SUGLI INTERI RELATIVI ED I POLINOMI

A.Letizia
Dipartimento di matematica. Universita' di Lecce.

Introduzione.

I proponenti del progetto pluriennale di ricerca **"Collaborazione tra Universita' e Scuola Secondaria Superiore. Problemi culturali e didattici nei nuovi Programmi di Matematica ed Informatica per la Scuola Secondaria Superiore"** mi hanno invitato a presentare alcune riflessioni riguardanti gli interi relativi ed i polinomi.

Cio' e' venuto spontaneo partendo dalla considerazione che l'estrema ricchezza del dominio degli interi e la dimestichezza che si ha con essi, con le loro operazioni e con alcune proprieta' di tale dominio, spesso portano, da una parte a non comprendere a pieno il ruolo di queste proprieta' e gli eventuali legami esistenti tra loro, dall'altra ad un uso "disinvolto" delle stesse.

Scopo di questa esposizione e' cercare di chiarire tali questioni, anche per giungere ad una migliore comprensione del mondo dei polinomi (...una volta detto cosa si intenda per polinomio!).

A tal fine e' sembrato opportuno cominciare annotando quanto sembra ben noto sugli interi, evidenziando via via i dubbi e le curiosita', per fare di questi la molla che spingera' ad una visione piu' consapevole di tutta una serie di fatti che, per essere tanti ed estremamente familiari, si finisce per non considerare piu' con la dovuta attenzione.

Ha collaborato al lavoro, con numerosi suggerimenti derivanti dalla sua lunga esperienza nella scuola secondaria superiore, la professoressa S. Leone.

1. LA RICCHEZZA DI $\mathbb{Z}$: RIFLESSIONI.

Indicato con $\mathbb{Z}$ l'insieme degli interi relativi, posto cioe' $\mathbb{Z}=\{....,-2,-1,0,1,2,...\}$, iniziamo col fare qualche "pettegolezzo" sugli interi al fine di costruirci un "inventario ragionato" dei fatti piu' noti di $\mathbb{Z}$, inventario che articoleremo in una successione di punti.

Punto 1. OPERAZIONI E PROPRIETA'.

Sappiamo che su $\mathbb{Z}$ sono definite due operazioni, cioe' due applicazioni

$+:\mathbb{Z}x\mathbb{Z}\longrightarrow\mathbb{Z}$ e $:\mathbb{Z}x\mathbb{Z}\longrightarrow\mathbb{Z}$

dette rispettivamente addizione e moltiplicazione.

Ne scaturisce subito che somma di interi a,b e' l'immagine, indicata con $a+b$ (al posto di $+[(a,b)]$), che l'applicazione addizione fa corrispondere alla coppia (a,b); quindi somma di interi e' un intero.

Analogamente prodotto di interi a,b e' un intero indicato con $a\cdot b$ o piu' semplicemente con ab.

Quanto sottolineato non ci meraviglia e d'altronde cio' non e' una caratteristica di $\mathbb{Z}$. Ben sappiamo, per esempio, che somme e prodotti di razionali sono razionali, che somme e prodotti di numeri complessi sono numeri complessi, che somme e prodotti di matrici sono matrici, che somme e prodotti di polinomi sono polinomi... ecc. ecc..

Riflettendo pero' su quanto detto viene spontaneo chiedersi: possiamo allora parlare di somma di monomi visto che in generale, come sappiamo, essa non e' un monomio?

Gia' un dubbio si fa strada...non scacciamolo, anche se in questo momento ci sembra di non poterlo chiarire; piuttosto annotiamo la domanda (sara' la prima di una serie..) e proseguiamo la nostra indagine ripromettendoci di ritornare in seguito su

questo.

Alcune proprieta' dell'addizione e della moltiplicazione in $\mathbb{Z}$ sono (o meglio dovrebbero essere!) ben note. Per completezza le riportiamo in uno schema riassuntivo:

(I) L'addizione e' associativa e commutativa. Inoltre valgono le seguenti proprieta':

$\forall a \in \mathbb{Z}$: $a+0=0+a=a$

$\forall a \in \mathbb{Z}$ $\exists b \in \mathbb{Z}$ $(a+b=b+a=0)$

(II) La moltiplicazione e' associativa e commutativa. Inoltre vale la proprieta':

$\forall a \in \mathbb{Z}$: $a \cdot 1 = 1 \cdot a = a$

(III) La moltiplicazione e' distributiva rispetto all'addizione.

Inoltre sussiste una proprieta' che e' un tipico esempio di proprieta' "occulta", nel senso che viene usata senza comprendere che la sua mancanza porterebbe al crollo di un'ala del castello di nozioni che riteniamo acquisite. Tale proprieta', nota come legge di annullamento del prodotto, dice che

(IV) $\forall a,b \in \mathbb{Z}$: $ab=0 \Leftrightarrow a=0$ oppure $b=0$.

Il sussistere di (I) viene espresso dicendo che $(\mathbb{Z},+)$ e' un gruppo commutativo con elemento neutro 0.

La (II) viene riassunta dicendo che $(\mathbb{Z},\cdot)$ e' un monoide commutativo con elemento neutro 1.

Il sussistere contemporaneo di (I),(II),(III) viene espresso affermando che $(\mathbb{Z},+,\cdot)$ e' un anello commutativo unitario. Si conviene infatti chiamare *anello commutativo unitario* ogni terna $(A,+,\cdot,)$ con A insieme non vuoto, $+,\cdot$, applicazioni da AxA in A (cioe' operazioni binarie in A) tali che:

(i) $\forall a,b \in A$: $a+b=b+a$; $\forall a,b,c \in A$: $a+(b+c)=(a+b)+c$;

$\exists z \in A \forall a \in A$ $(a+z=z+a=a)$ (si dimostra che tale z e' unico, viene

indicato con 0 ed e' detto elemento neutro rispetto all'addizione); $\forall a \in A \exists b \in A \ (a+b=b+a=0)$.

(ii) $\forall a,b \in A$: $a \cdot b = b \cdot a$; $\forall a,b,c \in A$: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

$\exists e \in A \ (a \cdot e = e \cdot a = a)$.

(Analogamente a quanto visto per 0, si dimostra che un tale e e' unico, viene indicato con 1 ed e' detto elemento neutro rispetto alla moltiplicazione.)

(iii) $\forall a,b,c \in A$: $a \cdot (b+c) = a \cdot b + a \cdot c$.

Infine il sussistere contemporaneo di (I),(II),(III),(IV) equivale ad affermare che $(\mathbb{Z},+,\cdot)$e' un dominio unitario. Si conviene infatti chiamare *dominio unitario*, in breve D.U., ogni anello commutativo unitario nel quale valga

(iv) $\forall a,b \in A$: $a \cdot b = 0 \Leftrightarrow a = 0$ oppure $b = 0$.

Punto 2. MULTIPLI, DIVISORI, ...

Dati $a,b \in \mathbb{Z}$ diciamo usualmente che a *divide* b, e scriviamo $a|b$, (da non confondersi con la frazione $\frac{a}{b}$ di numeratore a e denominatore b) se e solo se **esiste** $c \in \mathbb{Z}$ tale che $b = ca$.

Facciamo alcuni esempi per chiarire tale definizione.

L'intero 4 divide -8 perche' esiste $-2 \in \mathbb{Z}$ tale che $-8 = (-2) \cdot 4$, mentre non divide 5 perche' non esiste alcun intero che moltiplicato per 4 dia 5.

L'intero -7 divide 0 perche' esiste $0 \in \mathbb{Z}$ (non e' richiesto che c sia diverso da 0) tale che $0 = 0 \cdot (-7)$.

L'intero 0 non divide 2 perche' non esiste alcun intero che moltiplicato per 0 dia 2, mentre 0 divide 0 "ad abundantiam" in quanto $0 = 1 \cdot 0 = (-3) \cdot 0 = \ldots$(non e' richiesto che c sia unico).

Sappiamo che in $(\mathbb{Z},+,\cdot)$ valgono:

(i) $\forall a \in \mathbb{Z}$: $a|a$;

(ii) $\forall a,b,c \in \mathbb{Z}$: $a|b$, $b|c \Rightarrow a|c$.

Il sussistere di (i) e (ii) si esprime dicendo che la relazione "*...divide...*" e' un preordine in $\mathbb{Z}$.

E se a e b variano nell'insieme $\mathbb{N} = \{1,2,3,4,\ldots\}$ dei numeri

naturali invece che in tutto $\mathbb{Z}$?

Allora chiaramente (i) e (ii) valgono in particolare per ogni $a,b,c \in \mathbb{N}$; inoltre e' noto che in $\mathbb{N}$ (anche se forse non ci siamo soffermati sull'importanza dell'insieme rispetto al quale si svolgono le nostre considerazioni), vale:

(iii) $\forall a,b \in \mathbb{N}$: $a \mid b,\ b \mid a \Rightarrow a = b$.

Pertanto la relazione Δ definita in $\mathbb{N}$ ponendo:

$$\forall a,b \in \mathbb{N}: a \Delta b :\Leftrightarrow a \textit{ divide } b$$

e' una relazione d'ordine; quindi in $\mathbb{N}$, con il linguaggio proprio delle relazioni d'ordine, potremo dire che *"a e' minore o uguale b (rispetto a Δ)"* invece di *"a divide b"* e potremo scrivere $a \leq b(\Delta)$ invece di $a \mid b$.

E' opportuno notare come il comportamento di Δ sia diverso dal comportamento della relazione d'ordine usuale su $\mathbb{N}$ (indicata con $\leq$); infatti, mentre per ogni $a,b \in \mathbb{N}$ risulta che $a \leq b$ oppure che $b \leq a$, cio' non e' vero per Δ: se, per esempio, consideriamo i numeri naturali 5 e 7 osserviamo che 5 non e' minore o uguale a 7 rispetto a Δ (infatti 5 non divide 7) e che 7 non e' minore o uguale a 5 rispetto a Δ (infatti 7 non divide 5).

Notiamo anche che se $a \leq b(\Delta)$ allora $a \leq b$ rispetto alla relazione d'ordine usuale, ma non e' vero il viceversa. Infatti, 3 e' minore o uguale a 4 rispetto alla relazione d'ordine usuale, ma 3 non e'minore o uguale 4 rispetto a Δ.

Osserviamo infine che la (iii) non puo' essere estesa a $\mathbb{Z}$; infatti esistono almeno due elementi a,b di $\mathbb{Z}$ tali che ($a \mid b$, $b \mid a$) e $a \neq b$ (per esempio 2 e -2).

Punto 3. INTERI "PARTICOLARI".

In $\mathbb{Z}$ sappiamo esistere elementi "particolari"; cerchiamo di approfondire tali particolarita'.

(I) I primi numeri che vengono in mente sono 1 e -1.

Poniamo $\sqcup_{\mathbb{Z}} := \{1,-1\}$. La proprieta' di cui godono gli elementi di $\sqcup_{\mathbb{Z}}$ si esprime nel modo seguente:

$$"\forall a \in \sqcup_{\mathbb{Z}} \quad \exists b \in \mathbb{Z} \quad ab=1"$$

(osserviamo che di conseguenza $b \in \sqcup_{\mathbb{Z}}$).

Legata ad $\sqcup_{\mathbb{Z}}$ e' la relazione $\mathscr{R}$ (leggiamo *"...e' associato di.."*.) definita da:

$$\forall a,b \in \mathbb{Z} \qquad a \mathscr{R} b \ :\Leftrightarrow \ \exists u \in \sqcup_{\mathbb{Z}} \quad a=ub.$$

La relazione $\mathscr{R}$ e' di equivalenza ed esempi di classi di elementi equivalenti rispetto a $\mathscr{R}$ sono $[2]_{\mathscr{R}}=\{2,-2\}$,$[-7]_{\mathscr{R}}=\{7,-7\}$, $[0]_{\mathscr{R}}=\{0\}$; d'altra parte e' di verifica immediata il fatto che per ogni $a \in \mathbb{Z}$, $a \neq 0$ si ha che $[a]_{\mathscr{R}}=\{a,-a\}$.

(II) Altri interi particolari che vengono in mente sono 2,3,5, 7,11,....Qual e' o quali sono le proprieta' che li differenziano dagli altri? La nostra esperienza ci dice che questi numeri sono elementi $a \in \mathbb{Z}$ tali che $a \neq 0$, $a \notin \sqcup_{\mathbb{Z}}$ e per i quali valgono :

(P_1) $"\forall b,c \in \mathbb{Z} : a=bc \Rightarrow b \in \sqcup_{\mathbb{Z}}$ oppure $c \in \sqcup_{\mathbb{Z}}"$.

e

(P_2) $"\forall b,c \in \mathbb{Z} : a \mid bc \Rightarrow a \mid b$ oppure $a \mid c$ ".

Per non confonderci diciamo *irriducibile* un elemento $a \in \mathbb{Z}$, $a \neq 0$, $a \notin \sqcup_{\mathbb{Z}}$ che goda della proprieta' (P_1); diciamo *primo* un elemento $a \in \mathbb{Z}$, $a \neq 0$, $a \notin \sqcup_{\mathbb{Z}}$ che goda della proprieta' (P_2). Quindi i numeri 2,3,5,..... sono irriducibili **e** sono primi.

E i numeri -2,-3,-5,-7,....? Un attimo di riflessione ed intuiamo che anche questi interi, che sono diversi da 0 e non appartenenti a $\sqcup_{\mathbb{Z}}$, godono della proprieta' (P_1) **e** della proprieta' (P_2), sono cioe' irriducibili **e** primi.

Sempre la nostra esperienza ci suggerisce che nel <u>dominio unitario</u> $(\mathbb{Z},+,.)$ <u>essere irriducibile equivale ad essere primo</u>. Attenzione pero'! Questo non vuol dire che in $\mathbb{Z}$ la proprieta' (P_1) sia equivalente alla proprieta' (P_2). Infatti per il numero 0 si ha che esistono $a,b \in \mathbb{Z}$ tali che $0=a \cdot b$ e $a \notin \sqcup_{\mathbb{Z}}$ e $b \notin \sqcup_{\mathbb{Z}}$ (per esempio $a=0$ e $b=5$), circostanza questa che basta a garantire che 0 <u>non</u> gode della proprieta' (P_1); mentre possiamo facilmente verificare,

grazie alla legge di annullamento del prodotto, che 0 gode della proprieta' (P_2). Infatti se $0 \mid bc$ allora esiste $t \in \mathbb{Z}$ tale che $bc = t \cdot 0 = 0$ quindi $b = 0$ oppure $c = 0$ e pertanto, poiche' 0 divide 0, si ha che $0 \mid b$ oppure $0 \mid c$.

Ritornando comunque al fatto che in $\mathbb{Z}$ un elemento e' irriducibile se e solo se e' primo, siamo indotti a chiederci: perche' accade cio'? E' cosi' per gli elementi di un qualunque dominio unitario? E se cosi' non fosse, da quale proprieta' del dominio $(\mathbb{Z}, +, \cdot)$ dipende tale equivalenza? Le domande continuano ad affiorare.....comunque procediamo nel nostro elenco.

Punto 4. DIVISIONE COL RESTO.

E' noto che e' possibile estendere agli interi relativi il fatto che nell'insieme $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, costituito dai numeri naturali e dal numero 0, e' possibile "fare la divisione con il resto" intentendo con cio' affermare che, dati $a, b \in \mathbb{N}_0$ con $b \neq 0$ esistono (e sono in questo caso unici) $q, r \in \mathbb{N}_0$ tali che $a = qb + r$ con $0 \leq r < b$.

