NOZIONI ELEMENTARI SUGLI ANELLI

Si presentano qui alcune nozioni sugli anelli, sia come modello di strutture con due operazioni binarie, sia per l'importanza di queste strutture in tutte le sezioni della Matematica pura.

Con un piccolo abuso di linguaggio e come è consuetudine quando non vi siano ambiguità, gli anelli saranno identificati mediante i loro sostegni; ossia, un anello $\left(A,+,\cdot,1_A\right)$ sarà sovente denotato solo con A.

Prerequisiti[1]**:** insiemi, funzioni, relazioni d'equivalenza, operazioni e loro proprietà, strutture algebriche, insiemi numerici e calcolo combinatorio, gruppi.

Contenuto:

[1] Per ciascuno dei prerequisiti si veda il capitolo apposito.

§ 1 – ANELLI ASSOCIATIVI UNITARI

Un anello (generale) è una struttura algebrica $(A,+,\cdot)$ con due operazioni binarie, dove $(A,+)$ è un gruppo abeliano e valgono le due *proprietà distributive* (destra e sinistra) di $\cdot$ rispetto a $+$, ossia:

$$\forall a,b,c \in A, \begin{cases} a\cdot(b+c) = a\cdot b + a\cdot c \\ (a+b)\cdot c = a\cdot c + b\cdot c \end{cases}.$$

Se la moltiplicazione $\cdot$ ha la proprietà associativa, l'anello si dice *associativo*; se ha l'elemento neutro 1_A, l'anello si dice *unitario*.

Gli anelli che considereremo nel seguito saranno associativi ed unitari. Li chiameremo anelli, senza ulteriori aggettivi.

Un anello $(A,+,\cdot,1_A)$ è quindi per noi un gruppo abeliano rispetto all'addizione, un monoide rispetto alla moltiplicazione e valgono le due proprietà distributive, destra e sinistra, della moltiplicazione rispetto all'addizione.

Se la moltiplicazione $\cdot$ è commutativa l'anello si dice *commutativo*. $(\mathbf{Z},+,\cdot,1)$ è un esempio di anello commutativo. Altri anelli commutativi sono $(\mathbf{Q},+,\cdot,1)$ ed $(\mathbf{R},+,\cdot,1)$. Vediamo altri esempi di anelli.

ESEMPI 1.1.

1.1.A. *Anelli di funzioni.* Siano X un insieme ed $(A,+,\cdot,1_A)$ un anello. Nell'insieme A^X costituito dalle funzioni da X ad A definiamo le seguenti operazioni, dette operazioni *punto per punto*:

$$\forall f,g \in A^X, \forall x \in X, \begin{cases} (f+g)(x) = f(x)+g(x) \\ (f\cdot g)(x) = f(x)\cdot g(x) \\ (-f)(x) = -f(x) \end{cases}.$$

Consideriamo inoltre le due funzioni costanti **0** ed **1** tali che $\forall x \in X$, $\mathbf{0} : x \mapsto 0_A$ ed $\mathbf{1} : x \mapsto 1_A$. Si prova facilmente che con queste operazioni A^X è un anello in cui **0** è l'elemento neutro di + e **1** quello di $\cdot$. Se l'anello A è commutativo lo è anche l'anello delle funzioni. Di questo tipo sono gli anelli di funzioni studiate in Analisi Matematica, in cui X è un sottoinsieme non vuoto di **R** ed A = **R**.

1.1.B. - *Anelli di successioni.* Sia A un anello commutativo. Consideriamo l'insieme $A^{\mathbf{N}}$ delle *successioni*, cioè delle funzioni da **N** ad A. Oltre all'anello costruito come nell'esempio precedente, sullo stesso gruppo additivo definiamo la seguente moltiplicazione (detta *convoluzione*):

$$f * g : n \mapsto \sum_{j=0}^{n} f(n-j) \cdot g(j).$$

Questa operazione è associativa. Infatti, siano $f,g,h \in A^{\mathbf{N}}$. Per ogni $n \in \mathbf{N}$ si ha:

$$f * \big(g * h\big)\big(n\big) = \sum_{j=0}^{n} f\big(n-j\big) \cdot \big(g * h\big)\big(j\big) = \sum_{j=0}^{n} f\big(n-j\big) \cdot \underbrace{\sum_{i=0}^{j} g\big(j-i\big) \cdot h\big(i\big)}_{\text{prop. distributiva}} =$$

$$= \sum_{j=0}^{n} \sum_{i=0}^{j} f\big(n-j\big) \cdot g\big(j-i\big) \cdot h\big(i\big) = \sum_{i=0}^{n} \sum_{j=i}^{n} f\big(n-j\big) \cdot g\big(j-i\big) \cdot h\big(i\big)$$

