancora dimostrare che $p^2 \nmid g$ in A.

Assumiamo, per assurdo, che esista $e \in A = K[x_2, \ldots, x_n]$ tale che $p^2 e = g = a_2 x_2^{d_2} + \ldots + a_n x_n^{d_n}$. Denotiamo con $'$ la derivata rispetto all'indeterminata x_2. Allora

$$2pp'e + p^2 e' = d_2 a_2 x_2^{d_2 - 1}$$

Ciò implica (essendo $\operatorname{car} K = 0$) che $p = \lambda x_2^k$ per qualche $\lambda \in K$ e $k \in \mathbb{N} + 1$.

D'altra parte però $p | g$ e quindi $a_2 x_2^{d_2} + \ldots + a_n x_n^{d_n}$ dovrebbe essere un multiplo di x_2^k e ciò non è possibile se, come nelle nostre ipotesi, $n \geq 3$.

L'ipotesi che p sia primo non era necessaria al punto (5), ma solo al punto (2) per garantire che l'ideale P sia primo.

Osservazione 28.45. Siano $d, e \in \mathbb{N} + 1$ con $\operatorname{mcd}(d, e) = 1$ ed $a, b \in K \setminus 0$.

Allora il polinomio $ax^d + by^e$ è irriducibile.

Per la dimostrazione rimandiamo a Scheja/Storch 1589], vol. 2, p. 185. Il caso $y^2 - x^m$ con m dispari è stato dimostrato nella nota 24.23.

Definizione 28.46. Il *quoziente* $I : J$ di due ideali generalizzati I e J di un anello commutativo A è definito da

$$I : J := \{a \in A \mid aJ \subset I\}$$

È immediato che $I : J$ è un ideale generalizzato di A e che $I : J = A$ se e solo se $J \subset I$.

Lemma 28.47. *Siano I, J ideali generalizzati di $K[n]$ ed $X := \operatorname{Zeri}(I)$, $Y := \operatorname{Zeri}(J)$. Allora*

$$I : J \subset \mathcal{J}(X \setminus Y)$$

e quindi

$$\overline{X \setminus Y} \subset \operatorname{Zeri}(I : J)$$

Dimostrazione. Sia $f \in I : J$, ovvero $f \in K[n]$ con $fJ \subset I$.

Sia $\alpha \in X \setminus Y$. Allora esiste $g \in J$ tale che $g(\alpha) \neq 0$.

Per ipotesi però $fg \in I$ e quindi $f(\alpha)g(\alpha) = 0$. Ciò implica $f(\alpha) = 0$.

Lemma 28.48. *Siano $X, Y \subset K^n$. Allora $\mathcal{J}(X \setminus \overline{Y})\mathcal{J}(Y) \subset \mathcal{J}(X)$.*

Dimostrazione. Siano $f \in \mathcal{J}(X \setminus \overline{Y})$, $g \in \mathcal{J}(Y)$ ed $\alpha \in X$. Sia $g(\alpha) \neq 0$.

Allora $\alpha \notin \operatorname{Zeri}(\mathcal{J}(Y)) = \overline{Y}$ e quindi $\alpha \in X \setminus \overline{Y}$, per cui $f(\alpha) = 0$.

Proposizione 28.49. *Siano $X, Y \subset K^n$. Allora*

$$\mathcal{J}(X) : \mathcal{J}(Y) = \mathcal{J}(\overline{X} \setminus \overline{Y}) = \mathcal{J}(X \setminus \overline{Y})$$

Dimostrazione. (1) Per il lemma 28.47 abbiamo

$$\mathcal{J}(X) : \mathcal{J}(Y) \subset \mathcal{J}(\operatorname{Zeri}(\mathcal{J}(X)) \setminus \operatorname{Zeri}(\mathcal{J}(Y))) = \mathcal{J}(\overline{X} \setminus \overline{Y})$$

(2) Il lemma 28.48 implica $\mathcal{J}(X \setminus \overline{Y}) \subset \mathcal{J}(X) : \mathcal{J}(Y)$.

D'altra parte però $\mathcal{J}(\overline{X} \setminus \overline{Y}) \subset \mathcal{J}(X \setminus \overline{Y})$, cosicché otteniamo

$\mathcal{J}(\overline{X} \setminus \overline{Y}) \subset \mathcal{J}(X \setminus \overline{Y}) \subset \mathcal{J}(X) : \mathcal{J}(Y) \subset \mathcal{J}(\overline{X} \setminus \overline{Y})$

Proposizione 28.50. *Siano A un anello commutativo ed I, J ideali generalizzati di A. Allora*

$\sqrt{I : J} \subset \sqrt{I} : J = \sqrt{I} : \sqrt{J}$

Dimostrazione. (1) Sia $a \in \sqrt{I : J}$. Allora esiste $n \in \mathbb{N} + 1$ tale che $a^n J \subset I$. Per ogni $b \in J$ allora $a^n b \in I$ e quindi anche $(ab)^n \in I$, per cui $ab \in \sqrt{I}$.

(2) Siano $a \in \sqrt{I} : J$ e $b \in \sqrt{J}$. Allora esiste $n \in \mathbb{N} + 1$ tale che $b^n \in J$, per cui $ab^n \in \sqrt{I}$. Perciò esiste $m \in \mathbb{N} + 1$ con $(ab^n)^m \in I$. Ciò implica $(ab)^{nm} \in I$ e quindi $ab \in \sqrt{I}$.

(3) Ovviamente $\sqrt{I} : \sqrt{J} \subset \sqrt{I} : J$.

Osservazione 28.51. L'inclusione nella prop. 28.50 è tipicamente stretta.

Infatti se gli ideali generalizzati I e J sono distinti, ad esempio $J \not\subset I$, ma hanno lo stesso radicale, allora $\sqrt{I} : \sqrt{J} = A$, mentre $I : J \neq A$ e quindi anche $\sqrt{I : J} \neq A$.

Ad esempio se P è un ideale primo e Q un ideale P-primario con $Q \neq P$, allora si ha $\sqrt{Q : P} \neq A = P : P = \sqrt{Q} : \sqrt{P}$.

Osservazione 28.52. Siano I, J ideali generalizzati di $K[n]$ ed $X := \mathrm{Zeri}(I)$, $Y := \mathrm{Zeri}(J)$.

Allora $\overline{X \setminus Y} \subset \mathrm{Zeri}(\sqrt{I} : J) \subset \mathrm{Zeri}(I : J)$

Dimostrazione. Per l'oss. 12.4 $X = \mathrm{Zeri}(\sqrt{I})$, per cui dal lemma 28.47 otteniamo

$\overline{X \setminus Y} \subset \mathrm{Zeri}(\sqrt{I} : J) \subset \mathrm{Zeri}(I : J)$

Teorema 28.53. *K sia algebricamente chiuso ed I e J due ideali generalizzati di $K[n]$. Siano $X := \mathrm{Zeri}(I)$ ed $Y := \mathrm{Zeri}(J)$.*

Allora $\overline{X \setminus Y} = \mathrm{Zeri}(\sqrt{I} : J)$.

Dimostrazione. Siccome K è algebricamente chiuso, dal teorema degli zeri segue che $\mathcal{J}(X) = \mathcal{J}(\mathrm{Zeri}(I)) = \sqrt{I}$ e similmente $\mathcal{J}(Y) = \sqrt{J}$, cosicché dalla prop. 28.49 si ha $\sqrt{I} : \sqrt{J} = \mathcal{J}(X) : \mathcal{J}(Y) = \mathcal{J}(X \setminus Y)$, perché nelle nostre ipotesi $\overline{X} = X$ e $\overline{Y} = Y$. Perciò

$\mathrm{Zeri}(\sqrt{I} : J) \overset{28.50}{=} \mathrm{Zeri}(\sqrt{I} : \sqrt{J}) = \mathrm{Zeri}(\mathcal{J}(X \setminus Y)) = \overline{X \setminus Y}$

Osservazione 28.54. Se nel teorema 28.53 l'insieme X è irriducibile, l'enunciato diventa banale. Infatti allora $X \setminus Y$ è un aperto e per il lemma 15.4 si ha $\overline{X \setminus Y} = X$ oppure $X \setminus Y = \emptyset$ (il secondo caso è equivalente alla condizione $X \subset Y$).

Infatti il quoziente di ideali è, come mostrano anche l'oss. 28.55 e la nota 28.56, uno strumento per studiare o modificare insiemi che non sono irriducibili senza calcolare esplicitamente la decomposizione di X o di $\sqrt{I}$, la cui esistenza è stata dimostrata nel teorema 16.12 e nel cor. 16.13.

Osservazione 28.55. Siano A un anello commutativo, J un ideale generalizzato di A e $P \in \operatorname{Spec} A$. Allora:

(1) $J \subset P \Longrightarrow P : J = A$.

(2) $J \not\subset P \Longrightarrow P : J = P$.

Dimostrazione. (1) Chiaro.

(2) È chiaro che $P \subset P : J$.

Sia $a \in P : J$. Per ipotesi esiste $b \in J \setminus P$. Allora $ab \in P$ e ciò è possibile solo se $a \in P$, perché P è primo.

Nota 28.56. (1) Per il teorema 16.12 ogni sottoinsieme algebrico X di K^n può essere scritto nella forma $X = X_1 \cup \ldots \cup X_m$, dove gli insiemi X_i sono irriducibili. Sia $Y \subset K^n$ algebrico. Possiamo assumere che gli X_i siano numerati in modo tale che $X_1 \not\subset Y, \ldots, X_r \not\subset Y$ e $X_{r+1} \subset Y, \ldots, X_m \subset Y$. Per l'oss. 28.54 allora

$$\overline{X \setminus Y} = \overline{X_1 \setminus Y} \cup \ldots \cup \overline{X_m \setminus Y} = X_1 \cup \ldots \cup X_r$$

La dimostrazione dell'esistenza degli X_i era però non costruttiva, mentre il teorema 28.53 ci dà (nell'ipotesi che K sia algebricamente chiuso) uno strumento per calcolare l'insieme $\overline{X \setminus Y}$ in modo algebrico.

(2) Similmente, se K è algebricamente chiuso, per il corollario 16.13 ogni ideale radicale I di $K[n]$ può essere scritto nella forma $I = P_1 \cap \ldots \cap P_m$ con ideali primi P_j. Sia J un ideale generalizzato di $K[n]$. Allora possiamo di nuovo assumere che $J \not\subset P_1, \ldots, P_r$ e $J \subset P_{r+1}, \ldots, P_m$. Per il cor. 28.55 allora $I : J = (P_1 \cap \ldots \cap P_m) : J = (P_1 : J) \cap \ldots \cap (P_m : J) = P_1 \cap \ldots \cap P_r$.

Anche qui l'esistenza della decomposizione è stata dimostrata in modo non costruttivo, mentre esistono algoritmi per il calcolo del quoziente di ideali, per i quali rimandiamo a Cox/Little/O'Shea [22313], p. 196-197, Becker/Weispfenning [5737], p. 264-268, Hassett [21988], p. 118-119, Greuel/Pfister [16045], p. 79-81.

(3) Talvolta si riesce anche direttamente a trovare una decomposizione come al punto (1) tramite il quoziente di ideali, come mostrano gli esempi in Cox/Little/O'Shea [22312], p. 205-206, Schenck [16216], p. 15-16, Greuel/Pfister [16045], p. 81-83, Adams /Loustaunau [17310], p. 72-73.

Esempio 28.57. Sia K algebricamente chiuso con $\operatorname{car} K \neq 2$ e sia $C := \operatorname{Zeri}(y^2 - x^3 - x^2)$ il foglio di Cartesio. Dimostriamo che C non è isomorfo alla retta K. Dimostreremo prima che $\Gamma(C)$ è isomorfo alla K-algebra B dei polinomi $f \in K[x]$ per i quali $f(1) = f(-1)$ e poi che B non è isomorfa a $K[x]$.

(1) L'applicazione polinomiale $\varphi := (\varphi_1, \varphi_2) : K \longrightarrow C$ sia definita da $\varphi_1(t) = t^2 - 1$, $\varphi_2(t) = t(t^2 - 1)$. Allora su $C \setminus (0,0)$ esiste l'applicazione inversa data da $\underset{(x,y)}{\bigcirc} \dfrac{y}{x}$.

(2) Il polinomio $y^2 - x^3 - x^2$ è irriducibile e genera quindi $\mathcal{J}(C)$, perché K è algebricamente chiuso. Perciò $\Gamma(C) = K[x,y]/(y^2 - x^3 - x^2)$.

(3) L'applicazione φ è suriettiva, quindi per la prop. 25.14 l'omomorfismo $\varphi^\Gamma : \Gamma(C) \longrightarrow K[x]$ è iniettivo e induce perciò un isomorfismo tra $\Gamma(C)$ ed $\operatorname{Im} \varphi^\Gamma$. Esso è dato da $\varphi^\Gamma(g + \mathcal{J}(C)) = g(x^2 - 1, x(x^2 - 1))$ per ogni $g \in K[x,y]$.

(4) Dimostriamo adesso che $B := \operatorname{Im}\varphi^{\Gamma}$ consiste esattamente di quei polinomi $f \in K[x]$ per i quali $f(1) = f(-1)$:

Sia $f \in B$. Allora esiste $g \in K[x,y]$ tale che $f = g(x^2-1, x(x^2-1))$, per cui $f(1) = g(0,0) = f(-1)$.

Sia viceversa $f \in K[x]$ tale che $f(1) = f(-1)$. Separando i termini di grado pari e quelli di grado dispari in f possiamo scrivere $f = f_1(x^2) + xf_2(x^2)$ con $f_1, f_2 \in K[x]$. Per ipotesi i valori $f(1) = f_1(1) + f_2(1)$ ed $f(-1) = f_1(1) - f_2(1)$ coincidono e ciò implica $f_2(1) = 0$.

Perciò possiamo scrivere $f_2 = (x-1)f_3$ con $f_3 \in K[x]$, per cui

$$\begin{aligned} f &= f_1(x^2) + x(x^2-1)f_3(x^2) \\ &= f_1(x^2-1+1) + x(x^2-1)f_3(x^2-1+1) \in K[x^2-1, x(x^2-1)] = B \end{aligned}$$

(5) Siccome B è isomorfo a $\Gamma(C)$ per il punto (3), è sufficiente dimostrare che la K-algebra B non è isomorfa a $K[x]$.

