Università degli Studi Roma Tre
Dipartimento di Matematica e Fisica
Corso di Laurea Magistrale in Matematica

Sintesi della Tesi di Laurea Magistrale in Matematica

Polinomi a valori interi su insiemi di interi algebrici

Candidato
Lorenzo Guerrieri

Relatore
Prof.ssa Stefania Gabelli

Anno Accademico 2013-14
Ottobre 2014

Classificazione AMS: 13F20,13B25,11C08,11C20
Parole chiave: Polinomi a valori interi, Interi algebrici di grado limitato, Domini di Prüfer, Sottoinsiemi polinomialmente densi, Chiusura integrale.

Introduzione

Per tutti i numeri interi positivi x e $n \geq 0$, il coefficiente binomiale $\binom{x}{n}$ è chiaramente un numero intero e quindi il polinomio $\binom{X}{n} := \frac{X(X-1)\ldots(X-n+1)}{n!}$, dove $\binom{X}{0} := 1$, assume valori interi su tutti i numeri interi anche se i suoi coefficienti sono razionali. Questi tipi di polinomi sono esempi di polinomi a valori interi e sono noti fin dal 1600. Essi erano infatti usati nelle formule di interpolazione per approssimare le funzioni a valori reali. In particolare, compaiono nella formula di interpolazione di Gregory-Newton, che permette di espandere in una sommatoria di polinomi una funzione f di variabile reale in modo simile allo sviluppo in serie di Taylor-MacLaurin. Usando queste formule si ottiene infatti:

$$f(hx) \approx \sum_{k=0}^{n} \Delta^k f(0) \frac{x(x-1)\ldots(x-k+1)}{k!}$$

dove le differenze finite $\Delta^k f(0)$ sono definite, per $k \geq 0$, come:

$$\Delta^0 f(0) = f(h) - f(0) \text{ e } \Delta^k f(0) = \Delta(\Delta^{k-1} f(0)).$$

Questa formula esprime l'interpolazione della funzione f nei punti equidistanti $0, h, \ldots, nh$. Usando la formula di Gregory-Newton quando f è un polinomio di grado n e l'incremento h è uguale ad 1, è stato dimostrato che tutti i polinomi a valori interi sono esprimibili come combinazione lineare dei polinomi del tipo $\binom{X}{n}$.

Fino all'inizio del 1900 i polinomi a valori interi furono usati solo per scopi di calcolo e approssimazione, successivamente iniziarono invece ad essere studiati in una forma più sistematica come oggetti matematici in sé. Precisamente, nel 1919 furono pubblicati due articoli di Georg Polya e Alexander Ostrowski, entrambi intitolati **"Über ganzwertige Polynome in algebraischen Zahlkörpern"**, nei quali i polinomi a valori interi vennero studiati con metodi algebrici moderni. Polya e Ostrowski studiarono la struttura di $\mathbb{Z}$-modulo dei polinomi a valori interi su $\mathbb{Z}$ e considerarono anche polinomi a valori interi sugli anelli di interi algebrici di un campo numerico, cioè un'estensione algebrica finita di $\mathbb{Q}$. Un esempio di questi ultimi è il polinomio $\frac{X(X-1)}{i+1}$ che assume valori interi su tutti gli interi di Gauss e appartiene a $\mathbb{Q}[i][X]$ ma non a $\mathbb{Z}[i][X]$.

Ricordiamo che un intero algebrico α è un numero complesso che soddisfa una relazione di interezza su $\mathbb{Z}$, cioè è un numero tale che esista un polinomio monico $f \in \mathbb{Z}[X]$ con $f(\alpha) = 0$. Dato un campo $K = \mathbb{Q}(\theta)$, estensione algebrica finita di $\mathbb{Q}$, l'anello degli interi algebrici di K, denotato con $\mathcal{O}_K$, è definito come l'intersezione tra il campo K e l'anello $\mathcal{A}_\infty$ di tutti gli interi algebrici.

Polya si chiese quando l'insieme dei polinomi a valori interi a coefficienti in un campo K avesse una base come $\mathcal{O}_K$-modulo, come accade nel caso $K = \mathbb{Q}$. Più precisamente, cercò di capire in quali casi esista una base regolare, cioè una successione di polinomi a valori interi $\{f_k\}$ tale che f_k abbia grado k e ogni polinomio a valori interi f di grado n possa essere scritto nella forma:

$$f = a_0 f_0 + a_1 f_1 + \cdots + a_n f_n$$

con i coefficienti $a_k \in \mathcal{O}_K$.
In generale, l'esistenza di una base regolare dipende dalla struttura di alcuni particolari $\mathcal{O}_K$-moduli $\mathcal{I}_n$, generati dai coefficienti direttori dei polinomi a valori interi di grado n. È infatti stato dimostrato che i polinomi a valori interi sull'anello $\mathcal{O}_K$ hanno una base regolare se e solo se $\mathcal{I}_n$ è principale per ogni n.
Un passo avanti nello studio di questi argomenti ci fu nel 1936 con il lavoro di Thoralf Skolem. Egli considerò i polinomi a valori interi non più solo come uno $\mathbb{Z}$-modulo, ma anche con la struttura di anello e provò una particolare proprietà simile all'identità di Bezout. Mostrò infatti che, presi alcuni polinomi a valori interi $f_1, \ldots, f_m$ tali che $\mathrm{MCD}(f_1(a), \ldots, f_m(a)) = 1$ per ogni intero a, allora esistono altri polinomi a valori interi $f_1, \ldots, f_m$ tali che:

$$f_1 g_1 + \cdots + f_m g_m = 1.$$

Si può notare che questa proprietà non vale in generale in $\mathbb{Z}[X]$.
L'anello dei polinomi a valori interi su un qualsiasi dominio D con campo dei quozienti K viene formalmente definito come:

$$\mathrm{Int}(D) := \{f \in K[X] \mid f(D) \subseteq D\}.$$

Tra il 1971 e il 1977, grazie a numerosi contributi di Paul-Jean Cahen e Jean-Luc Chabert, lo studio di $\mathrm{Int}(D)$ raggiunse un alto livello di generalità e completezza. I due studiosi proposero dei lavori trattanti la struttura degli ideali e le proprietà moltiplicative e topologiche di questi anelli.
In quegli anni furono affrontati anche problemi relativi ai polinomi a valori interi su sottoinsiemi di K. Se E è un sottoinsieme di K si può definire:

$$\mathrm{Int}(E, D) := \{f \in K[X] \mid f(E) \subseteq D\}.$$

Alcuni lavori furono dedicati a capire quali sottoinsiemi E sono tali che $\mathrm{Int}(E, D) = \mathrm{Int}(D)$; in questo caso E sarà allora detto polinomialmente denso in D.
In particolare il lavoro di R. Gilmer del 1989, **"Sets that determine integer-valued polynomials"** ha permesso di caratterizzare completamente i sottoinsiemi polinomialmente densi di un qualsiasi dominio di Dedekind, quale ad esempio l'anello degli interi $\mathbb{Z}$ o quello degli interi algebrici di un campo K, $\mathcal{O}_K$.
Lo scopo di questo lavoro è quello di approfondire lo studio dei sottoinsiemi polinomialmente densi negli anelli di interi algebrici e più in generale studiare i polinomi a valori interi su insiemi qualsiasi di interi algebrici. Affronteremo degli interessanti problemi risolti recentemente seguendo principalmente l'articolo di Giulio Peruginelli **"Integer-Valued Polynomials over the set of algebraic integers of bounded degree"**. Come semplice conseguenza dei risultati di Gilmer, proveremo che, se $K = \mathbb{Q}(\theta)$ è un estensione algebrica di $\mathbb{Q}$ di grado $n \geq 1$ e denotiamo con $O_{K,n}$ l'insieme degli elementi di $\mathcal{O}_K$ di grado n su $\mathbb{Q}$, allora $O_{K,n}$ è polinomialmente denso in $\mathcal{O}_K$. Cioè si ha