Questo perché in ogni caso si ha $0 \le i \le j \le n$. Ora poniamo $k = j - i$. Allora, $n - j = \big(n-i\big) - k$, quindi sostituiamo ed otteniamo:

$$\sum_{i=0}^{n} \sum_{j=i}^{n} f(n-j) \cdot g(j-i) \cdot h(i) = \sum_{i=0}^{n} \left(\sum_{k=0}^{n-i} f(n-i-k) \cdot g(k) \right) \cdot h(i) = \sum_{i=0}^{n} f * g(n-i) \cdot h(i) = (f * g) * h(i)$$

L' elemento neutro è la funzione 1 tale che

$$1 : n \mapsto \begin{cases} 1_A & \text{se } n = 0 \\ 0_A & \text{se } n > 0 \end{cases}.$$

Indichiamo poi con + l'addizione punto per punto: allora $\left(A^{\mathbf{N}}, +, *, 1\right)$ è un anello ed è commutativo. La proprietà commutativa è immediata:

$$\big(f * g\big)\big(n\big) = \sum_{j=0}^{n} f\big(n-j\big) \cdot g\big(j\big) = \underbrace{\sum_{\lambda=0}^{n} f\big(\lambda\big) \cdot g\big(n-\lambda\big)}_{\text{posto } \lambda = n-k} = \big(g * f\big)\big(n\big)$$

Circa la proprietà distributiva della convoluzione rispetto alla addizione si ha:

$$f * (g+h)(n) = \sum_{j=0}^{n} f(n-j)\cdot(g+h)(j) = \sum_{j=0}^{n} f(n-j)\cdot\big(g(j)+h(j)\big) =$$

$$= \sum_{j=0}^{n}\big(f(n-j)\cdot g(j) + f(n-j)\cdot h(j)\big) = \sum_{j=0}^{n} f(n-j)\cdot g(j) + \sum_{j=0}^{n} f(n-j)\cdot h(j) = (f*g + f*h)(n)$$

e la commutatività rende superfluo verificare la distributività a sinistra.

Per esempio, sia A = **R**. La tabella mostra un po' di valori di due successioni f, g insieme con quelli di di f+g ed f∗g. Si ha: $f(n) = n^2$, $g(n) = 2n+1$, $(f+g)(n) = n^2 + 2n + 1 = (n+1)^2$, mentre $f * g(n) = \dfrac{n^4 + 2n^3 + 2n^2 + n}{6}$

n	0	1	2	3	4	5	6	7	8	9	10
f	0	1	4	9	16	25	36	49	64	81	100
g	1	3	5	7	9	11	13	15	17	19	21
f+g	1	4	9	16	25	36	49	64	81	100	121
f∗g	0	1	7	26	70	155	301	532	876	1365	2035

1.1.C. - *Gli anelli* $\boldsymbol{Z_m}$. Sia $m \in \mathbf{N}$, $m > 0$. Ricordiamo che, in **Z**, con mod(x,m) abbiamo denotato il resto della divisione di x per m.

Nell'insieme $\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$ abbiamo posto $x +_m y = \mathrm{mod}(x+y, m)$, ottenendo un gruppo ciclico. In questo insieme definiamo anche la seguente moltiplicazione: $x \cdot_m y = \mathrm{mod}(x\cdot y, m)$. Come vedremo più oltre, con un'opportuna rielaborazione del quoziente **Z**/m**Z**, si ha che questa moltiplicazione è associativa, commutativa e distributiva rispetto al +.

L'elemento neutro di $+_m$ è 0, quello di $\cdot_m$ è 1; l'opposto di x è m-x. Si può dimostrare che $(\mathbf{Z}_m, +_m, \cdot_m, 1)$ è un anello commutativo. Nel seguito, per comodità, le operazioni in quest'anello saranno denotate spesso con i simboli usuali + e · come in **Z**. Vediamo qui le tavole di addizione e moltiplicazione di $\mathbf{Z}_7$. Si nota subito che ogni elemento diverso da 0 è invertibile e che quindi si ha $\mathbf{Z}_7^* = \mathbf{Z}_7 \setminus \{0\}$. Si tratta di una proprietà che si ritrova nell'anello razionale **Q** ma non in **Z**.

