Alma Mater Studiorum · Università di Bologna

facoltà di scienze matematiche, fisiche e naturali
Corso di Laurea in Matematica
ordinamento vigente

POLINOMI BIIETTIVI

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof.
Libero Verardi

Presentata da:
Righetti Roberta

Prima Sessione
Anno Accademico 2010-2011

'l'essenza della matematica risiede nella sua libertá'

G.Cantor

Introduzione

Indice

Capitolo 1

Polinomi Biiettivi in $\mathbb{R}$

In generale, in algebra moderna, un polinomio ad una indeterminata x e a coefficienti in un anello $\mathbb{A}$ (che supponiamo essere commutativo) é un espressione formale del tipo

$$a_0x^0 + ... + a_nx^n + ... \tag{1.1}$$

dove a_0, a_1, a_2,... sono elementi di $\mathbb{A}$ t.c solo un numero finito di essi sono diversi da 0.
Ora dato un tale polinomio, si puó definire in un opportuno dominio $\mathbb{A}$ una funzione f: $\mathbb{A} \to \mathbb{A}$, (dove in questo primo caso sará $\mathbb{A} = \mathbb{R}$) detta funzione polinomiale associata di grado $\leq$ n (se $a_n \neq 0$), con n $\in \mathbb{N}$, facendo corrispondere ad ogni elemento x di $\mathbb{R}$ l'elemento:

$$\sum_{k=0}^{n} a_kx^k \tag{1.2}$$

si dice allora che si è calcolato il polinomio nell'elemento x ottenendone cosí la sua valutazione nell'elemento x del campo. Osserviamo pertanto che i polinomi possono essere visti sia da un punto di vista formale sia da un punto di vista funzionale e malgrado si presentino nella stessa forma ció non é mai causa di equivoci perché restano comunque concetti ben distinti. Non solo si possono dare esempi di anelli commutativi in cui a polinomi diversi é associata una medesima funzione polinomiale (ció accade ad esempio nel

caso di anelli finiti) ma nel caso della funzione polinomiale la x non viene pensata come un'indeterminata bensí come variabile nell'anello. Tuttavia, trattando di polinomi in $\mathbb{R}$ (discorso analogo in $\mathbb{C}$) i due concetti si possono identificare per il Principio di identitá dei polinomi. Dal punto di vista formale assegnare un polinomio a coefficienti in $\mathbb{K}$ o equivalentemente (per $\mathbb{K} = \mathbb{R}$, $\mathbb{C}$) una funzione polinomiale, significa assegnare la sequenza dei suoi coefficienti $a_0, a_1, ..., a_n$,..(la variabile non gioca nessun ruolo) allora per il Principio di identitá, secondo cui due polinomi in $\mathbb{K}[x]$ sono uguali se e solo se sono uguali le relative funzioni polinomiali, si vede che, ricordando la definizione di funzione polinomiale, due polinomi **p** e **q** sono uguali se e solo se $\forall$ x $\in \mathbb{R}$

$$\sum_{k=0}^{n} p_k x^k = \sum_{k=0}^{n} q_k x^k \tag{1.3}$$

$\forall k = 0...n, \quad p_k = q_k$.

Vogliamo ora definire la somma e il prodotto di polinomi, in maniera tale che l'insieme delle funzioni polinomiali reali divenga un anello commutativo che indicheremo con $\mathbb{R}[x]$.

Definizione. Siano **f**, **g** due polinomi cosí definiti

f= $a_0x^0 + ... + a_nx^n$+...

g= $b_0x^0 + ... + b_nx^n$+...

la somma di **f** e **g** é

f+**g**= $(a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + (a_3 + b_3)x^3$+...

il prodotto di **f** e **g** é

f$\cdot$ **g**= $(a_0 \cdot b_0) + (a_1 \cdot b_0 + a_0 \cdot b_1)x + (a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2)x^2 +$

$(a_3 \cdot b_0 + a_2 \cdot b_1 + a_1 \cdot b_2 + a_0 \cdot b_3)x^3 + ...$

In realtá quello che ora ci proporremo di studiare è la struttura di un sottoinsieme di $\mathbb{R}[x]$, l'insieme dei polinomi biiettivi reali, rispetto alla legge di composizione. In altre parole quello che vogliamo scoprire è se esistono polinomi reali biiettivi, come sono fatti e se formano un gruppo rispetto la composizione. Ovvero date due funzioni polinomiali f, g entrambe biiettive,

t.c

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad e \quad g(x) = \sum_{j=0}^{m} b_j x^j$$

vogliamo capire quando la composizione $f \circ g$ sia biiettiva, dove in base alla definizione

$$f \circ g = \sum_{i=0}^{n} a_i (\sum_{j=0}^{m} b_j x^j)^i \tag{1.4}$$

ovvero

$$f \circ g = \sum_{j=0}^{m} \cdot \sum_{i=0}^{n} a_i b_j^i x^{j \cdot i}$$

se esiste la funzione polinomiale identitá id(x) t.c $f \circ id(x) = id(x) \circ f =$ f; e se esiste l'elemento inverso f^{-1} anch'esso biiettivo t.c $f \circ f^{-1} =$ id(x).
Introduciamo prima un risultato dell'analisi che rappresenta un criterio che devono soddisfare le funzioni polinomiali, quindi in particolare le funzioni polinomiali biiettive.

Teorema 1.0.1.

Se la funzione f: $\mathbb{R} \to \mathbb{R}$ *è* definita come in (1.2) allora f $\in C^\infty(\mathbb{R}, \mathbb{R})$ e per ogni fissato $x_0 \in \mathbb{R}$, risulta

$$f(x) = \sum_{k=0}^{n} \frac{f^k(x_0)}{k!}(x - x_0)^k \tag{1.5}$$

$\forall x \in \mathbb{R}$.
Ovvero una funzione polinomiale, e quindi una funzione polinomiale biiettiva, non solo *è* 'infinitamente' derivabile ma ammette, in un punto iniziale x_0, lo sviluppo di Taylor.
Detto questo vogliamo innanzitutto definire una funzione polinomiale biiettiva cioé capire come si traduce l'iniettivitá e la suriettivitá nel caso di una funzione polinomiale. Coerentemente con la definizione classica di iniettivitá per cui presi due punti qualsiasi del dominio di una funzione f, x_1 e x_2 ad

esempio, t.c $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, (in realtá è un $\Leftrightarrow$) comprendiamo che l'eventuale esistenza di radici della funzione polinomiale (condizione necessaria perché sia suriettiva) implica che si riducano ad una sola. É fin troppo noto il caso della parabola che interseca in due punti distinti l'asse x (cioé ammette due radici distinte) e che, in corrispondenza di questi due valori, ha la stessa immagine contravvenendo cosí alla definizione stessa di iniettivitá. D'altra parte vedremo che l'esistenza della radice, è una condizione necessaria alla biettivitá, in particolare alla suriettivitá ma non è da sola sufficiente. Utilizziamo sempre l'esempio della parabola, questa volta consideriamo il caso in cui il vertice stia sull'asse x, che ammette una sola radice (con molteplicitá doppia) ma non è suriettiva, perché se il coefficiente direttore è positivo e la concavitá quindi è verso l'alto, non assume mai valori negativi. Vedremo, come nonostante l'unicitá della radice, tale funzione non è neanche iniettiva. Nell'intento di individuare e classificare le funzioni polinomiali biiettive siamo quindi di fronte al duplice problema, da una parte per garantire la suriettivitá cerchiamo tutte quelle funzioni polinomiali che ammettano radici. Dall'altra per garantire l'iniettivitá dobbiamo assicurarci che la funzione ne ammetta una sola. Ora un tipico esempio di funzioni iniettive è dato dalle funzioni strettamente monotone, funzioni crescenti o decrescenti. Diamo innanzitutto la seguente

Definizione Una funzione f: $\mathbb{R} \to \mathbb{R}$ si dice crescente (strettamente) se, per ogni coppia di punti $x_1 e x_2$ di $\mathbb{R}$ con $x_1 > x_2$, risulta $f(x_1) > f(x_2)$.
Nel considerare questo tipo di funzioni ci fa comodo richiamare il seguente

Lemma 1.0.2.