(6) Sia $u : K[x] \longrightarrow B$ un isomorfismo e sia $f := u(x)$. L'elemento non costante normato di grado minimo in B è x^2, per cui $\operatorname{grado} f = 2$, cosicché $u(x) = a + bx^2$ con $a, b \in K$ e $b \neq 0$. Ma allora $\operatorname{Im} u = K[x^2]$, mentre $x - x^3 \in B \setminus K[x^2]$.

29. Categorie

Categorie: oggetti e morfismi. Categorie concrete (categorie di insiemi). Un elenco di categorie concrete. Ogni insieme parzialmente ordinato è una categoria. Graduazioni. Categorie piccole. La categoria delle relazioni. Inversi a sinistra e a destra di un morfismo. Isomorfismi in una categoria. Monomorfismi ed epimorfismi. In ***Insiemi*** gli epimorfismi sono esattamente le applicazioni suriettive, i monomorfismi esattamente le applicazioni iniettive. In ***Gruppi*** gli epimorfismi coincidono con gli omomorfismi suriettivi, i monomorfismi con gli omomorfismi iniettivi, ma nella categoria ***Haus*** degli spazi di Hausdorff un'applicazione continua è un epimorfismo se è solo se è densa. In una categoria concreta ogni morfismo iniettivo è mono e ogni morfismo suriettivo è epi. La categoria duale. Se un morfismo ha un inverso a destra, allora è epi, e se possiede un inverso a sinistra, allora è mono. In una categoria concreta ogni isomorfismo è biiettivo. Un morfismo si chiama un bimorfismo se è mono ed epi. L'inclusione di un sottoinsieme denso di uno spazio di Hausdorff è un bimorfismo, ma i.g. non un isomorfismo. Se un epimorfismo possiede un inverso a sinistra, allora è un isomorfismo e quindi, per dualità, se un monomorfismo ha un inverso a destra, allora è un isomorfismo. Le definizioni di mono ed epi possono essere così riformulate: Un morfismo $f : X \longrightarrow Y$ è un monomorfismo se e solo se l'applicazione $\mathrm{Hom}(W, f) : \mathrm{Hom}(W, X) \longrightarrow \mathrm{Hom}(W, Y)$ è iniettiva per ogni W e un epimorfismo se e solo se l'applicazione $\mathrm{Hom}(f, Z) : \mathrm{Hom}(Y, Z) \longrightarrow \mathrm{Hom}(X, Z)$ è iniettiva per ogni Z. f possiede invece un inverso a destra se e solo se per ogni W l'applicazione $\mathrm{Hom}(W, f) : \mathrm{Hom}(W, X) \longrightarrow \mathrm{Hom}(W, Y)$ è suriettiva e un inverso a sinistra se e solo se per ogni Z l'applicazione $\mathrm{Hom}(f, Z) : \mathrm{Hom}(Y, Z) \longrightarrow \mathrm{Hom}(X, Z)$ è suriettiva.

Situazione 29.1. Sia $\mathcal{C}$ una categoria (def. 29.3), quando non indicato diversamente.

Nota 29.2. Per la fondazione insiemistica e la definizione precisa del concetto di *classe* (insieme generalizzato) rimandiamo alla letteratura (ad es. Pareigis [5943], p. 178-182, Adámek/Herrrlich/Strecker [22152], p. 13-17, Kashiwara/Schapira [22258], p. 10-11, Schubert [5945], vol. 1, p. 15-22).

Definizione 29.3. Una *categoria* $\mathcal{C}$ consiste dei seguenti ingredienti:

(1) Una classe $\mathrm{Ob}\,\mathcal{C}$, i cui elementi sono detti *oggetti* della categoria. Come d'uso comune, scriveremo spesso semplicemente $X \in \mathcal{C}$ invece di $X \in \mathrm{Ob}\,\mathcal{C}$.

(2) Per ogni coppia ordinata (X, Y) di elementi di $\mathrm{Ob}\,\mathcal{C}$ è dato un insieme $\mathrm{Hom}_{\mathcal{C}}(X, Y)$.

Gli elementi di $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ sono detti *morfismi* da X in Y nella categoria $\mathcal{C}$ o $\mathcal{C}$-morfismi da X ad Y. Essi vengono indicati da frecce come in $X \xrightarrow{f} Y$ o $f : X \longrightarrow Y$.

(3) Per $X, Y, X', Y' \in \mathcal{C}$ con $(X, Y) \neq (X', Y')$ si chiede che si abbia $\mathrm{Hom}_{\mathcal{C}}(X, Y) \cap \mathrm{Hom}_{\mathcal{C}}(X', Y') = \emptyset$.

(4) Per ogni tripla $X, Y, Z \in \mathcal{C}$ è data un'applicazione

$$\begin{array}{rcl} \mathrm{Hom}_{\mathcal{C}}(X, Y) \times \mathrm{Hom}_{\mathcal{C}}(Y, Z) & \longrightarrow & \mathrm{Hom}_{\mathcal{C}}(X, Z) \\ (f, g) & \longmapsto & gf \end{array}$$

(*composizione di morfismi*).

(5) Per $X \in \mathcal{C}$ è distinto un morfismo $\mathrm{id}_X \in \mathrm{Hom}_{\mathcal{C}}(X, X)$ che si chiama l'*identità* di X.

Quando è necessario indicare anche $\mathcal{C}$, scriviamo $\mathrm{id}_X^{\mathcal{C}}$ invece di id_X.

(6) Se $X \xrightarrow{f} Y$, $Y \xrightarrow{g} Z$, $Z \xrightarrow{h} U$ sono morfismi in $\mathcal{C}$, allora $(hg)f = h(gf)$.

(7) Se $X \xrightarrow{f} Y$ è un morfismo in $\mathcal{C}$, allora $f\,\mathrm{id}_X = f = \mathrm{id}_Y\, f$.

Definizione 29.4. La categoria $\mathcal{C}$ è detta *concreta*, quando è una categoria di insiemi e applicazioni nel senso seguente:

(1) Per ogni $X \in \mathcal{C}$ è definito in modo univoco un insieme $\widetilde{X}$.

(2) $\mathrm{Hom}_{\mathcal{C}}(X, Y) \subset \widetilde{Y}^{\widetilde{X}}$ per ogni $X, Y \in \mathcal{C}$.

(3) La composizione di morfismi in $\mathcal{C}$ coincide con la composizione di applicazioni.

(4) $\mathrm{id}_X^{\mathcal{C}} = \mathrm{id}_{\widetilde{X}}^{\textit{Insiemi}}$ per ogni $X \in \mathcal{C}$.

Questa definizione si trova ad es. in Semadeni/Wiweger [1141], p. 47.

Note 29.5. Elenchiamo adesso alcune delle categorie più importanti. Esse sono tutte concrete.

$\mathcal{C}$	$\mathrm{Ob}\,\mathcal{C}$	morfismi
Insiemi	insiemi	applicazioni
Insiemifiniti	insiemi finiti	applicazioni
Ipo	insiemi parzialmente ordinati	applicazioni monotone
Reticoli	reticoli	omomorfismi di reticoli
Top	spazi topologici	applicazioni continue
Haus	spazi di Hausdorff	applicazioni continue
Unif	spazi uniformi	applicazioni uniformemente continue
Semigruppi	semigruppi	omomorfismi di semigruppi
Monoidi	monoidi	omomorfismi di monoidi
Gruppi	gruppi	omomorfismi di gruppi
Ab	gruppi abeliani	omomorfismi di gruppi
$\boldsymbol{Mod}_A$	moduli su un anello A	applicazioni A-lineari
A–***Algebre***	algebre su un anello A	omomorfismi di A-algebre
Anelli	anelli	omomorfismi di anelli
Ancomm	anelli commutativi	omomorfismi di anelli
Mis	spazi misurabili	applicazioni misurabili
Diff	varietà differenziabili	applicazioni differenziabili

Esempio 29.6. Da un insieme parzialmente ordinato P otteniamo una categoria $\mathcal{C}$ nel modo seguente:

(1) $\mathrm{Ob}\,\mathcal{C} := P$.

(2) $\mathrm{Hom}_{\mathcal{C}}(a, b) := \begin{cases} \{(a, b)\} & \text{if } a \leq b \\ \emptyset & \text{altrimenti} \end{cases}$

$f \in \mathrm{Hom}_{\mathcal{C}}(a, b)$, $g \in \mathrm{Hom}_{\mathcal{C}}(b, c)$ significa quindi $a \leq b \leq c$, $f = (a, b)$ e $g = (b, c)$, cosicché possiamo definire $gf := (a, c)$. Dalla transitività di $\leq$ segue che questa composizione è ben definita e dalla riflessività abbiamo $\mathrm{id}_a^{\mathcal{C}} = (a, a)$.

Nella teoria dei fasci si usa il seguente caso speciale: Se X è uno spazio topologico, allora consideriamo l'insieme di tutti gli aperti di X ordinato mediante inclusione insiemistica.

Definizione 29.7. Una *graduazione* è una tripla (X, S, τ), dove X è un insieme, S è un monoide e $\tau \subset X \times S \times X$ è una relazione che soddisfa le seguenti condizioni, dove scriviamo $(x, y) \in s$ invece di $(x, s, y) \in \tau$, per ogni $x, y, z \in X$ ed ogni $s, t \in S$:

(1) $(x, x) \in 1_S$.

(2) $(x, y) \in s$ and $(y, z) \in t \implies (x, z) \in st$.

Graduazioni appaiono molto frequentemente in matematica, come mostrano gli esempi in Leardini [21719], p. 23-26.

Esempio 29.8. Da una graduazione (X, S, τ) otteniamo direttamente una categoria:

(1) $\mathrm{Ob}\,\mathcal{C} := X$.

(2) $\mathrm{Hom}_{\mathcal{C}}(x, y) := \{(x, y, s) \mid s \in S \text{ con } (x, y) \in s\}$.

Per $(x, y) \in s$ ed $(y, z) \in t$ definiamo la composizione

$$(y, z, t)(x, y, s) := (x, z, st)$$

Per $x \in X$ si ha $\mathrm{id}_x^{\mathcal{C}} = (x, x, 1_S)$.

Definizione 29.9. La categoria $\mathcal{C}$ è detta *piccola* se $\mathrm{Ob}\,\mathcal{C}$ è un insieme.

Le categorie degli esempi 29.6 e 29.8 sono piccole e non concrete. Nessuna delle categorie nella nota 29.5 è piccola.

Esempio 29.10. La categoria delle relazioni. Definiamo una categoria ***Rel*** nel modo seguente:

(1) $\mathrm{Ob}\,\textbf{\textit{Rel}} := \mathrm{Ob}\,\textbf{\textit{Insiemi}}$.

(2) $\mathrm{Hom}_{\textbf{\textit{Rel}}}(X, Y) := \{(X, Y, R) \mid R \subset X \times Y\}$.

(3) Per $R \subset X \times Y$, $S \subset Y \times Z$ definiamo la composizione mediante

$$(Y, Z, S)(X, Y, R) := (X, Z, T)$$

dove $T := \{(x, z) \mid \text{ esiste } y \in Y \text{ con } (x, y) \in R, (y, z) \in S\}$.

Definizione 29.11. Siano $X, Y \in \mathcal{C}$ ed $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y, X)$.

(1) g si chiama un *inverso destro* di f se $fg = \mathrm{id}_Y$ ed un *inverso sinistro* di f se $gf = \mathrm{id}_X$.

g è detto un *inverso* di f se è allo stesso tempo inverso a destra e a sinistra di f.

(2) f si chiama un *isomorfismo* se possiede un inverso.

Osservazione 29.12. Siano $X, Y \in \mathcal{C}$ ed $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

Siano $g, h \in \mathrm{Hom}_{\mathcal{C}}(Y, X)$ tali che $fg = \mathrm{id}_Y$ ed $hf = \mathrm{id}_X$. Allora $g = h$.

Concludiamo in particolare che f è un isomorfismo e che il suo inverso, che denoteremo con f^{-1}, è univocamente definito.

Dimostrazione. $h = h\,\mathrm{id}_Y = hfg = \mathrm{id}_X\, g = g$.

Definizione 29.13. Siano $X, Y \in \mathcal{C}$ ed $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

(1) f si chiama un *monomorfismo*, se per ogni $W \in \mathcal{C}$ ed ogni coppia di morfismi $g, h \in \mathrm{Hom}_{\mathcal{C}}(W, X)$ dall'uguaglianza $fg = fh$ segue $g = h$.

Più brevemente diremo allora anche che f è *mono*.

(2) f si chiama un *epimorfismo*, se per ogni $Z \in \mathcal{C}$ ed ogni coppia di morfismi $g, h \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$ l'uguaglianza $gf = hf$ implica $g = h$.

Diremo allora anche che f è *epi*.

Nota 29.14. (1) In ***Insiemi*** gli epimorfismi sono esattamente le applicazioni suriettive, i monomorfismi esattamente le applicazioni iniettive.

(2) In ***Gruppi*** gli epimorfismi coincidono con gli omomorfismi suriettivi, i monomorfismi con gli omomorfismi iniettivi.

(3) Un'applicazione continua $f : X \longrightarrow Y$ tra spazi di Hausdorff è un epimorfismo in ***Haus*** se e solo se $f(X)$ è denso in Y.

(4) In una categoria concreta ogni morfismo iniettivo è mono e ogni morfismo suriettivo è epi.

Dimostrazione. Per esempio Leardini [21719], p. 50-52.

Definizione 29.15. La categoria *duale* (o *opposta*) $\mathcal{C}^{\mathrm{opp}}$ si ottiene nel modo seguente:

(1) $\mathrm{Ob}\,\mathcal{C}^{\mathrm{opp}} := \mathrm{Ob}\,\mathcal{C}$.

(2) $\mathrm{Hom}_{\mathcal{C}^{\mathrm{opp}}}(X, Y) := \mathrm{Hom}_{\mathcal{C}}(Y, X)$.

(3) Per $f \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{opp}}}(X, Y)$, $g \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{opp}}}(Y, Z)$ la composizione è definita mediante $(gf, \mathrm{in}\,\mathcal{C}^{\mathrm{opp}}) := (fg, \mathrm{in}\,\mathcal{C})$.