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\cdot_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

PROPOSIZIONE 1.2. Sia $\left(A,+,\cdot,1_A\right)$ un anello. Allora:

a) per ogni $x\in A$, $x\cdot 0_A = 0_A\cdot x = 0_A$

b) Se $0_A = 1_A$, allora $A = \left\{0_A\right\}$ è l'anello *banale.*

c) L'insieme $A^* = \left\{x\in A \,\middle|\, \exists x^{-1}\in A\right\}$ è un gruppo rispetto alla moltiplicazione (detto *gruppo delle unità* dell'anello A).

d) Ogni $a\in A$ determina due endomorfismi del gruppo $\left(A,+\right)$, rispettivamente $\sigma_a : A\to A,\ \sigma_a\left(x\right) = a\cdot x,\quad \delta_a : A\to A,\ \delta_a\left(x\right) = x\cdot a$. Se $a\in A^*$ sono entrambi automorfismi.

Dimostrazione. a) $\forall x\in A,\ x\cdot 0_A = x\cdot\left(0_A+0_A\right) = x\cdot 0_A + x\cdot 0_A \Rightarrow x\cdot 0_A = 0_A$.

Analogamente si prova che $0_A\cdot x = 0_A$.

b) Se $0_A = 1_A$, allora $\forall x\in A,\ x = x\cdot 1_A = x\cdot 0_A = 0_A$.

c) Si ha $1_A{}^{-1} = 1_A \Rightarrow 1_A\in A^*$. Per ogni $a,b\in A^*, \left(a\cdot b\right)^{-1} = b^{-1}\cdot a^{-1}\Rightarrow a\cdot b\in A^*$.

Infine, per ogni $a\in A^*$ si ha: $\left(a^{-1}\right)^{-1} = a\Rightarrow a^{-1}\in A^*$. Poiché la moltiplicazione è associativa, allora abbiamo dimostrato che $\left(A^*,\cdot\right)$ è un gruppo.

d) Per la proprietà distributiva di $\cdot$ rispetto a $+$, per ogni $x,y\in A$ si ha:

$$\sigma_a\left(x+y\right) = a\cdot\left(x+y\right) = a\cdot x + a\cdot y = \sigma_a\left(x\right)+\sigma_a\left(y\right)$$

quindi σ_a è un endomorfismo di (A, +). Allo stesso modo si dimostra che lo è anche δ_a. Sia ora $a\in A^*$, allora esiste a^{-1} e si ha:

$$\forall x\in A,\ \sigma_{a^{-1}}\circ\sigma_a\left(x\right) = \sigma_{a^{-1}}\left(a\cdot x\right) = a^{-1}\cdot\left(a\cdot x\right) = \left(a^{-1}\cdot a\right)\cdot x = 1_A\cdot x = x,$$

quindi $\sigma_{a^{-1}}\circ\sigma_a = \mathrm{id}_A$. Analogamente, $\sigma_a\circ\sigma_{a^{-1}} = \mathrm{id}_A$ e dunque σ_a è invertibile e di conseguenza è un automorfismo di (A, +).

Un anello si dice *integro* se vale la *legge di annullamento del prodotto*:

$$x \cdot y = 0_A \Rightarrow x = 0_A \text{ oppure } y = 0_A.$$

Per esempio, $(\mathbf{Z}, +, \cdot, 1)$ è integro, mentre $(\mathbf{Z}_6, +, \cdot, 1)$ non lo è, in quanto $3 \cdot_6 2 = \text{mod}(3 \cdot 2, 6) = 0$. Un *dominio d'integrità* è un anello commutativo integro.

Circa il gruppo delle unità di un anello $(A, +, \cdot, 1_A)$, nel caso di $\mathbf{Z}$ gli elementi unitari sono 1 e -1. Nel caso di $\mathbf{Q}$ e di $\mathbf{Z}_7$, gli elementi unitari sono tutti gli elementi non nulli. Quando ciò accade in un anello commutativo, l'anello prende il nome di *campo*. Sono quindi campi $\mathbf{Q}$, $\mathbf{R}$ e $\mathbf{Z}_7$. Vediamo altri esempi.

ESEMPI 1.3.

1.3.A. - Sia dato l'anello $\mathbf{Z}_m$, $m > 1$. Un elemento $a \in \mathbf{Z}_m$ è invertibile se e solo se $MCD(a,m) = 1$. Infatti, $MCD(a,m) = 1 \Leftrightarrow \exists u,v \in \mathbf{Z}$ tali che $au+mv = 1$. Dividiamo u per m, ottenendo $u = mq+r$, con $0 < r < m$, quindi

$$1 = au+mv = ar+(aq+v)m \Rightarrow 1 = \text{mod}(ar,m) = a \cdot_m r$$

ed a è invertibile ed ha r per inverso.