Una funzione f, continua e iniettiva in un intervallo I, è monotona.

Quindi in altre parole quando ci troviamo a trattare con funzioni monotone siamo sicuri che queste sono, in particolare, iniettive. A questo punto se ci assicuriamo le condizioni sotto le quali tali funzioni ammettano anche uno zero ed uno solo abbiamo la funzione che stiamo cercando.
Una prima funzione polinomiale che possiede tali caratteristiche di monoto-

nia ($\Rightarrow$ iniettivitá) è senz'altro la funzione lineare $f(x) = m \cdot x + q$, con $m \neq 0$ (se m=0 otteniamo la retta f(x)=q che evidentemente non è mai nè iniettiva nè suriettiva). Possiamo osservare che una tale funzione lineare é anche suriettiva poiché l'immagine è tutto $\mathbb{R}$ e l'inversa è x= $\frac{y-q}{m}$ ovvero

$$y = \frac{x}{m} - \frac{q}{m} \tag{1.6}$$

infatti se la funzione in (1.6) la chiamiamo $f^{-1}(x)$ è immediato riconoscere che $f^{-1}(x) \circ f(x)$= id(x)=x.
Osserviamo che l'inversa è a tutti gli effetti un polinomio nel senso della definizione (1.2). Richiamiamo inoltre il teorema (1.0.1) per osservare che tale funzione inversa soddisfa anche le proprietá enunciate dal teorema, quindi possiamo affermare che la funzione lineare f(x)= $m \cdot x+q$ è senzaltro biiettiva.
Ci chiediamo se una tale funzione è chiusa rispetto la composizione. Ebbene la risposta è affermativa, vediamo. Date due funzioni lineari $f(x) = m \cdot x+q$, $g(x) = r \cdot x + k$ definiamo

$$f \circ g = m(r \cdot x + k) + q \quad ovvero \quad f \circ g = mr \cdot x + k + q$$

ora se poniamo s=k+q e mr=t otteniamo

$$f \circ g = t \cdot x + s$$

è immediato riconoscere che si tratta di una funzione analoga alle funzioni componenti, anch'essa iniettiva e suriettiva.
Abbiamo riscontrato precedentemente, in termini di ragionamento, che la parabola non è biiettiva perché non è mai nè iniettiva nè suriettiva, possiamo generalizzare tale osservazione per tutte le funzioni di grado pari? La risposta è affermativa.
Osserviamo che le funzioni quadratiche $f(x) = ax^2+bx+c$ hanno per grafico una parabola ottenibile dalla funzione $x \to x^2$ per trasformazioni affini. Per essere piú precisi, $f(x) = ax^2 + bx + c$ é ottenuta dalla composizione delle seguenti funzioni φ, f e $\tilde{f}$ t.c

$$\mathbb{R} \xrightarrow{\varphi} \mathbb{R} \xrightarrow{f} \mathbb{R}$$

dove φ é l'isometria $x \to$ x+**h**, con **h** $\in \mathbb{R}$ e f(x')= x'^{2} (dove x'= x+**h**) e $\tilde{f}$ é la trasformazione affine cosí definita $\tilde{f}(x') = f(x') + k$. Con tale composizione troviamo la parabola di equazione (x'-h)$^2 + k = a(x'^2 - 2hx' + h^2) + k$, ora se poniamo

$$h = -\frac{b}{2a} \quad e \quad k = c - ah^2$$

ritroviamo la funzione di partenza. Analogamente si potrebbe dimostrare per induzione che una qualsivoglia funzione polinomiale, in particolare di grado pari

$$f_1(x) = a_{2m}x^{2m} + a_{2m-1}x^{2m-1} + ... + a_{2m-(2m-1)}x^{2m-(2m-1)} + a_0 \quad m = 1, ..., n$$

é ottenibile da

$$\tilde{f}(x) = a_{2m}(x' - h)^{2m} + k$$

ovvero trasformando

$$f_2(x) = a_{2m}x^{2m}$$

Abbiamo osservato tutto ció per motivare il seguente fatto, le caratteristiche peculiari del polinomio $f_1(x)$ come la 'forma' e la convessitá sono in stretta relazione con il coefficiente direttore del polinomio, il coefficiente del grado piú alto, in questo caso a_{2m}, e poiché abbiamo ottenuto $f_1(x)$ da $f_2(x)$ per trasformazioni 'rigide' per loro definizione forma e convessitá non sono cambiate. Inoltre il segno stesso di $f_1(x)$, pur di prendere valori di x sufficientemente grandi, coincide con quello del termine direttore, cioé $a_{2m}x^{2m}$, quindi, in buona sostanza, coincide con quello di $f_2(x)$. Inoltre le due funzioni, $f_1(x)$ e $f_2(x)$ sono 'infiniti' dello stesso ordine, cioé $lim_{x\to\infty}\frac{f_1(x)}{f_2(x)} = c, c \neq 0$.
Allora possiamo restringere le nostre osservazioni sulla funzione $f_2(x)$ sapendo che varranno anche per $f_1(x)$.
Ora vediamo che se $a_{2m} > 0 \quad lim_{x\to\pm\infty}a_{2m}x^{2m} = +\infty$ quindi la funzione $f_2(x)$ é convessa, ovvero volge la concavitá verso l'alto, e poiché l'immagine di $f_2(x) = a_{2m}x^{2m}$ é l'intervallo $[0, +\infty[$ la funzione ammette un minimo assoluto visto che per valori di x piú grandi la funzione assume definitivamente

valori sempre piú grandi. Evidentemente una tale funzione non puó essere suriettiva. D'altra parte se $a_{2m} < 0 \quad lim_{x\to\pm\infty} a_{2m}x^{2m} = -\infty$ la funzione $f_2(x)$ sará concava, ovvero volgerá la concavitá verso il basso allora, per simmetria, l'immagine di $f_2(x)$ sará l'intervallo $]-\infty, 0]$ quindi la funzione avrá invece un massimo assoluto e neanche in questo caso potrá essere suriettiva. Dobbiamo riconoscere che la definizione rigorosa di convessitá richiederebbe che presi due punti qualsiasi $x_1, x_2 \in I$, t.c $x_1 < x_2$ e I intervallo reale (non banale), una funzione f: I $\to \mathbb{R}$ si dice convessa se é verificata la seguente

$$f(x) \leq f(x_1) + \frac{f(x_2) - f(x_1)}{x_2 - x_1}(x - x_1) \quad \forall x \in]x_1, x_2[$$

Tuttavia trattandosi di funzioni di grado pari omettiamo a priori tale verifica per via del carattere definitivo di crescenza o decrescenza della funzione.
A questo punto, visto che le funzioni di grado pari mal si prestano al nostro scopo, non essendo mai in nessun caso biiettive, in particolare suriettive, vediamo cosa succede se il grado della nostra funzione é dispari, ovvero la nostra funzione polinomiale é del tipo

$$f(x) = a_{2k+1}x^{2k+1} + a_{2k}x^{2k} + ...a_1x + a_0 \quad k = 1, ..., n$$

Entriamo nel vivo del discorso considerando il seguente

Corollario 1.0.3.