Osservazione 29.16. Siano $X, Y \in \mathcal{C}$ ed $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

(1) Se f ha un inverso a destra, allora f è epi.

(2) Se f ha un inverso a sinistra, allora f è mono.

Dimostrazione. (1) Siano $g, h : Y \longrightarrow Z$ tali che $gf = hf$.

Per ipotesi esiste $u : Y \longrightarrow X$ tale che $fu = \mathrm{id}_Y$. Allora

$g = g\,\mathrm{id}_Y = gfu = hfu = h\,\mathrm{id}_Y = h$.

(2) Per dualità, siccome un epimorfismo in $\mathcal{C}$ è la stessa cosa come un monomorfismo in $\mathcal{C}^{\mathrm{opp}}$, ecc.

Osservazione 29.17. In una categoria concreta ogni isomorfismo è biiettivo.

Proof. Chiaro, perché un'applicazione con un'inversa sinistra è iniettiva e un'applicazione con un'inversa destra è suriettiva.

Definizione 29.18. Siano $X, Y \in \mathcal{C}$ ed $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

f si chiama un *bimorfismo* se è allo stesso tempo mono ed epi.

Osservazione 29.19. Ogni isomorfismo è un bimorfismo.

Dimostrazione. Ciò segue dall'oss. 29.16.

Esempio 29.20. Siano X uno spazio di Hausdorff ed A un sottoinsieme denso di X.

Allora l'inclusione $i : A \longrightarrow X$ è un bimorfismo in ***Haus***.

Se $A \neq X$, allora i non è un isomorfismo.

Dimostrazione. (1) L'inclusione è iniettiva e quindi mono per il punto (4) della nota 29.14. Essa è epi per il punto (3) della stessa nota.

(2) Se $A \neq X$, l'inclusione non è un isomorfismo per l'oss. 29.17.

Osservazione 29.21. (1) Se un epimorfismo possiede un inverso a sinistra, allora è un isomorfismo.

(2) Se un monomorfismo ha un inverso a destra, allora è un isomorfismo.

Dimostrazione. (1) Siano $X, Y \in \mathcal{C}$, $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ epi e $g \in \mathrm{Hom}_{\mathcal{C}}(Y, X)$ tali che $gf = \mathrm{id}_X$. Allora $\mathrm{id}_Y f = f = f\,\mathrm{id}_X = fgf$.

Per ipotesi f è epi, cosicché $fg = \mathrm{id}_Y$.

(2) Per dualità.

Osservazione 29.22. Siano $X, Y \in \mathcal{C}$ ed $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

(1) f è mono se e solo se per ogni $W \in \mathcal{C}$ l'applicazione
$\mathrm{Hom}_{\mathcal{C}}(W, f) := \bigcirc_g fg : \mathrm{Hom}_{\mathcal{C}}(W, X) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(W, Y)$ è iniettiva.

(2) f è epi se e solo se per ogni $Z \in \mathcal{C}$ l'applicazione
$\mathrm{Hom}_{\mathcal{C}}(f, Z) := \bigcirc_g gf : \mathrm{Hom}_{\mathcal{C}}(Y, Z) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(X, Z)$ è iniettiva.

Dimostrazione. Ciò segue direttamente dalla def. 29.13.

Proposizione 29.23. *Siano $X, Y \in \mathcal{C}$ ed $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.*

(1) f possiede un inverso a destra se e solo se per ogni $W \in \mathcal{C}$ l'applicazione
$\mathrm{Hom}_{\mathcal{C}}(W, f) = \bigcirc_g fg : \mathrm{Hom}_{\mathcal{C}}(W, X) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(W, Y)$ *è suriettiva.*

(2) f possiede un inverso a sinistra se e solo se per ogni $Z \in \mathcal{C}$ l'applicazione
$\mathrm{Hom}_{\mathcal{C}}(f, Z) = \bigcirc_g gf : \mathrm{Hom}_{\mathcal{C}}(Y, Z) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(X, Z)$ *è suriettiva.*

Dimostrazione. (1) Assumiamo che f sia invertibile a destra, ad es. $fu = \mathrm{id}_Y$ per qualche $u \in \mathrm{Hom}_{\mathcal{C}}(Y, X)$. Siano $W \in \mathcal{C}$ ed $h : W \longrightarrow Y$.
Allora $h = \mathrm{id}_Y h = fuh$, quindi h appartiene all'immagine di $\bigcirc_g fg$.

Se viceversa la seconda condizione al punto (1) è soddisfatta, allora in particolare l'applicazione $\bigcirc_g fg : \mathrm{Hom}_{\mathcal{C}}(Y, X) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(Y, Y)$ è suriettiva.

Perciò esiste $u \in \mathrm{Hom}_{\mathcal{C}}(Y, X)$ tale che $fu = \mathrm{id}_Y$.

(2) Per dualità.

30. Funtori e trasformazioni naturali

Funtori covarianti e funtori controvarianti. I funtori $\mathrm{Hom}_{\mathcal{C}}(W,-)$ e $\mathrm{Hom}_{\mathcal{C}}(-,Z)$. L'insieme delle parti come caso speciale e corrispondente al funtore controvariante $\mathrm{Hom}_{\textit{Insiemi}}(-,2)$. Funtori definiti su un insieme parzialmente ordinato. Il gruppo di omologia di uno spazio topologico. Funtori fedeli e pienamente fedeli. Una categoria concreta può essere considerata come data da una coppia $(\mathcal{C},\mathcal{T})$, in cui $\mathcal{C}$ è una categoria e $\mathcal{T}:\mathcal{C}\longrightarrow\textit{Insiemi}$ è un funtore covariante fedele. Se $\mathcal{F}:\mathcal{C}\longrightarrow\mathcal{D}$ è un funtore covariante ed X,Y sono oggetti isomorfi in $\mathcal{C}$, allora $\mathcal{F}(X)$ ed $\mathcal{F}(Y)$ sono isomorfi in $\mathcal{D}$: categorie e funtori sono lo strumento del matematico per confrontare strutture di tipo differente e per la costruzione di invarianti. Composizione di funtori. Categorie isomorfe (un concetto raramente utile). Trasformazioni naturali. Prodotto di Hadamard di trasformazioni naturali. Isomorfismi di funtori. Costruzione diretta della composizione di due trasformazioni naturali. Se $\mathcal{F},\mathcal{G}:\mathcal{C}\longrightarrow\mathcal{D}$ sono due funtori covarianti ed $\eta:\mathcal{F}\longrightarrow\mathcal{G}$ è una trasformazione naturale, per $f\in\mathrm{Hom}_{\mathcal{C}}(X,Y)$ possiamo definire un morfismo $\eta_f:\mathcal{F}(X)\longrightarrow\mathcal{G}(Y)$ ponendo $\eta_f:=\eta_Y\mathcal{F}(f)=\mathcal{G}(f)\eta_X$. Si ha allora la relazione $\mathcal{G}(g)\eta_f=\eta_g\mathcal{F}(f)$. Queste relazioni caratterizzano le trasformazioni naturali. Composizione di trasformazioni naturali mediante $\theta\circ\eta:=\bigcirc_f\theta_{\eta_f}$. La relazione $(\theta*\eta)_{gf}=\theta_g\eta_f$. Legge distributiva: $(\theta'*\theta)\circ(\eta'*\eta)=(\theta'\circ\eta')*(\theta\circ\eta)$.

Situazione 30.1. $\mathcal{C},\mathcal{D},\mathcal{C}_1,\mathcal{C}_2,\mathcal{C}_3$ siano categorie.

Nella trattazione delle trasformazioni naturali seguiamo soprattutto Pumplün [16260], p. 81-99.

Definizione 30.2. Un *funtore covariante* $\mathcal{F}:\mathcal{C}\longrightarrow\mathcal{D}$ consiste dei seguenti dati:

(1) Ad ogni oggetto $X\in\mathcal{C}$ è associato un oggetto $\mathcal{F}(X)\in\mathcal{D}$.

(2) Ad ogni morfismo $f:X\longrightarrow Y$ in $\mathcal{C}$ è associato un morfismo

$\mathcal{F}(f):\mathcal{F}(X)\longrightarrow\mathcal{F}(Y)$ in modo tale che $\mathcal{F}(\mathrm{id}_X)=\mathrm{id}_{\mathcal{F}(X)}$

e $\mathcal{F}(gf)=\mathcal{F}(g)\mathcal{F}(f)$ se gf è definito in $\mathcal{C}$.

Definizione 30.3. Un *funtore controvariante* $\mathcal{F}:\mathcal{C}\longrightarrow\mathcal{D}$ consiste dei seguenti dati:

(1) Ad ogni oggetto $X\in\mathcal{C}$ è associato un oggetto $\mathcal{F}(X)\in\mathcal{D}$.

(2) Ad ogni morfismo $f:X\longrightarrow Y$ in $\mathcal{C}$ è associato un morfismo

$\mathcal{F}(f):\mathcal{F}(Y)\longrightarrow\mathcal{F}(X)$ in modo tale che $\mathcal{F}(\mathrm{id}_X)=\mathrm{id}_{\mathcal{F}(X)}$

e $\mathcal{F}(gf)=\mathcal{F}(f)\mathcal{F}(g)$ se gf è definito in $\mathcal{C}$.

Nota 30.4. Sia $W\in\mathcal{C}$ un oggetto fissato di $\mathcal{C}$. Per ogni $X\in\mathcal{C}$ allora $\mathrm{Hom}_{\mathcal{C}}(W,X)$ è un insieme ed ogni morfismo $f:X\longrightarrow Y$ in $\mathcal{C}$ induce un'applicazione canonica $\mathrm{Hom}_{\mathcal{C}}(W,f)=\bigcirc_g fg:\mathrm{Hom}_{\mathcal{C}}(W,X)\longrightarrow\mathrm{Hom}_{\mathcal{C}}(W,Y)$ che abbiamo già visto nell'oss. 29.22 e nella prop. 29.23.

Per morfismi $f_1:X\longrightarrow Y$, $f_2:Y\longrightarrow Z$ e $g:W\longrightarrow X$ in $\mathcal{C}$ si ha inoltre $\mathrm{Hom}_{\mathcal{C}}(W,f_2f_1)(g)=f_2f_1g=\mathrm{Hom}_{\mathcal{C}}(W,f_2)(\mathrm{Hom}_{\mathcal{C}}(W,f_1)(g))$, per cui

$$\mathrm{Hom}_{\mathcal{C}}(W,f_2f_1)=\mathrm{Hom}_{\mathcal{C}}(W,f_2)\circ\mathrm{Hom}_{\mathcal{C}}(W,f_1)$$

Infine $\mathrm{Hom}_{\mathcal{C}}(W,\mathrm{id}_X)(g)=\mathrm{id}_X\,g=g$ e quindi $\mathrm{Hom}_{\mathcal{C}}(W,\mathrm{id}_X)=\mathrm{id}_{\mathrm{Hom}_{\mathcal{C}}(W,X)}$.

Ciò mostra che

$$\mathrm{Hom}_{\mathcal{C}}(W,-) := (\bigcirc_X \mathrm{Hom}_{\mathcal{C}}(W,X), \bigcirc_f \mathrm{Hom}_{\mathcal{C}}(W,f))$$

è un funtore covariante $\mathcal{C} \longrightarrow$ ***Insiemi***.

Nota 30.5. Sia $Z \in \mathcal{C}$ un oggetto fissato di $\mathcal{C}$. Come nella nota 30.4 otteniamo allora un funtore controvariante $\mathcal{C} \longrightarrow$ ***Insiemi*** ponendo

$$\mathrm{Hom}_{\mathcal{C}}(-,Z) := (\bigcirc_X \mathrm{Hom}_{\mathcal{C}}(X,Z), \bigcirc_f \mathrm{Hom}_{\mathcal{C}}(f,Z))$$

Osservazione 30.6. Spesso per $X, Y \in \mathcal{C}$ gli insiemi $\mathrm{Hom}_{\mathcal{C}}(X,Y)$ possono essere dotati di una struttura (ad esempio algebrica o topologica) aggiuntiva in modo che appartengano a un'altra categoria $\mathcal{D}$. In tal caso i funtori covarianti risp. controvarianti (detti funtori Hom) delle note 30.4 e 30.5 diventano funtori $\mathcal{C} \longrightarrow \mathcal{D}$.

Mentre quindi l'uso dei funtori Hom ci permette di riportare questioni che vogliamo studiare nella categoria $\mathcal{C}$ a concetti insiemistici, esso in molti casi significa anche un arricchimento di struttura.

Esempio 30.7. Per un insieme X denotiamo, come sempre, con $\mathcal{P}(X)$ l'insieme delle parti di X. Se $f : X \longrightarrow Y$ è un'applicazione, possiamo definire l'applicazione

$$\mathcal{P}(f) := \bigcirc_B f^{-1}(B) : \mathcal{P}(Y) \longrightarrow \mathcal{P}(X)$$

Dalle relazioni $(g \circ f)^{-1}(C) = f^{-1}(g^{-1}(C))$ e $(\mathrm{id}_X)^{-1}(A) = A$ segue che $\mathcal{P} := (\bigcirc_X \mathcal{P}(X), \bigcirc_f \mathcal{P}(f))$ è un funtore controvariante ***Insiemi*** $\longrightarrow$ ***Insiemi***.

Esso può essere considerato come un esempio del funtore controvariante della nota 30.5, se, scrivendo $\{0,1\} = 2$, identifichiamo $\mathcal{P}(X)$ con $2^X = \mathrm{Hom}_{\textit{Insiemi}}(X,2)$, facendo corrispondere ogni sottoinsieme $A \subset X$ alla funzione caratteristica χ_A ed ogni $f \in 2^X$ all'insieme $(f = 1) = f^{-1}(1)$.

Per un'applicazione $f : X \longrightarrow Y$, $B \subset Y$ ed $x \in X$ abbiamo allora

$$(\chi_B \circ f)(x) = 1 \iff f(x) \in B \iff x \in f^{-1}(B) \iff \chi_{f^{-1}(B)}(x) = 1$$

cosicché effettivamente

$$\mathrm{Hom}_{\textit{Insiemi}}(f,2)(\chi_B) = \chi_B \circ f = \chi_{f^{-1}(B)} = \chi_{\mathcal{P}(f)}$$

In questo senso i funtori controvarianti $\mathcal{P}$ e $\mathrm{Hom}_{\textit{Insiemi}}(-,2)$ coincidono.