Inversamente, se a ha per inverso r si ha: $1 = a \cdot_m r = \text{mod}(ar,m)$, ossia esiste q tale che $ar+mq = 1$ e ciò implica $MCD(a,m) = 1$.

Pertanto, $\mathbf{Z}_m^* = \{a \in \mathbf{Z}_m \mid MCD(a,m) = 1\}$ ha $\varphi(m)$ elementi, dove φ è la funzione di Eulero. Ne segue che $\mathbf{Z}_m$ è un campo $\Leftrightarrow$ $\mathbf{Z}_m^* = \mathbf{Z}_m \setminus \{0\}$ $\Leftrightarrow$ $\varphi(m) = m-1$ $\Leftrightarrow$ m è primo.

Si osservi che se m è composto, ossia $m = pq$, con p, q minori di m, si ha $p \cdot_m q = \text{mod}(pq,m) = \text{mod}(m,m) = 0$, quindi $\mathbf{Z}_m$ non è un dominio d'integrità.

1.3.B. - *Ampliamento quadratico di un campo.* Sia K un campo. Prendiamo un elemento $u \in K$ che non sia il quadrato di altri elementi di K e consideriamo l'insieme $F = \left\{ \begin{bmatrix} a & b \cdot u \\ b & a \end{bmatrix} \mid a,b \in K \right\}$. Rispetto alle usuali operazioni con le matrici, si vede facilmente che F è un anello con unità e commutativo. Di più, poiché il determinante è $\Delta = a^2 - u \cdot b^2$ ed u non è un quadrato in K, allora solo la matrice

nulla è non invertibile. Escluso questo caso, si ha $\begin{bmatrix} a & b\cdot u \\ b & a \end{bmatrix}^{-1} = \frac{1}{\Delta}\begin{bmatrix} a & -bu \\ -b & a \end{bmatrix} \in F$. Pertanto, F è un campo. Si noti che il sottoinsieme delle matrici "scalari" $\left\{\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in K\right\}$ forma a sua volta un campo, "identificabile" con K. Identifichiamo cioè l'elemento $a \in K$ con la matrice $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$. Posto $i = \begin{bmatrix} 0 & u \\ 1 & 0 \end{bmatrix}$, si ha $i^2 = \begin{bmatrix} u & 0 \\ 0 & u \end{bmatrix} \equiv u$, quindi nel campo F l'elemento u è ora un quadrato. Infine, si ha: $\begin{bmatrix} a & b\cdot u \\ b & a \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} + \begin{bmatrix} 0 & u \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}$, che possiamo riscrivere come a+ib.

Con questa costruzione, a partire dal campo $\mathbf{Z}_3$, in cui 2 non è un quadrato, possiamo costruire un campo di ordine 9. A partire dal campo reale **R**, posto $u = -1$, si ottiene un campo che nel seguito chiameremo *campo complesso* **C**.

PROPOSIZIONE 1.4. a) Ogni campo $(K, +, \cdot, 1_K)$ è un dominio d'integrità

b) Ogni dominio d'integrità finito $(A, +, \cdot, 1_A)$ è un campo.

Dimostrazione. a) Siano a, b∈K, tali che $a \cdot b = 0_K$. Se $a = 0_K$ siamo a posto. Altrimenti, esiste l'inverso a^{-1} di a, perciò:

$$a \cdot b = 0_K \Rightarrow \underbrace{a^{-1} \cdot (a \cdot b)}_{=(a^{-1}\cdot a)\cdot b = b} = \underbrace{a^{-1} \cdot 0_K}_{=0_K} \Rightarrow b = 0_K$$

b) Sia a∈A, $a \neq 0_A$. Consideriamo la funzione $\sigma_a : A \to A$, $\sigma_a(x) = a \cdot x$. Per ogni x, y si ha $\sigma_a(x) = \sigma_a(y) \Rightarrow a \cdot x = a \cdot y \Rightarrow a \cdot (x - y) = 0_A$, e poiché $a \neq 0_A$ ed A è un dominio d'integrità, allora $x - y = 0_A \Rightarrow x = y$. Dunque, $\sigma_a : A \xrightarrow{1\text{–}1} A$. Ma A è finito, quindi ogni funzione iniettiva da A a se stesso è anche suriettiva. Quindi, in particolare, $1_A \in \mathrm{Im}(\sigma_a)$. Esiste cioè un elemento $\bar{x}$ tale che $a \cdot \bar{x} = \sigma_a(\bar{x}) = 1_A$, ossia a è invertibile. Dunque, $A^* = A \setminus \{0_A\}$ ed A è un campo.