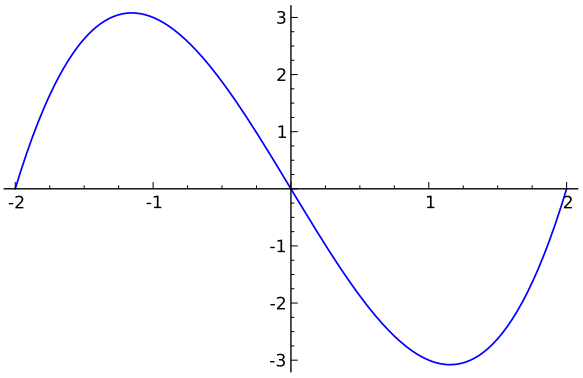
Un polinomio reale di grado dispari ha almeno una radice reale.
Dimostriamolo per via analitica. Se f é un polinomio reale di grado dispari, che potremmo supporre monico (il coefficiente direttore $a_{2k+1} = 1$), assumerá valori sia negativi che positivi a seconda che x sia negativo o positivo, in altre parole $lim_{x\to-\infty} x^{2k+1} = -\infty \quad$ e $\quad lim_{x\to+\infty} x^{2k+1} = +\infty$. Ora per un noto teorema dell'analisi, noto come Teorema degli zeri il quale afferma che se una funzione continua su un intervallo ammette sia valori positivi che negativi allora si annulla in qualche punto, resta provata la tesi.

Quindi nella scomposizione in fattori irriducibili di un tale polinomio interverrá sempre almeno un polinomio lineare.

Tuttavia che la funzione abbia grado dispari é solo condizione necessaria alla biiettivitá, non è sufficiente. Ad esempio ci sono polinomi di grado dispari che non sono iniettivi, consideriamo l'esempio di

$$f(x) = x^3 - 4x \quad \text{ovvero} \quad f(x) = x(x^2 - 4) \tag{1.7}$$

con l'ausilio del grafico è immediato riscontrare che ha 3 soluzioni.



Potremmo esibirne tantissimi di questi casi, tutti quelli che si scrivono come prodotto di polinomi e il cui grado risultante risulta dispari. Per garantire che la nostra funzione sia anche iniettiva (e che quindi abbia solo una radice) é necessario richiedere che la funzione sia sempre crescente o sempre decrescente, ovvero monotona.

Teorema 1.0.4.

Sia I un intervallo reale (non banale) e sia f: I $\to \mathbb{R}$ derivabile in ogni punto di I. Allora f é monotona strettamente crescente su I se e solo se
i) f'(x)$\geq 0 \quad \forall x \in I$;
ii) l'insieme F=$\{x \in I \quad t.c \quad f'(x) = 0\}$ non ha punti interni.
Dimostrazione. Se f é monotona strettamente crescente su I allora (per il Teorema sulla monotonía) deve essere f'(x)$\geq 0 \quad \forall x \in I$. Inoltre F non puó

avere punti interni in quanto se fosse $]x_0-\rho, x_0+\rho[\subseteq F$ per opportuni $x_0 \in I$ e $\rho > 0$ allora si avrebbe f'(x)$= 0\ \forall x \in]x_0-\rho, x_0+\rho[$ e quindi f sarebbe costante sull'intervallo $]x_0 - \rho, x_0 + \rho[$ contrariamente all'ipotesi di crescenza stretta. Viceversa, supponiamo che valgano i) ed ii). Anzitutto, per (i) risulta f $\uparrow$. Se poi, per assurdo, esistessero x_1, $x_2 \in I$ con $x_1 < x_2$ t.c $f(x_1) = f(x_2)$, f risulterebbe costante sull'intervallo $[x_1, x_2]$ poiché $f(x_1) \leq f(x) \leq f(x_2)$, per ogni $x \in [x_1, x_2]$. Quindi sarebbe $]x_1, x_2[\subseteq \{x \in I \quad t.c \quad f'(x) = 0\} \subseteq F$ ed il punto $x_0 = \frac{x_1+x_2}{2}$ risulterebbe interno ad F, contrariamente all'ipotesi ii).

Osserviamo che una funzione di grado dispari per essere iniettiva deve, nel senso di condizione necessaria e sufficiente, annullarsi in un solo punto, altrimenti nelle ipotesi del teorema, se ció non avvenisse potremmo sempre trovare in corrispondenza dei punti dove si annulla la funzione, un intorno aperto di punti dove si annulla la derivata prima. Contrariamente all'ipotesi che, l'insieme F, dei punti dove si annulla la derivata prima non abbia punti interni.
A questo punto ricordiamo un teorema dell'algebra che enuncia

Teorema 1.0.5.

Un polinomio reale di grado positivo si scompone come prodotto di fattori lineari e quadratici con discriminante negativo.

Possiamo quindi considerare funzioni polinomiali del tipo

$$f(x) = (x - c)^k \cdot q(x) \tag{1.8}$$

con k dispari e q(x) funzione polinomiale di grado pari e senza radici (ovvero con discriminante negativo).
Naturalmente sono incluse anche le funzioni $f(x) = (x - c)^k$ con k dispari, dove c puó anche essere nullo. Questo genere di funzioni soddisfano la surjettivitá perché ammettono radici (una sola con molteplicitá k) e sono iniettive nel senso del teorema (1.0.4) perché la derivata di una tale funzione *è* sempre

positiva.
Vediamo innanzitutto come si presenta la derivata della funzione in (1.8)

$$f'(x) = k(x-c)^{k-1} \cdot q(x) + (x-c)^k \cdot q'(x) \tag{1.9}$$

ovvero

$$f'(x) = (x-c)^{k-1}[k \cdot q(x) + (x-c) \cdot q'(x)]$$

Osserviamo che se k=1 allora

$$f'(x) = q(x) + (x-c) \cdot q'(x)$$

ne segue che la derivata, oltre a c, deve avere tutte radici di molteplicitá pari (se ci sono). Proviamo per induzione sul grado k, che la derivata della (1.8) é sempre fatta cosí. Il caso k=1 é provato, supponiamo vera la condizione per k= 3,5,...n-1 proviamola per n+1. Sia

$$f(x) = (x-c)^{n+1} \cdot q(x) \tag{1.10}$$

allora

$$f'(x) = (n+1)(x-c)^n \cdot q(x) + (x-c)^{n+1} \cdot q'(x)$$

ovvero

$$f'(x) = (x-c)^n[(n+1) \cdot q(x) + (x-c) \cdot q'(x)]$$

Ora il primo fattore (x-c)^n ha grado pari (perché n+1 era dispari) dentro la parentesi quadra ritroviamo q(x) polinomio irriducibile e il prodotto di due polinomi di grado dispari (x-c)$\cdot q'(x)$, ovvero un polinomio di grado pari, quindi tale derivata ha ancora oltre a c, tutte radici di molteplicitá pari (se esistono).
In conclusione condizione necessaria e sufficiente perché la funzione polinomiale sia biiettiva è che la derivata sia della forma

$$f'(x) = \prod_{j=0}^{r} (a_j x^2 + b_j x + c_j) \tag{1.11}$$

con le condizioni

$$a_j \neq 0 \quad \forall j$$

$$\Delta = b_j^2 - 4a_j c_j \leq 0 \quad \forall j$$

Vediamo il seguente esempio. Consideriamo la funzione derivata

$$f'(x) = x^2(x-1)^2(x^2+1) = x^6 - 2x^5 + 2x^4 - 2x^3 + x^2$$

Una sua primitiva é

$$f(x) = \frac{x^7}{7} - \frac{x^6}{3} + \frac{2x^5}{5} - \frac{x^4}{2} + \frac{x^3}{3}$$