Pur rimanendo ancora in ambiente insiemistico, il passaggio da X a $\mathcal{P}(X)$ permette spesso operazioni nuove, perché $\mathcal{P}(X)$ è più ricco di struttura di X.

Più in generale, se K è un campo, ad ogni applicazione $f : X \longrightarrow Y$ tra insiemi possiamo associare il funtore controvariante

$$\mathrm{Hom}_{\textit{Insiemi}}(-,K) = (\bigcirc_X K^X, \bigcirc_f \mathrm{Hom}_{\textit{Insiemi}}(f,K)) = (\bigcirc_X K^X, \bigcirc_f \bigcirc_\eta \eta \circ f)$$

e sfruttare successivamente la struttura di spazio vettoriale su K^X.

Esempio 30.8. Siano $(P, \leq)$ un insieme parzialmente ordinato e $\mathcal{D}$ una categoria. Se consideriamo P come una categoria come nell'esempio 29.6, allora un funtore covariante $\mathcal{F} : P \longrightarrow \mathcal{D}$ è dato nel seguente modo:

(1) Ad ogni $a \in P$ è associato un oggetto $\mathcal{F}(a) \in \mathcal{D}$.

(2) Per $a, b \in P$ con $a \leq b$ è definito un morfismo $\rho_{ab} : \mathcal{F}(a) \longrightarrow \mathcal{F}(b)$ tale che $\rho_{aa} = \mathrm{id}_{\mathcal{F}(a)}$ e $\rho_{bc}\rho_{ab} = \rho_{ac}$ se $a \leq b \leq c$.

Un funtore controvariante $P \longrightarrow \mathcal{D}$ è la stessa cosa come un funtore covariante $P^{\mathrm{opp}} \longrightarrow \mathcal{D}$, dove con P^{opp} denotiamo l'insieme parzialmente ordinato $(P, \leq^{\mathrm{opp}})$ in cui $a \leq^{\mathrm{opp}} b \iff b \leq a$ oppure, equivalentemente, la categoria duale a P come nella def. 29.15.

Esempio 30.9. In topologia algebrica ad ogni spazio topologico X per ogni $n \in \mathbb{N}$ si associa un gruppo abeliano $H_n(X)$, detto n-esimo *gruppo di omologia* di X, e ad ogni applicazione continua $f : X \longrightarrow Y$ un omomorfismo di gruppi $H_n(f) : H_n(X) \longrightarrow H_n(Y)$ in modo tale che $H_n : \boldsymbol{Top} \longrightarrow \boldsymbol{Ab}$ sia un funtore covariante.

Definizione 30.10. $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ sia un funtore covariante. Per ogni $X, Y \in \mathcal{C}$ possiamo allora definire un'applicazione

$$\begin{aligned} \mathcal{F}_{XY} : \mathrm{Hom}_{\mathcal{C}}(X, Y) &\longrightarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{F}(X), \mathcal{F}(Y)) \\ f &\longmapsto \mathcal{F}(f) \end{aligned}$$

$\mathcal{F}$ si dice

(1) *fedele*, se l'applicazione $\mathcal{F}_{XY}$ è iniettiva per ogni $X, Y \in \mathcal{C}$;

(2) *pienamente fedele*, se l'applicazione $\mathcal{F}_{XY}$ è biiettiva per ogni $X, Y \in \mathcal{C}$.

Esempio 30.11. Utilizzando il concetto di funtore, la def. 29.4 può essere riformulata in modo più preciso: Una *categoria concreta* è una coppia $(\mathcal{C}, \mathcal{T})$, in cui $\mathcal{C}$ è una categoria e $\mathcal{T} : \mathcal{C} \longrightarrow \boldsymbol{Insiemi}$ è un funtore covariante fedele (che *trascura* la struttura non insiemistica di $\mathcal{C}$).

La condizione che $\mathcal{T}$ sia fedele ci permette di considerare $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ come sottoinsieme di $\mathcal{T}(Y)^{\mathcal{T}(X)}$. Nella def. 29.4 abbiamo scritto $\widetilde{X}$ invece di $\mathcal{T}(X)$.

Lemma 30.12. *Siano $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ un funtore covariante, $X, Y \in \mathcal{C}$ ed $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ un isomorfismo.*

Allora $\mathcal{F}(f)$ è un isomorfismo in $\mathcal{D}$ con $(\mathcal{F}(f))^{-1} = \mathcal{F}(f^{-1})$.

Dimostrazione. Infatti

$$\mathcal{F}(f)\mathcal{F}(f^{-1}) = \mathcal{F}(ff^{-1}) = \mathcal{F}(\mathrm{id}_Y) = \mathrm{id}_{\mathcal{F}(Y)}$$

e

$$\mathcal{F}(f^{-1})\mathcal{F}(f) = \mathcal{F}(f^{-1}f) = \mathcal{F}(\mathrm{id}_X) = \mathrm{id}_{\mathcal{F}(X)}$$

Proposizione 30.13. *$\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ sia un funtore covariante ed X, Y oggetti isomorfi in $\mathcal{C}$.*

Allora $\mathcal{F}(X)$ ed $\mathcal{F}(Y)$ sono isomorfi in $\mathcal{D}$.

Dimostrazione. Ciò segue direttamente dal lemma 30.12.

Osservazione 30.14. Categorie e funtori sono lo strumento del matematico per confrontare strutture di tipo differente (spesso attraverso l'introduzione

di invarianti numerici o dotati di struttura - ciò avviene in modo sistematico attraverso le tecniche dell'algebra omologica che si basano fortemente sulle costruzioni della teoria delle categorie). Sia ad esempio $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ un funtore covariante e siano $X, Y \in \mathcal{C}$. Supponiamo di voler dimostrare che X ed Y non sono isomorfi in $\mathcal{C}$. Per la prop. 30.13 è sufficiente dimostrare che gli oggetti $\mathcal{F}(X)$ ed $\mathcal{F}(Y)$ non sono isomorfi in $\mathcal{D}$.

Molto spesso $\mathcal{D}$ è una categoria concreta (per esempio di gruppi o anelli) ed è talvolta relativamente facile decidere se $\mathcal{F}(X)$ ed $\mathcal{F}(Y)$ possano essere isomorfi - sicuramente non lo sono se possiedono cardinalità diverse oppure se $\mathcal{F}(X)$ è un gruppo ciclico ed $\mathcal{F}(Y)$ non è ciclico oppure se $\mathcal{F}(X)$ è un anello integro ed $\mathcal{F}(Y)$ contiene divisori di zero.

Osservazione 30.15. È ovvio come si definisce la composizione di due funtori covarianti.

Per ogni categoria $\mathcal{C}$ è inoltre definito il funtore (covariante) identico $\mathrm{Id}_{\mathcal{C}} := (\bigcirc\limits_{X} X, \bigcirc\limits_{f} f)$.

Definizione 30.16. Due categorie $\mathcal{C}$ e $\mathcal{D}$ si dicono *isomorfe*, se esistono funtori covarianti $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ e $\mathcal{G} : \mathcal{D} \longrightarrow \mathcal{F}$ tali che $\mathcal{G}\mathcal{F} = \mathrm{Id}_{\mathcal{C}}$ e $\mathcal{F}\mathcal{G} = \mathrm{Id}_{\mathcal{D}}$.

Ci si convince però facilmente che nelle applicazioni della teoria delle categorie questa condizione è troppo restrittiva come osservato ad esempio in Gelfand/Manin [21952], p. 70-71, e in Pumplün [16260], p. 46-47. Tra i pochi esempi di categorie isomorfe possiamo forse indicare la categoria degli spazi topologici finiti che è isomorfa alla categoria degli insiemi quasiordinati finiti. In questo caso si tratta comunque di una differenza praticamente soltanto linguistica.

Dobbiamo invece lavorare con un concetto più debole, quello dell'equivalenza di categorie, che introdurremo nel prossimo capitolo.

Definizione 30.17. Siano $\mathcal{F}, \mathcal{G} : \mathcal{C} \longrightarrow \mathcal{D}$ due funtori covarianti.
Una *trasformazione naturale* $\eta : \mathcal{F} \longrightarrow \mathcal{G}$ consiste in un sistema di morfismi $\mathcal{F}(X) \xrightarrow{\eta_X} \mathcal{G}(X)$ in $\mathcal{D}$ (uno per ogni $X \in \mathcal{C}$) tale che tutti i diagrammi

$$\begin{array}{ccc} \mathcal{F}(X) & \xrightarrow{\mathcal{F}(f)} & \mathcal{F}(Y) \\ {\scriptstyle \eta_X}\downarrow & & \downarrow{\scriptstyle \eta_Y} \\ \mathcal{G}(X) & \xrightarrow{\mathcal{G}(f)} & \mathcal{G}(Y) \end{array}$$

per $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ siano commutativi.

In modo analogo sono definite trasformazioni naturali tra funtori controvarianti.

Nota 30.18. Siano $\mathcal{F}, \mathcal{G}, \mathcal{H} : \mathcal{C} \longrightarrow \mathcal{D}$ tre funtori covarianti ed $\eta : \mathcal{F} \longrightarrow \mathcal{G}$, $\theta : \mathcal{G} \longrightarrow \mathcal{H}$ trasformazioni naturali.

Allora $\theta * \eta := \bigcirc\limits_{X} \theta_X \eta_X$ è una trasformazione naturale $\mathcal{F} \longrightarrow \mathcal{H}$.

$\theta * \eta$ si chiama il *prodotto di Hadamard* (o *puntuale*) di θ ed η.

Dimostrazione. Per $X, Y \in \mathcal{C}$ ed $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ abbiamo un diagramma

commutativo

$$\begin{array}{ccc}
\mathcal{F}(X) & \xrightarrow{\mathcal{F}(f)} & \mathcal{F}(Y) \\
{\scriptstyle \eta_X}\downarrow & & \downarrow{\scriptstyle \eta_Y} \\
\mathcal{G}(X) & \xrightarrow{\mathcal{G}(f)} & \mathcal{G}(Y) \\
{\scriptstyle \theta_X}\downarrow & & \downarrow{\scriptstyle \theta_Y} \\
\mathcal{H}(X) & \xrightarrow{\mathcal{H}(f)} & \mathcal{H}(Y)
\end{array}$$

Dal rettangolo esterno vediamo che $\theta * \eta$ è una trasformazione naturale $\mathcal{F} \longrightarrow \mathcal{H}$.

Osservazione 30.19. Sia $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ un funtore covariante. Allora $\mathrm{id}_{\mathcal{F}} := \bigcirc_X \mathrm{id}_{\mathcal{F}(X)}$ è una trasformazione naturale $\mathcal{F} \longrightarrow \mathcal{F}$ e per ogni funtore covariante $\mathcal{G} : \mathcal{C} \longrightarrow \mathcal{D}$ ed ogni trasformazione naturale $\eta : \mathcal{F} \longrightarrow \mathcal{G}$ si ha $\eta * \mathrm{id}_{\mathcal{F}} = \eta$ e $\mathrm{id}_{\mathcal{G}} * \eta = \eta$.

Dimostrazione. Chiaro.

Definizione 30.20. Siano $\mathcal{F}, \mathcal{G} : \mathcal{C} \longrightarrow \mathcal{D}$ due funtori covarianti ed $\eta : \mathcal{F} \longrightarrow \mathcal{G}$ e $\theta : \mathcal{G} \longrightarrow \mathcal{F}$ trasformazioni naturali.

θ si chiama un'*inversa a sinistra* di η se $\theta * \eta = \mathrm{id}_{\mathcal{F}}$ e un'*inversa a destra* di η se $\eta * \theta = \mathrm{id}_{\mathcal{G}}$.

θ si chiama un'*inversa* di η se è allo stesso tempo un'inversa sinistra e a destra di η. Ciò significa che per ogni $X \in \mathcal{C}$ i morfismi θ_X ed η_X devono essere invertibili con $\theta_X = (\eta_X)^{-1}$, per cui vediamo che l'inversa di η, quando esiste, è univocamente determinata. In particolare possiamo allora scrivere $\eta^{-1} := \theta$ avendo poi $\eta_X^{-1} = (\eta_X)^{-1}$ per ogni $X \in \mathcal{C}$.

Questi concetti (e quindi anche la notazione η^{-1}) si riferiscono sempre al prodotto di Hadamard e non alla composizione di trasformazioni naturali che introdurremo fra poco.

La trasformazione naturale η si chiama un *isomorfismo di funtori*, se possiede un'inversa.

I funtori $\mathcal{F}$ e $\mathcal{G}$ si dicono *isomorfi*, se esiste un isomorfismo di funtori $\mathcal{F} \longrightarrow \mathcal{G}$. In tal caso scriviamo $\mathcal{F} \cong \mathcal{G}$.

Osservazione 30.21. Siano $\mathcal{F}, \mathcal{G} : \mathcal{C} \longrightarrow \mathcal{D}$ due funtori covarianti ed $\eta : \mathcal{F} \longrightarrow \mathcal{G}$ una trasformazione naturale. Allora sono equivalenti:

(1) η è un isomorfismo di funtori.

(2) Per ogni $X \in \mathcal{C}$ il morfismo η_X è un isomorfismo in $\mathcal{D}$.

Dimostrazione. (1) $\implies$ (2): η sia un isomorfismo di funtori.

Abbiamo già visto nella def. 30.20 che allora per ogni $X \in \mathcal{C}$ il morfismo η_X è un isomorfismo.

(2) $\implies$ (1): Per ogni $X \in \mathcal{C}$ il morfismo η_X sia un isomorfismo. Allora ponendo $\theta_X := (\eta_X)^{-1}$, dobbiamo solo verificare che tutti i diagrammi

$$\begin{array}{ccc} \mathcal{G}(X) & \xrightarrow{\mathcal{G}(f)} & \mathcal{G}(Y) \\ {\scriptstyle\theta_X}\downarrow & & \downarrow{\scriptstyle\theta_Y} \\ \mathcal{F}(X) & \xrightarrow{\mathcal{F}(f)} & \mathcal{F}(Y) \end{array}$$

sono commutativi. Ma per ipotesi (cfr. def. 30.17) abbiamo $\mathcal{G}(f)\eta_X = \eta_Y\mathcal{F}(f)$, cosicché $(\eta_Y)^{-1}\mathcal{G}(f) = \mathcal{F}(f)(\eta_X)^{-1}$ ovvero $\theta_Y\mathcal{G}(f) = \mathcal{F}(f)\theta_X$.