Possiamo esprimere tale estensione dicendo che esiste un'applicazione

$\varphi: \mathbb{Z} - \{0\} \longrightarrow \mathbb{N}$ (..e' il valore assoluto)

tale che

i) per ogni $a, b \in \mathbb{Z} - \{0\}$, se $a \mid b$ allora $\varphi(a) \leq \varphi(b)$;

ii) per ogni $a, b \in \mathbb{Z}$, $b \neq 0$, esistono $q, r \in \mathbb{Z}$ tali che $a = qb + r$ con $r = 0$ oppure $\varphi(r) < \varphi(b)$.

Notiamo che in ii) non si parla di unicita' di q ed r. D'altra parte e' ben noto che, dati per esempio -8 e -5, esistono $q_1 = 1$, $r_1 = -3$ e $q_2 = -2$, $r_2 = 2$ tali che $-8 = 1 \cdot (-5) + (-3)$ con $|-3| < |-5|$ e $-8 = (-2) \cdot (-5) + (+2)$ con $|2| < |-5|$; ancora, dati per esempio 7 e 2, si ha che $7 = 3 \cdot 2 + 1$ con $|1| < |2|$ ed $7 = 4 \cdot 2 + (-1)$ con $|-1| < |2|$.

Osserviamo come l'ultimo esempio ci porta a riflettere sul fatto che, riguardo alla divisione col resto, ci troviamo ancora in una situazione nella quale i numeri naturali si comportano in modo diverso a seconda che si svolgano le nostre considerazioni considerando come ambiente $\mathbb{N}_0$ oppure $\mathbb{Z}$.

Punto 5. DECOMPOSIZIONE IN FATTORI IRRIDUCIBILI.

In $(\mathbb{Z},+,\cdot)$ "ogni" elemento e' irriducibile oppure prodotto "in modo unico" di un numero finito di elementi irriducibili. Per aiutarci a formalizzare tale fatto esaminiamo alcuni esempi ed osserviamo che:

$6=2\cdot3=(-2)\cdot(-3)=3\cdot2=(-3)\cdot(-2)$;

$-8=(-2)\cdot2\cdot2=(-2)\cdot(-2)\cdot(-2)=2\cdot(-2)\cdot(2)=\ldots\ldots$.

Si vede che le decomposizioni di uno stesso intero relativo hanno tutte lo stesso numero di fattori e che, a meno dell'ordine e di fattori associati, sono "praticamente" uguali. Pero', se decidiamo di usare solo gli irriducibili positivi, abbiamo bisogno anche di -1 e si ha:

$6=2\cdot3=3\cdot2$; $-8=(-1)\cdot2\cdot2\cdot2$; $-6=(-1)\cdot2\cdot3=(-1)\cdot3\cdot2$.

Possiamo anche decidere di usare solo gli irriducibili negativi, allora $6=(-2)\cdot(-3)=(-3)\cdot(-2)$; $-8=(-2)\cdot(-2)\cdot(-2)$.

E se decidessimo di usare 2,-3,5,-7,....? Allora.....

Riflettiamo un momento sull'espressione "decidere di usare". Indicato con P l'insieme degli irriducibili di $\mathbb{Z}$, ogni volta e' come fissare sugli irriducibili una cosiddetta *funzione di scelta*

$$\varphi : P/_{\mathscr{R}} \longrightarrow P$$
$$X \longmapsto x \in X$$

Infatti, essendo $P=\{2,-2,3,-3,5,-5,7,-7,\ldots\}$ e $P/_{\mathscr{R}}=\{\{2,-2\},\{3,-3\},\{5,-5\}\ldots\}$, nel primo caso abbiamo fissato la funzione φ che a $\{2,-2\}$ associa 2 , a $\{3,-3\}$ associa 3 , a $\{5,-5\}$ associa 5 e cosi di seguito , nel secondo caso abbiamo fissato la funzione φ che a $\{2,-2\}$ associa -2 , a $\{3,-3\}$ associa -3 e cosi' via . Per tanto, detti gli elementi di $\varphi(P/_{\mathscr{R}})$ *gli irriducibili fissati da* φ, si ha che nel primo caso gli irriducibili fissati dalla funzione di scelta sono 2,3.5,7...,nel secondo sono -2,-3,-5,-7,...cioe' gli irriducibili che volta per volta avevamo "deciso di usare"!

Formalizzando , possiamo dire :

(i) Per ogni $a\in\mathbb{Z}$ risulta che se $a\neq0$ e $a\notin \bigsqcup_{\mathbb{Z}}$ allora esistono

$p_1,p_2,\ldots,p_t \in \mathbb{Z}$ irriducibili tali che $a=p_1\cdot p_2\cdot\ldots\cdot p_t$.

(ii) Se $p_1\cdot p_2\cdot\ldots\cdot p_t=p_1\cdot p_2\cdot\ldots\cdot p_s$ con $p_1,..,p_t,q_1,..,q_s$ elementi irriducibili di $\mathbb{Z}$, allora t=s ed esiste una permutazione $\{i_1,\ldots,i_t\}$ dell'insieme $\{1,2,\ldots,t\}$ tale che $p_1 \mathscr{R} q_{i_1},..,p_t \mathscr{R} q_{i_t}$.

Inoltre , se fissiamo una funzione di scelta $\varphi: P/_{\mathscr{R}} \longrightarrow P$, dato $a\in\mathbb{Z}$, $a\neq 0$, $a\notin \sqcup_{\mathbb{Z}}$ esistono e sono unici $u\in\sqcup_{\mathbb{Z}}$ e $p_1,p_2,\ldots,p_t$ <u>irriducibili</u> <u>fissati</u> <u>da</u> φ <u>tali</u> <u>che</u> $a=u\cdot p_1\cdot p_2\cdot..\cdot p_t$.

Punto 6. GLI IDEALI DI $\mathbb{Z}$.

Tutti e soli i sottoinsiemi non vuoti H di $\mathbb{Z}$ tali che
i) $a,b\in H \Rightarrow a\text{-}b\in H$; ii) $a\in\mathbb{Z}$,$b\in H \Rightarrow a\cdot b\in H$
sono quelli costituiti da tutti i multipli di un fissato elemento.

Per esprimere cio' in modo sintetico conveniamo, dato un dominio unitario $(A,+,\cdot)$ di chiamare *ideale* ogni parte H non vuota di A soddisfacente i) e ii), e di definire *principale* ogni ideale H per il quale esiste $a\in H$ tale che $H=\{h\in A \mid \exists x\in A\ h=x\cdot a\}$. Con tale nomenclatura possiamo dire che per il dominio $(\mathbb{Z},+,\cdot)$ si ha che <u>ogni</u> <u>ideale</u> <u>e'</u> <u>principale</u>.

Punto 7. MASSIMO COMUN DIVISORE.

Dati a, $b\in\mathbb{Z}$ parliamo di massimo comune divisore fra a e b. E qui le domande sono tante: cos'e'? esiste? e' unico? abbiamo qualche regola per calcolarlo? gode di qualche proprieta'? in caso affermativo, da quali proprieta' di $(\mathbb{Z},+,\cdot)$ esse dipendono?

2.ESAME DELLE SINGOLE PROPRIETA' DI $(\mathbb{Z},+,\cdot)$.

A questo punto volendo esaminare eventuali correlazioni fra le proprieta' di $\mathbb{Z}$ precedentemente elencate e' opportuno fissare la nostra attenzione su di una proprieta' per volta. Quindi conviene svincolarci dagli interi e pensare ad un generico dominio unitario per il quale di volta in volta valga una delle proprieta'

considerate ai punti 4, 5, 6 del paragrafo1. Diamo pertanto le definizioni alle quali faremo riferimento.

Sia $(A,+,\cdot)$ un dominio unitario.

Definizione2.1 Posto $\sqcup_A := \{a \in A \mid \exists b \in A\ ab=1\}$, ogni elemento di $\sqcup_A$ e' detto *elemento invertibile* di A.

Definizione2.2. Dati $a,b \in A$ diremo che a e' *associato* di b (in simboli $a\mathscr{R}b$) se a e' il prodotto di b per un elemento di $\sqcup_A$ cioe': $"a\mathscr{R}b: \Leftrightarrow \exists u \in \sqcup_A\ a=ub"$.

Si verifica facilmente che la relazione $"\mathscr{R}"$ fra gli elementi di A e' una relazione di equivalenza.

Definizione2.3. Dati $a,b \in A$ diremo che a *divide* b (in simboli $a \mid b$) se esiste un elemento c di A tale che $b=ca$, cioe':
$a \mid b$ sta per $"\exists c \in A\ b=ca"$.

Definizione2.4. Con $a \in A$ diremo che a e' *irriducibile* se $a \neq 0, a \notin \sqcup_A$ e inoltre vale

(P_1) $\forall x,y \in A:\ a=xy \Rightarrow x \in \sqcup_A$ oppure $y \in \sqcup_A$.

Definizione2.5. Sia $a \in A$. Diremo che a e' *primo* se $a \neq 0$, $a \notin \sqcup_A$ e inoltre vale

(P_2) $\forall x,y \in A:\ a \mid xy \Rightarrow a \mid x$ oppure $a \mid y$.

Di dimostrazione immediata e' la seguente

Proposizione2.6. *Sia* $(A,+,\cdot)$ *un* D.U..*Si dimostra che:*

$\forall a \in A:$ *a primo* $\Rightarrow$ *a irriducibile.*

Osserviamo che la proposizione2.6. mette in evidenza la non eccezionalita' del fatto che nel dominio unitario $(\mathbb{Z},+,\cdot)$ ogni elemento primo sia irriducibile, cosa questa che accade in ogni dominio unitario e che dipende essenzialmente da alcune proprieta'

della moltiplicazione.

Ben diverso, come vedremo, sara' il discorso per quanto riguarda il sussistere o meno dell'implicazione "*a* irriducibile $\Rightarrow$ *a* primo".

Definizione2.7. Dato un dominio unitario $(A,+,\cdot)$ diremo che esso e' un *dominio a fattorizzazione unica* (D.F.U.) se valgono

(i) Per ogni $a\in A$ risulta che se $a\neq 0$ e $a\notin \sqcup_A$ allora esistono $p_1,p_2,\ldots,p_t\in A$ irriducibili tali che $a=p_1\cdot p_2\cdot\ldots\cdot p_t$.

(ii) Se $p_1\cdot p_2\cdot\ldots\cdot p_t=q_1\cdot q_2\cdot\ldots\cdot q_s$ con $p_1,p_2,\ldots,p_t,q_1,q_2,\ldots,q_s$ elementi irriducibili di A allora t=s ed esiste una permutazione $\{i_1,i_2,\ldots,i_t\}$ dell'insieme $\{1,2,..,t\}$ tale che $p_1\mathcal{R}q_{i_1},\ldots,p_t\mathcal{R}q_{i_t}$.

Si puo' dimostrare che, se esiste una funzione di scelta $\varphi: P/_{\mathcal{R}}\longrightarrow P$ dove $P=\{a\in A \mid a \text{ irriducibile}\}$, dato $a\in A$, $a\neq 0$, $a\notin \sqcup_A$ esistono e sono unici $u\in \sqcup_A$, $p_1,p_2,\ldots,p_t\in\varphi(P/_{\mathcal{R}})$ tali che $a=u\cdot p_1\cdot p_2\cdot\ldots\cdot p_t$.

Notiamo ora eplicitamente, perche' ci sara' utile in seguito, che:

Osservazione2.8. Dato un D.F.U. $(A,+,\cdot)$ con una assegnata funzione di scelta φ sugli irriducibili, per ogni $a\in A$, $a\neq 0$, $a\notin \sqcup_A$ si ha che esistono e sono unici $u\in \sqcup_A$ e $p_1,p_2,\ldots,p_n$ *irriducibili fissati da* φ e a due a due distinti, tali che $a=up_1^{h_1}p_2^{h_2}\cdot\ldots\cdot p_n^{h_n}$ dove h_i indica il numero di volte che p_i compare nella decomposizione di *a*.

Pertanto se *a* e *b* sono elementi di A non nulli e non invertibili allora, inserendo opportunamente nelle decomposizioni di *a* e di *b* eventuali elementi irriducibili con esponente 0, si avra':

$$a=up_1^{r_1}\cdot p_2^{r_2}\cdot\ldots\cdot p_n^{r_n}\qquad b=vp_1^{s_1}\cdot p_2^{s_2}\cdot\ldots\cdot p_n^{s_n}$$

con $r_i\geq 0$ e $s_i\geq 0$ per ogni $i\in\{1,\ldots,n\}$ e $p_1,p_2,\ldots,p_n$ irriducibili

fissati da φ.

Per esempio se a=-500, b=525 e φ e' la funzione di scelta che fissa gli irriducibili positivi si ha:
$a=(-1)\cdot 2^2\cdot 5^3=(-1)\cdot 2^2\cdot 3^0\cdot 5^3\cdot 7^0$
$b=1\cdot 3\cdot 5^2\cdot 7=\quad 1\cdot 2^0\cdot 3^1\cdot 5^2\cdot 7^1$.

Come e' usuale, data la definizione2.7, e' d'obbligo chiedersi se esistano domini a fattorizzazione unica . Sappiamo che almeno $(\mathbb{Z},+,\cdot)$ e' un tale dominio. Ne esistono altri? La nostra esperienza con i polinomi e con le loro "decomposizioni in fattori" ci induce a pensare che oltre a $(\mathbb{Z},+,\cdot)$ debba esserci qualche altro D.F.U., cosa che dara' ulteriore valore allo studio di queste strutture algebriche.

Definizione2.9. Dato un dominio unitario $(A,+,\cdot)$, diremo che esso e' un *dominio principale* (D.P.) se ogni ideale di $(A,+,\cdot)$ e' principale.

Anche a proposito dei domini principali ci chiediamo: esistono domini principali oltre a $(\mathbb{Z},+,\cdot)$?

Definizione2.10. Dato un anello commutativo unitario $(A,+,\cdot)$, chiameremo *funzione euclidea* su A una applicazione
φ:A-$\{0\}\longrightarrow\mathbb{N}_0$ tale che
(i) Per ogni $a,b\in A$ si ha che se $a \mid b$ allora $\varphi(a)\leq\varphi(b)$.
(ii) Per ogni $a,b\in A$, $b\neq 0$ esistono $q,r\in A$ tali che $a=qb+r$ con $r=0$ oppure $\varphi(r)<\varphi(b)$.

Definizione2.11. Dato un dominio unitario $(A,+,\cdot)$ diremo che esso e' un *dominio euclideo* (D.E.) se esiste una funzione euclidea su A.

Risponderemo anche per domini euclidei a domande analoghe a quelle poste per D.F.U. e per D.P.; per il momento enunciamo un

teorema dalla dimostrazione non immediata, per la quale rinviamo ad un qualunque testo di algebra per studenti di matematica (per esempio a quelli citati in bibliografia), teorema che chiarira' il legame esistente fra le proprieta' di $(\mathbb{Z},+,\cdot)$ elencate ai punti 4, 5, 6 del paragrafo1.

Teorema2.12. *Sia* $(A,+,\cdot)$ *un dominio unitario. Si dimostra che se* $(A,+,\cdot)$ *e' un* D.E. *allora* $(A,+,\cdot)$ *e' un* D.P. *e se* $(A,+,\cdot)$ *e' un* D.P. *allora* $(A,+,\cdot)$ *e' un* D.F.U.