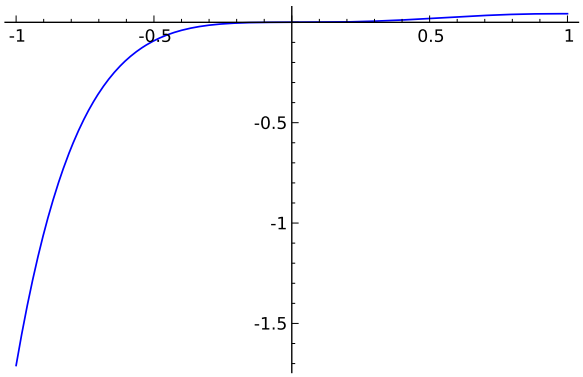
Ora studiando la funzione osserviamo che

$$f'(x) = 0 \quad per \quad x = 0, 1 \quad f''(x) = 0 \quad per \quad x = 0, 1$$

poiché

$$f'''(0) \neq 0 \quad e \quad f'''(1) \neq 0$$

allora in x=0, x=1 la funzione presenta due flessi con tangente orizzontale e poiché la f'(x) é sempre positiva la funzione é sempre crescente $\Rightarrow$ iniettiva. La suriettivitá discende dal grado dispari, quindi possiamo affermare che tale funzione é biiettiva. Vediamo il grafico della primitiva



Vediamo un altro esempio. Consideriamo la funzione derivata

$$f'(x) = x^2(x^2 + x + 1) = x^4 + x^3 + x^2$$

Una sua primitiva é

$$f(x) = \frac{x^5}{5} + \frac{x^4}{4} + \frac{x^3}{3}$$

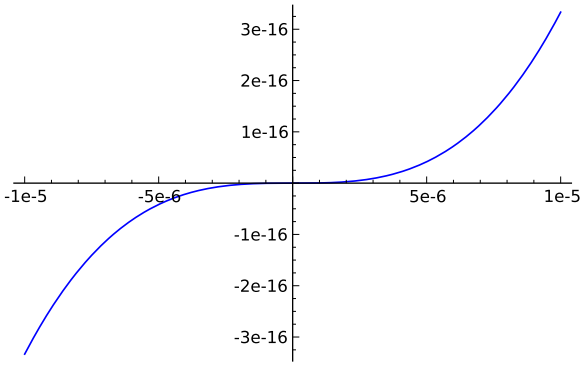
Ora studiando la funzione osserviamo che

$$f'(x) = 0 \quad per \quad x = 0 \quad f''(x) = 0 \quad per \quad x = 0$$

poiché

$$f'''(0) \neq 0$$

allora in x=0 la funzione presenta un flesso con tangente orizzontale e poiché la f'(x) é sempre positiva la funzione é sempre crescente $\Rightarrow$ iniettiva. Anche in questo caso é suriettiva, per via del grado dispari, quindi biiettiva.
Vediamo il grafico di questa primitiva



A questo punto ci chiediamo se la funzione in (1.8) *è* chiusa rispetto la composizione. Vediamo prima il caso in cui siano date due funzioni del tipo

$$f(x) = (x - c)^k; \quad g(x) = (x - a)^r \quad k, s \quad dispari$$

allora la composta sará

$$f \circ g = [(x - a)^r - c]^k$$

che *è* ancora di grado dispari, perché il termine direttore della funzione composta avrá grado $r \cdot k$, ancora dispari e sará ancora iniettiva e suriettiva perché la composizione di due funzioni iniettive e suriettive *è* ancora iniettiva e suriettiva. Vediamo la composizione nel caso in cui la funzione sia come in (1.8) cio*è* date

$$f(x) = (x - c)^k \cdot q(x); \quad g(x) = (x - a)^r \cdot s(x)$$

con k,r dispari e q(x), s(x) funzioni polinomiali di grado pari e senza radici. Allora la composta sará

$$f \circ g = [(x-a)^r \cdot s(x) - c]^k \cdot q((x-a)^r \cdot s(x)) \tag{1.12}$$

che è ancora di grado dispari, perché il termine direttore del primo fattore della (1.12) ha grado $r \cdot k$, ancora dispari, il secondo fattore è ancora un polinomio di grado pari perché il termine direttore ha grado $r\cdot$ (grado di q)= pari e sará ancora iniettiva e suriettiva per le stesse ragioni osservate prima. Vogliamo rivolgere un'attenzione particolare alla derivata della composta nel caso in cui si considerino due funzioni come in (1.8) $f(x) = (x-c)^k \cdot q(x)$; $g(x) = (x-a)^r \cdot s(x)$. Abbiamo visto che la loro composizione è

$$f \circ g = \{[(x-a)^r \cdot s(x)] - c\}^k \cdot q[(x-a)^r \cdot s(x)]$$

ora tenendo conto della definizione di derivata di una funzione composta (assunte tutte le condizioni di derivabilitá delle due funzioni f,g)

$$(f \circ g)' = f'(g) \cdot g'$$

ora avendo cura di sostituire alla x che compare come argomento della f la g(x), otteniamo

$$k\,\{[(x-a)^r \cdot s(x)] - c\}^{k-1} \cdot q[(x-a)^r \cdot s(x)] +$$

$$+[(x-a)^r \cdot s(x) - c]^k \cdot q'[(x-a)^r \cdot s(x) - c] \cdot [r(x-a)^{r-1} \cdot s(x) + (x-a)^r \cdot s'(x)]$$

Ora se poniamo l'espressione $[(x-a)^r \cdot s(x) - c] = \alpha$ otteniamo l'espressione decisamente piú leggibile

$$k \cdot \alpha^{k-1} \cdot q(\alpha + c) + \alpha^k \cdot q'(\alpha) \cdot \overbrace{r(x-a)^{r-1} \cdot s(x) + (x-a)^r \cdot s'(x)}^{derivata \quad di \quad g}$$

facendo attenzione a ció che succede ai gradi osserviamo che α^{k-1} è un polinomio di grado pari, perché α è il prodotto dei polinomi (a meno di una costante c), $(x-a)^r$ dove r è dispari, e s(x) polinomio di grado pari, il grado risultante di tale prodotto sará quindi dispari, ma poiché abbiamo α^{k-1} e k-1

è pari, allora per proprietá delle potenze, α^{k-1} sará pari. Ragionando similmente per tutti gli altri termini osserviamo che q$(\alpha + c)$ è un polinomio di grado pari, il prodotto tra α^k e q'(α) è pari, perché i polinomi sono entrambi dispari e per la proprietá delle potenze la somma di esponenti dispari è pari, e la derivata della g è come ci aspettavamo che fosse. Abbiamo cosí provato che le funzioni polinomiali biiettive sono chiuse rispetto alla composizione, in quanto anche la derivata della loro composizione è del tipo richiesto. Tuttavia il nostro proponimento é raggiunto solo in parte, in quanto noi volevamo provare se l'insieme dei polinomi biiettivi fosse o meno un gruppo rispetto alla legge di composizione, in particolare rispetto all'inverso. Vediamo che la risposta sfortunatamente é negativa, quando studiamo l'inversa di tali funzioni ci accorgiamo che una tale funzione non é un polinomio, vediamo.
Avevamo osservato, in prima battuta, che una funzione polinomiale qualsiasi, indipendentemente dal grado

$$f_1(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x^1 + a_0$$

é ottenibile da

$$\tilde{f}(x) = a_n(x' - h)^n + k$$

ovvero operando trasformazioni 'rigide' su

$$f_2(x) = a_n x^n$$

Allora, per quanto $f_1(x)$ e $f_2(x)$ esprimano analiticamente diverse relazioni tra i punti piano, riconosciamo che rappresentano lo stesso luogo geometrico. Quindi poiché forma, convessitá e segno della funzione $f_1(x)$ sono determinati dal termine direttore, in buona sostanza sono determinati dalla funzione $f_2(x)$. Detto questo, possiamo aspettarci che l'inversa di $f_2(x)$ $''assomigli''$ graficamente all'inversa di $f_1(x)$. E' inevitabile ammettere che é decisamente piú facile invertire, ad esempio