$$\mathrm{Int}(O_{K,n}, \mathcal{O}_K) = \mathrm{Int}(\mathcal{O}_K).$$

In seguito lavoreremo a dei problemi più complicati. Dato un intero $n \geq 1$, studieremo l'anello dei polinomi a coefficienti razionali e a valori interi sull'insieme $\mathcal{A}_n$ formato da tutti gli interi algebrici di grado su $\mathbb{Q}$ minore o uguale a n. Questo anello, introdotto da Loper e Werner in un articolo del 2012 è definito come:

$$\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n) := \{f \in \mathbb{Q}[X] \mid f(\mathcal{A}_n) \subseteq \mathcal{A}_n\}.$$

Notiamo che $\mathcal{A}_n$ non è un anello, dunque a priori non è certo che l'insieme dei polinomi a valori interi su di esso formi un anello. Tuttavia ciò accade perché è possibile ottenere $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$ come intersezione di anelli di polinomi a valori interi di tipo classico.
Il risultato principale che dimostreremo alla fine di questa tesi è il seguente: se denotiamo con A_n l'insieme degli interi algebrici di grado esattamente uguale a n, allora vale che A_n è polinomialmente denso in $\mathcal{A}_n$, cioè:

$$\mathrm{Int}_{\mathbb{Q}}(A_n, \mathcal{A}_n) = \mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n).$$

Per dimostrare ciò, introdurremo l'anello dei polinomi a valori interi sulla $\mathbb{Z}$-algebra delle matrici $n \times n$ a coefficienti interi. Tale anello è definito come:

$$\mathrm{Int}(M_n(\mathbb{Z})) := \{f \in \mathbb{Q}[X] \mid f(M) \in M_n(\mathbb{Z}), \forall M \in M_n(\mathbb{Z})\}.$$

Gli anelli di polinomi a valori interi su matrici sono l'esempio tipico dei più generali anelli di polinomi a valori interi su algebre. Lo studio di questi tipi di anelli è cominciato a partire dai primi anni del 2000 grazie ai lavori di S. Frisch ed è stato portato avanti negli anni recenti grazie anche ai lavori di Loper, Werner e Peruginelli. Attualmente, si stanno sviluppando molte ricerche in questo settore dell'algebra.
Per provare che A_n è polinomialmente denso in $\mathcal{A}_n$, sarà fondamentale provare che l'anello $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$ è un dominio di Prüfer ed è la chiusura integrale dell'anello $\mathrm{Int}(M_n(\mathbb{Z}))$.
Tutti i risultati di base riguardanti gli anelli di polinomi a valori interi sono dimostrati seguendo principalmente il lavoro monografico sull'argomento **"Integer-Valued Polynomials"**, scritto da Cahen e Chabert e pubblicato nel 1997. Segue una sintesi degli argomenti trattati in questa tesi.

0.1 Generalità su anelli di polinomi a valori interi

Sia D un dominio con campo dei quozienti K, allora definiamo l'insieme dei polinomi a valori interi su D come:

$$\mathrm{Int}(D) := \{f \in K[X] \mid f(D) \subseteq D\}.$$

$\mathrm{Int}(D)$ è un anello ed è anche un D-modulo. Vale la seguente catena di inclusioni:

$$D[X] \subseteq \mathrm{Int}(D) \subseteq K[X].$$

Il primo esempio storicamente studiato di questi anelli è l'anello dei polinomi a valori interi su $\mathbb{Z}$:

$$\mathrm{Int}(\mathbb{Z}) := \{f \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}.$$

In questo caso sappiamo che le precedenti inclusioni sono tutte inclusioni proprie:

$$\mathbb{Z}[X] \subsetneq \mathrm{Int}(\mathbb{Z}) \subsetneq \mathbb{Q}[X].$$

Infatti, ad esempio, il polinomio $\dfrac{X(X-1)}{2} \in \mathrm{Int}(\mathbb{Z}) \setminus \mathbb{Z}[X]$, mentre $\dfrac{X}{2} \in \mathbb{Q}[X] \setminus \mathrm{Int}(\mathbb{Z})$.
Il polinomio $\dfrac{X(X-1)}{2}$ corrisponde al polinomio binomiale $\binom{X}{2}$. I polinomi binomiali sono definiti, per ogni $n \geq 1$, come:

$$\binom{X}{n} := \frac{X(X-1)\dots(X-n+1)}{n!}.$$

Si definisce convenzionalmente $\binom{X}{0} := 1$. È di verifica immediata che essi sono tutti polinomi a valori interi su $\mathbb{Z}$. In particolare è stato dimostrato che essi formano una base di $\mathrm{Int}(\mathbb{Z})$ come $\mathbb{Z}$-modulo, vale a dire che ogni polinomio a valori interi su $\mathbb{Z}$ può essere espresso in modo unico come combinazione lineare a coefficienti interi dei polinomi $\binom{X}{n}$.

Alcuni problemi basilari sull'anello dei polinomi a valori interi su un dominio D riguardano il comportamento rispetto alle localizzazioni con sottoinsiemi moltiplicativamente chiusi di D. È di rilevante importanza il seguente risultato:

Teorema 0.1.1. *Siano D un dominio noetheriano e $S \subseteq D$ una parte moltiplicativa, allora:*

$$S^{-1}Int(D) = Int(S^{-1}D).$$

Se per $\mathrm{Int}(D)$ vale la proprietà descritta nel precedente teorema, diremo che $\mathrm{Int}(D)$ si comporta bene sotto le localizzazioni.

Si può definire anche l'anello dei polinomi a valori interi su un sottoinsieme $E \subseteq K$:

$$\mathrm{Int}(E, D) := \{f \in K[X] \mid f(E) \subseteq D\}.$$

$\mathrm{Int}(E, D)$ è un anello contenuto in $K[X]$. Nel caso in cui E sia un sottoinsieme proprio di D, si osserva che valgono le seguenti inclusioni tra gli anelli di polinomi a valori interi associati:

$$D[X] \subseteq \mathrm{Int}(D) \subseteq \mathrm{Int}(E, D).$$

Studieremo dei casi in cui la seconda di queste inclusioni è un'uguaglianza. Diamo adesso le definizioni di chiusura polinomiale di un anello e di sottoinsiemi polinomialmente densi e polinomialmente chiusi:

Definizione 0.1.2. *Siano $E, F \subseteq K$:*

- *La chiusura polinomiale di E è l'insieme:*

$$\overline{E} := \{x \in K \ / \ f(x) \in D \ , \forall f \in Int(E, D)\}.$$

- *E e F si dicono polinomialmente $D-$equivalenti se $Int(E,D) = Int(F,D)$.*
- *se $E = \overline{E}$ allora E si dice polinomialmente chiuso.*
- *se E è polinomialmente $D-$equivalente a D o, equivalentemente, $\overline{E} = D$ allora E si dice polinomialmente denso in D.*

Diamo alcuni semplici esempi:
D è polinomialmente chiuso, infatti il polinomio X assume valori in D solo su D.
L'insieme $\mathbb{N}$ dei numeri naturali è polinomialmente denso in $\mathbb{Z}$: infatti un polinomio $f \in \mathbb{Q}[X]$ di grado $n \geq 0$, è a valori interi su $\mathbb{Z}$ se e solo se assume valori interi su $n+1$ interi consecutivi.
Se D è infinito, altri esempi di sottoinsiemi polinomialmente densi sono i sottoinsiemi cofiniti di D, cioè gli insiemi $E \subseteq D$ tali che $D \setminus E$ è finito.
È stato dimostrato da R. Gilmer [17] un risultato che ci da una caratterizzazione per i sottoinsiemi polinomialmente densi di un dominio di Dedekind D (dominio integralmente chiuso, noetheriano e di dimensione 1) con campi residui finiti.

