Alma Mater Studiorum · Università di Bologna

facoltà di scienze matematiche, fisiche e naturali

Corso di Laurea in Matematica

ALGEBRE MONOUNARIE POLINOMIALI

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof.
Libero Verardi

Presentata da:
Roberta Mazzone

I Sessione
Anno Accademico 2011/12

A Marco.

Un altro passo verso il nostro futuro insieme..

Introduzione

Lo scopo di questo lavoro di tesi è stato lo studio delle algebre monounarie polinomiali negli anelli finiti $\mathbb{Z}_n$.
Riporto brevemente il percorso seguito nella stesura di questa relazione.
Nel primo capitolo si spiega cosa si intende per algebra monounaria, cioè la coppia (X, f) con X insieme sostegno e f operazione unaria su X. Nel presentare le principali caratteristiche di questa struttura, abbiamo prestato particolare attenzione alla sua rappresentazione geometrica attraverso l'uso di grafi orientati. Questo strumento ci permette di suddividere l'insieme di tutte le algebre monounarie in classi di isomorfismo; si mostra che due algebre sono isomorfe se la struttura dei grafi che le rappresentano è la stessa. Si conclude il primo capitolo con la definizione del prodotto diretto tra due algebre e le sue principali proprietà.
Nel secondo capitolo vengono richiamate nozioni e risultati sugli anelli che sono stati utili per il nostro lavoro. Per prima cosa si ricorda il concetto di anello insieme ad alcune proprietà, gli elementi invertibili e il gruppo moltiplicativo che costituiscono, i divisori dello zero, la definizione di campo e di dominio di integrità, il concetto di sottoanello e il sottoanello fondamentale, la caratteristica e il prodotto diretto tra due anelli. Vengono introdotte a seguire le definizioni di ideale (ideale proprio, massimale...), di anello quoziente e di omomorfismo di anelli; in particolare viene presentato il *teorema fondamentale di omomorfismo*, di rilevante importanza per l'analisi che abbiamo condotto. Secondo questo teorema se esiste un omomorfismo φ tra due anelli A e B, allora esiste un isomorfismo tra l'anello quoziente $A/Ker\,(\varphi)$

e l'immagine $\varphi(A)$; attraverso questo risultato si dimostra che se A_1 e A_2 sono due anelli e $I = I_1 \times I_2$ è l'ideale dell'anello prodotto $A_1 \times A_2$, allora $(A_1 \times A_2) / (I_1 \times I_2) \cong A_1/I_1 \times A_2/I_2$. Concludiamo il primo capitolo con un paragrafo dedicato alla costruzione dell'anello $\mathbb{Z}_m$, anello delle classi di equivalenza modulo m.

Dal terzo capitolo entriamo nel vivo di questo lavoro di tesi. Per prima cosa vengono date le definizioni di polinomio formale e funzione polinomiale:

se A è un anello commutativo allora si definisce un *polinomio* a coefficienti in A un'espressione $f(x) = \sum_i a_i x^i$, con $a_i \in A$ e x un simbolo;

se f è un polinomio allora è possibile associare a f una funzione, detta *polinomiale*, $\widetilde{f} : A \to A$ che ad ogni elemento $a \in A$ associa l'elemento $f(a)$ ottenuto dal polinomio $f(x)$ sostituendo x con a.

Il punto centrale è che non esiste, in generale, una corrispondenza biunivoca tra polinomi e funzioni polinomiali, poiché una stessa funzione può essere associata a diversi polinomi.

Ci si sofferma quindi sullo studio dei polinomi e delle funzioni polinomiali su un campo. Importante in tal senso è il *teorema di identità delle funzioni polinomiali* il quale sostiene che dato K campo infinito e $f(x)$ e $g(x)$ polinomi a coefficienti in K, allora $f(x) = g(x)$ come polinomi se e solo se f e g sono uguali come funzioni polinomiali. Al contrario se K è un campo finito con q elementi, si dimostra che i polinomi $f(x)$ e $g(x)$ sono uguali se $f(x) - g(x)$ è divisibile per il polinomio $x^q - x$. Un risultato molto interessante e utile per il nostro lavoro è che ogni funzione definita su un campo finito è polinomiale.

Successivamente viene presentato il concetto di congruenza e equivalenza modulo m tra polinomi che serve per definire il polinomio nullo modulo m cioè un polinomio a coefficienti interi che soddisfa la congruenza $f(x) \equiv 0$ modulo m o in altre parole un polinomio a coefficienti in $\mathbb{Z}_m$ che si annulla per ogni elemento di $\mathbb{Z}_m$. Si ha che $\forall m \in \mathbb{Z}$ il più semplice polinomio nullo modulo m è $\prod_{i=0}^{m-1}(x - i)$; se m è un primo e quindi $\mathbb{Z}_m$ è un campo, un polinomio nullo modulo p è $x^p - x$.

Si passa poi a studiare l'insieme I_0 dei polinomi identicamente nulli su un

anello A, facendo vedere che è un ideale di $A[x]$. Pertanto se A è un campo infinito si ha che $I_0 = \{0\}$, mentre se A è un campo finito con q elementi, allora $I_0 = (x^q - x)$.

Nell'ultimo capitolo vengono studiate le algebre monounarie polinomiali. Un algebra monounaria (X, f) è detta *polinomiale* se è isomorfa a un algebra $\left(\mathbb{Z}_n, f'\right)$, con f' funzione polinomiale. Quindi il primo passo è quello di individuare le funzioni polinomiali su un anello finito $\mathbb{Z}_n$. Si osserva che l'insieme delle funzioni polinomiali definite su un anello A è isomorfo all'anello quoziente $A[x]/I_0$; quindi il problema si sposta a quello di determinare l'ideale dei polinomi identicamente nulli sugli anelli $\mathbb{Z}_n$. Se n è primo, allora $I_0 = (x^n - x)$; la difficoltà si ha quando n non è primo.

Attraverso un lemma osserviamo che dati $p, q \in \mathbb{Z}$ con $MCD(p, q) = 1$ si ha che $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$, che $\mathbb{Z}_{pq}[x] \cong \mathbb{Z}_p[x] \times \mathbb{Z}_q[x]$ e che l'ideale I_{pq} dei polinomi identicamente nulli su $\mathbb{Z}_{pq}$ può essere scritto come prodotto diretto dell'ideale I_p dei polinomi identicamente nulli su $\mathbb{Z}_p$ e l'ideale I_q dei polinomi identicamente nulli su $\mathbb{Z}_q$. Questo implica anche che $\mathbb{Z}_{pq}[x]/I_{pq} \cong \mathbb{Z}_p[x]/I_p \times \mathbb{Z}_q[x]/I_q$. Si dimostra inoltre che ogni algebra polinomiale su $\mathbb{Z}_{pq}$ è isomorfa al prodotto diretto di un'algebra polinomiale su $\mathbb{Z}_p$ per una su $\mathbb{Z}_q$.

Segue che il calcolo delle funzioni polinomiali su $\mathbb{Z}_n$, con n qualsiasi, può essere ricondotto al caso $n = p^h$ con p primo e $h \geq 1$.

A questo punto abbiamo riportato un algoritmo per il computo delle classi di funzioni polinomiali su $\mathbb{Z}_n$ e delle classi di isomorfismo delle algebre polinomiali sullo stesso anello e due lemmi per determinare i generatori dell'ideale dei polinomi identicamente nulli.

Successivamente è stato introdotto il calcolo delle funzioni polinomiali, di quelle biettive e delle classi di isomorfismo delle algebre polinomiali per i casi $\mathbb{Z}_4$, $\mathbb{Z}_8$ e $\mathbb{Z}_9$. Il calcolo delle classi è stato eseguito mediante il software Excel e i grafi sono stati tracciati manualmente e confrontati sulla base delle loro caratteristiche topologiche.

A partire dai risultati ottenuti sono state ipotizzate delle congetture; in par-

ticolare ci siamo occupati di verificare (o meglio di smentire) una di queste: per ogni $n = p^h$, il gruppo G dei polinomi biettivi contiene un p-sottogruppo di Sylow del gruppo simmetrico S_n. Per fare ciò siamo andati ad analizzare il caso $\mathbb{Z}_{16}$.

Prima di questo abbiamo determinato il numero delle funzioni polinomiali per i casi $\mathbb{Z}_{25}$, $\mathbb{Z}_{49}$ e $\mathbb{Z}_{27}$ e ripercorso nel dettaglio il calcolo del caso $\mathbb{Z}_6$ per mostrare che le classi di isomorfismo delle algebre polinomiali possono essere meno rispetto alle attese.

Per il calcolo del gruppo delle funzioni polinomiali invertibili su $\mathbb{Z}_{16}$, abbiamo tentato una strada diversa, che non fa uso della verifica diretta ma utilizza un approccio combinatorio. Per prima cosa abbiamo verificato che l'ordine di G_4, G_8 e G_9 con questo nuovo metodo risultasse equivalente a quello ottenuto mendiante la verifica diretta e infine abbiamo determinato l'ordine di G_{16}, ottenendo $|G_{16}| \leq 2^{13}$. Poiché il 2-sottogruppo di Sylow ha ordine 2^{15}, si dimostra che la congettura è falsa. Per mezzo di un'analisi diretta è stato poi calcolato l'ordine esatto di questo gruppo che risulta essere proprio 2^{13}.

Abbiamo concluso questo lavoro di tesi esponendo una nuova congettura, supposta a seguito dell'analisi dei risultati ottenuti: dato $\mathbb{Z}_{2^n}$, il gruppo delle funzioni polinomiali invertibili su questo anello ha ordine $2^{\binom{n^2-n+1}{}}$.

Indice

Capitolo 1

Algebre monounarie

1.1 Definizioni

Definizione 1.1. Sia X un insieme sostegno e $f : X \to X$ un'applicazione, si definisce *algebra monounaria* la struttura algebrica (X, f), con f operazione unaria su X.

Definizione 1.2. Si chiama *ordine* dell'algebra (X, f) il numero $|X|$.
L'algebra è detta *finita* se il suo ordine è finito.

Osservazione 1. Se $|X| = n$ con n finito, esistono n^n diverse applicazioni da X a se stesso e quindi n^n algebre monounarie diverse sullo stesso insieme sostegno.

1.2 Rappresentazioni

Esistono diversi modi per rappresentare un'algebra monounaria finita. Consideriamo un insieme sostegno X finito con $n \geq 1$ elementi. Identificando l'insieme con quello dei primi n numeri naturali non nulli, la nostra algebra monounaria (X, f) si può rappresentare come segue:

- *Scrittura a due righe*

$$\begin{pmatrix} 1 & 1 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

- *Scrittura vettoriale*

$$\Big(f(1), \dots, f(n)\Big)$$

- *Scrittura matriciale*

$$m_{ij} = \begin{cases} 1 & \text{se } \ f(i) = j \\ 0 & \text{altrimenti} \end{cases}$$

  $M_f = [M_{ij}]$ di ordine n è detta *matrice di incidenza* di f tra X e se stesso.

Un'altra rappresentazione utile è quella geometrica attraverso l'uso di grafi orientati. Essa consiste nell'associare ad ogni algebra monounaria finita (X, f) un grafo orientato che si indica generalmente con $\Gamma = \Gamma(X, f)$ i cui vertici rappresentano gli elementi di X e le frecce che collegano i vertici sono tali che: dati x e $y \in X$, $x \to y \Leftrightarrow y = f(x)$. Poiché la freccia che unisce due nodi rappresenta la funzione f che caratterizza l'algebra, da ogni vertice uscirà una e una sola freccia. Partendo da un elemento $x_0 \in X$ e iterando l'applicazione di f si ottiene una successione finita di elementi di X

$$x_0 \to f(x_0) = x_1 \to \dots \to x_i \to \dots \to x_{j+1} = f(x_j)$$

tale che l'ultimo termine è uguale a un elemento di X già incontrato; sia x_i tale elemento. Si genera così un albero costituito dal *circuito* $x_i \dots x_j$ a cui è attaccato il cosidetto *co-albero* $x_0, x_1, \dots x_{i-1}$ che si innesta nell'elemento x_i. Prendendo poi un elemento non ancora incontrato e ripetendo il procedimento possiamo avere tre diverse situazioni:

- ritroviamo l'elemento x_k, $k \leq i - 1$ e quindi ingrandiamo l'albero;

- ritroviamo lo stesso circuito e costruiamo così un nuovo co-albero;

- incontriamo un nuovo circuito.

Nell'ultimo caso siamo di fronte a un'algebra costituita da più componenti connesse.
Il rango $r(f)$ dell'algebra (X, f) è il numero di tali componenti.

Definizione 1.3. Sia (X, f) un algebra monounaria. Due elementi $x, y \in X$ sono detti *connessi* se esiste una sequenza finita di elementi $x = x_0, x_1, \ldots, x_n = y$ ciascuno collegato con l'elemento successivo attraverso f.
Quindi può esistere un solo $j \in \{0, 1, \ldots, n\}$ tale che

$$x = x_0 \to x_1 \to \ldots \to x_j \leftarrow \ldots \leftarrow x_n = y$$

altrimenti avrei che da un x si ottengono due diversi valori per $f(x)$, cosa che contraddice il concetto di funzione.

Si dimostra che la relazione di connessione è una relazione d'equivalenza le cui classi sono dette *componenti connesse*.

Osservazione 2. Le classi d'equivalenza della connessione sono proprio le componenti del grafo.

Esempio 1.1. Sia (X, f) un algebra monounaria con $X = \mathbb{Z}_5$ e $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ tale che $f(x) = x^3 - 4$, dalle rappresentazioni viste otteniamo:

- Scrittura a due righe

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 & 0 \end{pmatrix}$$

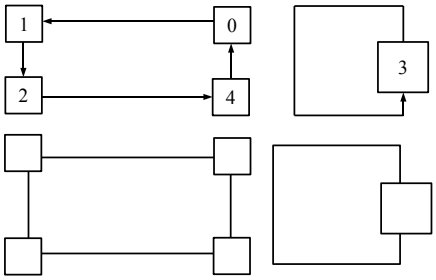
- Scrittura vettoriale

$$(1, 2, 4, 3, 0)$$

- Scrittura matriciale

$$M_f = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- Grafo



Per la lettura del grafo stilizzato si usano le seguenti convenzioni:

- i cicli sono orientati in senso antiorario;
- i co-alberi sono orientati verso il ciclo a cui sono connessi.

1.3 Algebre monounarie e grafi

A ogni algebra monounaria (X, f) è quindi possibile associare un grafo orientato $\Gamma = \Gamma(X, f)$ tale che:

1. Ogni vertice di Γ ha grado 1 in uscita;
2. I punti uniti di f ($f(x) = x$) sono rappresentati da un cappio;
3. I circuiti sono i cicli $C_{0,d}$ (vedi osservazione 3).

Inversamente, dato un grafo Γ che gode della prima proprietà, se indichiamo con X l'insieme dei vertici e poniamo $y = f(x)$ se $x \to y$, allora (X, f) è un algebra monounaria con $\Gamma = \Gamma(X, f)$ il suo grafo associato.

Definizione 1.4. • Due algebre monounarie (X, f) e $\left(X', f'\right)$ si dicono *isomorfe* se esiste una biezione $\Phi : X \to X'$ tale che $\forall x \in X$ $\Phi(f(x)) = f'(\Phi(x))$.

- Due grafi Γ, Γ' sono detti *isomorfi* se esiste una biezione ϕ tra i loro nodi, tale che per ogni coppia di nodi $x, y \in \Gamma$ si abbia $x \to y \Leftrightarrow \phi(x) \to \phi(y)$.

Proposizione 1.3.1. *Due algebre monounarie* $(X, f), \left(X', f'\right)$ *sono isomorfe se e solo se lo sono i rispettivi grafi* $\Gamma(X, f), \Gamma\left(X', f'\right)$

Dimostrazione. Sia $\Phi : X \to X'$ l'isomorfismo tra le algebre e $y = f(x)$. Poiché Φ è un isomorfismo vale $\Phi(f(x)) = f'(\Phi(x))$ che esprime la relazione $x \to y \Leftrightarrow \Phi(x) \to \Phi(y)$. Quindi $\phi = \Phi$ è un'isomorfismo tra i grafi.
Viceversa sia ϕ la biezione tale che per ogni $x, y \in \Gamma \quad x \to y \Leftrightarrow \phi(x) \to \phi(y)$, allora vale che $y = f(x) \Leftrightarrow \phi(f(x)) = f(\phi(x))$; quindi $\Phi = \phi$ è un isomorfismo tra le algebre.

Osservazione 3. Siano $0 \leq m \leq \infty$ e $1 \leq d \leq \infty$. Si indicano con $C_{m,d}$ le algebre monounarie isomorfe alle seguenti:

- Le algebre $C_{\infty,\infty}$ sono tutte quelle isomorfe a $(\mathbb{Z}, s)$ con $s(x) = x + 1$ (s è biettiva);

- Le algebre $C_{0,\infty}$ sono tutte quelle isomorfe a $(\mathbb{N}, s)$ con $s(x) = x + 1$ (s è iniettiva e $Im(s) = \mathbb{N} - \{0\}$);

- Le algebre $C_{m,d}$ con $0 \leq m \leq \infty$ e $1 \leq d < \infty$ sono tutte quelle isomorfe a $(\{x \in \mathbb{Z} | -m \leq x \leq d-1\}, \psi)$ con $\psi(x) = \begin{cases} x+1 & \text{se } x < d-1 \\ 0 & \text{se } x = d-1 \end{cases}$

  - Nel caso in cui $m = 0$ le algebre di tipo $C_{0,d}$ sono dette *cicli* e in tal caso ψ è una permutazione ciclica di lunghezza d.

  - Se $m > 0$ allora 0 è l'unico elemento con due preimmagini.
    Sul sottoinsieme $0, \ldots, d-1$ l'applicazione ψ agisce come un ciclo di lunghezza d. Se $d = 1$, 0 è un punto unito per ψ.
    Se $0 < m < \infty$ allora $Im(\psi) = \{-m+1, \ldots, d-1\}$, mentre se $m = \infty$ allora ψ è suriettiva.

- Le algebre $C_{m,\infty}$ del tipo $(\{x \in \mathbb{Z} | -m \leq x\}, s)$ con $s(x) = s+1$ sono tutte isomorfe a $C_{0,\infty}$.

Definizione 1.5. Supponiamo $X = X' = \{1, 2, \ldots, n\}$.
Si dice che due applicazioni $f, g : X \to X$ sono *coniugate* se esiste $\alpha \in S_n$ tale che $g = \alpha^{-1} \circ f \circ \alpha$.

Osservazione 4. Segue che due algebre monounarie $(X, f), (X, g)$ sono isomorfe se e solo se f e g sono coniugate.

1.4 Prodotto diretto

Definizione 1.6. Siano (X, f) e (Y, g) due algebre monounarie. E' possibile definire una nuova algebra $(X \times Y, f \times g)$ ponendo $(f \times g)(x, y) = (f(x), g(y))$ che viene detta *prodotto diretto* delle due algebre.

Osservazione 5.