$$f_2(x) = \frac{x^5}{5}$$

piuttosto che

$$f_1(x) = \frac{x^5}{5} + \frac{x^4}{4} + \frac{x^3}{3}$$

Vediamo che l'inversa di $f_2(x)$ é la funzione radice quinta, infatti

$$f_2^{-1} \circ f_2(x) = \sqrt[5]{5} \cdot \sqrt[5]{\frac{x^5}{5}} = x$$

Purtroppo per noi, peró anche se abbiamo trovato un'inversa approssimativa di $f_1(x)$ riscontriamo che tale funzione non é un polinomio nel senso della definizione di funzione polinomiale, perché gli esponenti delle funzioni polinomiali sono tutti numeri naturali, mentre l'inversa f_2^{-1} *è* una funzione il cui esponente *è* frazionario.
Concludendo osserviamo che, poiché qualsiasi sia il grado della funzione, purché dispari, siamo autorizzati ad affermare che per ogni k (ovviamente dispari) esistono polinomi biiettivi di grado k, ma non tutti sono chiusi rispetto l'inverso (ovvero solo le funzioni lineari lo sono) allora vale il seguente

Teorema 1.0.6.

Siano f, g polinomi biiettivi, allora f$\circ g$ é un polinomio biiettivo. Poiché anche l'identitá y=x é biiettivo (é il primo caso che abbiamo considerato) i polinomi biiettivi $\in \mathbb{R}[x]$ formano un monoide rispetto alla composizione. Inoltre, $\forall$ f biiettivo e $\forall$ k $\in \mathbb{R}$ anche f+k é biiettivo.

Capitolo 2

Polinomi Biiettivi in $\mathbb{C}$

Analogamente a quanto abbiamo visto in $\mathbb{R}$, dato un polinomio

$$a_0x^0 + ... + a_nx^n + ...$$

possiamo definire una funzione polinomiale in $\mathbb{C}$ tale che $f : \mathbb{C} \to \mathbb{C}$ fa corrispondere ad ogni elemento z di $\mathbb{C}$ l'elemento:

$$\sum_{k=0}^{n} a_k z^k \tag{2.1}$$

Diciamo allora che f(z) cosí definita é la funzione polinomiale di grado $\leq n$ (se $a_n \neq 0$), con n $\in \mathbb{N}$.
Ora, per il noto teorema fondamentale dell'algebra, il campo $\mathbb{C}$ é algebricamente chiuso, ovvero ciascun polinomio in $\mathbb{C}$ si scrive come prodotto di polinomi lineari. Vediamo come questo influisce sulla caratterizzazione dei polinomi biiettivi. Per definizione un campo $\mathbb{K}$ si dice algebricamente chiuso se ogni polinomio in $\mathbb{K}[x]$ di grado almeno 1 ha una radice in $\mathbb{K}$. Ora, poiché per un noto teorema, un polinomio irriducibile in $\mathbb{K}[x]$ ha una radice se e solo se ha grado 1, come conseguenza, un campo $\mathbb{K}$ é algebricamente chiuso se e solo se i polinomi irriducibili sono tutti e solo quelli di primo grado, ovvero ogni polinomio si scrive come prodotto di fattori lineari. Diamo la seguente

Definizione. Sia f un polinomio non nullo a coefficienti in $\mathbb{K}$, **a** un elemento di $\mathbb{K}$. La molteplicitá di **a** come radice di f, in simboli μ(f,**a**), *è* il massimo intero non negativo m tale che (x-**a**)^{m}divide$f$.
In altre parole m è il numero di volte in cui possiamo dividere f per (x-**a**).
Vale il seguente

Teorema 2.0.7.

Siano $a_1, ..., a_t$ le radici di un polinomio $f \in \mathbb{K}[x]$ di grado positivo. Allora, detta μ la molteplicitá di una radice di f, vale

$$\mu(f, a_1) + ... + \mu(f, a_t) = deg(f) \tag{2.2}$$

se e solo se f *è* un prodotto di fattori lineari (altrimenti vale $\leq$).
Quindi in $\mathbb{C}$ tutti i polinomi ammettono un numero di radici uguale al grado, se ciascuna radice viene contata con la propria molteplicitá. Come ovvia conseguenza se f *è* una funzione polinomiale di grado n (n>1) allora f puó scriversi come

$$(1) f(z) = a_n(z-z_0)^n \quad \text{oppure} \quad (2) f(z) = a_n(z-z_1)^{m_1} \cdot (z-z_2)^{m_2} \cdot ... (z-z_t)^{m_t}$$

nel caso in cui f ammetta una sola radice con molteplicitá pari a n, caso (1), nel caso in cui f ammetta t radici distinte e per il teorema visto prima, vale $m_1 + m_2 + ... + m_t = n$, caso(2) (il caso (2) puó anche essere fattorizzato come $f(z) = a_n(z - z_1) \cdot (z - z_2) \cdot ... (z - z_n)$ con $z_1, z_2, ..., \cdot z_n$ radici non tutte distinte). Come abbiamo osservato nel precedente capitolo, l'iniettivitá della funzione polinomiale richiederebbe che, se una funzione polinomiale ammette zeri, questi si riducano ad uno solo. Quindi, per iniettivitá, siamo costretti a considerare solo i casi in cui f si scriva cosí

$$f(z) = a_n(z - z_0)^n \tag{2.3}$$

ovvero possiamo considerare tutti e solo quei polinomi che ammettono una sola radice, con molteplicitá pari al grado.
D'altra parte non appena consideriamo il caso in cui f(z)=1, cioé

$$a_n(z - z_0)^n = 1 \quad ovvero \quad (z - z_0)^n = \frac{1}{a_n} \tag{2.4}$$

perdiamo ancora l'iniettivitá per via del seguente

Teorema 2.0.8.

Ogni numero complesso non nullo ha precisamente n radici n-esime distinte. Se $\beta^n = \alpha \neq 0$ e $w = cos(\frac{2\pi}{n}) + isin(\frac{2\pi}{n})$ allora le radici n-esime di α sono

$$\beta, w\beta, w^2\beta, ..., w^{n-1}\beta.$$

Quindi la (2.4) avrebbe n soluzioni distinte pari a

$$z = z_0 + k_i \quad 1 \leq i \leq n$$

e k_i radice n-esima di $\frac{1}{a^n}$.
Resta il caso in cui f sia una funzione lineare, ovvero

$$f(z) = a_0 + a_1 z \quad con \quad a_1 \neq 0 \tag{2.5}$$

altrimenti scritta

$$f(z) = m \cdot z + a_0 \quad con \quad m \neq 0$$

Per quanto visto precedentemente, una tale funzione è sempre iniettiva perché monotona, ammette inversa z= $\frac{f(z)-a_0}{m}$, ovvero

$$f^{-1}(z) = \frac{z}{m} - \frac{a_0}{m} \tag{2.6}$$

è suriettiva e chiusa rispetto la composizione (valgono le osservazioni fatte nel precedente capitolo). Per le ragioni viste sopra quindi gli unici polinomi biiettivi in $\mathbb{C}$ sono quelli di primo grado e poiché sono chiusi rispetto la composizione e l'inverso possiamo affermare che formano un gruppo rispetto la legge di composizione.