Definizione 0.1.3. *Un sottoinsieme E di un dominio di Dedekind D si dice completo di potenze prime se contiene una collezione completa di residui di P^k in D, per ogni ideale primo P diverso da (0) e per ogni intero positivo k.*

Teorema 0.1.4. *Sia D un dominio di Dedekind con campi residui finiti e sia $E \subseteq D$, allora le seguenti condizioni sono equivalenti:*
(1) E è polinomialmente denso in D.
(2) E è completo di potenze prime.

0.2 L'anello $\mathbf{Int}(\mathcal{O}_K)$

In questa sezione parleremo dei polinomi a valori interi sugli anelli di interi algebrici.
Sia θ un numero intero algebrico, vale a dire un numero complesso che è radice di un polinomio monico a coefficienti interi e sia $K = \mathbb{Q}(\theta)$ l'estensione algebrica di $\mathbb{Q}$ generata da θ. I campi di questo tipo sono detti campi numerici.
Se denotiamo con $\mathcal{A}_\infty$ il campo di tutti i numeri interi algebrici, possiamo definire l'anello degli interi algebrici di K come:

$$\mathcal{O}_K := \mathcal{A}_\infty \cap K.$$

Questo anello è, per definizione, la chiusura integrale di $\mathbb{Z}$ in K e le sue proprietà sono oggetto di studio della Teoria Algebrica dei Numeri, scienza sviluppatasi verso la fine del 1800.
È stato dimostrato che, per ogni campo numerico K di grado n su $\mathbb{Q}$, l'anello $\mathcal{O}_K$ è un dominio di Dedekind ed è inoltre uno $\mathbb{Z}$-modulo libero di rango n (ammette cioè una base su $\mathbb{Z}$ di n elementi). Anche gli ideali di $\mathcal{O}_K$ sono $\mathbb{Z}$-moduli liberi di rango n e ciò implica che, per ogni ideale $I \neq 0$, il quoziente $\mathcal{O}_K/I$ è un anello finito e quindi $\mathcal{O}_K$ è un dominio con

tutti i campi residui finiti.
Il campo dei quozienti di $\mathcal{O}_K$ è il campo K, quindi definiamo classicamente l'anello dei polinomi a valori interi su $\mathcal{O}_K$ come:

$$\mathrm{Int}(\mathcal{O}_K) := \{f \in K[X] \mid f(\mathcal{O}_K) \subseteq \mathcal{O}_K\}.$$

Il seguente Teorema ci permette di conoscere una proprietà importante degli anelli di polinomi a valori interi su un dominio di Dedekind:

Teorema 0.2.1. *Sia D un dominio di Dedekind con campi residui finiti. Allora Int(D) è un dominio di Prüfer.*

Quindi, dal fatto che $\mathcal{O}_K$ è un dominio di Dedekind con campi residui finiti, segue che $\mathrm{Int}(\mathcal{O}_K)$ ha molte buone proprietà: esso è infatti un dominio di Prüfer (Teorema 0.2.1), si comporta bene sotto le localizzazioni (0.1.1) e gli può essere applicato il criterio di Gilmer (Teorema 0.1.4) per trovarne i sottoinsiemi polinomialmente densi. Usando tale criterio si ottiene che, se chiamiamo $O_{K,n}$ il sottoinsieme di $\mathcal{O}_K$ formato dagli elementi che hanno grado n su $\mathbb{Q}$, cioè:

$$O_{K,n} := \{\alpha \in \mathcal{O}_K \mid \mathbb{Q}(\alpha) = K\},$$

allora:

Teorema 0.2.2. *Sia K un campo numerico di grado n su $\mathbb{Q}$. Allora $O_{K,n}$ è polinomialmente denso in $\mathcal{O}_K$.*

Come conseguenza di questo risultato e del fatto che $O_{K,n} \subseteq \mathcal{O}_K \setminus \mathbb{Z}$ si ha che:

Corollario 0.2.3. *$\mathcal{O}_K \setminus \mathbb{Z}$ è polinomialmente denso in $\mathcal{O}_K$.*

Si può ora considerare l'anello dei polinomi a coefficienti razionali che assumono valori interi su $\mathcal{O}_K$, ottenuto come contrazione di $\mathrm{Int}(\mathcal{O}_K)$ su $\mathbb{Q}[X]$. Questo anello è stato introdotto da Loper e Werner in [20] e si denota:

$$\mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_K) := \mathrm{Int}(\mathcal{O}_K) \cap \mathbb{Q}[X].$$

Naturalmente $\mathbb{Z}[X] \subseteq \mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_K)$. Se un polinomio $f \in \mathbb{Q}[X]$ è tale che $f(\mathcal{O}_K \setminus \mathbb{Z}) \subseteq \mathcal{O}_K$, allora, per il precedente corollario, $f \in \mathrm{Int}(\mathcal{O}_K)$ e, dal fatto che $f(\mathbb{Z}) \subseteq \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$, segue che $\mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_K) \subsetneq \mathrm{Int}(\mathbb{Z})$.
Il contenimento è proprio, infatti per ogni campo numerico K esistono numeri primi p per i quali esiste un ideale primo di $\mathcal{O}_K$ al di sopra di essi, il cui campo residuo contiene strettamente $\mathbb{F}_p$. Per tali primi p, il polinomio $\frac{X(X-1)\ldots(X-p+1)}{p}$ è in $\mathrm{Int}(\mathbb{Z})$ ma non in $\mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_K)$.
In [20] viene introdotto un altro anello di polinomi a valori interi. Dato un intero $n \geq 1$, denotiamo con $\mathcal{A}_n$ l'insieme degli interi algebrici di grado minore o uguale a n. Definiamo:

$$\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n) := \{f \in \mathbb{Q}[X] \mid f(\mathcal{A}_n) \subseteq \mathcal{A}_n\}.$$