- il prodotto diretto di algebre monounarie è un algebra monounaria;
- se ϕ è un isomorfismo tra (X, f) e $\left(X', f'\right)$ e ψ è un isomorfismo tra (Y, g) e $\left(Y', g'\right)$ allora la funzione $\phi \times \psi : X \times Y \to X' \times Y'$ è un isomorfismo tra le due algebre prodotto diretto;
- si ha che $|X \times Y| = |X| \cdot |Y|$;
- siano M_f e M_g le matrici di incidenza delle due algebre, si vede che la matrice del prodotto risulta essere il prodotto di Kronecker di M_f e M_g, cioè $M_{f \times g} = M_f \otimes M_g$[1];

[1]Se A è una matrice $m \times n$ e B è una matrice $p \times q$ allora il loro prodotto di Kronecker $A \otimes B$ è una matrice $mp \times nq$ definita a blocchi come segue

$$A \otimes B = \begin{pmatrix} a_{1,1}B & \ldots & a_{1,n}B \\ \vdots & \ddots & \vdots \\ a_{m,1}B & \ldots & a_{m,n}B \end{pmatrix}$$

- se f e $f^{'}$ sono permutazioni, anche $f \times f^{'}$ lo è;
- la connessione non si conserva per prodotti diretti.

Teorema 1.4.1. *Siano* (X, f) *e* $\left(X^{'}, f^{'}\right)$ *due algebre monounarie con* f *e* $f^{'}$ *biettive e sia* $\left(X \times X^{'}, \Phi\right)$ *il loro prodotto diretto, si dimostra che:*

1. *se* f *e* $f^{'}$ *sono cicli di lunghezza* $m = |X|$ *e* $n = \left|X^{'}\right|$ *e* $d = (m, n)$, *allora* Φ *è prodotto di* d *cicli di lunghezza* $mcm\,(m, n)$. *Se* $d = 1$ *allora* Φ *è un ciclo di lunghezza* mn.
2. *se* $f = c_1 \circ \ldots \circ c_m$ *e* $f^{'} = c_1^{'} \circ \ldots \circ c_n^{'}$ *cicli disgiunti, allora* $\Phi = \circ \left\{\left(c_i \times c_j^{'}\right) | 1 \leq i \leq m,\ \ 1 \leq j \leq n\right\}$.

Capitolo 2

Richiami sugli anelli

Definizione 2.1. Un *anello* è costituito da un insieme sostegno A sul quale sono definite due operazioni binarie:
$+ : A \text{ x } A \to A$ detta somma o addizione
$\cdot : A \text{ x } A \to A$ detta prodotto o moltiplicazione
tali che:

1. $(A, +)$ sia un gruppo abeliano, cioè:

   - L'addizione è associativa:
     $\forall a, b, c \in A \quad (a + b) + c = a + (b + c)$
   - 0 è l'elemento neutro per l'addizione:
     $\exists\, 0 \in A$ tale che $\forall a \in A \quad a + 0 = 0 + a = a$
   - Ogni elemento ha l'opposto:
     $\forall a \in A \quad \exists\, a' \in A$ tale che $a + a' = 0$
   - L'addizione è commutativa:
     $\forall a, b \in A \quad a + b = b + a$

2. $(A, \cdot, 1_A)$ sia un monoide, cioè:

   - La moltiplicazione è associativa:
     $\forall a, b, c \in A \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$

- 1 è l'elemento neutro per la moltiplicazione:
  $\forall a \in A \quad a \cdot 1 = 1 \cdot a = a$

3. La moltiplicazione è distributiva rispetto all'addizione:
   $\forall a, b, c \in A \quad (a+b) \cdot c = (a \cdot c) + (b \cdot c) \quad \text{e} \quad c \cdot (a+b) = (c \cdot a) + (c \cdot b)$

Se l'operazione $\cdot$ è commutativa, cioè vale $\forall a, b \in A \quad a \cdot b = b \cdot a$ allora l'anello $(A, +, \cdot, 1_A)$ si dice commutativo.

Esempio 2.1. $(\mathbb{Z}, +, \cdot, 1)$, $(\mathbb{Q}, +, \cdot, 1)$, $(\mathbb{R}, +, \cdot, 1)$, $(\mathbb{Z}_m, +, \cdot, [1]_m)$ con $m \in \mathbb{Z}$ sono tutti anelli commutativi.

Riportiamo di seguito alcune proprietà degli anelli e altri risultati che utilizzeremo nel corso di questa trattazione, omettendone le dimostrazioni. Per queste si rimanda al testo [1] o ad un qualunque testo di Algebra I.

Sia $(A, +, \cdot, 1_A)$ un anello commutativo, vale che:

- 0_A è elemento assorbente:
  $\forall a \in A \quad 0_A \cdot a = a \cdot 0_A = 0_A$
- 0_A e 1_A sono univocamente determinati
- vale la legge di cancellazione:
  $\forall a, b, c \in A \quad a + b = a + c \Rightarrow b = c$
- $\forall a \in A \quad (-1_A) \cdot a = -a$
- vale la regola dei segni.

Definizione 2.2. Sia $(A, +, \cdot, 1_A)$ un anello commutativo.
Un elemento $b \in A$ è detto *invertibile* se $\exists b' \in A$ tale che $b \cdot b' = b' \cdot b = 1_A$; b' viene detto *inverso* o *unità* di b.

Esempio 2.2. In $\mathbb{Z}$ solo 1 e -1 sono elementi invertibili mentre in $\mathbb{Q}$ tutti gli elementi non nulli sono unità.

Osservazione 6. L'insieme degli elementi invertibili di un anello $(A, +, \cdot, 1_A)$, solitamente indicato con A^*, forma un gruppo con l'operazione di prodotto detto *gruppo moltiplicativo* di A.

Definizione 2.3. Un anello commutativo in cui ogni elemento non nullo è invertibile si chiama *campo*.

Definizione 2.4. Sia $(A, +, \cdot, 1_A)$ un anello commutativo. Un elemento $a \in A$, $a \neq 0_A$ è un *divisore dello zero* se esiste $b \in A$, $b \neq 0_A$ tale che $a \cdot b = 0_A$.

Definizione 2.5. Un anello senza divisori dello zero viene detto *dominio di integrità*.

Osservazione 7.

- Un campo è sempre un dominio di integrità.

- Un dominio di integrità finito è sempre un campo.

Definizione 2.6. Sia $(A, +, \cdot, 1_A)$ un anello commutativo e sia $B \subset A$ un suo sottoinsieme.
Si dice che B è un *sottoanello* di A se:

1. $0_A,\ 1_A \in B$
2. $\forall a \in B \quad -a \in B$
3. $\forall a, b \in B \quad a + b,\ a \cdot b \in B$

Esempio 2.3. $\mathbb{Z}$ è sottoanello di $\mathbb{Q}$ e quest'ultimo è a sua volta sottoanello di $\mathbb{R}$.

Definizione 2.7. Sia $(A, +, \cdot, 1_A)$ un anello. L'insieme $< 1_A >= \{n \cdot 1_A / n \in \mathbb{Z}\}$ è detto *sottoanello fondamentale* di A.

Osservazione 8. Si dimostra facilmente che $< 1_A >$ è un sottoanello di A.

Definizione 2.8. Sia $(A, +, \cdot, 1_A)$ un anello.

- Se $| < 1_A > | = n \in \mathbb{N}$ allora si dice che l'anello ha *caratteristica* n.

- Se $| < 1_A > |$ è infinito allora si dice che l'anello ha *caratteristica* zero.

Definizione 2.9. Siano $(A, +_1, \cdot_1, 1_A)$ e $(B, +_2, \cdot_2, 1_B)$ due anelli.
Si definisce *prodotto diretto* di A e B, la struttura che si ottiene munendo il prodotto cartesiano $A \times B$ delle operazioni $+, *$ definite da:

- $(a_1, b_1) + (a_2, b_2) := (a_1 +_1 a_2, b_1 +_2 b_2)$
- $(a_1, b_1) * (a_2, b_2) := (a_1 \cdot_1 a_2, b_1 \cdot_2 b_2)$

con $a_1, a_2 \in A$ e $b_1, b_2 \in B$

Osservazione 9. Si dimostra che il prodotto diretto di anelli è ancora un anello con unità $(1_A, 1_B)$.

D'ora in poi, per comodità, indicheremo con A l'anello commutativo $(A, +, \cdot, 1_A)$, con 1 l'elemento neutro della moltiplicazione, con 0 l'elemento neutro dell'addizione e con ab il prodotto $a \cdot b$.

2.1 Ideali

Definizione 2.10. Sia I un sottoinsieme di un anello A. I viene detto:

- *ideale destro* di A se
  1. I è un sottogruppo additivo di A, cioè un gruppo additivo rispetto alla somma di A
  2. $\forall s \in I$ e $\forall a \in A \quad sa \in I$
- *ideale sinistro* di A se
  1. I è un sottogruppo additivo di A, cioè un gruppo additivo rispetto alla somma di A
  2. $\forall s \in I$ e $\forall a \in A \quad as \in I$.

Se I è sia ideale destro che sinistro, viene detto *bilaterale*.
Nel caso particolare in cui A è un anello commutativo, le due condizioni sono equivalenti e così si parla semplicemente di *ideale*.

Definizione 2.11. Un ideale I di A si dice *proprio* se $I \neq A$.

Definizione 2.12. Sia a un elemento di A anello commutativo. Si chiama *ideale generato* da a l'insieme dei multipli di a:

$$(a) = Aa = \{sa | s \in A\}$$

Proposizione 2.1.1. *Si dimostra che l'ideale generato da a è il più piccolo ideale contenente a.*

Lemma 2.1.2. *Sia I un ideale di un anello commutativo A. Allora sono equivalenti le seguenti condizioni:*

1. $I = A$
2. $1 \in I$
3. *I contiene un'unità*

In particolare per ogni elemento $a \in A$ si ha che $(a) = A$ se e solo se a è un'unità in A.

Definizione 2.13. Sia A una anello commutativo e I un ideale di A. Se esiste $a \in A$ tale che $I = (a)$, allora I è detto ideale *principale*.

Definizione 2.14. Siano $a_1, a_2, \ldots, a_n$ elementi di un anello commutativo A. Si chiama *ideale generato* da $a_1, \ldots, a_n$ l'insieme delle combinazioni lineari di $a_1, \ldots, a_n$, ossia:

$$(a_1, \ldots, a_n) = \{s_1 a_1 + \ldots + s_n a_n | s_1, \ldots, s_n \in A\}$$

Proposizione 2.1.3. *Si dimostra che l'ideale generato da $a_1, \ldots, a_n$ è un ideale ed è contenuto in qualsiasi ideale che contiene tutti gli $a_1, \ldots, a_n$.*

Definizione 2.15. Sia I un ideale di un anello commutativo A. I si dice ideale *massimale* se per ogni ideale J di A tale che $I \subseteq J \subseteq A$, si ha $I = J$ oppure $J = A$.

Esempio 2.4. Nell'anello commutativo $\mathbb{Z}$, l'ideale (p), con p primo, è un ideale massimale.
Infatti sia J un ideale di $\mathbb{Z}$ tale che $(p) \subset J \subseteq \mathbb{Z}$, allora esiste un elemento $a \in J \backslash (p)$. Dunque J contiene tutti i numeri della forma $ka+sp$ con $k, s \in \mathbb{Z}$. Ma poiché $1 = MCD\,(a, p)$, 1 si può scrivere come combinazione lineare di a e p, quindi $1 \in J$. Allora per il lemma 2.1.2 $J = \mathbb{Z}$.

Proposizione 2.1.4. *Sia A un anello commutativo non nullo. Allora A è un campo se e solo se gli unici ideali di A sono l'ideale nullo e A.*

Teorema 2.1.5. *Sia A un anello commutativo e I un ideale di A, allora l'anello quoziente A/I[1] è un campo se e solo se I è un ideale massimale.*

2.2 Omomorfismo di anelli

Definizione 2.16. Siano A, B due anelli.
Un omomorfismo di anelli è una funzione $\varphi : A \to B$ tale che:

1. $\forall a, b \in A \quad \varphi\,(a + b) = \varphi\,(a) + \varphi\,(b)$ in B
2. $\forall a, b \in A \quad \varphi\,(a \cdot b) = \varphi\,(a) \cdot \varphi\,(b)$ in B
3. $\varphi\,(1_A) = 1_B$ con $1_A, 1_B$ le unità moltiplicative di A e B.

La proprietà 1. dice che φ è un omomorfismo di gruppi e quindi vale che:

Lemma 2.2.1.
- $\varphi\,(0_A) = 0_B$
- $\forall a \in A \quad \varphi\,(-a) = -\varphi\,(a)$

[1] A/I è l'insieme dei laterali $I + a$ di I in A, ottenuto considerando I come sottogruppo additivo di A. Poiché $(A, +)$ è abeliano l'insieme dei laterali destri coincide con quello dei laterali sinistri.

Definizione 2.17. Un omomorfismo di anelli $\varphi : A \to B$ è detto:

- *monomorfismo* se è iniettivo, cioè se $\varphi(a) = \varphi(b) \Rightarrow a = b \quad \forall a, b \in A$
- *epimorfismo* se è suriettivo, cioè se $\forall b \in B \quad \exists a \in A$ tale che $\varphi(a) = b$.

Definizione 2.18. Sia $\varphi : A \to B$ un omomorfismo di anelli. Si definisce:

- *nucleo* di φ l'insieme $\quad Ker\varphi = \{x \in A | \varphi(x) = 0_B\}$
- *immagine* di φ l'insieme $\quad Im\varphi = \{\varphi(a) | a \in A\} = \varphi(A)$

Proposizione 2.2.2. *Sia $\varphi : A \to B$ un omomorfismo di anelli; si dimostra:*

1. *$Ker\varphi$ è un ideale di A;*
2. *$Im\varphi$ è un sottoanello di B.*

Proposizione 2.2.3. *Sia $\varphi : A \to B$ un omomorfismo di anelli.*
φ è iniettivo se e solo se $Ker\varphi = \{0\}$

Dimostrazione.
- Sia φ iniettivo.
  Sia $x \in Ker\varphi$, allora $\varphi(x) = 0_B = \varphi(0_A)$ quindi $x = 0_A$.
- Supponiamo $Ker\varphi = \{0\}$.
  Sia $\varphi(x) = \varphi(y)$, con $x, y \in A$, allora $0 = \varphi(x) - \varphi(y) = \varphi(x - y)$, quindi $x - y \in Ker\varphi$. Segue che $x - y = 0$ cioè $x = y$ e quindi φ è iniettiva.

Definizione 2.19. Si definisce *isomorfismo* un omomorfismo di anelli iniettivo e suriettivo.
Se esiste un isomorfismo $\varphi : A \to B$, allora A e B sono detti *isomorfi* ($A \cong B$).

Osservazione 10.
- L'identità da un anello a se stesso è un isomorfismo;
- L'inverso di un isomorfismo è un isomorfismo;
- La composizione di due isomorfismi è un isomorfismo.

Proposizione 2.2.4. *Sia $\varphi : A \to B$ un omomorfismo di anelli, I un ideale di A e J un ideale di B. Si ha che:*

1. *$\varphi(I)$ è un ideale di B se φ è suriettivo;*
2. *$\varphi^{-1}(J)$ è un ideale di A.*

Proposizione 2.2.5. *Siano A_1, A_2 due anelli. Allora le funzioni*
$\pi_1 : A_1 \times A_2 \to A_1$ con $\pi_1(a_1, a_2) \mapsto a_1$
$\pi_2 : A_1 \times A_2 \to A_2$ con $\pi_2(a_1, a_2) \mapsto a_2$
sono omomorfismi suriettivi di anelli.
Vengono chiamate prima e seconda proiezione *di $A_1 \times A_2$ sui suoi fattori.*

Teorema 2.2.6. *Sia $\varphi : A \to B$ un omomorfismo di anelli. Allora esiste un isomorfismo di anelli $\psi : A/Ker(\varphi) \to \varphi(A)$ con $\psi([x]) = \varphi(x)$.*

Teorema 2.2.7. *Siano A_1 e A_2 due anelli e I ideale dell'anello prodotto $A_1 \times A_2$.*
Si dimostra che esistono due ideali I_1 di A_1 e I_2 di A_2 tali che $I = I_1 \times I_2$

Dimostrazione. Sia $I_1 = \pi_1(I)$ e $I_2 = \pi_2(I)$, con π_1 e π_2 le proiezioni di $A_1 \times A_2$ su A_1 e A_2. Poiché le proiezioni sono degli omomorfismi suriettivi, per la prop 2.2.4 si ha che I_1 è ideale di A_1 e I_2 è ideale di A_2.
Resta da far vedere che $I = I_1 \times I_2$.

- Mostriamo che $I \subseteq I_1 \times I_2$:
  $\forall (a_1, a_2) \in I$ si ha $a_1 = \pi_1((a_1, a_2)) \in I_1$ e $a_2 = \pi_2((a_1, a_2)) \in I_2$.
- Mostriamo che $I_1 \times I_2 \subseteq I$:
  se $(a_1, a_2) \in I_1 \times I_2$, per la definizione di I_1 e I_2 esistono $k \in A_1$ e $h \in A_2$ tali che $(a_1, h), (k, a_2) \in I$. Poiché I è ideale di $A_1 \times A_2$ si ha che $(a_1, h)(1_{A_1}, 0_{A_2}) + (k, a_2)(0_{A_1}, 1_{A_2}) = (a_1, a_2) \in I$.

Teorema 2.2.8. *Siano A_1 e A_2 due anelli e $I = I_1 \times I_2$ un ideale dell'anello prodotto $A_1 \times A_2$. Si dimostra che*

$$(A_1 \times A_2)/I = (A_1 \times A_2)/(I_1 \times I_2) \cong A_1/I_1 \times A_2/I_2.$$

Dimostrazione. Consideriamo la funzione $\varphi : A_1 \times A_2 \to A_1/I_1 \times A_2/I_2$ tale che $\varphi(a_1, a_2) \mapsto (a_1 + I_1, a_2 + I_2)$ e mostriamo che è un omomorfismo.
Siano $(a_1, a_2), (a_1', a_2') \in A_1 \times A_2$

- $\varphi((a_1, a_2) + (a_1', a_2')) = \varphi(a_1 + a_1', a_2 + a_2') = ((a_1 + a_1') + I_1, (a_2 + a_2') + I_2) = (a_1 + I_1, a_2 + I_2) + (a_1' + I_1, a_2' + I_2) = \varphi((a_1, a_2)) + \varphi((a_1', a_2'))$
- $\varphi((a_1, a_2)(a_1', a_2')) = \varphi(a_1a_1', a_2a_2') = ((a_1a_1') + I_1, (a_2a_2') + I_2) = (a_1 + I_1, a_2 + I_2)(a_1' + I_1, a_2' + I_2) = \varphi((a_1, a_2))\varphi((a_1', a_2'))$
- $\varphi((1, 1)) = (1 + I_1, 1 + I_2)$

Ora $(a_1, a_2) \in Ker\varphi \Leftrightarrow \varphi((a_1, a_2)) = (0 + I_1, 0 + I_2) \Leftrightarrow (a_1, a_2) \in I_1 \times I_2$.
Quindi $Ker\varphi = I_1 \times I_2$.
Ma allora per il teorema 2.2.6 esiste un isomorfismo tra $(A_1 \times A_2) / (I_1 \times I_2)$ e $\varphi(A_1 \times A_2)$.
Sia ora $(a_1 + I_1, a_2 + I_2) \in A_1/I_1 \times A_2/I_2$, allora $\varphi(a_1, a_2) = (a_1 + I_1, a_2 + I_2)$, quindi φ è un omomorfismo suriettivo.
Allora $\varphi(A_1 \times A_2) = A_1/I_1 \times A_2/I_2$ e quindi $(A_1 \times A_2) / (I_1 \times I_2) \cong A_1/I_1 \times A_2/I_2$.