Proposizione 30.22. *Siano $\mathcal{F}_1, \mathcal{G}_1 : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ ed $\mathcal{F}_2, \mathcal{G}_2 : \mathcal{C}_2 \longrightarrow \mathcal{C}_3$ funtori covarianti, $\eta : \mathcal{F}_1 \longrightarrow \mathcal{G}_1$ e $\theta : \mathcal{F}_2 \longrightarrow \mathcal{G}_2$ trasformazioni naturali.*

Allora otteniamo una trasformazione naturale $\sigma : \mathcal{F}_2\mathcal{F}_1 \longrightarrow \mathcal{G}_2\mathcal{G}_1$ ponendo

$$\sigma_X := \mathcal{G}_2(\eta_X)\theta_{\mathcal{F}_1(X)}$$

per ogni $X \in \mathcal{C}_1$.

Dimostrazione. Siano $X, Y \in \mathcal{C}_1$ ed $f \in \mathrm{Hom}_{\mathcal{C}_1}(X, Y)$.

(1) Siccome $\theta : \mathcal{F}_2 \longrightarrow \mathcal{G}_2$ è una trasformazione naturale, dal morfismo $\mathcal{F}_1(f) : \mathcal{F}_1(X) \longrightarrow \mathcal{F}_1(Y)$ in $\mathcal{C}_2$ otteniamo in $\mathcal{C}_3$ un diagramma commutativo

$$\begin{array}{ccc} \mathcal{F}_2(\mathcal{F}_1(X)) & \xrightarrow{\mathcal{F}_2(\mathcal{F}_1(f))} & \mathcal{F}_2(\mathcal{F}_1(Y)) \\ {\scriptstyle\theta_{\mathcal{F}_1(X)}}\downarrow & & \downarrow{\scriptstyle\theta_{\mathcal{F}_1(Y)}} \\ \mathcal{G}_2(\mathcal{F}_1(X)) & \xrightarrow{\mathcal{G}_2(\mathcal{F}_1(f))} & \mathcal{G}_2(\mathcal{F}_1(Y)) \end{array}$$

(2) Siccome $\eta : \mathcal{F}_1 \longrightarrow \mathcal{G}_1$ è una trasformazione naturale, abbiamo in $\mathcal{C}_2$ un diagramma commutativo

$$\begin{array}{ccc} \mathcal{F}_1(X) & \xrightarrow{\mathcal{F}_1(f)} & \mathcal{F}_1(Y) \\ {\scriptstyle\eta_X}\downarrow & & \downarrow{\scriptstyle\eta_Y} \\ \mathcal{G}_1(X) & \xrightarrow{\mathcal{G}_1(f)} & \mathcal{G}_1(Y) \end{array}$$

da cui tramite il funtore $\mathcal{G}_2$ otteniamo in $\mathcal{C}_3$ un diagramma commutativo

$$\begin{array}{ccc} \mathcal{G}_2(\mathcal{F}_1(X)) & \xrightarrow{\mathcal{G}_2(\mathcal{F}_1(f))} & \mathcal{G}_2(\mathcal{F}_1(X)) \\ {\scriptstyle\mathcal{G}_2(\eta_X)}\downarrow & & \downarrow{\scriptstyle\mathcal{G}_2(\eta_Y)} \\ \mathcal{G}_2(\mathcal{G}_1(X)) & \xrightarrow{\mathcal{G}_2(\mathcal{G}_1(f))} & \mathcal{G}_2(\mathcal{G}_1(Y)) \end{array}$$

(3) Combinando in verticale i diagrammi commutativi costruiti nei punti (1) e (2) otteniamo un diagramma commutativo

$$\begin{array}{ccc} \mathcal{F}_2(\mathcal{F}_1(X)) & \xrightarrow{\mathcal{F}_2(\mathcal{F}_1(f))} & \mathcal{F}_2(\mathcal{F}_1(Y)) \\ {\scriptstyle\mathcal{G}_2(\eta_X)\theta_{\mathcal{F}_1(X)}}\downarrow & & \downarrow{\scriptstyle\mathcal{G}_2(\eta_Y)\theta_{\mathcal{F}_1(Y)}} \\ \mathcal{G}_2(\mathcal{G}_1(X)) & \xrightarrow{\mathcal{G}_2(\mathcal{G}_1(f))} & \mathcal{G}_2(\mathcal{G}_1(Y)) \end{array}$$

Definizione 30.23. Siano $\mathcal{F}, \mathcal{G} : \mathcal{C} \longrightarrow \mathcal{D}$ due funtori covarianti ed $\eta : \mathcal{F} \longrightarrow \mathcal{G}$ una trasformazione naturale.

Per ogni $X, Y \in \mathcal{C}$ ed ogni $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ otteniamo allora un diagramma commutativo

$$\begin{array}{ccc} \mathcal{F}(X) & \xrightarrow{\mathcal{F}(f)} & \mathcal{F}(Y) \\ {\scriptstyle \eta_X}\downarrow & & \downarrow{\scriptstyle \eta_Y} \\ \mathcal{G}(X) & \xrightarrow{\mathcal{G}(f)} & \mathcal{G}(Y) \end{array}$$

Seguendo un'idea che abbiamo trovato in Pumplün [16260], p. 86, possiamo quindi definire un morfismo $\eta_f : \mathcal{F}(X) \longrightarrow \mathcal{G}(Y)$ in $\mathcal{D}$ ponendo

$$\eta_f := \eta_Y \mathcal{F}(f) = \mathcal{G}(f)\eta_X$$

Osservazione 30.24. Siano $\mathcal{F}, \mathcal{G} : \mathcal{C} \longrightarrow \mathcal{D}$ due funtori covarianti ed $\eta : \mathcal{F} \longrightarrow \mathcal{G}$ una trasformazione naturale. Allora:

(1) Per ogni $X \in \mathcal{C}$ si ha $\eta_{\mathrm{id}_X} = \eta_X$.

(2) Per ogni $X, Y, Z \in \mathcal{C}$ ed ogni $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$ abbiamo un diagramma commutativo

$$\begin{array}{ccc} \mathcal{F}(X) & \xrightarrow{\mathcal{F}(f)} & \mathcal{F}(Y) \\ {\scriptstyle \eta_f}\downarrow & & \downarrow{\scriptstyle \eta_g} \\ \mathcal{G}(Y) & \xrightarrow{\mathcal{G}(g)} & \mathcal{G}(Z) \end{array}$$

ovvero la relazione

$$\mathcal{G}(g)\eta_f = \eta_g \mathcal{F}(f)$$

Dimostrazione. (1) $\eta_{\mathrm{id}_X} = \eta_X \mathcal{F}(\mathrm{id}_X) = \eta_X \, \mathrm{id}_{\mathcal{F}(X)} = \eta_X$.

(2) Secondo la def. 30.17 abbiamo un diagramma commutativo

$$\begin{array}{ccccc} \mathcal{F}(X) & \xrightarrow{\mathcal{F}(f)} & \mathcal{F}(Y) & \xrightarrow{\mathcal{F}(g)} & \mathcal{F}(Z) \\ {\scriptstyle \eta_X}\downarrow & & {\scriptstyle \eta_Y}\downarrow & & \downarrow{\scriptstyle \eta_Z} \\ \mathcal{G}(X) & \xrightarrow{\mathcal{G}(f)} & \mathcal{G}(Y) & \xrightarrow{\mathcal{G}(g)} & \mathcal{G}(Z) \end{array}$$

e quindi

$$\mathcal{G}(g)\eta_f = \mathcal{G}(g)\mathcal{G}(f)\eta_X = \eta_Z \mathcal{F}(g)\mathcal{F}(f) = \eta_g \mathcal{F}(f)$$

Proposizione 30.25. *Siano $\mathcal{F}, \mathcal{G} : \mathcal{C} \longrightarrow \mathcal{D}$ due funtori covarianti. Per ogni $X, Y \in \mathcal{C}$ ed ogni $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ sia dato un morfismo $\widetilde{\eta}_f : \mathcal{F}(X) \longrightarrow \mathcal{G}(Y)$ in modo tale che per $X, Y, Z \in \mathcal{C}$, $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ e $g \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$ si abbia sempre*

$$\mathcal{G}(g)\widetilde{\eta}_f = \widetilde{\eta}_g \mathcal{F}(f)$$

Se in queste ipotesi per $X \in \mathcal{C}$ poniamo $\eta_X := \widetilde{\eta}_{\mathrm{id}_X}$, allora η è una trasformazione naturale $\mathcal{F} \longrightarrow \mathcal{G}$ ed $\eta_f = \widetilde{\eta}_f$ nel senso della def. 30.23, per ogni morfismo f in $\mathcal{C}$.

Dimostrazione. Siano $X, Y \in \mathcal{C}$ ed $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$. Allora

$$\eta_Y \mathcal{F}(f) = \widetilde{\eta}_{\mathrm{id}_Y} \mathcal{F}(f) = \mathcal{G}(\mathrm{id}_Y)\widetilde{\eta}_f = \mathrm{id}_{\mathcal{G}(Y)}\, \widetilde{\eta}_f = \widetilde{\eta}_f$$
$$\mathcal{G}(f)\eta_X = \mathcal{G}(f)\widetilde{\eta}_{\mathrm{id}_X} = \widetilde{\eta}_f \mathcal{F}(\mathrm{id}_X) = \widetilde{\eta}_f\, \mathrm{id}_{\mathcal{F}(X)} = \widetilde{\eta}_f$$

Ciò mostra da un lato che η è veramente una trasformazione naturale $\mathcal{F} \longrightarrow \mathcal{G}$ e dall'altro che $\widetilde{\eta}_f = \eta_f$.

Lemma 30.26. *Siano $\mathcal{F}, \mathcal{G} : \mathcal{C} \longrightarrow \mathcal{D}$ due funtori covarianti ed $\eta : \mathcal{F} \longrightarrow \mathcal{G}$ una trasformazione naturale.*

Siano inoltre $X, Y, Z \in \mathcal{C}$ ed $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$. Allora

$\eta_{gf} = \mathcal{G}(g)\eta_f = \eta_g \mathcal{F}(f)$

Dimostrazione. Abbiamo

$\eta_{gf} = \eta_Z \mathcal{F}(gf) = \eta_Z \mathcal{F}(g)\mathcal{F}(f) = \eta_g \mathcal{F}(f)$
$\eta_{gf} = \mathcal{G}(gf)\eta_X = \mathcal{G}(g)\mathcal{G}(f)\eta_X = \mathcal{G}(g)\eta_f$

Definizione 30.27. Siano $\mathcal{F}_1, \mathcal{G}_1 : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ ed $\mathcal{F}_2, \mathcal{G}_2 : \mathcal{C}_2 \longrightarrow \mathcal{C}_3$ funtori covarianti, $\eta : \mathcal{F}_1 \longrightarrow \mathcal{G}_1$ e $\theta : \mathcal{F}_2 \longrightarrow \mathcal{G}_2$ trasformazioni naturali.

Per $X, Y \in \mathcal{C}_1$ ed $f \in \mathrm{Hom}_{\mathcal{C}_1}(X, Y)$ allora $\eta_f \in \mathrm{Hom}_{\mathcal{C}_2}(\mathcal{F}_1(X), \mathcal{G}_1(Y))$, per cui $\theta_{\eta_f} \in \mathrm{Hom}_{\mathcal{C}_3}(\mathcal{F}_2\mathcal{F}_1(X), \mathcal{G}_2\mathcal{G}_1(Y))$.

Possiamo quindi definire $\theta \circ \eta := \bigcirc_f \theta_{\eta_f}$.

$\theta \circ \eta$ si chiama la *composizione* delle trasformazioni naturali θ ed η.

Proposizione 30.28. *Nella situazione della def. 30.27 $\theta \circ \eta$ è una trasformazione naturale $\mathcal{F}_2\mathcal{F}_1 \longrightarrow \mathcal{G}_2\mathcal{G}_1$ e coincide con la trasformazione naturale σ della prop. 30.22.*

Dimostrazione. (1) Verfichiamo la condizione della prop. 30.25.

Per $X, Y, Z \in \mathcal{C}_1$ ed $f \in \mathrm{Hom}_{\mathcal{C}_1}(X, Y)$, $g \in \mathrm{Hom}_{\mathcal{C}_1(Y,Z)}$ deve quindi valere

$(\theta \circ \eta)_g \mathcal{F}_2\mathcal{F}_1(f) = \mathcal{G}_2\mathcal{G}_1(g)(\theta \circ \eta)_f$

Infatti

$$(\theta \circ \eta)_g \mathcal{F}_2\mathcal{F}_1(f) = \theta_{\eta_g} \mathcal{F}_2\mathcal{F}_1(f) \overset{30.26}{=} \theta_{\eta_g \mathcal{F}_1(f)} \overset{30.24}{=} \theta_{\mathcal{G}_1(g)\eta_f}$$
$$\overset{30.26}{=} \mathcal{G}_2\mathcal{G}_1(g)\theta_{\eta_f} = \mathcal{G}_2\mathcal{G}_1(g)(\theta \circ \eta)_f$$

(2) Perciò per la prop. 30.25 $\theta\eta$ definisce una trasformazione naturale $\mathcal{F}_2\mathcal{F}_1 \longrightarrow \mathcal{G}_2\mathcal{G}_1$, cosicché per ogni $X \in \mathcal{C}_1$ è defiito il morfismo $(\theta \circ \eta)_X$.

Sia quindi $X \in \mathcal{C}_1$. Allora $\eta_X \in \mathrm{Hom}_{\mathcal{C}_2}(\mathcal{F}_1(X), \mathcal{F}_2(X))$, per cui

$(\theta \circ \eta)_X = \theta_{\eta_X} = \mathcal{G}_2(\eta_X)\theta_{\mathcal{F}_1(X)} = \sigma_X$

Lemma 30.29. *Siano $\mathcal{F}, \mathcal{G}, \mathcal{H} : \mathcal{C} \longrightarrow \mathcal{D}$ tre funtori covarianti ed $\mathcal{F} \overset{\eta}{\longrightarrow} \mathcal{G} \overset{\theta}{\longrightarrow} \mathcal{H}$ trasformazioni naturali.*

Siano inoltre $X, Y, Z \in \mathcal{C}$ ed $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$. Allora:

(1) $gf \in \mathrm{Hom}_{\mathcal{C}}(X, Z)$.