Questo anello non è un anello classico di polinomi a valori interi; infatti l'insieme $\mathcal{A}_n$ non è un anello (ad esempio $\sqrt{2}, \sqrt{3} \in \mathcal{A}_2$ ma $\sqrt{2}+\sqrt{3} \notin \mathcal{A}_2$ perché ha grado 4 su $\mathbb{Q}$). Tuttavia le sue proprietà possono essere studiate esprimendolo come intersezione di anelli del tipo $\mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_K)$. Si verifica infatti facilmente che:

$$\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n) = \bigcap_{[K:\mathbb{Q}]\leq n} \mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_K),$$

dove l'intersezione è fatta sui campi numerici K di grado su $\mathbb{Q}$ minore o uguale ad n.
Si può osservare che, se α è un intero algebrico e $f \in \mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_{\mathbb{Q}(\alpha)})$ è un polinomio, allora $f(\alpha)$ è un intero algebrico di grado minore o uguale al grado di α. Abbiamo dunque l'uguaglianza $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n) = \mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n, \mathcal{A}_\infty)$.
Gli anelli $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$ e $\mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_K)$ risultano difficili da studiare perché ad essi non possono essere applicate le stesse tecniche che si usano per anelli classici di polinomi a valori interi, ma alcuni risultati sono stati ottenuti. È stato provato in [20] che questi anelli sono entrambi domini di Prüfer, la dimostrazione di ciò utilizza argomenti di teoria delle valutazioni.
Nel proseguimento di questo lavoro viene provato un risultato di Peruginelli [27], che mostra che gli interi algebrici di grado su $\mathbb{Q}$ esattamente uguale ad n formano un sottoinsieme polinomialmente denso di $\mathcal{A}_n$. Indicheremo questo insieme con A_n. Abbiamo quindi che:

Teorema 0.2.4. *Per ogni $n \geq 1$, A_n è polinomialmente denso in $\mathcal{A}_n$.*

0.3 Polinomi a valori interi su matrici

Siano D un dominio con campo dei quozienti K, $n \geq 1$ un numero intero e $M_n(D)$ la D-algebra delle matrici $n \times n$ a coefficienti in D. Dato un polinomio $f(X) = \sum_{j=0}^{m} a_j X^j$ a coefficienti in K e una matrice $M \in M_n(D)$, allora la matrice $f(M)$, ottenuta come $\sum_{j=0}^{m} a_j M^j$ (ponendo convenzionalmente $M^0 = I_n$), sarà generalmente una matrice ad entrate in K. Tuttavia, se $f(M)$ ha tutte le entrate in D, diremo che f è a valori interi su M.
Allora definiamo l'insieme:

$$\mathrm{Int}(M_n(D)) := \{f \in K[X] \mid f(M) \in M_n(D), \forall M \in M_n(D)\}$$

come l'insieme dei polinomi a valori interi su $M_n(D)$.
Si verifica facilmente che $\mathrm{Int}(M_n(D))$ è un anello che contiene $D[X]$ e, osservando che D può essere incluso in $M_n(D)$ tramite l'omomorfismo che manda ogni elemento $d \in D$ nella matrice dI_n, si vede anche che $\mathrm{Int}(M_n(D))$ è un sottoanello di $\mathrm{Int}(D)$.

Definizione 0.3.1. *Sia D un dominio e sia $M \in M_n(D)$, con $n \geq 2$. Allora l'annullatore di M in $D[X]$ è l'insieme: $N_{D[X]}(M) := \{g \in D[X] \,|\, g(M) = 0\}$.*

L'annullatore di una matrice M in $D[X]$ è un ideale di $D[X]$ ed è sempre non vuoto. Infatti, se indichiamo con p_M il polinomio caratteristico di M, abbiamo che, per il Teorema di Cayley-Hamilton, $p_M(M) = 0$ [1] e quindi $N_{D[X]}(M)$ contiene p_M.

Proposizione 0.3.2. *Sia $f(X) = g(X)/d \in K[X]$ con $g(X) \in D[X]$ e $d \in D \setminus \{0\}$. Allora:*

$$f(M) \in M_n(D) \Longleftrightarrow \overline{g} \in N_{\frac{D}{(d)}[X]}(\overline{M})$$

Dove con $\overline{g}$ e $\overline{M}$ si intendono le classi resto di g e di M modulo d.

Possiamo estendere questo risultato studiando i polinomi a valori interi su insiemi composti da più matrici.
Definiamo l'insieme $\mathcal{S} := \{f \in D[X] \,|\, f \text{ è monico di grado n}\}$. Se $S \subseteq \mathcal{S}$ denotiamo con $M_n^S(D)$ l'insieme delle matrici appartenenti a $M_n(D)$ il cui polinomio caratteristico p_M appartiene a S. Definiamo l'anello:

$$\mathrm{Int}(M_n^S(D)) := \mathrm{Int}(M_n^S(D), M_n(D)) := \{f \in K[X] \mid f(M) \in M_n(D), \forall M \in M_n^S\}$$

Nel caso particolare in cui $S = \{p(X)\}$ è composto da un solo polinomio, semplifichiamo la notazione ponendo: $M_n^S(D) = M_n^p(D) = \{M \in M_n(D) \text{ tali che } p_M = p\}$.
Possiamo inoltre osservare che $\mathrm{Int}(M_n^p(D)) = \bigcap_{M \in M_n^p} \mathrm{Int}\{M\}$ e quindi, per il risultato della proposizione precedente, si ha:

$$\mathrm{Int}(M_n^p(D)) = \Big\{ f(X) = \frac{g(X)}{d} \in K[X] \text{ tali che } \overline{g} \in \bigcap_{M \in M_n^p(D)} N_{\frac{D}{(d)}[X]}(\overline{M}) \Big\}.$$

L'intersezione degli annullatori delle matrici di polinomio caratteristico $p(X)$ è descritta dal seguente Lemma:

Lemma 0.3.3. *Sia D un anello commutativo e $p \in D[X]$. Allora*

$$\bigcap_{M \in M_n^p(D)} N_{D[X]}(M) = pD[X].$$

Da questo Lemma segue immediatamente la seguente caratterizzazione:

Lemma 0.3.4. *Sia $p \in \mathcal{S}$ e $f(X) = g(X)/d \in K[X]$, con $g(X) \in D[X]$, $d \in D$ e $d \neq 0$. Allora:*

$$f \in \mathit{Int}(M_n^p(D)) \Longleftrightarrow g \text{ è divisibile per } p \text{ mod } dD[X].$$

Corollario 0.3.5. *Per ogni polinomio $p \in \mathcal{S}$,*

$$\mathit{Int}(M_n^p(D)) = D[X] + p(X)K[X].$$

Dal fatto che $\mathrm{Int}(M_n^S(D)) = \bigcap_{p \in S} \mathrm{Int}(M_n^p(D))$, segue che:

Proposizione 0.3.6. *Sia $S \subseteq \mathcal{S}$ e $f(X) = g(X)/d \in K[X]$ allora:*

$$f \in \mathit{Int}(M_n^S(D)) \Longleftrightarrow g(X) \text{ è divisibile mod } dD[X] \text{ da ogni } p \in S$$

Osserviamo che quest'ultima proposizione ci da un metodo pratico per costruire polinomi in $\mathrm{Int}(M_n^S(D))$ nel caso in cui l'anello quoziente D/d sia finito. Infatti, preso un insieme completo di rappresentanti modulo d dei polinomi di S, il loro prodotto è sicuramente un polinomio in $\mathrm{Int}(M_n^S(D))$.

