UNIVERSITÀ DEGLI STUDI DI PADOVA
Dipartimento di Matematica "Tullio Levi-Civita"

Corso di Laurea Magistrale in Matematica

Fattorizzazione non unica nell'anello dei polinomi a valori interi

Relatore:
Giulio Peruginelli

Candidato:
Sabrina Civiero
Numero di matricola: 1191588

3 Luglio 2020 - Anno Accademico 2019/2020

Indice

Introduzione

L'argomento centrale di questa tesi è lo studio dell'anello dei polinomi a valori interi

$$\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[x] |\, f(\mathbb{Z}) \subseteq \mathbb{Z}\}.$$

Mentre inizialmente l'interesse principale era rivolto ai domini a fattorizzazione unica (UFD), ossia domini in cui ogni elemento non nullo e non invertibile ammette un'unica fattorizzazione in irriducibili a meno dell'ordine dei fattori e della moltiplicazione per invertibili (fattorizzazioni di questo tipo sono dette essenzialmente uguali, in caso contrario essenzialmente diverse), negli ultimi decenni si è iniziata a prestare maggiore attenzione ai domini non UFD: il fatto che esistano elementi che presentano fattorizzazioni essenzialmente diverse può dare informazioni utili sul dominio considerato. Studi di questo tipo sono stati condotti, ad esempio, da Geroldinger e Halter-Koch in [10].
Nel caso particolare dell'anello dei polinomi a valori interi è sorprendente che, nonostante valgano le inclusioni $\mathbb{Z}[x] \subseteq \mathrm{Int}(\mathbb{Z}) \subseteq \mathbb{Q}[x]$, dove $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$ sono UFD, $\mathrm{Int}(\mathbb{Z})$ non possieda questa proprietà, anzi, dato un qualunque sottoinsieme finito di $\mathbb{N} \setminus \{1\}$ di cardinalità n, eventualmente con elementi ripetuti, esiste un polinomio in $\mathrm{Int}(\mathbb{Z})$ con n fattorizzazioni essenzialmente diverse di lunghezza uguale agli elementi del sottoinsieme considerato, come mostrato in [8]; da notare che questo vale per un sottoinsieme finito, infatti, non solo verrà provato che $\mathrm{Int}(\mathbb{Z})$ è un dominio atomico, cioè ogni elemento non nullo e non invertibile ammette fattorizzazione, ma, sfruttando la caratterizzazione degli irriducibili, si vedrà anche che il numero di fattorizzazioni di ogni elemento non nullo e non invertibile è finito.
Interessanti in un anello non UFD sono anche gli elementi non assolutamente irriducibili, ossia elementi irriducibili x che ammettono almeno una potenza con fattorizzazione essenzialmente diversa dal prodotto di copie di x. In [16], viene mostrato che in $\mathrm{Int}(\mathbb{Z})$ è possibile costruire elementi f di questo tipo, alcuni che presentano tutte le potenze f^k con $k > 1$ con fattorizzazione essenzialmente diversa da $f \cdots f$ (k volte) di lunghezza k, altri che ammettono solo particolari potenze di f con fattorizzazione essenzialmente diversa dal prodotto di copie di f, in particolare di lunghezza differente.
Un'altra peculiarità di $\mathrm{Int}(\mathbb{Z})$ è che pur non essendo un dominio di Krull,

ma un dominio di Prüfer, è tale che per ogni elemento non nullo f il sottomonoide $[[f]]$ di $\mathrm{Int}(\mathbb{Z})$ costituito dai divisori in $\mathrm{Int}(\mathbb{Z})$ delle potenze di f è un monoide di Krull, ossia possiede una teoria di divisione; tutto ciò viene analizzato nel dettaglio in [9]. In particolare, è interessante notare che in $[[f]]$ si possono studiare le fattorizzazioni del polinomio f considerato.
Prima di studiare le proprietà dell'anello $\mathrm{Int}(\mathbb{Z})$, nel primo capitolo, dopo un'introduzione contenente definizioni e risultati riguardanti la fattorizzazione, verrà presentata una condizione necessaria e sufficiente affinchè un particolare tipo di anelli, gli anelli degli interi di campi di numeri, siano UFD; questa condizione è basata sulla nozione di elementi assolutamente irriducibili, che, come si vedrà, presenta dei legami con gli ideali del dominio considerato. Al termine del capitolo verrà anche studiato un esempio di un anello degli interi di un campo di numeri non UFD, ossia $\mathbb{Z}[\sqrt{-5}]$, ma che, nonostante questo, presenta un'altra importante proprietà, detta semifattorialità.
I restanti capitoli sono interamente dedicati all'anello $\mathrm{Int}(\mathbb{Z})$. Inizialmente verranno ricordate alcune proprietà di base utili nelle dimostrazioni successive, ad esempio una caratterizzazione degli elementi irriducibili di questo anello. Nel secondo capitolo verrà poi dimostrato, dopo aver presentato due esempi particolari che permettono di dedurre delle caratteristiche di $\mathrm{Int}(\mathbb{Z})$, il fatto che è sempre possibile costruire un polinomio a valori interi con fattorizzazioni di lunghezze prefissate.
Il terzo capitolo, è dedicato allo studio degli elementi non assolutamente irriducibili dell'anello dei polinomi a valori interi, partendo dalla costruzione esplicita, spesso seguita da esempi numerici, di elementi di questo tipo, per poi passare a dei risultati più generali che permettono di affermare che un elemento di $\mathrm{Int}(\mathbb{Z})$ non è assolutamente irriducibile.
Nell'ultimo capitolo, infine, non si discuterà più di problemi legati alla fattorizzazione, ma, dopo aver introdotto tutte le definizioni e i risultati necessari, verrà mostrato che, dato $f \in \mathrm{Int}(\mathbb{Z})$ non nullo, il sottomonoide $[[f]]$ di $\mathrm{Int}(\mathbb{Z})$ è un monoide di Krull.

Capitolo 1

Domini a fattorizzazione unica

In questo capitolo, dopo aver ricordato le nozioni principali e alcuni risultati significativi che riguardano la fattorizzazione, verrà mostrato l'importante ruolo di un particolare tipo di elementi, gli elementi assolutamente irriducibili.

1.1 Fattorizzazione in anelli commutativi

Prima di poter parlare di fattorizzazione e presentare alcuni esempi, bisogna ricordare alcune definizioni legate al concetto di divisibilità in un anello commutativo con identità:

Definizione 1.1. Sia R anello commutativo con identità 1.

(i) Dati $a, b \in R$, si dice che b *divide* a ($b \mid a$) se $\exists\, c \in R$ t.c. $a = bc$;

(ii) Si dice che un elemento $u \in R$ è un'*unità* o *invertibile* se $u \mid 1$;

(iii) Due elementi $a, b \in R$ si dicono *associati* se $a \mid b$ e $b \mid a$, ossia se $\exists\, u \in R$ invertibile t.c. $a = ub$;

(iv) Un elemento r non nullo e non invertibile si dice *irriducibile* se da $r = ab$ con $a, b \in R$, segue che a o b è invertibile;

(v) Un elemento $p \in R$ si dice *primo* se da $p \mid ab$ segue che $p \mid a$ o $p \mid b$.

Osservazione 1.2. Siano $a, b \in R$ irriducibili con R anello commutativo con identità; se $b \mid a$, allora a e b sono associati.

Dimostrazione. Se $b \mid a$, allora $\exists\, c \in R$ tale che $a = bc$, ma, siccome b è irriducibile quindi non invertibile, c deve essere un'unità (anche a è irriducibile). □

Definizione 1.3. Sia R un anello commutativo con identità e sia $r \in R$ non nullo e non invertibile. Una *fattorizzazione* di r è una scrittura del tipo

$$r = r_1 \cdots r_n,$$

dove $r_i \in R$ sono irriducibili $\forall\, i \in \{1, ..., n\}$ e $n \geq 1$ viene detta *lunghezza della fattorizzazione*; l'insieme dei numeri naturali n tali che esiste una fattorizzazione di r di lunghezza n viene indicato con $\mathcal{L}(r)$.
Due fattorizzazioni $r = r_1 \cdots r_n = s_1 \cdots s_m$ sono dette *essenzialmente uguali* se $n = m$ e, a meno di riordinare i fattori, r_i e s_i sono associati $\forall\, i \in \{1, ..., n\}$; in caso contrario sono dette *essenzialmente diverse*.
Un dominio si dice *atomico* se ogni elemento non nullo e non invertibile ammette fattorizzazione, mentre si dice a *fattorizzazione unica* (UFD) se è atomico e ogni elemento non nullo e non unità ammette un'unica fattorizzazione, a meno di fattorizzazioni essenzialmente uguali.

Esempio 1.4. L'anello

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} |\, a, b \in \mathbb{Z}\},$$

non è un UFD, infatti, se si considera, ad esempio, $6 \in \mathbb{Z}[\sqrt{-5}]$, si ha che

$$6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$$

e le due fattorizzazioni sono essenzialmente diverse. Per prima cosa, bisogna mostrare che gli elementi che compaiono nella scrittura di 6 sono irriducibili e per questo si può sfruttare una proprietà della funzione *norma*

$$\begin{aligned} N : \mathbb{Z}[\sqrt{-5}] &\longrightarrow \mathbb{N} \\ a + b\sqrt{-5} &\longmapsto a^2 + 5b^2, \end{aligned}$$

ossia il fatto che $N(xy) = N(x)N(y)\ \forall\, x, y \in \mathbb{Z}[\sqrt{-5}]$. Si supponga, ad esempio, che $1 + \sqrt{-5} = xy$; per la proprietà precedente, $6 = N(1 + \sqrt{-5}) = N(xy) = N(x)N(y)$, da cui segue che, essendo elementi di $\mathbb{N}$, $N(x), N(y) \in \{1, 2, 3, 6\}$. Dal momento che $N(x) = a^2 + 5b^2 = 2$ o 3 non ha alcuna soluzione con $a, b \in \mathbb{Z}$, si deve avere che $N(x) = 1$ o $N(x) = 6$, da cui segue che uno tra x e y è un'unità, dove si è usato il fatto che $z \in \mathbb{Z}[\sqrt{-5}]$ è un'unità se e solo se $N(z) = 1$ (una dimostrazione si può trovare in [15]). Perciò $1 + \sqrt{-5}$ è irriducibile e allo stesso modo si può dimostrare che anche 2, 3 e $1 - \sqrt{-5}$ lo sono. Essendo, poi, ± 1 le uniche unità in $\mathbb{Z}[\sqrt{-5}]$, le due fattorizzazioni di 6 sono essenzialmente diverse.

Per poter presentare un secondo esempio di anello non UFD, bisogna ricordare che se D è un dominio, K il suo campo delle frazioni e $\emptyset \neq S \subseteq K$ un sottoinsieme, si può definire l'anello

$$\mathrm{Int}(S, D) = \{f(x) \in K[x] |\, f(S) \subseteq D\}, \tag{1.1}$$

chiamato l'*anello dei polinomi a valori interi su* S; nel caso in cui $S = D$, si pone $\mathrm{Int}(D) = \mathrm{Int}(S, D)$. E' importante osservare che gli elementi invertibili di $\mathrm{Int}(S, D)$ coincidono con gli elementi invertibili di D.

Esempio 1.5. Se nella definizione (1.1) si pone $D = S = \mathbb{Z}$ e $K = \mathbb{Q}$ si ottiene

$$\mathrm{Int}(\mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] | f(\mathbb{Z}) \subseteq \mathbb{Z}\},$$

chiamato semplicemente *anello dei polinomi a valori interi*, che risulta essere un anello non UFD, come si vedrà nel capitolo successivo; è interessante osservare che $\mathbb{Z}[x] \subseteq \mathrm{Int}(\mathbb{Z}) \subseteq \mathbb{Q}[x]$ e sia $\mathbb{Z}[x]$ che $\mathbb{Q}[x]$ sono UFD, ma $\mathrm{Int}(\mathbb{Z})$ non lo è.

I risultati successivi riguardano la nozione di dominio atomico e il legame che questa ha con la *condizione ascendente sugli ideali principali* (ACCP). Si dice che un dominio D soddisfa ACCP se ogni catena ascendente di ideali principali di D è stazionaria.

Osservazione 1.6. Ogni dominio che soddisfa ACCP è atomico.

Dimostrazione. Sia D un dominio che soddisfa ACCP. Si supponga per assurdo che esista un elemento $a_0 \in D$ non nullo e non invertibile che non ammette fattorizzazione. In particolare, a_0 non è irriducibile, dunque $\exists\, a_1, b_1 \in D$ non nulli e non invertibili tali che $a_0 = a_1 b_1$. Se sia a_1 che b_1 ammettessero fattorizzazione, allora lo stesso accadrebbe per a_0, perciò almeno uno dei due, sia questo a_1, non si può scrivere come prodotto finito di irriducibili, in particolare, non essendo irriducibile, $\exists\, a_2, b_2 \in D$ non nulli e non invertibili tali che $a_1 = a_2 b_2$. Continuando in questo modo, $\forall\, n \geq 0$ $a_n = a_{n+1} b_{n+1}$ $\exists\, a_{n+1}, b_{n+1} \in D$ non nulli e non invertibili. Si ottiene così la catena ascendente di ideali principali $(a_0) \subseteq (a_1) \subseteq \cdots \subseteq (a_n) \subseteq \cdots$, che risulta essere strettamente ascendente: se, infatti, $(a_n) = (a_{n+1})$, allora $\exists\, u \in D$ invertibile tale che $a_n = u a_{n+1}$, quindi $a_{n+1}(u - b_{n+1}) = 0$, ma, essendo D un dominio e $a_{n+1} \neq 0$, si ha che $b_{n+1} = u$ è invertibile contro le ipotesi. Tutto ciò genera una contraddizione dal momento che in un dominio che soddisfa ACCP non possono esistere catene strettamente ascendenti di ideali principali, dunque D deve essere atomico. □

Nonostante P.M. Cohn, in [7], abbia affermato, senza dimostrarla, l'equivalenza delle nozioni di dominio che soddisfa ACCP e dominio atomico, A. Grams, in [11], ha costruito un esempio di dominio atomico che, però, non soddisfa ACCP, mostrando così che il viceversa dell'Osservazione (1.6) non vale.

Lemma 1.7. *Sia* $\mathrm{Int}(S, D)$ *l'anello definito in (1.1) con* S *un sottoinsieme di* D *infinito. Allora* $\mathrm{Int}(S, D)$ *soddisfa ACCP* $\iff$ D *soddisfa ACCP.*

Dimostrazione. ($\Rightarrow$) Sia $\{a_nD\}_{n\in\mathbb{N}}$ una catena ascendente di ideali principali di D. Dal momento che $D \subseteq \mathrm{Int}(S,D)$, $\{a_n\mathrm{Int}(S,D)\}_{n\in\mathbb{N}}$ è una catena ascendente di ideali principali di $\mathrm{Int}(S,D)$, dunque per ipotesi è stazionaria, ossia $\exists\, n_0 \in \mathbb{N}$ tale che $a_n\mathrm{Int}(S,D) = a_{n_0}\mathrm{Int}(S,D)$ $\forall\, n \geq n_0$. Perciò $\forall\, n \geq n_0$ $\exists\, u_n \in \mathrm{Int}(S,D)$ invertibile tale che $a_n = u_n a_{n_0}$, ma, dal momento che gli elementi invertibili di $\mathrm{Int}(S,D)$ coincidono con gli elementi invertibili di D, si ha che $a_nD = a_{n_0}D$ $\forall\, n \geq n_0$, cioè la catena $\{a_nD\}_{n\in\mathbb{N}}$ è stazionaria.
($\Leftarrow$) Sia ora $\{f_n\mathrm{Int}(S,D)\}_{n\in\mathbb{N}}$ una catena ascendente di ideali principali di $\mathrm{Int}(S,D)$. Dal momento che $\mathrm{Int}(S,D) \subseteq K[x]$, $\{f_nK[x]\}_{n\in\mathbb{N}}$ è una catena ascendente di ideali principali di $K[x]$, dunque $\exists\, n_0 \in \mathbb{N}$ tale che $f_nK[x] = f_{n_0}K[x]$ $\forall\, n \geq n_0$ (siccome $K[x]$ è PID, è un anello noetheriano, dunque soddisfa ACCP). Quindi $\forall\, n \geq n_0$ $\exists\, u_n \in K$ non nullo tale che $f_n = u_n f_{n_0}$. Dal momento che S è infinito per ipotesi, $\exists\, a \in S$ tale che $f_{n_0}(a) \neq 0$, dunque $\{f_n(a)D\}_{n\in\mathbb{N}}$ è una catena ascendente di ideali principali di D. Siccome D soddisfa ACCP, $\exists\, m_0 \geq n_0$ tale che $f_n(a)D = f_{m_0}(a)D$ $\forall\, n \geq m_0 \geq n_0$, cioè $\forall\, n \geq m_0$ $\exists\, v_n \in D$ invertibile tale che $f_n(a) = v_n f_{m_0}(a)$, dunque $f_n = v_n f_{m_0}$ $\forall\, n \geq m_0$, dove v_n è un invertibile di $\mathrm{Int}(S,D)$ (questo deriva dal fatto che f_n e f_{m_0} erano già associati in $K[x]$). Quest'ultima affermazione permette di concludere che la catena $\{f_n\mathrm{Int}(S,D)\}_{n\in\mathbb{N}}$ è stazionaria. □

Corollario 1.8. *L'anello* $\mathrm{Int}(\mathbb{Z})$ *è atomico.*

Dimostrazione. Grazie al Lemma (1.7), dal momento che $\mathbb{Z}$ soddisfa ACCP, anche $\mathrm{Int}(\mathbb{Z})$ soddisfa ACCP, dunque è atomico (Osservazione (1.6)). □

Gli anelli di polinomi a valori interi permettono di costruire un esempio di dominio non atomico:

Lemma 1.9. *Sia* $\mathrm{Int}(S,D)$ *l'anello definito in (1.1). Se* D *non è un campo e* S *è finito, allora* $\mathrm{Int}(S,D)$ *non è un dominio atomico.*

Dimostrazione. Essendo S un insieme finito, $S = \{a_1, ..., a_k\}$ con $k \in \mathbb{N}$ e $a_i \in D$ $\forall\, i \in \{1, ..., k\}$. Al variare di $\emptyset \neq I \subsetneq \{1, ..., k\}$, si possono definire i polinomi

$$h_I(x) = \prod_{i\in I}(x - a_i)$$

e a partire da questi si pone

$$z = \prod_{\emptyset\neq I\subsetneq\{1,...,k\}} \prod_{j\notin I} h_I(a_j) = \prod_{\emptyset\neq I\subsetneq\{1,...,k\}} \prod_{j\notin I} \prod_{i\in I}(a_j - a_i).$$

Preso ora $d \in D$ non nullo e non invertibile, basta dimostrare che il polinomio

$$f(x) = \frac{\prod_{i=1}^{k}(x - a_i)}{zd}$$

non ammette fattorizzazione in irriducibili in $\mathrm{Int}(S,D)$. Per prima cosa, occorre notare che $f \in \mathrm{Int}(S,D)$, infatti, $f(a_i) = 0 \; \forall \, i \in \{1,...,k\}$; inoltre, f non è irriducibile in $\mathrm{Int}(S,D)$, infatti, preso un qualunque elemento non nullo e non invertibile $c \in D$, si ha che f si può scrivere come $f(x) = c \cdot \left(\frac{f(x)}{c}\right)$, dove nessuno dei due fattori è invertibile in $\mathrm{Int}(S,D)$ (gli invertibili di $\mathrm{Int}(S,D)$ coincidono con gli elementi invertibili di D, in particolare sono polinomi costanti). Allo stesso modo, si può vedere che i polinomi del tipo $\frac{f(x)}{c}$ con $c \in D$ non nullo non possono essere irriducibili in $\mathrm{Int}(S,D)$. A questo punto basta mostrare che f non si può scrivere come prodotto in $\mathrm{Int}(S,D)$ di due polinomi entrambi non costanti. Si supponga per assurdo che questo sia possibile, ossia che $f(x) = g(x)h(x)$ con $g, h \in \mathrm{Int}(S,D)$ non costanti. Siccome questa scrittura vale anche in $K[x]$ che è un UFD, allora si deve avere che

$$g(x) = \frac{b_1}{c_1} \prod_{i \in I} (x - a_i) \text{ e}$$
$$h(x) = \frac{b_2}{c_2} \prod_{j \in J} (x - a_j),$$

dove $I \sqcup J = \{1,...,k\}$ con $\emptyset \neq I \subsetneq \{1,...,k\}$ e $b_1, b_2, c_1, c_2 \in D$ non nulli, in particolare si ha che $\frac{b_1}{c_1} \cdot \frac{b_2}{c_2} = \frac{1}{zd}$, cioè $\frac{b_1}{c_1} \cdot \frac{b_2}{c_2} zd = 1$. Essendo $g, h \in \mathrm{Int}(S,D)$, presi $m \in J$ e $n \in I$, $g(a_m), h(a_n) \in D$ e, grazie alle scritture di g e h, si ottiene

$$g(a_m) = \frac{b_1}{c_1} h_I(a_m) \text{ e}$$
$$h(a_n) = \frac{b_2}{c_2} h_J(a_n).$$

Dal momento che $h_I(a_m)h_J(a_n) \mid z$ in D, vuol dire che $\exists \, y \in D$ tale che $z = h_I(a_m)h_J(a_n)y$, dunque

$$1 = \frac{b_1}{c_1} \cdot \frac{b_2}{c_2} zd = \frac{b_1}{c_1} \cdot \frac{b_2}{c_2} h_I(a_m)h_J(a_n)yd = \underbrace{g(a_m)h(a_n)y}_{\in D} d,$$

ossia d è invertibile in D, contro le ipotesi. □

Nel caso di domini atomico, si possono definire anche altre quantità:

Definizione 1.10. Sia R un dominio atomico, per ogni elemento non nullo e non invertibile $r \in R$ si può definire l'*elasticità* come

$$\rho(r) = \sup \left\{ \frac{m}{n} \middle| \, m, n \in \mathcal{L}(r) \right\},$$

mentre, indicato con R' l'insieme degli elementi di R non nulli e non invertibili, l'*elasticità* di R è la quantità

$$\rho(R) = \sup_{r \in R'}(\rho(r)).$$

Un dominio atomico R si dice *totalmente elastico* se ogni numero razionale più grande di 1 è l'elasticità di un qualche $r \in R$.

Osservazione 1.11. Se D è un UFD, allora $\rho(x) = 1 \ \forall\, x \in D$ non nullo e non invertibile, da cui segue che $\rho(D) = 1$. Si dice che un dominio D è *semifattoriale* (HFD) se $\rho(D) = 1$.

Si sa che, se D è un dominio, ogni elemento primo è irriducibile, il viceversa, invece, non vale in generale, ma vale, ad esempio, nel caso in cui D sia UFD:

Lemma 1.12. *Sia D un dominio atomico. D è un UFD se e solo se ogni elemento irriducibile è primo.*

Dimostrazione. ($\Rightarrow$) Sia $x \in D$ irriducibile, $x \mid ab$, allora $\exists\, y \in D$ tale che $ab = xy$. Dato che D è atomico, $a = a_1 \cdot \cdots a_n$ e $b = b_1 \cdot \cdots b_m$ con a_i, b_j irriducibili $\forall\, i, j$ e si ha che $a_1 \cdot \cdots a_n\, b_1 \cdot \cdots b_m = xy$. Essendo, però, D un UFD, x, che è irriducibile, deve essere associato a uno degli elementi a sinistra dell'uguale. Se x è associato ad a_i con $i \in \{1, ..., n\}$, allora $x \mid a$; se, invece, è associato a uno dei b_j con $j \in \{1, ..., m\}$, allora $x \mid b$.
($\Leftarrow$) Sia $x \in D$ e $x = a_1 \cdot \cdots a_n = b_1 \cdot \cdots b_m$ due fattorizzazioni di x, dove tutti i fattori coinvolti sono irriducibili, quindi primi. Si ha che, ad esempio, $a_1 \mid b_1 \cdots b_m$, dunque, dato che a_1 è primo, deve dividere uno dei fattori b_j con $j \in \{1, ..., m\}$, sia questo b_1, in particolare, a_1 e b_1 risultano essere associati (Osservazione (1.2)). Utilizzando lo stesso ragionamento con ognuno degli a_i con $i \in \{1, ..., n\}$, si ottiene che le due fattorizzazioni sono essenzialmente uguali. □

A questo punto, per poter poi presentare dei criteri di irriducibilità per i polinomi, utili nei problemi di fattorizzazione che verranno affrontati in seguito, è necessario ricordare le definizioni di contenuto e divisore fisso di un polinomio:

Definizione 1.13. Sia D un dominio.

(i) Se $f \in D[x]$, si definisce il *contenuto di f*, indicato con $\mathsf{c}(f)$, l'ideale di D generato dai coefficienti di f. Se D è PID e $f(x) = \sum_{i=0}^{n} a_i x^i$, dove $a_i \in D \ \forall\, i \in \{0, ..., n\}$ e $n = deg(f)$, si ha che

$$\mathsf{c}(f) = (\gcd\,(a_i |\, i \in \{0, ..., n\})).$$

Se $\mathsf{c}(f) = D$, allora f si dice *primitivo*.

(ii) Se $S \subseteq D$ e $f \in \mathrm{Int}(S, D)$ non nullo, si definisce *divisore fisso di f su S*, indicato con $\mathsf{d}_S(f)$, l'ideale di D generato da $f(S)$ (se $S = D$, si pone $\mathsf{d}_D(f) = \mathsf{d}(f)$). Se D è PID, si ha che

$$\mathsf{d}_S(f) = (\gcd(f(s) | \, s \in S)).$$

Se $\mathsf{d}_S(f) = D$, allora f si dice a *immagine primitiva su S*.

In seguito, nel caso in cui D sia PID, gli ideali $\mathsf{c}(f)$ e $\mathsf{d}_S(f)$ verranno identificati con uno dei generatori.

Il seguente risultato presenta delle proprietà del contenuto e del divisore fisso di un polinomio; la prima affermazione viene dimostrata nel caso in cui D sia un UFD in [14, Lemma 2, p.152], dove viene presentata con il nome di *Lemma di Gauss*, la seconda, invece, vale nel caso di un dominio D generico e $S \subseteq D$:

Lemma 1.14.

(i) Siano $f, g \in D[x]$ con D UFD, allora $\mathsf{c}(fg) = \mathsf{c}(f)\mathsf{c}(g)$;

(ii) Siano $f, g \in \mathrm{Int}(S, D)$ non nulli con D dominio e $S \subseteq D$, allora $\mathsf{d}_S(fg) \subseteq \mathsf{d}_S(f)\mathsf{d}_S(g)$ (nel caso in cui D sia PID, si ha che $\mathsf{d}_S(f)\mathsf{d}_S(g) \mid \mathsf{d}_S(fg)$).

Osservazione 1.15. Sia D un dominio, $S \subseteq D$ e $f \in D[x]$. Se $\mathsf{d}_S(f) = D$, allora $\mathsf{c}(f) = D$.

Dimostrazione. Sia $f(x) = \sum_{i=0}^{n} a_i x^i$ con $a_i \in D \ \forall\, i \in \{0, ..., n\}$. Per mostrare che $\mathsf{c}(f) = D$ basta provare che $1 \in \mathsf{c}(f)$. Siccome $\mathsf{d}_S(f) = D$, si ha che $1 = \sum_{s \in S} \alpha_s f(s)$ dove $\alpha_s \in D \ \forall\, s \in S$ e solo un numero finito di questi è non nullo. Allora

$$1 = \sum_{s \in S} \alpha_s f(s) = \sum_{s \in S} \alpha_s \left(\sum_{i=0}^{n} a_i s^i \right) = \sum_{i=0}^{n} a_i \underbrace{\left(\sum_{s \in S} \alpha_s s^i \right)}_{\in D},$$

dunque $1 \in \mathsf{c}(f)$ dal momento che quest'ultimo è l'ideale di D generato dagli a_i per $i \in \{0, ..., n\}$. □

Osservazione 1.16. Sia D un dominio, $S \subseteq D$ e $f \in \mathrm{Int}(S, D)$ tale che $\mathsf{d}_S(f) = D$. Allora $\mathsf{d}_S(f^n) = D \ \forall\, n \in \mathbb{N}$ e per ogni divisore g di f in $\mathrm{Int}(S, D)$ si ha che $\mathsf{d}_S(g) = D$ (Lemma (1.14)(ii)).

Delle conseguenze utili del Lemma di Gauss sono date dai seguenti risultati:

Lemma 1.17. *Sia D un UFD, K il suo campo delle frazioni e $f \in D[x]$ primitivo e non costante. Allora f è irriducibile in $D[x] \iff f$ è irriducibile in $K[x]$.*

Lemma 1.18. *Sia $f \in \mathbb{Z}[x]$ con $\mathsf{d}(f) = 1$; f è irriducibile in $\mathbb{Z}[x] \iff f$ è irriducibile in* $\mathrm{Int}(\mathbb{Z})$.