Capitolo 3

Polinomi Biiettivi in $\mathbb{Z}_m$

Diamo la seguente definizione. Sia

$$p(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x] \tag{3.1}$$

Sia m un intero qualsiasi. Allora il polinomio

$$\overline{p}(x) = \sum_{k=0}^{n} [a_k]_m x^k \in \mathbb{Z}_m[x] \tag{3.2}$$

si dice la riduzione modulo m di p(x) e quindi

$$\overline{f} : \mathbb{Z}_m \to \mathbb{Z}_m \tag{3.3}$$

è la corrispondente funzione polinomiale.
Breve cenno delle classi di resto modulo m. Dati due interi a,b e un intero positivo m, detto modulo, diciamo che a e b sono congruenti modulo m, in simboli $a \equiv b$ (mod m), se a-b *è* divisibile per m.
Stiamo perció considerando l'omomorfismo suriettivo tra anelli di polinomi

$$\overline{\varphi_m} : \mathbb{Z}[x] \to \mathbb{Z}_m[x], \quad p \mapsto \overline{p} \tag{3.4}$$

che estende in modo naturale l'omomorfismo canonico suriettivo

$$\varphi_m : \mathbb{Z} \to \mathbb{Z}_m \tag{3.5}$$

($\overline{\varphi_m}$ *è* definito nel modo sopra indicato $\overline{\varphi_m}(\mathrm{p}) = \overline{p} = \sum_{k=0}^{n}[a_k]_m x^k$). Ora vogliamo considerare la seguente proprietá degli anelli finiti.

Teorema 3.0.9.

Se f *è* una funzione t.c f: $X \to Y$ e X,Y sono finiti con lo stesso numero di elementi, allora f: $X \to Y$ *è* suriettiva se e solo se *è* iniettiva.
Dim. Supponiamo che f sia suriettiva allora, per definizione, ogni elemento del codominio Y *è* immagine, attraverso f, di qualche elemento del dominio X. Supponiamo che (ragionando per assurdo) un certo y_0 del codominio sia immagine di due elementi del dominio x_1 e x_2, cioè $f(x_1) = f(x_2) = y_0$.
Allora, poiché X e Y hanno lo stesso numero, finito, di elementi ci saranno elementi del dominio non coinvolti nell'azione di f, ovvero $f^{-1}(Y) \subset X$ ma ció *è* assurdo perché avevamo supposto che f fosse un'applicazione suriettiva. Quindi f suriettiva $\Rightarrow$ f iniettiva. Per dimostrare l'implicazione inversa basta osservare che per iniettivitá si satura il codominio.
Ora vediamo che la funzione polinomiale definita su $\mathbb{Z}_m$ $\overline{f}$ *è* al tempo stesso iniettiva e suriettiva, quindi biiettiva, se e solo se $\overline{f} \in \mathbb{S}_{\mathbb{Z}_m}$ gruppo simmetrico su $\mathbb{Z}_m$ ($\cong \mathbb{S}_m$), ovvero

$$\overline{f}(x) = x^\sigma \tag{3.6}$$

per qualche σ elemento di $\mathbb{S}_m$. In altre parole, la funzione polinomiale $\overline{f}$ deve essere un'azione di $\mathbb{S}_m$ su $\mathbb{Z}_m$. Osserviamo che una tale $\overline{f}$, cosí come l'abbiamo definita in (3.6) *è* iniettiva e suriettiva perché in corrispondenza di $\sigma \in \mathbb{S}_m$ e $x_1, x_2 \in \mathbb{Z}_m$ vale $x_1^\sigma = x_2^\sigma \Leftrightarrow \overline{f}(x_1) = \overline{f}(x_2)$ vediamo.
Consideriamo $\overline{f}$: $\mathbb{Z}_m \to \mathbb{Z}_m$ associata al polinomio definito in (3.2) allora, ricordando che la funzione polinomiale *è* una valutazione del polinomio associato nell'elemento dell'anello, in corrispondenza del primo elemento che consideriamo del dominio avremo m possibili immagini di tale elemento, cioé m modi diversi perché $\overline{f}$ possa essere suriettiva. Per il secondo elemento del dominio ne avremo m-1, perché un elemento del codominio *è* giá stato 'assegnato', e cosí via...per l'ultimo elemento avremo una scelta obbligata. In conclusione una funzione polinomiale biiettiva ha $m\cdot(m-1)\cdot(m-2)\cdot\ldots\cdot(m-(k+1))$

scelte possibili, pari al numero delle disposizioni semplici.
Anche se non possiamo dire molto sul numero di funzioni biiettive in un anello $\mathbb{Z}_m$ con m qualsiasi, un tale criterio ci consente di individuare quelle funzioni polinomiali che non lo sono.
Vediamo un semplice esempio.
Sia m=4 consideriamo f(x)= $x^4 + x^3 + x^2 + x$ (mod 4), vediamo che una tale funzione non *è* iniettiva perché $f([0]_4) = f([1]_4) = f([3]_4) = 0$ $(= [0]_4)$. Per quanto osservato sopra una tale funzione non *è* neanche suriettiva.
Ora, date due funzioni polinomiali $\overline{f}$ e $\overline{g}$ qualsiasi, (tenendo bene a mente che sono funzioni di $\mathbb{S}_{\mathbb{Z}_m}$) anche la loro composizione sará polinomiale (ovvero una funzione di $\mathbb{S}_{\mathbb{Z}_m}$). Vediamo.
Consideriamo sempre m=4, quindi $\mathbb{Z}_4$ e supponiamo che $\overline{f}$ e $\overline{g}$ siano due funzioni polinomiali tali che

$$\overline{f}(1) = 2 \qquad \overline{g}(1) = 3$$

$$\overline{f}(2) = 4 \qquad \overline{g}(2) = 4 \quad (= [0]_4)$$

$$\overline{f}(3) = 1 \qquad \overline{g}(3) = 1$$

$$\overline{f}(4) = 3 \qquad \overline{g}(4) = 2$$

Se consideriamo la funzione composta, $\overline{f} \circ \overline{g}$, sará anch'essa polinomiale e biiettiva, ovvero una funzione di $\mathbb{S}_{\mathbb{Z}_m}$. In pratica

$$\overline{f}(\overline{g}(x)) = \overline{f}(3) = 1$$

$$\overline{f}(\overline{g}(x)) = \overline{f}(4) = 3$$

$$\overline{f}(\overline{g}(x)) = \overline{f}(1) = 2$$

$$\overline{f}(\overline{g}(x)) = \overline{f}(2) = 4$$

ricordando che l'argomento della $\overline{f}$ nella composizione *è* la $\overline{g}$ calcolata in $\mathbb{Z}_4$.
Ora vediamo che anche $id_{\mathbb{Z}_m}$: x $\mapsto$ x *è* polinomiale (*è* il polinomio banale $a_1x = x$ con $a_1 = 1$) ed *è* evidentemente iniettiva e suriettiva. Inoltre qualsiasi f si consideri in $\mathbb{S}_{\mathbb{Z}_m}$ (ricordando che tali funzioni sono permutazioni) il

periodo di f è finito (cioè supponendo che esista un intero k, t.c $f^k = 1$, si chiama periodo di f il minimo intero s tale che $f^s \neq 1$) quindi vale $\overline{f^{-1}} = \overline{f^k}$, ovvero l'inversa è la composizione della medesima funzione polinomiale k-volte. Ad esempio tornando all'esempio di prima

$$\overline{f}(1) = 2 \quad \overline{f}(2) = 4 \quad \overline{f}(3) = 1 \quad \overline{f}(4) = 3$$

osserviamo che l'intero k per cui $f^k = 1$ è 4, infatti $\overline{f^4}(1) = 1$, vediamolo in modo piú esplicito

$$\overline{f^4}(1) = \overline{f}(\overline{f}(\overline{f}(\overline{f}(1)))) = \overline{f}(\overline{f}(\overline{f}(2))) = \overline{f}(\overline{f}(4) = \overline{f}(3) = 1$$

In conclusione possiamo affermare che essendo le funzioni polinomiali biiettive in $\mathbb{Z}_m$ (ovvero le funzioni di $\mathbb{S}_{\mathbb{Z}_m}$) chiuse rispetto la composizione e rispetto l'inverso, la funzione identitá è polinomiale e biiettiva, ne segue che formano un sottogruppo $\mathbb{G}$ del gruppo simmetrico su $\mathbb{Z}_m$.