Consideriamo ora l'anello $\mathrm{Int}(M_n(\mathbb{Z}))$ dei polinomi a valori interi su matrici a coefficienti interi. In questo caso, i polinomi a valori interi sulle matrici con polinomio caratteristico irriducibile coincidono con quelli a valori interi su tutte le matrici in $M_n(\mathbb{Z})$.
Sia $\mathcal{S}_n^{irr} := \{p \in \mathbb{Z}[X] \text{ monici e irriducibili di grado n}\}$ e, per semplificare la notazione, denotiamo $M_n^{irr}(\mathbb{Z}) := M_n^{\mathcal{S}_n^{irr}}(\mathbb{Z})$. Dimostriamo dunque la seguente caratterizzazione di $\mathrm{Int}(M_n(\mathbb{Z}))$ [12, Prop.(6.2)]:

Proposizione 0.3.7. *Siano $n \geq 1$, $g \in \mathbb{Z}[X]$ e sia d un intero non nullo. Allora le seguenti condizioni sono equivalenti per un polinomio $f = g(X)/d \in \mathbb{Q}[X]$:*
(1) $f \in Int(M_n(\mathbb{Z}))$.
(2) g è divisibile modulo $d\mathbb{Z}[X]$ per tutti i polinomi in $\mathcal{S}_n$.
(3) g è divisibile modulo $d\mathbb{Z}[X]$ per tutti i polinomi in $\mathcal{S}_n^{irr}$.

L'importanza dell'anello $\mathrm{Int}(M_n(\mathbb{Z}))$ sta nel seguente risultato di Loper e Werner [20] che è fondamentale per ottenere la dimostrazione del Teorema 0.2.4.

Teorema 0.3.8. *Per ogni $n \geq 1$, l'anello $Int(M_n(\mathbb{Z}))$ non è integralmente chiuso e la sua chiusura integrale è $Int_{\mathbb{Q}}(\mathcal{A}_n)$.*

Un teorema simile al precedente riguarda gli anelli di polinomi a valori interi su matrici che hanno polinomio caratteristico (irriducibile) uguale al polinomio minimo di un intero algebrico appartenente a un fissato campo numerico K, estensione algebrica di $\mathbb{Q}$ di grado n. Si vede infatti facilmente che $\mathcal{S}_n^{irr} = \bigcup_{K \in Q_n} \mathcal{S}_{n,K}$, dove Q_n è l'insieme dei campi numerici di grado n su $\mathbb{Q}$ e $\mathcal{S}_{n,K}$ è l'insieme dei polinomi minimi degli interi algebrici di $\mathcal{O}_K$ di grado massimo n. Come notazione useremo $M_n^K(\mathbb{Z}) := M_n^{\mathcal{S}_{n,K}}(\mathbb{Z})$.
Definiamo dunque:

$$\mathrm{Int}(M_n^K(\mathbb{Z})) := \{f \in \mathbb{Q}[X] \mid f(M) \in M_n(\mathbb{Z}), \forall M \in M_n^K(\mathbb{Z})\}$$

L'anello di polinomi $\mathrm{Int}(M_n^K(\mathbb{Z}))$ contiene $\mathrm{Int}(M_n(\mathbb{Z}))$ e inoltre

$$\mathrm{Int}(M_n(\mathbb{Z})) = \bigcap_{K \in Q_n} \mathrm{Int}(M_n^K(\mathbb{Z})).$$

Non è immediato stabilire se $\mathrm{Int}(M_n^K(\mathbb{Z}))$ sia un sottoanello di $\mathrm{Int}(\mathbb{Z})$, ma ciò è una conseguenza del seguente teorema, provato da Peruginelli [27]:

Teorema 0.3.9. *Per ogni $n \geq 1$ e per ogni campo numerico K di grado n su $\mathbb{Q}$, $Int(M_n^K(\mathbb{Z}))$ non è integralmente chiuso e la sua chiusura integrale è $Int_{\mathbb{Q}}(\mathcal{O}_K)$.*

0.4 La chiusura integrale di $\mathbf{Int}(M_n(\mathbb{Z}))$

Per dimostrare il Teorema 0.3.8, in cui viene detto che l'anello dei polinomi a valori interi sulle matrici $\mathrm{Int}(M_n(\mathbb{Z}))$ ha come chiusura integrale l'anello $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$, abbiamo seguito il lavoro di Loper e Werner "**Generalized rings of integer-valued polynomials**" [20]. Il primo passo per ottenere il risultato cercato è quello di dimostrare che $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$ è un dominio di Prüfer.
Per fare ciò è necessario andare a descrivere gli anelli di valutazione al di sopra di $\mathrm{Int}(\mathbb{Z})$.
Abbiamo visto che $\mathrm{Int}(\mathbb{Z})$ è un dominio di Prüfer (segue dal Teorema 0.2.1 perché $\mathbb{Z}$ è un dominio di Dedekind con campi residui finiti) e quindi le sue localizzazioni negli ideali primi sono anelli di valutazione. Possiamo descrivere gli ideali primi di $\mathrm{Int}(\mathbb{Z})$ [5, Prop. V.2.7]:

Proposizione 0.4.1. *Per Int($\mathbb{Z}$) valgono le seguenti proprietà:*
1) Gli ideali primi di Int($\mathbb{Z}$) al di sopra di un ideale primo (p) di $\mathbb{Z}$ sono in corrispondenza biunivoca con gli elementi del completamento p-adico $\widehat{\mathbb{Z}_p}$ di $\mathbb{Z}$: ad ogni elemento $\alpha \in \widehat{\mathbb{Z}_p}$ corrisponde l'ideale massimale:

$$\mathfrak{M}_{p,\alpha} := \{f \in Int(\mathbb{Z}) \ , \ f(\alpha) \in \widehat{p\mathbb{Z}_p}\}.$$

Questi ideali non sono finitamente generati e quindi Int($\mathbb{Z}$) non è noetheriano.
2) Gli ideali primi non nulli al di sopra di (0) sono in corrispondenza biunivoca con i polinomi monici e irriducibili in $\mathbb{Q}[X]$. Ad ogni polinomio monico e irriducibile q corrisponde l'ideale:

$$\mathfrak{B}_q = q\mathbb{Q}[X] \cap Int(\mathbb{Z}).$$

3) L'ideale $\mathfrak{M}_{p,\alpha}$ è di altezza 1 se $\alpha \in \widehat{\mathbb{Z}_p}$ è trascendente su $\mathbb{Q}$, altrimenti contiene l'ideale primo $\mathfrak{B}_q$ dove q è il polinomio minimo di α e quindi ha altezza 2.
4) Gli ideali massimali di Int($\mathbb{Z}$) sono tutti e soli quelli del tipo $\mathfrak{M}_{p,\alpha}$.