Dimostrazione. ($\Leftarrow$) Sia $f = gh$ con $g, h \in \mathbb{Z}[x] \subseteq \mathrm{Int}(\mathbb{Z})$. Siccome f è irriducibile in $\mathrm{Int}(\mathbb{Z})$, uno tra g e h deve essere invertibile in $\mathrm{Int}(\mathbb{Z})$, ma, essendo ± 1 gli unici invertibili in $\mathrm{Int}(\mathbb{Z})$ e anche in $\mathbb{Z}[x]$, uno tra g e h deve essere invertibile in $\mathbb{Z}[x]$.
($\Rightarrow$) Sia $f = gh$ con $g, h \in \mathrm{Int}(\mathbb{Z}) \subseteq \mathbb{Q}[x]$. Sicuramente f è non costante (se lo fosse, dato che $\mathsf{d}(f) = 1$, allora $f = \pm 1$, ma questo non è possibile perché f è irriducibile, dunque non invertibile), quindi, siccome è irriducibile in $\mathbb{Z}[x]$, è irriducibile anche in $\mathbb{Q}[x]$ (questo fatto discende dal Lemma di Gauss come viene mostrato in [14, Lemma 3, p.153]). Per questo motivo, uno tra g e h, si supponga sia g, deve essere invertibile in $\mathbb{Q}[x]$, ossia deve essere costante, in particolare, essendo un elemento in $\mathrm{Int}(\mathbb{Z})$, deve stare in $\mathbb{Q} \cap \mathrm{Int}(\mathbb{Z}) = \mathbb{Z}$. Dato che $\mathsf{d}(g) = 1$ (Lemma (1.14)(ii)), l'unico modo è che $g = \pm 1$, cioè che sia invertibile in $\mathrm{Int}(\mathbb{Z})$. □

Infine, è necessario ricordare un risultato che permette di determinare l'irriducibilità di un polinomio in $\mathbb{Z}[x]$:

Lemma 1.19 (*Criterio di Eisenstein*)**.** *Sia $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$. Se $\exists\, p \in \mathbb{Z}$ primo tale che $p \mid a_k\ \forall\, k \in \{0, ..., n-1\}$, $p \nmid a_n$ e $p^2 \nmid a_0$, allora f è irriducibile in $\mathbb{Z}[x]$.*

1.2 Elementi assolutamente irriducibili

Questa sezione, i cui risultati sono tratti da [6], è interamente dedicata a un particolare tipo di elementi irriducibili, detti assolutamente irriducibili, che stanno alla base della fattorizzazione unica di un particolare tipo di anelli che verrà presentato in seguito. Si parte, prima di tutto, dalla definizione:

Definizione 1.20. Sia R un anello commutativo con identità. Un elemento $r \in R$ irriducibile si dice *assolutamente irriducibile* se $\forall\, n \in \mathbb{N}$, $n > 1$, tutte le fattorizzazioni di r^n sono essenzialmente uguali a $r^n = r \cdots r$ (n volte); in caso contrario r è *non assolutamente irriducibile.*

Osservazione 1.21. Ogni elemento primo di un dominio D è assolutamente irriducibile.

Dimostrazione. Sia $p \in D$ un primo. Si può provare che ogni divisore irriducibile di p^n con $n \geq 1$ è associato a p, dunque p è irriducibile (caso $n = 1$) e assolutamente irriducibile. Sia, quindi, $q \in D$ irriducibile tale che $q \mid p^n$, allora $p^n = a_n q\ \exists\, a_n \in D$, ma, siccome p è primo, $p \mid a_n$ o $p \mid q$. Nel primo caso, si ha che $a_n = p a_{n-1}\ \exists\, a_{n-1} \in D$, dunque $p^n = p a_{n-1}\, q$ e, dal momento che D è un dominio, $p^{n-1} = a_{n-1} q$. Si può continuare in questo modo finchè non si ottiene che $p \mid q$ o finchè non si arriva a $p = a_1 q$. In questo caso,

$p \nmid a_1$: se fosse così, $p = pa_0\, q$, da cui seguirebbe che q è invertibile (non è possibile perchè è irriducibile). Quindi, in ogni caso, $p \mid q$, ma, dato che q è irriducibile, devono essere associati (Osservazione (1.2)). □

1.2.1 Relazione tra elementi assolutamente irriducibili e ideali

I risultati che verranno enunciati e dimostrati mettono in evidenza la relazione tra elementi assolutamente irriducibili e ideali di un dominio D. Per la dimostrazione del primo di questi, bisogna ricordare il seguente Lemma:

Lemma 1.22 (*Lemma di Zorn*)**.** *Sia $(\mathcal{I}, \leq)$ un insieme parzialmente ordinato con $\mathcal{I} \neq \emptyset$. Se ogni catena $\mathcal{C}$, ossia ogni sottoinsieme di $\mathcal{I}$ totalmente ordinato, ammette maggiorante, allora $\mathcal{I}$ ammette elemento massimale.*

Lemma 1.23. *Sia $x \in D$ irriducibile, x è assolutamente irriducibile $\iff$ per ogni $y \in D$ irriducibile non associato a x esiste P ideale primo di D tale che $x \notin P$ e $y \in P$ (si dice che x può essere separato da y tramite l'ideale primo P).*

Dimostrazione. ($\Rightarrow$) Sia $y \in D$ irriducibile non associato a x e si indichi con S l'insieme moltiplicativamente chiuso $\{x^n | \, n \in \mathbb{N}\}$. Allora $S \cap (y) = \emptyset$: si supponga per assurdo che $\exists\, z \in S \cap (y)$, dunque $z = x^n = yr \; \exists\, n \in \mathbb{N}, r \in D$, ma, essendo x assolutamente irriducibile, y dovrebbe essere associato a x, che è in contraddizione con le ipotesi su y. Sia ora

$$\mathcal{I} = \{I \text{ ideale di } D | \, (y) \subseteq I, S \cap I = \emptyset\},$$

ordinato tramite l'inclusione; il fatto che $S \cap (y) = \emptyset$ permette di dire che $\mathcal{I} \neq \emptyset$. Ogni catena $\mathcal{C} = \{I_k\}_{k \in K}$ in $\mathcal{I}$ ammette maggiorante: $I = \cup_{k \in K} I_k$ è un ideale di D, contiene (y) e ha intersezione vuota con S perché tutti gli I_k con $k \in K$ hanno queste due proprietà. Perciò per il Lemma di Zorn $\mathcal{I}$ ammette elemento massimale P. Dato che $S \cap P = \emptyset$ e $(y) \subseteq P$, allora $x \notin P$ e $y \in P$, quindi basta solo dimostrare che P è primo. Si supponga per assurdo che esistano $x_1, x_2 \notin P$ tali che $x_1 x_2 \in P$, allora, siccome $P \subsetneq (P, x_i)$ per $i = 1, 2$, per la massimalità di P si ha che $(P, x_i) \notin \mathcal{I}$, ossia $(P, x_i) \cap S \neq \emptyset$. Quindi $\exists\, s_i \in S$ per $i = 1, 2$ tali che $s_i \in (P, x_i)$, cioè $s_i = y_i + r_i x_i \; \exists\, y_i \in P, r_i \in D$. Si ha che l'elemento di S

$$s_1 s_2 = (y_1 + r_1 x_1)(y_2 + r_2 x_2) = y_1 y_2 + y_1 r_2 x_2 + r_1 x_1 y_2 + r_1 x_1 r_2 x_2$$

risulta essere anche in P, poiché P è un ideale e $x_1 x_2 \in P$, ma questo è assurdo perché $P \in \mathcal{I}$. Perciò P è primo.
($\Leftarrow$) Per mostrare che x è assolutamente irriducibile, basta mostrare che ogni divisore irriducibile y di x^n con $n > 1$ è associato a x. Si supponga per assurdo che y non sia associato a x, allora per ipotesi $\exists\, P$ ideale primo di D tale che $x \notin P$ e $y \in P$. Dato che $x^n = yr$, allora $x^n \in P$, la contraddizione viene dal fatto che P è primo, ma $x \notin P$. □

Lemma 1.24. *Sia $x \in D$ irriducibile, se $(x) = M^k$ con M ideale massimale di D e $k \in \mathbb{N}$, allora x può essere separato tramite un ideale primo da qualsiasi irriducibile y a esso non associato e tale che (y) è prodotto di ideali primi.*

Dimostrazione. Sia $y \in D$ irriducibile e non associato a x tale che $(y) = P_1 \cdots P_n$ con P_i primi per $i \in \{1, ..., n\}$. Si supponga per assurdo che $\forall\, Q$ ideale primo tale che $y \in Q$, si ha che $x \in Q$. Dato che $(y) = P_1 \cdots P_n \subseteq P_i$ $\forall\, i \in \{1, ..., n\}$, allora $y \in P_i$ e dunque anche $x \in P_i$. Perciò $\forall\, i \in \{1, ..., n\}$ $M^k = (x) \subseteq P_i$, da cui segue che $M \subseteq P_i$: sia $z \in M$, dato che P_i è primo, da $z^k \in P_i$ si ottiene che $z \in P_i$. Essendo, poi, M massimale e $P_i \neq D$ $\forall\, i \in \{1, ..., n\}$ (P_i primo), si deve avere che $M = P_i$ $\forall\, i \in \{1, ..., n\}$, dunque $(y) = M^n$. A questo punto si possono verificare due casi: se $k \leq n$, allora $M^n = (y) \subseteq (x) = M^k$ $(x \mid y)$; se, invece, $n \leq k$, allora $(x) = M^k \subseteq M^n = (y)$ $(y \mid x)$. In entrambi i casi x e y sono associati, poiché irriducibili (Osservazione (1.2)), e ciò contraddice le ipotesi iniziali. □

Lemma 1.25. *Sia $x \in D$ assolutamente irriducibile e (x) prodotto di ideali primi. Se per almeno uno di questi ideali primi, sia questo P, esiste y irriducibile tale che $(y) = P^m$ con $m \in \mathbb{N}$, allora $(x) = P^m$.*

Dimostrazione. Sia $(x) = P_1 \cdots P_n$ con P_i ideali primi $\forall\, i \in \{1, ..., n\}$, per ipotesi $(y) = P_i^m$ $\exists\, i \in \{1, ..., n\}, y \in D$ irriducibile. Sia Q un ideale primo tale che $y \in Q$, allora $P_i^m = (y) \subseteq Q$ e, essendo Q primo, $P_i \subseteq Q$. Siccome $(x) = P_1 \cdots P_n \subseteq P_i \subseteq Q$, si ha che $x \in Q$. Per il Lemma (1.23), x e y devono essere associati, ossia $(x) = (y) = P_i^m$. □

Osservazione 1.26. Un dominio D può possedere alcune o tutte queste proprietà:

(a) Ogni ideale principale generato da un elemento irriducibile di D è prodotto di ideali primi;

(b) Per ogni ideale primo non nullo P esiste m tale che $P^m = (y)$ con y irriducibile in D;

(c) Ogni ideale primo non nullo è massimale.

A seconda delle proprietà possedute dal dominio D considerato, valgono differenti condizioni come mostrato in questo Teorema:

Teorema 1.27. *Sia $x \in D$ irriducibile e si considerino le seguenti condizioni:*

(1) (x) è potenza di un ideale massimale;

(2) $rad(x)$ è un ideale massimale (da ricordare che, se I è un ideale di D, $rad(I) = \{x \in D |\, x^n \in I,\, \exists\, n \in \mathbb{N}\}$ viene detto ideale radicale di I);

(3) x è assolutamente irriducibile;

(4) (x) è potenza di un ideale primo.

Allora, con riferimento alle proprietà elencate nell'Osservazione (1.26),

(i) (1) $\Longrightarrow$ (2);

(ii) Se D soddisfa (c), allora (4) $\Longrightarrow$ (1);

(iii) Se D soddisfa (a), allora (2) $\Longrightarrow$ (1) $\Longrightarrow$ (3);

(iv) Se D soddisfa (a) e (b), allora (3) $\Longrightarrow$ (4).

Se D soddisfa (a), (b) e (c), allora (1) $\Longleftrightarrow$ (2) $\Longleftrightarrow$ (3) $\Longleftrightarrow$(4).

Dimostrazione.

(i) Omessa

(ii) Se $(x) = P^k$ con P primo che è anche massimale per ipotesi, allora (x) è potenza di un ideale massimale.

(iii) Dato che D soddisfa (a), $(x) = P_1 \cdots P_n$ con P_i ideali primi $\forall\, i \in \{1, ..., n\}$.
(2) $\Rightarrow$ (1) Per ipotesi $rad(x) = M$ con M ideale massimale. Se $y \in rad(x) = M$, $\exists\, k \in \mathbb{N}$ tale che $y^k \in (x) = P_1 \cdots P_n \subseteq P_i\ \forall\, i \in \{1, ..., n\}$, dunque $M \subseteq P_i \neq D$ e, dato che M è massimale, $P_i = M\ \forall\, i \in \{1, ..., n\}$, perciò $(x) = M^n$.
(1) $\Rightarrow$ (3) Segue dai Lemmi (1.23) e (1.24) (per tutti gli y irriducibili non associati a x il loro ideale principale è prodotto di ideali primi).

(iv) Segue dal Lemma (1.25).

□

1.2.2 Elementi assolutamente irriducibili e fattorizzazione unica

Mentre i risultati precedenti riguardavano un generico dominio D, ora verrà presentato un importante Teorema che mette in luce il ruolo fondamentale degli elementi assolutamente irriducibili nella fattorizzazione in particolari anelli, gli anelli degli interi di campi di numeri, di cui ora verrà ricordata la definizione e le principali caratteristiche.

Definizione 1.28. Un *campo di numeri* è un sottocampo di $\mathbb{C}$ che ha dimensione finita, come spazio vettoriale, su $\mathbb{Q}$; in particolare, si può dimostrare che ogni campo di numeri è della forma $\mathbb{Q}[\alpha]$, con $\alpha \in \mathbb{C}$ un elemento algebrico su $\mathbb{Q}$, ossia radice di un polinomio a coefficienti in $\mathbb{Q}$.

Definizione 1.29. Un elemento di $\mathbb{C}$ si dice *intero algebrico* se è radice di un polinomio monico a coefficienti in $\mathbb{Z}$. L'insieme degli interi algebrici di un campo di numeri viene detto *anello degli interi* di questo campo di numeri ed è un suo sottoanello.

Esempio 1.30. Il campo $\mathbb{Q}[\sqrt{-5}]$ è un campo di numeri, infatti $\sqrt{-5}$ è radice del polinomio $x^2+5 \in \mathbb{Q}[x]$, e il suo anello degli interi risulta essere $\mathbb{Z}[\sqrt{-5}]$, l'anello dell'esempio (1.4)(la dimostrazione di questo risultato si può trovare in [15, Corollary 2, p.11]).

Osservazione 1.31. Ogni anello degli interi di un campo di numeri possiede le proprietà (a), (b) e (c) elencate nell'Osservazione (1.26), in particolare la proprietà (a) deriva dal *Teorema fondamentale della teoria degli ideali* che afferma che ogni ideale non nullo e diverso dal dominio stesso è prodotto di ideali primi (le dimostrazioni di questi fatti si possono trovare in [15, Chapter 3]). Dunque , le condizioni (1), (2), (3) e (4) del Teorema (1.27) sono equivalenti, ossia un elemento irriducibile $x \in D$ è assolutamente irriducibile $\iff rad(x)$ è massimale $\iff (x)$ è potenza di un ideale massimale (dato che ideali primi e massimali coincidono, in queste equivalenze massimale può sempre essere sostituito con primo).

Dopo aver ricordato le definizioni necessarie, è possibile enunciare il Teorema più importante di questa sezione:

Teorema 1.32. *Sia D l'anello degli interi di un campo di numeri. Per ogni elemento non nullo e non invertibile $x \in D$ esistono x_1,..., $x_k \in D$ assolutamente irriducibili e $m \in \mathbb{N}$ minimale tale che*

$$x^m = x_1 \cdots x_k \tag{1.2}$$

e questa decomposizione, detta rappresentazione per decadimento atomico di x, è unica a meno dell'ordine dei fattori e della moltiplicazione per invertibili.

Dimostrazione. Sia $x \in D$ non nullo e non invertibile, allora (x) è non nullo e non coincide con l'intero D, dunque $(x) = P_1 \cdots P_k$, esistono degli ideali primi P_i con $i \in \{1, ..., k\}$, inoltre $\forall\, i \in \{1, ..., k\}\ \exists\, y_i$ irriducibili in D e $m_i \in \mathbb{N}$ tali che $(y_i) = P_i^{m_i}$, in particolare questo prova che y_i è assolutamente irriducibile (Osservazione (1.31)). Sia ora $m = \operatorname{lcm}(m_i |\, i \in \{1, ..., k\})$ e $m = m_i n_i$ con $n_i \in \mathbb{N}$, allora

$$(x^m) = (x)^m = \prod_{i=1}^{k} P_i^m = \prod_{i=1}^{k} (P_i^{m_i})^{n_i} = \prod_{i=1}^{k} (y_i)^{n_i} = \left(\prod_{i=1}^{k} y_i^{n_i} \right).$$

Dall'uguaglianza di questi due ideali si ottiene che x^m e $\prod_{i=1}^{k} y_i^{n_i}$ sono associati, cioè $\exists\, u \in D$ invertibile tale che $x^m = u \prod_{i=1}^{k} y_i^{n_i}$. A questo punto

basta notare che, ad esempio, uy_1, essendo associato a y_1, è assolutamente irriducibile (Teorema (1.27)), dunque $x^m = (uy_1)y_1^{n_1-1}\prod_{i=2}^{k} y_i^{n_i}$ è prodotto di elementi assolutamente irriducibili. Bisogna ora mostrare l'unicità della scrittura, siano $\prod_{i=1}^{k} x_i^{k_i} = \prod_{j=1}^{h} y_j^{h_j}$ con $x_i, y_j \in D$ assolutamente irriducibili, $k, h, k_i, h_j \in \mathbb{N}\ \forall\, i, j$. Per l'Osservazione (1.31), $(x_i) = P_i^{n_i}$ e $(y_j) = Q_j^{m_j}$ con P_i, Q_j ideali primi di D, $n_i, m_j \in \mathbb{N}\ \forall\, i, j$, quindi

$$\prod_{i=1}^{k} P_i^{k_i n_i} = \prod_{i=1}^{k} (x_i)^{k_i} = \prod_{j=1}^{h} (y_j)^{h_j} = \prod_{j=1}^{h} Q_j^{h_j m_j}.$$

Dato che questa scrittura è unica (Osservazione (1.31)), si ha che $k = h$, ogni P_i deve essere uguale a uno dei Q_j, a meno di riordinare i fattori, si può supporre che $P_i = Q_i$, $k_i = h_i$ e $n_i = m_i\ \forall\, i, j$, perciò $(x_i) = (y_i)$, ossia x_i e y_i sono associati. □

Corollario 1.33. *L'anello degli interi di un campo di numeri è UFD $\iff$ ogni elemento irriducibile è assolutamente irriducibile.*

Dimostrazione. Per prima cosa bisogna mostrare che D è atomico, sia, quindi, $x \in D$ non nullo e non invertibile. Se x è irriducibile non c'è nulla da mostrare, se, invece, x è riducibile, allora $\exists\, x_1, x_2 \in D$ non invertibili tali che $x = x_1 x_2$. Utilizzando le proprietà della funzione norma, definita in [15, Chapter 2], si ha che $N(x) = N(x_1)N(x_2)$. Se entrambi x_1 e x_2 sono irriducibili in D, allora questa è una fattorizzazione di x, altrimenti se uno o entrambi sono riducibili, si supponga ad esempio di essere nel secondo caso, anche questi si possono scrivere come $x_1 = y_1 y_2$ e $x_2 = z_1 z_2\ \exists\, y_1, y_2, z_1, z_2 \in D$ non invertibili. La norma di x diventa dunque $N(x) = N(y_1)N(y_2)N(z_1)N(z_2)$. Si può procedere in questo modo scrivendo ogni volta i fattori riducibili come prodotto di due non invertibili e questo procedimento deve terminare in un numero finito di passi perchè ogni fattore trovato ha norma che divide $N(x)$ e, essendo questa in $\mathbb{Z}$ (come viene dimostrato in [15, Corollary 2, p.16]), ammette fattorizzazione in irriducibili in $\mathbb{Z}$.
($\Rightarrow$) Sia $x \in D$ irriducibile. Se D è un UFD, allora tutte le fattorizzazioni di x^n con $n > 1$ sono essenzialmente uguali a

$$x^n = \underbrace{x \cdots x}_{n\ volte},$$

dunque tutti gli elementi irriducibili che dividono x^n devono essere associati a x, ossia x è assolutamente irriducibile.
($\Leftarrow$) Sia $x \in D$ non nullo e non invertibile. Dato che D è atomico,

$$x = x_1 \cdots x_n$$

con $x_i \in D$ irriducibili $\forall\, i \in \{1, ..., n\}$. Dal momento che, però, tutti gli x_i sono assolutamente irriducibili, si ottiene l'unicità della decomposizione (Teorema (1.32)), dunque D è UFD. □

Negli anelli degli interi di campi di numeri che non sono UFD è interessante analizzare la relazione tra l'elasticità degli elementi e la quantità, chiamata *tasso di decadimento*, definita nel seguente modo: sia $x \in D$ non nullo e non invertibile, per il Teorema (1.32) x ammette rappresentazione per decadimento atomico $x^m = x_1 \cdots x_k$ con $m \in \mathbb{N}$ minimale e $x_i \in D$ assolutamente irriducibili $\forall\, i \in \{1, ..., k\}$, il tasso di decadimento di x è

$$\vartheta(x) = \frac{k}{m}.$$

Data una qualunque decomposizione $x^n = y_1 \cdots y_l$ con $y_j \in D$ assolutamente irriducibili $\forall\, j \in \{1, ..., l\}$, si può calcolare il tasso di decadimento come $\vartheta(x) = \frac{l}{n}$, infatti, dal momento che $x^{mn} = (x_1 \cdots x_k)^n = (y_1 \cdots y_l)^m$, per l'unicità della decomposizione (Teorema (1.32)) si ha che $kn = ml$. Il tasso di decadimento gode di un'importante proprietà:

$$\vartheta(xy) = \vartheta(x) + \vartheta(y) \tag{1.3}$$

$\forall\, x, y \in D$ non nulli e non invertibili.

Dimostrazione. Siano $x^m = x_1 \cdots x_k$ e $y^n = y_1 \cdots y_l$ le rappresentazioni per decadimento atomico di x e y. Allora, essendo

$$(xy)^{mn} = (x^m)^n (y^n)^m = (x_1 \cdots x_k)^n (y_1 \cdots y_l)^m$$

una decomposizione in assolutamente irriducibili di x^{mn}, si ha che

$$\vartheta(x\,y) = \frac{nk + ml}{mn} = \frac{k}{m} + \frac{l}{n} = \vartheta(x) + \vartheta(y).$$

□

Corollario 1.34. *Sia D l'anello degli interi di un campo di numeri.*

(i) D è semifattoriale $\iff \vartheta(x) = 1$ per ogni $x \in D$ irriducibile;

(ii) $\rho(D)$ è finita $\iff$ è finita anche la quantità

$$\sup\left\{\vartheta(x), \vartheta(x)^{-1} \middle|\, x \in D \ \textit{irriducibile}\right\}.$$

Dimostrazione.

(i) ($\Rightarrow$) Sia $x \in D$ irriducibile e $x^m = x_1 \cdots x_k$ la sua rappresentazione per decadimento atomico. Essendo $\rho(x^m) = 1$ e $x_1 \cdots x_k = x \cdots x$ (m volte) due fattorizzazioni in irriducibili di x^m, allora si deve avere $k = m$, ossia $\vartheta(x) = 1$.
($\Leftarrow$) Sia $x \in D$ non nullo e non invertibile e siano $x = x_1 \cdots x_k = y_1 \cdots y_l$

due fattorizzazioni in irriducibili di x. Per la proprietà (1.3) ed essendo $\vartheta(x_i) = 1 = \vartheta(y_j)\ \forall\, i, j$, si ottiene

$$k = \sum_{i=1}^{k} \vartheta(x_i) = \vartheta(x_1 \cdots x_k) = \vartheta(y_1 \cdots y_l) = \sum_{j=1}^{l} \vartheta(y_j) = l,$$

dunque $\rho(x) = 1$.

(ii) ($\Rightarrow$) Sia $x \in D$ irriducibile con rappresentazione per decadimento atomico $x^m = x_1 \cdots x_k$. Essendo $x^m = x_1 \cdots x_k = x \cdots x$ (m volte) due fattorizzazioni in irriducibili di x^m, si ha che $\vartheta(x) = \frac{k}{m}, \vartheta(x)^{-1} = \frac{m}{k} \leq \rho(x^m) \leq \rho(D)$, dunque $\sup\{\vartheta(x), \vartheta(x)^{-1} |\, x \in D \text{ irriducibile}\} \leq \rho(D) \lneqq +\infty$.
($\Leftarrow$) Sia $x \in D$ non nullo e non invertibile e siano $x = x_1 \cdots x_k = y_1 \cdots y_l$ due fattorizzazioni in irriducibili di x. Posto $\vartheta(a) = \min\{\vartheta(x_i)|, i \in \{1, ..., k\}\}$ e $\vartheta(b) = \max\{\vartheta(y_j)|\, j \in \{1, ..., l\}\}$ e utilizzando la proprietà (1.3), si ha che

$$k\vartheta(a) \leq \sum_{i=1}^{k} \vartheta(x_i) = \vartheta(x_1 \cdots x_k) = \vartheta(y_1 \cdots y_l) = \sum_{j=1}^{l} \vartheta(y_j) \leq l\vartheta(b),$$

cioè $\frac{k}{l} \leq \vartheta(b)\vartheta(a)^{-1}$. Essendo $\sup\{\vartheta(x), \vartheta(x)^{-1} |\, x \in D \text{ irriducibile}\}$ finito, si conclude che anche $\rho(D)$ è una quantità finita.

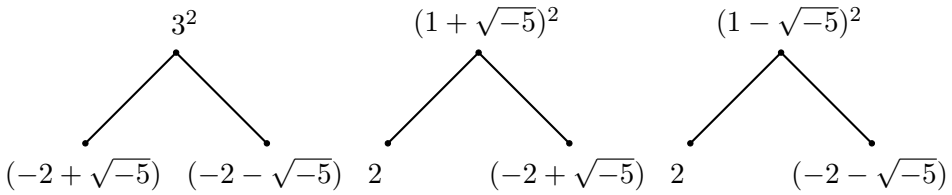
□

1.2.3 Semifattorialità di $\mathbb{Z}[\sqrt{-5}]$

Nell'esempio (1.4) si è visto che $\mathbb{Z}[\sqrt{-5}]$ non è UFD, in particolare $2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$ sono due fattorizzazioni di 6 essenzialmente diverse. Da notare che gli elementi 2, 3 e $1 \pm \sqrt{-5}$ sono irriducibili, come è stato mostrato nell'esempio (1.4), ma non primi: se per assurdo lo fossero, allora sarebbero tutti assolutamente irriducibili (Osservazione (1.21)), dunque per il Teorema (1.32) le due fattorizzazioni dovrebbero essere essenzialmente uguali. Inoltre, si può mostrare che 2 è assolutamente irriducibile (è un esempio di elemento assolutamente irriducibile che non è primo e questo prova che in domini generici, non UFD, non vale il viceversa dell'Osservazione (1.21)), mentre 3 e $1 \pm \sqrt{-5}$ non sono assolutamente irriducibili, infatti

$$\begin{aligned} 3^2 &= (-2 + \sqrt{-5})(-2 - \sqrt{-5}), \\ (1 + \sqrt{-5})^2 &= 2(-2 + \sqrt{-5}) \text{ e} \\ (1 - \sqrt{-5})^2 &= 2(-2 - \sqrt{-5}) \end{aligned}$$

con $-2 \pm \sqrt{-5}$ assolutamente irriducibili.



L'assoluta irriducibilità di 2 e $-2 \pm \sqrt{-5}$ deriva dal fatto che ogni ideale non nullo di $\mathbb{Z}[\sqrt{-5}]$ si scrive in modo unico come prodotto di ideali primi (Osservazione (1.31)). Chiamati $P = (2, 1+\sqrt{-5})$, $Q = (3, 1+\sqrt{-5})$ e $Q' = (3, 1-\sqrt{-5})$, questi risultano essere degli ideali primi di $\mathbb{Z}[\sqrt{-5}]$. Infatti, si ha che, ad esempio, $|\mathbb{Z}[\sqrt{-5}]/(2)| = 4$, dunque, essendo $(2) \subsetneq P = (2, 1+\sqrt{-5}) \subsetneq \mathbb{Z}[\sqrt{-5}]$, $|\mathbb{Z}[\sqrt{-5}]/P| = 2$, da cui segue che P è massimale e perciò primo (Osservazione (1.31)). Allo stesso modo, si può mostrare che anche Q e Q' sono ideali primi di $\mathbb{Z}[\sqrt{-5}]$. Inoltre, si vede che

$$(2) = P^2, \ \ (3) = Q \cdot Q', \ \ (1+\sqrt{-5}) = P \cdot Q \ \ \text{e} \ \ (1-\sqrt{-5}) = P \cdot Q'$$

e, essendo

$$(1+\sqrt{-5})^2 = P^2 \cdot Q^2 \ \text{ e } \ (1-\sqrt{-5})^2 = P^2 \cdot Q'^2$$

(tutte queste uguaglianze possono essere facilmente mostrate notando che i generatori di un prodotto di ideali sono i prodotti dei generatori), allora

$$(-2+\sqrt{-5}) = Q^2 \ \text{ e } \ (-2-\sqrt{-5}) = Q'^2.$$

Da queste osservazioni si deduce che gli elementi 2 e $-2 \pm \sqrt{-5}$ sono assolutamente irriducibili per l'Osservazione (1.31) (l'ideale da loro generato è potenza di un ideale primo). A seguito di queste considerazioni, si ha che

$$6^2 = 2^2 \cdot 3^2 = (1+\sqrt{-5})^2(1-\sqrt{-5})^2 = 2 \cdot 2 \cdot (-2+\sqrt{-5})(-2-\sqrt{-5})$$

è la rappresentazione per decadimento atomico di 6.