E' chiaro a questo punto come la possibilita' di "fare la divisione col resto" sia la proprieta' di $(\mathbb{Z},+,\cdot)$ che garantisce la principalita' degli ideali di tale dominio e di conseguenza garantisce l'esistenza, per ogni elemento non nullo e non invertibile di $\mathbb{Z}$, di una decomposizione in fattori irriducibili "unica" nel senso espresso in (ii) della definizione2.7.

Torniamo ora al teorema2.12 ed osserviamo che, se indichiamo con E la classe dei domini euclidei, con P quella dei domini principali, con F quella dei domini a fattorizzazione unica, possiamo esprimere il risultato in esso contenuto dicendo che $E \subseteq P \subseteq F$ e possiamo visualizzarlo con la seguente figura1 che, come si vede, e', a questo punto, estremamente "vuota".

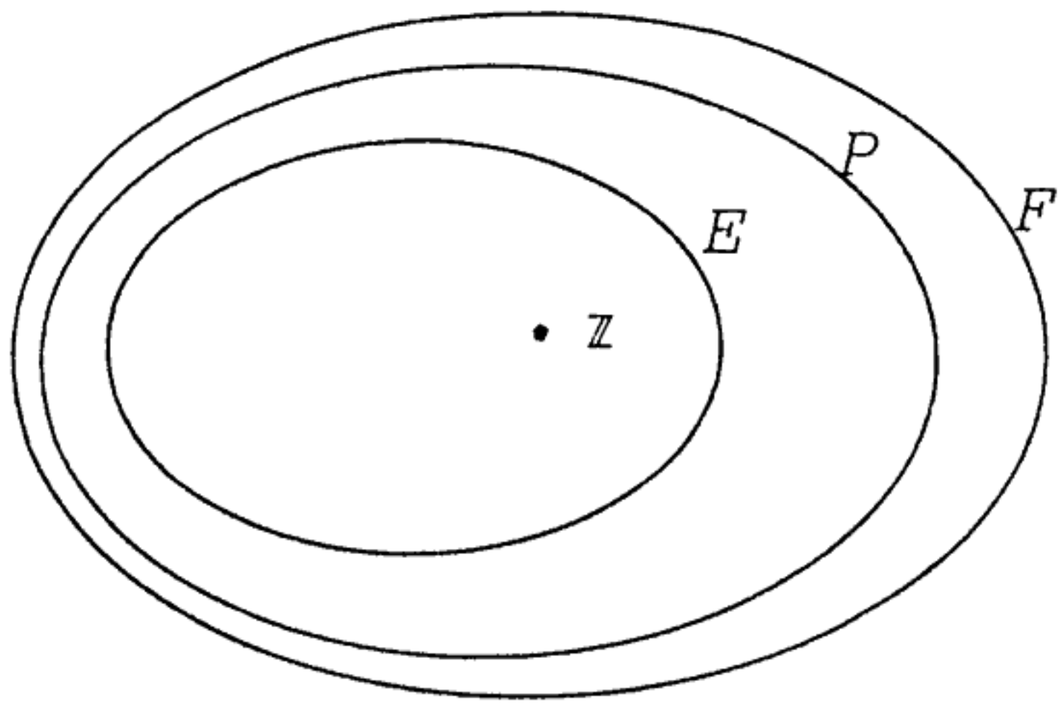

fig. 1

Formulato cosi', si evidenzia come tale teorema, da una parte appaga la curiosita' di conoscere l'eventuale "gerarchia" esistente fra le proprieta' di $(\mathbb{Z},+,\cdot)$ elencate ai punti 4, 5, 6 del paragrafo1, dall'altra fa sorgere nuovi problemi in quanto ci induce a chiederci (oltre a se e' possibile "riempire" alquanto la figura) se la classe e' contenuta propriamente nella classe e se la classe e' contenuta propriamente nella classe , cioe' ci impone le domande:

(1) Esiste un dominio unitario che sia D.F.U. e non sia D.P.?
(2) Esiste un dominio unitario che sia D.P. e non D.E.?

Non viene in mente una risposta immediata; pertanto, ripromettendoci di tornare in seguito sull'argomento, prendiamo nota anche di questi problemi e passiamo ad enunciare un teorema che ci chiarira' perche' in $(\mathbb{Z},+,\cdot)$ essere irriducibile equivale ad essere primo. Daremo in tal modo risposta ad un'altra delle domande dalle quali aveva preso le mosse la nostra indagine.

Teorema2.13. *Sia* $(A,+,\cdot)$ *un* D.F.U..*Si dimostra che*:
$\forall a \in A$: *a irriducibile* $\Rightarrow$ *a primo.*

Si vede cosi', data anche la proposizione2.6, come sia la proprieta' di essere D.F.U. la "responsabile" del fatto che ogni numero intero e' irriducibile se e solo se e' primo.

Ora e' pero' spontaneo domandarci: esistono domini unitari nei quali non e' vero che ogni elemento irriducibile sia primo?

A questa domanda diamo subito risposta mostrando un esempio di dominio unitario nel quale esiste almeno un elemento irriducibile e non primo.

EsempioE_1 Consideriamo il campo $(\mathbb{R},+,\cdot)$ dei numeri reali e il sottoinsieme di $\mathbb{R}$ dato da $A:=\{\alpha \in R \mid \exists a,b \in \mathbb{Z}\ \alpha=a+b\sqrt{10}\}$. Poiche' per ogni a,b,c,d elementi di $\mathbb{Z}$ risulta:

$$(a+b\sqrt{10})+(c+d\sqrt{10})=(a+c)+(b+d)\sqrt{10}$$

e

$$(a+b\sqrt{10})\cdot(c+d\sqrt{10})=(ac+10bd)+(ad+bc)\sqrt{10},$$

si ha che la somma e il prodotto, rispettivamente secondo l'addizione e la moltiplicazione in $\mathbb{R}$, di elementi di A sono elementi di A. Quindi l'addizione la moltiplicazione in $\mathbb{R}$, ristrette ad A, sono operazioni in A che continueremo ad indicare con $+$ e $\cdot$.

E' opportuno notare a questo punto che non tutti i sottinsiemi di $\mathbb{R}$ si comportano come il sottinsieme A che abbiamo definito: se, per esempio, consideriamo $B=\{0,1,2,3\}\subseteq\mathbb{R}$ si vede che $2+3\notin B$ e $2\cdot 3\notin B$, pertanto l'addizione e la moltiplicazione in $\mathbb{R}$ non inducono operazioni in B.

Ritornando ora alla struttura $(A,+,\cdot)$ e' facile verificare:

(I) $(A,+,\cdot)$ e' D.U. avente $0+0\sqrt{10}$ come elemento neutro rispetto all'addizione e $1+0\sqrt{10}$ come elemento neutro rispetto alla moltiplicazione.

(II) Ogni $a\in\mathbb{Z}$ e' elemento di A avendosi $a=a+0\sqrt{10}$.

(III) $\forall a,b\in\mathbb{Z}$: $\quad a+b\sqrt{10}=0 \Leftrightarrow a=0$ e $b=0$.

Infatti se $a+b\sqrt{10}=0$ e $b=0$ allora anche $a=0$ e quindi la tesi. Dimostriamo percio' che se $a+b\sqrt{10}=0$ allora $b=0$. Infatti se $b\neq 0$ si ha anche $a\neq 0$ (altrimenti b sarebbe 0), inoltre e' chiaro che $a\neq\pm 1$ e $b\neq\pm 1$; pertanto essendo $(\mathbb{Z},+,\cdot)$ un D.F.U., a e b sono decomponibili in fattori irriducibili. Cio' conduce ad un assurdo poiche', essendo $a^2=b^2 10=2\cdot 5\cdot b^2$, si avrebbe che l'irriducibile 2 comparirebbe in due decomposizioni del numero $c=a^2=2\cdot 5\cdot b^2$ a sinistra un numero pari di volte e a destra un numero dispari di volte.

Da (III) segue:

(IV) $\forall a,b,c,d\in\mathbb{Z}$: $\quad a+b\sqrt{10}=c+d\sqrt{10} \Leftrightarrow a=b$ e $c=d$.

(V) Con $\alpha=a+b\sqrt{10}\in A$, posto $\bar{\alpha}=(a-b\sqrt{10})$ e $\|\alpha\|=\alpha\bar{\alpha}=a^2-10b^2$,ed osservato che $\|\alpha\|\in\mathbb{Z}$, si ha che: $\alpha\in\sqcup_A \Leftrightarrow \|\alpha\|=\pm 1$.

Infatti se $\alpha\in\sqcup_A$ esiste $\beta\in A$ tale che $\alpha\beta=1+0\sqrt{10}$ e pertanto $\|\alpha\beta\|=\|\alpha\|\cdot\|\beta\|=1$ e quindi $\|\alpha\|=\pm 1$. Viceversa, se $\|\alpha\|=\pm 1$, si ha $\alpha\bar{\alpha}=1$ oppure $\alpha\bar{\alpha}=-1$. Quindi $\alpha\bar{\alpha}=1$ oppure $\alpha(-\bar{\alpha})=1$ e pertanto $\alpha\in\sqcup_A$.

Dimostriamo ora che:

(VI) $2\in A$ e' un elemento irriducibile e non primo in A.

Essendo $2\neq 0$ e, grazie a (V), $\|2\|=4\neq 1$, abbiamo che 2 e' un elemento di A non nullo e non invertibile; resta da provare:

(i) 2 non soddisfa la proprieta' (P_2) della definizione2.5

(ii) 2 soddisfa la proprieta' (P_1) della definizione2.4

Per verificare (i) dobbiamo dimostrare quanto segue:

non e' vero che $(\forall\alpha,\beta\in A: 2\mid\alpha\beta\Rightarrow 2\mid\alpha$ oppure $2\mid\beta)$. Cio' e' garantito dall'esistenza di $\alpha=4+\sqrt{10}$ e di $\beta=4-\sqrt{10}$ elementi di A tali che $2\mid\alpha\beta$ ed inoltre $2\nmid\alpha$ e $2\nmid\beta$. Infatti esiste $3\in A$ tale che $\alpha\beta=16-10=6=3\cdot 2$ e pertanto $2\mid\alpha\beta$; se poi per assurdo supponiamo che $2\mid\alpha$ deve esistere un elemento $a+b\sqrt{10}\in A$ tale che $\alpha=4+\sqrt{10}=2\cdot(a+b\sqrt{10})$; da cio' seguirebbe, dato (III), che $2b=1$ e tale risultato e' assurdo poiche' in $\mathbb{Z}$ non esistono elementi b che moltiplicati per 2 diano per risultato 1. Analogamente si prova che $2\nmid\beta$.

Notiamo come il numero 2, che e' *primo* se considerato come elemento di $\mathbb{Z}$, perda tale proprieta' quando viene considerato come elemento di A; cio' ci induce a riflettere, ancora una volta, sull'importanza di tenere sempre presente l'ambiente al quale vogliamo riferirci.

Meno immediata e' la dimostrazione di (ii) per la quale procediamo nel modo seguente.

Dovendo dimostrare che

$$\forall\alpha,\beta\in A:\ 2=\alpha\beta \Rightarrow \alpha\in\sqcup_A \text{ oppure } \beta\in\sqcup_A$$

bastera' dimostrare, grazie alla caratterizzazione degli elementi di $\sqcup_A$ espressa al punto (IV), che

$$\forall\alpha,\beta\in A:\ 2=\alpha\beta \Rightarrow \|\alpha\|=\pm 1 \text{ oppure } \|\beta\|=\pm 1.$$

Siano pertanto $\alpha,\beta\in A$ con $\alpha\beta=2$; verifichiamo che $\|\alpha\|=\pm 1$ oppure che

$\|\beta\| = \pm 1$. Da $2 = \alpha\beta$ segue $\|2\| = 4 = \|\alpha\beta\| = \|\alpha\| \cdot \|\beta\|$ quindi, poiche' $\|\alpha\|$ e $\|\beta\|$ sono interi relativi, si ha che $\|\alpha\|$ e' un divisore di 4 in $\mathbb{Z}$. Allora i casi possibili sono

(a) $\|\alpha\| = \pm 1$; (b) $\|\alpha\| = \pm 2$; (c) $\|\alpha\| = \pm 4$.

Poiche' l'eventualita' (c) comporta $\|\beta\| = \pm 1$, resta da dimostrare che $\|\alpha\| \neq \pm 2$ per ogni $\alpha \in A$, risultato che si consegue provando che:

(*) non esistono $a,b \in \mathbb{Z}$ tali che $a^2\text{-}10b^2 = 2$ e non esistono $a,b \in \mathbb{Z}$ tali che $a^2\text{-}10b^2 = -2$.

A tal fine bastera' verificare che:

(**) non esistono $x,y \in \mathbb{Z}$ tali che $x^2\text{-}10y = 2$ e che non esistono $x,y \in \mathbb{Z}$ tali che $x^2\text{-}10y = -2$. [1]

Supponiamo che esistano $x,y \in \mathbb{Z}$ tali che $x^2\text{-}10y = 2$. Dividiamo x per 10, cosi' $x = 10q + r$ con $0 \leq r \leq 9$. Allora $x^2 = 100q^2 + 20qr + r^2$. Sostituendo questa espressione nella prima uguaglianza di (**), si ottiene che $r^2\text{-}2 = 10(y\text{-}10q^2\text{-}2qr)$ cioe' si ottiene che $r^2\text{-}2$ e' un multiplo di 10 il che e' assurdo come puo' dedursi calcolando $r^2\text{-}2$ al variare di r tra 0 e 9. [2]

In modo analogo si prova che non esistono $x,y \in \mathbb{Z}$ tali che $x^2\text{-}10y = -2$.

E' chiaro che il dominio $(A, +, \cdot)$ dell'esempio precedente non e' un dominio a fattorizzazione unica in quanto, se lo fosse, ogni suo elemento irriducibile dovrebbe essere primo (cfr.teorema2.12) mentre abbiamo appena visto che cio' non e' vero. Alla luce di cio' la figura1 diventa la seguente figura2.

---

[1] Si dimostra infatti che (**) implica (*) e questo si prova verificando che la negazione di (*) implica la negazione di (**). Cio' e' vero in quanto, se esistessero $a,b \in \mathbb{Z}$ tali che $a^2\text{-}10b^2 = \pm 2$, allora $x = a$ e $y = b^2$ sarebbero elementi di $\mathbb{Z}$ tali che $x^2\text{-}10y = \pm 2$.

[2] Dimostrazione immediata di cio' puo' aversi con il passaggio alle classi dei resti modulo 10.