Diremo che un sovranello di valutazione V di $\mathrm{Int}(\mathbb{Z})$ è unitario se è centrato su un ideale massimale di $\mathbb{Z}$, cioè se $V \cap \mathbb{Z} = p\mathbb{Z}$ per un certo numero primo $p \in \mathbb{Z}$.
Le localizzazioni rispetto agli ideali massimali sono gli anelli

$$V_{p,\alpha} := \mathrm{Int}(\mathbb{Z})_{\mathfrak{M}_{p,\alpha}} = \left\{ \frac{f(X)}{g(X)} \in \mathbb{Q}(X) \mid \frac{f(\alpha)}{g(\alpha)} \in \widehat{\mathbb{Z}_p} \right\}$$

dove $p \in \mathbb{Z}$ e α è un elemento del completamento p-adico $\widehat{\mathbb{Z}_p}$ di $\mathbb{Z}$. Per ogni p e per ogni α, l'anello $V_{p,\alpha}$ è un anello di valutazione unitario.
Gli anelli di valutazione non unitari sopra $\mathrm{Int}(\mathbb{Z})$ sono le localizzazioni di $\mathrm{Int}(\mathbb{Z})$ rispetto agli ideali primi non massimali $\mathfrak{B}_q$ e sono del tipo:

$$V_q := \mathrm{Int}(\mathbb{Z})_{\mathfrak{B}_q} = \left\{ \frac{g(X)}{h(X)} \in \mathbb{Q}(X) \mid q(X) \text{ non divide } h(X) \right\}.$$

dove $q \in \mathbb{Q}[X]$ è un polinomio irriducibile e non costante. Notiamo che, per ogni q, V_q contiene $\mathbb{Q}[X]$ e quindi coincide con l'anello di valutazione q-adica di $\mathbb{Q}[X]$. Abbiamo dunque che:

Proposizione 0.4.2. *Con le notazioni precedenti, valgono le seguenti proprietà:*
1) Gli anelli $V_{p,\alpha}$ sono sovranelli di valutazione unitari di Int($\mathbb{Z}$) e inoltre ogni sovranello di valutazione unitario di Int($\mathbb{Z}$) è del tipo $V_{p,\alpha}$ per qualche $p \in \mathbb{Z}$ e $\alpha \in \widehat{\mathbb{Z}_p}$.
2) Gli anelli V_q sono sovranelli di valutazione non unitari di Int($\mathbb{Z}$) e inoltre ogni sovranello di valutazione non unitario di Int($\mathbb{Z}$) è del tipo V_q per qualche polinomio $q \in \mathbb{Z}[X]$ irriducibile e non costante.
3) Il campo residuo di $V_{p,\alpha}$ è il campo con p elementi.
4) L'ideale massimale di $V_{p,\alpha}$ è l'ideale principale generato dal primo p.

Un anello di valutazione sopra Int($\mathbb{Z}$) è chiaramente anche un sovranello di valutazione di $\mathbb{Z}[X]$. Il prossimo risultato ci dice quando un sovranello di valutazione di $\mathbb{Z}[X]$ contiene anche Int($\mathbb{Z}$):

Proposizione 0.4.3. *Sia V un sovranello di valutazione unitario di $\mathbb{Z}[X]$ con ideale massimale M tale che esiste un primo p di $\mathbb{Z}$ appartenente a M. Allora V è un sovranello di valutazione di Int($\mathbb{Z}$) se e solo se valgono le seguenti proprietà:*
(a) $\mid V/M \mid = p$.
(b) $pV = M$.

Da questi fatti segue che Int($\mathbb{Z}$) è uguale all'intersezione dei suoi sovranelli di valutazione unitari, che sono infatti le sue localizzazioni negli ideali massimali.
Ora, per ogni numero primo p scegliamo una collezione $\mathcal{C}_p := \{V_i \mid i \in \Lambda_p\}$ di anelli di valutazione unitari al di sopra di $\mathbb{Z}[X]$, tali che le valutazioni a loro associate estendano la valutazione p-adica di $\mathbb{Q}$. Per ogni i, sia M_i l'ideale massimale di V_i e assumiamo che valgano le due seguenti condizioni:
$(*)$ esiste un intero positivo e_p tale che $M_i^{e_p} \subseteq pV_i$ per ogni $i \in \Lambda_p$.
$(**)$ esiste un intero positivo f_p tale che $\mid V_i/M_i \mid \leq p^{f_p}$ per ogni $i \in \Lambda_p$.

Notiamo che sotto queste condizioni l'ideale M_i è principale generato da un elemento π_i ed esiste un intero positivo t tale che $M_i^t = pV_i$.
Data questa collezione di anelli di valutazione definiamo:

$$D := \bigcap_{p \in \mathbb{P}} \Big(\bigcap_{i \in \Lambda_p} V_i \Big) \cap \mathbb{Q}[X],$$

Notiamo che se $e_p = f_p = 1$ per ogni primo p, allora la collezione è formata solamente dagli anelli di valutazione che soddisfano le proprietà (a) e (b) della Proposizione 0.4.3 e quindi $D = \text{Int}(\mathbb{Z})$.
Quindi intersecando un numero maggiore di anelli (alcuni dei quali non soddisfano le proprietà (a) e (b)), otterremo un sottoanello proprio di Int($\mathbb{Z}$). Vale il seguente teorema:

Teorema 0.4.4. *Il dominio D, definito come sopra, è un dominio di Prüfer.*

Per dimostrare questo risultato si fa vedere che le localizzazioni di D nei suoi ideali massimali sono anelli di valutazione.
Sia K un campo numerico di grado n su $\mathbb{Q}$. Gli anelli $\mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_K)$ e $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$ possono allora essere ottenuti come intersezione di sovranelli unitari di $\mathrm{Int}(\mathbb{Z})$ per i quali valgono le proprietà $(*)$ e $(**)$ ponendo, per ogni numero primo p, $e_p = f_p = n$ e quindi:

Teorema 0.4.5. *Per ogni campo numerico K, l'anello $Int_{\mathbb{Q}}(\mathcal{O}_K)$ è un dominio di Prüfer.*

Teorema 0.4.6. *Per ogni $n \geq 1$, $Int_{\mathbb{Q}}(\mathcal{A}_n)$ è un dominio di Prüfer.*

Si può dunque procedere con la dimostrazione del Teorema 0.3.8. Utilizzando la caratterizzazione degli elementi di $\mathrm{Int}(M_n(\mathbb{Z}))$ (Proposizione 0.3.7), si prova facilmente il seguente risultato:

Proposizione 0.4.7. *Per ogni $n \geq 1$, $Int(M_n(\mathbb{Z})) \subsetneq Int_{\mathbb{Q}}(\mathcal{A}_n)$.*

Da ciò segue che la chiusura integrale di $\mathrm{Int}(M_n(\mathbb{Z}))$ è contenuta nella chiusura integrale di $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$. Inoltre $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$ è di Prüfer, perciò è integralmente chiuso e quindi per provare il Teorema 0.3.8 è sufficiente mostrare che:

Teorema 0.4.8. *Per ogni $n \geq 1$, l'anello $Int_{\mathbb{Q}}(\mathcal{A}_n)$ è intero su $Int(M_n(\mathbb{Z}))$.*

0.5 Anelli di polinomi a valori interi su insiemi di interi algebrici

Adesso studiamo in generale gli anelli di polinomi a coefficienti in $\mathbb{Q}$ e a valori interi su insiemi arbitrari di interi algebrici. Si possono esprimere alcuni di questi anelli come pullback di $\mathbb{Q}[X]$ e trovare un legame tra essi e gli anelli di polinomi a valori interi su matrici a coefficienti in $\mathbb{Z}$. Dopo aver esaminato varie proprietà di tali anelli, si possono infine dimostrare il Teorema 0.3.9 e il Teorema 0.2.4.