(2) $\theta * \eta$ è una trasformazione naturale $\mathcal{F} \longrightarrow \mathcal{H}$.

(3) $(\theta * \eta)_{gf} \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{F}(X), \mathcal{H}(Z))$.

(4) $\eta_f \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{F}(X), \mathcal{G}(Y))$.

(5) $\theta_g \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{G}(Y), \mathcal{H}(Z))$.

(6) ***Quindi*** $\theta_g \eta_f \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{F}(X), \mathcal{H}(Z))$.

(7) $(\theta * \eta)_{gf} = \theta_g \eta_f$.

Dimostrazione. Dobbiamo solo dimostrare il punto (7). Siccome $\eta : \mathcal{F} \longrightarrow \mathcal{G}$ è una trasformazione naturale, abbiamo un diagramma commutativo

$$\begin{array}{ccc} \mathcal{F}(Y) & \xrightarrow{\mathcal{F}(g)} & \mathcal{F}(Z) \\ {\scriptstyle \eta_Y}\downarrow & & \downarrow{\scriptstyle \eta_Z} \\ \mathcal{G}(Y) & \xrightarrow{\mathcal{G}(g)} & \mathcal{G}(Z) \end{array}$$

Perciò

$$(\theta * \eta)_{gf} = (\theta * \eta)_Z \mathcal{F}(gf) = \theta_Z \eta_Z \mathcal{F}(g)\mathcal{F}(f) = \theta_Z \mathcal{G}(g) \eta_Y \mathcal{F}(f) = \theta_g \eta_f$$

Teorema 30.30 (legge distributiva). *Siano* $\mathcal{F}_1, \mathcal{G}_1, \mathcal{H}_1 : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ *ed* $\mathcal{F}_2, \mathcal{G}_2, \mathcal{H}_2 : \mathcal{C}_2 \longrightarrow \mathcal{C}_3$ *funtori covarianti e siano date trasformazioni naturali* $\mathcal{F}_1 \xrightarrow{\eta} \mathcal{G}_1 \xrightarrow{\eta'} \mathcal{H}_1$ *e* $\mathcal{F}_2 \xrightarrow{\theta} \mathcal{G}_2 \xrightarrow{\theta'} \mathcal{H}_2$. *Allora:*

(1) Per le costruzioni finora viste sono definite le trasformazioni naturali

$$\begin{aligned} \mathcal{F}_1 &\xrightarrow{\eta' * \eta} \mathcal{H}_1 \\ \mathcal{F}_2 &\xrightarrow{\theta' * \theta} \mathcal{H}_2 \\ \mathcal{F}_2\mathcal{F}_1 &\xrightarrow{(\theta' * \theta) \circ (\eta' * \eta)} \mathcal{H}_2\mathcal{H}_1 \\ \mathcal{F}_2\mathcal{F}_1 &\xrightarrow{\theta \circ \eta} \mathcal{G}_2\mathcal{G}_1 \xrightarrow{\theta' \circ \eta'} \mathcal{H}_2\mathcal{H}_1 \\ \mathcal{F}_2\mathcal{F}_1 &\xrightarrow{(\theta' \circ \eta') * (\theta \circ \eta)} \mathcal{H}_2\mathcal{H}_1 \end{aligned}$$

(2) Vale la legge distributiva

$$(\theta' * \theta) \circ (\eta' * \eta) = (\theta' \circ \eta') * (\theta \circ \eta)$$

Dimostrazione. Dobbiamo solo dimostrare il punto (2). Sia $X \in \mathcal{C}_1$. Allora

$$\begin{aligned} ((\theta' * \theta) \circ (\eta' * \eta))_X &= (\theta' * \theta)_{(\eta' * \eta)_X} = (\theta' * \theta)_{\eta'_X \eta_X} \overset{30.29}{=} \theta'_{\eta'_X} \theta_{\eta_X} \\ &= (\theta' \circ \eta')_X (\theta \circ \eta)_X = ((\theta' \circ \eta') * (\theta \circ \eta))_X \end{aligned}$$

31. Equivalenza di categorie

Un funtore $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ si chiama un'*equivalenza* (tra categorie), se esiste un funtore covariante $\mathcal{G} : \mathcal{D} \longrightarrow \mathcal{C}$ tale che $\mathcal{FG} \cong \mathrm{Id}_{\mathcal{D}}$ e $\mathcal{GF} \cong \mathrm{Id}_{\mathcal{C}}$ oppure, equivalentemente, se $\mathcal{F}$ è pienamente fedele e per ogni $Y \in \mathcal{D}$ esiste un $X \in \mathcal{C}$ con $Y \cong \mathcal{F}(X)$. Sottocategorie e sottocategorie piene. Ogni categoria $\mathcal{C}$ possiede una sottocategoria piena che contiene per ogni classe di isomorfia in $\mathcal{C}$ un unico rappresentante. L'equivalenza tra categorie è una relazione riflessiva, simmetrica e transitiva. Un'equivalenza trasforma monomorfismi in monomorfismi ed epimorfismi in epimorfismi. La categoria degli spazi metrici e la categoria degli spazi topologici metrizzabili sono equivalenti. La categoria degli spazi compatti e di Hausdorff è equivalente al duale della categoria delle C*-algebre commutative. La categoria degli insiemi algebrici su un campo algebricamente chiuso K è equivalente al duale della categoria delle K-algebre polinomiali ridotte.

Situazione 31.1. $\mathcal{C}, \mathcal{D}, \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ siano categorie.

Osservazione 31.2. In questo capitolo per la maggior parte ci limiteremo alla formulazione di concetti ed enunciati, rimandando per le dimostrazioni, spesso piuttosto complicate, alla letteratura.

Ciò non ci deve troppo preoccupare, perché nel seguito degli appunti non faremo uso degli enunciati di questo capitolo che vengono presentati solo con scopi informativi e per inquadrare i risultati del cap. 24 nell'ambito della teoria delle categorie.

In verità anche in quella teoria più generale il concetto di equivalenza viene spesso usato più come un principio conduttore (cfr. Pumplün [16260], p. 47) secondo il quale, date due categorie equivalenti, un teorema vale in una delle due se e solo se il suo analogo è valido nell'altra. A differenza dalla teoria della dualità, siccome il concetto di teorema analogo non è facilmente precisabile, in genere bisogna effettuare le dimostrazioni in entrambe le categorie.

Definizione 31.3. Un funtore covariante $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ si chiama un'*equivalenza* (tra categorie), se esiste un funtore covariante $\mathcal{G} : \mathcal{D} \longrightarrow \mathcal{C}$ tale che $\mathcal{FG} \cong \mathrm{Id}_{\mathcal{D}}$ e $\mathcal{GF} \cong \mathrm{Id}_{\mathcal{C}}$.

$\mathcal{G}$ si chiama allora un *quasiinverso* di $\mathcal{F}$.

L'isomorfia di funtori è stata definita nella def. 30.20, il funtore identico nell'oss. 30.15.

Le categorie $\mathcal{C}$ e $\mathcal{D}$ si chiamano *equivalenti*, se esiste un'equivalenza $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$. Scriviamo in tal caso $\mathcal{C} \sim \mathcal{D}$.

Osservazione 31.4. Il quasiinverso di un'equivalenza di categorie in genere non è univocamente determinato. Cfr. Gelfand/Manin [21952], p. 71.

Teorema 31.5. *Un funtore covariante $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ è un'equivalenza se e solo se $\mathcal{F}$ è pienamente fedele e per ogni $Y \in \mathcal{D}$ esiste un $X \in \mathcal{C}$ tale che $Y \cong \mathcal{F}(X)$.*

Dimostrazione. Funtori pienamente fedeli sono stati definiti nella def. 30.10. La dimostrazione del teorema è piuttosto ardua e si trova ad esempio in Gelfand/Manin [21952], p. 71-72, Adámek/Herrlich/Strecker [22152], p. 86, Menini [21831], p. 11-14, Awodey [21916], p. 173-175, Holme [22469], p. 152-154, Kashiwara/Shapira [22258], p. 22.

Definizione 31.6. Una categoria $\mathcal{C}_0$ si dice *sottocategoria* di $\mathcal{C}$, se sono soddisfatte le seguenti condizioni:

(1) Per ogni $X \in \mathcal{C}_0$ si ha $X \in \mathcal{C}$.

(2) Per ogni $X \in \mathcal{C}_0$ si ha $\mathrm{id}_X^{\mathcal{C}_0} = \mathrm{id}_X^{\mathcal{C}}$.

(3) Per ogni $X, Y \in \mathcal{C}_0$ si ha $\mathrm{Hom}_{\mathcal{C}_0}(X, Y) \subset \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

(4) Per $X, Y, Z \in \mathcal{C}_0$ ed $f \in \mathrm{Hom}_{\mathcal{C}_0}(X, Y)$, $g \in \mathrm{Hom}_{\mathcal{C}_0}(Y, Z)$ la composizione gf in $\mathcal{C}_0$ coincide con la composizione in $\mathcal{C}$.

$\mathcal{C}_0$ si chiama in tal caso una *sottocategoria piena*, se in (3) vale l'uguaglianza, cioè se per ogni $X, Y \in \mathcal{C}_0$ si ha $\mathrm{Hom}_{\mathcal{C}_0} = \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

Osservazione 31.7. $\mathcal{C}_0$ sia una sottocategoria di $\mathcal{C}$. Allora l'inclusione $(\bigcirc\limits_X X, \bigcirc\limits_f f) : \mathcal{C}_0 \longrightarrow \mathcal{C}$ è un funtore covariante ben definito.

Teorema 31.8. *Esiste una sottocategoria piena $\mathcal{C}_0$ di $\mathcal{C}$ tale che sono soddisfatte le seguenti condizioni:*

(1) L'inclusione $\mathcal{C}_0 \longrightarrow \mathcal{C}$ è un'equivalenza di categorie.

(2) Se $X, Y \in \mathcal{C}_0$ sono tali che $X \cong Y$, allora $X = Y$.

Dimostrazione. Kashiwara/Shapira [22258], p. 21-22.

Si osservi che la condizione che $\mathcal{C}_0$ sia una sottocategoria piena implica che X ed Y sono isomorfi in $\mathcal{C}_0$ se e solo se sono isomorfi in $\mathcal{C}$.

Proposizione 31.9. *Siano date equivalenze $\mathcal{F}_1 : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ ed $\mathcal{F}_2 : \mathcal{C}_2 \longrightarrow \mathcal{C}_3$ e sia $\mathcal{G}_1$ un quasiinverso di $\mathcal{F}_1$, $\mathcal{G}_2$ un quasiinverso di $\mathcal{F}_2$.*

Allora il funtore composto $\mathcal{F}_2\mathcal{F}_1$ è un'equivalenza di categorie e $\mathcal{G}_1\mathcal{G}_2$ è un suo quasiinverso.

Dimostrazione. Anche questa dimostrazione non è facile e si trova ad esempio in Schubert [5945], secondo volume, p. 3.

Corollario 31.10. *L'equivalenza tra categorie è una relazione riflessiva, simmetrica e transitiva.*

Dimostrazione. Riflessività e simmetria seguono direttamente dalla def. 31.3, la transitività dalla prop. 31.9.

Proposizione 31.11. *$\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ sia un'equivalenza. Allora $\mathcal{F}$ trasforma monomorfismi in monomorfismi ed epimorfismi in epimorfismi.*

Dimostrazione. Siano $X, Y \in \mathcal{C}$ ed $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

(1) f sia un monomorfismo. Siano $T \in \mathcal{D}$ ed $u, v \in \mathrm{Hom}_{\mathcal{D}}(T, \mathcal{F}(X))$ tali che $\mathcal{F}(f)u = \mathcal{F}(f)v$.

Per il teorema 31.5 esistono un oggetto $S \in \mathcal{C}$ ed un isomorfismo $\alpha : \mathcal{F}(S) \longrightarrow T$.

Allora $u\alpha, v\alpha \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{F}(S), \mathcal{F}(X))$ e inoltre, siccome $\mathcal{F}$ è pienamente fedele, esistono $u', v' \in \mathrm{Hom}_{\mathcal{C}}(S, X)$ tali che $u\alpha = \mathcal{F}(u'), v\alpha = \mathcal{F}(v')$.

Ciò implica $\mathcal{F}(fu') = \mathcal{F}(f)u\alpha = \mathcal{F}(f)v\alpha = \mathcal{F}(fv')$ e quindi, per la fedeltà di $\mathcal{F}$, si ha $fu' = fv'$. Siccome f è un monomorfismo, da ciò segue $u' = v'$

e quindi anche $u\alpha = \mathcal{F}(u') = \mathcal{F}(v') = v\alpha$. Ma α è un isomorfismo, per cui $u = v$.

(2) Se f è un epimorfismo, si ragiona allo stesso modo.

Esempio 31.12. Siano $\mathcal{C}$ la categoria degli spazi metrici con le applicazioni continue come morfismi e $\mathcal{D}$ la categoria degli spazi topologici metrizzabili.

Sia $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ il funtore che associa ad ogni spazio metrico lo spazio topologico a cui corrisponde e ad ogni funzione continua tra spazi metrici questa stessa funzione.

Allora $\mathcal{F}$ è un'equivalenza, perché soddisfa evidentemente le condizioni del teorema 31.5, ma non è un isomorfismo.

Nota 31.13. (1) Sia A un'algebra (unitale) di Banach commutativa (su $\mathbb{C}$). Il teorema di Gelfand-Mazur implica che per ogni $\mathfrak{m} \in \operatorname{Max} A$ l'algebra di Banach $A/\mathfrak{m}$ è isomorfa a $\mathbb{C}$ e determina quindi un'omomorfismo di algebre di Banach $\theta_{\mathfrak{m}} : A \longrightarrow \mathbb{C}$, ponendo $\theta_{\mathfrak{m}}(a) := \lambda$, dove λ è l'unico $\lambda \in \mathbb{C}$ per il quale $a - \lambda \in \mathfrak{m}$.