2.3 L'anello $\mathbb{Z}_m$

Definizione 2.20. Siano $a, b \in \mathbb{Z}$ e $m \in \mathbb{Z}$, $m \neq 0$ detto *modulo*. Diciamo che a e b sono *congrui modulo* m, $a \equiv b \pmod m$, se $a - b$ è divisibile per m. Equivalentemente diciamo $a \equiv b \pmod m$ se a e b differiscono per un multiplo di m, cioè se esiste un $k \in \mathbb{Z}$ tale che $a = b + km$.

Osservazione 11. Dire che a è congruo a 0 mod m è equivalente a dire che a è divisibile per m.

Proposizione 2.3.1. *Si dimostra che la relazione di congruenza è una relazione d'equivalenza.*

Lemma 2.3.2. *Sia $a \in \mathbb{Z}$ e $m \in \mathbb{Z}$, $m \neq 0$. Esiste un unico $r \in \mathbb{Z}$, $0 \leq r < m$ tale che $a \equiv r \pmod{m}$.*
Questo r viene detto resto di a modulo m *ed è il resto della divisione di a per m.*

Dimostrazione. Supponiamo che esistano $r, s \in \mathbb{Z}$, $0 \leq r \leq s < m$ tale che $a \equiv r \pmod{m}$ e $a \equiv s \pmod{m}$, allora per le proprietà simmetrica e transitiva si ha $r \equiv s \pmod{m}$; allora $0 \leq s-r < m$ e quindi $s-r$ è multiplo di m se e solo se $s - r = 0$ cioè $s = r$.

Vediamo ora alcune proprietà della relazione di congruenza:

1. Se $a \equiv b \pmod{m}$ e $k \in \mathbb{Z}$, allora $a + k \equiv b + k \pmod{m}$ e $ka \equiv kb \pmod{m}$.
2. Se $ka \equiv kb \pmod{m}$ e $(k, m) = 1$, allora $a \equiv b \pmod{m}$.
3. Se $a \equiv b \pmod{m}$ e $a' \equiv b' \pmod{m}$, allora $a + a' \equiv b + b' \pmod{m}$ e $aa' \equiv bb' \pmod{m}$.
4. Se $a \equiv b \pmod{m}$ e $n > 0$, allora $a^n \equiv b^n \pmod{m}$.
5. Se $a \equiv b \pmod{m}$, allora $-a \equiv -b \pmod{m}$.

D'ora in poi, dove risulta chiaro, indicheremo $[a]_m$ semplicemente con $[a]$ o con a.

2.3.1 Classi di congruenza

Abbiamo visto quindi che la relazione di congruenza modulo un intero positivo m è una relazione di equivalenza sull'insieme degli interi e quindi dividerà gli interi in classi di equivalenza dette *classi di congruenza*.

Definizione 2.21. Se a è un intero, la classe di congruenza di a modulo m è $[a]_m = \{x \in \mathbb{Z} | x \equiv a \pmod{m}\} = \{a + km | k \in \mathbb{Z}\}$.

Osservazione 12. Ogni intero sta in un'unica classe di congruenza.

Lemma 2.3.3. *Ogni classe di congruenza modulo m contiene uno e un solo intero r con $0 \leq r < m$.*

Corollario 2.3.4. *Esistono esattamente m classi di congruenza modulo m, cioè $[0]_m, [1]_m, \ldots, [m-1]_m$.*

L'insieme delle classi di congruenza modulo m viene indicato con $\mathbb{Z}_m$ ed è possibile definire su questo insieme le operazioni di *somma* e *prodotto*.

Definizione 2.22. Siano α e β due classi di congruenza modulo m. Siano poi $a, b \in \mathbb{Z}$ tali che $\alpha = [a]$ e $\beta = [b]$; allora la somma e prodotto delle classi α e β sono definiti nel seguente modo:

$$\alpha + \beta = [a] + [b] = [a + b] \qquad \alpha\beta = [a]\,[b] = [ab]$$

e l'*opposto* di α è definito $-\alpha = [-a]$.

Osservazione 13. Con le operazioni di somma e prodotto $(\mathbb{Z}_m, +, \cdot, [1]_m)$ è un anello commutativo.

Proposizione 2.3.5. *Sia $\alpha = [a]$ un elemento dell'anello $\mathbb{Z}_m$.*
Allora esiste un β tale che $\alpha \cdot \beta = [1]$ se e solo se $(a, m) = 1$

Dimostrazione. Sia $\beta = [b] \in \mathbb{Z}_m$ tale che $[a]\,[b] = [1]$ allora esiste un intero q tale che $ab = 1 + qm$ quindi $MCD\,(a, m) = 1$.
Viceversa se $MCD\,(a, m) = 1$, per l'identità di Bèzout, esistono b, r interi tali che $ab + mr = 1$, cioè in $\mathbb{Z}_m$ vale $[a]\,[b] = [1]$.

Se p è un primo, allora ogni intero non divisibile per p è relativamente primo a p. Si ha quindi:

Proposizione 2.3.6. *Se p è un primo, ogni elemento di $\mathbb{Z}_p$ è invertibile.*
Allora $(\mathbb{Z}_p, +, \cdot, 1_p)$ con p primo, è un campo.

Proposizione 2.3.7. *Sia $[a] \in \mathbb{Z}_m$. Allora $[a]$ non è un divisore dello zero se e solo se $MCD\,(a, m) = 1$.*

Capitolo 3

Polinomi e funzioni polinomiali

I polinomi possono essere visti dal punto di vista formale o dal punto di vista funzionale. Nel primo caso si parla di polinomi formali , mentre nel secondo di funzioni polinomiali .

3.1 Polinomi formali

Prendiamo in esame i polinomi in una indeterminata.

Definizione 3.1. Sia A un anello commutativo e sia x un simbolo.
Un *polinomio* in x a coefficienti in A è un'espressione del tipo

$$f = f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots = \sum a_i x^i$$

dove gli a_i sono elementi di A detti *coefficienti di grado i* di f e sono tali che solo un numero finito di essi è diverso da 0; x è detto *indeterminata*. L'insieme dei polinomi in x a coefficienti in A si indica con $A[x]$.

I polinomi in $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ si diranno rispettivamente polinomi *interi, razionali, reali, complessi*.

Sia g un altro polinomio in x a coefficienti in A,

$$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n + \ldots = \sum b_i x_i$$

Allora $f(x) = g(x)$ se e solo se $\forall i \geq 0 \quad a_i = b_i$.

Definizione 3.2. Si chiama *polinomio nullo* il polinomio con i coefficienti tutti nulli e si indica con 0.
Si chiama polinomio *costante* un polinomio che abbia i coefficienti di grado positivo tutti nulli $f_c(x) = c + 0x + 0x^2 + \ldots$. Questo polinomio si può anche pensare come elemento di A.
Si chiama *monomio* un polinomio che ha solo un termine non nullo.

Definizione 3.3. Sia $f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + \ldots \in A[x]$ un polinomio non nullo. Viene detto *grado* del polinomio f e si indica con $deg(f)$, il più grande numero intero non negativo i tale che $a_i \neq 0$. In tal caso a_i è detto *coefficiente direttore* di f.
Un polinomio non nullo con coefficiente direttore uguale a 1 è detto *polinomio monico*.
Sia f il polinomio nullo; allora per convenzione si pone $deg(f) = -\infty$.

Dal punto di vista formale, assegnare un polinomio a coefficienti in A, $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ equivale ad assegnare la sequenza ordinata dei suoi coefficienti $a_0, a_1, \ldots a_n$. Quindi è possibile vedere un polinomio come la successione $(a_0, a_1, \ldots, a_n, \ldots)$ dei suoi coefficienti nella quale i termini da un certo indice in poi sono tutti nulli.

Definizione 3.4. Si definisce *polinomio formale* a coefficienti in un anello commutativo A, la successione $\mathbb{N} \to A$ *definitivamente nulla*. In particolare il polinomio $(0, 1, 0, \ldots, 0, \ldots)$ è l'indeterminata x.

Definiamo ora la somma e il prodotto di polinomi, in modo che $A[x]$ divenga un anello commutativo contenente A come sottoanello.
Richiediamo inoltre che la potenza n-esiama dell'elemento x sia il polinomio x^n e che il prodotto di un polinomio costante a con il polinomio x^n sia il polinomio ax^n:

Definizione 3.5. Siano $f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ e $g = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$ due polinomi a coefficienti nell'anello A, e sia ad esempio $m \geq n$. Si definisce:

- Somma di f e g:
  $f + g = (a_0 + b_0) + (a_1 + b_1) x + (a_2 + b_2) x^2 + \ldots + (a_n + b_n) x^n + b_{n+1} x^{n+1} + \ldots + b_m x^m$
  con l'i-esimo coefficiente dato da $(f + g)_i = a_i + b_i$.

- Prodotto di f e g:
  $fg = (a_0 b_0) + (a_1 b_0 + a_0 b_1) x + (a_2 b_0 + a_1 b_1 + a_0 b_2) x^2 + (a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3) x^3 + \ldots$
  con l'i-esimo coefficiente dato da $(fg)_i = \sum_{j+k=i} a_j b_k$.

Proposizione 3.1.1. *L'insieme $A[x]$ con le operazioni di somma e prodotto, con i polinomi 0 e 1 come zero e come identità, forma un anello commutativo. L'opposto di un polinomio f è definito da $(-f)_i = -(f_i)$.*
Inoltre si ha che la funzione $\varphi : A \to A[x]$ tale che $\varphi(a) = a + 0x + 0x^2 + \ldots$ è un monomorfismo di anelli, la cui immagine è un sottoanello isomorfo ad A.

Osservazione 14. Siano $f, g \in A[x]$ due polinomi allora:

- $deg(f + g) \leq max(deg(f), deg(g))$
- $deg(f - g) \leq max(deg(f), deg(g))$
- $deg(fg) \leq deg(f) + deg(g)$

Se A è un dominio di integrità allora:

- $deg(fg) = deg(f) + deg(g)$
- il coefficiente direttore di fg è il prodotto dei coefficienti direttori di f e di g; in particolare il prodotto di polinomi monici è un polinomio monico.

Proposizione 3.1.2. *Sia A un anello commutativo. Allora $A[x]$ è un dominio di integrità se e solo se lo è A.*

Dimostrazione. Se $A[x]$ è un dominio di integrità, essendo A il sottoanello dei polinomi costanti, allora anche A è un dominio di integrità.
Viceversa sia A un dominio di integrità. Siano $f(x), g(x) \in A[x]$ non nulli, allora $deg(fg) = deg(f) + deg(g)$, quindi fg non è il polinomio nullo. Quindi $A[x]$ è un dominio d'integrità.

Proposizione 3.1.3. *Sia A un dominio di integrità. Un polinomio in $A[x]$ è invertibile se e solo se è costante ed è invertibile come elemento di A.*

Dimostrazione. Se un polimomio costante è invertibile in A è ovviamente invertibile in $A[x]$.
Viceversa supponiamo ora che $f \in A[x]$ sia invertibile, cioè esista un $g \in A[x]$ tale che $fg = 1$. Allora $0 = deg(1) = deg(f) + deg(g)$; poiché f e g sono diversi da 0 avremo $deg(f) = deg(g) = 0$. Perciò f e g sono costanti, quindi sono in A. Allora f è invertibile come elemento di A.

In altre parole le unità di $A[x]$ sono le unità di A. Ad esempio le unità in $\mathbb{Z}[x]$ sono i due polinomi costanti 1 e -1. Questa proposizione non è vera in generale quando A non è un dominio; per esempio in $\mathbb{Z}_4[x]$ si ha $(1+2x)(1-2x) = 1 - 4x^2 = 1$, mentre $2 \neq 0$ e quindi $1 + 2x$ è invertibile senza essere costante.
Se A è un anello commutativo, si può far vedere che $A[x]$ contiene dei polinomi invertibili non costanti se e solo se A contiene degli elementi nilpotenti [1] non nulli.

Definizione 3.6. Sia A un dominio di integrità. Un polinomio $f(x) \in A[x]$ si dice *irriducibile* se ogni sua fattorizzazione $f(x) = g(x)\,h(x)$ con $g(x), h(x) \in A[x]$ è tale che uno dei due polinomi abbia grado zero.

Vediamo ora il caso particolare di polinomi definiti su un campo. Abbiamo già visto che un campo è un anello commutativo K in cui ogni elemento non nullo è invertibile, cioè $\forall a \neq 0$, $a \in K$, $\exists b \in K$ tale che $ab = 1$.

[1] Un elemento a di A si dice *nilpotente* se esiste un intero $n > 0$ tale che $a^n = 0$

Se K è un campo, allora l'insieme dei polinomi in x a coefficienti in K è un dominio di integrità, in cui gli elementi invertibili sono i polinomi costanti diversi dal polinomio nullo. (Segue dalle proposizioni 3.1.2 e 3.1.3)

Teorema 3.1.4. *(Teorema della divisione tra polinomi) Siano f e g due polinomi in $K[x]$ con K un campo e $f \neq 0$. Allora esistono due polinomi q ed r con $deg(r) < deg(f)$, tali che $g = qf + r$. Inoltre q ed r sono univocamente determinati da f e g.*
(Ovviamente f divide g in $K[x]$ se e solo se $r = 0$).

Anche in questa sezione per le dimostrazioni si rimanda al testo [1].

Osservazione 15. Il teorema della divisione per polinomi vale anche in un dominio d'integrità A, purchè il coefficiente direttore di $g(x)$ sia invertibile in A.

Definizione 3.7. Un elemento $a \in A$ con A dominio di integrità, è detto *radice* o *zero* di un polinomio $f(x) \in A[x]$ se $f(a) = 0$.

Teorema 3.1.5. *Sia $f(x)$ un polinomio con coefficienti in un dominio K e sia $a \in K$ una radice di f. Allora $x - a$ divide $f(x)$.*

Dimostrazione. Dividendo f per $x-a$, possiamo scrivere $f(x) = (x-a)\,q(x) + r(x)$, con $deg(r) < deg(x-a) = 1$. Ma allora $r(x)$ deve essere una costante che indichiamo con r. Quindi $f(x) = (x-a)\,q(x) + r$, da cui $0 = f(a) = 0 \cdot q(a) + r$, cioè $r = 0$. Quindi $(x-a)$ divide f.

Questo teorema vale anche nei domini di integrità.

Definizione 3.8. Sia A un anello e sia $f(x) = a_0 + a_1x + \ldots + a_nx^n$ un polinomio di $A[x]$.
Dato $a \in A$ possiamo definire un elemento $f(a) \in A$ come $f(a) = a_0 + a_1a + \ldots a_na^n$.

Proposizione 3.1.6. *Sia K un campo. Allora si dimostra che $K[x]$ è un anello a ideali principali; un generatore di un ideale non nullo I è un polinomio di grado minimo $\in I$.*

Proposizione 3.1.7. *Siano K un campo e $f(x)$ un polinomio in $K[x]$. Allora $K[x]/(f(x))$ è un campo se e solo se $f(x)$ è irriducibile.*

Definizione 3.9. Sia f un polinomio non nullo a coefficienti in K e sia a un elemento di K. La *molteplicità di a* come radice di f, in simboli $\mu = \mu(f, a)$, è il massimo intero non negativo tale che $(x-a)^{\mu}$ divide f.

Corollario 3.1.8. *Sia K un campo.*
Il numero delle radici di un polinomio non supera il grado.
La somma delle molteplicità delle radici non supera il grado.

3.2 Funzioni polinomiali

Definizione 3.10. Sia $A[x]$ l'anello dei polinomi in x a coefficienti nell'anello commutativo A.
Ad ogni polinomio $f \in A[x]$ possiamo associare una funzione $\widetilde{f} : A \to A$ che associa ad ogni $a \in A$ la valutazione $f(a)$ di $f(x)$ in a.
Le funzioni così ottenute sono dette *funzioni polinomiali*.

Sia F l'insieme di tutte le funzioni polinomiali di A in se stesso.
E' possibile definire in tale insieme le operazioni di somma e prodotto, tenendo conto delle operazioni definite su A:

- $(p+q)(a) = p(a) + q(a)\ \forall a \in A$
- $(pq)(a) = p(a)\, q(a)\ \forall a \in A$

Due funzioni polinomiali sono uguali se assumono gli stessi valori in corrispondenza di ogni $a \in A$.

Osservazione 16. Si dimostra che F con le operazioni appena definite è un anello commutativo.

- L'elemento neutro rispetto all'addizione, lo zero, è la funzione polinomiale che associa ad ogni $a \in A$ l'elemento 0_A.

- La funzione unità di F è la funzione polinomiale che associa ad ogni $a \in A$ l'elemento 1_A, cioè la funzione costante uguale a 1_A.

- La funzione opposta di p è la funzione $-p$ tale che $(-p)(a) = -p(a)$ $\forall a \in A$.

A questo punto si pone il seguente problema:
Dati due polinomi f e $g \in A[x]$, di grado rispettivamente n e m a coefficienti nell'anello commutativo A:

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \quad g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$$

e supponendo che le funzioni polinomiali associate $\widetilde{f}$ e $\widetilde{g}$ siano uguali, si può concludere che $f = g$?
In generale la risposta è negativa. Mostriamo qualche controesempio:

Esempio 3.1. 1. Sia $A = \mathbb{Z}_2[x]$ e siano $f(x) = x$ e $g(x) = x^3$ due polinomi diversi; le funzioni polinomiali a esse associate sono invece uguali.

2. Sia $A = \mathbb{Z}_3[x]$ e sia $f = x^3 - x$ diverso dal polinomio nullo; invece la funzione polinomiale $\mathbb{Z}_3 \to \mathbb{Z}_3$ ad esso associata, assume il valore 0 per ogni $a \in \mathbb{Z}_3$ ed è quindi la funzione nulla.

Lemma 3.2.1. *Se K è un campo infinito allora $f(a) = 0$ $\forall a \in K$ se e solo se $f = 0$, cioè f è il polinomio identicamente nullo.*

Dimostrazione. Se $f = 0$ ovviamente $f(a) = 0$ $\forall a \in K$.
Viceversa se $f(a) = 0$ $\forall a \in K$, allora f avrà un numero infinito di radici ma per il corollario 3.1.8 questo può succedere solo se $f = 0$.

Teorema 3.2.2. *(Teorema di identità delle funzioni polinomiali) Sia K un campo infinito e siano $f(x)$ e $g(x)$ polinomi a coefficienti in K.*
Allora $f(x) = g(x)$ come polinomi se e solo se $f = g$ come funzioni polinomiali.

Dimostrazione.

- Se $f(x) = g(x)$ come polinomi, allora $\forall a \in K$ si ha $f(a) = g(a)$, quindi $f = g$ come funzioni polinomiali.

- Se $f(x)$ e $g(x)$ sono due polinomi e vale che $\forall a \in K \ f(a) = g(a)$ allora il polinomio $h(x) = f(x) - g(x)$ è un polinomio tale che $\forall a \in K \ h(a) = 0$. Allora per il lemma 3.2.1 $h(x)$ è il polinomio identicamente nullo. Quindi $f(x) = h(x)$ sono uguali come polinomi.

In generale si ha che se A è un anello finito non nullo allora vi saranno infiniti polinomi in $A[x]$, ma solo un numero finito di funzioni da A ad A. Perciò la corrispondenza che manda un polinomio nella funzione polinomiale non può essere iniettiva.

Lemma 3.2.3. *Sia K un campo finito con q elementi.*
Allora $\forall a \in K$, $a \neq 0$ si ha $a^{q-1} = 1$

Proposizione 3.2.4. *Sia K un campo finito con q elementi e sia $f(x) \in K[x]$.*
Allora $f(a) = 0 \ \forall a \in K$ se e solo se f è divisibile per $x^q - x$ in $K[x]$.

Dimostrazione.