Dati un intero algebrico α e un polinomio $f \in \mathbb{Q}[X]$, allora il valore $f(\alpha)$ è un elemento del campo numerico $K = \mathbb{Q}(\alpha)$ e, se $f(\alpha)$ è intero su $\mathbb{Z}$, allora esso deve appartenere all'anello degli interi algebrici di $\mathbb{Q}(\alpha)$, cioè $\mathcal{O}_K$. Ciò non accade sempre, infatti in generale $f(\alpha)$ potrebbe non essere intero su $\mathbb{Z}$. Se $f \in \mathbb{Z}[X]$, allora sicuramente $f(\alpha) \in \mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$, ma si possono trovare anche polinomi f non a coefficienti interi tali che $f(\alpha) \in \mathcal{O}_K$. Definiamo i due seguenti anelli:

$$R_\alpha := \mathrm{Int}_{\mathbb{Q}}(\{\alpha\}, \mathbb{Z}[\alpha]) = \{f \in \mathbb{Q}[X] \mid f(\alpha) \subseteq \mathbb{Z}[\alpha]\}$$

$$S_\alpha := \mathrm{Int}_{\mathbb{Q}}(\{\alpha\}, \mathcal{O}_K) = \{f \in \mathbb{Q}[X] \mid f(\alpha) \subseteq \mathcal{O}_K\}.$$

Notiamo che $\mathbb{Z}[X] \subset R_\alpha \subseteq S_\alpha \subset \mathbb{Q}[X]$, e quindi che R_α e S_α sono $\mathbb{Z}[X]$-algebre. Esaminiamo alcune proprietà di questi anelli.
In generale $\mathbb{Z}[\alpha]$ è contenuto in $\mathcal{O}_K$, il suo campo dei quozienti è sempre K ($\mathbb{Z}[\alpha]$ è un ordine di K) e la chiusura integrale di $\mathbb{Z}[\alpha]$ in K è ovviamente $\mathcal{O}_K$. Il contenimento tra R_α e S_α può essere stretto: ad esempio se $\alpha = 2\sqrt{2}$, allora $\mathcal{O}_K = \mathbb{Z}(\sqrt{2})$ e, se prendiamo $f = X/2$, allora $f \in S_\alpha \setminus R_\alpha$ ($\sqrt{2} \notin \mathbb{Z}[2\sqrt{2}]$).
Per questi anelli vale il seguente risultato:

Proposizione 0.5.1. *Sia α un intero algebrico e $K = \mathbb{Q}(\alpha)$. Allora $R_\alpha = S_\alpha$ se e solo se $\mathbb{Z}[\alpha] = \mathcal{O}_K$.*

Si dimostrano altre proprietà di R_α e S_α utilizzando risultati generali sui pullbacks [15].

Definizione 0.5.2. *Siano dati un anello commutativo A, un suo ideale I e un sottoanello B del quoziente $\frac{A}{I}$. Se π è l'omomorfismo canonico da A in $\frac{A}{I}$, diciamo che l'anello $D = \pi^{-1}(B)$ è il pullback del seguente diagramma commutativo:*

$$\begin{array}{ccc} D & \longrightarrow & B \\ \downarrow & & \downarrow \\ A & \xrightarrow{\pi} & \frac{A}{I} \end{array}$$

Proposizione 0.5.3. *Sia α un intero algebrico di grado $n \geq 1$. Allora R_α e S_α sono pullbacks di $\mathbb{Q}[X]$. In particolare $R_\alpha = \mathbb{Z}[X] + M_\alpha$, dove M_α è l'ideale massimale di $\mathbb{Q}[X]$ generato dal polinomio minimo di α su $\mathbb{Z}$, che indichiamo con $m_\alpha(X)$. Inoltre S_α è un dominio di Prüfer ed è la chiusura integrale di R_α nel suo campo dei quozienti $\mathbb{Q}(X)$.*

Questa proposizione e il Lemma 0.3.4 ci danno un collegamento immediato tra alcuni di questi anelli di polinomi e gli anelli di polinomi a valori interi sulle matrici:

Corollario 0.5.4. *Sia α un intero algebrico di grado $n \geq 1$ e $m_\alpha(X)$ il suo polinomio minimo. Allora:*

$$R_\alpha = Int(M_n^{m_\alpha}(\mathbb{Z})).$$

Possiamo costruire anelli di polinomi a valori interi su insiemi arbitrari di interi algebrici di grado limitato intersecando gli anelli del tipo R_α e S_α.
Sia $n \geq 1$ e sia $\mathcal{A}_n$ l'insieme di tutti gli interi algebrici di grado minore o uguale ad n. Dato un sottoinsieme $\mathcal{A} \subseteq \mathcal{A}_n$, definiamo:

$$\mathcal{R}_\mathcal{A} := \bigcap_{\alpha \in \mathcal{A}} R_\alpha \subseteq \mathcal{S}_\mathcal{A} := \bigcap_{\alpha \in \mathcal{A}} S_\alpha.$$

Notiamo che, come nel caso in cui $\mathcal{A}$ è composto da un solo elemento, si ha $\mathbb{Z}[X] \subset \mathcal{R}_\mathcal{A} \subseteq \mathcal{S}_\mathcal{A} \subset \mathbb{Q}[X]$, e quindi che $\mathcal{R}_\mathcal{A}$ e $\mathcal{S}_\mathcal{A}$ sono $\mathbb{Z}[X]$-algebre.
In generale per un insieme $\mathcal{A} \subseteq \mathcal{A}_n$ abbiamo $\mathcal{S}_\mathcal{A} = \mathrm{Int}_\mathbb{Q}(\mathcal{A}, \mathcal{A}_n)$. Nel caso $\mathcal{A} = \mathcal{A}_n$ otteniamo

chiaramente $\mathcal{S}_{\mathcal{A}_n} = \mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$ e se $n = 1$ otteniamo $\mathcal{S}_{\mathbb{Z}} = \mathrm{Int}(\mathbb{Z})$.
Dal fatto che $\mathcal{S}_{\mathcal{A}}$ è un sovranello di $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$, il quale è un dominio di Prüfer per il Teorema 0.4.6, segue il prossimo risultato:

Proposizione 0.5.5. *Sia $n \geq 1$. Per ogni sottoinsieme $\mathcal{A} \subseteq \mathcal{A}_n$ l'anello $\mathcal{S}_{\mathcal{A}}$ è un dominio di Prüfer.*

Il teorema fondamentale riguardante questi anelli è una generalizzazione del Teorema 0.3.8 e si dimostra in modo simile.

Teorema 0.5.6. *Sia $n \geq 1$. Allora, per ogni sottoinsieme $\mathcal{A}$ di $\mathcal{A}_n$, $\mathcal{S}_{\mathcal{A}}$ è la chiusura integrale di $\mathcal{R}_{\mathcal{A}}$.*

Da ciò seguono le dimostrazioni dei Teoremi 0.3.9 e 0.2.4.
Dato un insieme $S \subset \mathbb{Z}[X]$ di polinomi monici e irriducibili di grado n, vogliamo esprimere l'anello dei polinomi a valori interi su $M_n^S(\mathbb{Z})$ come intersezione degli anelli R_α. Siccome un polinomio monico e irriducibile a coefficienti interi è sempre il polinomio minimo di qualche intero algebrico, otteniamo:

$$\mathrm{Int}(M_n^S(\mathbb{Z})) = \bigcap_{p \in S} \mathrm{Int}(M_n^p(\mathbb{Z})) = \bigcap_{m_\alpha \in S} R_\alpha = \mathcal{R}_{\mathcal{A}(S)},$$

dove $\mathcal{A}(S) \subseteq \mathcal{A}_n$ è l'insieme delle radici in $\mathbb{C}$ dei polinomi $p(X) \in S$.
Risulta dunque:

$$\mathrm{Int}(M_n^S(\mathbb{Z})) = \mathcal{R}_{\mathcal{A}(S)} \subseteq \mathcal{S}_{\mathcal{A}(S)} = \mathrm{Int}_{\mathbb{Q}}(\mathcal{A}(S), \mathcal{A}_n).$$