Un altro risultato che si può mostrare è che $\mathbb{Z}[\sqrt{-5}]$ è un dominio semifattoriale nonostante non sia un UFD (dunque è un esempio del fatto che non vale il viceversa dell'Osservazione (1.11)), equivalentemente, per il Corollario (1.34), tutti gli elementi irriducibili di questo anello hanno tasso di decadimento 1. Per mostrare questo fatto, per prima cosa bisogna ricordare una definizione: se, in generale, D è l'anello degli interi di un campo di numeri, si può definire una relazione di equivalenza sull'insieme di tutti gli ideali di D ponendo, dati I e J due ideali, $I \sim J$ se $\exists\, \alpha, \beta \in D$ tali che $\alpha I = \beta J$. L'insieme di tutte le classi di equivalenza, che risulta essere un gruppo abeliano finito, viene detto *gruppo delle classi di* D. Un importante Teorema la cui dimostrazione si può trovare in [5, Theorem 6.10] è il seguente:

Teorema 1.35. *Il gruppo delle classi di* $\mathbb{Z}[\sqrt{-5}]$ *è* $\mathbb{Z}/2\mathbb{Z}$.

Il gruppo delle classi di $\mathbb{Z}[\sqrt{-5}]$ è dunque costituito dalla classe degli ideali principali e dalla classe degli ideali non principali.

Corollario 1.36. *Se* I, J *sono ideali non nulli e non principali di* $\mathbb{Z}[\sqrt{-5}]$, *allora* IJ *è principale.*

Necessaria per la dimostrazione del fatto che $\mathbb{Z}[\sqrt{-5}]$ è semifattoriale è una caratterizzazione degli elementi irriducibili di questo anello:

Proposizione 1.37. *Sia* $x \in \mathbb{Z}[\sqrt{-5}]$ *un elemento non nullo e non invertibile, allora* x *è irriducibile* $\iff (x) = P$ *con* P *ideale primo di* $\mathbb{Z}[\sqrt{-5}]$ *oppure* $(x) = P_1P_2$ *con* P_1 *e* P_2 *ideali primi non principali di* $\mathbb{Z}[\sqrt{-5}]$.

Dimostrazione. ($\Rightarrow$) Per l'Osservazione (1.31), (x) si scrive in modo unico come prodotto di ideali primi. Se (x) è un ideale primo, allora la tesi è provata. Altrimenti, $(x) = P_1 \cdots P_k$ con P_i ideali primi di $\mathbb{Z}[\sqrt{-5}]$ $\forall\, i \in \{1, ..., k\}$ e $k \geq 2$. Nessuno di questi ideali può essere principale: si supponga per assurdo che $\exists\, i \in \{1, ..., k\}$ tale che P_i sia principale, sia questo, ad esempio, P_1, $P_1 = (x_1)$ con x_1 primo in $\mathbb{Z}[\sqrt{-5}]$. Per il Teorema (1.35), $P_2 \cdots P_k = (x_2)$ con x_2 non nullo e non invertibile, dunque $(x) = (x_1)(x_2) = (x_1x_2)$, cioè x e x_1x_2 sono associati, quindi $\exists\, u \in \mathbb{Z}[\sqrt{-5}]$ invertibile tale che $x = (ux_1)x_2$, contro l'irriducibilità di x (ux_1 e x_2 non sono invertibili). Bisogna ora mostrare che $k = 2$. Sicuramente k è pari per il Teorema (1.35), si supponga per assurdo che $k > 2$. Per il Teorema (1.35) e il Corollario (1.36), si ha che $P_1P_2 = (y_1)$ e $P_3 \cdots P_k = (y_2)$ con y_1 e y_2 non nulli e non invertibili in $\mathbb{Z}[\sqrt{-5}]$. Come in precedenza, $x = (uy_1)y_2$ con $u \in \mathbb{Z}[\sqrt{-5}]$ invertibile, contro l'irriducibilità di x.
($\Leftarrow$) Se $(x) = P$ con P ideale primo di $\mathbb{Z}[\sqrt{-5}]$, allora x è primo e dunque irriducibile (Osservazione (1.21)). Se, invece, $(x) = P_1P_2$ con P_1 e P_2 ideali primi non principali e $x = yz$ con y non nullo e non invertibile, per mostrare che x è irriducibile bisogna provare che z è invertibile. Dal momento che $P_1P_2 = (x) = (yz) = (y)(z)$, per l'unicità della decomposizione come podotto di ideali primi (Osservazione (1.31)), si ha che $(y) = P_1P_2$ ($(y) \neq P_1, P_2$ poiché questi sono supposti essere non principali). Per questo motivo, $(z) = (1)$, ossia z è invertibile. □

Teorema 1.38. *Sia* $x \in \mathbb{Z}[\sqrt{-5}]$ *non nullo e non invertibile, allora ogni fattorizzazione in irriducibili in* $\mathbb{Z}[\sqrt{-5}]$ *ha la stessa lunghezza.*

Dimostrazione. Sia $x \in \mathbb{Z}[\sqrt{-5}]$ non nullo e non invertibile, per l'Osservazione (1.31), $(x) = P_1 \cdots P_k$ con P_i ideali primi $\forall\, i \in \{1, ..., k\}$. Si supponga che d di questi ideali siano principali, siano questi i primi d, ossia $P_i = (y_i)$ con $i \in \{1, ..., d\}$ e $y_i \in \mathbb{Z}[\sqrt{-5}]$ primi, perciò irriducibili. Sicuramente, per il Teorema (1.35), si ha che $k - d$ deve essere pari, dunque i restanti

$k - d = 2n$ ideali risultano essere non principali. Le varie fattorizzazioni in irriducibili di x essenzialmente diverse derivano dai diversi modi di formare n coppie tra questi ideali non principali, infatti, per la Proposizione (1.37), si ha che il prodotto di due di questi ideali è un ideale principale generato da un elemento irriducibile. Dunque, una volta scelte le coppie, si ottiene

$$(x) = (y_1) \cdots (y_d)(z_1) \cdots (z_n) = (y_1 \cdots y_d z_1 \cdots z_n)$$

e ogni fattorizzazione in irriducibili di x è essenzialmente uguale a $x = y_1 \cdots y_d z_1 \cdots z_n$. Perciò, indipendentemente da come vengono scelte le coppie tra gli ideali $P_{d+1}, ..., P_k$, tutte le fattorizzazioni di x sono di lunghezza $d + n$. □

Corollario 1.39. *L'anello* $\mathbb{Z}[\sqrt{-5}]$ *è un dominio semifattoriale.*

Capitolo 2

L'anello dei polinomi a valori interi

Questo capitolo è dedicato all'anello Int($\mathbb{Z}$): verranno presentate alcune proprietà significative di questo anello per poi andare a costruire particolari elementi che mostrano il fatto che Int($\mathbb{Z}$) non è UFD.

2.1 Proprietà di Int($\mathbb{Z}$)

Un importante ruolo in Int($\mathbb{Z}$) viene svolto dai *polinomi binomiali*, ossia

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!},$$

con n intero non negativo.

Lemma 2.1. *I polinomi binomiali appartengono all'anello dei polinomi a valori interi.*

Dimostrazione. Sia $n \geq 0$; bisogna mostrare che $\binom{z}{n} \in \mathbb{Z}\ \forall\, z \in \mathbb{Z}$. Dalla definizione del coefficiente binomiale, si ha che se $0 \leq z < n$, allora $\binom{z}{n} = 0$, mentre se $z \geq n$, allora $\binom{z}{n} \in \mathbb{N}$. Se, invece, $z < 0$, si mostra per induzione su n che $\binom{z}{n} = (-1)^n\binom{-z+n-1}{n} \in \mathbb{Z}$. Infatti, se $n = 1$, $\binom{z}{1} = z = (-1)^1\binom{-z}{1}$; si supponga ora che sia vero per n, dunque si ha

$$\binom{z}{n+1} = \binom{z}{n}\frac{z-n}{n+1} = (-1)^n\binom{-z+n-1}{n}\frac{z-n}{n+1} = (-1)^{n+1}\binom{-z+n}{n+1}$$

□

Lemma 2.2. *I polinomi binomiali non solo sono una base di* $\mathbb{Q}[x]$ *su* $\mathbb{Q}$*, ma sono anche una base di* Int($\mathbb{Z}$) *su* $\mathbb{Z}$*.*

Dimostrazione. I polinomi binomiali formano una base di $\mathbb{Q}[x]$ su $\mathbb{Q}$ dal momento che esiste un polinomio di questo tipo per ogni grado. Per quanto riguarda la seconda affermazione, invece, per il Lemma (2.1), $\binom{x}{k} \in \mathrm{Int}(\mathbb{Z})$ $\forall\, k \geq 0$, in particolare ogni loro combinazione lineare a coefficienti in $\mathbb{Z}$ è un polinomio a valori interi. Sia ora $f \in \mathrm{Int}(\mathbb{Z}) \subseteq \mathbb{Q}[x]$ di grado n, allora per

$$f(x) = \sum_{k=0}^{n} a_k \binom{x}{k},$$

con $a_k \in \mathbb{Q}\ \forall\, k \in \{0, ..., n\}$. Si dimostra per induzione su $k < n$ che $a_k \in \mathbb{Z}$: se $k = 0$, $a_0 = f(0) \in \mathbb{Z}$; si supponga ora che sia vero per k, allora $g_k(x) = f(x) - \sum_{i=0}^{k} a_i \binom{x}{i} \in \mathrm{Int}(\mathbb{Z})$, dunque in particolare $g_k(k+1) = a_{k+1} \in \mathbb{Z}$. □

Grazie a questa importante proprietà dei polinomi binomiali, è possibile presentare un facile criterio per verificare se un polinomio a coefficienti razionali sia o meno un polinomio a valori interi:

Corollario 2.3. *Sia $f \in \mathbb{Q}[x]$ di grado n.*

(i) $f \in \mathrm{Int}(\mathbb{Z}) \iff f(i) \in \mathbb{Z}\ \forall\, i \in \{0, ..., n\}$;

(ii) $f \in \mathrm{Int}(\mathbb{Z}) \iff f$ *è a valori interi su* $n+1$ *interi consecutivi.*

Dimostrazione.

(i) ($\Rightarrow$) Per definizione di $\mathrm{Int}(\mathbb{Z})$.
($\Leftarrow$) Dato che $f \in \mathbb{Q}[x]$, $\exists\, a_k \in \mathbb{Q}$ con $k \in \{0, ..., n\}$ tali che $f(x) = \sum_{k=0}^{n} a_k \binom{x}{k}$ (Lemma (2.2)). Per mostrare che $f \in \mathrm{Int}(\mathbb{Z})$, basta mostrare per induzione su $k < n$ che $a_k \in \mathbb{Z}\ \forall\, k \in \{0, ..., n\}$ (Lemma (2.2)). Per $k = 0$ si ha $a_0 = f(0) \in \mathbb{Z}$; si supponga sia vero per k, allora

$$f(k+1) = a_0 + a_1 \binom{k+1}{1} + ... + a_{k+1}$$

$$a_{k+1} = f(k+1) - a_0 - a_1 \binom{k+1}{1} - ... - a_k \binom{k+1}{k} \in \mathbb{Z}$$

(ii) ($\Rightarrow$) Per definizione di $\mathrm{Int}(\mathbb{Z})$.
($\Leftarrow$) Si supponga che $f(z+i) \in \mathbb{Z}\ \forall\, i \in \{0, ..., n\}$, $\exists\, z \in \mathbb{Z}$, allora per il punto (i) $f(x+z) = \sum_{k=0}^{n} a_k \binom{x}{k} \in \mathrm{Int}(\mathbb{Z})$ (cioè $a_k \in \mathbb{Z}\ \forall\, k \in \{0, ..., n\}$), dunque $f(x) = \sum_{k=0}^{n} a_k \binom{x-z}{k} \in \mathrm{Int}(\mathbb{Z})$.

□

Corollario 2.4. *Sia $f \in \mathrm{Int}(\mathbb{Z})$ di grado al massimo n, allora $n!f \in \mathbb{Z}[x]$.*

Dimostrazione. Sia $f(x) = \sum_{k=0}^{m} a_k \binom{x}{k}$ con $m \leq n$ e $a_k \in \mathbb{Z}\ \forall\, k \in \{0, ..., m\}$ (Lemma (2.2)); dato che $k! \mid n!\ \forall\, k \in \{0, ..., m\}$, allora $n!f \in \mathbb{Z}[x]$. □

I coefficienti interi tramite cui ogni polinomio a valori interi si scrive come combinazione lineare dei polinomi binomiali possono essere espressi tramite le seguenti quantità che verranno ora definite.

Definizione 2.5. Sia R un anello commutativo, data $f : \mathbb{Z} \longrightarrow R$ una mappa, per $n \geq 0$ si possono definire ricorsivamente le seguenti quantità:

$$\triangle^0 f(x) = f(x)$$
$$\triangle^n f(x) = \triangle^{n-1} f(x+1) - \triangle^{n-1} f(x)$$

Lemma 2.6. *Sia f come sopra, allora*

$$\triangle^n f(x) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} f(x+i) \tag{2.1}$$

Dimostrazione. La dimostrazione procede per induzione su n: se $n = 0$, si ottiene $\triangle^0 f(x) = f(x)$; si supponga sia vero per n, allora

$$\begin{aligned}
&\triangle^{n+1} f(x) = \triangle^n f(x+1) - \triangle^n f(x) = \\
&= \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} f(x+1+i) - \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} f(x+i) = \\
&= \sum_{k=1}^{n+1} (-1)^{n-k+1} \binom{n}{k-1} f(x+k) - \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(x+k) = \\
&= f(x+n+1) + \sum_{k=1}^{n} (-1)^{n-k} f(x+k) \left(-\binom{n}{k-1} - \binom{n}{k} \right) + (-1)^{n+1} f(x) = \\
&= f(x+n+1) + \sum_{k=1}^{n} (-1)^{n+1-k} f(x+k) \binom{n+1}{k} + (-1)^{n+1} f(x) = \\
&= \sum_{k=0}^{n+1} (-1)^{n+1-k} \binom{n+1}{k} f(x+k)
\end{aligned}$$

□

Lemma 2.7. *Sia $f \in \mathrm{Int}(\mathbb{Z})$ di grado n,*

$$f(x) = \sum_{k=0}^{n} a_k \binom{x}{k},$$

con $a_k \in \mathbb{Z}$ $\forall\, k \in \{0, ..., n\}$. Allora $a_k = \triangle^k f(0)$ $\forall\, k \in \{0, ..., n\}$.

Dimostrazione. Utilizzando l'espressione

$$f(i) = \sum_{k=0}^{n} a_k \binom{i}{k}$$

e la formula (2.1) si ottiene

$$\begin{aligned}
\triangle^k f(0) &= \sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}\sum_{j=0}^{n}a_j\binom{i}{j} = \\
&= \sum_{j=0}^{n}a_j\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}\binom{i}{j} = \\
&= \sum_{j=0}^{n}a_j\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{j}\binom{k-j}{i-j} = \\
&= \sum_{j=0}^{n}a_j\binom{k}{j}\sum_{r=0}^{k}(-1)^{r}\binom{k-j}{r} = \\
&= \sum_{j=0}^{n}a_j\binom{k}{j}\left(\sum_{r=0}^{k-j}(-1)^{r}\binom{k-j}{r} + \sum_{r=k-j+1}^{k}(-1)^{r}\binom{k-j}{r}\right) = \\
&= \sum_{j=0}^{n}a_j\binom{k}{j}(1-1)^{k-j} = a_k
\end{aligned}$$

Nelle uguaglianze precedenti è stata sfruttata l'identità $\binom{k}{i}\binom{i}{j} = \binom{k}{j}\binom{k-j}{i-j}$ e il fatto che $\binom{k-j}{r} = 0$ per $r > k-j$. □

Il risultato seguente mostra come calcolare in modo più semplice il divisore fisso di un polinomio a valori interi:

Lemma 2.8. *Sia $f \in \mathrm{Int}(\mathbb{Z})$ di grado n e si definiscano*

(i) $d_1 = \sup\left\{n \in \mathbb{N} |\ \frac{1}{n}f(x) \in \mathrm{Int}(\mathbb{Z})\right\}$;

(ii) $d_2 = \gcd\left(f(z) |\ z \in \mathbb{Z}\right)$;

(iii) $d_3 = \gcd\left(f(z) |\ 0 \le z \le n\right)$.

Allora $d_1 = d_2 = d_3$.

Dimostrazione. Dalla definizione di d_1, si ha che $\frac{1}{d_1}f(z) \in \mathbb{Z}\ \forall\, z \in \mathbb{Z}$, dunque $d_1 \mid f(z)\ \forall\, z \in \mathbb{Z}$ e per questo $d_1 \mid d_2$, in particolare $d_1 \le d_2$. Viceversa, siccome $d_2 \mid f(z)\ \forall\, z \in \mathbb{Z}$, ossia $\frac{1}{d_2}f(x) \in \mathrm{Int}(\mathbb{Z})$, $d_2 \le d_1$. Segue, quindi, l'uguaglianza. Per il Lemma (2.2), $f(x) = \sum_{k=0}^{n} a_k\binom{x}{k}$, esistono $a_k \in \mathbb{Z}$ $\forall\, k \in \{0, ..., n\}$; in particolare $a_k = \triangle^k f(0)\ \forall\, k \in \{0, ..., n\}$ (Lemma (2.7)), cioè

$$a_k = \sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}f(i),$$

dove si è utilizzata l'espressione (2.1). Dato che $d_3 \mid f(i)\ \forall\, i \in \{0,...,k\}$, allora $d_3 \mid a_k\ \forall\, k \in \{0,...,n\}$ e perciò $d_3 \mid f(z)\ \forall z \in \mathbb{Z}$. Dunque, essendo $\frac{1}{d_3} f(x) = \sum_{k=0}^{n} \frac{a_k}{d_3} \binom{x}{k} \in \mathrm{Int}(\mathbb{Z})$, si ha $d_3 \leq d_1 \leq d_2$, da cui segue l'uguaglianza. □

A questo punto verranno descritte delle condizioni che permettono di affermare che un polinomio $f \in \mathbb{Q}[x]$ è a valori interi, in particolare, verranno caratterizzati gli elementi irriducibili di questo anello, dando anche alcuni esempi numerici.

Lemma 2.9. *Sia $f \in \mathbb{Q}[x]$ non nullo, allora $\exists!\, a, b \in \mathbb{N}$ con $\gcd(a,b) = 1$ e $g \in \mathbb{Z}[x]$ primitivo tali che*

$$f(x) = \frac{ag(x)}{b}. \tag{2.2}$$

Per f nella forma (2.2), valgono le seguenti affermazioni:

(i) $f \in \mathrm{Int}(\mathbb{Z}) \iff b \mid \mathsf{d}(g)$;

(ii) Se f è irriducibile e non costante in $\mathrm{Int}(\mathbb{Z})$, allora $a = 1$ e $b = \mathsf{d}(g)$.

Dimostrazione. Dato che $f \in \mathbb{Q}[x]$, allora

$$f(x) = \sum_{k=0}^{n} \frac{a_k}{b_k} x^k,$$

con $a_k, b_k \in \mathbb{Z}$, $\gcd(a_k, b_k) = 1$ e $b_k \neq 0\ \forall\, k \in \{0,...,n\}$. Basta porre $b = \gcd(b_k |\, k \in \{0,...,n\})$, $h(x) = \sum_{k=0}^{n} \frac{b}{b_k} a_k x^k \in \mathbb{Z}[x]$ e $a = \mathsf{c}(h)$ per ottenere

$$f(x) = \frac{h(x)}{b} = \frac{\mathsf{c}(h) g(x)}{b} = \frac{ag(x)}{b}$$

Ora bisogna mostrare le due affermazioni:

(i) Si ha che $f \in \mathrm{Int}(\mathbb{Z}) \iff f(z) = \frac{ag(z)}{b} \in \mathbb{Z}\ \forall\, z \in \mathbb{Z} \iff b \mid g(z)\ \forall\, z \in \mathbb{Z}$ (poiché $\gcd(a,b) = 1$) $\iff b \mid \mathsf{d}(g)$;

(ii) Essendo $f \in \mathrm{Int}(\mathbb{Z})$, $b \mid \mathsf{d}(g)$ per il punto (i), dunque $\exists\, c \in \mathbb{N}$ tale che $\mathsf{d}(g) = bc$. Dato che f è irriducibile in $\mathrm{Int}(\mathbb{Z})$, dalla scrittura $f(x) = ac \frac{g(x)}{\mathsf{d}(g)}$ si deduce che uno tra ac e $\frac{g(x)}{\mathsf{d}(g)}$ deve essere invertibile in $\mathrm{Int}(\mathbb{Z})$; sicuramente $\frac{g(x)}{\mathsf{d}(g)}$ non lo può essere perché g è non costante, dunque $ac = 1$, da cui si deduce che $a = 1 = c$.

□

Esempio 2.10. Si considerino i polinomi

$$f(x) = \frac{9}{2}x^3 + \frac{3}{4}x^2 + 6 = \frac{18x^3 + 3x^2 + 24}{4} = \frac{3(6x^3 + x^2 + 8)}{4} \text{ e}$$
$$g(x) = \frac{9}{4}x^4 + \frac{3}{4}x^2 + 3 = \frac{3(3x^4 + x^2 + 4)}{4}$$

espressi nella forma (2.2), con $a = 3$ e $b = 4$ ($\gcd(a, b) = 1$). Nel primo caso si ha che $f'(x) = 6x^3 + x^2 + 8$ è primitivo con $\mathsf{d}(f') = 1$, quindi, dato che $4 \nmid \mathsf{d}(f') = 1$, allora $f \notin \mathrm{Int}(\mathbb{Z})$. Al contrario, chiamato $g'(x) = 3x^4 + x^2 + 4$, si vede che $\mathsf{d}(g') = 4$, percò $g \in \mathrm{Int}(\mathbb{Z})$ dal momento che $4 \mid \mathsf{d}(g') = 4$ (Lemma (2.9)(i)).

Lemma 2.11. *Sia $f \in \mathbb{Q}[x]$ non nullo, allora f si può scrivere in modo unico (a meno del segno di a e del segno e dell'indicizzazione dei g_i) come*

$$f(x) = \frac{a}{b} \prod_{i \in I} g_i(x), \tag{2.3}$$

dove $a \in \mathbb{Z}$, $b \in \mathbb{N}$ con $\gcd(a, b) = 1$, I è un insieme finito e $g_i \in \mathbb{Z}[x]$ primitivo e irriducibile $\forall\, i \in I$.
Inoltre, se $f \in \mathrm{Int}(\mathbb{Z})$ è non costante ed è espresso nella forma (2.3), f è irriducibile in $\mathrm{Int}(\mathbb{Z}) \iff a = \pm 1$, $b = \mathsf{d}\left(\prod_{i \in I} g_i(x)\right)$ e

$$\begin{gathered} \nexists\, \emptyset \neq J \subsetneq I, b_1, b_2 \in \mathbb{N} \text{ t.c.} \\ b = b_1 b_2, b_1 = \mathsf{d}\left(\prod_{j \in J} g_j(x)\right) \text{ e } b_2 = \mathsf{d}\left(\prod_{i \in I \setminus J} g_i(x)\right). \end{gathered} \tag{2.4}$$

Dimostrazione. La prima affermazione discende dal fatto che i polinomi in $\mathbb{Z}[x]$ si possono sempre scrivere in modo unico come prodotto di irriducibili ($\mathbb{Z}[x]$ è un UFD) e la dimostrazione procede come nel caso della scrittura (2.2).
Per quanto riguarda, invece, la seconda affermazione si ha:
($\Rightarrow$) Se f è irriducibile in $\mathrm{Int}(\mathbb{Z})$, $a = \pm 1$ e $b = \mathsf{d}\left(\prod_{i \in I} g_i(x)\right)$ (Lemma (2.9)(ii)). Si supponga ora per assurdo che $\exists\, \emptyset \neq J \subsetneq I$ e $b_1, b_2 \in \mathbb{N}$ tali che $b = b_1 b_2$, $b_1 = \mathsf{d}\left(\prod_{j \in J} g_j(x)\right)$ e $b_2 = \mathsf{d}\left(\prod_{i \in I \setminus J} g_i(x)\right)$, allora

$$f(x) = \frac{\prod_{j \in J} g_j(x)}{b_1} \cdot \frac{\prod_{i \in I \setminus J} g_i(x)}{b_2} \in \mathrm{Int}(\mathbb{Z}) \tag{2.5}$$

e, essendo f irriducibile, uno dei due fattori dovrebbe essere invertibile; la contraddizione viene dal fatto che nessuno dei due è costante, poiché $\emptyset \neq J \subsetneq I$.
($\Leftarrow$) Dato che $b = \mathsf{d}\left(\prod_{i \in I} g_i(x)\right)$, in nessuna fattorizzazione di f possono comparire costanti non invertibili, ma ogni fattore irriducibile deve essere

del tipo $\frac{\prod_{j\in J} g_j(x)}{b_1}$ con $\emptyset \neq J \subsetneq I$ e $b_1 = \mathsf{d}\left(\prod_{j\in J} g_j(x)\right)$. Dunque f si scriverebbe come in (2.5), con il primo fattore irriducibile e il secondo in $\mathrm{Int}(\mathbb{Z})$, ossia $b_2 \mid \mathsf{d}\left(\prod_{i\in I\setminus J} g_i(x)\right)$ (Lemma (2.9)(i)); b_2, però, non può essere un divisore proprio perché altrimenti $b = b_1 b_2$ sarebbe divisore proprio di $\mathsf{d}\left(\prod_{i\in I} g_i(x)\right)$, contro le ipotesi iniziali. Da questa contraddizione, segue che f deve essere irriducibile. □

Esempio 2.12. Si considerino i polinomi

$$f(x) = -\frac{2}{5}x^2 + 2x - \frac{12}{5} = \frac{-2x^2+10x-12}{5} = \frac{-2(x-3)(x-2)}{5} \text{ e}$$
$$g(x) = -\frac{1}{2}x^2 + \frac{5}{2}x - 3 = \frac{-1(x-3)(x-2)}{2}$$

espressi nella forma (2.3); in entrambi i casi si ha $g_1(x) = x-3$ e $g_2(x) = x-2$ e questi risultano essere primitivi e irriducibili in $\mathbb{Z}[x]$ con $\mathsf{d}(g_1) = 1 = \mathsf{d}(g_2)$, mentre $\mathsf{d}(g_1 g_2) = 2$. Nel caso di f, dal momento che $5 = b \nmid \mathsf{d}(g_1 g_2) = 2$, allora $f \notin \mathrm{Int}(\mathbb{Z})$ (Lemma (2.9)(i)). Al contrario, g non solo è in $\mathrm{Int}(\mathbb{Z})$, ma è anche irriducibile, infatti $b = 2 = \mathsf{d}(g_1 g_2)$ e non può esistere l'insieme J del Lemma (2.11) poiché $\mathsf{d}(g_1)d(g_2) \neq \mathsf{d}(g_1 g_2)$.

Il seguente Corollario, pur essendo un risultato già visto nel capitolo precedente (Corollario (1.8)), permette di vedere una dimostrazione alternativa di questa importante proprietà dell'anello $\mathrm{Int}(\mathbb{Z})$:

Corollario 2.13. *L'anello* $\mathrm{Int}(\mathbb{Z})$ *è atomico.*

Dimostrazione. Sia $f \in \mathrm{Int}(\mathbb{Z})$ espresso nella forma (2.3) e si indichi con $g(x) = \prod_{i\in I} g_i(x)$. Dato che $b \mid \mathsf{d}(g)$, $\exists\, c \in \mathbb{Z}$ tale che $\mathsf{d}(g) = bc$ in modo che f si possa scrivere come $f(x) = ac\frac{g(x)}{\mathsf{d}(g)}$. Dal momento che $ac \in \mathbb{Z}$, ac si può scrivere come prodotto di irriducibili in $\mathbb{Z}$, che risultano irriducibili anche in $\mathrm{Int}(\mathbb{Z})$. Se poi $\frac{g(x)}{\mathsf{d}(g)}$ è irriducibile in $\mathrm{Int}(\mathbb{Z})$, si ottiene subito la fattorizzazione cercata, altrimenti lo si può scrivere come prodotto di due fattori di grado minore come nell'espressione (2.5) e reiterare il procedimento fino ad ottenere solo elementi irriducibili. □

Un'altra conseguenza interessante dei risultati appena visti è che:

Corollario 2.14. *Ogni elemento non nullo e non invertibile di* $\mathrm{Int}(\mathbb{Z})$ *ammette un numero finito di fattorizzazioni in irriducibili in* $\mathrm{Int}(\mathbb{Z})$.