- Se $f(x)$ è divisibile per $x^q - x$, allora $f(x) = (x^q - x)\, g(x)$, con $g(x) \in K[x]$. Per il lemma si ha che $a^{q-1} - 1 = 0 \ \forall a \in K$, con $a \neq 0$. Quindi ogni $a \neq 0$ è radice del polinomio $x^{q-1} - 1$. Inoltre 0 è radice di x quindi ogni $a \in K$ è radice di $x(x^{q-1} - 1) = x^q - x$. Quindi il polinomio $f(x) = (x^q - x)\, g(x)$ si annulla per tutti gli elementi di K.

- Sia $f(a) = 0 \ \forall a \in K$. $f(x) = (x^q - x)\, g(x) + r(x)$, con $r = 0$ o $deg(r) < deg(x^q - x) = q$. Quindi $r(x) = f(x) - (x^q - x)\, g(x)$ e $r(a) = f(a) - (a^q - a)\, g(a) = 0 \ \forall a \in K$. Allora il polinomio $r(a)$ ha q radici in K. Ma per il corollario 3.1.8 questo si ha solo se $r = 0$.

Corollario 3.2.5. *Sia K un campo finito con q elementi e siano $f, g \in K[x]$.*
Allora $f(a) = g(a) \ \forall a \in K$ se e solo se $f(x) - g(x)$ è divisibile per $x^q - x$.

3.2.1 Funzioni e funzioni polinomiali su un campo

Proposizione 3.2.6. *Se p è un numero primo, allora ogni funzione $f : \mathbb{Z}_p \to \mathbb{Z}_p$ è una funzione polinomiale, cioè può essere rappresentata da un polinomio.*
Equivalentemente, ogni funzione su $\{0, \ldots, p-1\}$ è un polinomio mod p.

Dato che se p è un primo allora $\mathbb{Z}_p$ è un campo, la proposizione precedente è una conseguenza del seguente teorema:

Teorema 3.2.7. *Sia A un anello commutativo finito. Se A è un campo allora ogni funzione $f : A \to A$ è una funzione polinomiale.*
Se A non è un campo esistono funzioni non polinomiali.

Dimostrazione. Mostriamo che se A non è un campo esistono funzioni non polinomiali.
Se A non è un campo, allora non è un dominio di integrità, quindi esiste un divisore dello zero, cioè un elemento $c \neq 0$ in A tale che $ca = 0$ per qualche $a \in A$, $a \neq 0$.
Sia $A = \{a_1 = 0, \ldots, a_n\}$. Consideriamo il polinomio di grado n

$$g(x) = \prod_{i=1}^{n} (x - a_i)$$

che si annulla $\forall x \in A$. Se una funzione $A \to A$ può essere rappresentata da un polinomio, allora tale polionomio può essere scelto di grado $\leq n-1$. Infatti il polinomio $g(x)$ è monico e l'essere nullo implica che $x^n = p_{n-1}$, con p_{n-1} di grado minore di n. Allora i termini di grado $\geq n$ possono essere sostituiti con termini di grado $< n$. Il numero di tutti i polinomi di grado $\leq n-1$ è pari a n^n così come il numero di funzioni $f : A \to A$. Così sembrerebbe che ogni funzione possa essere rappresentata da un polinomio; ma non è così. Infatti esiste un polinomio di grado $n-1$, che non è il polinomio nullo, al quale corrisponde una funzione identicamente nulla.

$$f(x) = c \prod_{i=2}^{n} (x - a_i) = c\,(x - a_2) \cdots (x - a_n)$$

è un polinomio di grado $n-1$ tale che $f(x) = 0\ \forall a_i,\ i \geq 2$; inoltre si ha $f(0) = c(-1)^{n-1} a_2 a_3 \cdots a_n$. Poiché c è un divisore dello zero, esiste un $a_i \neq 0,\ i \geq 2$ tale che $ca_i = 0$. Segue quindi che $f(0) = 0$; cioè ad un polinomio $\neq 0$ corrisponde una funzione polinomiale identicamente nulla. Ne segue che almeno una funzione da A ad A non può essere rappresentata da un polinomio.
Facciamo vedere ora che se A è un campo ad ogni funzione da A ad A viene associato un polinomio di $A[x]$.
Sia A un campo finito con n elementi e sia $p(x) \in A[x]$ un polinomio di grado $\leq n-1$. Allora per il corollario 3.1.8, $p(x)$ ha al più $n-1$ radici distinte in A, quindi non può essere la funzione nulla. Siano poi $p(x)$ e $q(x)$ due polinomi distinti di $A[x]$ di grado $\leq n-1$. Allora per il corollario 3.2.2 non può essere $p(x) = q(x)\ \ \forall x \in A$; quindi $p(x)$ e $q(x)$ non coincidono come funzioni. Quindi agli n^n polinomi distinti di grado $\leq n-1$ vengono associate n^n funzioni distinte da A ad A.

3.3 Polinomi sull'anello $\mathbb{Z}_{pq}$

Teorema 3.3.1. *Siano $p, q \in \mathbb{Z}$, $p, q \neq 0$ relativamente primi tra loro.*
Allora vale che $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$

Dimostrazione. Consideriamo l'omomorfismo di anelli $\varphi : \mathbb{Z} \to \mathbb{Z}_p \times \mathbb{Z}_q$ tale che $\varphi(k) = \left([k]_p, [k]_q\right)$.
Il nucleo di φ è $Ker\varphi = \left\{k \in \mathbb{Z} | \varphi(k) = \left([0]_p, [0]_q\right)\right\}$.
Quindi $k \in Ker\varphi \Leftrightarrow \left([k]_p, [k]_q\right) = \left([0]_p, [0]_q\right) \Leftrightarrow p|k$ e $q|k \Rightarrow pq|k \Leftrightarrow k \in (pq)$.
Quindi $Ker\varphi = (pq)$. Ma allora per il teorema 2.2.6, esiste un isomorfismo

$$\Psi : \mathbb{Z}/(pq) \to \varphi(\mathbb{Z})$$
$$[k]_{pq} \mapsto \left([k]_p, [k]_q\right)$$

dove $\mathbb{Z}/(pq) = \mathbb{Z}_{pq}$ e $\varphi(\mathbb{Z}) \subset \mathbb{Z}_p \times \mathbb{Z}_q$. Poiché Ψ è biunivoca, l'immagine $\varphi(\mathbb{Z})$ avrà tanti elementi quanti ne ha $\mathbb{Z}_{pq}$, cioè pq. Ma pq è anche il numero

di elementi di $Z_p \times Z_q$, quindi $\varphi(Z) = \mathbb{Z}_p \times \mathbb{Z}_q$.
Da cui si ottiene $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$.

Teorema 3.3.2. *Siano $p, q \in \mathbb{Z}$, $p, q \neq 0$, relativamente primi tra loro. Allora $\mathbb{Z}_{pq}[x] \cong \mathbb{Z}_p[x] \times \mathbb{Z}_q[x]$.*

Dimostrazione. Consideriamo la funzione

$$\varphi : \mathbb{Z}_{pq}[x] \to \mathbb{Z}_p[x] \times \mathbb{Z}_q[x]$$

tale che

$$[a_0]_{pq} + \ldots + [a_n]_{pq} x^n \mapsto \left([a_0]_p + \ldots + [a_n]_p x^n, [a_0]_q + \ldots + [a_n]_q x^n\right)$$

Si dimostra che φ è un isomorfismo di anelli.
Siano $f(x) = [a_0]_{pq} + \ldots + [a_n]_{pq} x^n$, $g(x) = [b_0]_{pq} + \ldots + [b_n]_{pq} x^n$ due polinomi a coefficienti in $\mathbb{Z}_{pq}$. Allora:

- $\varphi(f(x) + g(x)) =$
  $= \left([a_0]_{pq} + [b_0]_{pq}\right) + \ldots + \left([a_n]_{pq} + [b_n]_{pq}\right) x^n =$
  $= [a_0 + b_0]_{pq} + \ldots + [a_n + b_n]_{pq} x^n =$
  $= \left([a_0 + b_0]_p + \ldots + [a_n + b_n]_p x^n, [a_0 + b_0]_q + \ldots + [a_n + b_n]_q x^n\right) =$
  $= \left([a_0]_p + \ldots + [a_n]_p x^n\right) + \left([b_0]_p + \ldots + [b_n]_p x^n\right),$
  $\left([a_0]_q + \ldots + [a_n]_q x^n\right) + \left([b_0]_q + \ldots + [b_n]_q x^n\right) =$
  $= \left([a_0]_p + \ldots + [a_n]_p x^n, [a_0]_q + \ldots + [a_n]_q x^n\right) +$
  $+ \left([b_0]_p + \ldots + [b_n]_p x^n, [b_0]_q + \ldots + [b_n]_q x^n\right) =$
  $= \varphi(f(x)) + \varphi(g(x))$

- $\varphi(f(x)\, g(x)) =$
  $= \left([a_0]_{pq} [b_0]_{pq}\right) + \ldots + \left([a_n]_{pq} [b_n]_{pq}\right) x^n =$
  $= [a_0 b_0]_{pq} + \ldots + [a_n b_n]_{pq} x^n =$
  $= \left([a_0 b_0]_p + \ldots + [a_n b_n]_p x^n, [a_0 b_0]_q + \ldots + [a_n b_n]_q x^n\right) =$
  $= \left([a_0]_p + \ldots + [a_n]_p x^n\right) \cdot \left([b_0]_p + \ldots + [b_n]_p x^n\right),$

$$\left([a_0]_q + \ldots + [a_n]_q x^n\right) \cdot \left([b_0]_q + \ldots + [b_n]_q x^n\right) =$$
$$= \left([a_0]_p + \ldots + [a_n]_p x^n, [a_0]_q + \ldots + [a_n]_q x^n\right) \cdot$$
$$\cdot \left([b_0]_p + \ldots [b_n]_p x^n, [b_0]_q + \ldots + [b_n]_q x^n\right) =$$
$$= \varphi(f(x))\,\varphi(g(x))$$

- $\varphi(1) = \left([1]_p, [1]_q\right)$

In questo modo abbiamo dimostrato che φ è un omomorfismo.
Vediamo che è iniettivo:
Siano $f(x), g(x) \in \mathbb{Z}_{pq}[x]$ come sopra; allora $\varphi(f(x)) = \varphi(g(x))$ se e solo se $\left([a_0]_p + \ldots + [a_n]_p x^n, [a_0]_q + \ldots + [a_n]_q x^n\right) = \left([b_0]_p + \ldots + [b_n]_p x^n, [b_0]_q + \ldots [b_n]_q x^n\right)$, cioè se e solo se:
$[a_0]_p + \ldots + [a_n]_p x^n = [b_0]_p + \ldots + [b_n]_p x^n \Leftrightarrow [a_i]_p = [b_i]_p \quad \forall i$
$[a_0]_q + \ldots + [a_n]_q x^n = [b_0]_q + \ldots + [b_n]_q x^n \Leftrightarrow [a_i]_q = [b_i]_q \quad \forall i$
Quindi $f(x) = g(x)$.
Dimostriamo infine che φ è suriettivo:
Sia $(g(x), h(x)) = \left([a_0]_p + \ldots + [a_n]_p x^n, [a_0]_q + \ldots [a_n]_q x^n\right) \in \mathbb{Z}_p[x] \times \mathbb{Z}_q[x]$, allora esiste $f(x) = [a_0]_{pq} + \ldots + [a_n]_{pq} x^n \in \mathbb{Z}_{pq}$ tale che $\varphi(f(x)) = (g(x), h(x))$.
Quindi $\varphi(\mathbb{Z}_{pq}[x]) = \mathbb{Z}_p[x] \times \mathbb{Z}_q[x]$.

3.4 Polinomi congrui e equivalenti *mod m*

Definizione 3.11. Siano $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ e $g(x) = b_0 + b_1 x + \ldots + b_n x^n$ due polinomi a coefficienti in $\mathbb{Z}$.
Si dice che $f(x)$ e $g(x)$ sono *congrui* modulo m, $f \equiv g \ mod\ m$, se $\forall i = 0, \ldots, n$, $a_i \equiv b_i \ mod\ m$.

Definizione 3.12. Due polinomi $f(x)$ e $g(x)$ a coefficienti in $\mathbb{Z}$ si dicono *equivalenti* modulo m se $\forall x \in \mathbb{Z}$, $f(x) \equiv g(x) \ mod\ m$

Lemma 3.4.1. *Siano $f(x), g(x) \in \mathbb{Z}[x]$.*
Se $f \equiv g \ mod\ m$ allora $\forall x \in \mathbb{Z}$, $f(x) \equiv g(x) \ mod\ m$.

Dimostrazione. Se $f \equiv g \ mod \ m$ allora $a_i \equiv b_i \ mod \ m$, $\forall i = 0, \ldots, n$.
Poiché $\forall x \in \mathbb{Z}, x \equiv x \ mod \ m$, si ha $a_i x^i \equiv b_i x^i \ mod \ m$, $\forall i \geq 0, \forall x \in \mathbb{Z}$.
Ne segue $\sum_i a_i x^i \equiv \sum_i b_i x^i \ mod \ m$, $\forall x \in \mathbb{Z}$. Quindi $\forall x \in \mathbb{Z}$, $f(x) \equiv g(x)$ *mod* m.

In generale non vale il viceversa. Vediamo sotto quali condizioni è verificato:

Lemma 3.4.2. *Siano* $f(x) = a_0 + a_1 x$ *e* $g(x) = b_0 + b_1 x$, *due polinomi di grado uno a coefficienti in* $\mathbb{Z}_m$.
f *e* g *sono equivalenti mod* m *se e solo se sono congrui modulo* m.

Dimostrazione. Supponiamo che $f(x)$ e $g(x)$ siano equivalenti modulo m, cioè $\forall x \in \{0, \ldots, m-1\}$, $f(x) \equiv g(x) \ mod \ m$.
Allora $f(x) - g(x) = (a_1 - b_1)x + (a_0 - b_0) \equiv 0 \ mod \ m$.

- Per $x = 0$ si ha $a_0 \equiv b_0 \ mod \ m$;
- Per $x = 1$ si ha $a_1 + a_0 \equiv b_1 + b_0 \ mod \ m$

Quindi i due polinomi sono congrui *mod* m.
Viceversa se $f \equiv g \ mod \ m$, allora sono equivalenti per il lemma 3.4.1

Lemma 3.4.3. *Se due polinomi* $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ *e* $g(x) = b_0 + b_1 x + \ldots + b_r x^r$ *sono equivalenti modulo* m,
allora $a_0 \equiv b_0 \ mod \ m$.

Dimostrazione. Se $x = 0$ si ha $f(x) - g(x) = a_0 - b_0 \equiv 0 \ mod \ m$.

Lemma 3.4.4. *Sia* p *un primo e sia* $g \geq 1$.
Due polinomi $f(x) = a_0 + a_1 x + \ldots a_{p-1} x^{p-1}$ *e sia* $g(x) = b_0 + b_1 x + \ldots + b_{p-1} x^{p-1}$ *sono equivalenti mod* p^d *se e solo se sono congrui mod* p^d.

3.4.1 Polinomi nulli *mod m*

Definizione 3.13. Un polinomio $f(x)$ di grado $n \geq 0$ *mod* m si definisce *polinomio nullo* di grado n *mod* m se $\forall x \in \mathbb{Z}, f(x) \equiv 0 \ mod \ m$.

Equivalentemente un polinomio nullo *mod* m è un polinomio definito su $\mathbb{Z}_m$ e che si annulla per tutti gli elementi dell'insieme.

Vediamo alcune proprietà:

1. Se $f(x) = a_0 + a_1x + \ldots + a_nx^n$ è un polinomio nullo *mod* m, allora $a_0 \equiv 0 \ mod \ m$.

2. Se $f(x)$ è un polinomio nullo *mod* m, allora $af(x)$ è ancora un polinomio nullo *mod* m, con $a \in \mathbb{Z}$.

3. $f(x)$ è un polinomio nullo *mod* m se e solo se $af(x)$ è un polinomio nullo *mod* m, con $MCD(a, m) = 1$.

4. Se $f(x)$ è un polinomio nullo *mod* m e $a|m$, allora $f(x)$ è un polinomio nullo *mod* a.

Osservazione 17. $\forall m \in \mathbb{Z}$, il più semplice polinomio nullo *mod* m è

$$f(x) = \prod_{i=0}^{m-1} (x - i)$$

3.4.2 Polinomi nulli *mod p*

Indichiamo con $w_0(m)$ il più piccolo intero $n \geq 1$ tale che esiste un polinomio nullo di grado n *mod* m e con $w_1(m)$ il più piccolo intero $n \geq 1$ tale che esiste un polinomio nullo monico di grado n *mod* m.

Teorema 3.4.5. *Sia p un primo.*
Allora $w_0(p) = w_1(p) = p$.

Dimostrazione. Per prima cosa osserviamo che il polinomio monico $f(x) = x^p - x$ di grado p è nullo *mod* p.
Bisogna quindi far vedere che non esistono polinomi nulli *mod* p di grado $\leq p - 1$.
Sia $g(x) = a_{p-1}x^{p-1} + \ldots + a_0$ un polinomio di grado $\leq p - 1$ e supponiamo per assurdo che $g(x)$ sia un polinomio nullo *mod* p.

Allora per definizione si ha che $\forall x \in \mathbb{Z}$, $g(x) \equiv 0 \ mod\ p$; cioè $g(x)$ è equivalente al polinomio 0.
Ma per il lemma 3.4.4 sappiamo che due polinomi di grado $\leq p-1$ equivalenti *mod p* sono anche congrui *mod p*; quindi $g(x)$ è congruo al polinomio 0 *mod p*. Segue così che $a_i \equiv 0 \ mod\ p \ \forall i = 0, \ldots, p-1$, che è un assurdo.

Teorema 3.4.6. *Sia p un primo e $f(x)$ un polinomio nullo di grado p modulo p.*
Allora $g(x)$ è un polinomio nullo mod p se e solo se $g(x) \equiv f(x)\,q(x)$ mod p, con $q(x)$ polinomio arbitrario mod p.

Dimostrazione. Sia $g(x)$ un polinomio nullo *mod p*. Allora per il lemma 3.1.4 si ha $g(x) = f(x)\,q(x) + r(x)$, con $r(x)$ polinomio di grado $\leq p-1$ *mod p*. Ma $f(x)\,q(x)$ è un polinomio nullo *mod p*, quindi anche $r(x)$ è un polinomio nullo *mod p*. Sempre per il lemma 3.4.4 si ha che $r(x)$ è congruo a zero *mod p*.
Quindi $g(x) \equiv f(x)\,q(x)\ mod\ p$.

Corollario 3.4.7. *Sia p un primo.*
Allora $f(x)$ è un polinomio nullo mod p se e solo se $f(x) \equiv (x^p - x)\,q(x)$ mod p, con $q(x)$ un polinomio nullo mod p.

Dimostrazione. Il corollario è un caso particolare della proposizione 3.2.4 quando come campo finito si considera $\mathbb{Z}_p$, ma è anche una conseguenza del teorema precedente poiché $x^p - x$ è un polinomio nullo *mod p*.

Corollario 3.4.8. *Siano p un primo e $f(x)$ un polinomio nullo di grado p mod p.*
Allora $f(x) \equiv a\,(x^p - x)\ mod\ p$, con $MCD(a,p) = 1$.
Cioè $x^p - x$ è l'unico polinomio nullo monico mod p.

Dimostrazione. Il corollario è conseguenza del teorema precedente.
Si osserva che $f(x)$ è congruo al polinomio zero *mod p* se $MCD(a,p)$ è maggiore di 1, cioè $a \equiv 0\ mod\ p$.