Per il Teorema 0.5.6, si ha che $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}(S))$ è la chiusura integrale di $\mathrm{Int}(M_n^S(\mathbb{Z}))$. Da questo seguono facilmente i due risultati già anticipati:

Scegliendo S uguale all'insieme dei polinomi minimi degli interi algebrici di K di grado massimo n, si ha:

$$\mathrm{Int}(M_n^K(\mathbb{Z})) = \mathcal{R}_{O_{K,n}} \subseteq \mathcal{S}_{O_{K,n}} = \mathrm{Int}_{\mathbb{Q}}(O_{K,n}) = \mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_K),$$

dove l'ultima uguaglianza segue dal fatto che $O_{K,n}$ è polinomialmente denso in $\mathcal{O}_K$ (Teorema 0.2.2). Quindi, per il Teorema 0.5.6, $\mathrm{Int}_{\mathbb{Q}}(\mathcal{O}_K)$ è la chiusura integrale di $\mathrm{Int}(M_n^K(\mathbb{Z}))$. Inoltre, il contenimento è proprio, infatti i due anelli sarebbero uguali se e solo se, $\mathbb{Z}[\alpha] = \mathcal{O}_{\mathbb{Q}_\alpha}$ per ogni $\alpha \in O_{K,n}$. Ma ci sono moltissimi interi algebrici α per i quali ciò non vale.

Per provare che $\mathrm{Int}_{\mathbb{Q}}(A_n, \mathcal{A}_n) = \mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$, siccome $A_n = \bigcup_{K \in Q_n} O_{K,n}$ possiamo scrivere:

$$\mathrm{Int}(M_n(\mathbb{Z})) = \bigcap_{K \in Q_n} \mathrm{Int}(M_n^K(\mathbb{Z})) = \bigcap_{K \in Q_n} \mathcal{R}_{O_{K,n}} = \mathcal{R}_{A_n}.$$

Da ciò, per il Teorema 0.5.6, segue che la chiusura integrale di $\mathrm{Int}(M_n(\mathbb{Z}))$ è $\mathcal{S}_{A_n} = \mathrm{Int}_{\mathbb{Q}}(A_n, \mathcal{A}_n)$. Ma, per il Teorema 0.3.8, la chiusura integrale di $\mathrm{Int}(M_n(\mathbb{Z}))$ è $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$ e quindi tali due anelli sono uguali.

Bibliografia

[1] M.F. Atiyah, I.G. MacDonald. *Introduzione all'algebra commutativa.* Feltrinelli, Milano (1981)

[2] D. Brizolis. *A theorem on Prüfer rings of integer-valued polynomials.* Comm. Algebra 7, 1065-1077, (1979)

[3] W. C. Brown. *Matrices over Commutative Rings.* vol.169 of Pure and Applied Mathematics, Dekker, (1993)

[4] W. C. Brown. *Null ideals and spanning ranks of matrices.* Comm. Algebra 26, 2401-2417, (1998)

[5] P.-J. Cahen, J.-L. Chabert. *Integer-Valued Polynomials.* American Mathematical Society, Providence (1997)

[6] J.-L. Chabert, S.T. Chapman, W. W. Smith. *A Basis for the ring of Polynomials Integer-Valued on Prime Numbers.* European Journal of Combinatorics 28, 754-761, (2007)

[7] J.-L. Chabert, S.T. Chapman, W. W. Smith. *Algebraic Properties of the Ring of Integer-Valued Polynomials on Prime Numbers.* Communications in Algebra, 25(6), 1945-1959, (1997)

[8] J.-L. Chabert. *Anneaux de polynomes à valeurs entières et anneaux de Fatou.* Bull. Soc. Math. France 99, 273-283, (1971)

[9] J.-L. Chabert. *Les idéaux premiers de l'anneau des polynômes à valeurs entières.* J. reine angew. Math. 293/294, 275-283, (1977)

[10] J.-L. Chabert. *Un anneau de Prüfer.* J. Algebra 107, 1-17, (1987)

[11] J.-L. Chabert. *Une caractérisation des polynômes prenant des valeurs entières sur tous les nombres premiers.* Canadian Mathematical Bulletin, t. 39, 402-407, (1996)

[12] S. Frisch. *Integer-valued polynomials on algebras.* J. of Algebra 373, 414-425, (2013)

[13] S. Frisch. *Integrally Closed Domains, Minimal Polynomials, and Null ideals of Matrices.* Comm. Algebra 32, 2015-2017, (2004)

[14] S. Frisch. *Polynomial Separation of Points in Algebras.* S. Chapman(ed.), Arithmetical Properties of Commutative Rings and Modules (Chapel Hill Conf.), 249-254, Dekker (2005)

[15] S. Gabelli, E. Houston. *Ideal theory in pullbacks.* Non-Noetherian commutative ring theory, Math. Appl., 520 Kluwer Acad. Publ., Dordrecht, 199-227, (2000)

[16] R. Gilmer. *Multiplicative Ideal Theory.* Marcel Dekker Inc., New York (1972)

[17] R. Gilmer. *Sets that determine integer-valued polynomials.* J. Number Theory 33 no.1, 95-100, (1989)

[18] K. György. *Sur les polynômes à coefficients entiers et de discriminant donné.* III, Publ. Math. Debrecen 23, 419-426, (1976)

[19] D. Hilbert. *Die Theorie der algebraischen Zahlkörper.* in Jahresbericht der Deutschen Mathematiker-Vereinigung 4, 175-546, (1894-95)

[20] K.A. Loper, N.J. Werner. *Generalized rings of integer-valued polynomials.* J. Number Theory 132, 2481-2490, (2012)

[21] D.L. McQuillan. *On a theorem of R.Gilmer.* J. Number Theory 39, 245-250, (1991)

[22] D.L. McQuillan. *On ideals in Prüfer domains of polynomials.* Arch. Math. 45, 517-527, (1985)

[23] J.S. Milne. *Algebraic Number Theory.* (v3.04) disponibile online sul sito dell'autore www.jmilne.org/math/. (2012)

[24] J.S. Milne. *Fields and Galois Theory.* (v4.30) disponibile online sul sito dell'autore www.jmilne.org/math/. (2012)

[25] M. Nagata. *Local rings.* Interscience, New York, (1962)

[26] A. Ostrowski. *Über ganzwertige Polynome in algebraischen Zahlkörpern.* Ebenda, 117-124, (1919)

[27] G. Peruginelli. *Integral-Valued Polynomials over the set of algebraic integers of bounded degree.* J. Number Theory 137, 241-255, (2014)

[28] G. Peruginelli, N.J. Werner. *Integral closure of rings of integer-valued polynomials on algebras* Commutative Algebra: Recent Advances in Commutative Rings, Integer-Valued Polynomials, and Polynomial Functions, M. Fontana, S. Frisch and S. Glaz (editors), Springer, pp. 293-305 (2014)

[29] G. Polya. *Über ganzwertige Polynome in algebraischen Zahlkörpern.* Journal für die reine und angewandte Mathematik 149, 97-116, (1919)

[30] E. G. Strauss. *Functions periodic modulo each of a sequence of integers.* Duke Mathematical Journal 19, 379-395, (1952)