Dimostrazione. Sia $f \in \mathrm{Int}(\mathbb{Z})$ non nullo e non invertibile espresso nella forma (2.3) e si indichi con $g(x) = \prod_{i\in I} g_i(x)$. Le possibili fattorizzazioni di f, al variare di $c \in \mathbb{N}$ tale che $bc \mid \mathsf{d}(g)$, sono del tipo

$$f(x) = a_1 \cdots a_n c_1 \cdots c_m \prod_{j=1}^{k} \frac{\prod_{i\in I_j} g_i(x)}{d_j},$$

dove $a = a_1 \cdots a_n$ e $c = c_1 \cdots c_m$ sono le fattorizzazioni in irriducibili in $\mathbb{Z}$ di a e c, $I = \sqcup_{j=1}^{k} I_j$, $bc = \prod_{j=1}^{k} d_j$ e $d_j = \mathsf{d}\left(\prod_{i \in I_j} g_i(x)\right)$. □

Osservazione 2.15. Non esistono elementi primi in $\mathrm{Int}(\mathbb{Z})$, infatti, se esistesse un elemento $f \in \mathrm{Int}(\mathbb{Z})$ primo, allora (f) sarebbe un ideale primo principale, ma questo non è possibile perché in $\mathrm{Int}(\mathbb{Z})$ non esistono ideali primi finitamente generati (una dimostrazione di questo fatto si può trovare in [4, Corollary 15]). In particolare, questo fatto mostra che $\mathrm{Int}(\mathbb{Z})$ non è un UFD, infatti, è un dominio atomico, ma gli elementi irriducibili non possono essere primi (Lemma (1.12)).

Molto utile in ciò che segue sarà la mappa, detta *valutazione p-adica*,

$$\begin{aligned} v_p : \mathbb{Q} &\longrightarrow \mathbb{Z} \\ \frac{a}{b}p^n &\longmapsto n \ \text{ con } \ p \nmid ab \\ 0 &\longmapsto \infty \end{aligned} \tag{2.6}$$

dove $p \in \mathbb{Z}$ è un primo; quindi, dato un numero intero z, $v_p(z)$ è l'esponente della massima potenza di p che divide z. Le due proprietà principali di questa mappa, comuni a tutte le mappe di valutazione, sono:

(i) $v_p(ab) = v_p(a) + v_p(b)\ \forall\, a, b \in \mathbb{Z}$;

(ii) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}\ \forall\, a, b \in \mathbb{Z}$.

Questa mappa verrà utilizzata per trovare il divisore fisso di alcuni polinomi andando a determinare per ogni primo p la massima potenza divide il divisore fisso sfruttando i risultati seguenti.

Osservazione 2.16. Sia $f \in \mathbb{Z}[x]$ e p un primo, allora

$$v_p(\mathsf{d}(f)) = \min_{z \in \mathbb{Z}} v_p(f(z)).$$

Lemma 2.17 (*Identità di Legendre*)**.** *Sia $n \geq 1$ un intero,*

$$v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Dimostrazione. Per determinare $v_p(n!)$ basta contare, $\forall\, k \geq 1$, tutti i multipli di p^k minori o uguali di n, che, però, non siano multipli di p^{k+1}, questi risultano essere $\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$. Perciò si ottiene

$$\begin{aligned} v_p(n!) &= \sum_{k \geq 1} k \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) = \\ &= \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor + 2\left\lfloor \frac{n}{p^2} \right\rfloor - 2\left\lfloor \frac{n}{p^3} \right\rfloor + \ldots = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor \end{aligned}$$

□

Lemma 2.18. *Sia $f \in \mathbb{Z}[x]$ primitivo di grado n e p un primo, allora*

$$v_p(\mathsf{d}(f)) \leq \sum_{k\geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor = v_p(n!).$$

In particolare, se $p \mid \mathsf{d}(f)$, allora $p \leq n$.

Dimostrazione. Sia $g = \frac{f}{\mathsf{d}(f)} \in \mathrm{Int}(\mathbb{Z})$, allora

$$\mathsf{d}(f)\mathbb{Z} = \{n \in \mathbb{Z} |\, ng \in \mathbb{Z}[x]\}$$

($\subseteq$) Sia $\mathsf{d}(f)n \in \mathsf{d}(f)\mathbb{Z}$, allora $\mathsf{d}(f)ng = \mathsf{d}(f)n\frac{f}{\mathsf{d}(f)} = nf \in \mathbb{Z}[x]$.
($\supseteq$) Sia $n \in \mathbb{Z}$ tale che $ng \in \mathbb{Z}[x]$, allora $n\frac{f}{\mathsf{d}(f)} \in \mathbb{Z}[x]$, quindi, dato che f è primitivo, $\mathsf{d}(f) \mid n$, ossia $n \in \mathsf{d}(f)\mathbb{Z}$.
Per il Corollario (2.4), $n! \in \{n \in \mathbb{Z} |\, ng \in \mathbb{Z}[x]\} = \mathsf{d}(f)\mathbb{Z}$, perciò $\mathsf{d}(f) \mid n!$.
Da questo segue che $v_p(\mathsf{d}(f)) \leq v_p(n!)$. □

Osservazione 2.19. Per dimostrare che se $f \in \mathbb{Z}[x]$ è primitivo e $p \mid \mathsf{d}(f)$ allora $p \leq deg(f)$ si può anche ragionare in questo modo: dato che $p \mid \mathsf{d}(f)$, $f(z) \equiv 0 \pmod p$, dunque f ha p radici distinte in $\mathbb{Z}/p\mathbb{Z}$ e perciò $p \leq deg(f)$.

2.2 Costruzione di polinomi con fattorizzazioni di determinate lunghezze

Scopo di questa sezione è presentare un risultato importante che caratterizza $\mathrm{Int}(\mathbb{Z})$, ossia che dato un qualunque sottoinsieme finito non vuoto di cardinalità n di $\mathbb{N} \setminus \{1\}$, eventualmente contenente degli elementi ripetuti, si può sempre costruire un polinomio in $\mathrm{Int}(\mathbb{Z})$ che abbia n fattorizzazioni in $\mathrm{Int}(\mathbb{Z})$ di lunghezza uguale agli elementi del sottoinsieme di $\mathbb{N}$ considerato.

Per prima cosa bisogna ricordare un importante Teorema su cui si baseranno molte delle dimostrazioni seguenti, ossia il *Teorema Cinese del Resto*.

Teorema 2.20 (*Teorema Cinese del Resto*)**.** *Dati $t > 1$ numeri naturali $n_1, ..., n_t \geq 1$ con $\gcd(n_i, n_j) = 1\ \forall\, i \neq j$ e $a_1, ..., a_t \in \mathbb{Z}$, esiste $x \in \mathbb{Z}$ soluzione del sistema di congruenze $x \equiv a_i \pmod{n_i}$ $\forall\, i \in \{1, ..., t\}$ e tutte queste soluzioni sono congrue modulo $n = n_1 \cdots n_t$.*

Un altro aspetto che è necessario ricordare riguarda i sistemi completi di residui modulo un numero naturale. Dato un numero naturale $n \geq 1$, un *sistema completo di residui modulo n* è un sottoinsieme di $\mathbb{Z}$ di n elementi $\{a_1, ..., a_n\}$ con la proprietà che $\forall\, z \in \mathbb{Z}\ \exists!\, i \in \{1, ..., n\}$ tale che $z \equiv a_i \pmod n$.

Lemma 2.21. *Per ogni primo p esiste un sistema completo di residui modulo p che non contiene un sistema completo di residui modulo qualsiasi altro primo.*

Dimostrazione. Sia $q \neq p$ un altro primo. Se $q > p$ un sistema completo di residui modulo p non può mai contenere un sistema completo di residui modulo q. Se, invece, $q < p$, basta determinare a_i con $i \in \{1, ..., p\}$ risolvendo il sistema di congruenze

$$\begin{cases} a_i \equiv i \pmod{p} \\ a_i \equiv 1 \pmod{q} \end{cases}$$

Dal momento che $\gcd(p, q) = 1$, il Teorema Cinese del Resto garantisce l'esistenza di questi a_i che formano il sistema completo di residui modulo p cercato. □

A questo punto è possibile enunciare il risultato più importante di questa sezione:

Lemma 2.22. *Sia I un insieme finito e siano $f_i \in \mathbb{Z}[x]$ con $i \in I$ polinomi monici di grado $n_i \geq 1$. Allora, $\forall\, i \in I$ si possono costruire dei polinomi $F_i \in \mathbb{Z}[x]$ monici irriducibili con $deg(F_i) = deg(f_i) = n_i$, $F_i \neq F_j$ $\forall\, i \neq j$ e tali che, preso un qualunque $J \subseteq I$ e posto $g_i = F_i$ per $i \in J$ e $g_i = f_i$ per $i \in I \setminus J$, si ha*

$$\mathsf{d}\left(\prod_{i \in K} g_i\right) = \mathsf{d}\left(\prod_{i \in K} f_i\right)$$

$\forall\, K \subseteq I$.

Dimostrazione. Si ponga $n = \sum_{i \in I} n_i$; chiamati $p_1, ..., p_s$ tutti i primi minori o uguali di n, si definisca $\alpha_i = v_{p_i}(n!)$. Fissato ora $i \in I$ e un primo $q > n$, bisogna cercare $\varphi_i \in \mathbb{Z}[x]$ di grado minore di f_i in modo tale che $F_i = f_i + \varphi_i$ risulti irriducibile per il criterio di Eisenstein. Posto, dunque,

$$f_i(x) = x^{n_i} + \sum_{k=0}^{n_i - 1} a_{ik} x^k \text{ e}$$

$$\varphi_i(x) = \sum_{h=0}^{m_i} b_{ih} x^h,$$

dove $m_i = deg(\varphi_i) = \max\{k \in \{0, ..., n_i - 1\} |\, a_{ik} \neq 0\} < n_i$, $a_{ik}, b_{ih} \in \mathbb{Z}$ $\forall\, k, h$, si cerca b_{ik} con $k \in \{1, ..., m_i\}$ che soddisfa il seguente sistema di congruenze

$$\begin{cases} b_{ik} \equiv -a_{ik} \pmod{q} \\ b_{ik} \equiv 0 \pmod{p_l^{\alpha_l}} \ \forall\, l \in \{1, ..., s\} \end{cases}$$

e b_{i0} che soddisfa quest'altro sistema di congruenze

$$\begin{cases} b_{i0} \equiv -a_{i0} + q \pmod{q^2} \\ b_{i0} \equiv 0 \pmod{p_l^{\alpha_l}} \ \forall\, l \in \{1, ..., s\} \end{cases}$$

L'esistenza dei b_{ik} è garantita dal Teorema Cinese del Resto, dal momento che in entrambi i casi i naturali rispetto a cui si fanno le congruenze sono a due a due coprimi. In particolare si ha che $\prod_{l=1}^{s} p_l^{\alpha_l} \mid b_{ik}\ \forall\, k \in \{0, ..., m_i\}$, dunque $\varphi_i \in \left(\prod_{l=1}^{s} p_l^{\alpha_l}\right) \mathbb{Z}[x]$.
Per far sì che tutti gli F_i siano tra loro distinti, dopo aver definito un ordine totale $(I, \leq)$, nel caso in cui $\exists\, j < i$ tale che $F_i = F_j$, basta sostituire F_i con $F_i + q^2 \prod_{l=1}^{s} p_l^{\alpha_l}$.
Per quanto riguarda, invece, l'ultima affermazione, per prima cosa bisogna osservare che, essendo $\prod_{i\in K} g_i$ (rispettivamente $\prod_{i\in K} f_i$) primitivo poiché monico, i primi che possono dividere $\mathsf{d}(\prod_{i\in K} g_i)$ (rispettivamente $\mathsf{d}(\prod_{i\in K} f_i)$) sono tra i p_i con $i \in \{1, ..., s\}$ che sono minori o uguali di $\sum_{i\in K} n_i$ e per questi primi vale $v_{p_i}\left(\mathsf{d}\left(\prod_{i\in K} g_i\right)\right) \leq v_{p_i}(n!) = \alpha_i$ (rispettivamente $v_{p_i}\left(\mathsf{d}\left(\prod_{i\in K} f_i\right)\right) \leq v_{p_i}(n!)$) (Lemma (2.18)). Inoltre $\forall\, z \in \mathbb{Z}$ e $\forall\, l \in \{1, ..., s\}$ vale

$$\prod_{i\in K} g_i(z) \equiv \prod_{i\in K} f_i(z)\ \ (mod\ p_l^{\alpha_l}),$$

infatti

$$\begin{aligned}
\prod_{i\in K} g_i(z) &= \prod_{j\in(K\cap J)} g_j(z) \prod_{i\in K\setminus(K\cap J)} g_i(z) = \\
&= \prod_{j\in(K\cap J)} F_j(z) \prod_{i\in K\setminus(K\cap J)} f_i(z) = \\
&= \prod_{j\in(K\cap J)} (f_j(z) + \varphi_j(z)) \prod_{i\in K\setminus(K\cap J)} f_i(z) \equiv \\
&\equiv \prod_{j\in(K\cap J)} f_j(z) \prod_{i\in K\setminus(K\cap J)} f_i(z) = \prod_{i\in K} f_i(z)\ \ (mod\ p_l^{\alpha_l}),
\end{aligned}$$

dove la congruenza è dovuta al fatto che, essendo $\varphi_i \in \left(\prod_{l=1}^{s} p_l^{\alpha_l}\right) \mathbb{Z}[x]$, $\varphi_i(z) \equiv 0 \pmod{p_l^{\alpha_l}}\ \forall\, l \in \{1, ..., s\}$. Quindi

$$p_l^{\beta_l} \mid \mathsf{d}\left(\prod_{i\in K} g_i\right) \iff p_l^{\beta_l} \mid \mathsf{d}\left(\prod_{i\in K} f_i\right),$$

dove $\beta_l \leq \alpha_l$, da cui segue che $\mathsf{d}\left(\prod_{i\in K} g_i\right) = \mathsf{d}\left(\prod_{i\in K} f_i\right)$. □

Un altro risultato che sarà molto utile nelle costruzioni che verranno presentate è dato dal seguente Lemma:

Lemma 2.23. *Sia $p \in \mathbb{Z}$ un primo e*

$$g(x) = \frac{\prod_{i\in I} f_i(x)}{p} \ \in\ \mathrm{Int}(\mathbb{Z}),$$

dove $I \neq \emptyset$ è un insieme finito, $f_i \in \mathbb{Z}[x]$ è primitivo e irriducibile $\forall\, i \in I$ e $p = \mathsf{d}\left(\prod_{i\in I} f_i(x)\right)$. Allora tutte le fattorizzazioni in $\mathrm{Int}(\mathbb{Z})$ di g sono

essenzialmente uguali a

$$g(x) = \frac{\prod_{j\in J} f_j(x)}{p} \prod_{i\in I\setminus J} f_i(x), \tag{2.7}$$

con $J \subseteq I$ *minimale tale che* $p = \mathsf{d}\left(\prod_{j\in J} f_j(x)\right)$.

Dimostrazione. Un fattore irriducibile di g deve essere del tipo $\frac{\prod_{j\in J} f_j(x)}{p_1}$ con $\emptyset \neq J \subseteq I$, $p_1 = \mathsf{d}\left(\prod_{j\in J} f_j(x)\right)$ e $p_1 \mid p$; quest'ultima condizione, dato che p è primo, implica che $p_1 = 1$ o $p_1 = p$, ma si può supporre che valga $p_1 = p$. In questo modo si scrive g come nell'espressione (2.7), ma bisogna mostrare che i fattori sono irriducibili. Usando la proprità (1.14)(ii) si vede che

$$\mathsf{d}\left(\prod_{j\in J} f_j(x)\right) \mathsf{d}\left(\prod_{i\in I\setminus J} f_i(x)\right) \mid \mathsf{d}\left(\prod_{i\in I} f_i(x)\right) = p$$

e, essendo $p = \mathsf{d}\left(\prod_{j\in J} f_j(x)\right)$, si ha che $\mathsf{d}\left(\prod_{i\in I\setminus J} f_i(x)\right) = 1$. Sempre grazie alla proprietà (1.14)(ii),

$$\mathsf{d}(f_i) \mid \mathsf{d}\left(\prod_{i\in I\setminus J} f_i(x)\right) = 1 \ \ \forall\, i \in I \setminus J,$$

perciò $\mathsf{d}(f_i) = 1\ \forall\, i \in I \setminus J$. I polinomi f_i con $i \in I \setminus J$ sono tutti irriducibili in $\mathrm{Int}(\mathbb{Z})$ (Lemma (1.18)). Bisogna ora mostrare che J è minimale. Se per assurdo J non fosse minimale, allora $\exists\, \emptyset \neq J' \subsetneq J$ con $p = \mathsf{d}\left(\prod_{j\in J'} f_j(x)\right)$. Se si scrive

$$\frac{\prod_{j\in J} f_j(x)}{p} = \frac{\prod_{j\in J'} f_j(x)}{p} \prod_{i\in J\setminus J'} f_i(x),$$

si ha che entrambi i fattori sono non costanti, dunque non invertibili in $\mathrm{Int}(\mathbb{Z})$, contro il fatto che $\frac{\prod_{j\in J} f_j(x)}{p}$ è irriducibile in $\mathrm{Int}(\mathbb{Z})$. □

Prima di analizzare il caso generale, verranno proposti due esempi, ognuno seguito anche da un esempio numerico, in cui compariranno particolari lunghezze delle fattorizzazioni del polinomio cercato; questi esempi porteranno poi a dedurre delle proprietà dell'anello $\mathrm{Int}(\mathbb{Z})$.

Costruzione 2.24. Sia $n \geq 0$. È sempre possibile costruire un polinomio $h \in \mathrm{Int}(\mathbb{Z})$ che ammette esattamente due fattorizzazioni in irriducibili in $\mathrm{Int}(\mathbb{Z})$ essenzialmente diverse, di lunghezze 2 e $n + 2$.

Dimostrazione. Sia p un primo con $p > n+1$. Sia $\{a_1, ..., a_p\}$ un sistema completo di residui modulo p che non contenga un sistema completo di residui modulo $q\ \forall\, q < p$ primo (esiste per il Lemma (2.21)). Si definiscano i polinomi

$$f(x) = (x - a_2) \cdots (x - a_p) \text{ e}$$
$$g(x) = (x - a_{n+2}) \cdots (x - a_p),$$

monici e non costanti ($p \geq n+2 \geq 2$). Per il Lemma (2.22), si possono costruire i polinomi $F(x)$ e $G(x) \in \mathbb{Z}[x]$ monici, diversi tra loro e irriducibili in $\mathbb{Z}[x]$ con $deg(f) = deg(F)$ e $deg(g) = deg(G)$ tali che il divisore fisso di un qualunque prodotto tra i polinomi $f(x)$, $g(x)$ e $(x - a_i)$ al variare di $i \in \{1, ..., n+1\}$ (anche questi ultimi sono monici e irriducibili in $\mathbb{Z}[x]$) è uguale al divisore fisso dello stesso prodotto in cui $f(x)$ e $g(x)$ vengono sostituiti con $F(x)$ e $G(x)$. A questo punto basta definire

$$h(x) = \frac{F(x)(x - a_1) \cdots (x - a_{n+1})G(x)}{p}$$

e dimostrare che

$$p = \mathsf{d}\left(F(x)(x - a_1) \cdots (x - a_{n+1})G(x)\right) =$$
$$= \mathsf{d}\left(f(x)(x - a_1) \cdots (x - a_{n+1})g(x)\right),$$

dove la seconda uguaglianza segue dal Lemma (2.22). Per fare questo, si prenda $z \in \mathbb{Z}$, dal momento che $\{a_1, ..., a_p\}$ è un sistema completo di residui modulo p, $\exists\, i_z \in \{1, ..., p\}$ tale che $z \equiv a_{i_z} \pmod{p}$, ossia $p \mid (z - a_{i_z})$. Si osservi che

$$f(x)(x - a_1) \cdots (x - a_{n+1})g(x) = (x - a_1) \prod_{i=2}^{p} (x - a_i)^2,$$

dunque $p \mid f(z)(z - a_1) \cdots (z - a_{n+1})g(z)$ e, siccome questo vale $\forall\, z \in \mathbb{Z}$, allora $p \mid \mathsf{d}\left(f(x)(x - a_1) \cdots (x - a_{n+1})g(x)\right)$. Inoltre, si può vedere che $v_p\left(\mathsf{d}\left(f(x)(x - a_1) \cdots (x - a_{n+1})g(x)\right)\right) = 1$, infatti, $\forall\, z \in \mathbb{Z}$ tale che $z \equiv a_1 \pmod{p}$ si ha che $p^2 \nmid f(z)(z - a_1) \cdots (z - a_{n+1})g(z)$ (in questo prodotto il fattore $(x - a_1)$ compare con esponente 1). L'unica cosa che resta da mostrare è che nessun altro primo divide $\mathsf{d}\left(f(x)(x - a_1) \cdots (x - a_{n+1})g(x)\right)$: sia, quindi, $q \neq p$ un primo, dato che $\{a_1, ..., a_p\}$ è sistema completo di residui modulo p che non contiene un sistema completo di residui modulo q, allora $\exists\, z \in \mathbb{Z}$ tale che $z \not\equiv a_i \pmod{q}\ \forall\, i \in \{1, ..., p\}$, perciò $q \nmid \mathsf{d}\left(f(x)(x - a_1) \cdots (x - a_{n+1})g(x)\right)$. Tutto ciò permette di concludere che $p = \mathsf{d}\left(f(x)(x - a_1) \cdots (x - a_{n+1})g(x)\right)$. Essendo soddisfatte tutte le ipotesi del Lemma (2.23) (tutti i fattori che compaiono al numeratore di h sono monici, dunque primitivi, e irriducibili in $\mathbb{Z}[x]$), si ha che h ha solamente

due fattorizzazioni essenzialmente diverse in $\mathrm{Int}(\mathbb{Z})$, cioè

$$h(x) = \frac{F(x)(x-a_1)}{p} \cdot (x-a_2)\cdots(x-a_{n+1})G(x) \text{ e}$$
$$h(x) = F(x) \cdot \frac{(x-a_1)\cdots(x-a_{n+1})G(x)}{p},$$

la prima di lunghezza $n+2$ e la seconda di lunghezza 2. Le fattorizzazioni sono solo queste poiché $\mathsf{d}(F(x)(x-a_1)) = p = \mathsf{d}((x-a_1)\cdots(x-a_{n+1})G(x))$ e il numero di fattori è il più piccolo possibile affinchè questo valga (infatti nei prodotti $f(x)(x-a_1)$ e $(x-a_1)\cdots(x-a_{n+1})g(x)$ compaiono tutti i fattori $(x-a_i)$ con $i \in \{1,...,p\}$ con esponente 1). □

Esempio 2.25. Siano $n = 1$ e $p = 3$ ($p > 2$). Risolvendo il sistema di congruenze nella dimostrazione del Lemma (2.21) (l'unico primo minore di p è 2) si ottiene il sistema completo di residui modulo 3 $\{1,3,5\}$; si può porre $a_1 = 1$, $a_2 = 3$ e $a_3 = 5$ e si può procedere come nella costruzione (2.24) definendo

$$f(x) = (x-3)(x-5) = x^2 - 8x + 15 \text{ e}$$
$$g(x) = x - 5.$$

A questo punto, dati $f(x)$, $g(x)$, $(x-1)$ e $(x-3)$, bisogna determinare $F(x)$ e $G(x)$ come nella dimostrazione del Lemma (2.22), ma, essendo $g(x)$ già irriducibile, si può porre $G(x) = g(x) = x - 5$; la somma dei gradi di questi polinomi risulta essere 5, dunque $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ sono i primi minori o uguali di 5 e di conseguenza $\alpha_1 = v_2(5!) = 3$, $\alpha_2 = v_3(5!) = 1$ e $\alpha_3 = v_5(5!) = 1$. Dopo aver scelto $q = 7 > 5$, per determinare $F(x)$ bisogna calcolare i coefficienti di $\varphi(x) = b_1x + b_0$ che soddisfano ai due sistemi di congruenze

$$\begin{cases} b_0 \equiv -15 + 7 \ (mod\ 49) \\ b_0 \equiv 0 \ (mod\ 8) \\ b_0 \equiv 0 \ (mod\ 3) \\ b_0 \equiv 0 \ (mod\ 5) \end{cases}$$

$$\begin{cases} b_1 \equiv 8 \ (mod\ 7) \\ b_1 \equiv 0 \ (mod\ 8) \\ b_1 \equiv 0 \ (mod\ 3) \\ b_1 \equiv 0 \ (mod\ 5) \end{cases}$$

Utilizzando il programma *Mathematica*, che sfrutta il Teorema Cinese del Resto, si ottengono $b_0 = 1560$ e $b_1 = 120$, dunque $F(x) = x^2 + 112x + 1575$ e

$$h(x) = \frac{(x^2 + 112x + 1575)(x-1)(x-3)(x-5)}{3},$$

le cui fattorizzazioni in Int($\mathbb{Z}$) sono

$$h(x) = \frac{(x^2+112x+1575)(x-1)}{3} \cdot (x-3)(x-5) \text{ e}$$
$$h(x) = (x^2+112x+1575) \cdot \frac{(x-1)(x-3)(x-5)}{3}.$$

Corollario 2.26. $\rho(\text{Int}(\mathbb{Z})) = \infty$.

Dimostrazione. Sia $n \geq 0$, per l'esempio (2.24), $\exists\, f_n \in \text{Int}(\mathbb{Z})$ tale che $\rho(f_n) = \frac{n+2}{2}$. Perciò esiste una successione $\{f_n\}_{n\geq 0} \subseteq \text{Int}(\mathbb{Z})$ di elementi non nulli e non invertibili tale che

$$\lim_{n\to+\infty} \rho(f_n) = \lim_{n\to+\infty} \frac{n+2}{2} = \infty,$$

dunque $\rho(\text{Int}(\mathbb{Z})) = \sup_{f\in\text{Int}(\mathbb{Z})'} \rho(f) = \infty$. □

Costruzione 2.27. Siano $1 \leq m \leq n$. È sempre possibile costruire un polinomio $h \in \text{Int}(\mathbb{Z})$ che ammette esattamente due fattorizzazioni in Int($\mathbb{Z}$) essenzialmente diverse, di lunghezze $m+1$ e $n+1$.