In un anello $(A, +, \cdot, 1_A)$ il periodo di 1_A nel gruppo additivo (A, +) si chiama *caratteristica* di A. Per esempio **Z** ha caratteristica infinita (e però si usa

dire che ha caratteristica *zero*), mentre $\mathbf{Z}_m$ e l'anello $\mathbf{Z}_m{}^X$ delle funzioni da un insieme qualunque $X \neq \emptyset$ a $\mathbf{Z}_m$ hanno caratteristica m. Vediamo ora il caso dei dominii d'integrità e dei campi.

TEOREMA 1.5. Sia A un anello.

a) Se la caratteristica di A è finita, ogni elemento ha nel gruppo additivo il periodo divisore della caratteristica.

b) Se A è un dominio d'integrità, ogni elemento non nullo ha nel gruppo additivo il periodo uguale alla caratteristica.

c) Se l'anello A è un dominio d'integrità allora la caratteristica o è zero oppure è un numero primo p.

d) Se A è un dominio d'integrità di caratteristica p, allora (A, +) è un p-gruppo abeliano elementare.

Dimostrazione. a) Per ogni $a \in A$ e per ogni $n \in \mathbf{N}$, si ha

$$na = \underbrace{a + a + \ldots a}_{n} = \underbrace{1_A \cdot a + 1_A \cdot a + \ldots 1_A \cdot a}_{n} = \underbrace{\left(1_A + \ldots + 1_A\right)}_{n} \cdot a = \left(n1_A\right) \cdot a .$$

Dunque se n è il periodo di 1_A allora $n1_A = 0_A \Rightarrow na = 0_A \Rightarrow$ n multiplo di $|a|$.

b) Se $a \neq 0_A$, essendo A un dominio d'integrità si ha $0_A = na = \left(n1_A\right) \cdot a \Leftrightarrow n1_A = 0_A$, quindi a ed 1_A hanno lo stesso periodo.

c) Sia n la caratteristica di A, e sia $n \neq 0$. Sia n non primo, $n = rs$, con r ed s divisori propri di n. Allora, per la proprietà distributiva, si ha:

$$0_A = n1_A = rs1_A = \underbrace{1_A + \ldots + 1_A}_{rs} = \underbrace{\left(1_A + \ldots + 1_A\right)}_{r} \cdot \underbrace{\left(1_A + \ldots + 1_A\right)}_{s} = r1_A \cdot s1_A$$

ed essendo A un dominio d'integrità, si ha $r1_A = 0_A$ oppure $s1_A = 0_A$, contro la minimalità di n come periodo di 1_A. Pertanto, n è primo.

d) Segue da b) e da c).

Dato un anello $\left(A, +, \cdot, 1_A\right)$, un *sottoanello* è costituito da un sottoinsieme B chiuso rispetto alla somma, allo zero, agli opposti, al prodotto ed all'unità di A, ed è a sua volta un anello. In particolare, (B, +) è un sottogruppo di (A, +) e $\left(B, \cdot, 1_A\right)$ è un *sottomonoide* di $\left(A, \cdot, 1_A\right)$. Ne segue che anche per i sottoanelli vale

il teorema di Lagrange, ossia nel caso finito l'ordine di un sottoanello è un divisore dell'ordine delll'anello.

Come nel caso dei sottogruppi, anche l'intersezione di una famiglia di sottoanelli è un sottoanello. Il *sottoanello generato da un sottoinsieme* è l'intersezione di tutti i sottoanelli che lo contengono. L'intersezione di tutti i sottoanelli prende il nome di *sottoanello fondamentale* dell'anello. Per caratterizzarlo, dato un anello A ed un elemento a∈A, denotiamo nel seguito con **Z**a l'insieme dei suoi multipli interi, ossia il sottogruppo di (A, +) generato da a.

PROPOSIZIONE 1.6. Sia A un anello. Allora il sottoanello fondamentale coincide col sottogruppo $\mathbf{Z}1_A$.

Dimostrazione. Basta dimostrare che $\mathbf{Z}1_A$ è chiuso rispetto alla moltiplicazione. Siano $m1_A$, $n1_A$ due multipli di 1_A. Se uno dei due è nullo, è ovvio.