Corollario 3.4.9. *Sia p un primo. Allora*
$\prod_{i=0}^{p-1}(x-i) = x(x-1)\cdots(x-(p-1)) \equiv (x^p - x) \ mod\ p.$

Teorema 3.4.10. *Sia p un primo e sia d un intero ≥ 1. Allora $w_0\left(p^d\right) = p$. Cioè un polinomio nullo mod p^d ha grado $\geq p$.*

Dimostrazione. La dimostrazione è simile a quella del teorema 3.4.5.

3.5 L'ideale dei polinomi identicamente nulli

Sia A un anello commutativo. Indichiamo con I_0 l'insieme di tutti i polinomi identicamente nulli su A.

Teorema 3.5.1. *I_0 è un ideale di $A[x]$.*

Dimostrazione. Siano $p(x), q(x) \in I_0$. Per definizione si ha che
$p(x) = 0, q(x) = 0\ \forall x \in A$, quindi anche $p(x) + q(x) = 0\ \forall x \in A$.
Inoltre $\forall p(x) \in I_0$, $\forall g(x) \in A[x], p(x)g(x) \in I_0$, poiché $p(x)g(x) = 0\ \forall x \in A$.

Teorema 3.5.2. *Sia K un campo. Si ha che:*

- *Se K è infinito allora $I_0 = \{0\}$*
- *Se K è finito con q elementi allora I_0 è generato dal polinomio $x^q - x$.*

Dimostrazione.

- Sia K un campo infinito e sia $p(x) \in K[x]$.
  Per il lemma 3.2.1 sappiamo che $p(x) = 0\ \forall x \in K$ se e solo se p è il polinomio identicamente nullo.
  Ne segue che $I_0 = \{0\}$.
- Sia K un campo finito con q elementi e sia $p(x) \in K[x]$.
  Segue dalla proposizione 3.2.4 che $p(x) = 0$ se e solo se $p(x)$ è divisibile per $x^q - x$.
  Questo significa che ogni polinomio in I_0 può essere scritto come $f(x)(x^q - x)$

per qualche $f(x) \in K[x]$.
Per definizione di ideale generato da un solo elemento si ha che $I_0 = (x^q - x)$.

Se si vuole individuare l'ideale dei polinomi identicamente nulli sugli anelli $\mathbb{Z}_m$, bisogna distinguere il caso in cui m è un intero qualsiasi dal caso in cui m è un primo.

- Se m è un primo, sappiamo che $\mathbb{Z}_m$ è un campo. Allora per il teorema 3.5.2, l'ideale dei polinomi identicamente nulli su $\mathbb{Z}_m$ è generato dal polinomio $x^m - x \in \mathbb{Z}_m$.

- Se m non è primo, allora si deve trovare un insieme di generatori per I_0; cioè un insieme di polinomi di grado $\leq m$ che siano identicamente nulli e che non siano combinazioni lineari di altri polinomi identicamente nulli su $\mathbb{Z}_m$.

3.5.1 Ideale dei polinomi identicamente nulli in $\mathbb{Z}_{pq}$

Proposizione 3.5.3. *Siano p, q interi positivi, con p, q relativamente primi tra loro. Sia I_{pq} l'ideale dei polinomi identicamente nulli su $\mathbb{Z}_{pq}$.*
Allora esistono I_p ideale di $\mathbb{Z}_p[x]$ e I_q ideale di $\mathbb{Z}_q[x]$ tali che

1. $I_{pq} = I_p \times I_q$
2. $\mathbb{Z}_{pq}[x]/I_{pq} \cong \mathbb{Z}_p[x]/I_p \times \mathbb{Z}_q[x]/I_q$

Dimostrazione. 1. Segue dal teorema 2.2.7, poiché
$\mathbb{Z}_{pq}[x] \cong \mathbb{Z}_p[x] \times \mathbb{Z}_q[x]$

2. Segue dal teorema 2.2.8.

Teorema 3.5.4. *Sia $I_{pq} = I_p \times I_q$ l'ideale dei polinomi nulli su $\mathbb{Z}_{pq}$. Allora I_p è l'ideale dei polinomi identicamente nulli su $\mathbb{Z}_p$ e I_q è l'ideale dei polinomi identicamente nulli su $\mathbb{Z}_q$*

Dimostrazione. Sia $f_{pq}(x) = [a_0]_{pq} + \ldots + [a_n]_{pq} x^n \in \mathbb{Z}_{pq}[x]$ un polinomio identicamente nullo su $\mathbb{Z}_{pq}$.
Abbiamo visto che a tale polinomio corrisponde la coppia $(f_p(x), f_q(x)) = \left([a_0]_p + \ldots + [a_n]_p x^n, [a_0]_q + \ldots + [a_n]_q x^n\right) \in \mathbb{Z}_p[x] \times \mathbb{Z}_q[x]$.
Dobbiamo far vedere che $f_p(x)$ e $f_q(x)$ sono polinomi identicamente nulli su $\mathbb{Z}_p$ e $\mathbb{Z}_q$.
Se $f(x) = a_0 + \ldots + a_n x^n$ è un polinomio nullo *mod* pq, allora si ha che $\forall x \in \mathbb{Z}$, $f(x) \equiv 0$ *mod* pq.
Questo implica che $\forall x \in \mathbb{Z}$, $pq | f(x) \Leftrightarrow f(x) = kpq, k \in \mathbb{Z}$.
Allora $p|f(x)$ e $q|f(x)$ e quindi $\forall x \in \mathbb{Z}, f(x) \equiv 0$ *mod* p e $f(x) \equiv 0$ *mod* q.
Viceversa se $\forall x \in \mathbb{Z}$, $f(x) \equiv 0$ *mod* p e $f(x) \equiv 0$ *mod* q allora $p|f(x)$ e $q|f(x)$. Ma essendo $MCD(p,q) = 1, pq|f(x)$ e quindi $f(x) \equiv 0$ *mod* pq.

Ne segue che lo studio dei polinomi identicamente nulli su $\mathbb{Z}_m$ si riconduce al caso delle potenze dei primi.
Se $m = p_1^{k_1} \cdots p_r^{k_r}$ allora:

$$\mathbb{Z}_m \cong \mathbb{Z}_{{p_1}^{k_1}} \times \ldots \times \mathbb{Z}_{{p_r}^{k_r}}$$

$$\mathbb{Z}_m[x] \cong \mathbb{Z}_{{p_1}^{k_1}}[x] \times \ldots \times \mathbb{Z}_{{p_r}^{k_r}}[x]$$

$$I_m = I_{{p_1}^{k_1}} \times \ldots \times I_{{p_r}^{k_r}}$$

dove I_m è l'ideale dei polinomi identicamente nulli in $\mathbb{Z}_m$ e $I_{{p_i}^{k_i}}$ è l'ideale dei polinomi identicamente nulli in $\mathbb{Z}_{{p_i}^{k_i}}$. Quindi:

$$\mathbb{Z}_m[x]/I_m \cong \mathbb{Z}_{{p_1}^{k_1}}[x]/I_{{p_1}^{k_1}} \times \ldots \times \mathbb{Z}_{{p_r}^{k_r}}[x]/I_{{p_r}^{k_r}}.$$

Esempio 3.2. Sia $m = 6 = 3 \times 2$ allora:
$\mathbb{Z}_3[x]/I_3$ con $I_3 = (x^3 - x)$ ha $27 = 3^3$ elementi, $\mathbb{Z}_2[x]/I_2$ con $I_2 = (x^2 - x)$ ha $4 = 2^2$ elementi.
Allora l'anello delle funzioni polinomiali su $\mathbb{Z}_6$, $\mathbb{Z}_6[x]/I_6$, ha $27 \times 4 = 108$ elementi.

Purtroppo, nel caso m non un primo, un ideale di $\mathbb{Z}_m[x]$ non è necessariamente principale; pertanto trovare chi lo genera non è banale.
A questo sarà dedicato parte del prossimo capitolo.

Capitolo 4

Algebre monounarie polinomiali

Definizione 4.1. Sia X un insieme con $n \geq 2$ elementi e sia $f : X \to X$. L'algebra (X, f) è detta monounaria *polinomiale* se è isomorfa ad un'algebra $\left(\mathbb{Z}_n, f'\right)$, con f' funzione polinomiale.

Denotiamo con PA_n l'insieme delle classi d'isomorfismo delle algebre polinomiali su $\mathbb{Z}_n$.
Quello che ci proponiamo di determinare è il numero di elementi di quest'insieme.

Facciamo alcune premesse:
Sia X un insieme con n elementi $n \geq 2$ e sia $\left(X^X, \circ, id_X\right)$ il monoide delle funzioni da X a se stesso; esso contiene il gruppo simmetrico S_X come gruppo delle unità.
Sia $X = \mathbb{Z}_n$ e identifichiamo con $\{0, \ldots, n-1\}$ i suoi elementi. Con le operazioni di somma e prodotto punto per punto si ottiene l'anello $\left(\left(\mathbb{Z}_n\right)^{\mathbb{Z}_n}, +, \cdot, 1\right)$ delle funzioni da $\mathbb{Z}_n$ a se stesso, che è commutativo, di caratteristica n e con n^n elementi.
Abbiamo già visto che ogni polinomio $\sum_{i=0}^{m} a_i x^i$, con $m \geq 0$ e $a_i \in \mathbb{Z}_n$ in $\mathbb{Z}_n[x]$ determina la funzione polinomiale $f : \mathbb{Z}_n \to \mathbb{Z}_n$, $f(x) = \sum_{i=0}^{m} a_i x^i$ e

abbiamo osservato che polinomi diversi possono produrre la stessa funzione polinomiale e che non tutte le funzioni $f : \mathbb{Z}_n \to \mathbb{Z}_n$ sono polinomiali.

Il calcolo delle classi di isomorfismo delle algebre polinomiali dipende strettamente dal calcolo delle funzioni polinomiali distinte da $\mathbb{Z}_n$ a $\mathbb{Z}_n$. Quindi preliminarmente ci occuperemo di questo problema.

Osservazione 18. L'applicazione $\mu : \mathbb{Z}_n[x] \to (\mathbb{Z}_n)^{\mathbb{Z}_n}$, che ad ogni polinomio associa la corrispondente funzione polinomiale è un morfismo di anelli, la cui immagine è l'anello delle funzioni polinomiali su $\mathbb{Z}_n$, che indichiamo con $PF_n[x]$ e il cui nucleo $Ker(\mu)$ è un ideale di $\mathbb{Z}_n[x]$, l'ideale dei polinomi identicamente nulli.

Per il teorema fondamentale di omomorfismi per gli anelli (teorema 2.2.6) si ha che $\mu(\mathbb{Z}_n[x]) = Im(\mu) = PF_n[x] \cong \mathbb{Z}_n[x]/Ker(\mu)$.

Quindi per determinare tutte le funzioni polinomiali bisogna determinare il nucleo di μ e l'ordine di $\mathbb{Z}_n[x]/Ker(\mu)$.
Un altro calcolo interessante è quello delle funzioni polinomiali biettive, cioè l'insieme $G = PF_n[x] \cap S_n$.

Osservazione 19. Poiché la composizione di funzioni polinomiali è ancora polinomiale, ne segue che G costituisce un gruppo rispetto alla composizione.

Se n è primo abbiamo già visto che ogni $f : \mathbb{Z}_n \to \mathbb{Z}_n$ è polinomiale, in particolare le biezioni sono a loro volta polinomi. $Ker(\mu)$ è generato dal polinomio $x^n - x$ (vedi teorema 3.5.2). In questo caso $G \cong S_n$.
Come avevamo già messo in luce, il problema si pone se n non è primo.

4.1 Risultati generali

Lemma 4.1.1. *Siano m, n due numeri naturali coprimi. Sappiamo che $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ (teorema 3.3.1). Allora:*

1. $\mathbb{Z}_{mn}[x] \cong \mathbb{Z}_m[x] \times \mathbb{Z}_n[x]$;

2. $PF_{mn}[x] \cong PF_m[x] \times PF_n[x]$*;*

3. $PF_{mn}[x] \cap S_{mn} = (PF_m[x] \cap S_m) \times (PF_n[x] \cap S_n)$.

Dimostrazione. 1. vedi teorema 3.3.2;

2. vedi proposizione 3.5.3;

3. Sia $\vartheta : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$ l'isomorfismo tra due anelli e f, g due funzioni biettive.
   La coppia $(f, g) : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_n$ induce la funzione suriettiva $\varphi : \mathbb{Z}_{mn} \to \mathbb{Z}_{mn}$, $\varphi = \vartheta \circ (f, g) \circ \vartheta^{-1}$; quindi φ è una biezione.
   Se f, g sono polinomiali allora anche φ lo è, quindi $\varphi \in PF_{mn}[x] \cap S_{mn}$.
   Inversamente se φ è una funzione polinomiale biettiva in $\mathbb{Z}_{mn}$, da 2. sappiamo che determina una coppia (f, g) di funzioni polinomiali che devono essere iniettive e quindi biettive; quindi si avrà $(f, g) \in (PF_m[x] \cap S_m) \times (PF_n[x] \cap S_n)$.
   La funzione Φ che associa alla coppia $(f, g) \in (PF_m[x] \cap S_m) \times (PF_n[x] \cap S_n)$ la funzione $\varphi = \vartheta \circ (f, g) \circ \vartheta^{-1}$, ha quindi come immagine $PF_{mn}[x] \cap S_{mn}$.
   Dominio e codominio sono due gruppi rispetto alla composizione (lemma 19), Φ è un omomorfismo e il suo nucleo è costituito dalle coppie (f, g) a cui corrisponde l'identità.
   Facciamo vedere che Φ è iniettiva.
   Per tali coppie (f, g), $\forall (i, r) \in \mathbb{Z}_m \times \mathbb{Z}_n$ si ha:

$$\begin{cases} f : i \to j \\ g : r \to s \end{cases}$$

$$\begin{cases} h = \vartheta(i, r) \\ k = \vartheta(j, s) \end{cases}$$

   Quindi

$$\Phi(f, g) : h \to k.$$

   Se fosse $i \neq j$ oppure $r \neq s$, allora $h \neq k$ e $\Phi(h, k) \neq id$.
   Quindi f e g sono identità e Φ è iniettiva.

Dal lemma precedente segue che il calcolo delle funzioni polinomiali su $\mathbb{Z}_n$, con n qualsiasi, può essere ricondotto al caso $n = p^h$, con p primo e $h \geq 1$.
Facciamo vedere a questo punto che ogni algebra polinomiale appartenente a PA_{mn} è isomorfa al prodotto diretto di un'algebra polinomiale appartenente a PA_m per una appartenente a PA_n, indipendentemente dai rappresentanti scelti.
Ricordiamo preliminarmente che date due algebre monounarie (X, f) e (Y, g), possiamo definire una nuova algebra monounaria $(X \times Y, h)$ ponendo $\forall x \in X, \forall y \in Y$, $h(x, y) = (f(x), g(x))$. Mostriamo ora il seguente risultato:

Lemma 4.1.2. *Siano* $(X, f) \cong (X', f')$, $(Y, g) \cong (Y', g')$ *algebre monounarie, allora dette* h, h' *le operazioni prodotto diretto in* $X \times Y$ *e in* $X' \times Y'$*, si ha* $(X \times Y, h) \cong (X' \times Y', h')$.

Dimostrazione. Siano $\alpha : X \to X'$, $\beta : Y \to Y'$ due isomorfismi. Poniamo

$$\Phi : X \times Y \to X' \times Y' \quad \Phi(x) = (\alpha(x), \beta(y))$$

Allora Φ è ovviamente suriettiva e poiché ha dominio e codominio finiti e equipotenti, sarà anche iniettiva. Inoltre $\forall (x, y) \in X \times Y$ si ha:

$$\Phi(h(x, y)) = \Phi(f(x), g(x)) = (\alpha(f(x)), \beta(g(y))) = h'(\alpha(x), \beta(y)) = h'(\Phi(x, y)),$$

quindi Φ è un isomorfismo di algebre monounarie.

Osservazione 20. Dal lemma 4.1.2 segue che per studiare il prodotto diretto ci si può limitare ad un rappresentante per ogni classe d'isomorfismo. Pertanto nel nostro caso si ha che dato $p(x) = (p_m(x), p_n(x))$ e date (X_m, f_m), (X_n, f_n) due algebre monounarie di ordini m e n rispettivamente, tali che $(X_m, f_m) \cong (\mathbb{Z}_m, p_m[x])$ e $(X_n, f_n) \cong (\mathbb{Z}_n, p_n[x])$ allora si ha $(\mathbb{Z}_{mn}, p(x)) \cong (X_m, f_m) \times (X_n, f_n)$. Pertanto il prodotto di algebre polinomiali è polinomiale e fattori isomorfi danno prodotti isomorfi.
Il viceversa non è detto che valga, cioè due algebre polinomiali di $\mathbb{Z}_{mn}$ potrebbero essere isomorfe anche se provengono da fattori non isomorfi. Ad

esempio esistono tre classi di isomorfismo di algebre polinomiali d'ordine 2 e sette di ordine 3, ma solo diciannove classi d'ordine 6 contro le ventuno attese[1].

A questo punto riportiamo di seguito un algoritmo per il computo delle classi di funzioni polinomiali su $\mathbb{Z}_n$ e delle classi di isomorfismo delle algebre polinomiali sullo stesso anello:

1. Si determina $w_1(m)$. Questo ci dà il grado massimo, $m-1$, delle funzioni polinomiali su $\mathbb{Z}_n$.

2. Per $k \leq m-1$ e per $a \neq 0$, si cerca di esprimere, quando possibile, il monomio ax^k come combinazione lineare di termini di grado inferiore. Questo limita il coefficiente b di bx^k ad essere minore di a.

3. Si calcola quindi il numero di funzioni polinomiali distinte su $\mathbb{Z}_n$.

4. Si cercano ora le funzioni polinomiali biettive che, come abbiamo visto, formano un gruppo G rispetto alla composizione.
   Si può partire dal gruppo H[2] delle permutazioni α della forma $ax+b$ con a invertibile e b qualsiasi in $\mathbb{Z}_n$. Di ogni funzione α si trova prima l'espressione algebrica dell'inversa e, per ogni funzione polinomiale f si determina la coniugata $\alpha^{-1}(f(\alpha(x)))$. Si considera dunque l'azione di H per coniugio sull'insieme delle funzioni polinomiali su $\mathbb{Z}_n$, le cui orbite determinano una prima ripartizione di $PF_n[x]$ in classi di algebre monounarie isomorfe. Per questo passo risulta indispensabile l'uso di software.

5. Si trovano ora le altre funzioni polinomiali biettive e quindi l'intero gruppo G. Mediante l'azione di G, si costruiscono le nuove classi di coniugio delle funzioni polinomiali, che ampliano le classi dell'azione del sottogruppo H.

[1] Questo aspetto viene mostrato nel dettaglio nella sezione 4.3.

[2] H è il prodotto semidiretto di $\mathbb{Z}_n$ per $\mathbb{Z}_n^*$, di ordine $n\varphi(n)$, con φ funzione di Eulero.

6. Infine si traccia il grafo di ogni classe trovata, per vedere se ci sono classi da accorpare in S_n. Fatto questo, la lista delle classi d'isomorfismo di funzioni polinomiali sarà completa.