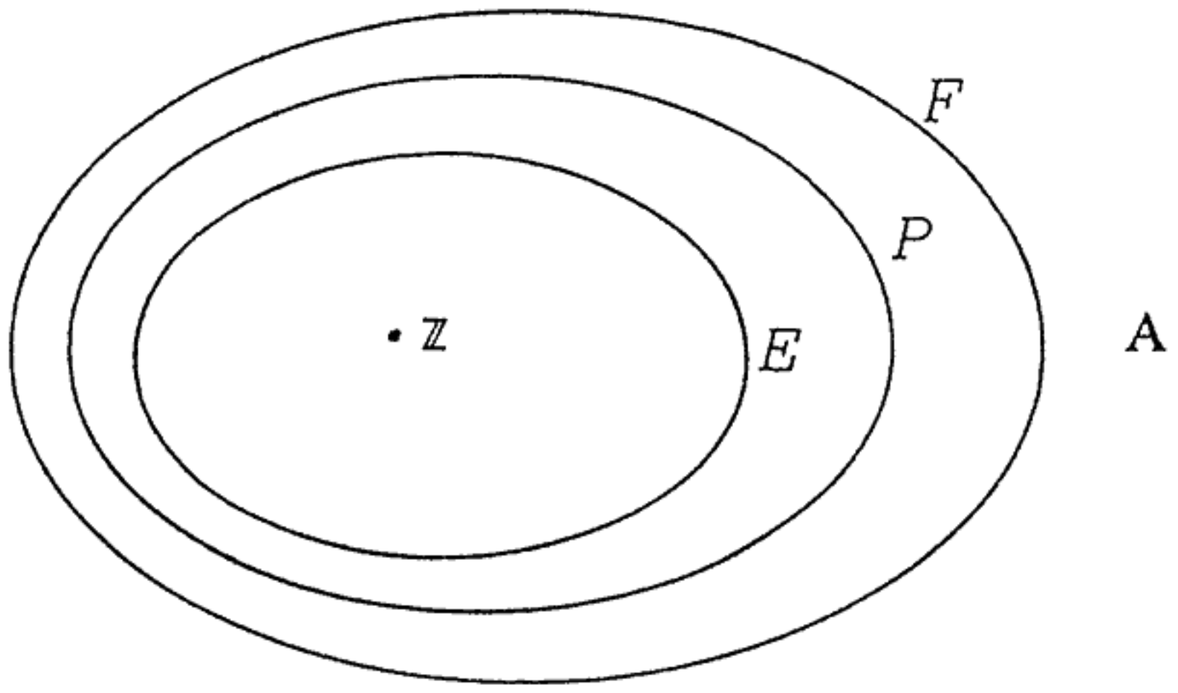

fig.2

Comunque, a proposito dell'esempio E_1, puo' essere interessante parlare di un memorabile errore commesso da un grande matematico (nessuno e' infallibile!..). Facciamo questo perche', da una parte, vogliamo evidenziare come anche gli errori possano essere "fruttuosi" e dall'altra, perche' vogliamo mettere in guardia dal ritenere veri risultati che, per analogia con casi familiari, ci "sembrano" veri. L'errore del quale parliamo e' quello in cui incorse E.E.Kummer (1810-1893) tentando di risolvere un famoso problema di teoria dei numeri. Egli era convinto che, per analogia con $\mathbb{Z}$, domini come il dominio $(A,+,\cdot)$, prima considerato, dovessero essere a fattorizzazione unica. Comunque nel momento in cui l'errore fu manifesto, lo stesso Kummer e soprattutto R.Dedekind (1831-1916) furono spinti ad indagare sulla questione; si scopri' che esistono domini unitari (noti oggi come domini di Dedekind) nei quali, pur non potendosi parlare di "fattorizzazione unica" per gli elementi, si puo', in modo opportuno, parlare di fattorizzazione unica per gli *ideali*, concetto questo introdotto dallo stesso Dedekind allo scopo di chiarire le questioni di cui abbiamo parlato e diventato poi, come sappiamo, strumento non solo per la teoria dei numeri ma anche per tanti altri settori della matematica.

3. MASSIMI COMUN DIVISORI.

Ora , cosi' come ci eravamo ripromessi di fare, passiamo a questioni riguadanti massimo comun divisore e cio' allo scopo di dare risposta alle domande annotate a tale proposito al punto7 del paragrafo1.

Il primo problema che si presenta e' quello di dare una definizione nella quale riconoscere l'idea che abbiamo a proposito di massimo comun divisore tra numeri naturali. Abbiamo gia' visto che in un generico dominio unitario possiamo tranquillamente parlare di divisori e quindi di divisori comuni, non ci sembra pero' altrettanto immediato estendere il concetto di "massimo" divisore comune; infatti per far questo sembrerebbe essere necessaria una relazione d'ordine che, in un generico dominio unitario, non sempre abbiamo a disposizione. Per cercare di superare questa difficolta' e' quindi opportuno penetrare meglio nelle proprieta' che caratterizzano il massimo comun divisore fra due numeri naturali. Consideriamo pertanto, per esempio, 12, 18 e il loro massimo comun divisore 6; vediamo che 6 non e' solo "il piu' grande", nel senso usuale della parola, tra i numeri 1,2,3,6, che sono in $\mathbb{N}$ i divisori comuni a 12 e 18, ma gode della proprieta'che ogni divisore comune a 12 e 18 e' anche un divisore di 6, cosa che puo' essere espressa dicendo che, per ogni $c \in \mathbb{N}$, risulta:

(*) se $c \mid 12$ e $c \mid 18$ allora $c \mid 6$.

Alla luce di questo esempio si intuisce come possa essere trasferita in un generico dominio unitario la nozione di massimo comune divisore; inoltre, tenendo presente il punto2 del paragrafo1, l'affermazione (*) ci dice che se in $\mathbb{N}$ c e' un divisore comune a 12 e 18, allora $c \leq 6(\Delta)$; cioe' 6 e' effettivamente, fra i divisori comuni a 12 e 18, "il piu' grande" ma lo e' rispetto alla relazione d'ordine Δ in $\mathbb{N}$, della quale abbiamo parlato al punto2 del paragrafo1.

Premesso cio', con $(A,+,\cdot)$ un dominio unitario, possiamo dare la seguente

Definizione3.1 Dati $a,b\in A$ chiamiamo *massimo comun divisore* di a e b **un** elemento $d\in A$ che goda delle seguenti proprieta':

i)$d \mid a$ e $d \mid b$; ii)$\forall c\in A$: $(c \mid a,\ c \mid b \Rightarrow c \mid d)$.

Posto m.c.d.$(a,b):=\{d\in A \mid d$ verifica i) e ii)$\}$ si vede, qualunque sia $b\in A$, che:

se $a=0$ allora $b\in$ m.c.d.(a,b)

se $a\in \sqcup_A$ allora $a\in$ m.c.d.(a,b)

se $a=b$ allora $a\in$ m.c.d.(a,b);

quindi in ogni dominio unitario $(A,+,\cdot)$, per particolari elementi a,b, si ha che m.c.d.$(a,b)\neq\phi$, inoltre si puo' verificare facilmente che se $d\in$m.c.d.(a,b) allora $[d]_{\mathscr{R}}=$m.c.d.(a,b). Ricordando che con $[d]_{\mathscr{R}}$ si e' indicato l'insieme degli elementi di A equivalenti a d rispetto alla relazione *"..e' associato di.."*, si vede che se a e b sono elementi di A possedenti un massimo comun divisore allora, in generale, essi ne posseggono piu' di uno e questi sono fra loro associati, cioe' differiscono per un elemento invertibile.

Questo e' quanto possiamo dire in generale senza ulteriori ipotesi sul dominio $(A,+,\cdot)$; cominciamo quindi con l'aggiungere la proprieta' di fattorizzazione unica. In tale caso si ha il seguente

Teorema3.2 *Sia* $(A,+,\cdot)$ D.F.U. *con una fissata una funzione di scelta sugli irriducibili; allora per ogni* $a,b\in A$ *risulta* m.c.d.$(a,b)\neq\phi$.

Dim. Esclusi i casi banali, siano (vedi osservazione2.8)

$$a=up_1^{r_1}\cdot p_2^{r_2}\cdot\ldots\cdot p_n^{r_n} \qquad b=vp_1^{s_1}\cdot p_2^{s_2}\cdot\ldots\cdot p_n^{s_n}$$

con $r_i\geq 0$ e $s_i\geq 0$ per ogni $i\in\{1,\ldots,n\}$ e $p_1,p_2,\ldots p_n$ irriducibili fissati dalla funzione di scelta.

Posto per ogni $i\in\{1,\ldots n\}$ $w_i=\min\{r_i,s_i\}$ si verifica che

$d=p_1^{w_1}\cdot\ldots\cdot p_n^{w_n}\in$m.c.d.$(a,b)$.

Notiamo che l'elemento d, di cui alla dimostrazione del teorema3.2, e', nel caso di $(\mathbb{Z},+,\cdot)$, esattamente quello che siamo abituati a trovare "considerando i fattori irriducibili comuni una sola volta col piu' piccolo esponente". Illustriamo cio' con un esempio e siano pertanto

$a=2200=1\cdot 2^3\cdot 5^2\cdot 11=1\cdot 2^3\cdot 3^0\cdot 5^2\cdot 7^0\cdot 11^1$

$b=-315=(-1)\cdot 3^2\cdot 5\cdot 7=(-1)\cdot 2^0\cdot 3^2\cdot 5^1\cdot 7^1\cdot 11^0$

Si ha cosi', dato il teorema3.2, che un massimo comun divisore di a e b risulta essere $d=2^0\cdot 3^0\cdot 5^1\cdot 7^0\cdot 11^0=5$, cioe' esattamente l'elemento che avremmo trovato applicando la ben nota regola che prevede la decomposizione in fattori irriducibili.

Va qui notato che di solito, nella applicazione meccanica della regola per il calcolo di m.c.d., manca la consapevolezza di "aver deciso di usare gli irriducibili positivi", cioe' la consapevolezza di aver tacitamente fissato una funzione di scelta. Inoltre, in genere, non si considera con la dovuta attenzione il fatto che se 5 e' un massimo comun divisore lo e' anche -5.

A questo punto osserviamo che il teorema3.2 fornisce per un D.F.U. $(A,+,\cdot)$ la garanzia dell'esistenza di un massimo comun divisore per ogni $a,b\in A$ dandoci una regola per calcolarlo basata sulla decomposizione di a e b in fattori irriducibili. Tale regola e' pero' estremamente "scomoda" in quanto nella maggior parte dei casi, pur sapendo che una decomposizione esiste, o non siamo in grado di esibirla (riusciamo sempre a decomporre un polinomio?..) o lo facciamo con molta fatica. Viene cosi' spontaneo chiederci se in un dominio principale, che e' un dominio a fattorizzazione unica (cfr.teorema2.11) "un poco piu' ricco" di proprieta', si possa avere qualche altra informazione riguardo al massimo comun divisore di due elementi oltre al fatto che esiste.

Il teorema che segue, del quale per brevita' omettiamo la

dimostrazione, per altro molto semplice, appaga la nostra curiosita'.

Teorema3.3 *Siano* $(A,+,\cdot)$ *un* D.P., $a,b\in A$, $d\in$m.c.d.(a,b). *Si dimostra che esistono* $x,y\in A$ *tali che* $d=xa+yb$.

Come si vede, anche il teorema3.3 fornisce informazioni sulla esistenza di certi elementi (in genere non unici), senza peraltro che dalla dimostrazione possa dedursi qualche informazione sulla loro determinazione.

Se pero' $(A,+,\cdot)$ e' un dominio euclideo (pertanto D.P. e quindi D.F.U.), dati $a,b\in A$, possiamo non solo asserire che esiste $d\in$m.c.d.(a,b) e che esistono almeno un x e un y elementi di A tali che $d=xa+yb$, ma anche dare un algoritmo per determinarli. Illustriamo cio'.

Siano $(A,+,\cdot)$ un dominio euclideo, $\varphi:A\longrightarrow\mathbb{N}_0$ come nella definizione2.10, $a,b\in A$.

Se $b\neq 0$, esistono $q_0,r_0\in A$ tali che $a=q_0b+r_0$ ed $r_0=0$ oppure $\varphi(r_0)<\varphi(b)$.

Se $r_0\neq 0$, esistono $q_1,r_1\in A$ tali che $b=q_1r_0+r_1$ ed $r_1=0$ oppure $\varphi(r_1)<\varphi(r_0)$.

Se $r_1\neq 0$, esistono $q_2,r_2\in A$ tali che $r_0=q_2r_1+r_2$ ed $r_2=0$ oppure $\varphi(r_2)<\varphi(r_1)$.

Pertanto, osservato che ad un certo punto dovremo trovare un resto uguale a 0 (altrimenti avremmo infiniti numeri naturali $\varphi(r_0),\varphi(r_1),\varphi(r_2),.,$compresi tra 0 e $\varphi(b)$), indichiamo con r_{n+1} il primo resto uguale a 0. Si ha cosi' la seguente tabella:

$$a=q_0b+r_0$$
$$b=q_1r_0+r_1$$
$$r_0=q_2r_1+r_2$$
$$r_1=q_3r_2+r_3$$
$$\cdots\cdots\cdots$$
$$r_{n-2}=q_nr_{n-1}+r_n$$
$$r_{n-1}=q_{n+1}r_n.$$

Si dimostra, usando la definizione, che $r_n \in$ m.c.d.(a,b).
Per determinare un x e un y tali che $r_n = xa+yb$, si procede, tenendo presente la tabella precedente, come segue:

$r_0 = a+(-q_0)b,$
$r_1 = b+(-q_1)r_0 = b+(-q_1)[a+(-q_0)b] = (-q_1)a+(1+q_1q_0)b,$
$r_2 = r_0+(-q_2)r_1 = [a+(-q_0)b]+(-q_2)[(-q_1)a+(1+q_1q_0)b] =$
$= (1+q_1q_2)a+(-q_0-q_2-q_0q_1q_2)b.$
Cosi' continuando si determina $r_n = xa+yb.$

Facciamo un semplice esempio con a=36 e b=15.
Avendosi $36 = 2\cdot 15+6$, $15 = 2\cdot 6+3$, $6 = 2\cdot 3+0$, risulta che 3, ultimo resto diverso da 0, e' un massimo comun divisore di 36 e 15. Determiniamo x,y tali che $3 = x\cdot 36+y\cdot 15$ procedendo cosi' come abbiamo illustrato; pertanto:
$6 = 1\cdot 36+(-2)\cdot 15;$
$3 = 1\cdot 15+(-2)\cdot 6 = 1\cdot 15+(-2)[1\cdot 36+(-2)\cdot 15] = (-2)\cdot 36+5\cdot 15.$

A questo punto, ripensando a quanto puo' essere lungo e noioso decomporre in fattori irriducibili numeri interi che siano solo "alquanto grandi", risulta chiaro come, in generale, sia il metodo dell'algoritmo euclideo (basato sulla proprieta' euclidea di $(\mathbb{Z},+,\cdot)$), piu' che il metodo dell'algoritmo della decomposizione in fattori irriducibili (basato sulla proprieta' di $(\mathbb{Z},+,\cdot)$ di essere D.F.U.) quello a cui far riferimento per la ricerca di massimi comun divisori, tanto piu' che la conoscenza di questo metodo permette in alcuni casi di individuare a "vista" il massimo comun divisore tra due numeri. Per esempio, solo "guardando" i numeri

$a = 32442131$ e
$b = 64884263$

riconosciamo che $b = 2\cdot a+1$ e questo, alla luce di quanto abbiamo precedentemente esposto, garantisce che:

$1 \in$ m.c.d.$(32442131,64884263)$.

D'altra parte possiamo "misurare" la maggiore efficienza del

metodo euclideo rispetto all'altro usando come misura il "tempo macchina" di un calcolatore al quale sia richiesto di trovare, con l'algoritmo euclideo e con l'algoritmo della decomposizione in fattori irriducibili, un massimo comun divisore tra due numeri assegnati.

Adesso, consapevoli di dover riflettere ancora su domande alle quali non abbiamo dato risposta, terminiamo qui la parte della nostra esposizione dedicata a $\mathbb{Z}$. Nei paragrafi successivi vedremo come i polinomi ci aiuteranno a fornire risposte a domande che ne sono ancora prive mentre, tutto cio' che abbiamo fin qui esposto, ci permettera' di guardare ad essi in modo piu' consapevole di quanto, forse, non abbiamo fatto finora.