Dimostrazione. La dimostrazione procede in modo molto simile a quella della costruzione (2.24). Sia $p > mn$ un primo e $s = p - mn$. Si consideri un sistema completo R di residui modulo p che non contenga un sistema completo di residui modulo $q\ \forall\, q < p$ primo (esiste per il Lemma (2.21)) e avente i seguenti elementi

$$R = \{r(i,j) |\, 1 \leq i \leq m, 1 \leq j \leq n\} \cup \{b_1, ..., b_s\}.$$

Si definiscano i polinomi monici e non costanti

$$f_i(x) = \prod_{j=1}^{n} (x - r(i,j)) \text{ per } i \in \{1, ..., m\} \text{ e}$$
$$g_j(x) = \prod_{i=1}^{m} (x - r(i,j)) \text{ per } j \in \{1, ..., n\};$$

per il Lemma (2.22), si possono costruire i polinomi F_i e G_j con $i \in \{1, ..., m\}$ e $j \in \{1, ..., n\}$ tutti diversi tra loro, monici, irriducibili in $\mathbb{Z}[x]$ e con $deg(f_i) = deg(F_i)$ e $deg(g_j) = deg(G_j)$, tali che il divisore fisso di un qualsiasi prodotto tra f_i, g_j e $(x-b_k)$ con $i \in \{1, ..., m\}$, $j \in \{1, ..., n\}$ e $k \in \{1, ..., s\}$ (questi ultimi sono monici e irriducibili in $\mathbb{Z}[x]$) è uguale al divisore fisso dello stesso prodotto in cui f_i viene sostituito con F_i e g_j viene sostituito con G_j. Il polinomio cercato risulta essere

$$h(x) = \frac{1}{p}(x - b_1) \cdots (x - b_s) \prod_{i=1}^{m} F_i(x) \prod_{j=1}^{n} G_j(x),$$

infatti, dal momento che h soddisfa tutte le ipotesi del Lemma (2.23), ossia tutti i fattori sono primitivi, poiché monici, e irriducibili in $\mathbb{Z}[x]$ e, come fatto nella dimostrazione dell'esempio (2.24), è possibile far vedere che $p = \mathsf{d}\left((x-b_1)\cdots(x-b_s)\prod_{i=1}^{m}F_i(x)\prod_{j=1}^{n}G_j(x)\right)$, allora risulta che h ha due fattorizzazioni in $\mathrm{Int}(\mathbb{Z})$ essenzialmente diverse

$$h(x) = \frac{(x-b_1)\cdots(x-b_s)\prod_{i=1}^{m}F_i(x)}{p}\cdot\prod_{j=1}^{n}G_j(x) \text{ e}$$
$$h(x) = \prod_{i=1}^{m}F_i(x)\cdot\frac{(x-b_1)\cdots(x-b_s)\prod_{j=1}^{n}G_j(x)}{p},$$

la prima di lunghezza $n+1$ e la seconda di lunghezza $m+1$. Queste sono le uniche due fattorizzazioni possibili poiché i prodotti $(x-b_1)\cdots(x-b_s)\prod_{i=1}^{m}F_i(x)$ e $(x-b_1)\cdots(x-b_s)\prod_{j=1}^{n}G_j(x)$ sono gli unici in cui compaiono una sola volta tutti i fattori del tipo $(x-r)$ con $r \in R$ con esponente 1. □

Esempio 2.28. Siano $m = 1$, $n = 2$ e $p = 3$, dunque $s = 1$. Un sistema completo di residui modulo 3 che non contenga un sistema completo di residui modulo 2 è $\{1, 3, 5\}$ (come nell'esempio (2.25)). Ponendo $r(1,1) = 1$, $r(1,2) = 3$ e $b_1 = 5$, si ottengono i polinomi

$$f_1(x) = (x-1)(x-3) = x^2 - 4x + 3,$$
$$g_1(x) = x - 1 \text{ e}$$
$$g_2(x) = x - 3.$$

Come fatto nell'esempio (2.25), ossia seguendo la dimostrazione del Lemma (2.22), e sfruttando il programma *Mathematica*, se si sceglie come primo $q = 7$ (essendo la somma dei gradi dei polinomi considerati, a cui va aggiunto $x-5$, uguale a 5), si ha che $p_1 = 2$ e $\alpha_1 = 3$, $p_2 = 3$ e $\alpha_2 = 1$, $p_3 = 5$ e $\alpha_3 = 1$ e si trova $F_1(x) = x^2 + 476x + 2163$, mentre si può porre $G_1(x) = g_1(x) = x - 1$ e $G_2(x) = g_2(x) = x - 3$. Dunque si ottiene

$$h(x) = \frac{1}{3}(x-5)(x^2+476x+2163)(x-1)(x-3)$$

e due fattorizzazioni in $\mathrm{Int}(\mathbb{Z})$ essenzialmente diverse risultano essere

$$h(x) = \frac{(x-5)(x^2+476x+2163)}{3}\cdot(x-1)(x-3) \text{ e}$$
$$h(x) = (x^2+476x+2163)\cdot\frac{(x-5)(x-1)(x-3)}{3}.$$

Corollario 2.29. $\mathrm{Int}(\mathbb{Z})$ *è totalmente elastico.*

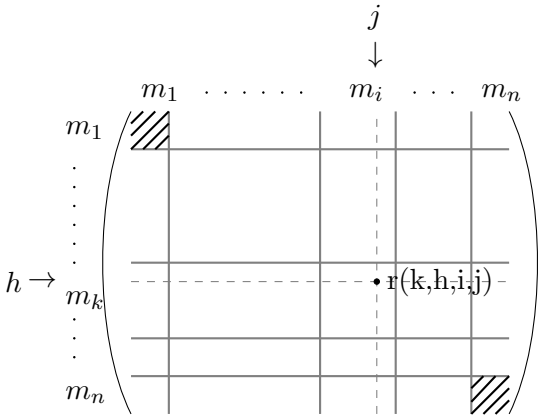
Dimostrazione. Sia $\frac{a}{b} \in \mathbb{Q}$ con $\frac{a}{b} \geq 1$ e $a, b \in \mathbb{N}$, $b \neq 0$. Se si pone $a = n+1$ e $b = m+1$, per l'esempio (2.27) esiste $f \in \mathrm{Int}(\mathbb{Z})$ tale che $\rho(f) = \frac{n+1}{m+1} = \frac{a}{b}$. □

Teorema 2.30 (Caso generale)**.** *Siano* $1 \leq m_1 \leq \cdots \leq m_n$ *numeri naturali, allora si può costruire un polinomio* $h \in \mathrm{Int}(\mathbb{Z})$ *che abbia esattamente* n *fattorizzazioni in* $\mathrm{Int}(\mathbb{Z})$ *essenzialmente diverse, di lunghezze* m_1+1*,...,* m_n+1*.*

Dimostrazione. Siano $N = \left(\sum_{i=1}^{n} m_i\right)^2 - \sum_{i=1}^{n} m_i^2 = \sum_{1\leq i<j\leq n} 2m_i m_j$, $p > N$ un primo e $s = p - N$. Si consideri un sistema completo R di residui modulo p che non contenga un sistema completo di residui modulo $q \; \forall \, q < p$ primo (esiste per il Lemma (2.21)) e avente i seguenti elementi

$$R = R_0 \cup \{b_1, ..., b_s\} \text{ con}$$
$$R_0 = \{r(k,h,i,j) | \, 1 \leq k \leq n, 1 \leq h \leq m_k, 1 \leq i \leq n, 1 \leq j \leq m_i, i \neq k\}$$

Gli elementi di R_0 si possono vedere come le entrate di una matrice: basta considerare una matrice quadrata $m \times m$ con $m = \sum_{i=1}^{n} m_i$, suddivisa in n^2 blocchi di dimensione $m_i \times m_j$ con $i, j \in \{1, ..., n\}$; $r(k,h,i,j) \in R_0$ è l'elemento che sta nella h-esima riga del k-esimo blocco di righe e nella j-esima colonna dell'i-esimo blocco di colonne, come mostrato nella figura seguente. Dato che $\nexists \, r(k,h,i,j)$ se $i = k$, allora i blocchi diagonali di dimensione $m_i \times m_i$ con $i \in \{1, ..., n\}$ vengono lasciati vuoti. Le entrate di questa matrice risultano essere esattamente N, dunque $|R_0| = N$.



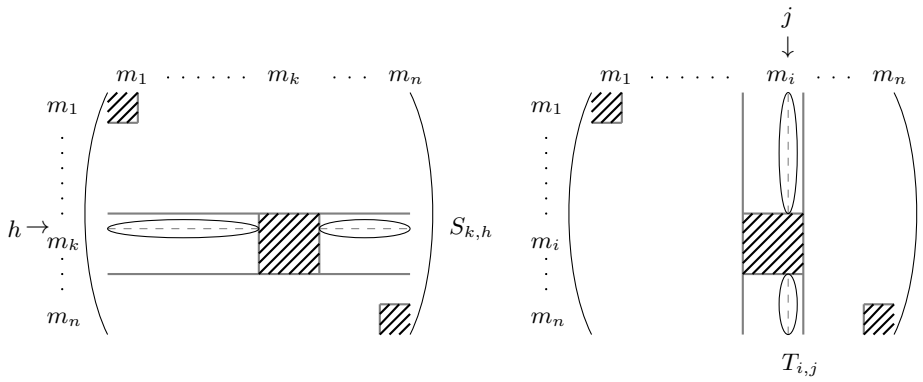
Si definiscano ora due sottoinsiemi di R_0: fissati $k \in \{1, ..., n\}$ e $h \in \{1, ..., m_k\}$

$$S_{k,h} = \{r(k,h,i,j) | \, 1 \leq i \leq n, 1 \leq j \leq m_i, i \neq k\}$$

contiene tutti gli elementi dell'h-esima riga del k-esimo blocco di righe della matrice costruita precedentemente; invece, fissati $i \in \{1, ..., n\}$ e $j \in \{1, ..., m_i\}$

$$T_{i,j} = \{r(k,h,i,j) | \, 1 \leq k \leq n, 1 \leq h \leq m_k, i \neq k\}$$

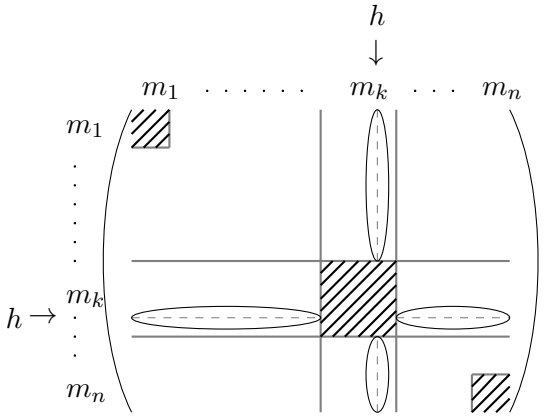
contiene tutti gli elementi della j-esima colonna dell'i-esimo blocco di colonne (i due insiemi appena definiti sono rappresentati nelle figure sottostanti).



Fissati $k \in \{1, ..., n\}$ e $h \in \{1, ..., m_k\}$, si considerino i polinomi

$$f_h^{(k)}(x) = \prod_{s \in S_{k,h}} (x - s) \prod_{t \in T_{k,h}} (x - t)$$

monici e non costanti, le cui radici sono rappresentate nella seguente figura



Per il Lemma (2.22), si possono costruire i polinomi $F_h^{(k)}$ con $k \in \{1, ..., n\}$ e $h \in \{1, ..., m_k\}$ tutti diversi tra loro, monici, irriducibili in $\mathbb{Z}[x]$ e tali che $deg(f_h^{(k)}) = deg(F_h^{(k)})$ con la proprietà che il divisore fisso di un qualsiasi prodotto tra $f_h^{(k)}$ con $k \in \{1, ..., n\}$ e $h \in \{1, ..., m_k\}$ e $(x - b_l)$ con $l \in \{1, ..., s\}$ (anche questi ultimi polinomi sono monici e irriducibili in $\mathbb{Z}[x]$) è uguale al divisore fisso dello stesso prodotto in cui al posto di $f_h^{(k)}$ si sostituisce $F_h^{(k)}$. Il polinomio cercato risulta essere

$$h(x) = \frac{1}{p}(x - b_1) \cdots (x - b_s) \prod_{k=1}^{n} \prod_{h=1}^{m_k} F_h^{(k)}(x),$$

infatti soddisfa a tutte le ipotesi del Lemma (2.23), ossia tutti i fattori sono primitivi, poiché monici, e irriducibili in $\mathbb{Z}[x]$ e si può mostrare che

$$p = \mathsf{d}\left((x-b_1)\cdots(x-b_s)\prod_{k=1}^{n}\prod_{h=1}^{m_k}F_h^{(k)}(x)\right) = \\ = \mathsf{d}\left((x-b_1)\cdots(x-b_s)\prod_{k=1}^{n}\prod_{h=1}^{m_k}f_h^{(k)}(x)\right)$$

come nella dimostrazione dell'esempio (2.24), dunque le fattorizzazioni di h in $\mathrm{Int}(\mathbb{Z})$ essenzialmente diverse sono

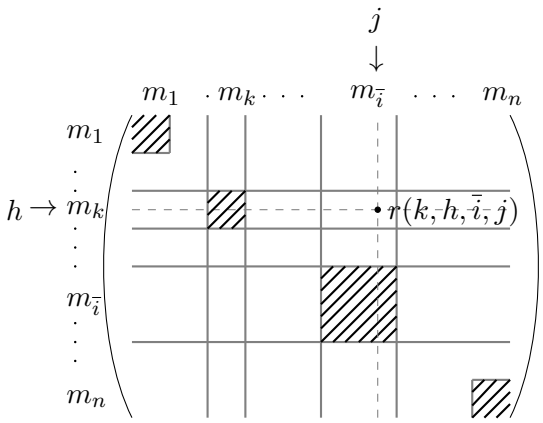
$$h(x) = F_1^{(i)}\cdots F_{m_i}^{(i)}\cdot\frac{(x-b_1)\cdots(x-b_s)\prod_{k\neq i}\prod_{h=1}^{m_k}F_h^{(k)}(x)}{p}$$

al variare di $i\in\{1,...,n\}$ e sono di lunghezza m_i+1. Fissato $\bar{i}\in\{1,...,n\}$, per provare che le fattorizzazioni sono solo queste, bisogna far vedere che $(x-b_1)\cdots(x-b_s)\prod_{k\neq\bar{i}}\prod_{h=1}^{m_k}F_h^{(k)}(x)$ è costituito dal più piccolo numero di fattori in modo tale che

$$p = \mathsf{d}\left((x-b_1)\cdots(x-b_s)\prod_{k\neq\bar{i}}\prod_{h=1}^{m_k}F_h^{(k)}(x)\right) = \\ = \mathsf{d}\left((x-b_1)\cdots(x-b_s)\prod_{k\neq\bar{i}}\prod_{h=1}^{m_k}f_h^{(k)}(x)\right),$$

ossia bisogna mostrare che nel prodotto $\prod_{k\neq\bar{i}}\prod_{h=1}^{m_k}f_h^{(k)}(x)$ compaiono tutti i fattori del tipo $(x-r)$ con $r\in R_0$ e che non si può prendere un numero minore di fattori affinchè questo accada. Per quanto riguarda la prima affermazione, fissato $t\in\{1,...,n\}$, $t\neq\bar{i}$, $\prod_{h=1}^{m_t}f_h^{(t)}(x)$ ha come radici $r(t,h,i,j)$ con $h\in\{1,...,m_t\}$, $i\in\{1,...,n\}$, $j\in\{1,...,m_i\}$, $t\neq i$ e $r(k,h,t,j)$ con $k\in\{1,...,n\}$, $h\in\{1,...,m_k\}$, $j\in\{1,...,m_t\}$, $t\neq k$, ossia tutti gli elementi del t-esimo blocco di righe e di colonne; l'unica cosa, quindi, da verificare è che gli elementi $r(\bar{i},h,i,j)$ con $h\in\{1,...,m_{\bar{i}}\}$, $i\in\{1,...,n\}$, $j\in\{1,...,m_i\}$, $i\neq\bar{i}$ e $r(k,h,\bar{i},j)$ con $k\in\{1,...,n\}$, $h\in\{1,...,m_k\}$, $j\in\{1,...,m_{\bar{i}}\}$, $k\neq\bar{i}$ sono radici di qualcuno dei polinomi in $\prod_{k\neq\bar{i}}\prod_{h=1}^{m_k}f_h^{(k)}(x)$:

(i) $r(k,h,\bar{i},j)\in S_{k,h}$, dunque è radice di $f_h^{(k)}$ con $k\neq\bar{i}$ e $h\in\{1,...,m_k\}$;



(ii) $r(\bar{i},h,i,j) \in T_{i,j}$, dunque è radice di $f_j^{(i)}$ con $i \neq \bar{i}$ e $j \in \{1,...,m_i\}$.

Si supponga ora di eliminare uno dei polinomi in $\prod_{k\neq\bar{i}} \prod_{h=1}^{m_k} f_h^{(k)}(x)$, sia questo $f_s^{(t)}$ con $t \neq \bar{i}$ e $s \in \{1,...,m_t\}$, allora gli elementi $r(t,h,\bar{i},j)$ con $h \in \{1,...,m_t\}$, $j \in \{1,...,m_{\bar{i}}\}$ e $r(\bar{i},h,t,j)$ con $h \in \{1,...,m_{\bar{i}}\}$, $j \in \{1,...,m_t\}$ non sono più radici del nuovo polinomio ottenuto eliminando $f_s^{(t)}$. □

Corollario 2.31. *Per ogni sottoinsieme finito* $\mathcal{S} \subseteq \mathbb{N} \setminus \{1\}$ $\exists\, f \in \mathrm{Int}(\mathbb{Z})$ *tale che* $\mathcal{S} = \mathcal{L}(f)$.

Capitolo 3

Elementi non assolutamente irriducibili in Int($\mathbb{Z}$)

In questo capitolo verranno studiati gli elementi non assolutamente irriducibili dell'anello Int($\mathbb{Z}$). Dopo aver costruito degli esempi di polinomi $f \in$ Int($\mathbb{Z}$) che ammettono una o più potenze con fattorizzazioni in irriducibili in Int($\mathbb{Z}$) essenzialmente diverse, tutte della stessa lunghezza o di lunghezze differenti, questi esempi verranno generalizzati per ottenere delle condizioni che permettono di affermare che un elemento di Int($\mathbb{Z}$) non è assolutamente irriducibile.

3.1 Costruzione di elementi non assolutamente irriducibili in Int($\mathbb{Z}$)

Tutti gli esempi di questa sezione saranno costruiti seguendo uno stesso schema:

1) Costruzione del polinomio f;

2) Dimostrazione che $f \in$ Int($\mathbb{Z}$) è irriducibile provando che sono soddisfatte tutte le condizioni del Lemma (2.11);

3) Descrizione delle fattorizzazioni in Int($\mathbb{Z}$) delle potenze di f essenzialmente diverse dal prodotto di copie di f.

Alcune costruzioni saranno seguite anche da un esempio numerico.

Per prima cosa bisogna introdurre una notazione: se G è un gruppo moltiplicativo, l'ordine di un elemento $g \in G$ verrà indicato con $ord(g)$ ed è il più piccolo intero positivo n tale che $g^n = 1_G$, dove 1_G è l'identità del gruppo preso in considerazione. Prima di analizzare gli esempi, è anche necessario

ricordare che se p è un primo dispari e $n \geq 1$ è un numero naturale, gli elementi invertibili dell'anello $\mathbb{Z}/p^n\mathbb{Z} = \{0, ..., p^n - 1\}$

$$(\mathbb{Z}/p^n\mathbb{Z})^* = \{u \in \mathbb{Z}/p^n\mathbb{Z} \mid \gcd(u, p^n) = 1\}$$

formano un gruppo ciclico di ordine $\varphi(p^n) = p^{n-1}(p-1)$ (dove φ è la funzione di Eulero). Posto $\varphi(p^n) = 2k$, si può definire l'omomorfismo di gruppi

$$\begin{aligned} \psi : (\mathbb{Z}/p^n\mathbb{Z})^* &\longrightarrow (\mathbb{Z}/p^n\mathbb{Z})^* \\ x &\longmapsto x^k \end{aligned}$$

Dato che $x^{2k} \equiv 1 \pmod{p^n}$ $\forall\, x \in (\mathbb{Z}/p^n\mathbb{Z})^*$, allora $x^k \equiv \pm 1 \pmod{p^n}$, da cui segue che $\psi((\mathbb{Z}/p^n\mathbb{Z})^*) = \{\pm 1\}$. Siccome per il primo Teorema di isomorfismo

$$\psi((\mathbb{Z}/p^n\mathbb{Z})^*) \cong \frac{(\mathbb{Z}/p^n\mathbb{Z})^*}{ker\psi},$$

in particolare questi due gruppi hanno lo stesso ordine, ossia $|ker\psi| = \frac{|(\mathbb{Z}/p^n\mathbb{Z})^*|}{|\psi((\mathbb{Z}/p^n\mathbb{Z})^*)|} = k$.

Lemma 3.1. *Con riferimento alle notazioni precedenti si ha che*

$$ker\psi = \{x \in (\mathbb{Z}/p^n\mathbb{Z})^* \mid \exists\, y \in (\mathbb{Z}/p^n\mathbb{Z})^* \text{ t.c. } x \equiv y^2 \ (mod\ p^n)\},$$

cioè $ker\psi$ è costituito dai quadrati modulo p^n.

Dimostrazione. ($\supseteq$) Sia $x \in (\mathbb{Z}/p^n\mathbb{Z})^*$, $x \equiv y^2 \pmod{p^n}$ $\exists\, y \in (\mathbb{Z}/p^n\mathbb{Z})^*$. Dato che $x^k \equiv y^{2k} \equiv 1 \pmod{p^n}$, si ha che $x \in ker\psi$.
($\subseteq$) Sia $x \in ker\psi$ e z un generatore di $(\mathbb{Z}/p^n\mathbb{Z})^*$. Allora $\exists\, t \in \mathbb{N}$ tale che $x \equiv z^t \pmod{p^n}$, perciò $1 \equiv x^k \equiv z^{kt} \pmod{p^n}$, da cui segue che $ord(z) = 2k \mid kt$, ossia t deve essere pari. Allora $x \equiv (z^s)^2 \pmod{p^n}$ $(t = 2s)$, cioè x è un quadrato modulo p^n. □

Le costruzioni seguenti portano a definire un polinomio $f \in \mathrm{Int}(\mathbb{Z})$ che ha tutte le potenze f^k con $k > 1$ con fattorizzazioni in irriducibili in $\mathrm{Int}(\mathbb{Z})$ della stessa lunghezza.

Costruzione 3.2 (Potenza di un solo primo a denominatore)**.**

1) Sia p un primo dispari e $n > 1$ un numero naturale. Si consideri il polinomio
$$h(x) = x^{p^{n-1}(p-1)} - q,$$
dove q è un primo tale che $q \equiv 1 \pmod{p^{n+1}}$ (dunque anche modulo p^n) e $q > p^{n-1}(p-1) + n$. Siano ora $a_1, ..., a_n \in \mathbb{Z}$ tali che

   (i) $a_i \equiv 0 \pmod{p}$ $\forall\, i \in \{1, ..., n\}$;

   (ii) $\exists\, k \in \{0, ..., p-1\}$ tale che $a_i \not\equiv kp \pmod{p^2}$ $\forall\, i \in \{1, ..., n\}$;

(iii) $a_i \not\equiv 0 \pmod{l}$ $\forall\, i \in \{1, ..., n\}$, $\forall\, l$ primo tale che $l \leq p^{n-1}(p-1)+n$, $l \neq p$.

Il polinomio cercato risulta essere

$$f(x) = \frac{h(x)\prod_{i=1}^{n}(x-a_i)}{p^n}.$$

2) Si noti per prima cosa che tutti i polinomi al numeratore di f sono irriducibili in $\mathbb{Z}[x]$ (h lo è per il criterio di Eisenstein) e primitivi, poiché monici. Ora bisogna far vedere che

$$p^n = \mathsf{d}\left(h(x)\prod_{i=1}^{n}(x-a_i)\right); \tag{3.1}$$

la dimostrazione si articola in quattro fasi:

(i) $\min_{u\notin p\mathbb{Z}} v_p(h(u)) = n$ (in realtà per la dimostrazione basta che $v_p(h(u)) \geq n$ $\forall\, u \notin p\mathbb{Z}$);

(ii) $\min_{w\in p\mathbb{Z}} v_p\left(\prod_{i=1}^{n}(w-a_i)\right) = n$;

(iii) $v_p\left(\mathsf{d}\left(h(x)\prod_{i=1}^{n}(x-a_i)\right)\right) = n$;

(iv) $\forall\, l \neq p$ primo, $l \nmid \mathsf{d}\left(h(x)\prod_{i=1}^{n}(x-a_i)\right)$.

Dimostrazione.

(i) Sia $u \notin p\mathbb{Z}$; dato che $\gcd(u,p) = \gcd(u,p^n) = 1$, allora $u \in (\mathbb{Z}/p^n\mathbb{Z})^*$. Siccome

$$u^{\varphi(p^n)} = u^{p^{n-1}(p-1)} \equiv 1 \equiv q \ \ (mod\ \ p^n),$$

si ha che $v_p(h(u)) \geq n$. Se, però, si prende come u il generatore di $(\mathbb{Z}/p^{n+1}\mathbb{Z})^*$, allora

$$u^{p^{n-1}(p-1)} \not\equiv 1 \equiv q \ \ (mod\ \ p^{n+1})$$

dal momento che $ord(u) = p^n(p-1) > p^{n-1}(p-1)$. Dunque in questo caso risulta che $v_p(h(u)) = n$.

(ii) Sia $w \in p\mathbb{Z}$. Dato che $p \mid w$ e $p \mid a_i$ $\forall\, i \in \{1, ..., n\}$ (prima ipotesi sugli a_i), allora $p^n \mid \prod_{i=1}^{n}(w-a_i)$, ossia $v_p\left(\prod_{i=1}^{n}(w-a_i)\right) \geq n$. Sia ora w tale che $w \not\equiv a_i \pmod{p^2}$ $\forall\, i \in \{1, ..., n\}$ (esiste per la seconda ipotesi sugli a_i). Allora, siccome $p^2 \nmid (w-a_i)$ $\forall\, i \in \{1, ..., n\}$, $p^{n+1} \nmid \prod_{i=1}^{n}(w-a_i)$, cioè $v_p\left(\prod_{i=1}^{n}(w-a_i)\right) = n$.

(iii) Sia $z \in \mathbb{Z}$: se $z \notin p\mathbb{Z}$, $v_p(h(z)) \geq n$, mentre $v_p\left(\prod_{i=1}^n (z-a_i)\right) = 0$ ($z \not\equiv a_i \pmod p \ \forall\, i \in \{1,...,n\}$); se $z \in p\mathbb{Z}$, $v_p\left(\prod_{i=1}^n (z-a_i)\right) \geq n$ e $v_p(h(z)) = 0$ ($z \equiv 0 \pmod p$), dunque $v_p\left(\mathsf{d}\left(h(x)\prod_{i=1}^n (x-a_i)\right)\right) \geq n$. Però $p^{n+1} \nmid \mathsf{d}\left(h(x)\prod_{i=1}^n (x-a_i)\right)$: se $w \in p\mathbb{Z}$ è tale che $w \not\equiv a_i \pmod{p^2}\ \forall\, i \in \{1,...,n\}$, allora $v_p\left(h(w)\prod_{i=1}^n (w-a_i)\right) = n$.

(iv) Sia $l \neq p$ un primo. Se $l \leq p^{n-1}(p-1)+n < q$, allora si ottiene che $l \nmid \mathsf{d}\left(h(x)\prod_{i=1}^n (x-a_i)\right)$: $l \nmid h(0)\prod_{i=1}^n (0-a_i) = (-1)^{n+1} q \prod_{i=1}^n a_i$, poiché $l \nmid q$, essendo diverso da questo, e $l \nmid a_i\ \forall\, i \in \{1,...,n\}$ per ipotesi. Se, invece, $l > p^{n-1}(p-1)+n = deg\left(h(x)\prod_{i=1}^n (x-a_i)\right)$, il risultato segue dal Lemma (2.18).

□

Per provare l'irriducibilità bisogna ora mostrare che vale la seconda condizione (2.4) del Lemma (2.3):

Dimostrazione. Bisogna notare che $\mathsf{d}(h(x)) = 1 = \mathsf{d}\left(\prod_{i=1}^n (x-a_i)\right)$. Scelto poi un qualunque $\emptyset \neq I \subsetneq \{1,...,n\}$, $\mathsf{d}\left(\prod_{i\in I}(x-a_i)\right) = 1$: sicuramente questo divisore fisso deve essere una potenza di p (proprietà (1.14)(ii)), ma se $z \notin p\mathbb{Z}$, allora $p \nmid \prod_{i\in I}(z-a_i)$. Allo stesso tempo, $\mathsf{d}\left(h(x)\prod_{i\notin I}(x-a_i)\right) \neq p^n$: se $z \notin p\mathbb{Z}$, $p^n \mid h(z)\prod_{i\notin I}(z-a_i)$; se, invece, $z \in p\mathbb{Z}$, allora $p^{n-|I|} \mid h(z)\prod_{i\notin I}(z-a_i)$ ed $\exists\, w \in p\mathbb{Z}$ tale che $v_p\left(h(w)\prod_{i\notin I}(w-a_i)\right) = n-|I|$, dunque $\mathsf{d}\left(h(x)\prod_{i\notin I}(x-a_i)\right) = p^{n-|I|} \neq p^n$ ($I \neq \emptyset$). □

3) Supponendo che almeno due tra $a_1,...,a_n$ siano diversi, ad esempio a_1 e a_2, e preso un qualsiasi $k > 1$, si ha che

$$f^k = \frac{h(x)(x-a_1)^2\prod_{i=3}^n (x-a_i)}{p^n} \cdot \frac{h(x)(x-a_2)^2\prod_{i=3}^n (x-a_i)}{p^n} \cdot \underbrace{f\cdots f}_{k-2 \text{ volte}}$$

è una fattorizzazione di f^k in Int($\mathbb{Z}$) essenzialmente diversa da $f\cdots f$ (k volte) ($a_1 \neq a_2$), ma con la stessa lunghezza.

Esempio 3.3. Siano $n = 2$ e $p = 3$. Il primo q va scelto in modo tale che $q \equiv 1 \pmod{3^3}$ e che $q > 3\cdot 2 + 2 = 8$, dunque si può prendere, ad esempio, $q = 109$. Invece a_1 e a_2 devono essere multipli di 3, diversi tra loro e non multipli dei primi diversi da 3 minori o uguali di 8, perciò $a_1 = 3$ e $a_2 = 9$ (da notare che non rappresentano tutte le classi divisibili per 3 modulo 9). Allora

$$f(x) = \frac{h(x)(x-a_1)(x-a_2)}{p^n} = \frac{(x^6-109)(x-3)(x-9)}{9} \text{ e}$$

una fattorizzazione in Int(ℤ) di f^k con $k > 1$ essenzialmente diversa da $f \cdots f$ (k volte) risulta essere

$$f^k = \frac{(x^6 - 109)(x-3)^2}{9} \cdot \frac{(x^6 - 109)(x-9)^2}{9} \cdot \underbrace{f \cdots f}_{k-2 \text{ volte}}$$

Costruzione 3.4 (Un primo e una potenza di un primo a denominatore)**.**

1) Siano $p \neq q$ due primi dispari e $n \geq 2q$ un numero naturale. Si consideri il polinomio

$$h(x) = x^{p^{n-1}(p-1)} - r,$$

con r un primo tale che $r \equiv 1 \pmod{p^{n+1}}$ e $r > p^{n-1}(p-1) + n$. Siano poi $a_1, ..., a_n \in \mathbb{Z}$ tali che

(i) $a_i \equiv 0 \pmod{p}$ $\forall\, i \in \{1, ..., n\}$;

(ii) $\exists\, k \in \{0, ..., p-1\}$ tale che $a_i \not\equiv kp \pmod{p^2}$ $\forall\, i \in \{1, ..., n\}$;

(iii) $a_1, ..., a_q$ formano un sistema completo di residui modulo q, mentre $a_i \equiv 1 \pmod{q}$ $\forall\, i \in \{q+1, ..., n\}$;

(iv) $a_i \not\equiv 0 \pmod{l}$ $\forall\, i \in \{1, ..., n\}$, $\forall\, l$ primo tale che $l \leq p^{n-1}(p-1)+n$, $l \neq p, q$.