Introduciamo un lemma che ci dà delle condizioni per determinare i generatori di $Ker\mu$:

Lemma 4.1.3. *Sia h un divisore di n, $n = hq$. Allora:*

1. *Il polinomio $f(x) = h\prod_{r=0}^{q-1}(x-r)$ appartiene a $Ker\mu$.*
2. *Sia m il minimo intero positivo tale che q divida $m!$.*
   Allora $g(x) = h\prod_{i=0}^{m-1}(x+i)$ appartiene a $Ker\mu$.
3. *Sia r il minimo intero positivo tale che n divida $r!$.*
   Allora $p(x) = \prod_{j=0}^{r-1}(x+j)$ appartiene a $Ker\mu$.

Dimostrazione. 1. Sia $x = qs + r$, con $0 \leq r < q$. Allora $h(x-r) = hqs \equiv 0\ (mod\ n)$ e quindi $f(x) = 0$ per ogni $x \in \mathbb{Z}_n$.

2. Segue da una proprietà aritmetica: per ogni terna d'interi positivi k, n, m, se k divide $m!$ allora k divide $\prod_{i=0}^{m-1}(n+i)$.

3. Segue da 2. per $h = 1$.

Il primo problema è quindi quello di trovare un polinomio monico di grado minimo che sia identicamente nullo. Un polinomio monico di grado n esiste ed è ovviamente $p(x) = \prod_{i=0}^{n-1}(x-i)$, ma se n non è primo, ne esistono di grado inferiore e il punto 3. del lemma precedente ci permette di trovarne uno, anche se potrebbero essercene altri di grado minore.
Riducendo i risultati appena dimostrati al caso di n potenza di un primo si ottiene:

Lemma 4.1.4. *Siano $n = p^h$, con p primo e $h \geq 1$. Allora:*

1. *Il polinomio $p(x) = \prod_{i=0}^{p-1}(x+i)^h$, monico di grado ph è nullo per ogni $x \in \mathbb{Z}_n$.*

2. *Sia m il minimo numero positivo tale che p^h divida $m!$.*
   Allora $q(x) = \prod_{i=0}^{m-1}(x+i)$ è monico di grado m ed è nullo per ogni $x \in \mathbb{Z}_n$.

Osservazione 21. Ricordiamo che l'ordine del gruppo G, essendo un sottogruppo del gruppo simmetrico su n oggetti, deve dividere $n!$.

4.2 Esempi di algebre monounarie polinomiali in $\mathbb{Z}_n$, n potenza di un primo

Riportiamo in questa sezione i risultati ottenuti per il calcolo delle algebre monounarie polinomiali negli anelli $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_9$.

4.2.1 Il caso dell'anello $\mathbb{Z}_4$

Consideriamo $f : \mathbb{Z}_4 \to \mathbb{Z}_4$; esistono $4^4 = 256$ funzioni diverse di cui $4! = 24$ biettive.
Dal lemma 4.1.3 si ha che $n = 4 = 2 \cdot 2$ quindi $h = 2$ e $q = 2$; allora:

1. $f(x) = 2 \cdot \prod_{r=0}^{1}(x-r) = 2x(x-1)$ è identicamente nullo in $\mathbb{Z}_4$.

2. Il più piccolo m tale che 2 divida $m!$ è $m = 2$ quindi
   $g(x) = 2 \cdot \prod_{i=0}^{1}(x+i) = 2x(x+1)$ è identicamente nullo in $\mathbb{Z}_4$.

3. Il più piccolo r tale che 4 divida $r!$ è $r = 4$ quindi
   $p(x) = \prod_{j=0}^{3}(x+j) = x(x+1)(x+2)(x+3)$ è identicamente nullo in $\mathbb{Z}_4$.

Da 1. (e analogamente da 2.) si ottiene che il polinomio $2x^2 + 2x$ è identicamente nullo in $\mathbb{Z}_4$, quindi $2x^2 \equiv 2x$, da cui segue anche $2x^3 = x \cdot 2x^2 \equiv x \cdot 2x = 2x^2 \equiv 2x$.
Da 3. invece si ha che un polinomio monico di grado 4 identicamente nullo è $x(x+1)(x+2)(x+3) \equiv x^4 + 2x^3 + 3x^2 + 2x$. Per le identità precedenti

si ha che questo polinomio si riduce al polinomio $x^4 + 2x + 3x^2 + 2x = x^4 + 4x + 3x^2 = x^4 + 3x^2$.

Dal lemma 4.1.4 si ha che $n = 4 = 2^2$ quindi $p = 2$ e $h = 2$; allora:

1. $p(x) = \prod_{i=0}^{1}(x+i)^2 = x^2(x+1)^2$ è un polinomio monico identicamente nullo in $\mathbb{Z}_4$.

Questa condizione mi da il polinomio $x^2(x+1)^2 = x^4 + 2x^3 + x^2 \equiv x^4 + 2x^2 + x^2 = x^4 + 3x^2$ ottenuto dal punto 1. del lemma 4.1.3.

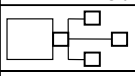
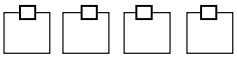
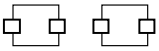
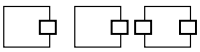
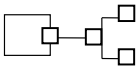
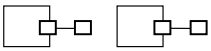
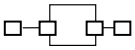
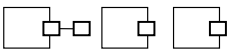
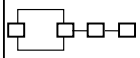
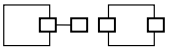
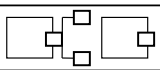
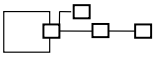
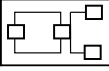
Si ottiene così la serie di identità: $x^4 = x^2$ e $2x^3 = 2x^2 = 2x$. Infine, nessun polinomio monico di grado 3 è identicamente nullo.
Il nucleo dell'omomorfismo μ sarà quindi l'ideale di $\mathbb{Z}_4[x]$ generato dai polinomi $2x^2 + 2x$ e $x^4 + 3x^2$. Allora le funzioni polinomiali sull'anello $\mathbb{Z}_4$ si riconducono tutte alla forma

$$ax^3 + bx^2 + cx + d \text{ con } a, b \in \{0, 1\}$$

Pertanto esistono solo $2 \cdot 2 \cdot 4 \cdot 4 = 64$ funzioni polinomiali delle 256 esistenti da $\mathbb{Z}_4$ a $\mathbb{Z}_4$. Di queste 4 sono costanti e 12 sono di primo grado. Tra quelle di primo grado solo 8 sono biettive e sono tutte quelle della forma $\pm x + p$, con $p = 0, 1, 2, 3$ e costituiscono un gruppo isomorfo al gruppo diedrale D_4. Ora $8 = |D_4|$ è un divisore massimale di $24 = |S_4|$, (ossia 8 è l'ordine dei 2-sottogruppi di Sylow[3] del gruppo simmetrico S_4), inoltre esistono biezioni non polinomiali; allora 8 è anche l'ordine del gruppo G dei polinomi biettivi. A questo punto per determinare le classi di isomorfismo delle algebre polinomiali di ordine 4 possiamo procedere come indicato nell'algoritmo; determinando prima il coniugio rispetto al gruppo G e poi riunendo in una sola le classi di algebre isomorfe, scoperte disegnandone i grafi.

[3]Sia G un gruppo e p un numero primo che divida l'ordine di G. Sia $|G| = p^k m$, con m non divisibile per p (dunque p^k è la massima potenza di p che divide l'ordine di G). Si definisce p-sottogruppo di Sylow di G ogni sottogruppo di G di ordine p^k. Il teorema di Sylow afferma l'esistenza di un tale sottogruppo e tutti i sottogruppi di ordine p^k sono coniugati in G e quindi isomorfi tra loro.

Si ottiene che esistono 14 classi di isomorfismo di algebre polinomiali, che coinvolgono in tutto 152 funzioni, circa il 59% del totale.

n°	Rappresentante	Grafo	N° coniugati
1	0		4
2	X		1
3	X+1		6
4	X+2		3
5	3x		6
6	2x		12
7	X^2		12
8	X^2+1		12
9	X^3		12
10	X^3+1		24
11	X^3+2		12
12	X^3+x		12
13	X^3+x+1		24
14	X^3+x+2		12

4.2.2 Il caso dell'anello $\mathbb{Z}_8$

Consideriamo $f : \mathbb{Z}_8 \to \mathbb{Z}_8$; esistono $8^8 = 16.777.216$ funzioni diverse di cui $8! = 40.320$ biettive.
Dal lemma 4.1.3 si ha che $n = 8 = 4 \cdot 2$ quindi $h_1 = 4$, $q_1 = 2$ e $h_2 = 2$, $q_2 = 4$; allora:

1. $f_1(x) = 4 \cdot \prod_{r=0}^{1}(x - r) = 4x(x - 1)$
   $f_2(x) = 2 \cdot \prod_{r=0}^{3}(x - r) = 2x(x - 1)(x - 2)(x - 3)$
   sono identicamente nulli in $\mathbb{Z}_8$.

2. Il più piccolo m_1 tale che 2 divida $m_1!$ è $m_1 = 2$ e il più piccolo m_2 tale che 4 divida $m_2!$ è $m_2 = 4$ quindi
   $g_1(x) = 4\prod_{i=0}^{1}(x + i) = 4x(x + 1)$
   $g_2(x) = 2\prod_{i=0}^{3}(x + i) = 2x(x + 1)(x + 2)(x + 3)$
   sono identicamente nulli in $\mathbb{Z}_8$.

3. Il più piccolo r tale che 8 divida $r!$ è $r = 4$ quindi
   $p(x) = \prod_{j=0}^{3}(x + j) = x(x + 1)(x + 2)(x + 3)$ è identicamente nullo in $\mathbb{Z}_8$.

Da 1. (e analogamente da 2.) si ottiene che i polinomi $2x^4+6x^2$ e $4x^2-4x$ sono identicamente nulli in $\mathbb{Z}_8$, quindi $2x^4 \equiv 2x^2$ e $4x^2 \equiv 4x$, da cui segue $4x^3 = x \cdot 4x^2 \equiv x \cdot 4x = 4x^2 \equiv 4x$.
Da 3. invece si ha che un polionomio monico di grado 4 identicamente nullo è $x(x + 1)(x + 2)(x + 3) \equiv x^4 + 6x^3 + 3x^2 + 6x$. Per le identità precedenti si ha che questo polinomio si riduce al polinomio $x^4 + 2x^3 + 3x^2 + 2x$.

Dal lemma 4.1.4 si ha che $n = 8 = 2^3$ quindi $p = 2$ e $h = 3$; allora:

1. $p(x) = \prod_{i=0}^{1}(x + i)^3 = x^3(x + 1)^3$ è un polinomio monico identicamente nullo in $\mathbb{Z}_8$.

Questa condizione dà un polinomio monico di grado 6; poiché ho trovato un polinomio monico identicamente nullo in $\mathbb{Z}_8$ di grado minore, posso tra-

lasciarla.

Non essendoci polinomi monici di grado 3 identicamente nulli, in $\mathbb{Z}_8$ le funzioni polinomiali distinte hanno la forma

$$a_3x^3 + a_2x^2 + a_1x + a_0 \text{ con } 0 \leq a_i \leq 3 \text{ } per \text{ ogni } i = 3, 2$$

Pertanto esistono $4 \cdot 4 \cdot 8 \cdot 8 = 1.024$ funzioni polinomiali distinte.
Si calcola che i polinomi biettivi sono 128: di cui 32 di I grado della forma $a_1x + a_0$ con a_1 dispari, 32 di II grado della forma $2x^2 + a_1x + a_0$ e 64 di III grado con coefficiente direttore 2.
Si noti che 128 è l'ordine dei 2-sottogruppi di Sylow di S_8.
Il coniugio rispetto a questo gruppo fornisce 67 classi di coniugio, di cui 20 del gruppo G stesso. Le classi d'isomorfismo di algebre monounarie polinomiali di ordine 8 si riducono a 45 e coinvolgono 156.648 funzioni, lo $0,93\%$ del totale.

4.2.3 Il caso dell'anello $\mathbb{Z}_9$

Consideriamo $f : \mathbb{Z}_9 \to \mathbb{Z}_9$; esistono $9^9 = 387.420.489$ funzioni diverse di cui $9! = 362.880$ biettive.
Dal lemma 4.1.3 si ha che $n = 9 = 3 \cdot 3$ quindi $h = 3$ e $q = 3$; allora:

1. $f(x) = 3 \cdot \prod_{r=0}^{2}(x - r) = 2x(x - 1)(x - 2)$ è identicamente nullo in $\mathbb{Z}_9$.

2. Il più piccolo m tale che 3 divida $m!$ è $m = 3$ quindi
   $g(x) = 3 \cdot \prod_{i=0}^{2}(x + i) = 3x(x + 1)(x + 2)$ è identicamente nullo in $\mathbb{Z}_9$

3. Il più piccolo r tale che 9 divida $r!$ è $r = 6$ quindi
   $p(x) = \prod_{j=0}^{5}(x + j) = x(x + 1)(x + 2)(x + 3)(x + 4)(x + 5)$ è identicamente nullo in $\mathbb{Z}_9$.

Da 1. (e analogamente da 2.) si ottiene che il polinomio $3x^3 + 6x$ è identicamente nullo in $\mathbb{Z}_9$, quindi $3x^3 \equiv 3x$, da cui segue anche $3x^5 = x^2 \cdot 3x^3 \equiv$

$x^2 \cdot 3x = 3x^3 \equiv 3x$ e $3x^4 = x \cdot 3x^3 \equiv x \cdot 3x = 3x^2$.
Da 3. invece si ha che un polinomio monico di grado 6 identicamente nullo è $x\,(x+1)\,(x+2)\,(x+3)\,(x+4)\,(x+5) \equiv x^6 + 6x^5 + 4x^4 + 4x^2 + 3x$.

Dal lemma 4.1.4 si ha che $n = 9 = 3^3$ quindi $p = 3$ e $h = 3$; allora:

1. $p(x) = \prod_{i=0}^{2} (x+i)^2 = x^2\,(x+1)^2\,(x+2)^2$ è un polinomio monico identicamente nullo in $\mathbb{Z}_9$

Questa condizione mi da il polinomio $x^6+6x^5+4x^4+3x^3+4x^2 \equiv x^6-2x^4+x^2$ ottenuto dal punto 1. del lemma 4.1.3. Non esistono polinomi monici di grado minore di 6 identicamente nulli [4].
Quindi in $\mathbb{Z}_9$ le funzioni polinomiali si riconducono tutte alla forma:

$$a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \ \textit{con}\ 0 \le a_i \le 2 \ \textit{per ogni}\ i = 5, 4, 3$$

Pertanto esistono $3 \cdot 3 \cdot 3 \cdot 9 \cdot 9 \cdot 9 = 19.683$ funzioni polinomiali.
I polinomi biettivi sono in tutto 1.296 e il loro gruppo G contiene un 3-sottogruppo di Sylow di S_9 di ordine 3^4.
Per determinare le classi d'isomorfismo, bisogna trovare prima i 1.296 polinomi biettivi, per ciascuno bisogna determinare l'espressione polinomiale dell'inversa e poi le classi di coniugio rispetto al gruppo G da essi costituito. Si ottengono così 146 classi di coniugio. Tracciando il grafo di ciascuna di esse e accorpando le classi di algebre isomorfe, si trovano 136 classi distinte contenenti 5.045.852 algebre polinomiali, circa $1,3\%$ del totale.

Per tutti i casi il calcolo è stato eseguito mediante il software Excel e poi i grafi sono stati tracciati manualmente e confrontati sulla base delle loro caratteristiche topologiche. Per ciascun grafo Γ è possibile determinare il gruppo degli automorfismi $Aut(\Gamma)$ (cioè degli isomorfismi con se stesso). Il numero di algebre con quel grafo è allora $\frac{n!}{|Aut(\Gamma)|}$.

[4] Si verifica imponendo che il generico polinomio di grado 5 sia identicamente nullo su $\mathbb{Z}_9$; si ricava che tutti i coefficienti, compreso il coefficiente direttore, devono essere congrui a 3 o a 9.

4.2.4 Congetture

A partire dai risultati ottenuti nei casi appena analizzati, si possono ipotizzare delle congetture:

1. Per ogni $n = p^h$, il gruppo G dei polinomi biettivi contiene un p-sottogruppo di Sylow del gruppo simmetrico S_n.

2. Se $n = 2^h$, il gruppo G dei polinomi biettivi coincide con un 2-sottogruppo di Sylow del gruppo simmetrico S_n.

Osservazione 22. Si osserva che il gruppo H dei polinomi di I grado invertibili, ha ordine $p^h \cdot \varphi\left(p^h\right) = p^{2h-1} \cdot (p-1)$ e quindi G ha ordine multiplo di $p-1$.

Se le congetture sono vere, si può avanzare la seguente previsione:

- Per $n = 16$, divisore di 6!, si hanno funzioni polinomiali di grado massimo 5. Un sottogruppo di Sylow di S_{16} ha ordine 2^{15}, quindi G dovrebbe avere quest'ordine.

Prima di andare ad analizzare nel dettaglio il caso dell'anello $\mathbb{Z}_{16}$, riportiamo nei paragrafi successivi quanto ottenuto per il calcolo del numero delle funzioni polinomiali negli anelli $\mathbb{Z}_{25}$, $\mathbb{Z}_{49}$ e $\mathbb{Z}_{27}$ e mostriamo nel paragrafo 4.3 quanto già accennato in precedenza riguardo al fatto che due algebre polinomiali di $\mathbb{Z}_{mn}$ potrebbero essere isomorfe anche se provengono da fattori non isomorfi.

4.2.5 Funzioni polinomiali nell'anello $\mathbb{Z}_{25}$

Sia $f : \mathbb{Z}_{25} \to \mathbb{Z}_{25}$; esistono 25^{25} funzioni diverse, di cui 25! biettive.

Dal lemma 4.1.3 si ha che $n = 25 = 5 \cdot 5$ quindi $h = 5$ e $q = 5$; allora:

1. $f(x) = 5 \cdot \prod_{r=0}^{4} (x - r) = 5x(x-1)(x-2)(x-3)(x-4)$ è identicamente nullo in $\mathbb{Z}_{25}$.

2. Il più piccolo m tale che 5 divida $m!$ è $m = 5$ quindi $g(x) = 5 \cdot \prod_{i=0}^{4} (x + i)$ è identicamente nullo in $\mathbb{Z}_{25}$

3. Il più piccolo r tale che 25 divida $r!$ è $r = 10$ quindi $p(x) = \prod_{j=0}^{9}(x+j) = x(x+1)(x+2)\cdots(x+9)$ è un polinomio monico identicamente nullo in $\mathbb{Z}_{25}$ di grado 10.

Da 1. (e analogamente da 2.) si ottiene che il polinomio $5x^5 + 20x$ è identicamente nullo in $\mathbb{Z}_{25}$, quindi $5x^5 \equiv 5x$, da cui segue $5x^9 \equiv 5x^8 \equiv 5x^7 \equiv 5x^6 \equiv 5x^5 \equiv 5x$.

Dal lemma 4.1.4 si ha che $n = 25 = 5^2$ quindi $p = 5$ e $h = 2$; allora:

1. $p(x) = \prod_{i=0}^{4}(x+i)^2 = x^2(x+1)^2(x+2)^2(x+3)^2(x+4)^2$ è un polinomio monico identicamente nullo di grado 10 in $\mathbb{Z}_{25}$.

Se si mostra che non esistono polinomi monici di grado minore di 10 identicamente nulli, allora in $\mathbb{Z}_{25}$ le funzioni polinomiali si riconducono tutte alla forma:

$$a_9x^9 + a_8x^8 + a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

con $0 \leq a_i \leq 4$ per ogni $i = 5, 6, 7, 8, 9$ e con $0 \leq a_i \leq 24$ per ogni $i = 0, 1, 2, 3, 4$.