4. POLINOMI IN UNA "VARIABILE"

Sin dalla scuola media inferiore acquisiamo il concetto di polinomio in una variabile tanto che in genere, forse non sempre facilmente, riusciamo a riconoscere fra certe scritture, per esempio tra

(1) $3x^2+2x+1$; (2) $\pi x+3$; (3) $f(x)=4x^3-2x+5$;

(4) $2\cos^2 x+3\cos x+4$; (5) $\frac{2}{3}x+5,\overline{2}$ (6) $\cos 30x^4+\log 2x^3+2$;

quelle che rappresentano polinomi in x a coefficienti numerici. Le cose invece si complicano quando ci poniamo il problema di dare la definizione di polinomio in una "variabile" o, come diremo spesso piu' semplicemente, di polinomio.

Alla luce della nozione di operazione su di un insieme, nozione sulla quale abbiamo tanto insistito all'inizio di questa esposizione, e' chiaro che appare per lo meno contraddittorio parlare di polinomio come "somma di monomi, intendendo per monomio un'espressione contenente prodotti di fattori numerici e letterali". Infatti come dare significato all'espressione $2\cdot x+5$? In quale insieme sono definite le operazioni alle quali in questo caso facciamo riferimento? A quale insieme appartiene x? e $2\cdot x$?

Ne' ci appare soddisfacente la linea adottata da coloro che parlano di $2\cdot x+5$ come di una espressione in cui x e' "variabile" in un opportuno insieme numerico; in tal caso perche' dare a dei numeri il nome di polinomio?

Si vede cosi' che non e' piu' rinviabile cercare di dare una definizione soddisfacente di polinomio in una "variabile" e soprattutto cercare di capire da dove trae origine una certa "tradizione". Infatti non possiamo escludere che ci sia un ambito nel quale affermazioni come "somma di monomi" abbiano significato, ne' possiamo escludere che ci sia un'ottica in cui sia chiaro il collegamento tra certi oggetti che sappiamo addizionare, moltiplicare, in alcuni casi scomporre in fattori, ecc. ed altri oggetti, che, pur assomigliando a polinomi, sono

funzioni, tanto che ad un certo punto cominciamo ad interessarci alla loro continuita', alle loro derivate, ai loro massimi e minimi.

Come abbiamo gia' fatto in altre occasioni cominciamo col riflettere su quanto riteniamo acquisito a questo riguardo; ci rendiamo allora conto che, nelle nostre manipolazioni, $x, x^2, x^3, \ldots$ hanno una funzione, per cosi' dire, di servizio. Infatti, quando verifichiamo l'uguaglianza di due polinomi in x, confrontiamo i coefficienti di x, i coefficienti di x^2, i coefficienti di x^3,...e i "termini noti" intesi anche come coefficienti di x^0; quando addizioniamo due polinomi, addizioniamo i cefficienti di x, i coefficienti di x^2, i coefficienti di x^3...e i "termini noti".

Questo ci fa intuire che il ruolo fondamentale in un polinomio e' svolto dai suoi coefficienti tanto che, se decidessimo di usare carta a quadretti e di scrivere i polinomi ordinati secondo le potenze decrescenti di x scrivendo anche i coefficienti che sono 0, potremmo confrontare o addizionare polinomi anche senza l'ausilio di x. Spieghiamoci con un esempio e consideriamo:

$f = -5x^6+2x^3+7x^8-4-x^2 = \quad 7x^8+0x^7-5x^6+0x^5+0x^4+2x^3-1x^2+0x-4$;

$g = x^3+2 = \quad = 1x^3+0x^2+0x+2$;

Procediamo scrivendo i coefficienti di f e di g incolonnando quelli che corrispondono allo stesso esponente di x (e' chiara l'analogia con l'addizione fra numeri naturali per la quale, usando la consueta scrittura posizionale, si incolonnano le unita', si incolonnano le decine, si incolonnano le centinaia, ecc...); sommiamo i coefficienti "in colonna", si ha allora (leggendo "*fis*i" come posizione del coefficiente di x^i) la tabella:

	*fs*10	*fs* 9	*fs* 8	*fs* 7	*fs* 6	*fs* 5	*fs* 4	*fs* 3	*fs* 2	*fs* 1	*fs* 0	
f			+7	0	-5	0	0	+2	-1	0	- 4	+
g								+1	0	0	+2	=
f+g			+7	0	-5	0	0	+3	-1	0	- 2	

Nella tabella precedente "leggiamo" che
$f+g= +7x^8+0x^7-5x^6+0x^5+0x^4+3x^3-1x^2+0x-2= 7x^8-5x^6+3x^3-1x^2-2$, cioe' il polinomio che avremmo ottenuto applicando l'usuale regola di calcolo.

Anche per moltiplicare f e g possiamo procedere con tecnica analoga mutuata dalla regola per moltiplicare due numeri naturali. Infatti proviamo a seguire questa idea per trovare $f \cdot g$. In questo caso avremo la seguente tabella:

	x^{11}	x^{10}	x^9	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0	
f				+7	0	- 5	0	0	+2	-1	0	- 4	
g									+1	0	0	+2	=
				+ 14	0	- 10	0	0	+4	-2	0	- 8	
			0	0	0	0	0	0	0	0	0		
		0	0	0	0	0	0	0	0	0			
	+7	0	-5	0	0	+2	-1	0	- 4				
$f \cdot g$	+7	0	-5	+ 14	0	- 8	-1	0	0	-2	0	- 8	

Anche qui leggiamo che:
$f \cdot g=7x^{11}+0x^{10}-5x^9+14x^8+0x^7-8x^6-1x^5+0x^4+0x^3-2x^2+0x-8=$
$=7x^{11}-5x^9+14x^8-8x^6-1x^5-2x^2-8.$
(controllare moltiplicando nel modo usuale!...).

Viste le considerazioni fatte e' ora spontaneo ipotizzare una definizione di polinomio svincolata da x (cosa che a livello di definizione sembrava darci maggior fastidio) e data in termini di coefficienti "messi in ordine"; cio' non e' difficile in quanto ci aiuta in questo la nozione di successione, o meglio quella di successione definitivamente nulla.

Premesso che, dato un insieme A non vuoto, diciamo *successione definitivamente nulla* di elementi di A ogni applicazione $f:\mathbb{N}_0 \longrightarrow A$ per la quale esista $t \in \mathbb{N}_0$ tale che $f(i)=0$ per ogni $i>t$

(o, equivalentemente, tale che $f(i)\neq 0$ solo per un numero finito di elementi $i\in\mathbb{N}_0$), diamo la seguente

Definizione4.1 *Sia $(A,+,\cdot)$ un anello commutativo unitario. Dicesi polinomio su A una successione di elementi di A definitivamente nulla.*

Come si vede, in questa definizione si fa riferimento a concetti tutti noti a livello di scuola secondaria superiore o comunque facilmente giustificabili.

D'ora in avanti "visualizzeremo" un polinomio su A rappresentandolo con $(a_0,a_1,a_2,\ldots,a_t,0,0,0,\ldots.)$ dove l'indice t e' quello di cui si parla nella definizione di successione definitivamente nulla e parleremo dell'elemento a_i come dell'elemento di posto i; inoltre indicheremo con S_A l'insieme dei polinomi su A.

Osservazione4.2 Data la definizione4.1, due polinomi $f=(a_0,a_1,\ldots,a_n,\ldots)$ e $g=(b_0,b_1,\ldots,b_m\ldots)$ sono uguali se e solo se per ogni $i\in\mathbb{N}_0$ risulta $a_i=b_i$. (Si confronti questa osservazione col **Principio di identita' dei polinomi**, del quale parleremo alla fine del paragrafo5, per cogliere aspetti comuni e differenze profonde).

Introduciamo ora il concetto di grado di un polinomio e quello di coefficiente direttore.

Definizione4.3 Sia $(A,+,\cdot)$ un anello commutativo unitario e $f=(a_0,a_1,\ldots,a_t,0,0,\ldots)\in S_A$.
Chiameremo $a_0,a_1,..,a_t$, *coefficienti di* f e, se $a_t\neq 0$, diremo che a_t e' il *coefficiente direttore* di f e che t e' il *grado di* f (in simboli $t=\delta(f)$).

Alla luce delle definizioni date si ha che:

$(0,0,0,\ldots,0,\ldots)$ non ha grado ne' coefficiente direttore;
$(a_0,0,0,\ldots.)$,con $a_0 \neq 0$, ha grado 0 e coefficiente direttore a_0;
$(a_0,a_1,0,0,..)$, con $a_1 \neq 0$, ha grado 1 e coefficiente direttore a_1;
.....
$(a_0,a_1,..,a_t,0,0,\ldots)$, con $a_t \neq 0$, ha grado t e coefficiente direttore a_t.

Non e' difficile verificare che, dati $f=(a_0,a_1,\ldots,a_r,0,0,\ldots)$ e $g=(b_0,b_1,\ldots,b_s,0,0,\ldots)$ elementi di S_A, le successioni $s=(s_0,s_1,\ldots,s_i,\ldots)$, con $s_i=a_i+b_i$ per ogni $i\in\mathbb{N}_0$, e $p=(p_0,p,\ldots,p_i,\ldots.)$, con $p_i=a_0b_i+a_1b_{i-1}+\ldots.+a_ib_0$ per ogni $i\in\mathbb{N}_0$, sono elementi di S_A (cioe' sono successioni definitivamente nulle). Pertanto sono operazioni in S_A l'applicazione

$+:S_A xS_A \longrightarrow S_A$ che alla coppia (f,g) associa s
e l'applicazione
$\cdot:S_A xS_A \longrightarrow S_A$ che alla coppia (f,g) associa p.

Riguardo alla struttura $(S_A,+,\cdot)$ si dimostra il seguente

Teorema4.4 *Dato un anello commutativo unitario* $(A,+,\cdot)$ *risulta che:*

(i) *la struttura* $(S_A,+,\cdot)$ *e' un anello commutativo unitario con* $(0,0,0,\ldots)$ *elemento neutro rispetto all'addizione e* $(1,0,0,\ldots)$ *elemento neutro rispetto alla moltiplicazione.*

(ii) *l'insieme* $A^*=\{(a,0,0,..)\}_{a\in A}$ *e' un sottoanello di* $(S_A,+,\cdot)$ *isomorfo all'anello* $(A,+,\bullet.)$.

(iii) *Gli elementi invertibili di* $(S_A,+,\cdot)$ *sono tutti e soli gli elementi invertibili di* $(A^*,+,\cdot)$; *cioe'* $\sqcup_{S_A}=\sqcup_{A^*}$.

E' opportuno a questo punto sottolineare come da (iii) discenda immediatamente che polinomi di grado diverso da 0 non potranno mai essere elementi invertibili dell'anello $(S_A,+,\cdot)$; ma attenzione,

con questo non intendiamo dire che ogni polinomio di grado 0 e' invertibile in $(S_A,+,\cdot)$!

Naturalmente, definito $(S_A,+,\cdot)$, si puo' pensare di semplificare la "scrittura" dei suoi elementi facendo, per esempio, le seguenti posizioni:

$\mathbf{a}=(a,0,0,.....)$ per ogni $a\in A$;

$\mathrm{x}=(0,1,0,0,...)$. (Notiamo che x rappresenta la successione i cui elementi sono tutti nulli tranne quello che si trova nel posto 1 e che e' uguale ad 1).

Immediate conseguenze di queste posizioni sono:

I) $\mathbf{0}=(0,0,0,....)$ e $\mathbf{1}=(1,0,0,....)$ sono rispettivamente l'elemento neutro rispetto all'addizione e l'elemento neutro rispetto alla moltiplicazione nell'anello $(S_A,+,\cdot)$.

II) Ricordando come sono definite le potenze di un elemento appartenente al sostegno di un anello, risulta:

$\mathrm{x}^0=\mathbf{1}=(1,0,0,...)$;

$\mathrm{x}^2=\mathrm{x}\cdot\mathrm{x}=(0,1,0,0,0,...)\cdot(0,1,0,0,...)=(0,0,1,0,0,.....)$;

$\mathrm{x}^3=\mathrm{x}^2\cdot\mathrm{x}=(0,0,1,0,0,...)\cdot(0,1,0,0,...)=(0,0,0,1,0,0,...)$;

in generale si puo' dimostrare che

$\forall i\in\mathbb{N}_0$: $\mathrm{x}^i=\mathrm{x}^{i-1}\cdot\mathrm{x}=(0,0,...,1,0,0,...)$ e' la successione i cui elementi sono tutti nulli tranne quello che si trova al posto i e che e' uguale a 1.

Inoltre, ricordando le proprieta' delle potenze in un anello, si ha :

$$\forall i,j\in\mathbb{N}\ :\quad \mathrm{x}^i\cdot\mathrm{x}^j=\mathrm{x}^{i+j}\quad\text{e}\quad(\mathrm{x}^i)^j=\mathrm{x}^{ij}.$$

III) $\mathbf{a}\cdot\mathrm{x}=(a,0,0,...)\cdot(0,1,0,0,...)=(0,a,0,0,...)$;

$\mathbf{a}\cdot\mathrm{x}^2=(a,0,0,...)\cdot(0,0,1,0,...)=(0,0,a,0,0,..)$;

in generale e' dimostrabile che

$\forall i\in\mathbb{N}_0$: $\mathbf{a}\cdot\mathrm{x}^i=(0,0,...,a,0,0,...)$ e' la successione avente a al posto i e 0 in tutti gli altri posti.

Inoltre, ricordando che la moltiplicazione che abbiamo definito in S_A e' associativa, commutativa e distributiva rispetto all'addizione , si ha:

$(\mathbf{a}\cdot x^i)\cdot(b\cdot x^j)=(\mathbf{a}\cdot\mathbf{b})\cdot(x^i\cdot x^j)=\mathbf{ab}\cdot x^{i+j}$;
$(\mathbf{a}\cdot x^i)+(b\cdot x^i)=(\mathbf{a}+\mathbf{b})\cdot x^i$.

IV) $\mathbf{a}_0+\mathbf{a}_1\cdot x+\mathbf{a}_2\cdot x^2+\ldots+\mathbf{a}_t\cdot x^t=(a_0,0,0,\ldots)+(0,a_1,0,0,\ldots)+$
$+(0,0,a_2,0,0,\ldots)+\ldots+(0,0,\ldots,a_t,0,0,\ldots)=$
$=(a_0,a_1,a_2,\ldots.,a_t,0,0,\ldots)$.

Come si vede, se $(A,+,\cdot)$ e' un anello commutativo unitario, il polinomio $(a_0,a_1,\ldots.,a_t,0,0,\ldots)\in S_A$ e' **rappresentabile**, con le convenzioni fatte, con la scrittura

(*) $$\mathbf{a}_0+\mathbf{a}_1x^1+\mathbf{a}_2x^2+\ldots.+\mathbf{a}_tx^t.$$

In quest'ottica, se conveniamo di chiamare *monomi* i polinomi della forma $\mathbf{a}x^1$, potremo dire che ogni polinomio e' una somma di monomi.

É chiaro ora come in questo ambito x non sia "variabile" in un insieme bensi' sia un elemento dell'insieme S_A, precisamente e' la successione (0,1,0,0,..).

D'ora in avanti, ad evidenziare le posizioni fatte, indicheremo l'insieme S_A con il ben noto simbolo A[x] e, sempre applicando le proprieta' dell'addizione e della moltiplicazione in A[x] nonche' i risultati dati alla fine del punto III), si avra' che gli elementi di A[x], rappresentati nella forma (*), possono essere addizionati e moltiplicati con le usuali regole di calcolo.