Il polinomio cercato risulta essere

$$f(x) = \frac{h(x) \prod_{i=1}^{n}(x - a_i)}{qp^n}.$$

2) Anche in questo caso i polinomi a numeratore di f sono irriducibili (h lo è per il criterio di Eisenstein) e primitivi, poiché monici. Bisogna ora mostrare che

$$qp^n = \mathsf{d}\left(h(x) \prod_{i=1}^{n}(x - a_i)\right)$$

Dimostrazione. Il fatto che $v_p\left(\mathsf{d}\left(h(x) \prod_{i=1}^{n}(x - a_i)\right)\right) = n$ si dimostra come quanto fatto nella costruzione (3.2) per l'espressione (3.1). L'unica cosa che bisogna provare è che $v_q\left(\mathsf{d}\left(h(x) \prod_{i=1}^{n}(x - a_i)\right)\right) = 1$. Di sicuro $q \mid h(z) \prod_{i=1}^{n}(z - a_i)$, infatti, $\forall\, z \in \mathbb{Z}$ $\exists!\, i_z \in \{1, ..., q\}$ tale che $z \equiv a_{i_z} \pmod{q}$ (per la terza ipotesi sugli a_i); al contrario $q^2 \nmid \mathsf{d}\left(h(x) \prod_{i=1}^{n}(x - a_i)\right)$ dato che, ad esempio, per $z = 0$ si ha che $q^2 \nmid (-1)^{n+1} r \prod_{i=1}^{n} a_i$ ($\exists!\, i \in \{1, ..., n\}$ tale che $a_i \equiv 0 \pmod{q}$ e $q \neq r$). □

Per quanto riguarda la condizione (2.4) del Lemma (2.3), si può procedere in modo analogo a quanto fatto nella costruzione (3.2) mostrando che se $\emptyset \neq I \subseteq \{1, ..., n\}$ e $\{1, ..., q\} \subseteq I$, allora $\mathsf{d}\left(\prod_{i \in I}(x - a_i)\right) = q$ (a_1,...,a_q

sono un sistema completo di residui modulo q), in caso contrario questo divisore fisso risulta essere 1. In seguito, basta far vedere che nel primo caso $\mathsf{d}\left(h(x)\prod_{i\notin I}(x-a_i)\right) \neq p^n$, mentre nel secondo caso questo risulta diverso da qp^n.

3) Per $k>1$, f^k ha una fattorizzazione in Int($\mathbb{Z}$) essenzialmente diversa da $f\cdots f$ (k volte) che risulta essere

$$f^k = \frac{h(x)\prod_{i=1}^{q}(x-a_i)^2\prod_{j=2q+1}^{n}(x-a_j)}{q^2p^n}\cdot \\ \cdot\frac{h(x)\prod_{i=q+1}^{2q}(x-a_i)^2\prod_{j=2q+1}^{n}(x-a_j)}{p^n}\cdot\underbrace{f\cdots f}_{k-2 \text{ volte}}.$$

Esempio 3.5. Siano $p=5$, $q=3$ e $n=6$. Il primo r deve essere preso in modo tale che $r\equiv 1 \pmod{5^7}$ e $r>5^5\cdot 4+6=12506$, dunque si può scegliere $r=937501$. Invece, a_1, a_2, a_3 devono essere un sistema completo di residui modulo 3 e multipli di 5, perciò si possono scegliere $a_1=5$, $a_2=15$, $a_3=25$, mentre come a_4, a_5, a_6 si possono prendere delle potenze di 5 (in questo modo non sono multipli di nessun primo diverso da 3 e 5 minore o uguale di 12506) che siano congrue a 1 modulo 3, ad esempio, $a_4=625$, $a_5=15625$, $a_6=390625$ (da notare che gli a_i non rappresentano tutte le classi divisibili per 5 modulo 25). Quindi

$$f(x)=\frac{(x^{12500}-937501)(x-5)(x-15)(x-25)(x-625)(x-15625)(x-390625)}{3\cdot 5^6}$$

e se $k>1$ una fattorizzazione in Int($\mathbb{Z}$) di f^k essenzialmente diversa da $f\cdots f$ (k volte) è

$$f^k=\frac{(x^{12500}-937501)(x-5)^2(x-15)^2(x-25)^2}{3^2\cdot 5^6}\cdot \\ \cdot\frac{(x^{12500}-937501)(x-625)^2(x-15625)^2(x-390625)^2}{5^6}\cdot\underbrace{f\cdots f}_{k-2 \text{ volte}}$$

Costruzione 3.6 (Due potenze di primi a denominatore)**.**

1) Dati $q<p$ due primi dispari e $1<m\leq n$ due numeri naturali, sia

$$t=\operatorname{lcm}(q^{m-1}(q-1),p^{n-1}(p-1))$$

e si consideri poi il polinomio

$$h(x)=x^t-r,$$

con r un primo e $r\equiv 1 \pmod{p^{n+1}q^{m+1}}$ e $r>t+n$. Siano poi $a_1,...,a_n\in\mathbb{Z}$ tali che

(i) $a_i \equiv 0 \pmod{p}\ \forall\, i \in \{1, ..., n\}$;

(ii) $\exists\, k \in \{0, ..., p-1\}$ tale che $a_i \not\equiv kp \pmod{p^2}\ \forall\, i \in \{1, ..., n\}$;

(iii) $a_j \equiv 0 \pmod{q}\ \forall\, j \in \{1, ..., m\}$, $a_k \equiv 1 \pmod{q}\ \forall\, k \in \{m+1, ..., n\}$;

(iv) $\exists\, h \in \{0, ..., q-1\}$ tale che $a_j \not\equiv hq \pmod{q^2}\ \forall\, j \in \{1, ..., m\}$;

(v) $a_i \not\equiv 0 \pmod{l}\ \forall\, i \in \{1, ..., n\}$, $\forall\, l$ primo tale che $l \leq t + n$, $l \neq p, q$.

Allora il polinomio cercato risulta essere

$$f(x) = \frac{h(x) \prod_{i=1}^{n} (x - a_i)}{p^n q^m}.$$

2) Nuovamente i polinomi al numeratore di f sono irriducibili in $\mathbb{Z}[x]$ (h lo è per il criterio di Eisenstein) e primitivi, poiché monici. A questo punto si può mostrare, come fatto nella costruzione (3.2) per l'espressione (3.1), che

$$p^n q^m = \mathsf{d}\left(h(x) \prod_{i=1}^{n} (x - a_i) \right),$$

osservando che $v_p(h(u)) \geq n\ \forall\, u \notin p\mathbb{Z}$ (essendo $t = kp^{n-1}(p-1)\ \exists\, k \in \mathbb{N}$ e $u \in (\mathbb{Z}/p^n\mathbb{Z})^*$, si ha che $ord(u) = p^{n-1}(p-1)$, ossia $u^{p^{n-1}(p-1)} \equiv 1 \pmod{p^n}$), $v_q(h(w)) \geq m\ \forall\, w \notin q\mathbb{Z}$, $\min_{u \in p\mathbb{Z}} \left(\prod_{i=1}^{n} (u - a_i) \right) = n$ e $\min_{w \in q\mathbb{Z}} \left(\prod_{i=1}^{n} (w - a_i) \right) = m$. Per quanto riguarda, invece, la condizione (2.4) del Lemma (2.3), il ragionamento è lo stesso usato nella costruzione (3.2).

3) Sia $k > 1$, f^k ammette delle fattorizzazioni in Int($\mathbb{Z}$) essenzialmente diverse da $f \cdots f$ (k volte): se tra $a_1, ..., a_m$ ci sono almeno due elementi diversi, ad esempio a_1 e a_2, si ha

$$\begin{aligned} f^k = & \frac{h(x)(x - a_1)^2 \prod_{i=3}^{n} (x - a_i)}{p^n q^m} \cdot \\ & \cdot \frac{h(x)(x - a_2)^2 \prod_{i=3}^{n} (x - a_i)}{p^n q^m} \cdot \underbrace{f \cdots f}_{k-2 \text{ volte}}, \end{aligned}$$

mentre se tra $a_{m+1}, ..., a_n$ ce ne sono almeno due di diversi, ad esempio a_{m+1} e a_{m+2}, allora

$$\begin{aligned} f^k = & \frac{h(x)(x - a_{m+2})^2 \prod_{i \neq m+1, m+2} (x - a_i)}{p^n q^m} \cdot \\ & \cdot \frac{h(x)(x - a_{m+2}) \prod_{i \neq m+1, m+2} (x - a_i)}{p^n q^m} \cdot \underbrace{f \cdots f}_{k-2 \text{ volte}}. \end{aligned}$$

Esempio 3.7. Siano $q = 3$, $p = 5$, $m = 2$ e $n = 4$, dunque $t = lcm(6, 500) = 1500$. Si scelga, poi, r primo tale che $r \equiv 1 \pmod{5^5 3^3}$ e $r > 1500+4 = 1504$, ad esempio, sia $r = 506251$. Si possono scegliere $a_1 = 15$, $a_2 = 45$, $a_3 = 25$, $a_4 = 625$, infatti, a_1 e a_2 sono multipli di 3 e di 5 (e non rappresentano tutte le classi divisibili per 3 modulo 9), mentre a_3 e a_4 sono potenze di 5 congrue a 1 modulo 3 (da notare che gli a_i non rappresentano tutte le classi divisibili per 5 modulo 25). Dunque

$$f(x) = \frac{(x^{1500} - 506251)(x-15)(x-45)(x-25)(x-625)}{3^2 5^4} \text{ e,}$$

alcune fattorizzazioni in Int($\mathbb{Z}$) di f^k con $k > 1$ essenzialmente diverse da $f \cdots f$ (k volte) sono

$$\begin{aligned} f^k =& \frac{(x^{1500} - 506251)(x-15)^2(x-25)(x-625)}{3^2 5^4} \cdot \\ & \cdot \frac{(x^{300} - 506251)(x-45)^2(x-25)(x-625)}{3^2 5^4} \cdot \underbrace{f \cdots f}_{k-2 \text{ volte}} \text{ e} \\ f^k =& \frac{(x^{1500} - 506251)(x-15)(x-45)(x-25)^2}{3^2 5^4} \cdot \\ & \cdot \frac{(x^{1500} - 506251)(x-15)(x-45)(x-625)^2}{3^2 5^4} \cdot \underbrace{f \cdots f}_{k-2 \text{ volte}} \end{aligned}$$

Negli esempi che seguono verrà costruito un polinomio $f \in$ Int($\mathbb{Z}$) per cui solo alcune potenze hanno fattorizzazioni essenzialmente diverse dal prodotto di copie di f e, in particolare, risultano avere lunghezze differenti. La prima costruzione, come fatto in precedenza, può essere poi estesa al caso di polinomi che presentano potenze di più di un primo a denominatore.

Costruzione 3.8 (Potenza di un solo primo a denominatore)**.**

1) Sia p un primo dispari e $n > m$ due numeri naturali. Si definiscano i polinomi

$$\begin{aligned} c(x) &= x^{\frac{p^{n-1}(p-1)}{2}} - q \text{ e} \\ d(x) &= x^{\frac{p^{n-1}(p-1)}{2}} - r, \end{aligned}$$

dove q e r sono due primi, $q \equiv 1 \pmod{p^{n+1}}$, $r \equiv -1 \pmod{p^{n+1}}$ e $q, r > p^{n-1}(p-1) + m$. Siano poi $a_1, ..., a_m \in \mathbb{Z}$ tali che

(i) $a_i \equiv 0 \pmod{p}$ $\forall\, i \in \{1, ..., m\}$;

(ii) $\exists\, k \in \{0, ..., p-1\}$ tale che $a_i \not\equiv kp \pmod{p^2}$ $\forall\, i \in \{1, ..., m\}$;

(iii) $a_i \not\equiv 0 \pmod{l}$ $\forall\, i \in \{1, ..., m\}$, $\forall\, l$ primo tale che $l \leq p^{n-1}(p-1)+m$, $l \neq p$.

Allora il polinomio cercato risulta essere

$$f(x) = \frac{c(x)d(x)\prod_{i=1}^{m}(x-a_i)}{p^m}.$$

2) Tutti i polinomi al numeratore di f sono irriducibili in $\mathbb{Z}[x]$ (c e d lo sono per il criterio di Eisenstein) e primitivi, poiché monici. Bisogna mostrare che

$$p^m = \mathsf{d}\left(c(x)d(x)\prod_{i=1}^{m}(x-a_i)\right);$$

l'unica differenza rispetto alla dimostrazione nella costruzione (3.2) dell'espressione (3.1) sta nel fatto che bisogna provare che

$$\min_{u\notin p\mathbb{Z}} v_p(c(u)d(u)) = n \tag{3.2}$$

(anche se in realtà per ciò che segue basta sapere che $v_p(c(u)d(u)) \geq n$ $\forall\, u \notin p\mathbb{Z}$).

Dimostrazione. Sia $u \notin p\mathbb{Z}$, allora $v_p(c(u)d(u)) \geq n$: $v_p(c(u)) \geq n \iff u$ è un quadrato modulo p^n ($u^{\frac{p^{n-1}(p-1)}{2}} \equiv q \equiv 1 \pmod{p^n} \iff u \in ker\psi$ $\iff u$ è un quadrato modulo p^n (Lemma (3.1))); al contrario, $v_p(d(u)) \geq n \iff u$ non è un quadrato modulo p^n. In particolare, sia u un generatore del gruppo $(\mathbb{Z}/p^{n+1}\mathbb{Z})^*$ e perciò anche un generatore di $(\mathbb{Z}/p^n\mathbb{Z})^*$; quest'ultimo fatto permette di dire che $v_p(d(u)) \geq n$ ($u^{\frac{p^{n-1}(p-1)}{2}} \not\equiv 1 \pmod{p^n}$ perché l'ordine di u in $(\mathbb{Z}/p^n\mathbb{Z})^*$ è $\varphi(p^n) = p^{n-1}(p-1) > \frac{p^{n-1}(p-1)}{2}$), ma, in realtà, vale l'uguaglianza: se fosse $u^{\frac{p^{n-1}(p-1)}{2}} \equiv r \equiv -1 \pmod{p^{n+1}}$ e quindi $u^{p^{n-1}(p-1)} \equiv 1 \pmod{p^{n+1}}$, questo andrebbe contro il fatto che l'ordine di u in $(\mathbb{Z}/p^{n+1}\mathbb{Z})^*$ è $\varphi(p^{n+1}) = p^n(p-1)$. Dal momento che, invece, $v_p(c(u)) = 0$ ($u^{\frac{p^{n-1}(p-1)}{2}} \equiv -1 \not\equiv 1 \pmod{p}$), si ha che $v_p(c(u)d(u)) = n$. □

Per quanto riguarda, invece, la condizione (2.4) del Lemma (2.3) che permette di concludere l'irriducibilità di f si può ragionare nello stesso modo utilizzato nella costruzione (3.2).

3) La potenza f^n ammette una fattorizzazione in Int($\mathbb{Z}$) essenzialmente diversa da $f \cdots f$ (n volte) che risulta essere

$$f^n = \prod_{i=1}^{m} \frac{c(x)d(x)(x-a_i)^n}{p^n} \cdot c(x)^{n-m}d(x)^{n-m}$$

di lunghezza $2n - m > n$ (da notare che $c(x)$ e $d(x)$ sono irriducibili in Int($\mathbb{Z}$) essendo irriducibili in $\mathbb{Z}[x]$ e $\mathsf{d}(c) = 1 = \mathsf{d}(d)$ (Lemma (1.18))).

Il motivo per cui f^n ha due fattorizzazioni essenzialmente diverse di lunghezza differente è dovuto al fatto di aver scelto i due polinomi $c(x)$ e $d(x)$ anzichè il solo $h(x)$.

Esempio 3.9. Siano $p = 3$ e $3 = n > m = 2$. Si scelgano poi i primi q e r in modo che $q \equiv 1 \pmod{3^4}$ e $r \equiv -1 \pmod{3^4}$ e $q, r > 3^2 \cdot 2 + 2 = 20$, basta prendere $q = 163$ e $r = 647$. Invece, $a_1 = 3$ e $a_2 = 9$ soddisfano alle ipotesi, infatti sono potenze di 3 e non rappresentano tutte le classi divisibili per 3 modulo 9. Dunque

$$f(x) = \frac{(x^9 - 163)(x^9 - 647)(x - 3)(x - 9)}{3^2},$$

mentre una fattorizzazione di f^3 essenzialmente diversa da $f \cdot f \cdot f$ risulta essere

$$\begin{aligned} f^3 =& \frac{(x^9 - 163)(x^9 - 647)(x - 3)^3}{3^3} \cdot \\ & \cdot \frac{(x^9 - 163)(x^9 - 647)(x - 9)^3}{3^3} (x^9 - 163)(x^9 - 647). \end{aligned}$$

Costruzione 3.10.

1) Sia $p > 3$ un primo. Siano $a_1, ..., a_p$ un sistema completo di residui modulo p che non contenga un sistema completo di residui modulo q $\forall\, q < p$ primo (esiste per il Lemma (2.21)). Si definiscano ora i polinomi

$$\begin{aligned} g_1(x) &= (x - a_2)^2 (x - a_3)^2 \prod_{i=4}^{p} (x - a_i), \\ g_2(x) &= (x - a_1)^2 (x - a_3)^2 \prod_{i=4}^{p} (x - a_i) \text{ e} \\ g_3(x) &= (x - a_1)^2 (x - a_2)^2 \prod_{i=1}^{4} (x - a_i) \end{aligned}$$

monici e non costanti. Per il Lemma (2.22), esistono dei polinomi G_i con $i \in \{1, 2, 3\}$ monici, diversi tra loro, irriducibili in $\mathbb{Z}[x]$ e con $deg(g_i) = deg(G_i)$ tali che il divisore fisso di un qualsiasi prodotto dei g_i è uguale al divisore fisso dello stesso prodotto in cui i g_i sono sostituiti dai G_i. Il polinomio cercato risulta essere

$$f(x) = \frac{G_1 G_2 G_3}{p^3}.$$

2) I polinomi al numeratore di f sono irriducibili in $\mathbb{Z}[x]$ e primitivi, poiché monici, per come sono stati costruiti. Bisogna mostrare che

$$p^3 = \mathsf{d}\left(G_1 G_2 G_3\right) = \mathsf{d}\left(g_1 g_2 g_3\right).$$

Per come sono stati definiti i g_i si ha che

$$g_1(x)g_2(x)g_3(x) = (x-a_1)^4(x-a_2)^4(x-a_3)^4\prod_{i=4}^{p}(x-a_i)^3;$$

se $z \in \mathbb{Z}$, $\exists!\, i_z \in \{1,...,p\}$ tale che $z \equiv a_{i_z} \pmod p$, dunque se $i_z \in \{1,2,3\}$, $v_p\left(g_1(z)g_2(z)g_3(z)\right) = 4$, mentre, se $i_z \in \{4,...,p\}$, questa valutazione vale 3. Allora $v_p\left(\mathsf{d}\left(g_1g_2g_3\right)\right) = 3$. Se, invece, $q \neq p$ è un primo, esisterà sempre $z \in \mathbb{Z}$ tale che $z \not\equiv a_i \pmod q$ $\forall\, i \in \{1,...,p\}$, dunque $q \nmid \mathsf{d}\left(g_1g_2g_3\right)$. A questo punto bisogna mostrare che vale la condizione (2.4) del Lemma (2.3): sicuramente $\mathsf{d}(G_i) = \mathsf{d}(g_i) = 1$ $\forall\, i \in \{1,2,3\}$ (il fattore $(x-a_i)$ non compare in g_i e $a_1,...,a_p$ sono un sistema completo di residui modulo p), inoltre, $\forall\, i \neq j$ $\mathsf{d}(G_iG_j) = \mathsf{d}(g_ig_j) = p^2$, infatti

$$g_i(x)g_j(x) = (x-a_i)^2(x-a_j)^2(x-a_k)^4\prod_{h=4}^{p}(x-a_h)^2,$$

dove $k \in \{1,2,3\}$, $k \neq i,j$.

3) In questo caso si ha che f^2 ammette una fattorizzazione in Int($\mathbb{Z}$) essenzialmente diversa da $f \cdot f$ che risulta essere

$$f^2 = \frac{G_1G_2}{p^2} \cdot \frac{G_1G_3}{p^2} \cdot \frac{G_2G_3}{p^2}$$

di lunghezza 3.

3.2 Generalizzazioni

In questa sezione, generalizzando le costruzioni della sezione precedente, verranno descritte delle condizioni sufficienti affinchè un polinomio $f \in \mathrm{Int}(\mathbb{Z})$ irriducibile sia non assolutamente irriducibile. Spesso, questo polinomio irriducibile f sarà del tipo

$$f(x) = \frac{\prod_{i\in I} g_i(x)}{b}, \tag{3.3}$$

dove $I \neq \emptyset$ è un insieme finito, $b > 1$ è un numero naturale e $g_i \in \mathbb{Z}[x]$ sono primitivi e irriducibili $\forall\, i \in I$.

Prima di tutto, però, sono necessarie alcune definizioni:

Definizione 3.11. Sia $f \in \mathrm{Int}(\mathbb{Z})$ irriducibile espresso nella forma (3.3). Due sottoinsiemi $\emptyset \neq J_1, J_2 \subsetneq I$ si dicono *intercambiabili* se $J_1 \cap J_2 = \emptyset$ e

$$\mathsf{d}\left(\prod_{i\in J_1} g_i(x)\prod_{j\in I\setminus J_2} g_j(x)\right) = \mathsf{d}\left(\prod_{i\in J_2} g_i(x)\prod_{j\in I\setminus J_1} g_j(x)\right) = b.$$

I due insiemi si dicono, invece, *a elementi disgiunti* se

$$\{g_i |\, i \in J_1\} \cap \{g_i |\, i \in J_2\} = \emptyset.$$

Definizione 3.12. Sia $I \neq \emptyset$ un insieme finito e $f_i \in \mathbb{Z}[x]$ polinomi primitivi e irriducibili $\forall\, i \in I$. Sia $p \mid \mathsf{d}\left(\prod_{i\in I} f_i(x)\right)$, f_k con $k \in I$ si dice *indispensabile per* p se $p \nmid \mathsf{d}\left(\prod_{\substack{i\in I\\ i\neq k}} f_i(x)\right)$, ossia se $\exists\, z \in \mathbb{Z}$ tale che $v_p(f_k(z)) > 0$, ma $v_p(f_i(z)) = 0\ \forall\, i \neq k$.

Lemma 3.13. *Sia $f \in \mathrm{Int}(\mathbb{Z})$ irriducibile espresso nella forma (3.3). Se esistono due sottoinsiemi $\emptyset \neq J_1, J_2 \subsetneq I$ intercambiabili e a elementi disgiunti, allora f non è assolutamente irriducibile.*

Dimostrazione. Per ogni $k > 1$ si ha

$$f^k = \frac{\prod_{i\in J_1} g_i(x) \prod_{j\in I\setminus J_2} g_j(x)}{b} \cdot \frac{\prod_{i\in J_2} g_i(x) \prod_{j\in I\setminus J_1} g_j(x)}{b} \cdot \underbrace{f \cdots f}_{k-2 \text{ volte}}$$

e questa risulta essere una fattorizzazione in irriducibili in Int($\mathbb{Z}$) di f^k essenzialmente diversa da $f \cdots f$ (k volte). □

Esempio 3.14. Il polinomio f, irriducibile in Int($\mathbb{Z}$), costruito nell'esempio (3.2) soddisfa alle ipotesi di questo Lemma, infatti, posto $g_0(x) = h(x)$ e $g_i(x) = x - a_i\ \forall\, i \in \{1, ..., p\}$, si ha che $I = \{0, ..., p\}$ e i sottoinsiemi di I non vuoti $J_1 = \{1\}$ e $J_2 = \{2\}$ sono a elementi disgiunti e intercambiabili, da questo segue, come si è visto, che f non è assolutamente irriducibile.

Lemma 3.15. *Sia $f \in \mathrm{Int}(\mathbb{Z})$ irriducibile espresso nella forma (3.3), ma con $b = p$ primo. Allora non esistono sottoinsiemi di I intercambiabili.*

Dimostrazione. Si supponga per assurdo che esistano $\emptyset \neq J_1, J_2 \subsetneq I$ intercambiabili. Siccome f è irriducibile in Int($\mathbb{Z}$), allora $p = \mathsf{d}\left(\prod_{i\in I} g_i(x)\right)$ e, soprattutto, $\forall\, \emptyset \neq J \subsetneq I\ \ \mathsf{d}\left(\prod_{j\in J} g_j(x)\right) \neq p$, ossia ogni g_i con $i \in I$ è indispensabile per p. Da questo segue che $g_i \neq g_j\ \forall\, i \neq j$ e, quindi, essendo $J_1 \cap J_2 = \emptyset$, si ha che questi due sottoinsiemi sono anche a elementi disgiunti. Sia ora $k \in J_1$ e $z_k \in \mathbb{Z}$ tale che $v_p(g_k(z_k)) > 0$ mentre $v_p(g_i(z_k)) = 0\ \forall\, i \neq k$ (g_k è indispensabile per p), dunque

$$v_p\left(\prod_{j\in J_2} g_j(z_k) \prod_{i\in I\setminus J_1} g_i(z_k)\right) = 0$$

(g_k non compare nel prodotto). Perciò $p \nmid \mathsf{d}\left(\prod_{j\in J_2} g_j(x) \prod_{i\in I\setminus J_1} g_i(x)\right)$, contro la definizione di sottoinsiemi di I intercambiabili, ossia

$$\mathsf{d}\left(\prod_{j\in J_2} g_j(x) \prod_{i\in I\setminus J_1} g_i(x)\right) = \mathsf{d}\left(\prod_{j\in J_1} g_j(x) \prod_{i\in I\setminus J_2} g_i(x)\right) = p$$

□

Lemma 3.16. *Sia $f \in \mathrm{Int}(\mathbb{Z})$ irriducibile espresso nella forma (3.3) e sia $\mathbb{P}$ l'insieme di tutti i primi che dividono b, in modo che $b = \prod_{p\in\mathbb{P}} p^{e_p}$ con $e_p \in \mathbb{N}$. Se esiste $\emptyset \neq J \subsetneqq I$ tale che $\forall\, p \in \mathbb{P}$ e $z \in S_p$ si ha che*

$$v_p\left(\prod_{j\in J} g_j(z)\right) > e_p, \tag{3.4}$$

dove

$$S_p = \{z \in \mathbb{Z} |\ \prod_{j\in J} g_j(z) \equiv 0 \ \ (mod\ \ p)\},$$

allora f non è assolutamente irriducibile.

Dimostrazione. Sia $n = \max\{e_p |\, p \in \mathbb{P}\}$ e $k = n + 1$, allora da

$$f^k = \frac{\left(\prod_{j\in J} g_j(x)\right)^n \left(\prod_{i\in I\setminus J} g_i(x)\right)^k}{b^k} \cdot \prod_{j\in J} g_j(x)$$

si può ottenere una fattorizzazione in Int(ℤ) di f^k essenzialmente diversa da $f \cdots f$ (k volte): essendo Int(ℤ) un dominio atomico, basta mostrare che il primo fattore è un polinomio a valori interi. Per fare questo, bisogna notare che $\forall\, z \in \mathbb{Z}$, $p \in \mathbb{P}$

$$v_p\left(\left(\prod_{j\in J} g_j(z)\right)^n \left(\prod_{i\in I\setminus J} g_i(z)\right)^k\right) =$$
$$= n\, v_p\left(\prod_{j\in J} g_j(z)\right) + k\, v_p\left(\prod_{i\in I\setminus J} g_i(z)\right) \geq e_p k,$$

dove la prima uguaglianza segue dalle proprietà della valutazione p-adica. Infatti, se $z \in S_p$, dalla condizione (3.4) si ha che

$$v_p\left(\prod_{j\in J} g_j(z)\right) = e_p + t \ \text{ con } \ t \geq 1,$$

quindi

$$n\, v_p\left(\prod_{j\in J} g_j(z)\right) + k\, v_p\left(\prod_{i\in I\setminus J} g_i(z)\right) \geq n\, v_p\left(\prod_{j\in J} g_j(z)\right) =$$
$$= n(e_p + t) \geq e_p(n+1) = e_p k,$$

essendo $t \geq 1$ e $n \geq e_p \ \forall p \in \mathbb{P}$. Dal momento che f è un polinomio a valori interi, $\mathsf{d}\left(\prod_{i\in I} g_i(x)\right) = b$, cioè $\forall p \in \mathbb{P}$, $z \in \mathbb{Z}$ $v_p\left(\prod_{i\in I} g_i(z)\right) = v_p\left(\prod_{j\in J} g_j(z)\right) + v_p\left(\prod_{i\in I\setminus J} g_i(z)\right) \geq e_p$, dunque se $z \notin S_p$, ossia z è tale che $v_p\left(\prod_{j\in J} g_j(z)\right) = 0$, si ha che $v_p\left(\prod_{i\in I\setminus J} g_i(z)\right) \geq e_p$. Grazie a questa osservazione si può concludere che per $z \notin S_p$

$$n\, v_p\left(\prod_{j\in J} g_j(z)\right) + k\, v_p\left(\prod_{i\in I\setminus J} g_i(z)\right) = k\, v_p\left(\prod_{i\in I\setminus J} g_i(z)\right) \geq e_p k.$$

□

Esempio 3.17. Il polinomio f della costruzione (3.8) soddisfa a tutte le ipotesi del Lemma (3.16): come è stato mostrato, è irriducibile in Int(ℤ) ed è espresso nella forma (3.3), infatti, ponendo $g_0(x) = c(x)$, $g_1(x) = d(x)$ e $g_i(x) = x - a_{i-1}\ \forall i \in \{2, ..., m+1\}$, si ha che $I = \{0, ..., m+1\}$, mentre l'insieme J risulta essere $J = \{0, 1\}$. Infatti, si ha che

$$S_p = \{z \in \mathbb{Z} |\, z \notin p\mathbb{Z}\},$$

inoltre, per $z \in S_p$,

$$v_p(c(z)d(z)) \geq \min_{u\notin p\mathbb{Z}} v_p(c(u)d(u)) = n > m.$$

Dunque, come si è visto, f non è assolutamente irriducibile.