Pertanto avremmo $5^5 \cdot 25^5 = 5^5 \cdot 5^{10} = 5^{15}$ funzioni polinomiali.

4.2.6 Funzioni polinomiali nell'anello $\mathbb{Z}_{49}$

Sia $f : \mathbb{Z}_{49} \to \mathbb{Z}_{49}$; esistono 49^{49} funzioni diverse, di cui 49! biettive.

Dal lemma 4.1.3 si ha che $n = 49 = 7 \cdot 7$ quindi $h = 7$ e $q = 7$; allora:

1. $f(x) = 7 \cdot \prod_{r=0}^{6}(x-r) = 7x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)$ è identicamente nullo in $\mathbb{Z}_{49}$.

2. Il più piccolo m tale che 7 divida $m!$ è $m = 7$ quindi $g(x) = 7 \cdot \prod_{i=0}^{6}(x+i)$ è identicamente nullo in $\mathbb{Z}_{49}$

3. Il più piccolo r tale che 49 divida $r!$ è $r = 14$ quindi
   $p(x) = \prod_{j=0}^{13}(x+j) = x(x+1)(x+2)\cdots(x+13)$ è un polinomio monico identicamente nullo in $\mathbb{Z}_{49}$ di grado 14.

Da 1. (e analogamente da 2.) si ottiene che il polinomio $7x^7 + 42x$ è identicamente nullo in $\mathbb{Z}_{49}$, quindi $7x^7 \equiv 7x$, da cui segue $7x^{13} \equiv 7x^{12} \equiv 7x^{11} \equiv 7x^{10} \equiv 7x^9 \equiv 7x^8 \equiv 7x^7 \equiv 7x$.

Dal lemma 4.1.4 si ha che $n = 49 = 7^2$ quindi $p = 7$ e $h = 7$; allora:

1. $p(x) = \prod_{i=0}^{6}(x+i)^2 = x^2(x+1)^2(x+2)^2(x+3)^2(x+4)^2(x+5)^2(x+6)^2$
   è un polinomio monico identicamente nullo di grado 14 in $\mathbb{Z}_{49}$.

Se si mostra che non esistono polinomi monici di grado minore di 14 identicamente nulli, allora in $\mathbb{Z}_{49}$ le funzioni polinomiali si riconducono tutte alla forma:

$$a_{13}x^{13}+a_{12}x^{12}+a_{11}x^{11}+a_{10}x^{10}+a_9x^9+a_8x^8+a_7x^7+a_6x^6+a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$$

con $0 \leq a_i \leq 6$ per ogni $i = 7, 8, 9, 10, 11, 12, 13$ e con $0 \leq a_i \leq 48$ per ogni $i = 0, 1, 2, 3, 4, 5, 6$.
Pertanto avremmo $7^7 \cdot 49^7 = 7^7 \cdot 7^{14} = 7^{21}$ funzioni polinomiali.

4.2.7 Funzioni polinomiali nell'anello $\mathbb{Z}_{27}$

Sia $f : \mathbb{Z}_{27} \to \mathbb{Z}_{27}$; esistono 27^{27} funzioni diverse di cui 27! biettive.
Dal lemma 4.1.3 si ha che $n = 27 = 3 \cdot 9$ quindi $h_1 = 3$, $q_1 = 9$ e $h_2 = 9$, $q_2 = 3$; allora:

1. $f_1(x) = 3 \cdot \prod_{r=0}^{8}(x-r) = 3x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)(x-7)(x-8)$
   $f_2(x) = 9 \cdot \prod_{r=0}^{2}(x-r) = 9x(x-1)(x-2)$
   sono identicamente nulli in $\mathbb{Z}_{27}$.

2. Il più piccolo m_1 tale che 9 divida $m_1!$ è $m_1 = 6$ e il più piccolo m_2 tale che 3 divida $m_2!$ è $m_2 = 3$ quindi

$g_1(x) = 3\prod_{i=0}^{5}(x+i) = 3x(x+1)(x+2)(x+3)(x+4)(x+5)$
$g_2(x) = 9\prod_{i=0}^{2}(x+i)$
sono identicamente nulli in $\mathbb{Z}_{27}$.

3. Il più piccolo r tale che 27 divida $r!$ è $r = 9$ quindi
$p(x) = \prod_{j=0}^{8}(x+j)$ è un polinomio monico identicamente nullo in $\mathbb{Z}_{27}$ di grado 9.

Da 1. si ottiene che i polinomi $3x^9 - 18x^6 + 8x^5 + 24x^3$ e $9x^3 - 18x$ sono identicamente nulli in $\mathbb{Z}_{27}$, quindi $3x^9 \equiv 18x^6 - 8x^5 + 3x^3$ e $9x^3 \equiv 9x$.
Da 2. si ha che $3x^6 + 18x^5 + 12x^4 + 12x^2 + 9x$ è un polinomio identicamente nullo quindi $3x^6 \equiv 9x^5 - 12x^4 - 12x^2 + 9x$.

Dal lemma 4.1.4 si ha che $n = 27 = 3^3$ quindi $p = 3$ e $h = 3$; allora:

1. $p(x) = \prod_{i=0}^{2}(x+i)^3 = x^3(x+1)^3(x+2)^3$ è un polinomio monico identicamente nullo su $\mathbb{Z}_{27}$.

Se si mostra che non esistono polinomi monici di grado minore di 9 identicamente nulli, allora in $\mathbb{Z}_{27}$ le funzioni polinomiali si riconducono tutte alla forma:

$$a_8x^8 + a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

con $0 \leq a_i \leq 2$ per ogni $i = 7, 7, 8$, con $0 \leq a_i \leq 8$ per ogni $i = 3, 4, 5$ e con $0 \leq a_i \leq 26$ per ogni $i = 0, 1, 2$.
Pertanto avremmo $3^3 \cdot 9^3 \cdot 27^3 = 3^3 \cdot 3^6 \cdot 3^9 = 3^{18}$ funzioni polinomiali.

4.3 Il caso dell'anello $\mathbb{Z}_6$

Andiamo ad analizzare nel dettaglio il caso $n = 6$, per mostrare che le classi d'isomorfismo di algebre polinomiali possono essere meno rispetto alle attese; cioè, nonostante il lemma 4.1.1 ci dica che $\mathbb{Z}_{mn}[x] \cong \mathbb{Z}_m[x] \times$

$\mathbb{Z}_n[x]$, $PF_{mn}[x] \cong PF_m[x] \times PF_n[x]$, $PF_{mn}[x] \cap S_{mn} = (PF_m[x] \cap S_m) \times (PF_n[x] \cap S_n)$, per le classi di isomorfismo non vale un discorso analogo. Infatti, come già affermato in precedenza, esistono 3 classi di isomorfismo per $n = 2$, 7 per $n = 3$ ma solo 19 per $n = 6$ e non 21 come ci si aspetterebbe. Consideriamo $f : \mathbb{Z}_6 \to \mathbb{Z}_6$; esistono $6^6 = 46.656$ funzioni diverse di cui $6! = 720$ biettive.

Dal lemma 4.1.3 si ha che $n = 4 = 2 \cdot 3$ quindi $h_1 = 2$, $q_1 = 3$ e $h_2 = 3$, $q_2 = 2$; allora:

1. $f_1(x) = 2 \cdot \prod_{r=0}^{2}(x - r) = 2x(x-1)(x-2)$
   $f_2(x) = 3 \cdot \prod_{r=0}^{1}(x - r) = 3x(x-1)$
   sono identicamente nulli in $\mathbb{Z}_6$.

2. Il più piccolo m_1 tale che 3 divida $m_1!$ è $m_1 = 3$ e il più piccolo m_2 tale che 2 divida $m_2!$ è $m_2 = 2$ quindi
   $g_1(x) = 2\prod_{i=0}^{2}(x + i) = 2x(x+1)(x+2)$
   $g_2(x) = 3\prod_{i=0}^{1}(x + i) = 3x(x+1)$
   sono identicamente nulli in $\mathbb{Z}_6$.

3. Il più piccolo r tale che 6 divida $r!$ è $r = 3$ quindi
   $p(x) = \prod_{j=0}^{2}(x + j) = x(x+1)(x+2)$ è identicamente nullo in $\mathbb{Z}_6$.

Da 1. (e analogamente da 2.) si ottiene che i polinomi $2x^3 + 4x$ e $3x^2 - 3x$ sono identicamente nulli in $\mathbb{Z}_6$, quindi $2x^3 \equiv 2x$ e $3x^2 \equiv 3x$.

Da 3. invece si ha che un polionomio monico di grado 3 identicamente nullo è $x(x+1)(x+2) \equiv x^3 + 3x^2 + 2x$. Per le identità precedenti si ha che questo polinomio si riduce al polinomio $x^3 + 5x$.

Il nucleo $Ker(\mu)$ dell'omomorfismo μ è l'ideale di $\mathbb{Z}_6[x]$ generato dai polinomi $3x^2 + 3x$ e $x^3 + 5x$.

Allora ogni funzione polinomiale distinta è del tipo $ax^2 + bx + c$, con $a = 0, 1, 2$, quindi ci sono in tutto $3 \cdot 6 \cdot 6 = 108 (= 2^2 \cdot 3^3)$ funzioni polinomiali distinte.

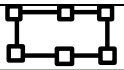
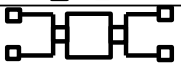
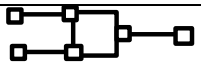
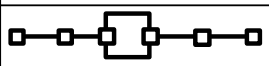
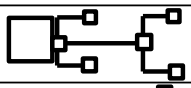
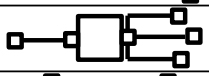
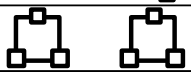
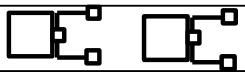
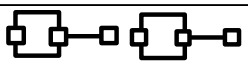
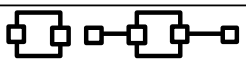
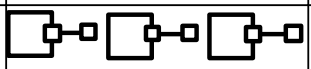
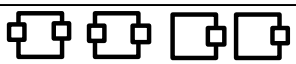
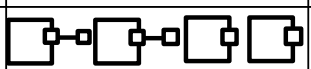
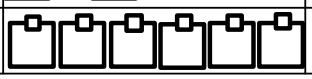
Per determinare quante sono le classi di isomorfismo delle algebre polinomiali, iniziamo con lo stabilire quali polinomi sono biettivi. Sia $f(x) = ax^2 + bx + c$,

con $a = 0, 1, 2$. Osserviamo che, posto $g(x) = ax^2 + bx$, allora $|Im(f)| = |Im(g)|$, quindi f è biettiva se e solo se lo è g. Si ha intanto $(a, b) \neq (0, 0)$.

- Se $a = 0$ allora b deve essere invertibile in $\mathbb{Z}_6$, quindi $b = \pm 1$. Quindi ci sono $2 \cdot 6$ polinomi invertibili con $a = 0$; cioè quelli del tipo $\pm x + c$.
- Sia $a = 1$:
  - Se b è pari, $b = 2b'$, allora $f(x) = \left(x + b'\right)^2 + \left(c - b'^2\right)$, ma in $\mathbb{Z}_6$ ci sono solo 4 quadrati e quindi $|Im(f)| \leq 4$.
  - Se b è dispari, allora $x^2 + b \cdot x$ è sempre pari, quindi $|Im(f)| \leq 3$.
- Se $a = 2$ allora $f(x)$ è l'opposta di $h(x) = x^2 - (b + 3) \cdot x - c$ (poiché $3x^2 \equiv 3x$), che per il punto precedente non è biettiva, dunque non lo è nemmeno f.

Pertanto esistono solo $12 (= 2! \cdot 3!)$ polinomi biettivi che costituiscono un sottogruppo H di S_6 rispetto alla composizione, isomorfo al gruppo D_6 dell'esagono regolare. L'azione di questo gruppo determina una prima suddivisione in classi di coniugio che, mediante l'esame dei rispettivi grafi, produce la suddivisione definitiva in 19 classi. Sono coinvolte tutte le 108 funzioni polinomiali e in tutto ci sono 2.867 algebre polinomiali, il 6% del totale.

Di seguito viene riportata una tabella riassuntiva, con l'elenco delle algebre polinomiali di ordine 6, comprendente per ciascuna una funzione polinomiale come rappresentante della classe, il numero di funzioni polinomiali coniugate e il numero di algebre coniugate.

n°	Rappresentante	Grafo	Polinomi Coniugati	Algebre Coniugate
1	0		6	6
2	$x+1$		2	120
3	3x+1		3	90
4	4x+1		3	120
5	x^2+1		6	360
6	x^2+x		12	180
7	x^2+x+1		12	120
8	$x+2$		2	40
9	2x		6	360
10	3x		3	90
11	x^2+2		12	360
12	x^2+3		6	180
13	x^2+4		6	360
14	x^2+x+2		12	120
15	$x+3$		1	15
16	4x		3	120
17	5x		6	45
18	x^2		6	180
19	x		1	1

4.4 Un approccio combinatorio

Nei paragrafi precedenti abbiamo determinato l'ordine del gruppo G_n costituito dalle funzioni polinomiali biettive da $\mathbb{Z}_n$ a se stesso rispetto alla

composizione, ottenendo $|G_4| = 8$, $|G_8| = 128$, $|G_9| = 1296$. Questi valori sono stati ricavati direttamente via computer, man mano si creava il catalogo delle funzioni polinomiali.
E' possibile tentare un approccio diverso, che non faccia uso della verifica diretta, seguendo un metodo combinatorio che presenteremo in questa sezione. Partiamo con delle definizioni che ci saranno utili per la comprensione del metodo.

Definizione 4.2. Sia $f : \mathbb{Z}_n \to \mathbb{Z}_n$ e $x_0 \in \mathbb{Z}_n$.
Esistono certamente dei polinomi $p \in \mathbb{Z}_n[x]$ tali che $f(x_0) = p(x_0)$: ad esempio $p(x) = x + (f(x_0) - x_0)$.
Sia $P(x_0, f)$ l'insieme di tali polinomi.
$\forall p \in P(x_0, f)$ sia poi $U_{p,f}(x_0) = \{x \in X | p(x) = f(x)\}$.
Si definisce *grado di algebricità locale* di f in x_0 il massimo numero di elementi di questi insiemi $U_{p,f}(x_0)$ e lo si denota con $ad_{x_0}(f)$.

Osservazione 23. f è polinomiale se e solo se $ad_{x_0}(f) = \mathbb{Z}_n$.

Definizione 4.3. Sia $f : \mathbb{Z}_n \to \mathbb{Z}_n$. Diremo che f ha *grado di algebricità* k se esistono $x_1, \ldots, x_k \in X$ distinti ed un polinomio $p \in \mathbb{Z}_n[x]$ tali che $\forall i$, $1 \leq i \leq k$, $f(x_i) = p(x_i)$, mentre la stessa cosa non vale per $k + 1$.
Denotiamo con $ad(f)$ il suo grado di algebricità.

Osservazione 24. Per ogni i risulta $ad_{x_i}(f) \leq ad(f)$. Inoltre $ad(f)$ è il massimo degli $ad_{x_0}(f)$ al variare di $x_0 \in \mathbb{Z}_n$.

Ad ogni funzione è possibile associare il suo grado di algebricità. Si ha allora una partizione dell'insieme delle funzioni $f : \mathbb{Z}_n \to \mathbb{Z}_n$ in classi d'equivalenza rispetto a tale grado.

$$f \approx g \Leftrightarrow ad(f) = ad(g)$$

Se n è primo c'è una sola classe, quella delle funzioni polinomiali, tutte di grado n. Se n non è primo ce ne sono di grado inferiore.

Sfruttiamo questo concetto di approssimazione polinomiale per il calcolo delle funzioni polinomiali biettive e verifichiamo che, anche attraverso questo nuovo procedimento otteniamo gli stessi risultati per i casi $n = 4$, $n = 8$, $n = 9$.

4.4.1 L'ordine di G_4

Dalla sezione precedente sappiamo che un polinomio su $\mathbb{Z}_4$ è riconducibile alla forma $p(x) = a_0 + a_1x + a_2x^2 + a_3x^3$, con $0 \leq a_3 \leq 1$, $0 \leq a_2 \leq 1$. Consideriamo ora una funzione $f : \mathbb{Z}_4 \to \mathbb{Z}_4$ e poniamo $p(i) = b_i = f(i)$, $0 \leq i \leq 3$. Riducendo *mod* 4 si ottiene il seguente sistema:

$$\begin{cases} a_0 = b_0 \\ a_0 + a_1 + a_2 + a_3 = b_1 \\ a_0 + 2a_1 = b_2 \\ a_0 + 3a_1 + a_2 + 3a_3 = b_3 \end{cases}$$

Se f è polinomiale le equazioni sono tutte compatibili; quindi con alcuni passaggi si ottiene:

$$\begin{cases} a_0 = b_0 \\ a_1 + a_2 + a_3 = b_1 + 3b_0 \\ 2a_1 = 3b_0 + b_2 \\ 2a_3 = b_0 + 3b_1 + 3b_2 + b_3 \end{cases}$$

da cui

$$\begin{cases} b_0 + b_2 \text{ pari} \\ b_1 + b_3 \text{ pari} \end{cases}$$

Si dimostra che queste due condizioni esprimono l'incompatibilità di una o due equazioni rispetto alle altre; quindi f è polinomiale se e solo se sono verificate entrambe.

Esplicitiamo le condizioni:

$$\begin{cases} b_2 = b_0 + 2t_0 \\ b_3 = b_1 + 2t_1 \end{cases}, \text{ con } 0 \leq t_i \leq 1.$$

Il polinomio sarà biettivo se i 4 valori sono tutti distinti.
La coppia $\{b_0, b_2\}$ può allora coincidere o con $\{0, 2\}$ o con $\{1, 3\}$ e analogamente la coppia $\{b_1, b_3\}$. Pertanto, scelto b_0, una delle coppie $\{0, 2\}$ o $\{1, 3\}$ è fissata, quindi per $\{b_1, b_3\}$ resta la scelta solo dell'altra coppia. Quindi per ciascuna delle 4 scelte per b_0, ce n'è solo una per b_2, due per b_1 e solo una per b_3. Si ritrova quindi che G_4 ha $4 \cdot 1 \cdot 2 \cdot 1 = 2^3 = 8$ elementi.