A questo punto non e' superfluo notare che e' stato a partire da un generico anello commutativo unitario $(A,+,\cdot)$ che abbiamo costruito l'anello $(A[x],+,\cdot)$ dei polinomi su A o, come anche diremo, dei polinomi a coefficienti in A. D'altra parte e' ben

noto che anche gli anelli commutativi unitari "non sono tutti uguali". Infatti gia' $(\mathbb{Z},+,\cdot)$ e' un anello commutativo unitario nel quale vale la legge di annullamento del prodotto, il che non e' poco. Se invece consideriamo l'anello $(\mathbb{Z}_6,+,\cdot)$ dove $\mathbb{Z}_6=\{[0],[1],[2],[3],[4],[5]\}$ e' l'insieme delle classi dei resti modulo 6, questo e' un anello commutativo unitario per il quale non vale la legge di annullamento del prodotto (basta osservare che le classi [2] e [3] sono diverse dalla classe [0] ed hanno come prodotto la classe [6] che, come e' noto, coincide con la classe [0]).

Se consideriamo i numeri razionali, questi con le usuali operazioni di addizione e di moltiplicazione costituiscono un *campo*, cioe' un anello commutativo unitario, indicato con $(\mathbb{Q},+,\cdot)$, nel quale, non solo vale la legge di annullamento del prodotto, ma risulta anche che $\sqcup_{\mathbb{Q}}=\mathbb{Q}-\{0\}$, il che e' come dire che ogni elemento non nullo di $\mathbb{Q}$ e' dotato di inverso rispetto alla moltiplicazione (cosa che, come sappiamo, non accade in $\mathbb{Z}$). E struttura di campo hanno anche gli anelli commutativi unitari $(\mathbb{R},+,\cdot)$ e $(\mathbb{C},+,\cdot)$ dove con $\mathbb{R}$ abbiamo indicato l'insieme dei numeri reali e con $\mathbb{C}$ quello dei numeri complessi.

Ancora campi sono, per esempio, $(\mathbb{Z}_2,+,\cdot)$ e $(\mathbb{Z}_5,+,\cdot)$ solo che questi a differenza di quelli precedenti sono campi finiti. Siamo cosi portati a chiederci se l'eventuale ulteriore ricchezza di proprieta' dell'anello $(A,+,\cdot)$ influenzi l'anello $(A[x],+,\cdot)$. Per cercare di renderci conto di come stanno le cose proviamo a fare qualche operazione con polinomi a coefficienti in $(\mathbb{Z}_6,+,\cdot)$ che e' un anello molto "povero" rispetto agli altri anelli commutativi unitari considerati.

Siano pertanto $f=[2]x^3+[1]x-[3]$ e $g=[3]x$ elementi di $\mathbb{Z}_6[x]$; calcoliamo il prodotto h di f e g, si ha:

$h=f\cdot g=([2]x^3+[1]x-[3])\cdot([3]x)=[6]x^4+[3]x^2-[9]x=$

$=[0]x^4+[3]x^2-[3]=[3]x^2-[3]$.

Si nota subito che il polinomio f divide h, in quanto esiste g tale che $f\cdot g=h$, ma il grado di f non e' minore o uguale del grado

di h, in quanto $\delta(f)=3$ e $\delta(h)=2$, pertanto si ha:

Osservazione4.5 L'applicazione $\varphi:\mathbb{Z}_6[x]-\{0\}\longrightarrow\mathbb{N}_0$ che ad $f\in\mathbb{Z}_6[x]-\{0\}$ associa $\delta(f)\in\mathbb{N}_0$ non e' una funzione euclidea sull'anello $(\mathbb{Z}_6[x],+,\cdot)$ in quanto non soddisfa la condizione (i) della definizione2.10.

Inoltre risulta che $\delta(f\cdot g)=2$ mentre $\delta(f)+\delta(g)=3+1=4$, per tanto nell'anello $(\mathbb{Z}_6[x],+,\cdot)$ non vale la regola secondo la quale moltiplicando due polinomi di grado rispettivamente r ed s (quindi polinomi non nulli) si ottiene un polinomio di grado $r+s$ (che e' di conseguenza ancora un polinomio non nullo).
D'altra parte non ci siamo mai imbattuti in polinomi a coefficienti interi o razionali o reali per i quali non valesse la regola suddetta; e' lecito allora ipotizzare che in questi anelli tale regola valga per ogni coppia di polinomi non nulli e, qualora questa ipotesi dovesse risultare vera, sara' doveroso chiedersi da quale proprieta' degli anelli dei coefficienti dipenda cio'.

Le risposte ci sono date dal seguente

Teorema4.6 *Sia* $(A,+,\cdot)$ *un anello commutativo unitario. Sono equivalenti le seguenti affermazioni:*
(i) $(A,+,\cdot)$ *e' un dominio unitario;*
(ii) $(A[x],+,\cdot)$ *e' un dominio unitario;*
(iii) $\forall f,g\in A[x]-\{0\}$: $\delta(f)+\delta(g)=\delta(fg)$.

Dunque se in un anello commutativo unitario $(A,+,\cdot)$ vale la legge di annullamento del prodotto tale proprieta' viene estesa a $(A[x],+,\cdot)$ ed in questo anello vale la (iii) del teorema4.6.

D'altra parte, tenendo presente le osservazioni fatte subito dopo il teorema4.4, si ha che gli elementi di $\mathbb{Q}[x]$ di grado maggiore di 0 non sono invertibili e pertanto il dominio $(\mathbb{Q}[x],+,\cdot)$ non e' un campo, pur essendo campo il suo anello dei coefficienti.

Quindi, ricapitolando, si ha che esistono proprieta' di un anello commutativo unitario $(A,+,\cdot)$ che vengono "trasmesse" a $(A[x],+,\cdot)$ (per esempio essere D.U.) ed altre che non lo sono (per esempio essere campo); pertanto, visti i domini unitari a cui siamo interessati, e' spontaneo chiedesi:

Se $(A,+,\cdot)$ e' euclideo lo e' anche $(A[x],+,\cdot)$?
Se $(A,+,\cdot)$ e' principale lo e' anche $(A[x],+,\cdot)$?
Se $(A,+,\cdot)$ e' D.F.U. lo e' anche $(A[x],+,\cdot)$?

Vediamo subito che la risposta alla seconda domanda e' no. Infatti $(\mathbb{Z},+,\cdot)$ e' principale e $(\mathbb{Z}[x],+,\cdot)$ non lo e' (se cosi fosse, essendo $1\in$m.c.d.$(2,x)$, dovrebbero esistere, per il teorema3.3, $f,g\in\mathbb{Z}[x]$ tali che $1=f\cdot 2+g\cdot x$, e cio' e' falso come puo' verificarsi facilmente).

Da quanto abbiamo appena detto segue che anche la risposta alla prima domanda e' no. Infatti $(\mathbb{Z},+,\cdot)$ e' euclideo e $(\mathbb{Z}[x],+,\cdot)$ non lo e' (se lo fosse, dato il teorema 2.11, sarebbe principale!) e pertanto possiamo affermare che non esistono funzioni euclidee su $\mathbb{Z}[x]$.

Quindi, riflettendo sulle considerazioni appena fatte, deduciamo subito che l'applicazione

$$\varphi:\ \mathbb{Z}[x]-\{0\}\longrightarrow\mathbb{N}_0$$
$$f\in\mathbb{Z}[x]-\{0\}\longmapsto\delta(f)\in\mathbb{N}_0$$

pur soddisfacendo alla condizione (i) della definizione2.10 in quanto $(\mathbb{Z},+\cdot)$ e' un dominio di integrita', non puo' essere una funzione euclidea su $\mathbb{Z}[x]$, e pertanto non soddisfa la condizione (ii) della definizione2.10.

Ora e' necessario fare attenzione se vogliamo raccordare la nostra esperienza con le considerazioni fatte: dire che l'applicazione φ non soddisfa la condizione (ii) della definizione2.10 significa semplicemente che esistono polinomi

$f,g\in\mathbb{Z}[x]$, con $g\neq\mathbf{0}$, per i quali non esistono $q,r\in\mathbb{Z}[x]$ tali che $f=q\cdot g+r$, con $r=\mathbf{0}$ oppure di grado minore del grado di g. E cio' e' in perfetto accordo con la nostra esperienza secondo la quale, per esempio, possiamo "trovare un quoziente e un resto" in $\mathbb{Z}[x]$ per i polinomi $f=\mathbf{3}x^3+\mathbf{5}x-\mathbf{2}$ e $g=x^2+\mathbf{4}$ mentre cio' non e' possibile per i polinomi $f=\mathbf{3}x^2$ e $g=\mathbf{2}x$.

A questo punto, vista la ricchezza di risultati che si hanno in un anello euclideo, possiamo cercare di capire quali proprieta' richiedere per l'anello commutativo unitario $(A,+,\cdot)$ perche' $(A[x],+,\cdot)$ risulti un dominio euclideo.

A tale scopo ripensiamo a quanto facciamo usualmente ed osserviamo che, dati $f=\mathbf{5}x^3+\mathbf{2}x^2-\mathbf{1}$ e $g=\mathbf{3}x^2-\mathbf{4}x$ elementi di $\mathbb{Z}[x]$, mentre per essi non possiamo trovare in $\mathbb{Z}[x]$ un "quoziente e un resto" cio' e' possibile per i polinomi $h=\mathbf{3}^2\cdot f$ e g; infatti, con $q=\mathbf{15}x+\mathbf{26}$ e $r=\mathbf{104}x-\mathbf{9}$, si ha $h=q\cdot g+r$ con $\delta(r)<\delta(g)$.

Quanto visto per i polinomi f e g non e' eccezionale, infatti si puo' dimostrare il seguente

Teorema4.7 *Siano* $(A,+,\cdot)$ *un* D.U. *e* $f,g\in A[x]-\{\mathbf{0}\}$. *Si dimostra che esistono* $q,r\in A[x]$ *tali che* $\mathbf{a}^k\cdot f=q\cdot g+r$, *dove a* e' *il coefficiente direttore di* g, $k=\max\{\delta(f)-\delta(g)+1,0\}$, *ed inoltre* $r=0$ *oppure* $\delta(r)<\delta(g)$.

Dal teorema4.7 segue subito che se **a** e' un elemento invertibile allora $f=(\mathbf{a}^{-k}q)\cdot g+\mathbf{a}^{-k}r$, pertanto esistono $q_1=\mathbf{a}^{-k}q$ e $r_1=\mathbf{a}^{-k}r$ tali che $f=q_1g+r_1$ con $r_1=0$ oppure $\delta(r_1)<\delta(g)$; possiamo cosi' concludere che se $(C,+,\cdot)$ e' un campo, considerata la funzione

$$\delta:C[x]-\{\mathbf{0}\}\longrightarrow\mathbb{N}_0$$

che ad $f\neq\mathbf{0}$ associa il suo grado, essa e' tale che:

i) $\forall f,g\in C[x]-\{\mathbf{0}\}$: $f\mid g\Rightarrow\delta(f)\leq\delta(g)$;

ii) $\forall f,g\in C[x]$, $g\neq\mathbf{0}$ esistono $q,r\in C[x]$ tali che $f=q\cdot g+r$ con $r=\mathbf{0}$ oppure $\delta(r)<\delta(g)$.

Quindi:

Teorema4.8 *Se* $(C,+,\cdot)$ *e'un campo allora, e solo allora,* $(C[x],+,\cdot)$ *e',* con la funzione δ, *un dominio euclideo.*

Come conseguenza immediata del teorema precedente si ha che se $(C,+,\cdot)$ e' un campo allora $(C[x],+,\cdot)$ e' un dominio principale e quindi a fattorizzazione unica.

Il teorema4.8 svolge un ruolo importante nella dimostrazione, non immediata, del seguente

Teorema4.9 *Se* $(A,+,\cdot)$ *e' un dominio a fattorizzazione unica allora* $(A[x],+,\cdot)$ *e' un dominio a fattorizzazione unica.*

Riusciamo cosi' a sapere che $(\mathbb{Z}[x],+,\cdot)$, che abbiamo gia' osservato non essere euclideo ne' principale, e' un dominio a fattorizzazione unica e pertanto esso fornisce un esempio di D.F.U. che non e' D.P.; questo ci dice che la classe P dei domini principali e' inclusa propriamente nella classe F dei domini a fattorizzazione unica e rispondiamo cosi' ad una delle domande alle quali non avevamo saputo rispondere nella prima parte di questa esposizione.

Ma non basta; i risultati ottenuti ci permettono anche di dire che oltre a $(\mathbb{Z},+,\cdot)$ esistono altri domini euclidei, per esempio $(\mathbb{Q}[x],+,\cdot)$, $(\mathbb{R}[x],+,\cdot)$, $(\mathbb{C}[x],+,\cdot)$, $(\mathbb{Z}_2[x],+,\cdot)$,...; inoltre non e' difficile dimostrare che il sottoinsieme G del campo dei complessi dato da $G=\{z\in\mathbb{C} \mid \exists a,b\in\mathbb{Z}\ z=a+bi\}$, con le usuali operazioni fra complessi, e' un dominio euclideo noto come dominio degli interi di Gauss.

Concludiamo questa parte facendo notare che con dimostrazione non immediata si puo' stabilire che i sottoinsiemi di $\mathbb{C}$ dati da $B_d=\{z\in\mathbb{C} \mid \exists a,b\in\mathbb{Z} z=a+b\sqrt{d}\}$, con $d\in\{-19,-43,-67,-163\}$, sono, rispetto alle usuali operazioni in $\mathbb{C}$, domini principali e non euclidei.

A questo punto siamo in condizioni di "arricchire" anche la

figura2. Si ha infatti la seguente figura3:

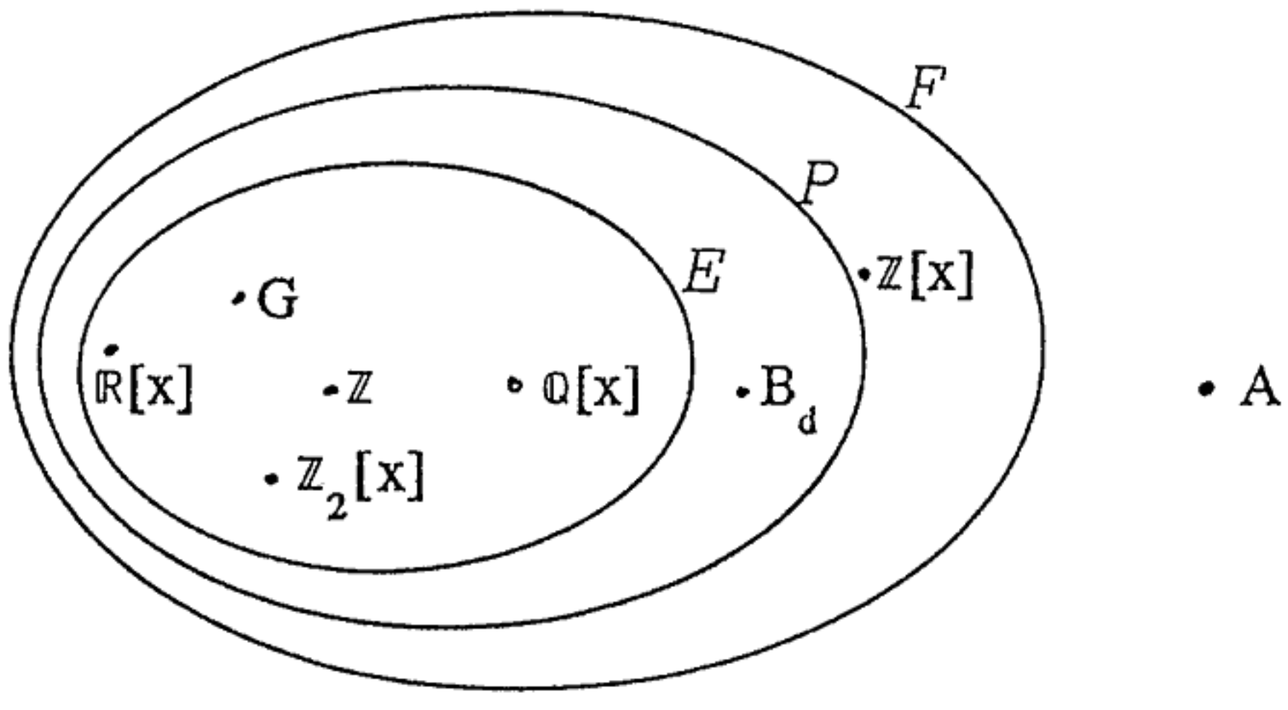

fig.3

Chiaramente ora si pone il problema di generalizzare la definizione di polinomio in una "variabile", dando quella di polinomio in piu' "variabili"; pero' prima di passare a questo argomento cerchiamo di chiarire da dove trae origine la tradizione di chiamare "variabile" l'elemento x dell'insieme A[x]; a tale scopo nel seguente numero introdurremo la nozione di funzione polinomiale e ne illustreremo i collegamenti con i polinomi.