Viceversa per ogni omomorfismo di algebre di Banach $\theta : A \longrightarrow \mathbb{C}$ si ha $\operatorname{Ker} \theta \in \operatorname{Max} A$, ottenendo così una biiezione naturale tra $\operatorname{Max} A$ e gli omomorfismi di algebre di Banach $A \longrightarrow \mathbb{C}$.

(2) Siano A e B algebre di Banach commutative ed $u : A \longrightarrow B$ un omomorfismo. Dal punto (1) otteniamo un'applicazione $\operatorname{Max} B \longrightarrow \operatorname{Max} A$ attraverso l'applicazione $\bigcirc\!\!\!\!\!\!\int_{\eta} \eta \circ u$. Sia $\mathfrak{m} = \operatorname{Ker} \eta$.

Allora $a \in \operatorname{Ker} \eta \circ u \iff u(a) \in \operatorname{Ker} \eta \iff a \in u^{-1}(\mathfrak{m})$ e quindi si ha $u^{-1}(\mathfrak{m}) = \operatorname{Ker} \eta \circ u \in \operatorname{Max} A$.

(3) Una C*-algebra commutativa è un'algebra di Banach commutativa A con un'involuzione, cioè un'applicazione $* : A \longrightarrow A$ tale che $a^{**} = a$, $(a+b)^* = a^* + b^*$, $(ab)^* = a^* b^*$ e $(\lambda a)^* = \overline{\lambda} a^*$ per $a, b \in A$ e $\lambda \in \mathbb{C}$, nella quale chiediamo che valga $\|a^* a\| = \|a\|^2$ per ogni $a \in A$.

(4) Sia X uno spazio compatto e di Hausdorff. Allora $C(X, \mathbb{C})$ è una C*-algebra con l'involuzione data da $f^* = \overline{f}$.

(5) Siano $\mathcal{C}$ la categoria degli spazi topologici compatti e di Hausdorff e $\mathcal{D}$ la categoria delle C*-algebre commutative.

(6) Per il teorema di Gelfand/Naimark per ogni C*-algebra commutativa A esiste uno spazio topologico X, compatto e di Hausdorff, tale che $A \cong C(X, \mathbb{C})$ in $\mathcal{D}$. Si può infatti prendere $X = \operatorname{Max} A$ con la A-topologia.

(7) Sia $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}^{\mathrm{opp}}$ il funtore covariante definito da $\mathcal{F}(X) := C(X, \mathbb{C})$ ed $\mathcal{F}(\varphi) := \bigcirc\!\!\!\!\!\!\int_{\eta} \eta \circ \varphi$. Dal teorema di Stone-Weierstrass segue che $\mathcal{F}$ è fedele e dal punto (2) vediamo che $\mathcal{F}$ è anche pienamente fedele.

(8) Per il punto (6) ogni oggetto di $\mathcal{D}$ è isomorfo a un $\mathcal{F}(X)$, cosicché dal teorema 31.5 segue che $\mathcal{F}$ è un'equivalenza di categorie.

Per dettagli si cfr. Hirzebruch/Scharlau [1145] oppure Baldini [21963].

Teorema 31.14. *Siano K un campo algebricamente chiuso, $\mathcal{C}$ la categoria dei sottoinsiemi algebrici di qualche K^n e $\mathcal{D}$ la categoria delle K-algebre polinomiali e ridotte.*

Allora il funtore covariante $\mathcal{F} := (\bigcirc_X \mathcal{O}(X), \bigcirc_\varphi \eta \circ \varphi) : \mathcal{C} \longrightarrow \mathcal{D}^{\mathrm{opp}}$ è un'equivalenza di categorie.

Dimostrazione. (1) Per il cor. 26.8 il funtore $\mathcal{F}$ è ben definito.

(2) Siano $X, Y \in \mathcal{C}$. Per il cor. 24.12 abbiamo una biiezione naturale $\mathcal{O}(X,Y) \longleftrightarrow \mathrm{Hom}_{\mathcal{D}}(\mathcal{O}(Y), \mathcal{O}(X))$ e ciò mostra che $\mathcal{F}$ è pienamente fedele.

(3) Per il teorema 26.9 ogni oggetto di $\mathcal{D}$ è isomorfo a un $\mathcal{O}(X)$ per $X \in \mathcal{C}$.

(4) Dal teorema 31.5 segue che $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}^{\mathrm{opp}}$ è un'equivalenza di categorie.

(5) Se non volessimo appellarci al teorema 31.5 (che non abbiamo dimostrato), potremmo dimostrare direttamente che il funtore $\mathcal{G} : \mathcal{D}^{\mathrm{opp}} \longrightarrow \mathcal{C}$ è un quasiinverso di $\mathcal{F}$, se per $A = K[n]/I$ (con I un ideale radicale) poniamo $\mathcal{G}(A) := \mathrm{Zeri}(I)$ e per un omomorfismo $u : K[m]/J \longrightarrow K[n]/I$ con $u(x_i + J) = f_i + I$ definiamo $\mathcal{G}(u) := (f_1, \ldots, f_m)_{\mathrm{Zeri}(I) \longrightarrow \mathrm{Zeri}(J)}$, usando la costruzione del lemma 24.29.

Teorema 31.15. *Sia $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ un funtore pienamente fedele (ad esempio un'equivalenza di categorie). Siano $X, Y \in \mathcal{C}$. Allora:*

(1) $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ è un isomorfismo se e solo se $\mathcal{F}(f)$ è un isomorfismo.

(2) X ed Y sono isomorfi in $\mathcal{C}$ se e solo se $\mathcal{F}(X)$ ed $\mathcal{F}(Y)$ sono isomorfi in $\mathcal{D}$.

Dimostrazione. (1) Se f è un isomorfismo, allora anche $\mathcal{F}(f)$ è un isomorfismo per il lemma 30.12.

Sia invece $\mathcal{F}(f)$ un isomorfismo con inverso v. Siccome $\mathcal{F}$ è pienamente fedele, esiste $g \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ tale che $v = \mathcal{F}(g)$.

Allora abbiamo

$\mathcal{F}(\mathrm{id}_Y) = \mathrm{id}_{\mathcal{F}(Y)} = \mathcal{F}(f)v = \mathcal{F}(f)\mathcal{F}(g) = \mathcal{F}(fg)$ e quindi $fg = \mathrm{id}_Y$,

$\mathcal{F}(\mathrm{id}_X) = \mathrm{id}_{\mathcal{F}(X)} = v\mathcal{F}(f) = \mathcal{F}(g)\mathcal{F}(f) = \mathcal{F}(gf)$ e quindi $gf = \mathrm{id}_X$,

usando entrambe le volte che $\mathcal{F}$ è fedele.

(2) Se X ed Y sono isomorfi, allora $\mathcal{F}(X)$ ed $\mathcal{F}(Y)$ sono isomorfi per il punto (1).

Sia invece $u : \mathcal{F}(X) \longrightarrow \mathcal{F}(Y)$ un isomorfismo. Siccome $\mathcal{F}$ è pienamente fedele, esiste $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ tale che $u = \mathcal{F}(f)$. Per il punto (1) f è un isomorfismo.

32. Una dimostrazione elementare di $\dim \mathbf{K[n]} = \mathbf{n}$

Siano $Q \in \operatorname{Spec} A[x]$, $P := Q \cap A$ e $P[x] \neq Q$: allora $\operatorname{alt} Q = 1 + \operatorname{alt} P[x]$ e $\operatorname{alt} Q/P[x] = 1$. Il teorema 32.9 è il risultato principale del capitolo: Se Q appartiene a $\operatorname{Spec} A[n]$ e $P := Q \cap A$, allora $\operatorname{alt} Q = \operatorname{alt} P[n] + \operatorname{alt} Q/P[n] \leq n + \operatorname{alt} P[n]$. Ne deriva come conseguenza immediata che per un campo K si ha $\dim K[n] = n$. Una caratterizzazione della dimensione di un anello commutativo dovuta a Coquand e Lombardi.

Situazione 32.1. Sia A un anello commutativo $\neq 0$.

Come nella def. 27.13 denotiamo con $\operatorname{alt} P$ l'altezza di un ideale primo P.

Presentiamo in questo capitolo una dimostrazione elementare, ma tecnicamente intricata e fine, della relazione $\dim K[n] = n$ per un campo K, dovuta a Brewer/ [22642], per la quale seguiamo l'esposizione in Watkins [22453], p. 140-144.

Osservazione 32.2. Useremo i seguenti fatti, in genere senza menzionarli esplicitamente:

(1) $Q \in \operatorname{Spec} A[x] \Longrightarrow Q \cap A \in \operatorname{Spec} A$.

(2) Se P è un ideale generalizzato di A, allora $P \in \operatorname{Spec} A$ se e solo se $P[x] \in \operatorname{Spec} A[x]$.

(3) Se J è un ideale generalizzato di $A[x]$, allora $(J \cap A)[x] \cap A = J \cap A \subset (J \cap A)[x] \subset J$.

Dimostrazione. (1) Oss. 27.19.

(2) Prop. 27.10.

(3) È chiaro che $J \cap A \subset (J \cap A)[x] \subset J$ e ciò (oppure l'oss. 27.8) implica

$J \cap A \subset (J \cap A)[x] \cap A \subset J \cap A$

Lemma 32.3. *Siano $Q \in \operatorname{Spec} A[x], P := Q \cap A$ e $\operatorname{alt} P = 0$.*

Se $P[x] \neq Q$, allora $\operatorname{alt} P[x] = 0$.

Dimostrazione. Assumiamo, per assurdo, che $\operatorname{alt} P[x] \geq 1$. Allora esiste $Q_0 \in \operatorname{Spec} A[x]$ tale che $Q_0 \subsetneqq P[x] \subsetneqq Q$.

Per il lemma 27.27 allora $Q_0 \cap A \subsetneqq Q \cap A = P$ e ciò implica $\operatorname{alt} P \geq 1$, in contrasto alle ipotesi.

Lemma 32.4. *Siano $Q \in \operatorname{Spec} A[x], P := Q \cap A$ e $\operatorname{alt} P = 0$.*

Se $P[x] \neq Q$, allora $\operatorname{alt} Q = 1$.

Dimostrazione. (1) Sicuramente $\operatorname{alt} Q \geq 1$, perché $(P[x], Q)$ è una catena di Krull.

(2) Assumiamo, per assurdo, che $\operatorname{alt} Q \geq 2$. Allora esistono $Q_0, Q_1 \in \operatorname{Spec} A[x]$ con $Q_0 \subsetneqq Q_1 \subsetneqq Q$.

Per il lemma 27.27 allora $Q_0 \cap A \subsetneqq Q \cap A = P$, ma ciò non è possibile perché $\operatorname{alt} P = 0$.

Lemma 32.5. *Siano $Q \in \operatorname{Spec} A[x]$ e $P := Q \cap A$.*

Se $P[x] \neq Q$*, allora* $\operatorname{alt} Q = 1 + \operatorname{alt} P[x]$.

Dimostrazione. (1) L'enunciato è banale se $\operatorname{alt} P = \infty$, perché in tal caso anche $\operatorname{alt} P[x] = \infty$, come segue dal lemma 27.17.

(2) Assumiamo quindi che $\operatorname{alt} P < \infty$ e dimostriamo il lemma per induzione su $m := \operatorname{alt} P$.

$m = 0$: Questo caso segue dal lemma 32.4.

$m - 1 \longrightarrow m$: Certamente $\operatorname{alt} Q \geq 1 + \operatorname{alt} P[x]$, essendo $P[x] \subsetneqq Q$.

Dimostriamo che per ogni $Q_1 \in \operatorname{Spec} A[x]$ con $Q_1 \subsetneqq Q$ si ha $\operatorname{alt} Q_1 \leq \operatorname{alt} P[x]$.

Siano $Q_1 \in \operatorname{Spec} A[x]$ tale che $Q_1 \subsetneqq Q$ e $P_1 := Q_1 \cap A \subset P$.

Consideriamo i due casi possibili $P_1 = P$ e $P_1 \subsetneqq P$.

(a) Sia $P_1 = P$. Allora

$$P[x] = P_1[x] = (Q_1 \cap A)[x] \subset Q_1 \subsetneqq Q$$

e

$$P[x] \cap A = (Q \cap A)[x] \cap A \overset{32.2}{=} Q \cap A$$

cosicché dal lemma 27.27 segue $P[x] = Q_1$ e quindi $\operatorname{alt} Q_1 = \operatorname{alt} P[x]$.

(b) Sia $P_1 \subsetneqq P$: Allora $P_1[x] = (Q_1 \cap A)[x] \subset Q_1$. Consideriamo i casi $P_1[x] = Q_1$ e $P_1[x] \subsetneqq Q_1$.

(b1) Sia $P_1[x] = Q_1$. Allora $\operatorname{alt} Q_1 = \operatorname{alt} P_1[x] \leq \operatorname{alt} P[x]$.

(b2) Sia $P_1[x] \subsetneqq Q_1$. Adesso però $P_1 \subsetneqq P$ e quindi $\operatorname{alt} P_1 < \operatorname{alt} P = m$, per cui possiamo applicare l'ipotesi di induzione, per la quale $\operatorname{alt} Q_1 = 1 + \operatorname{alt} P_1[x]$.

Per il lemma 27.7 però anche $P_1[x] \subsetneqq P[x]$ e quindi

$$\operatorname{alt} Q_1 = 1 + \operatorname{alt} P_1[x] \leq \operatorname{alt} P[x]$$

Lemma 32.6. *Siano* $Q \in \operatorname{Spec} A[x_1]$ *e* $P := Q \cap A$*. Sia* $n \geq 2$*.*

Se $P[x_1] \neq Q$*, allora* $\operatorname{alt} Q[x_2, \ldots, x_n] = 1 + \operatorname{alt} P[x_1, \ldots, x_n]$.

Dimostrazione. Poniamo

$$\widetilde{A} := A[x_2, \ldots, x_n],\ \widetilde{Q} := Q[x_2, \ldots, x_n] \subset A[x_1, \ldots, x_n] = \widetilde{A}[x_1]$$
$$\widetilde{P} := \widetilde{Q} \cap \widetilde{A} = Q[x_2, \ldots, x_n] \cap A[x_2, \ldots, x_n] = (Q \cap A)[x_2, \ldots, x_n] = P[x_2, \ldots, x_n]$$

Per la prop. 27.10 $\widetilde{Q} \in \operatorname{Spec} \widetilde{A}[x_1]$ e quindi $\widetilde{P} \in \operatorname{Spec} \widetilde{A}$.