Capitolo 4

Polinomi Biiettivi in $\mathbb{Z}_p$

Richiamiamo la notazione vista in $\mathbb{Z}_m$. Sia

$$p(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x] \tag{4.1}$$

Sia p un intero, primo, qualsiasi. Allora il polinomio

$$\overline{p}(x) = \sum_{k=0}^{n} [a_k]_p x^k \in \mathbb{Z}_p[x] \tag{4.2}$$

si dice la riduzione modulo p di p(x) e quindi

$$\overline{f} : \mathbb{Z}_p \to \mathbb{Z}_p \tag{4.3}$$

è la corrispondente funzione polinomiale. Osserviamo che, a differenza di quanto avveniva in $\mathbb{Z}_m$, ogni funzione f: $\mathbb{Z}_p \to \mathbb{Z}_p$ *è* polinomiale, fondamentalmente perché $\mathbb{Z}_p$ non ha divisori dello zero, vediamo. Diamo la seguente

Definizione.
Sia $\mathbb{A}$ un anello commutativo. Un elemento a $\in \mathbb{A}$ *è* un divisore dello 0 se esiste un b$\neq$ 0 in $\mathbb{A}$ con $a \cdot b$=0. Diremo anche che a divide 0.

Teorema 4.0.10.

Sia m un intero positivo e $\alpha = [a]$ una classe in $\mathbb{Z}_m$. Allora α *è* un divisore dello 0 se e solo se (a,m)>1.
Ora questa proprietá degli anelli finiti, che non siano campi, evidenzia un limite nel momento in cui considerato un certo polinomio vogliamo valutarlo, attraverso la corrispondente funzione polinomiale, in un $\mathbb{Z}_m$ qualsiasi. Ad esempio, posto m=4, consideriamo il polinomio p(x)= a_3x^3 di terzo grado, ora se consideriamo la corrispondente funzione polinomiale $\overline{f}$(x)= $[a_3]_4x^3$ con $a_3 \neq 0$, riscontriamo un comportamento un pó lacunoso, in quanto $x^3 \equiv 0$ (mod 4) per x=2, ovvero per certi valori (appunto i divisori dello zero) 'collassa' il grado, contravvenendo alla stessa definizione di funzione polinomiale che assicura che la funzione ha grado n se il coefficente n-esimo *è* diverso dallo zero. In un campo $\mathbb{Z}_p$ con p primo questo non succede mai perché vale il Teorema di Fermat, per cui $x^{p-1} \equiv 1$ (mod p), con x intero qualsiasi, e la congruenza $x^{p-1} \equiv 0$ (mod p) *è* verificata soltanto nel caso in cui x=0.
Quindi considerato ciò, poiché tutte le funzioni f: $\mathbb{Z}_p \to \mathbb{Z}_p$ sono polinomiali, se le pensiamo come le funzioni biiettive del gruppo simmetrico, troviamo che questo insieme coincide con $\mathbb{S}_p$. Ora, poiché vale

Teorema 4.0.11.

Sia $\mathbb{A}$ un insieme con n elementi, n>0. Allora $\mathbb{S}(\mathbb{A})$ ha n! elementi.

Ovvero le biiezioni da un insieme finito $\mathbb{A}$ di ordine n in sè stesso sono n!, quindi possiamo affermare che l'insieme dei polinomi biiettivi in $\mathbb{Z}_p$ ha p! elementi. A questo punto vogliamo individuare tali polinomi. Con questo intento possiamo restringere la nostra attenzione, senza perdere di generalitá, ai polinomi di grado $\leq p-1$ in quanto per il Teorema di Fermat vale

$$x^p \equiv x \Rightarrow x^{p+1} \equiv x^2 \Rightarrow x^{p+2} \equiv x^3 \Rightarrow ...x^{2p-2} \equiv x^{p-1} \tag{4.4}$$

cioè ogni esponente maggiore di p si comporta nello stesso modo di un esponente piú piccolo, compreso tra 0 e p-1.

Iniziamo dal campo $\mathbb{Z}_2$, tenendo conto di (4.4) possiamo osservare che ci sono i polinomi di primo grado della forma f(x)= ax+b e questi soltanto. Tali polinomi formano un sottogruppo di $\mathbb{S}_p$ di ordine p(p-1). L'ordine del sottogruppo di un gruppo finito, per il Teorema di Lagrange, deve dividere l'ordine del gruppo e p(p-1) *è* dato dal numero delle disposizioni semplici di n elementi in k modi diversi, $\mathbf{D}_{n,k} = \frac{n!}{(n-k)!}$. Osserviamo infatti che gli elementi di $\mathbb{Z}_2$ sono 0,1 e le possibili disposizioni o 'collocazioni' per questi due elementi sono due, un elemento come coefficiente della x e un elemento come termine noto, quindi $\frac{2!}{(2-2)!}$, ricordando che 0!=1. Quindi in $\mathbb{Z}_2$ i polinomi biiettivi sono solo due (ricordiamo che $\forall \hat{a} \in \mathbb{Z}$ t.c $a \equiv \hat{a}$ (mod m) vale $\hat{a} \in [a]_m$), ed entrambi di primo grado.
Vediamo in $\mathbb{Z}_3$. Ci saranno sempre i polinomi di primo grado, che rappresentano sempre un sottogruppo di $\mathbb{S}_p$ di ordine p(p-1) ma ovviamente saranno di piú per la precisione $\frac{3!}{(3-2)!}$ ovvero 6, dati dalle seguenti espressioni (tutte le possibili disposizioni semplici degli elementi di $\mathbb{Z}_3$)

$$x, \quad 2x, \quad x+1, \quad x+2, \quad 2x+1, \quad 2x+2$$

Ricordando che l'insieme dei polinomi biiettivi in un campo $\mathbb{Z}_p$ coincide con il gruppo simmetrico $\mathbb{S}_p$ e che, per quanto osservato precedentemente, l'ordine di $\mathbb{S}_p$ *è* p!, concludiamo che tanto in $\mathbb{Z}_2$ quanto in $\mathbb{Z}_3$ i polinomi biiettivi sono tutti e solo quelli di primo grado perché in entrambi i casi p!= p(p-1).
Vediamo che 'qualcosa' cambia in $\mathbb{Z}_5$ visto che 5!≠ 5(5-1), ovvero il numero dei polinomi di primo grado, che per la formula vista sopra *è* 20, non satura il numero dei polinomi biiettivi in $\mathbb{Z}_5$ che *è* 5! ovvero 120. Comprendiamo quindi che in $\mathbb{Z}_5$ ci sono anche polinomi biiettivi di grado > 1, vediamo in dettaglio. In generale un polinomio di grado due del tipo $ax^2 + bx + c$ (a≠ 0) *è* biiettivo $\Leftrightarrow$ $ax^2 + bx$ lo *è*. Ora vediamo che $ax^2 + bx$ = x(ax+b) ha due radici: $[0]_5$ e -$\frac{b}{a}$ che (tenendo conto del fatto che in un campo tutti gli elementi tranne lo zero sono invertibili) sará $[\tilde{b}]_5 \cdot [a^{-1}]_5$ dove $\tilde{b} \equiv$ -b (mod 5)). Dunque, volendo richiedere la biiettivitá, possiamo ammettere solo il caso in cui b = $[0]_5$. Ma in questo caso, pur ottenendo il polinomio ax^2, non soddisfiamo la condizione di biettivitá perché tale polinomio non *è* biiettivo,