4.4.2 L'ordine di G_8

Nel paragrafo precedente abbiamo visto che un polinomio in $\mathbb{Z}_8$ è riconducibile alla forma $a_0 + a_1x + a_2x^2 + a_3x^3$, con $0 \leq a_i \leq 3$ per ogni $i = 3, 2$. Consideriamo ora una funzione $f : \mathbb{Z}_8 \to \mathbb{Z}_8$ e poniamo $p(i) = b_i = f(i)$, $0 \leq i \leq 7$.

$$\begin{cases} a_0 = b_0 \\ a_0 + a_1 + a_2 + a_3 = b_1 \\ a_0 + 2a_1 + 4a_2 + 8a_3 = b_2 \\ a_0 + 3a_1 + 9a_2 + 27a_3 = b_3 \\ a_0 + 4a_1 + 16a_2 + 64a_3 = b_4 \\ a_0 + 5a_1 + 25a_2 + 125a_3 = b_5 \\ a_0 + 6a_1 + 36a_2 + 216a_3 = b_6 \\ a_0 + 7a_1 + 49a_2 + 343a_3 = b_7 \end{cases}$$

Riducendo *mod* 8 si ottiene il sistema:

$$\begin{cases} a_0 = b_0 \\ a_0 + a_1 + a_2 + a_3 = b_1 \\ a_0 + 2a_1 + 4a_2 = b_2 \\ a_0 + 3a_1 + a_2 + 3a_3 = b_3 \\ a_0 + 4a_1 = b_4 \\ a_0 + 5a_1 + a_2 + 5a_3 = b_5 \\ a_0 + 6a_1 + 4a_2 = b_6 \\ a_0 + 7a_1 + a_2 + 7a_3 = b_7 \end{cases}$$

Da cui:

$$\begin{cases} b_2 - b_0 = 2a_1 + 4a_2 \\ b_4 - b_2 = 2a_1 + 4a_2 \\ b_6 - b_4 = 2a_1 + 4a_2 \end{cases} e \begin{cases} b_3 - b_1 = 2a_1 + 2a_3 \\ b_5 - b_1 = 4a_1 + 4a_3 \\ b_7 - b_1 = 6a_1 + 6a_3 \end{cases}$$

Quindi, esprimendo b_2, b_4, b_6 in funzione di b_0 e b_3, b_5, b_7 in funzione di b_1 e ponendo $a_1 + a_3 = t$ si ottiene:

$$\begin{cases} b_2 = b_0 + 2a_1 + 4a_2 \\ b_4 = b_0 + 4a_1 \\ b_6 = b_0 + 6a_1 + 4a_2 \end{cases} e \begin{cases} b_3 = b_1 + 2t \\ b_5 = b_1 + 4t \\ b_6 = b_1 + 6t \end{cases}$$

Si ha che:

- a_1 deve essere dispari altrimenti b_4 sarebbe uguale a b_0;
- b_2 può valere solamente $b_0 + 2$ o $b_0 + 6$;
- b_6 può valere rispettivamente $b_0 + 6$ o $b_0 + 2$.

Dunque per $\{b_0, b_2, b_4, b_6\}$ possiamo avere solo le due sequenze $\{b_0, b_0 + 2, b_0 + 4, b_0 + 6\}$ e $\{b_0, b_0 + 6, b_0 + 4, b_0 + 2\}$; quindi ci sono $8 \times 2 = 16$ possibilità.

Mentre per $\{b_1, b_3, b_5, b_7\}$ si ha che:

- t deve essere dispari altrimenti b_5 sarebbe uguale a b_1;

- t e $t+4$ danno la stessa lista quindi t può valere solo 1 o 3;

- b_1 ha solo le 4 possibilità diverse da b_0, b_2, b_4, b_6.

Pertanto questa seconda quaterna ha solo 8 possibilità.

Le due quaterne sono indipendenti: se b_0 è pari, allora lo sono anche b_2, b_4, b_6, quindi b_1 è necessariamente dispari e lo sono anche b_3, b_5, b_7 e viceversa.
Si ritrova quindi che G_8 ha $2^3 \cdot 2 \cdot 2^2 \cdot 2 = 2^7 = 128$ elementi.

4.4.3 L'ordine di G_9

Abbiamo visto che un polinomio in $\mathbb{Z}_9$ è riconducibile alla forma $p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5$, con $0 \leq a_i \leq 2$ per ogni $i = 5, 4, 3$.
Consideriamo ora una funzione $f : \mathbb{Z}_9 \to \mathbb{Z}_9$ e poniamo $p(i) = b_i = f(i)$, $0 \leq i \leq 8$.

$$\begin{cases} a_0 = b_0 \\ a_0 + a_1 + a_2 + a_3 + a_4 + a_5 = b_1 \\ a_0 + 2a_1 + 4a_2 + 8a_3 + 16a_4 + 32a_5 = b_2 \\ a_0 + 3a_1 + 9a_2 + 27a_3 + 81a_4 + 243a_5 = b_3 \\ a_0 + 4a_1 + 16a_2 + 64a_3 + 256a_4 + 1024a_5 = b_4 \\ a_0 + 5a_1 + 25a_2 + 125a_3 + 625a_4 + 3125a_5 = b_5 \\ a_0 + 6a_1 + 36a_2 + 216a_3 + 1296a_4 + 7776a_5 = b_6 \\ a_0 + 7a_1 + 49a_2 + 343a_3 + 2401a_4 + 16807a_5 = b_7 \\ a_0 + 8a_1 + 64a_2 + 512a_3 + 4096a_4 + 32768a_5 = b_8 \end{cases}$$

Riducendo *mod* 9 si ottiene il sistema:

$$\begin{cases} a_0 = b_0 \\ a_0 + a_1 + a_2 + a_3 + a_4 + a_5 = b_1 \\ a_0 + 2a_1 + 4a_2 + 8a_3 + 7a_4 + 5a_5 = b_2 \\ a_0 + 3a_1 = b_3 \\ a_0 + 4a_1 + 7a_2 + a_3 + 4a_4 + 7a_5 = b_4 \\ a_0 + 5a_1 + 7a_2 + 8a_3 + 4a_4 + 2a_5 = b_5 \\ a_0 + 6a_1 = b_6 \\ a_0 + 7a_1 + 4a_2 + a_3 + 7a_4 + 4a_5 = b_7 \\ a_0 + 8a_1 + a_2 + 8a_3 + a_4 + 8a_5 = b_8 \end{cases}$$

Se f è polinomiale le equazioni sono tutte compatibili.
Sostituendo la prima espressione alla quarta e la settima, la seconda alla quinta e l'ottava e la terza alle restanti si ottiene:

$$\begin{cases} a_0 = b_0 \\ a_0 + a_1 + a_2 + a_3 + a_4 + a_5 = b_1 \\ a_0 + 2a_1 + 4a_2 + 8a_3 + 7a_4 + 5a_5 = b_2 \\ b_3 = b_0 + 3a_1 \\ b_4 = b_1 + 3a_1 + 6a_2 + 3a_4 + 6a_5 \\ b_5 = b_2 + 3a_1 + 3a_2 - 3a_4 - 3a_5 \\ b_6 = b_0 + 6a_1 \\ b_7 = b_1 + 6a_1 + 3a_2 + 6a_4 + 3a_5 \equiv b_1 + 6a_1 + 12a_2 + 6a_4 + 12a_5 \\ b_8 = b_2 + 6a_1 - 3a_2 - 6a_4 + 3a_5 \equiv b_2 + 6a_1 + 6a_2 - 6a_4 - 6a_5 \end{cases}$$

Che equivale a:

$$\begin{cases} a_0 = b_0 \\ a_0 + a_1 + a_2 + a_3 + a_4 + a_5 = b_1 \\ a_0 + 2a_1 + 4a_2 + 8a_3 + 7a_4 + 5a_5 = b_2 \\ b_3 = b_0 + 3a_1 \\ b_4 = b_1 + 3\,(a_1 + 2a_2 + a_4 + 2a_5) \\ b_5 = b_2 + 3\,(a_1 + a_2 - a_4 - a_5) \\ b_6 = b_0 + 6a_1 \\ b_7 = b_1 + 6\,(a_1 + 2a_2 + a_4 + 2a_5) \\ b_8 = b_2 + 6\,(a_1 + a_2 - a_4 - a_5) \end{cases}$$

Esplicitando le condizioni si ottiene:

$$\begin{cases} b_3 = b_0 + 3t_0 \\ b_4 = b_1 + 3t_1 \\ b_5 = b_2 + 3t_2 \\ b_6 = b_0 + 6t_0 \\ b_7 = b_1 + 6t_1 \\ b_8 = b_2 + 6t_2 \end{cases}, \text{ con } 0 \leq t_i \leq 2.$$

A questo punto per trovare il numero di funzioni biettive procediamo come per i casi precedenti.
Le sei condizioni suddividono i valori in tre terne: $\{b_0, b_3, b_6\}$, $\{b_1, b_4, b_7\}$ e $\{b_2, b_5, b_8\}$ che possono assumere i valori: $\{0, 3, 6\}$, $\{1, 4, 7\}$ e $\{2, 5, 8\}$. Quindi partendo da una terna qualsiasi, ad esempio $\{b_0, b_3, b_6\}$, ci sono 9 possibili valori per b_0, due per b_1 e solo uno per b_2; a seguire, considerando ad esempio la terna $\{b_1, b_4, b_7\}$ restano 6 possibili valori per b_1, due per b_4 e uno per b_7; infine tre valori per b_2, due per b_5 e uno per b_8. Si ritrova quindi che G_9 ha $9 \cdot 2 \cdot 1 \cdot 6 \cdot 2 \cdot 1 \cdot 3 \cdot 2 \cdot 1 = 1296$ elementi.

4.4.4 L'ordine di G_{16}

Il passo finale di questa trattazione è quello di andare a verificare se la congettura fatta nella sezione 4.2.4 è verificata anche nel caso di $\mathbb{Z}_{16}$.

Per prima cosa andiamo a vedere a quale forma può essere ricondotto un generico polinomio in $\mathbb{Z}_{16}$.
Sia $f : \mathbb{Z}_{16} \to \mathbb{Z}_{16}$; esistono 16^{16} funzioni diverse di cui 16! biettive.
Dal lemma 4.1.3 si ha che $n = 16 = 8 \cdot 2 = 4 \cdot 4 = 2 \cdot 8$ quindi $h_1 = 8, q_1 = 2$, $h_2 = 4, q_2 = 4$ e $h_3 = 2, q_3 = 8$; allora:

1. $f_1(x) = 8 \prod_{r=0}^{1} (x - r) = 8x(x - 1)$
   $f_2(x) = 4 \prod_{r=0}^{3} (x - r) = 4x(x - 1)(x - 2)(x - 3)$
   $f_2(x) = 2 \prod_{r=0}^{7} (x - r) = 2x(x - 1)(x - 2)(x - 3)(x - 4)(x - 5)(x - 6)(x - 7)$
   sono identicamente nulli in $\mathbb{Z}_{16}$.

2. Il più piccolo m_1 tale che 2 divida $m_1!$ è $m_1 = 2$, il più piccolo m_2 tale che 4 divida $m_2!$ è $m_2 = 4$ e il più piccolo m_3 tale che 8 divida $m_3!$ è $m_3 = 4$ quindi:
   $g_1(x) = 8 \prod_{i=0}^{1} (x + i) = 8x(x + 1)$
   $g_2(x) = 4 \prod_{i=0}^{3} (x + i) = 4x(x + 1)(x + 2)(x + 3)$
   $g_3(x) = 2 \prod_{i=0}^{3} (x + i) = 2x(x + 1)(x + 2)(x + 3)$
   sono identicamente nulli in $\mathbb{Z}_{16}$.

3. Il più piccolo r tale che 16 divida $r!$ è $r = 6$ quindi
   $p(x) = \prod_{j=0}^{5} (x + j) = x(x + 1)(x + 2)(x + 3)(x + 4)(x + 5)$ è identicamente nullo in $\mathbb{Z}_{16}$.

Da f_1 e f_2 (e analogamente da g_1 e g_2) si ottiene che i polinomi $8x^2 - 8x$ e $4x^4 + 12x^2$ sono identicamente nulli in $\mathbb{Z}_{16}$, quindi $8x^2 \equiv 8x$ e $4x^4 \equiv 4x^2$, da cui segue $8x^5 \equiv 8x^4 \equiv 8x^3 \equiv 8x^2 \equiv 8x$.
Da g_3 si ha che $2x^4 + 12x^3 + 6x^2 + 12x$ è un polinomio identicamente nullo in $\mathbb{Z}_{16}$ quindi $2x^4 \equiv 4x^3 + 10x^2 + 4x$.
Da 3. invece si ha che un polinomio monico di grado 6 identicamente nullo è $x(x + 1)(x + 2)(x + 3)(x + 4)(x + 5)$.
Dal lemma 4.1.4 si ha che $n = 16 = 2^4$ quindi $p = 2$ e $h = 4$; allora:

1. $p(x) = \prod_{i=0}^{1} (x + i)^4 = x^4 (x + 1)^4$ è un polinomio monico identica-

mente nullo in $\mathbb{Z}_{16}$.

Questa condizione dà un polinomio monico di grado 8; poiché ho trovato un polinomio monico identicamente nullo in $\mathbb{Z}_{16}$ di grado minore, posso tralasciarla.
Non essendoci polinomi monici di grado 5 identicamente nulli, in $\mathbb{Z}_{16}$ le funzioni polinomiali distinte hanno la forma $a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$, con $0 \leq a_4, a_5 \leq 1$ e $0 \leq a_2, a_3 \leq 7$.
Pertanto esistono $2 \cdot 2 \cdot 8 \cdot 8 \cdot 16 \cdot 16 = 2^{16}$ funzioni polinomiali distinte.

Consideriamo ora una funzione $f : \mathbb{Z}_{16} \to \mathbb{Z}_{16}$ e poniamo $p(i) = b_i = f(i)$, $0 \leq i \leq 15$.

$$a_0 = b_0$$

$$a_1 + a_2 + a_3 + a_4 + a_5 = b_1$$

$$a_0 + 2a_1 + 4a_2 + 8a_3 = b_2$$

$$a_0 + 3a_1 + 9a_2 + 11a_3 + a_4 + 3a_5 = b_3$$

$$a_0 + 4a_1 = b_4$$

$$a_0 + 5a_1 + 9a_2 + 13a_3 + a_4 + 3a_5 = b_5$$

$$a_0 + 6a_1 + 4a_2 + 8a_3 = b_6$$

$$a_0 + 7a_1 + a_2 + 7a_3 + a_4 + 7a_5 = b_7$$

$$a_0 + 8a_1 = b_8$$

$$a_0 + 9a_1 + a_2 + 9a_3 + a_4 + 9a_5 = b_9$$

$$a_0 + 10a_1 + 4a_2 + 8a_3 = b_{10}$$

$$a_0 + 11a_1 + 9a_2 + 3a_3 + a_4 + 11a_5 = b_{11}$$

$$a_0 + 12a_1 = b_{12}$$

$$a_0 + 13a_1 + 9a_2 + 5a_3 + a_4 + 13a_5 = b_{13}$$

$$a_0 + 14a_1 + 4a_2 + 8a_3 = b_{14}$$

$$a_0 + 15a_1 + a_2 + 15a_3 + a_4 + 15a_5 = b_{15}$$

Esprimendo $b_3, b_5, b_7, b_9, b_{11}, b_{13}, b_{15}$ in funzione di b_1 e $b_2, b_4, b_6, b_8, b_{10}, b_{12}, b_{14}$ in funzione di b_0 si ottiene:

$$\begin{cases} b_3 = b_1 + 2t_1 + 8t_2 \\ b_5 = b_1 + 4t_1 + 8t_2 \\ b_7 = b_1 + 6t_1 \\ b_9 = b_1 + 8t_1 \\ b_{11} = b_1 + 10t_1 + 8t_2 \\ b_{13} = b_1 + 12t_1 + 8t_2 \\ b_{15} = b_1 + 14t_1 \end{cases} \quad e \quad \begin{cases} b_2 = b_0 + 2a_1 + 4t_3 \\ b_4 = b_0 + 4a_1 \\ b_6 = b_0 + 6a_1 + 4t_3 \\ b_8 = b_0 + 8a_1 \\ b_{10} = b_0 + 10a_1 + 4t_3 \\ b_{12} = b_0 + 12a_1 \\ b_{14} = b_0 + 14a_1 + 4t_3 \end{cases}$$

con $t_1 = a_1 + a_3 + a_5$, $t_2 = a_2 + a_3$ e $t_3 = 4\,(a_2 + 2a_3)$.
Per il primo sistema si ha che:

- t_1 deve essere dispari altrimenti b_9 sarebbe uguale a b_1 inoltre per $t_1 = 1, 3, 5, 7$ ottengo la stessa lista che per $t_1 = 9, 11, 13, 15$;

- t_2 può essere o 0 o 1;

Per il secondo sistema deve valere:

- a_1 deve essere dispari altrimenti b_8 sarebbe uguale a b_0 inoltre per $a_1 = 1, 3, 5, 7$ ottengo la stessa lista che per $a_1 = 9, 11, 13, 15$;

- t_3 può assumere solo i valori $0, 1, 2, 3$;

- b_0 può assumere tutti i valori eccetto quelli di $b_1, b_3, b_5, b_7, b_9, b_{11}, b_{13}, b_{15}$.

Inoltre si ha che:

- poiché $t_1 = a_1 + a_3 + a_5$ deve essere dispari e a_1 anche, $a_3 + a_5$ deve essere pari;

- se b_1 è pari allora lo sono anche $b_3, b_5, b_7, b_9, b_{11}, b_{13}, b_{15}$ e quindi $b_0, b_2, b_4, b_6, b_8, b_{10}, b_{12}, b_{14}$ devono essere dispari, altrimenti se b_1 è dispari si ha il viceversa. Quindi necessariamente $b_1 - b_0 = a_1 + a_2 + a_3 + a_4 + a_5$ deve essere dispari; poiché a_1 è dispari e $a_3 + a_5$ è pari, allora $a_2 + a_4$ deve essere pari. Allora $b_1 = a_1 + a_2 + a_3 + a_4 + a_5$ deve necessariamente essere dispari.

Quindi per $\{b_1, b_3, b_5, b_7, b_9, b_{11}, b_{13}, b_{15}\}$ si hanno $8 \cdot 4 \cdot 2$ possibili scelte, mentre per $\{b_0, b_2, b_4, b_6, b_8, b_{10}, b_{12}, b_{14}\}$ ce ne sono $8 \cdot 4 \cdot 4$.
Si ritrova quindi che l'ordine di G_{16} sarà sicuramente $\leq 2^3 \cdot 2^2 \cdot 2 \cdot 2^3 \cdot 2^2 \cdot 2^2 = 2^{13}$.

Ora $16! = 2^{15} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$, quindi il 2-sottogruppo di Sylow ha ordine 2^{15}.
Pertanto si conclude che la congettura esposta nella sezione 4.2.4 è falsa.

Attraverso una verifica diretta, con l'ausilio di un piccolo programma, siamo andati a determinare esattamente il numero di funzioni polinomiali biettive su $\mathbb{Z}_{16}$ che risulta essere proprio 2^{13}.

4.5 Conclusione

Analizzando i risultati ottenuti per i casi $\mathbb{Z}_4$, $\mathbb{Z}_8$ e $\mathbb{Z}_{16}$ per i quali abbiamo mostrato che l'ordine del gruppo delle funzioni polinomiali biettive è rispettivamente $|G_4| = 2^3$, $|G_8| = 2^7$ e $|G_{16}| = 2^{13}$, si può formulare la seguente congettura:

Congettura 4.5.1. *L'ordine del gruppo delle funzioni polinomiali biettive su* $\mathbb{Z}_{2^n}$ *è* $2^{\binom{n^2-n+1}{}}$.

Bibliografia

[1] A. Vistoli, Note di Algebra, Bologna 1993/94.

[2] M. Bianchi, A. Gillio, L. Verardi, Monounary Simple Algebras, Contemporary Mathematics Vol 402, 2004, pagine 119-132.

[3] Gelosi Giacomo, Classificazione di Algebre Monounarie, tesi di Laurea Magistrale in Matematica, A.A. 2010/2011, Bologna.

[4] Accogli Marilena, Polinomi e funzioni polinomiali negli anelli $\mathbb{Z}_n$, tesi di Laurea Triennale in Matematica, Ottobre 2007, Bologna.

[5] L. Verardi, Algebre Mono-unarie Polinomiali.

Ringraziamenti

Al termine di questa tesi un particolare ringraziamento va al mio relatore, il prof. Libero Verardi, per la sua completa disponibilità e pazienza, per avermi sempre seguita e indirizzata durante questo percorso e messa in condizione di svolgere con entusiasmo un lavoro interessante e piacevole.