Inoltre $\widetilde{P}[x_1] \neq \widetilde{Q}$ per il lemma 27.7 (applicato più volte), cosicché possiamo applicare il lemma 32.5, ottenendo

$$\operatorname{alt} \widetilde{Q} = 1 + \operatorname{alt} \widetilde{P}[x_1]$$

e quindi $\operatorname{alt} Q[x_2, \ldots, x_n] = 1 + \operatorname{alt} P[x_1, \ldots, x_n]$

Definizione 32.7. In analogia alla def. 22.2 per un ideale generalizzato I di A ed $n \in \mathbb{N} + 1$ poniamo $I[n] := I[x_1, \ldots, x_n]$.

Osservazione 32.8. Siano $Q \in \operatorname{Spec} A[x]$ e $P = Q \cap A$.

Se $P[x] \neq Q$, allora $\operatorname{alt} Q/P[x] = 1$.

Dimostrazione. Siccome $P[x]$ è primo, l'ipotesi $P[x] \neq Q$ implica $\operatorname{alt} Q/P[x] \geq 1$. Assumiamo che $\operatorname{alt} Q/P[x] \geq 2$.

Allora esiste $Q_1 \in \operatorname{Spec} A[x]$ con $P[x] \subsetneqq Q_1 \subsetneqq Q$. Ma $P[x] \cap A \overset{32.2}{=} Q \cap A$, e ciò è in contrasto con il lemma 27.27.

Teorema 32.9. *Siano $Q \in \operatorname{Spec} A[n]$ e $P := Q \cap A$. Allora*

$$\operatorname{alt} Q = \operatorname{alt} P[n] + \operatorname{alt} Q/P[n] \leq n + \operatorname{alt} P[n]$$

Dimostrazione. Induzione su n.

$n = 1$: Allora abbiamo $Q \in \operatorname{Spec} A[x]$ e $P = Q \cap A$ e bisogna dimostrare che

$$\operatorname{alt} Q = \operatorname{alt} P[x] + \operatorname{alt} Q/P[x] \leq 1 + \operatorname{alt} P[x]$$

Ciò è vero se $P[x] = Q$, mentre per $P[x] \subsetneqq Q$ dal lemma 32.5 abbiamo

$$\operatorname{alt} Q = 1 + \operatorname{alt} P[x] \overset{32.8}{=} \operatorname{alt} Q/P[x] + \operatorname{alt} P[x]$$

$n - 1 \longrightarrow n$: Siano $B := A[x_1]$, $Q_1 := Q \cap B$ ed $N := Q_1[x_2, \ldots, x_n]$.

Allora $Q \in \operatorname{Spec} A[n] = \operatorname{Spec} B[x_2, \ldots, x_n]$ e per induzione si ha

$$\operatorname{alt} Q = \operatorname{alt} Q_1[x_2, \ldots, x_n] + \operatorname{alt} Q/Q_1[x_2, \ldots, x_n] \leq n - 1 + \operatorname{alt} Q_1[x_2, \ldots, x_n]$$

cosicché

$$\operatorname{alt} Q = \operatorname{alt} N + \operatorname{alt} Q/N \leq n - 1 + \operatorname{alt} N$$

Osserviamo che $P[x_1] = (Q \cap A)[x_1] = Q[x_1] \cap A[x_1] \subset Q \cap B = Q_1$.

(a) Sia $P[x_1] = Q_1$. Allora $N = P[n]$, quindi si ha

$$\operatorname{alt} Q = \operatorname{alt} P[n] + \operatorname{alt} Q/P[n] \leq n - 1 + \operatorname{alt} P[n]$$

(b) Sia $P[x_1] \subsetneqq Q_1$. Siccome $Q_1 \in \operatorname{Spec} A[x_1]$, dal lemma 32.6 otteniamo $\operatorname{alt} Q_1[x_2, \ldots, x_n] = 1 + \operatorname{alt} P[n]$ e con ciò

$$\operatorname{alt} N = 1 + \operatorname{alt} P[n]$$

(b1) Applicando l'ipotesi di induzione si ha

$$\operatorname{alt} Q = \operatorname{alt} Q_1[x_2, \ldots, x_n] + \operatorname{alt} Q/Q_1[x_2, \ldots, x_n] \leq n - 1 + \operatorname{alt} Q_1[x_2, \ldots, x_n]$$

e quindi

$$\operatorname{alt} Q = \operatorname{alt} N + \operatorname{alt} Q/N \leq n - 1 + \operatorname{alt} N = n - 1 + 1 + \operatorname{alt} P[n] = n + \operatorname{alt} P[n]$$

(b2) Abbiamo quindi dimostrato una parte dell'enunciato del teorema, e dobbiamo ancora dimostrare che $\operatorname{alt} Q = \operatorname{alt} P[n] + \operatorname{alt} Q/P[n]$.

Siccome però è ovvio che $\operatorname{alt} Q \geq \operatorname{alt} P[n] + \operatorname{alt} Q/P[n]$, è sufficiente dimostrare la disuguaglianza $\operatorname{alt} Q \leq \operatorname{alt} P[n] + \operatorname{alt} Q/P[n]$.

(b3) Dall'ipotesi $P[x_1] \subsetneqq Q_1$ per il lemma 27.7 segue

$$P[n] \subsetneqq Q_1[x_2, \ldots, x_n] = N \quad \text{e quindi} \quad \operatorname{alt} Q/P[n] \geq 1 + \operatorname{alt} Q/N$$

Perciò

$$\operatorname{alt} Q \overset{(b1)}{=} \operatorname{alt} N + \operatorname{alt} Q/N = \operatorname{alt} P[n] + 1 + \operatorname{alt} Q/N \leq \operatorname{alt} P[n] + \operatorname{alt} Q/P[n]$$

Teorema 32.10. *Sia K un campo.*

Allora $\dim K[n] = n$.

Dimostrazione. (1) Dal cor. 27.18 sappiamo che $\dim K[n] \geq n$.

Ciò si vede anche considerando la catena di Krull
$(0, \smile(x_1), \smile(x_1, x_2), \ldots, \smile(x_1, \ldots, x_n))$.

(2) Sia $Q \in \operatorname{Spec} K[n]$. Allora $P := Q \cap K = 0$ (necessariamente, perché il campo K non possiede ideali $\neq 0$) e quindi $P[n] = 0$, cosicché dal teorema 32.9 segue $\operatorname{alt} Q \leq n + \operatorname{alt} P[n] = n + 0 = n$.

Osservazione 32.11. Vedremo in un capitolo successivo (come conseguenza del teorema dell'ideale principale di Krull) che per un anello commutativo *noetheriano* si ha sempre

$$\dim A[n] = n + \dim A$$

Nota 32.12. Il teorema 32.9 può essere anche dedotto dalla seguente caratterizzazione della dimensione di un anello commutativo che si trova in Coquand/Lombardi [22443].

Per $f_0, \ldots, f_n, a_0, \ldots, a_n \in A$ e $k_0, \ldots, k_n \in \mathbb{N}$ definiamo $[f_0, k_0, a_0, \ldots, f_n, k_n, a_n]$ ricorsivamente tramite

$$[f_0, k_0, a_0] := f_0^{k_0}(1 + a_0 f_0)$$
$$[f_0, k_0, a_0, \ldots, f_n, k_n, a_n] := f_0^{k_0}([f_1, k_1, a_1, \ldots, f_n, k_n, a_n] + a_0 f_0)$$

Allora sono equivalenti:

(1) $\dim A \leq n$.

(2) Per ogni $f_0, \ldots, f_n \in A$ esistono $a_0, \ldots, a_n \in A$ e $k_0, \ldots, k_n \in \mathbb{N}$ tali che $[f_0, k_0, a_0, \ldots, f_n, k_n, a_n] = 0$.

Bibliografia

J. Adámek/H. Herrlich/G. Strecker: Abstract and concrete categories. Dover 2009. [22152]

W. Adams/P. Loustaunau: An introduction to Gröbner bases. AMS 1994. [17310]

M. Atiyah/I. Macdonald: Introduction to commutative algebra. Westview Press 1969.
Trad. ital.: Introduzione all'algebra commutativa. Feltrinelli 1981. [3518]

S. Awodey: Category theory. Oxford UP 2010. [21916]

C. Baciu/M. Kreuzer: Algebraisches Öl. Mitt. DMV 19 (2011), 142-147. [22675]

L. Baldini: Strumenti della topologia generale in analisi funzionale. Tesi LT Univ. Ferrara 2011. [21963]

E. Ballico: Examples of uniquely solvable polynomial multivariate interpolation problems (Lagrange, partial Hermite or Birkhoff). Int. J. Pure Appl. Math. 36/2 (2007), 273-278. [22531]

T. Becker/V. Weispfenning: Gröbner bases. Springer 1993. [5737]

C. de Boor: Polynomial interpolation in several variables. In R. De Millo/J. Rice (ed.): Studies in computer science. Plenum Press 1994, 87-119. [22529]

N. Bourbaki: Commutative algebra. Ch. 1-7. Springer 1989. [3329]

J. Brewer/W. Heinzer/P. Montgomery/E. Rutter: Krull dimension of polynomial rings. Springer LN Math. 311 (1973), 26-45. [22642]

M. Brodmann: Algebraische Geometrie. Birkhäuser 1989. [1026]

R. Brüske/F. Ischebeck/F. Vogel: Kommutative Algebra. Bibl. Inst. 1989. [1224]

D. Bump: Algebraic geometry. World Scientific 2001. [16218]

T. Coquand/H. Lombardi: A short proof for the Krull dimension of a polynomial ring. Am. Math. Monthly 112 (2005), 826-829. [22443]

D. Cox/J. Little/D. O'Shea: Ideals, varieties, and algorithms. Springer 2007. [22312]

D. Cox/J. Little/D. O' Shea: Using algebraic geometry. Springer 2005. [18321]

D. Dummit/R. Foote: Abstract algebra. Wiley 2004. [16966]

D. Eisenbud: Commutative algebra with a view toward algebraic geometry. Springer 1995. [11998]

R. Engelking: General topology. Heldermann 1989. [715]

J. Eschgfäller: Almost topological spaces. Ann. Univ. Ferrara 30 (1984), 163-183. [7331]

K. Fieseler/L. Kaup: Algebraische Geometrie. Heldermann 2005. [19875]

S. Gabelli: Teoria delle equazioni e teoria di Galois. Springer 2008. [21928]

M. Gasca/T. Sauer: On the history of multivariate polynomial interpolation. J. Comp. Appl. Math. 122 (2000), 23-35. [22532]

S. Gelfand/Yu. Manin: Methods of homological algebra.

Springer 2010. [21952]

U. Görtz/T. Wedhorn: Algebraic geometry I. Vieweg 2010. [21712]

G. Greuel/G. Pfister: A SINGULAR introduction to commutative algebra. Springer 2002. [16045]

R. Hartshorne: Algebraic geometry. Springer 1977. [1470]

B. Hassett: Introduction to algebraic geometry. Cambridge UP 2008. [21988]

D. Heldt/M. Kreuzer/S. Pokutta/H. Poulisse: Algebraische Modellierung mit Methoden der approximativen Computeralgebra und Anwendungen in der Ölindustrie. OR-News November 2006, 5p. [20478]

D. Heldt/M. Kreuzer/S. Pokutta/H. Poulisse: Approximate computation of zero-dimensional polynomial ideals. J. Symb. Comp. 44 (2009), 1566-1591. [22676]

F. Hirzebruch/W. Scharlau: Einführung in die Funktionalanalysis. Bibl. Inst. 1971. [1145]

A. Holme: A royal road to algebraic geometry. Springer 2011. [22469]

M. Kashiwara/P. Schapira: Categories and sheaves. Springer 2010. [22258]

O. Keller: Vorlesungen über algebraische Geometrie. Akademische Verlagsgesellschaft 1974. [1760]

G. Kemper: A course in commutative algebra. Springer 2011. [21951]

M. Kreuzer/H. Poulisse/L. Robbiano: From oil fields to Hilbert schemes. In L. Robbiano/J. Abbott (ed.): Approximate commutative algebra. Springer 2009, 1-54. [22678]

M. Kreuzer/L. Robbiano: Computational commutative algebra 1. Springer 2000. [16944]

T. Lam/M. Reyes: A prime ideal principle in commutative algebra. J. Algebra 319/7 (2008), 3006-3027. [21984]

C. Leardini: Reti di Petri e analisi formale di concetti. Tesi LS Univ. Ferrara 2010. [21719]

H. Matsumura: Commutative ring theory. Cambridge UP 2002. [2460]

C. Menini: Categories. Appunti Univ. Ferrara, 2009. [21831]

D. Mumford: The red book of varieties and schemes. Springer LN Math. 1358 (1999). [22023]

B. Pareigis: Kategorien und Funktoren. Teubner 1969. [5943]

D. Patil/U. Storch: Introduction to algebraic geometry and commutative algebra. World Scientific 2010. [22111]

D. Perrin: Algebraic geometry. Springer 2008. [21031]

D. Pumplün: Elemente der Kategorientheorie. Spektrum 1999. [16260]

M. Reid: Undergraduate commutative algebra. Cambridge UP 1995. [16215]

H. Reiffen/G. Scheja/U. Vetter: Algebra. Bibl. Inst. 1969. [1799]

G. Scheja/U. Storch: Lehrbuch der Algebra. 2 volumi. Teubner 1994. [1589]

H. Schenck: Computational algebraic geometry. Cambridge UP 2003. [16216]

H. Schubert: Kategorien. 2 volumes. Springer 1970. [5945]

A. Seidenberg: A note on the dimension theory of rings. Pac. J. Math. 3 (1953), 505-512. [22456]

A. Seidenberg: On the dimension theory of rings II. Pac. J. Math. 4 (1954), 603-614. [22457]

H. Stetter: Numerical polynomial algebra. SIAM 2004. [18343]

Z. Semadeni/A. Wiweger: Einführung in die Theorie der Kategorien und Funktoren. Teubner 1979. [1141]

B. Tennison: Sheaf theory. Cambridge UP 2007. [22704]

J. Watkins: Topics in commutative ring theory. Princeton UP 2007. [22453]