5.FUNZIONI POLINOMIALI.

Sia $(A,+,\cdot)$ un anello commutativo unitario e sia $f=(a_0,a_1,\ldots,a_t,0,0,\ldots)=a_0+a_1x+\ldots+a_tx^t\in A[x]$. Consideriamo l'applicazione :

$$f^*: \quad A \longrightarrow A$$
$$v\in A \longmapsto a_0+a_1v+\ldots+a_tv^t\in A.$$

Chiameremo f^* *funzione polinomiale associata al polinomio f.*

Siano $f=(a_0,a_1,\ldots,a_t,0,0,\ldots)$, $g=(b_0,b_1,\ldots,b_r,0,0,\ldots)\in A[x]$;

ci chiediamo:

1) Se $f=g$ possiamo dire che $f^*=g^*$?
2) Se $f^*=g^*$ possiamo dire che $f=g$?

La risposta alla domanda 1) e' chiaramente affermativa visto che $f=g$ se e solo se $a_i=b_i$ per ogni $i\in\mathbb{N}_0$ (cfr. Osservazione4.2) e che quindi, in questo caso, risulta essere $f^{*0}(v)=g^*(v)$ per ogni $v\in A$.

La risposta alla domanda 2) non appare altrettanto immediata; per tanto e' opportuno provare a costruire degli esempi di funzioni polinomiali, esempi che possano aiutarci ad immaginare in quale direzione muoverci per cercare di intravedere una risposta.

EsempioE$_2$. Siano $f=[1]x^3+[2]x$ e $g=[0]$ polinomi a coefficienti nell'anello $(\mathbb{Z}_3,+,\cdot)$ delle classi dei resti modulo 3. Si ha che:

$$f^*:\begin{cases}[0]\longrightarrow[1]\cdot[0]^2+[2]\cdot[0]=[0]\\ [1]\longrightarrow[1]\cdot[1]^3+[2]\cdot[1]=[3]=[0]\\ [2]\longrightarrow[1]\cdot[2]^3+[2]\cdot[2]=[12]=[0]\end{cases}\qquad g^*:\begin{cases}[0]\longrightarrow[0]\\ [1]\longrightarrow[0].\\ [2]\longrightarrow[0]\end{cases}$$

Si vede cosi' che $f^*=g^*$ pur essendo chiaramente $f\neq g$.
Da cio' possiamo dedurre una prima informazione: se $(A,+,\cdot)$ e' un anello commutativo unitario finito non possiamo dire che due polinomi a coefficienti in A sono uguali se hanno funzioni polinomiali uguali (abbiamo appena visto che questo non accade neanche quando l'anello finito $(A,+,\cdot)$ e' tanto particolare da essere addirittura un campo, come e' il caso di $(\mathbb{Z}_3,+,\cdot)$).

Rivolgiamo allora la nostra attenzione a polinomi a coefficienti in un anello commutativo unitario infinito e, per renderci conto di quanto "pesi" il fatto di essere infinito, costruiamo un anello di polinomi a coefficienti in un anello commutativo unitario che sia infinito e che non sia neanche dominio di integrita'.

EsempioE$_3$.Consideriamo l'insieme B delle successioni di elementi dell'insieme $\mathbb{Z}_2=\{[0],[1]\}$. Scriviamo gli elementi di B nella forma

$(b_1,b_2,b_3,....)$ dove ogni b_i e' [0] oppure [1]. Sfruttando l'addizione e la moltiplicazione dell'anello $(\mathbb{Z}_2,+,\cdot)$ definiamo un'addizione e una moltiplicazione in B ponendo:

$$(b_1,b_2,b_3,.....)+(c_1,c_2,c_3,...)=(b_1+c_1,\ b_2+c_2,\ b_3+c_3,....)$$
$$(b_1,b_2,b_3,.....)\cdot(c_1,c_2,c_3,...)=(b_1\cdot c_1,\ b_2\cdot c_2,\ b_3\cdot c_3,....).$$

E' facile verificare che $(B,+,\cdot)$ e' un anello commutativo unitario infinito avente $\zeta=([0],[0],[0],.....)$ e $\upsilon=([1],[1],[1],....)$ rispettivamente elemento neutro rispetto all'addizione e elemento neutro rispetto alla moltiplicazione (attenzione non lasciamoci ingannare dalle successioni! Gli elementi di B non sono polinomi: la moltiplicazione non e' la stessa e elementi di B non sono soltanto le successioni definitivamente nulle).

Osserviamo che $(B,+,\cdot)$ non e' un dominio d'integrita'; infatti $([1],[0],[0],[0],...)$ e $([0],[1],[0],[0],...)$ sono elementi di B diversi da ζ ed il cui prodotto e' ζ.

In B[x] consideriamo il polinomio nullo g e il polinomio non nullo $f=x\cdot(x-\upsilon)$. Chiaramente la funzione polinomiale g^* associata al polinomio nullo g fa corrispondere ad ogni elemento di B lo zero di B, cioe' l'elemento ζ.

Determiniamo l'elemento di B che l'applicazione f^* fa corrispondere al generico elemento $(b_1,b_2,b_3,...)\in B$. Si ha:

$f^*((b_1,b_2,b_2,...))=$
$=(b_1,b_2,b_3,...)\cdot\{(b_1,b_2,b_2,....)-([1],[1],[1]...)\}=$
$=(b_1,b_2,b_3,...)\cdot(b_1-[1],b_2-[1],b_3-[1],.....)=$
$=(b_1(b_1-[1]),\ b_2(b_2-[1]),\ b_3(b_3-[1]),\ .....).$

Pero' ogni b_i e' [0] oppure [1], quindi

$f^*((b_1,b_2,b_3,....))=([0],[0],[0],...).$

Si vede cosi' che ai polinomi distinti f e g corrispondono funzioni polinomiali uguali.

Tutto cio' ci induce a pensare che per una eventuale risposta positiva alla domanda 2) non basta aggiungere sull'anello

commutativo unitario $(A,+,\cdot)$ l'ipotesi che sia infinito.

A questo punto potremmo facilmente essere presi dallo sconforto! Ma all'ulteriore piccolo passo, che consiste nel chiedersi cosa accadra' se consideriamo anelli di polinomi a coefficienti in un dominio unitario infinito, la nostra costanza sara' premiata; infatti si dimostra il seguente teorema, noto come **Principio di identita' dei polinomi.**

Teorema5.1 *Sia* $(A,+,\cdot)$ *un dominio di integrita'* infinito. *Siano* $f,g\in A[x]$. *Si dimostra che* $f=g$ *se e solo se* $f^*=g^*$.

A proposito del principio di identita' dei polinomi evidenziamo come, ponendoci domande e mostrando controesempi di cose "ovvie", abbiamo chiarito il significato e i limiti di tale "principio" che sottointende diversi aspetti non sempre chiaramente esposti nei libri di testo delle scuole secondarie superiori (ed anche in certi testi universitari!).

Osserviamo che se $(A,+,\cdot)$ e' un dominio di integrita' infinito, il teorema5.1 puo' consentire di identificare il polinomio $f\in A[x]$ con l'applicazione polinomiale f^*. Questo punto di vista e' quello solitamente seguito in analisi e in geometria algebrica classica dove, avendosi a che fare con polinomi a coefficienti nel campo dei complessi (che e' un dominio di integrita' infinito) i polinomi vengono identificati con la corrispondente funzione polinomiale e di consegueza, coerentemente con questo punto di vista, viene dato ad x il nome di "variabile".

Appagata con le considerazioni svolte anche la curiosita' di sapere da dove trae origine il nome di "variabile" dato ad x, nome che in seguito adotteremo anche noi, passiamo a parlare di polinomi in piu' variabili cercando di dare di questi una definizione che generalizzi quella data per polinomi in una variabile.

6.POLINOMI IN PIU' "VARIABILI".

Sia $n\in\mathbb{N}$ e sia $\mathbb{N}_0^{(n)}$ l'insieme delle n-ple $(i_1,i_2,...,i_n)$ di elementi di $\mathbb{N}_0$. Poniamo $(i):=(i_1,i_2,..,i_n)\in\mathbb{N}_0^{(n)}$.

Definizione6.1 Sia $(A,+,\cdot)$ un anello commutativo unitario e $n\in\mathbb{N}$. Dicesi *polinomio su* A *in* n *variabili* ogni applicazione $f:\mathbb{N}_0^{(n)}\longrightarrow A$ *quasi ovunque nulla* cioe', tale che $f((i))\neq 0$ solo per un numero finito di elementi $(i)\in\mathbb{N}_0^{(n)}$.

Se identifichiamo $\mathbb{N}_0^{(1)}$ con $\mathbb{N}_0$ ed identifichiamo (i_1) con i_1, dalla definizione6.1 segue che un polinomio su A in una variabile e' una applicazione $f:\mathbb{N}_0\longrightarrow A$ tale che $f(i)\neq 0$ solo per un numero finito di elementi $i\in\mathbb{N}_0$; cioe' si ottiene la definizione4.1.

Indicato con $S_A^{(n)}$ l'insieme dei polinomi su A in n variabili, e dati $f,g\in S_A^{(n)}$, possiamo dimostrare che:
(I) l'applicazione $s:\mathbb{N}_0^{(n)}\longrightarrow A$, che ad ogni $(i)\in\mathbb{N}_0^{(n)}$ associa $f((i))+g((i))$, e' un'applicazione quasi ovunque nulla cioe' e' un elemento di $S_A^{(n)}$;
(II) l'applicazione $p:\mathbb{N}_0^{(n)}\longrightarrow A$, che ad ogni $(i)\in\mathbb{N}_0^{(n)}$ associa $\sum_{(t)+(h)=(i)} f((t))\cdot g((h))$, dove $(t)+(h)=(t_1+h_1,t_2+h_2,\ldots,t_n+h_n)$, e' un'applicazione quasi ovunque nulla, cioe' e' un elemento di $S_A^{(n)}$.

Pertanto sono operazioni in $S_A^{(n)}$ l'applicazione

$+:S_A^{(n)}x\ S_A^{(n)}\longrightarrow S_A^{(n)}$ che alla coppia (f,g) associa s

e l'applicazione

$\cdot:S_A^{(n)}x\ S_A^{(n)}\longrightarrow S_A^{(n)}$ che alla coppia (f,g) associa p.

Per fare qualche esempio di prodotto e somma di polinomi in piu' variabili, sia $n=3$ e sia $A=\mathbb{Z}$.

EsempioE_4. Consideriamo $f,g \in S_{\mathbb{Z}}^{(3)}$ definiti da:

$$f:\begin{cases}(1,2,3)\longrightarrow -5\\(0,1,0)\longrightarrow 2\\(i)\longrightarrow 0 \qquad \text{se (i) e' diverso da (1,2,3) e da (0,1,0).}\end{cases}$$

$$g:\begin{cases}(1,2,0)\longrightarrow 1\\(0,1,0)\longrightarrow 9\\(2,1,0)\longrightarrow 4\\(i)\longrightarrow 0 \qquad \text{se (i) e' diverso da (1,2,0),(0,1,0) e (2,1,0).}\end{cases}$$

Si avra' allora che la somma $s=f+g$ e' la funzione:

$$s:\begin{cases}(1,2,3)\longrightarrow f((1,2,3))+g((1,2,3))=-5+0=-5\\(0,1,0)\longrightarrow f((0,1,0))+g((0,1,0))=2+9=11\\(1,2,0)\longrightarrow f((1,2,0))+g((1,2,0))=0+1=1\\(2,1,0)\longrightarrow f((2,1,0))+g((2,1,0))=0+4=4\\(i)\longrightarrow 0 \quad \text{se (i) e' diverso da (1,2,3),(0,1,0),(1,2,0) e da (2,1,0).}\end{cases}$$

EsempioE_5 Per il prodotto di due polinomi diamo un cenno di come procedere per determinare $p=f\cdot g$ con $f,g \in S_{\mathbb{Z}}^{(3)}$ e definiti come segue:

$$f:\begin{cases}(0,0,0)\longrightarrow 2\\(0,1,0)\longrightarrow 3\\(i)\longrightarrow 0 \qquad \text{se (i) e' diverso da (0,0,0) e da (0,1,0);}\end{cases}$$

$$g:\begin{cases}(1,0,0)\longrightarrow 4\\(0,1,0)\longrightarrow 5\\(i)\longrightarrow 0 \qquad \text{se (i) e' diverso da (1,0,0) e da (0,1,0).}\end{cases}$$

Calcoliamo, per esempio, il valore che la funzione p assume in (0,0,0), in (0,1,0) e in (2,1,0).

Si ha:

$$p((0,0,0))=f((0,0,0))\cdot g((0,0,0))=2\cdot 0=0;$$

$$p((0,1,0))=f((0,0,0))\cdot g((0,1,0))+f((0,1,0))\cdot g((0,0,0))=2\cdot 5+3\cdot 0=10$$

$$\begin{aligned}p((2,1,0))&=f((0,0,0))\cdot g((2,1,0)+f((1,0,0)\cdot g((1,1,0))+\\&+f((2,0,0))\cdot g((0,1,0))+f((0,1,0))\cdot g((2,0,0))+\\&+f((1,1,0))\cdot g((1,0,0))+f((2,1,0))\cdot g((0,0,0))=2\cdot 0+0\cdot 0+0\cdot 5+3\cdot 0+\\&+0\cdot 4+0\cdot 0=0;\end{aligned}$$

Con l'addizione e la moltiplicazione precedentemente definite in $S_A^{(n)}$ si ha (a prezzo di calcoli abbastanza "pesanti"):

Teorema6.1 *Dato un anello commutativo unitario* $(A,+,\cdot)$, *si dimostra che la struttura* $(S_A^{(n)},+,\cdot)$ *e' un anello commutativo unitario.*

Come si vede dagli esempi E_4 ed E_5, tenendo presenti le definizioni date, e' stata cosa gia' molto laboriosa assegnare semplici polinomi in piu' variabili ed e' stata cosa molto pesante eseguire un'addizione e "cominciare" ad eseguire una moltiplicazione. Pertanto, non e' una questione accademica o estetica cercare di giungere ad una rappresentazione dei polinomi in piu' variabili, la quale permetta non solo un'agevole assegnazione di essi ma, soprattutto, un agevole modo di operare con essi. L'importanza dell'uso di una opportuna rappresentazione e' d'altra parte evidente, se si ricorda che, dall'antichita' fino all'avvento (nel secolo XV) della nostra moderna **rappresentazione** posizionale dei numeri naturali, i progressi nell'arte del calcolo furono minimi e che operazioni, ora alla portata di un bambino, richiedevano ad uno specialista giorni di complicato lavoro.