Lemma 3.18. *Sia $f \in \mathrm{Int}(\mathbb{Z})$ irriducibile espresso nella forma (3.3) con $b = p^n$, p primo e $n > 1$ un numero naturale. Sia poi $\mathbb{Z} = S_1 \sqcup S_2$ una partizione di $\mathbb{Z}$ con S_1 e S_2 non vuoti. Se esiste $\emptyset \neq J \subsetneq I$ tale che*

$$v_p\left(\gcd\left(\prod_{j\in J} g_j(s) |\, s \in S_1\right)\right) > n, \tag{3.5}$$

$$v_p\left(\gcd\left(\prod_{j\in J} g_j(s) |\, s \in S_2\right)\right) = e \ \text{ con } \ 1 \leq e < n \ \text{ e} \tag{3.6}$$

$$v_p\left(\gcd\left(\prod_{i\in I\setminus J} g_i(s) |\, s \in S_2\right)\right) \geq n - e, \tag{3.7}$$

allora f non è assolutamente irriducibile.

Dimostrazione. Chiamata m la quantità (3.5) e posto $k = m - e$, da

$$f^k = \frac{\left(\prod_{j\in J} g_j(x)\right)^{n-e}\left(\prod_{i\in I\setminus J} g_i(x)\right)^k}{p^{(n-e)m}} \cdot \left(\frac{\prod_{j\in J} g_j(x)}{p^e}\right)^{m-n} \tag{3.8}$$

si può ottenere una fattorizzazione in Int($\mathbb{Z}$) di f^k essenzialmente diversa da $f \cdots f$ (k volte). Per prima cosa va notato che gli esponenti che compaiono in (3.8) sono corretti, infatti, $(n-e)+(m-n) = k$ e $(n-e)m+e(m-n) = kn$. A questo punto, dal momento che Int($\mathbb{Z}$) è un dominio atomico, basta mostrare che tutti i fattori in (3.8) sono polinomi a valori interi. Sicuramente, il fattore $\frac{\prod_{j\in J} g_j(x)}{p^e} \in \mathrm{Int}(\mathbb{Z})$, infatti per le ipotesi (3.5) e (3.6) si ha che $\mathsf{d}\left(\prod_{j\in J} g_j(x)\right) = p^e$. Inoltre, nessun divisore irriducibile di questo fattore può essere associato a f. Per quanto riguarda, invece, il primo fattore, ossia $\frac{\left(\prod_{j\in J} g_j(x)\right)^{n-e}\left(\prod_{i\in I\setminus J} g_i(x)\right)^k}{p^{(n-e)m}}$, si può facilmente mostrare che è un polinomio a valori interi: sia $s \in S_1$, allora, per la definizione di m,

$$(n-e)\, v_p\left(\prod_{j\in J} g_j(s)\right) + k\, v_p\left(\prod_{i\in I\setminus J} g_i(s)\right) \geq (n-e)m;$$

sia $s \in S_2$, per le condizioni (3.6) e (3.7) si ha

$$\begin{aligned}&(n-e)\, v_p\left(\prod_{j\in J} g_j(s)\right) + k\, v_p\left(\prod_{i\in I\setminus J} g_i(s)\right) \geq \\ &\geq (n-e)e + k(n-e) = (n-e)m.\end{aligned}$$

□

Esempio 3.19. Il Lemma (3.18) può essere applicato al polinomio f della costruzione (3.10): è stato mostrato che f è un polinomio irriducibile in Int($\mathbb{Z}$) ed è espresso nella forma (3.3) con $b = p^3$ e $I = \{1, 2, 3\}$. Preso un qualsiasi $J \subseteq I$ con due elementi, $J = \{i, j\}$, detto k l'elemento di $I \setminus J$, si ha che

$$v_p(\gcd(G_i(z)G_j(z)|\, z \equiv a_k \pmod p)) = 4 > 3 = n,$$

dunque $S_1 = \{z \in \mathbb{Z}|\, z \equiv a_k \pmod p\}$ e $S_2 = \mathbb{Z} \setminus S_1$ e anche le condizioni (3.6) e (3.7) risultano essere soddisfatte dal momento che

$$\begin{aligned}&v_p(\gcd(G_i(z)G_j(z)|\, z \not\equiv a_k \pmod p)) = 2 = e < 3 = n \text{ e} \\ &v_p(\gcd(G_k(z)|\, z \not\equiv a_k \pmod p)) = 2 \geq n - e = 3 - 2 = 1,\end{aligned}$$

perciò, come si è visto, f non è assolutamente irriducibile.

Capitolo 4

Sottomonoidi di Krull di Int($\mathbb{Z}$)

Obiettivo di questo capitolo è definire dei sottomonoidi di Int($\mathbb{Z}$) che si dimostreranno poi essere dei monoidi di Krull. La definizione di questi ultimi verrà presentata dopo aver ricordato alcune nozioni riguardanti in generale i monoidi:

Definizione 4.1. Un *monoide* $(M, \cdot)$ è un insieme M dotato di un'operazione $\cdot$ associativa, chiuso rispetto a questa e con un elemento neutro 1_M (in questo caso si è usata la notazione moltiplicativa); se l'operazione è anche commutativa, allora M si dice monoide *commutativo*.
Un sottoinsieme $N \subseteq M$ è un *sottomonoide* se è chiuso rispetto all'operazione di M e $1_M \in N$.
Dato un sottoinsieme finito $X = \{a_1, ..., a_n\} \subseteq M$ con M monoide commutativo, il *sottomonoide di M generato da X* è costituito dagli elementi

$$[X] = \left\{ \prod_{i=1}^{n} a_i^{e_i} | \, e_i \geq 0 \right\}.$$

Un monoide M si dice *cancellativo* se da $ab = ac$ con $a, b, c \in M$ segue che $b = c$.

Esempio 4.2. Sia $F \subseteq \mathbb{Q}[x]$ finito costituito da polinomi irriducibili e a due a due non associati, $F = \{q_1, ..., q_n\}$. Il sottomonoide di $\mathbb{Q}[x]$ generato da F e dagli elementi non nulli di $\mathbb{Q}$ è formato da tutti i polinomi in $\mathbb{Q}[x]$ i cui fattori irriducibili sono tutti in F, infatti

$$[F] = \left\{ c \prod_{i=1}^{n} q_i^{e_i} | \, c \in \mathbb{Q}^*, e_i \geq 0 \ \ \forall \, i \in \{1, ..., n\} \right\}.$$

Definizione 4.3. Dati due monoidi $(M, \cdot)$ e $(N, *)$, una mappa $\varphi : M \longrightarrow N$ si dice *omomorfismo di monoidi* se $\varphi(1_M) = 1_N$ e $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$

$\forall\, a, b \in M$ (da questa proprietà segue che se $a \mid b$ in M, allora $\varphi(a) \mid \varphi(b)$ in N).
Un omomorfismo di monoidi $\varphi : M \longrightarrow N$ si dice *omomorfismo di divisione* se $\forall\, a, b \in M$ $\varphi(a) \mid \varphi(b)$ in N implica che $a \mid b$ in M.
Una *teoria di divisione* è, invece, un omomorfismo di divisione $\varphi : M \longrightarrow N$ dove N è un monoide libero commutativo e tale che $\forall\, b \in N\ \exists\, a_1, ..., a_n \in M$ tali che $b = \gcd(\varphi(a_i) | \, i \in \{1, ..., n\})$, ossia $b \mid \varphi(a_i)$ $\forall\, i \in \{1, ..., n\}$ e se $c \mid \varphi(a_i)$ $\forall\, i \in \{1, ..., n\}$, allora $c \mid b$.

Definizione 4.4. Un monoide M viene detto *monoide di Krull* se è un monoide commutativo e cancellativo che possiede una teoria di divisione.

Definizione 4.5. Un dominio D viene detto *dominio di Krull* se, indicato con $\mathrm{Spec}^1(D)$ l'nsieme degli ideali primi di altezza 1 di D, valgono le seguenti condizioni:

(i) Se $P \in \mathrm{Spec}^1(D)$, la localizzazione D_P di D rispetto a P è DVR;

(ii) $D = \cap_{P \in \mathrm{Spec}^1(D)} D_P$;

(iii) Ogni elemento non nullo $x \in D$ appartiene solo a un numero finito di ideali in $\mathrm{Spec}^1(D)$.

Un importante Teorema, la cui dimostrazione si può trovare in [13], lega domini e monoidi di Krull:

Teorema 4.6. *Un dominio D è di Krull se e solo se $D \setminus \{0\}$ è un monoide di Krull.*

Altre definizioni utili riguardano, invece, l'anello dei polinomi a valori interi:

Definizione 4.7. Siano D un dominio, K il suo campo delle frazioni e $S \subseteq D$. Dato $f \in \mathrm{Int}(S, D)$, si definisce il sottomonoide di $\mathrm{Int}(S, D)$ (visto come monoide moltiplicativo)

$$[[f]] = \{g \in \mathrm{Int}(S, D) | f^n = g \cdot h, \exists\, n \in \mathbb{N}, h \in \mathrm{Int}(S, D)\}.$$

Osservazione 4.8. Il sottomonoide $[[f]]$, per come è stato definito, risulta essere chiuso per divisione: se $g \in [[f]]$, ossia $g \mid f^n$ $\exists\, n \in \mathbb{N}$, e $h \in \mathrm{Int}(S, D)$ è tale che $h \mid g$, allora $h \mid f^n$, cioè $h \in [[f]]$ (tutte le divisioni si intendono in $\mathrm{Int}(S, D)$).

Definizione 4.9. Sia D un dominio, K il suo campo delle frazioni e $T \subseteq K$. Si dice *chiusura polinomiale di T* l'insieme

$$\overline{T} = \{x \in K | \, \forall\, f \in \mathrm{Int}(T, D), f(x) \in D\},$$

che risulta essere il più grande sottoinsieme di K contenente T tale che

$$\mathrm{Int}(T, D) = \mathrm{Int}(\overline{T}, D).$$

Nei risultati seguenti sarà utile una generalizzazione di questa nozione, ossia quella di *chiusura polinomiale di T relativa a $\mathcal{F}$*, dove $\mathcal{F} \subseteq K[x]$ è un sottoinsieme, che risulta essere

$$C_{\mathcal{F}}(T) = \{x \in K | \forall\, f \in \mathcal{F} \cap \mathrm{Int}(T, D), f(x) \in D\}.$$

Se $T \subseteq S \subseteq K$ e $S \subseteq C_{\mathcal{F}}(T)$, allora T si dice *D-polinomialmente denso in S relativamente a $\mathcal{F}$* e, in questo caso, si ha

$$\mathrm{Int}(T, D) \cap \mathcal{F} = \mathrm{Int}(S, D) \cap \mathcal{F}.$$

I risultati di questa sezione, che qui saranno presentati nel caso particolare dell'anello Int($\mathbb{Z}$), sono trattati nel caso di un generico dominio di Krull D in [9].

Per prima cosa, bisogna fare alcune osservazioni sulla valutazione p-adica definita in (2.6). Questa mappa risulta essere una valutazione discreta con anello di valutazione corrispondente

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} |\, v_p(x) \geq 0\},$$

cioè la localizzazione di $\mathbb{Z}$ rispetto all'ideale primo $p\mathbb{Z}$; in particolare, $\mathbb{Z}_{(p)}$ è un dominio di valutazione discreta (DVR) (dunque PID, che implica UFD) che ha come unico ideale massimale $p\mathbb{Z}_{(p)}$.

Osservazione 4.10. Dalle proprietà della valutazione p-adica, si ha che se $a, b \in \mathbb{Q}$ sono tali che $v_p(a) \neq v_p(b)$, allora

$$v_p(a + b) = \min\{v_p(a), v_p(b)\}.$$

Osservazione 4.11. Sia $S \subseteq \mathbb{Z}_{(p)}$ e $f \in \mathrm{Int}(S, \mathbb{Z}_{(p)})$. Allora

$$\min_{s \in S} v_p(f(s)) = v_p(\mathtt{d}_S(f)).$$

La valutazione v_p, come mostrato in [12], induce su $\mathbb{Q}$ una topologia, infatti, si può per prima cosa definire

$$|x|_p = \mathrm{e}^{-v_p(x)}$$

$\forall\, x \in \mathbb{Q}$ e, a partire da questo, la metrica

$$d_p(x, y) = |x - y|_p = \mathrm{e}^{-v_p(x-y)}$$

$\forall\, x, y \in \mathbb{Q}$, che induce la topologia p-adica su $\mathbb{Q}$ le cui palle sono sottoinsiemi di $\mathbb{Q}$ del tipo

$$B(x, r) = \{y \in \mathbb{Q} |\, v_p(x - y) \geq r\},$$

per $x \in \mathbb{Q}$ e $r \in \mathbb{Z}, r \geq 0$.

Definizione 4.12. Sia $S \subseteq \mathbb{Q}$. Un elemento $x \in S$ si dice punto isolato di S nella topologia p-adica se $\exists\, r \in \mathbb{Z}, r \geq 0$ tale che $B(x,r) \cap S = \{x\}$.

Notazione 4.1. In tutti i risultati che seguono $p \in \mathbb{Z}$ sarà un primo, $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ e v_p la valutazione discreta associata a $\mathbb{Z}_{(p)}$ appena definita. Inoltre, dato D un UFD, verrà sempre indicato con H un sottoinsieme finito non vuoto di $D[x]$ contenente polinomi irriducibili e a due a due non associati, mentre $\mathcal{H}$ sarà il sottomonoide di $D[x]$ generato da H e dagli elementi invertibili di D. Si utilizzerà, invece, la notazione $\mathcal{H}_f$ per indicare il sottomonoide di $D[x]$ generato dagli elementi invertibili di D e dai fattori irriducibili e a due a due non associati di $f \in D[x]$ (l'insieme costituito da questi fattori si indicherà con H_f).

Il primo lemma permette di caratterizzare i sottoinsiemi polinomialmente densi.

Lemma 4.13. *Siano $T \subseteq S \subseteq \mathbb{Q}$ e $\mathcal{F} \subseteq \mathbb{Q}[x]$ sottoinsieme. Se $\forall\, f \in \mathcal{F}$*

$$\min_{t\in T} v_p(f(t)) = \min_{s\in S} v_p(f(s)),$$

allora T è $\mathbb{Z}_{(p)}$-polinomialmente denso in S relativamente a $\mathcal{F}$. Se $\mathcal{F}$ è chiuso per moltiplicazione per elementi non nulli di $\mathbb{Q}$, le due affermazioni sono equivalenti.

Dimostrazione. ($\Rightarrow$) Bisogna mostrare che $S \subseteq C_{\mathcal{F}}(T)$. Sia dunque $f \in \mathcal{F} \cap \mathrm{Int}(T, \mathbb{Z}_{(p)})$; dal momento che $f(t) \in \mathbb{Z}_{(p)}\ \forall\, t \in T$, allora $v_p(f(t)) \geq 0$ $\forall\, t \in T$, da cui segue che $\min_{s\in S} v_p(f(s)) = \min_{t\in T} v_p(f(t)) \geq 0$. Quindi, $f(s) \in \mathbb{Z}_{(p)}\ \forall\, s \in S$.
($\Leftarrow$) Per questa implicazione si supponga che $\mathcal{F}$ sia chiuso per moltiplicazione per elementi non nulli di $\mathbb{Q}$. Sicuramente, dal momento che $T \subseteq S$, $\forall\, f \in \mathcal{F}$ $\min_{t\in T} v_p(f(t)) \geq \min_{s\in S} v_p(f(s))$. Si supponga ora per assurdo che $\exists\, f \in \mathcal{F}$ tale che le due quantità siano diverse, ossia $\exists\, \alpha \in \mathbb{Z}$ tale che $\min_{t\in T} v_p(f(t)) \geq \alpha > \min_{s\in S} v_p(f(s))$, e sia $a \in \mathbb{Q}$ tale che $v_p(a) = -\alpha$. Allora $af \in \mathcal{F} \cap \mathrm{Int}(T, \mathbb{Z}_{(p)})$, infatti, $\forall\, t \in T$

$$v_p(af(t)) = v_p(a) + v_p(f(t)) \geq -\alpha + \min_{t\in T} v_p(f(t)) \geq 0,$$

però $af \notin \mathrm{Int}(S, \mathbb{Z}_{(p)})$, dal momento che, se $\overline{s} \in S$ è tale che $\min_{s\in S} v_p(f(s)) = v_p(f(\overline{s}))$, si ha che

$$v_p(af(\overline{s})) = -\alpha + v_p(f(\overline{s})) < 0.$$

Tutto ciò contraddice l'ipotesi che T è $\mathbb{Z}_{(p)}$-polinomialmente denso in S relativamente a $\mathcal{F}$. □

Osservazione 4.14. Dato $f \in \mathbb{Q}[x]$, si può considerare il campo di spezzamento L di f su $\mathbb{Q}$, ossia l'estensione finita che si ottiene da $\mathbb{Q}$ aggiungendo tutte le radici di f. Sia $w : L \longrightarrow \mathbb{Z}$ una valutazione che estende la valutazione p-adica $v_p : \mathbb{Q} \longrightarrow \mathbb{Z}$ a tutto L, ossia $w|_{\mathbb{Q}} = v_p$, e si indichi con W l'anello di valutazione corrispondente a w ($W \cap \mathbb{Q} = \mathbb{Z}_{(p)}$). Si indichino con $a_1, ..., a_n$ le radici di f in W, cioè $w(a_i) \geq 0 \ \forall\, i \in \{1, ..., n\}$, mentre $b_1, ..., b_m$ le radici di f non in W, ossia $w(b_j) < 0 \ \forall\, j \in \{1, ..., m\}$. Dunque $L = \mathbb{Q}(a_1, ..., a_n, b_1, ..., b_m)$ e in L si può fattorizzare f nel seguente modo

$$f(x) = c\prod_{i=1}^{n}(x - a_i)\prod_{j=1}^{m}(x - b_j),$$

con $c \in \mathbb{Q}^*$. Dato un elemento $s \in \mathbb{Z}_{(p)}$, $f(s) \in \mathbb{Q}$ e si può determinare, sfruttando le proprietà della valutazione,

$$\begin{aligned} v_p(f(s)) = w(f(s)) &= w(c) + \sum_{i=1}^{n} w(s - a_i) + \sum_{j=1}^{m} w(s - b_j) = \\ &= w(c) + \sum_{i=1}^{n} w(s - a_i) + \sum_{j=1}^{m} w(b_j), \end{aligned} \tag{4.1}$$

dove l'ultima uguaglianza è dovuta al fatto che $w(s - b_j) = w(b_j) \ \forall\, j \in \{1, ..., m\}$, dal momento che $w(s) = v_p(s) > w(b_j)$ (Osservazione (4.10)). Dunque è importante notare che la parte di $v_p(f(s))$ nella formula (4.1) che dipende da s è quella data da $w(s - a_i) \ \forall\, i \in \{1, ..., n\}$.

Prima di proseguire, bisogna ricordare un importante Teorema la cui dimostrazione si può trovare in [10, Theorem 1.5.3]. Prima di tutto, per $n \in \mathbb{N}$, si può definire un ordine parziale $\leq$ su $\mathbb{N}^n$: dati $x = (x_1, ..., x_n), y = (y_1, ..., y_n) \in \mathbb{N}^n$, $x \leq y$ se $x_i \leq y_i \ \forall\, i \in \{1, ..., n\}$. Dato $N \subseteq \mathbb{N}^n$ sottoinsieme, un elemento $x \in N$ si dice *elemento minimale* di N se $\forall\, y \in N$ tale che $y \leq x$ segue che $x = y$. L'insieme degli elementi minimali di N si indica con $\mathrm{Min}(N)$.

Teorema 4.15 (Dickson)**.** *Dato un qualunque $N \subseteq \mathbb{N}^n$ sottoinsieme, l'insieme degli elementi minimali di N risulta essere un insieme finito e $\forall\, x \in N$ $\exists\, y \in$ Min(N) tale che $y \leq x$.*

Sfruttando questo Teorema, è possibile mostrare un risultato sull'esistenza di sottoinsiemi polinomialmente densi finiti:

Proposizione 4.16. *Siano H e $\mathcal{H}$ come in (4.1), dove si considera $D = \mathbb{Q}$. Allora, dato $S \subseteq \mathbb{Z}_{(p)}$, $\exists\, T \subseteq S$ finito tale che $\forall\, f \in \mathcal{H}$*

$$\min_{t \in T} v_p(f(t)) = \min_{s \in S} v_p(f(s)); \tag{4.2}$$

in particolare, T risulta essere $\mathbb{Z}_{(p)}$-polinomialmente denso in S relativamente a $\mathcal{H}$. Inoltre, se nessuna radice dei polinomi in H è un punto isolato di S nella topologia p-adica, allora T non contiene nessuna di queste radici.

Dimostrazione. Se $H = \{q_1, ..., q_l\}$, gli elementi di $\mathcal{H}$ sono del tipo $c\prod_{i=1}^{l} q_i^{e_i}$ con $c \in \mathbb{Q}^*$ e $e_i \geq 0\ \forall\, i \in \{1, ..., l\}$. Come fatto nell'Osservazione (4.14), sia ora L il campo di spezzamento dei polinomi di H su $\mathbb{Q}$, w una estensione di v_p a tutto L e W l'anello di valutazione corrispondente a w. In L ogni q_i con $i \in \{1, ..., l\}$ si scrive come

$$q_i(x) = c_i \prod_{j=1}^{n_i}(x - a_{ij}) \prod_{k=1}^{m_i}(x - b_{ik}),$$

dove $c_i \in \mathbb{Q}^*$, $n_i, m_i \in \mathbb{N}$ non entrambi nulli, $a_{ij} \in W\ \forall\, j \in \{1, ..., n_i\}$ ($w(a_{ij}) \geq 0$) e $b_{ik} \notin W\ \forall\, k \in \{1, ..., m_i\}$ ($w(b_{ik}) < 0$) (sicuramente almeno uno tra gli n_i con $i \in \{1, ..., l\}$ deve essere non nullo altrimenti il risultato è ovvio). Quindi, un generico elemento $f \in \mathcal{H}$ è del tipo

$$f(x) = d\prod_{i=1}^{l}\left(\prod_{j=1}^{n_i}(x - a_{ij})^{e_i} \prod_{k=1}^{m_i}(x - b_{ik})^{e_i}\right),$$

con $d \in \mathbb{Q}^*$. Per l'Osservazione (4.14),

$$\begin{gathered}\min_{t\in T} v_p(f(t)) = \min_{s\in S} v_p(f(s)) \iff \\ \min_{t\in T}\sum_{i=1}^{l}\sum_{j=1}^{n_i} e_i w(t - a_{ij}) = \min_{s\in S}\sum_{i=1}^{l}\sum_{j=1}^{n_i} e_i w(s - a_{ij}).\end{gathered} \tag{4.3}$$

Se si considera il sottoinsieme

$$N = \{(w(s - a_{ij}))_{i=1,...,l,j=1,...,n_i} \,|\, s \in S\} \subseteq \mathbb{N}^{\sum_{i=1}^{l} n_i},$$

per il Teorema di Dickson si sa che questo sottoinsieme ammette un sottoinsieme finito di elementi minimali, ossia $\exists\, T \subseteq S$ finito tale che

$$\mathrm{Min}(N) = \{(w(t - a_{ij}))_{i=1,...,l,j=1,...,n_i} \,|\, t \in T\}$$

e $\forall\, s \in S\ \exists\, t \in T$ tale che

$$(w(t - a_{ij}))_{i=1,...,l,j=1,...,n_i} \leq (w(s - a_{ij}))_{i=1,...,l,j=1,...,n_i}, \tag{4.4}$$

in particolare, $w(t - a_{ij}) \leq w(s - a_{ij})\ \forall\, i \in \{1, ..., l\}, j \in \{1, ..., n_i\}$. Bisogna ora mostrare che, costruito T in questo modo, $\forall\, f \in \mathcal{H}$ vale la condizione (4.3). Sicuramente, dal momento che $T \subseteq S$, $\min_{t\in T}\sum_{i=1}^{l}\sum_{j=1}^{n_i} e_i w(t - a_{ij}) \geq \min_{s\in S}\sum_{i=1}^{l}\sum_{j=1}^{n_i} e_i w(s - a_{ij})$. Si supponga per assurdo che siano diversi e sia $\overline{s} \in S$ tale che $\min_{s\in S}\sum_{i=1}^{l}\sum_{j=1}^{n_i} e_i w(s - a_{ij}) = \sum_{i=1}^{l}\sum_{j=1}^{n_i} e_i w(\overline{s} -$

a_{ij}). Per il Teorema di Dickson $\exists\, \bar{t} \in T$ tale che vale la condizione (4.4), dunque si ottiene

$$\sum_{i=1}^{l}\sum_{j=1}^{n_i} e_i w(\bar{t} - a_{ij}) \geq \min_{t\in T} \sum_{i=1}^{l}\sum_{j=1}^{n_i} e_i w(t - a_{ij}) >$$
$$> \sum_{i=1}^{l}\sum_{j=1}^{n_i} e_i w(\bar{s} - a_{ij}) \geq \sum_{i=1}^{l}\sum_{j=1}^{n_i} e_i w(\bar{t} - a_{ij}),$$

che risulta essere una contraddizione. Questo prova che T soddisfa la condizione (4.2) e, dal momento che $\mathcal{H}$ è chiuso per moltiplicazione per elementi non nulli di $\mathbb{Q}$, per il Lemma (4.13) T risulta essere $\mathbb{Z}_{(p)}$-polinomialmente denso in S relativamente a $\mathcal{H}$.
Bisogna, infine, mostrare che, se nessuna radice dei polinomi in H è un punto isolato di S nella topologia p-adica, allora T non contiene nessuna di queste radici. Si supponga quindi per assurdo che $\exists\, \bar{t} \in T$ che sia radice di uno dei polinomi in H, si può supporre che $\bar{t} = a_{11}$, dunque si ottiene

$$(w(\bar{t} - a_{ij}))_{i=1,\dots,l,j=1,\dots,n_i} = (\infty, \dots).$$

Posto $n > \max\{w(\bar{t} - a_{ij}) |\, (i,j) \neq (1,1)\}$, si sa che, dal momento che $\bar{t}$ non è un punto isolato di S rispetto alla topologia p-adica, $B(\bar{t}, n) \cap S \supsetneq \{\bar{t}\}$, quindi $\exists\, \bar{s} \in S$, $\bar{s} \neq \bar{t}$ tale che $\bar{s} \in B(\bar{t}, n)$. Da quest'ultima affermazione si deduce che $\bar{s} = \bar{t} + u$, dove $w(u) \geq n > w(\bar{t} - a_{ij})\ \forall\, (i,j) \neq (1,1)$. In particolare si ha che

$$w(\bar{s} - a_{ij}) = w(\bar{s} - \bar{t} + \bar{t} - a_{ij}) = \min\{w(\bar{t} - a_{ij}), w(u)\} = w(\bar{t} - a_{ij})$$

$\forall\, (i,j) \neq (1,1)$ ($w(\bar{t} - a_{ij}) < n \leq w(u)$ per come è stato scelto n). Dunque, dal momento che $\bar{s} \neq \bar{t}$, si ha che

$$(w(\bar{s} - a_{ij}))_{i=1,\dots,l,j=1,\dots,n_i} < (w(\bar{t} - a_{ij}))_{i=1,\dots,l,j=1,\dots,n_i}$$

e questo genera una contraddizione dato che $(w(\bar{t} - a_{ij}))_{i=1,\dots,l,j=1,\dots,n_i} \in \mathrm{Min}(N)$. □

Prima di enunciare il Teorema successivo, bisogna ricordare che se $h \in \mathbb{Q}[x]$ è un polinomio irriducibile, si può definire la valutazione discreta

$$v_h : \mathbb{Q}(x)^* \longrightarrow \mathbb{Z}$$

che associa a ogni $g \in \mathbb{Q}[x]$ non nullo l'esponente con cui h compare nella fattorizzazione in irriducibili di g in $\mathbb{Q}[x]$ ($\mathbb{Q}[x]$ è un UFD). Per ogni elemento non nullo di $\mathbb{Q}(x)$ del tipo $\dfrac{g_1}{g_2}$ si pone, invece, $v_h\left(\dfrac{g_1}{g_2}\right) = v_h(g_1) - v_h(g_2)$.

Un'altra cosa da ricordare è che la somma diretta di un numero finito di copie di $\mathbb{N}$ (con notazione additiva), ossia $\bigoplus_{i=1}^{n}(\mathbb{N},+)$, è un monoide libero commutativo in cui la somma è definita componente per componente e l'elemento neutro è $(0,...,0)$. Particolari elementi di $\bigoplus_{i=1}^{n}(\mathbb{N},+)$ sono i vettori coordinati, indicati con e_i, che hanno tutte le entrate nulle tranne la i-esima che è uguale a 1. Inoltre, si ha che, se $x=(x_1,...,x_n), y=(y_1,...,y_n) \in \bigoplus_{i=1}^{n}(\mathbb{N},+)$, $x \mid y$ se $\exists\, z \in \bigoplus_{i=1}^{n}(\mathbb{N},+)$ tale che $y=x+z$ e questo equivale a dire che $x \leq y$, ossia $x_i \leq y_i \ \forall\, i \in \{1,...,n\}$. Dunque, dato un qualunque sottoinsieme $\{x_i=(x_{i1},...,x_{in}) |\, i \in I\} \subseteq \bigoplus_{i=1}^{n}(\mathbb{N},+)$, si ha che

$$\gcd(x_i |\, i \in I) = (\min(x_{i1} |\, i \in I),...,\min(x_{in} |\, i \in I)).$$

Teorema 4.17. *Siano H e $\mathcal{H}$ come in (4.1), dove si considera $D=\mathbb{Q}$. Allora, dato $S \subseteq \mathbb{Z}_{(p)}$ tale che nessuna radice dei polinomi in H sia un punto isolato di S nella topologia p-adica e posto $\mathcal{F}=\mathcal{H}\cap \mathrm{Int}(S,\mathbb{Z}_{(p)})$, $\exists\, T \subseteq S$ finito $\mathbb{Z}_{(p)}$-polinomialmente denso in S relativamente a $\mathcal{H}$ che non contiene radici dei polinomi in H. Inoltre, la mappa*

$$\begin{aligned} \varphi : \mathcal{F} &\longrightarrow \bigoplus_{h\in H}(\mathbb{N},+) \oplus \bigoplus_{t\in T}(\mathbb{N},+) \\ g &\longmapsto ((v_h(g) |\, h \in H),(v_p(g(t)) |\, t \in T)) \end{aligned} \tag{4.5}$$

è un omomorfismo di divisione; in particolare, se T è minimale, φ è una teoria di divisione.