in particolare iniettivo, perché $a \cdot [1^2]_5 = a \cdot [4^2]_5 = a$). Dunque i polinomi di secondo grado non sono biiettivi. Che dire di quelli di terzo grado?
Consideriamo il polinomio $ax^3 + bx^2 + cx + d$ (a$\neq 0$) di terzo grado, anche in questo caso osserviamo che $ax^3 + bx^2 + cx + d$ *è* biiettivo $\Leftrightarrow$ $ax^3 + bx^2 + cx$ lo *è* $\Leftrightarrow$ $x(x^2 + \frac{b}{a}x + \frac{c}{a})$ lo *è*.
Ora posto $b' = \frac{b}{a}$; $c' = \frac{c}{a}$ (a$\neq 0$) consideriamo il polinomio $x(x^2 + b'x + c')$ che si annulla sicuramente in x=0, ora per la biiettivitá, x=0 deve essere l'unica radice, pertanto devono verificarsi uno dei due seguenti casi: o il polinomio $x^2 + b'x + c'$ si annulla anch'esso in x=0 (e questo si verifica se e solo se $c' = [0]_5$) oppure il suo discriminante $(b')^2 - 4c' = (b')^2 + c' \pmod 5$ non deve essere un quadrato in $\mathbb{Z}_5$, ovvero il polinomio $x^2 + b'x + c'$ deve essere irriducibile in $\mathbb{Z}_5$. Vediamo che, posto $\Delta = (b')^2 + c'$, non *è* un quadrato in $\mathbb{Z}_5$ quando $\Delta = 2$, oppure $\Delta = 3$, ovvero quando $c' = 2 - (b')^2$ caso (1); oppure $c' = 3 - (b')^2$ caso (2). Si distinguono i seguenti: caso (1) $c' = 2{,}1$ e 3 per $(b')^2 = 0{,}1$ e 4 rispettivamente (a meno di congruenze); caso (2) $c' = 3{,}2$ e 4 per $(b')^2 = 0{,}1$ e 2 rispettivamente (a meno di congruenze). Vediamo la seguente tabella che indica i valori (di b' e c') che devono comparire nel polinomio $x^2 + b'x + c'$ affinché la condizione di biiettivitá sia soddisfatta

b'	c'
0	2
1	1
2	3
3	3
4	1

oppure

b'	c'
0	3
1	2
2	4
3	4
4	2

Ci sono quindi le seguenti possibilitá

$x(x^2 + 2)$ $x(x^2 + x + 1)$ $x(x^2 + 2x + 3)$ $x(x^2 + 3x + 3)$ $x(x^2 + 4x + 1)$

$x(x^2 + 3)$ $x(x^2 + x + 2)$ $x(x^2 + 2x + 4)$ $x(x^2 + 3x + 4)$ $x(x^2 + 4x + 2)$

Ora per verifica diretta (ponendo x=0,1,2,3,4 (mod 5)) proviamo l'iniettività dei suddetti polinomi ad esempio prendendo il primo polinomio x(x^2+2) verifichiamo

x	x(x^2+2)
0	0
1	3
2	2
3	3
4	2

Osserviamo che il polinomio assume lo stesso valore, 3, in corrispondenza di x=1, 3. Questo ci basta per scartarlo dalla lista dei polinomi biiettivi. Procedendo con tale verifica su tutti gli altri polinomi riscontriamo che risultano iniettivi i seguenti

$$x(x^2+2x+3) \quad x(x^2+3x+3) \quad x(x^2+x+2) \quad x(x^2+2x+4) \qquad (4.5)$$

Ora ricordando che avevamo posto $b' = \frac{b}{a}$; $c' = \frac{c}{a}$ (a$\neq$ 0) e che il polinomio di partenza era $ax^3 + bx^2 + cx + d$, quindi moltiplicando tutti i polinomi della lista (4.5) per a e sommando loro d (al variare di a e d in $\mathbb{Z}_5$) otteniamo ben 20 diversi polinomi per ciascuno di essi, tale numero *è* dato sempre da $\mathbf{D}_{n,k} = \frac{n!}{(n-k)!}$ dove n= 5 ovvero tutti i possibili valori di a tra gli elementi del campo, k=2 inteso come quantitá di modi attraverso i quali assegnare tali valori, uno per b' e uno per c', quindi in totale avremo 80 polinomi biiettivi di terzo grado. Resta fuori il caso in cui $b' = c' = 0$ in corrispondenza dei quali valori troviamo il polinomio x(x^2) che ha radice tripla x=0. Ora, al variare di a e d in $\mathbb{Z}_5$ troveremo 20 polinomi del tipo $ax^3 + d$, che vanno a sommarsi agli 80 precedentemente individuati. Ora ricordando i 20 polinomi lineari che avevamo riconosciuti come polinomi biiettivi, in apertura del

discorso, in totale avremo in $\mathbb{Z}_5$ ben 120 polinomi biiettivi, che è il numero che ci aspettavamo di trovare visto che l'insieme dei polinomi biiettivi di $\mathbb{Z}_5$ coincide con $\mathbb{S}_5$. Con questo riscontriamo anche che nessun altro polinomio di grado ≤ 4 puó quindi essere biiettivo in $\mathbb{Z}_5$.

Diamo una tabella riassuntiva delle funzioni polinomiali di ordine piccolo sull'anello $\mathbb{Z}_m$ per $1 \leq m \leq 10$. Nella seconda riga c'è il numero di elementi dell'anello delle funzioni polinomiali. Nella terza riga l'ordine del gruppo $\mathbb{G}_m$ di quelle biiettive e nella quarta il tipo di gruppo.

m	1	2	3	4	5	6	7	8	9	10
$\lvert\mathbf{P}_{A_n}\rvert$	1	4	27	64	3125	108	7^7	1024	19683	12500
$\lvert\mathbf{G}_m\rvert$	1	2	6	8	120	12	720	128	1296	240
$\mathbf{G}_m$	id	$\mathbf{S}_2$	$\mathbf{S}_3$	$\mathbf{D}_4$	$\mathbf{S}_5$	$\mathbf{D}_6$	$\mathbf{S}_7$	2-Syl	?	$\mathbf{S}_2\times\ \mathbf{S}_5$

Legenda:

• $\mathbf{S}_m$ è il gruppo simmetrico su m elementi. Se m è primo, allora $G_m \cong S_m$

• $\mathbf{D}_m$ è il gruppo delle simmetrie dell' m-agono regolare.

• Per m = 8, poiché $8! = 2^7 \cdot 3^2 \cdot 5 \cdot 7$, il gruppo G_8, di ordine $128 = 2^7$, è uno dei 2-sottogruppi di Sylow di S_8, e la sua struttura è ben nota.

• Per m=9, G_9 ha ordine $1296 = 2^4 \cdot 3^4$ e poiché $9! = 2^7 \cdot 3^4 \cdot 5 \cdot 7$, allora G_9 contiene almeno uno dei 3-sottogruppi di Sylow di S_9, ma la sua struttura è da determinare.

• Un teorema afferma che se n= m· q, con m e q coprimi, allora $G_n \cong \mathrm{G}_m \times \mathrm{G}_q$. Ne consegue che, per esempio, $G_6 \cong G_3 \times G_2 \cong S_3 \times S_2 \cong D_6$. Analogamente, $G_{10} \cong G_2 \times G_5 \cong S_2 \times S_5$, d'ordine $2 \cdot 120 = 240$. Pertanto, la tabella per l'ordine G_m si puó agevolmente ampliare, con l'esclusione delle potenze dei primi > 10 e dei loro multipli. Il primo caso aperto è per m=16.