Allo scopo di arrivare alla rappresentazione usuale degli elementi di $S_A^{(n)}$, tenendo presente anche quanto abbiamo fatto per

i polinomi in una variabile, siano $\mathbf{a},x_1,x_2,\ldots,x_n$ le funzioni da $\mathbb{N}_0^{(n)}$ in A (cioe' i polinomi in n variabili) definite nel modo seguente:

$$\mathbf{a}:\begin{cases}(0,0,0,..,0)\longrightarrow a\\ \qquad (i)\longrightarrow 0 \qquad\qquad \text{se } (i)\neq(0,0,..,0)\end{cases}$$

$$x_1:\begin{cases}(1,0,0,..,0)\longrightarrow 1\\ \qquad (i)\longrightarrow 0 \qquad\qquad \text{se } (i)\neq(1,0,..,0)\end{cases}$$

$$x_2:\begin{cases}(0,1,0,..,0)\longrightarrow 1\\ \qquad (i)\longrightarrow 0 \qquad\qquad \text{se } (i)\neq(0,1,..,0)\end{cases}$$

.....

$$x_n:\begin{cases}(0,0,0,..,1)\longrightarrow 1\\ \qquad (i)\longrightarrow 0 \qquad\qquad \text{se } (i)\neq(0,0,..,1)\end{cases}$$

Visto come sono definiti i polinomi $\mathbf{a},x_1,x_2,\ldots x_n$ e come e' definita la moltiplicazione fra polinomi, possiamo calcolare (e si immagina con quanta buona volonta'!) il prodotto

$$(*)\qquad f=\mathbf{a}\cdot x_1^{\alpha_1}\cdot x_2^{\alpha_2}\cdot\ldots\cdot x_n^{\alpha_n};$$

si vede cosi' che l'applicazione f e' data da:

$$f=\mathbf{a}\cdot x_1^{\alpha_1}\cdot x_2^{\alpha_2}\cdot\ldots\cdot x_n^{\alpha_n}:\begin{cases}(\alpha_1,\alpha_2,\ldots,\alpha_n)\longrightarrow a\\ \qquad (i)\longrightarrow 0 \quad \text{se } (i)\neq(\alpha_1,\alpha_2,..,\alpha_n)\end{cases}$$

Ai polinomi della forma (*) diamo il nome di *monomi*.

Ora non e' difficile verificare che, effettuato il seguente calcolo,

$$\mathbf{a}_1\cdot x_1^{\alpha_1^{(1)}}\cdot x_2^{\alpha_2^{(1)}}\cdot..\cdot x_n^{\alpha_n^{(1)}}+\mathbf{a}_2\cdot x_1^{\alpha_1^{(2)}}\cdot x_2^{\alpha_2^{(2)}}\cdot..\cdot x_n^{\alpha_n^{(2)}}+\quad+\mathbf{a}_r\cdot x_1^{\alpha_1^{(r)}}\cdot x_2^{\alpha_2^{(r)}}\cdot\ldots\cdot x_n^{\alpha_n^{(r)}}$$

si ottiene il polinomio f dato da:

$$f:\begin{cases}(\alpha_1^{(1)},\ldots,\alpha_n^{(1)})\longrightarrow a_1\\(\alpha_1^{(2)},\ldots,\alpha_n^{(2)})\longrightarrow a_2\\\ldots..\\(\alpha_1^{(r)},\ldots,\alpha_n^{(r)})\longrightarrow a_r\end{cases}$$

Ed ecco quindi come, chiarito il contesto, possiamo dire che un polinomio e' una somma di monomi (non simili, come aggiungono alcuni!).

Inoltre e' chiaro che le usuali regole per trovare somme e prodotti di polinomi non sono altro che l'applicazione successiva delle proprieta' dell'addizione e della moltiplicazione definite in $S_A^{(n)}$.

Per renderci conto di quanto sia comodo **rappresentare** un polinomio come somma di monomi, ritorniamo ai polinomi f,g dell'esempio E_4; essi, usando x,y,z invece di x_1,x_2,x_3, sono rappresentabili nel seguente modo:

$f=-5xy^2z^3+2y$ $g=1xy^2+9y+4x^2y$ e quindi

$f+g=-5xy^2z^3+11y+1xy^2+4x^2y$ cioe' il polinomio s che avevamo trovato nell'esempio E_4.

Cosi nell'esempio E_5 si ha:

$f=2+3x$ $g=4x+5y$ e quindi

$f\cdot g=8x+10y+12x^2+15xy$ cioe' il polinomio p che avevamo cominciato a trovare applicando la definizione di moltiplicazione tra polinomi.

E' evidente che a questo punto si pone un problema di carattere didattico non indifferente in quanto e' manifesta a tutti la difficolta' di presentare a ragazzi di scuola secondaria superiore, nel modo che abbiamo esposto, anche solo i polinomi in due variabili. Esistono pero' alcuni teoremi, coinvolgenti la natura *trascendente* delle variabili e dei quali e' qui impossibile anche solo riportare gli enunciati, (comunque il lettore

volenteroso potra' provare a leggere Zariski-Samuel "Commutative algebra" Vol. I pag.25-39) che, oltre a chiarire alcune questioni sull'anello $(S_A^{(n)},+,\cdot)$, ci aiutano a scegliere la strategia da seguire per avvicinare, in un modo coerente, i ragazzi ai polinomi in piu' variabili.

Tali teoremi garantiscono che l'anello $(S_A^{(n)},+,\cdot)$ dei polinomi nelle n variabili $x_1,\ldots,x_n$, e a coefficienti in A puo' essere "identificato" (i teoremi ai quali pensiamo puntualizzano proprio il significato di questa "identificazione") con l'anello dei polinomi in **una** qualunque delle variabili e i cui coefficienti sono polinomi su A nelle n-1 variabili rimanenti.

Questo riguardare $(S_A^{(n)},+,\cdot)$ come l'anello $(S_{A_1}^{(1)},+,\cdot)$ dove $A_1:=S_A^{(n-1)}$, da una parte ci aiuta a penetrare meglio in questioni riguardanti il "trasferimento" di proprieta' dall'anello $(A,+,\cdot)$ all'anello $(S_A^{(n)},+,\cdot)$, dall'altra ci fornisce una indicazione su come parlare ai ragazzi di polinomi in due variabili, poi di polinomi in tre variabili, e cosi' via.

Possiamo infatti procedere nel seguente modo.

Sia $(A,+,\cdot)$ un anello commutativo unitario; costruito l'anello commutativo unitario $(A[x],+,\cdot)$ ed indicato con A_1 l'insieme A[x], possiano considerare l'anello dei polinomi a coefficienti in A_1 e nella variabile y; a tale anello, cioe' all'anello $(A_1[y],+,\cdot)$, diamo il nome di anello dei polinomi a coefficienti in A e nelle variabili x,y. Si vede allora come i polinomi in due variabili e a coefficienti in A siano polinomi in una variabile i cui coefficienti sono polinomi (in una variabile e a coefficienti in A).

Costruito cosi' $(A_1[y],+,\cdot)$ e posto $A_2:=A_1[y]$ avremo i polinomi nelle variabili x,y,z, e a coefficienti in A, costruendo l'anello commutativo unitario $(A_2[z],+,\cdot)$; cosi' di seguito potranno costruirsi i polinomi, a coefficienti in A, in quattro variabili e poi in cinque e cosi' via.

Come si vede, si e' passati da un'ottica nella quale c'era un'assegnazione globale di n variabili in cui riconoscere i polinomi in una variabile come caso particolare, ad un'ottica nella quale abbiamo un'assegnazione successiva di variabili a partire dai polinomi in una variabile. Non si pensi pero' che la scelta di tale ottica, che sembra piu' semplice, non abbia un costo.

Infatti, essendo in tale impostazione x=(0,1,0,0,..) e y=((0,0,0,..), (1,0,0,...), (0,0,0,...),.....), i polinomi nelle variabili x,y saranno sempre polinomi nella variabile y e a coefficienti polinomi in x e non potranno essere riguardati come polinomi nella variabile x e a coefficienti polinomi in y (in tal caso, secondo la definizione alla quale stiamo facendo riferimento, dovrebbe essere y=(0,1,0,0,..) e x=((0,0,0,..), (1,0,0,...), (0,0,0,...),.....); invece e' possibile fare cio' quando i polinomi nelle variabili x ed y vengono definiti cosi' come abbiamo fatto all'inizio del paragrafo.

Ci sembra comunque questo un costo non eccessivo, anche perche' ci impone uno sforzo di coerenza nell'ambito della quale dovremo imparare a riconoscere situazioni in cui, tenendo presente le definizioni che abbiamo deciso di dare, non potremo dire tutto quello che avremmo potuto con uno sforzo iniziale maggiore. Questo e', a mio avviso, ancora un buon motivo per adottare tale tipo di impostazione in quanto da cio' si potra' trarre lo spunto per un discorso che, prendendo le mosse dalla matematica, vada a coinvolgere la formazione "etica" dei ragazzi.

Passiamo ora a qualche considerazione riguardante polinomi in piu' variabili in relazione all'anello dei coefficienti.

Si ha infatti:

(I) Mentre l'anello dei polinomi a coefficienti in un campo e in una variabile e', con la funzione euclidea δ, un dominio

euclideo (vedi teorema4.8) non possiamo dire altrettanto per l'anello dei polinomi in due variabili a coefficienti in un campo. Infatti tali anelli sono polinomi in una variabile ma a coefficienti in un anello di polinomi che non e 'un campo (vedi (iii) del teorema4.4).

Questo, ricordando quanto abbiamo detto a proposito della proprieta' euclidea di un dominio, non e' una perdita da poco; basti pensare che, mentre, per esempio in $(\mathbb{Q}[x],+,\cdot)$, possiamo ricorrere all'algoritmo euclideo per la ricerca di un massimo comun divisore fra due polinomi dei quali non riusciamo a trovare una decomposizione in fattori irriducibili (pur sapendo che una tale decomposizione esiste!), cio' non e' piu' possibile quando andiamo a considerare i polinomi in x,y ed a coefficienti in $\mathbb{Q}$. Infatti in tale anello potremo dividere un polinomio f solo per particolari polinomi g non nulli (per esempio quelli aventi il coefficiente direttore invertibile) e questo anche se gli esercizi di solito proposti hanno l'accortezza di scegliere i polinomi g "buoni"! Potremo pero' sempre fare riferimento al teorema4.7. Per esempio, dati i polinomi a coefficienti in $\mathbb{Q}$ e nelle variabili x e y:

$f=y^4+(3x^2+2)y^3-2xy+3x$

$g=(x+1)y^2+3x^2$

osserviamo che essi sono polinomi in y a coefficienti in $\mathbb{Q}[x]$ e che il coefficiente direttore di g e' $x+1$. Pertanto potremo dividere per g il polinomio $h=(x+1)^k\cdot f$ dove $k=\max\{4-2+1,0\}=3$.

(II) Se $(A,+,\cdot)$ e' un dominio a fattorizzazione unica allora $(A[x],+,\cdot)$ e' un dominio a fattorizzazione unica (vedi teorema4.9) quindi e' tale l'anello dei polinomi in y ed a coefficienti in A[x]. Pertanto l'anello dei polinomi in due variabili e a coefficienti in un D.F.U. e' un D.F.U. e tale sara' ogni anello di polinomi in n variabili e a coefficienti in un D.F.U.

Possiamo cosi' modificare la figura3 ed ottenere la seguente

figura4:

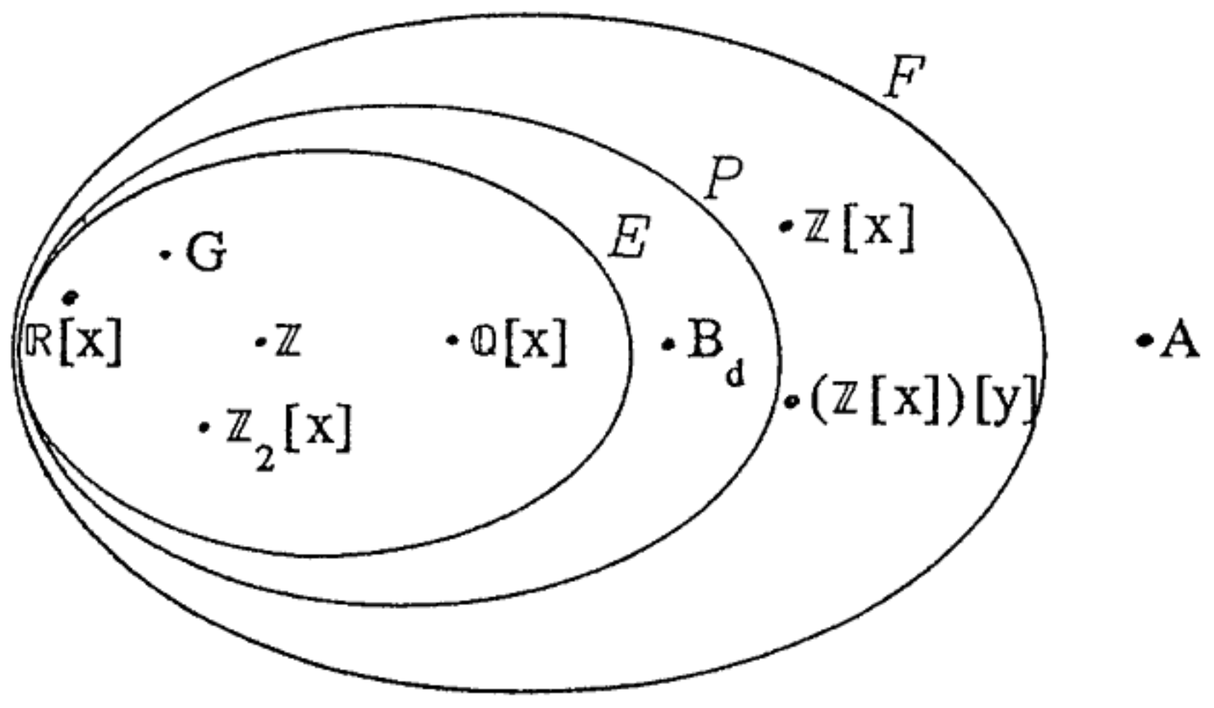

fig.4

Facendo notare che con quanto finora detto abbiamo solo "sbirciato" nel mondo dei polinomi, terminiamo qui la nostra esposizione senza con questo voler dire che si concludono qui i discorsi iniziati nel paragrafo 1.

Qui non vi e' conclusione.
Chi ha detto che si debba concludere? Qui non vi e' fortuna da predire e nemmeno consigli da dare.

Buon viaggio.

W.James (1842-1910)

Bibliografia

M.Curzio Lezioni di algebra.
Liguori editore.(Napoli)

H.Decoste Des anneaux principaux, non euclidiens.
Ann. Sc. Math. Quebec 5, 103-114 (1981).

I.N.Herstein Algebra.
Editori riuniti. (Roma)

A.Robinson Numbers and ideals.
Holden-Day,Inc.(London)

O.Zariski-P.Samuel Commutative Algebra.
D.Van Nostrand Company,Inc.(New York)