Dimostrazione. Per la Proposizione (4.16) esiste un sottoinsieme $T \subseteq S$ finito $\mathbb{Z}_{(p)}$-polinomialmente denso in S relativamente a $\mathcal{H}$ che non contiene radici di polinomi in H; per ottenere un T che sia minimale, facendo riferimento alla dimostrazione della Proposizione (4.16), basta considerare i sottoinsiemi $T' \subseteq T$ tali che $(w(t_1-a_{ij}))_{i=1,...,l,j=1,...,n_i} = (w(t_2-a_{ij}))_{i=1,...,l,j=1,...,n_i}$ $\forall\, t_1,t_2 \in T'$ e per ognuno di questi sottoinsiemi selezionare un unico elemento da inserire nell'insieme T minimale da costruire.
Bisogna, ora, mostrare che φ è un omomorfismo di divisione. Per prima cosa bisogna notare che la mappa φ è ben definita, poiché $v_p(g(t)) \lneqq \infty$ $\forall\, g \in \mathcal{F}, t \in T$, infatti, T non contiene radici di polinomi in H e, dal momento che gli elementi di $\mathcal{H}$ sono tutti i polinomi di $\mathbb{Q}[x]$ i cui fattori irriducibili sono in H, T non contiene neppure radici di elementi di $\mathcal{H}$, dunque $g(t) \neq 0\ \forall\, g \in \mathcal{F}, t \in T$. Inoltre, φ è un omomorfismo di monoidi, infatti, $\varphi(1)=(0,...,0)$ e se $f,g \in \mathcal{F}$

$$\begin{aligned} &\varphi(fg) = ((v_h(fg) |\, h \in H),(v_p(f(t)g(t)) |\, t \in T)) = \\ &= ((v_h(f) |\, h \in H),(v_p(f(t)) |\, t \in T)) + ((v_h(g) |\, h \in H),(v_p(g(t)) |\, t \in T)) = \\ &= \varphi(f)+\varphi(g). \end{aligned}$$

A questo punto bisogna mostrare che φ è un omomorfismo di divisione; siano quindi $f,g \in \mathcal{F}$ tali che $\varphi(f) \mid \varphi(g)$. Posto $\overline{f}=\dfrac{g}{f}$, dal momento che $v_h(f) \leq$

$v_h(g)\ \forall\, h \in H$, ossia $v_h(\overline{f}) \geq 0\ \forall\, h \in H$, si ha che $\overline{f} \in \mathbb{Q}[x]$ e sicuramente $\overline{f} \in \mathcal{H}$; dal fatto che $v_p(f(t)) \leq v_p(g(t))\ \forall\, t \in T$, ossia $v_p(\overline{f}(t)) \geq 0\ \forall\, t \in T$, si deduce che $\overline{f}(t) \in \mathbb{Z}_{(p)}\ \forall\, t \in T$, cioè $\overline{f} \in \mathrm{Int}(T, \mathbb{Z}_{(p)})$. Dunque, siccome $\overline{f} \in \mathcal{H} \cap \mathrm{Int}(T, \mathbb{Z}_{(p)})$ e T è $\mathbb{Z}_{(p)}$-polinomialmente denso in S relativamente a $\mathcal{H}$, allora $\overline{f} \in \mathcal{H} \cap \mathrm{Int}(S, \mathbb{Z}_{(p)}) = \mathcal{F}$, di conseguenza $f \mid g$ in $\mathcal{F}$.
Ora, supponendo che T sia minimale, bisogna mostrare che φ è una teoria di divisione; in questo caso, basta provare che ogni vettore coordinato è gcd di un numero finito di immagini tramite φ di elementi di $\mathcal{F}$. Si può supporre che $H \subseteq \mathbb{Z}_{(p)}[x]$, in modo che $H \subseteq \mathcal{F}$, e che tutti gli elementi di H siano primitivi. Per arrivare alla conclusione sono necessarie delle osservazioni:

(i) $p \in \mathcal{F}$ e $v_h(p) = 0\ \forall\, h \in H$, mentre $v_p(p(t)) = v_p(p) = 1\ \forall\, t \in T$ (p è polinomio costante);

(ii) $h \in H \subseteq \mathcal{F}$ e $v_h(h) = 1$, ma $v_k(h) = 0\ \forall\, k \in H, k \neq h$;

(iii) $\forall\, t \in T\ \exists\, g_t \in \mathcal{F}$ tale che $v_p(g_t(t)) = 0$ e $v_p(g_t(r)) > 0\ \forall\, r \in T, r \neq t$;

(iv) $\forall\, t \in T, h \in H\ \exists\, g_{th} \in \mathcal{F}$ tale che $v_p(g_{th}(t)) = 0$ e $v_h(g_{th}) > 0$.

L'affermazione (iii) deriva dal fatto che T è minimale, dunque, fissato $t \in T$, $T \setminus \{t\}$ non è $\mathbb{Z}_{(p)}$-polinomialmente denso in S relativamente ad $\mathcal{H}$, ossia, per il Lemma (4.13), $\exists\, k \in \mathcal{H}$ tale che

$$\min_{r \in T \setminus \{t\}} v_p(k(r)) > \min_{s \in S} v_p(k(s)).$$

Dal momento che, però, per il Lemma (4.13)

$$\min_{r \in T} v_p(k(r)) = \min_{s \in S} v_p(k(s)),$$

si deve avere che questa quantità è uguale a $v_p(k(t))$. Si può quindi porre $g_t(x) = p^{-v_p(k(t))}k(x)$; sicuramente $g_t \in \mathcal{H}$ perchè k vi appartiene, inoltre, dato $s \in S$, si ha che

$$v_p(g_t(s)) = -v_p(k(t)) + v_p(k(s)) \geq -v_p(k(t)) + \min_{s \in S} v_p(k(s)) = 0,$$

dunque $g_t \in \mathrm{Int}(S, \mathbb{Z}_{(p)})$, quindi $g_t \in \mathcal{F}$. Si osserva anche che $v_p(g_t(t)) = 0$ e per $r \in T, r \neq t$,

$$v_p(g_t(r)) = -v_p(k(t)) + v_p(k(r)) \geq -v_p(k(t)) + \min_{r \in T \setminus \{t\}} v_p(k(r)) > 0.$$

Per quanto riguarda l'affermazione (iv), invece, fissati $t \in T, h \in H$, basta scegliere $k \in \mathcal{F}$ tale che $v_h(k) > 0$ e porre $g_{th}(x) = p^{-v_p(k(t))}k(x)g_t(x)^{v_p(k(t))}$. Sicuramente, $g_{th} \in \mathcal{H}$ dal momento che sia k che g_t vi appartengono, bisogna, però mostrare che $g_{th} \in \mathrm{Int}(S, \mathbb{Z}_{(p)})$. Si osserva che

$$v_p(g_{th}(t)) = -v_p(k(t)) + v_p(k(t)) + v_p(k(t))\underbrace{v_p(g_t(t))}_{=0} = 0,$$

mentre per $r \in T, r \neq t$ si ha

$$v_p(g_{th}(r)) = -v_p(k(t)) + v_p(k(r)) + v_p(k(t))v_p(g_t(r)) = \\ = v_p(k(t))(\underbrace{v_p(g_t(r)) - 1}_{\geq 0}) + \underbrace{v_p(k(r))}_{\geq 0} \geq 0,$$

poiché $k \in \mathrm{Int}(S, \mathbb{Z}_{(p)})$. Dunque, $g_{th} \in \mathrm{Int}(T, \mathbb{Z}_{(p)}) \cap \mathcal{H}$ e, siccome T è $\mathbb{Z}_{(p)}$-polinomialmente denso in S relativamente a $\mathcal{H}$, allora $g_{th} \in \mathrm{Int}(S, \mathbb{Z}_{(p)}) \cap \mathcal{H} = \mathcal{F}$. Manca solo da provare che $v_h(g_{th}) > 0$ e questo è vero perché

$$v_h(g_{th}) = \underbrace{v_h(k)}_{>0} + \underbrace{v_p(k(t))v_h(g_t)}_{\geq 0} > 0.$$

Grazie a queste osservazioni si vede che se $h \in H$, il vettore coordinato e_h si ottiene come

$$e_h = \gcd(\{\varphi(g_{th}) | \, t \in T\} \cup \{\varphi(h)\}),$$

mentre, per $t \in T$ il vettore coordinato e_t risulta essere

$$e_t = \gcd(\{\varphi(g_r) | \, r \neq t\} \cup \{\varphi(p)\}).$$

□

Prima di enunciare il Corollario che segue direttamente da questo Teorema, bisogna provare il seguente Lemma:

Lemma 4.18. *Sia $S \subseteq \mathbb{Z}_{(p)}$ e $f \in \mathrm{Int}(S, \mathbb{Z}_{(p)})$. Si prendano poi $g \in [[f]]$ e $a \in \mathbb{Q}$. Se $-\min_{s \in S} v_p(g(s)) \leq v_p(a) \leq 0$, allora $ag \in [[f]]$.*

Dimostrazione. Dato che $g \in [[f]]$, $\exists\, h \in \mathrm{Int}(S, \mathbb{Z}_{(p)})$, $n \in \mathbb{N}$ tali che $f^n = gh$, quindi si può scrivere $f^n = (ag)(a^{-1}h)$. Entrambi i fattori sono elementi di $\mathrm{Int}(S, \mathbb{Z}_{(p)})$: dato $s \in S$, si ha $v_p(ag(s)) = v_p(a) + v_p(g(s)) \geq v_p(a) + \min_{s \in S} v_p(g(s)) \geq 0$, mentre $v_p(a^{-1}h(s)) = -v_p(a) + v_p(h(s)) \geq 0$. Dunque $ag \in [[f]]$. □

Corollario 4.19. *Sia $f \in \mathrm{Int}(S, \mathbb{Z}_{(p)})$ non nullo, dove $S \subseteq \mathbb{Z}_{(p)}$ è tale che nessuna radice di f è un punto isolato di S nella topologia p-adica, e siano poi H_f e $\mathcal{H}_f$ come in (4.1), dove si considera $D = \mathbb{Q}$. Allora $\exists\, T \subseteq S$ finito tale che T è $\mathbb{Z}_{(p)}$-polinomialmente denso in S relativamente a $\mathcal{H}_f$ e non contiene nessuna radice di f. Inoltre la mappa*

$$\psi : [[f]] \longrightarrow \bigoplus_{h \in H_f} (\mathbb{N}, +) \oplus \bigoplus_{t \in T} (\mathbb{N}, +) \\ g \longmapsto ((v_h(g) | \, h \in H_f), (v_p(g(t)) | \, t \in T))$$

è un omomorfismo di divisione; in particolare, se $\mathsf{d}_S(f) \neq 1$ e T è minimale, ψ è una teoria di divisione.

Dimostrazione. Per la Proposizione (4.16), esiste un sottoinsieme $T \subseteq S$ finito $\mathbb{Z}_{(p)}$-polinomialmente denso in S relativamente a $\mathcal{H}_f$, inoltre, T non contiene radici di polinomi in H_f, dunque non contiene radici di f, essendo gli elementi di H_f i fattori irriducibili di f. Dal momento poi che $[[f]] \subseteq \mathcal{H}_f \cap \mathrm{Int}(S, \mathbb{Z}_{(p)})$, si ha che $\psi = \varphi|_{[[f]]}$, dove φ è la mappa (4.5), che per il Teorema (4.17) risulta essere un omomorfismo di divisione, quindi anche ψ lo è. Nel caso particolare in cui $\mathsf{d}_S(f) \neq 1$, si ha che $[[f]] = \mathcal{H}_f \cap \mathrm{Int}(S, \mathbb{Z}_{(p)})$. Per provare questa affermazione basta mostrare che $[[f]] \supseteq \mathcal{H}_f \cap \mathrm{Int}(S, \mathbb{Z}_{(p)})$. Per prima cosa, si scriva f come $f = c\tilde{f}$ con $c \in \mathbb{Q}^*$ e $\tilde{f} \in \mathbb{Z}_{(p)}[x]$ primitivo. A questo punto, bisogna notare che $f(S) \subseteq \mathbb{Z}_{(p)}$ e il fatto che $\mathsf{d}_S(f) \neq 1$ implica che $\mathsf{d}_S(f)$ non è invertibile in $\mathbb{Z}_{(p)}$, ossia appartiene all'unico ideale massimale di $\mathbb{Z}_{(p)}$, che risulta essere $p\mathbb{Z}_{(p)}$, dunque $v_p(\mathsf{d}_S(f)) > 0$. Sia ora un qualsiasi $b \in \mathbb{Z}_{(p)} \setminus \{0\}$, allora, per l'assioma di Archimede, $\exists\, m \in \mathbb{N}$ tale che $mv_p(\mathsf{d}_S(f)) \geq v_p(b) - v_p(c)$. Dunque si ottiene che

$$f^{m+1} = f^m \cdot f = f^m \cdot c\tilde{f} = (f^m c b^{-1}) b\tilde{f},$$

dove entrambi i fattori appartengono a $\mathrm{Int}(S, \mathbb{Z}_{(p)})$: dato $s \in S$, per le proprietà della valutazione v_p,

$$v_p(f^m(s)cb^{-1}) = mv_p(f(s)) + v_p(c) - v_p(b) \geq mv_p(\mathsf{d}_S(f)) + v_p(c) - v_p(b) \geq 0,$$

dove si è usato il fatto che $\min_{s\in S} v_p(f(s)) = v_p(\mathsf{d}_S(f))$ (Osservazione (4.11)); invece, $b\tilde{f} \in \mathrm{Int}(S, \mathbb{Z}_{(p)})$, poiché $b \in \mathbb{Z}_{(p)} \setminus \{0\}$ e $\tilde{f} \in \mathbb{Z}_{(p)}[x]$. Dunque $b\tilde{f} \in [[f]]$ $\forall\, b \in \mathbb{Z}_{(p)} \setminus \{0\}$. Inoltre, essendo $[[f]]$ chiuso per divisione, anche tutti i divisori in $\mathbb{Z}_{(p)}[x]$ di $b\tilde{f}$ sono in $[[f]]$ (sono sicuramente elementi di $\mathrm{Int}(S, \mathbb{Z}_{(p)})$), quindi, in particolare, appartengono a $[[f]]$ tutti gli elementi non nulli di $\mathbb{Z}_{(p)}$, i divisori irriducibili di $\tilde{f}$ in $\mathbb{Z}_{(p)}[x]$ e, siccome $[[f]]$ è chiuso per moltiplicazione, anche tutti i loro prodotti; questi ultimi polinomi, dato che $\mathbb{Z}_{(p)}$ è UFD, sono primitivi perché $\tilde{f}$ lo è (Lemma (1.14)(i)) e sono per questo irriducibili anche in $\mathbb{Q}[x]$ (Lemma (1.17)), dunque, assieme agli elementi non nulli di $\mathbb{Q}$, generano $\mathcal{H}_f$. Grazie al Lemma (4.18), si ottiene poi che $[[f]]$ contiene tutti i prodotti di uno di questi polinomi per un elemento $a \in \mathbb{Q}$ tale che $v_p(a) < 0$ e che questo prodotto sia un elemento di $\mathrm{Int}(S, \mathbb{Z}_{(p)})$. In questo modo, si ottiene che $[[f]] = \mathcal{H}_f \cap \mathrm{Int}(S, \mathbb{Z}_{(p)})$, quindi se si sceglie T minimale, per il Teorema (4.17) si ha che ψ è una teoria di divisione. □

Per poter dimostrare il Teorema fondamentale di questo capitolo, è necessario il seguente Lemma:

Lemma 4.20. *Siano $S \subseteq \mathbb{Z}_{(p)}$ e $f \in \mathbb{Z}_{(p)}[x]$ tale che $\mathsf{d}_S(f) = 1$. Siano H_f e $\mathcal{H}_f$ come in (4.1), dove si considera $D = \mathbb{Z}_{(p)}$; si supponga anche che gli elementi di H_f siano primitivi (in questo modo corrispondono ai fattori irriducibili di f in $\mathbb{Q}[x]$ per il Lemma (1.17)). Allora*

(i) $[[f]] = \mathcal{H}_f$;

(ii) *Ogni $g \in [[f]]$ è un elemento di $\mathbb{Z}_{(p)}[x]$ primitivo e tale che $\mathsf{d}_S(g) = 1$;*

(iii) *Siano $g, h \in [[f]]$, $g \mid h$ in $[[f]] \iff g \mid h$ in $\mathbb{Q}[x]$;*

(iv) *La mappa*

$$\begin{aligned} \varphi : [[f]] &\longrightarrow \bigoplus_{h \in H_f} (\mathbb{N}, +) \\ g &\longmapsto (v_h(g) |\, h \in H_f) \end{aligned}$$

è una teoria di divisione.

Dimostrazione. Se $H_f = \{q_1, ..., q_k\}$, gli elementi di $\mathcal{H}_f$ sono del tipo

$$g(x) = c \prod_{i=1}^{k} q_i^{e_i},$$

dove c è un elemento invertibile di $\mathbb{Z}_{(p)}$ e $e_i \geq 0 \; \forall \, i \in \{1, ..., k\}$, in particolare, $g \in \mathbb{Z}_{(p)}[x]$. Se si sceglie $n = \max(e_i |\, i \in \{1, ..., k\})$, allora $g \mid f^n$ in $\mathbb{Z}_{(p)}[x]$, dunque $g \in [[f]]$. In questo modo di ottiene che $\mathcal{H}_f \subseteq [[f]]$. Dal momento che $\mathsf{d}_S(f) = 1$, f è primitivo, inoltre, tutte le potenze di f sono a immagine primitiva su S e dunque primitive e anche tutti i divisori in $\mathbb{Z}_{(p)}[x]$ di una potenza di f hanno la stessa caratteristica (Osservazioni (1.15) e (1.16)), perciò questo vale anche per gli elementi di $\mathcal{H}_f$. Ora basta mostrare che $[[f]] \subseteq \mathcal{H}_f$; sia, quindi, $g \in [[f]]$, si ha $f^n = gh \; \exists \, n \in \mathbb{N}, h \in \mathrm{Int}(S, \mathbb{Z}_{(p)})$. Sicuramente, g e h possono essere espressi come $g = c\tilde{g}$ e $h = d\tilde{h}$ con $c, d \in \mathbb{Q}$ e $\tilde{g}, \tilde{h} \in \mathcal{H}_f$, dunque $\tilde{g}, \tilde{h}$ sono a immagine primitiva su S. Per l'Osservazione (4.11), sia $\overline{s} \in S$ tale che $v_p(\tilde{g}(\overline{s})) = \min_{s \in S} v_p(\tilde{g}(s)) = v_p(\mathsf{d}_S(\tilde{g}))$. Allora

$$0 \leq v_p(g(\overline{s})) = v_p(c) + v_p(\tilde{g}(\overline{s})) = v_p(c),$$

ossia c, e in modo analogo anche d, sono elementi di $\mathbb{Z}_{(p)}$. Sfruttando poi il fatto che $f^n, \tilde{g}, \tilde{h}$ sono primitivi e il Lemma (1.14)(i), si ha che

$$1 = \mathsf{c}(f^n) = cd\mathsf{c}(\tilde{g})\mathsf{c}(\tilde{h}) = cd,$$

cioè c, d sono invertibili in $\mathbb{Z}_{(p)}$, dunque $g \in \mathcal{H}_f$. Quindi $[[f]] = \mathcal{H}_f \subseteq \mathbb{Z}_{(p)}[x]$ e, come mostrato prima, tutti gli elementi di $[[f]]$ sono primitivi e a immagine primitiva su S. In questo modo, sono stati provati i primi due punti, gli altri due seguono facilmente. □

Teorema 4.21. *Sia $f \in \mathrm{Int}(\mathbb{Z})$ non nullo, siano poi H_f e $\mathcal{H}_f$ come in (4.1), dove si considera $D = \mathbb{Q}$. Si definisca poi*

$$\mathcal{P} = \{p \in \mathbb{Z} |\, p \text{ primo}, f \notin \mathbb{Z}_{(p)}[x] \text{ o } f \in \mathbb{Z}_{(p)}[x] \text{ e } v_p(f(\mathbb{Z})) > 0\}.$$

Allora $\forall\, p \in \mathcal{P}\ \exists\, T_p \subseteq \mathbb{Z}$ *finito tale che* T_p *è* $\mathbb{Z}_{(p)}$*-polinomialmente denso in* $\mathbb{Z}$ *relativamente a* $\mathcal{H}_f$ *e non contiene radici di* f*. Inoltre, la mappa*

$$\begin{aligned}\varphi : [[f]] &\longrightarrow \bigoplus_{h\in H_f}(\mathbb{N},+)\oplus\bigoplus_{p\in\mathcal{P}}\bigoplus_{t\in T_p}(\mathbb{N},+)\\ g &\longmapsto ((v_h(g)|\, h\in H_f),((v_p(g(t))|\, t\in T_p)|\, p\in\mathcal{P}))\end{aligned}$$

è un omomorfismo di divisione.

Dimostrazione. Fissato $p \in \mathcal{P}$, per la Proposizione (4.16), posto $S = \mathbb{Z}$, l'insieme finito T_p esiste e non contiene radici di polinomi in H_f, ossia non contiene nessuna radice di f. Questo rende φ una mappa ben definita poiché T_p non contiene nessuna radice di elementi in $[[f]]$, essendo questi fattori di una potenza di f, dunque $v_p(g(t)) \lneqq \infty\ \forall\, p \in \mathcal{P}, t \in T_p, g \in [[f]]$. Inoltre, il fatto che φ sia un omomorfismo di monoidi deriva dalle proprietà delle valutazioni v_h con $h \in H_f$ e v_p con $p \in \mathcal{P}$ come visto nella dimostrazione del Teorema (4.17). Quindi, bisogna solamente mostrare che, dati $g_1, g_2 \in [[f]]$, se $\varphi(g_1) \mid \varphi(g_2)$, allora $g_1 \mid g_2$ in $[[f]]$. Se si dimostra che $\overline{g} = \frac{g_2}{g_1} \in \mathbb{Q}[x]$ (e questo è vero dal momento che $v_h(g_1) \leq v_h(g_2)\ \forall\, h \in H_f$), automaticamente $\overline{g}$ divide una potenza di f, dunque resta solo da provare che $\overline{g} \in \mathrm{Int}(\mathbb{Z})$, ma essendo $\mathbb{Z} = \cap_{p\ \mathrm{primo}}\mathbb{Z}_{(p)}$, se si mostra che $\overline{g} \in \mathrm{Int}(\mathbb{Z}, \mathbb{Z}_{(p)})\ \forall\, p$ primo, si ha che, preso $z \in \mathbb{Z}$, $\overline{g}(z) \in \mathbb{Z}_{(p)}\ \forall\, p$ primo, dunque sta nell'intersezione, ossia $\mathbb{Z}$. Quindi, è necessario mostrare che $\overline{g} \in \mathrm{Int}(\mathbb{Z}, \mathbb{Z}_{(p)})\ \forall\, p$ primo. A questo punto bisogna distinguere due casi a seconda che p appartenga o meno a $\mathcal{P}$. Se $p \in \mathcal{P}$, si può considerare la mappa π_p, proiezione su $\bigoplus_{h\in H_f}(\mathbb{N},+)\oplus \bigoplus_{t\in T_p}(\mathbb{N},+)$, e si ottiene che $\pi_p \circ \varphi(g_1) \mid \pi_p \circ \varphi(g_2)$. Dopo aver definito $\mathcal{F}_p = \mathcal{H}_f \cap \mathrm{Int}(\mathbb{Z}, \mathbb{Z}_{(p)})$, si può porre

$$\begin{aligned}\varphi_p : \mathcal{F}_p &\longrightarrow \bigoplus_{h\in H_f}(\mathbb{N},+)\oplus\bigoplus_{t\in T_p}(\mathbb{N},+)\\ g &\longmapsto ((v_h(g)|\, h\in H_f),(v_p(g(t))|\, t\in T_p)),\end{aligned}$$

mappa che per il Teorema (4.17) risulta essere un omomorfismo di divisione. Siccome $[[f]] \subseteq \mathcal{F}_p$, si ha che $\pi_p \circ \varphi = \varphi_p|_{[[f]]}$, dunque, dal fatto che $\varphi_p(g_1) \mid \varphi_p(g_2)$ si deduce che $g_1 \mid g_2$ in $\mathcal{F}_p$, ossia $\overline{g} \in \mathcal{F}_p$, in particolare $\overline{g} \in \mathrm{Int}(\mathbb{Z}, \mathbb{Z}_{(p)})$. Se, invece, $p \notin \mathcal{P}$, allora $f \in \mathbb{Z}_{(p)}[x]$ e $v_p(f(\mathbb{Z})) = 0$, ossia, visto $f \in \mathrm{Int}(\mathbb{Z}, \mathbb{Z}_{(p)})$, si ha che $\mathsf{d}_{\mathbb{Z}}(f) = 1$. Quindi, per il Lemma (4.20)(iii), si ha che $\overline{g} \in \mathrm{Int}(\mathbb{Z}, \mathbb{Z}_{(p)})$ poiché $g_1 \mid g_2$ in $\mathbb{Q}[x]$. □

Corollario 4.22. *Per ogni elemento non nullo* $f \in \mathrm{Int}(\mathbb{Z})$*, il sottomonoide* $[[f]]$ *di* $\mathrm{Int}(\mathbb{Z})$ *è un monoide di Krull.*

Dimostrazione. Sicuramente $[[f]]$ è un monoide commutativo e cancellativo, inoltre, la mappa definita nel Teorema (4.21) è un omomorfismo di divisione; la conclusione del fatto che $[[f]]$ è un monoide di Krull si può trovare in [10, Theorem 2.4.8]. □

Bibliografia

[1] Anderson D. F., Cahen P. J., Chapman S. T., Smith W. W., *Some factorization properties of the ring of integer-valued polynomials*, Lecture Notes in Pure and Applied Mathematics, vol. 171, New York: Dekker, pp. 125-142, 1995.

[2] Cahen P. J., Chabert J. L., *Elasticity for integral-valued polynomials*, J. Pure Appl. Algebra, vol. 103, no. 3, pp. 303-311, 1995.

[3] Cahen P. J., Chabert J. L., *Integer-valued polynomials*, Amer. Math. Soc. Surveys and Monographs, 48, Providence, 1997.

[4] Cahen P. J., Chabert J. L., *What you should know about integer-valued polynomials*, The American Mathematical Monthly, 123:4, pp. 311-337, 2016.

[5] Chapman S. T., Gotti F., Gotti M., *How do elements really factor in* $\mathbb{Z}[\sqrt{-5}]$*?*, Advances in Commutative Algebra, Springer Trends in Mathematics, Birkhauser, Singapore, pp. 171-195, 2019.

[6] Chapman S.T., Krause U., *A closer look at non-unique factorization via atomic decay and strong atoms*, in Progress in commutative algebra 2 — Closures, Finiteness and Factorization, pp. 301–315, Walter de Gruyter, Berlin, 2012.

[7] Cohn P. M., *Bèzout rings and their subrings*, Proceedings of the Cambridge Philosophical Society, vol. 64, issue 02, p. 251, 1968.

[8] Frisch S., *A construction of integer-valued polynomials with prescribed sets of lengths of factorizations*, Monatsh. Math., vol. 171, 341-350, 2013.

[9] Frisch S., *Relative polynomial closure and monadically Krull monoids of integer-valued polynomials*, Multiplicative Ideal Theory and Factorization Theory, Springer Proc. Math. Stat., vol. 170, Springer, Cham, pp. 145–157, 2016.

[10] Geroldinger A., Halter-Koch F., *Non-unique factorizations, algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics, vol. 278, Chapman and Hall/CRC, 2006.

[11] Grams A., *Atomic domains and the ascending chain condition*, Math. Proc. Cambridge Philos. Soc., vol. 75, pp. 321-329, 1974.

[12] Koblitz N., *p-adic numbers, p-adic analysis, and zeta-functions*, Graduate Texts in Mathematics, Vol 58, Springer-Verlag, 1984.

[13] Krause U., *On monoids of finite real character*, Proc. Am. Math. Soc., vol. 105, pp. 546 – 554, 1989.

[14] Jacobson N., *Basic Algebra I*, second ed., W. H. Freeman and Company, New York, 2009.

[15] Marcus D. A., *Number fields*, Springer-Verlag, New York, 1977.

[16] Nakato S., *Non-absolutely irreducible elements in the ring of integer-valued polynomials*, Comm. Algebra, 48(4):1–14, 2020.

[17] Narkiewicz W., *Polynomial mappings*, Lecture Notes in Mathematics, vol. 1600, Springer-Verlag, Berlin, 1995.