Siano m, n positivi, allora per la proprietà distributiva si ha:

$$m1_A \cdot n1_A = \underbrace{(1_A + \ldots + 1_A)}_{m} \cdot \underbrace{(1_A + \ldots + 1_A)}_{n} = \underbrace{1_A \cdot 1_A + \ldots + 1_A \cdot 1_A}_{mn} = mn1_A$$

Inoltre, essendo (-m) 1_A = -(m1_A) e, per ogni a, b∈A, $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$, allora l'uguaglianza $m1_A \cdot n1_A = (mn)1_A$ vale anche per m, n interi.

Siano dati due anelli A e B. Sul prodotto diretto $(A \times B, +)$ dei loro gruppi additivi definiamo la seguente moltiplicazione: per ogni $a_1, a_2 \in A$, $b_1, b_2 \in B$,

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2).$$

La moltiplicazione appena definita è distributiva rispetto al +, è associativa ed ha elemento neutro $1_{A\times B} = (1_A, 1_B)$. La struttura $(A \times B, +, \cdot, 1_{A\times B})$ è quindi un anello, detto *prodotto diretto esterno* dei due anelli dati. Se i due anelli sono commutativi, anche il prodotto diretto lo è, e viceversa. Le dimostrazioni sono lasciate per esercizio.

ESEMPI 1.7.

1.7.A. - Il prodotto diretto di due anelli non banali A e B non è mai un dominio d'integrità. Infatti, $(1_A, 0_B) \neq (0_A, 0_B) \neq (0_A, 1_B)$, ma $(1_A, 0_B) \cdot (0_A, 1_B) = (0_A, 0_B) = 0_{A\times B}$

In particolare, il prodotto diretto di due campi non è un campo.

1.7.B. - Mediante gli anelli $\mathbf{Z}_m$ si possono costruire anelli finiti come loro prodotti diretti. La caratteristica di $\mathbf{Z}_m \times \mathbf{Z}_n$ è mcm(m,n), dato che è il periodo dell'unità nel gruppo additivo, che sappiamo essere il prodotto diretto dei due gruppi ciclici additivi di $\mathbf{Z}_m$ e $\mathbf{Z}_n$ (si veda il § 1 degli appunti sui gruppi).

Per esempio, vediamo l'anello $\mathbf{Z}_2 \times \mathbf{Z}_2$. Ha 4 elementi, ha caratteristica 2 e la moltiplicazione ha l'idempotenza, ossia ogni elemento è il quadrato di se stesso. Un simile anello è detto *booleano.*

+	(0,0)	(1,1)	(1,0)	(0,1)
(0,0)	(0,0)	(1,1)	(1,0)	(0,1)
(1,1)	(1,1)	(0,0)	(0,1)	(1,0)
(1,0)	(1,0)	(0,1)	(0,0)	(1,1)
(0,1)	(0,1)	(1,0)	(1,1)	(0,0)

·	(0,0)	(1,1)	(1,0)	(0,1)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(1,1)	(0,0)	(1,1)	(1,0)	(1,0)
(1,0)	(0,0)	(1,0)	(1,0)	(0,0)
(0,1)	(0,0)	(0,1)	(0,0)	(0,1)

OSSERVAZIONE 1.8. Nei gruppi si dimostra che se G = H×K allora i due sottoinsiemi $\overline{H} = \{(h,1_K) \mid h \in H\}$ e $\overline{K} = \{(1_H,k) \mid k \in K\}$ sono sottogruppi isomorfi ad H e K rispettivamente (ricordiamo che in notazione additiva si ha $\overline{H} = \{(h,0_K) \mid h \in H\}$, $\overline{K} = \{(0_H,k) \mid k \in K\}$).

Nel prodotto diretto di due anelli A e B, i due sottoinsiemi $\overline{A} = \{(a,0_B) \mid a \in A\}$, $\overline{B} = \{(0_A,k) \mid b \in B\}$ sono quindi sottogruppi di $(A \times B,+)$, sono chiusi rispetto alla moltiplicazione di A×B, sono anelli perché hanno anche l'unità, rispettivamente $(1_A,0_B)$ e $(0_A,1_B)$, ma non sono sottoanelli di A×B, perché non contengono l'unità $(1_A,1_B)$ di A×B.

Sia dato un campo F. Un *sottocampo* è un sottoanello che contiene gli inversi dei propri elementi non nulli. L'intersezione di sottocampi è un sottocampo a sua volta, e la dimostrazione è lasciata per esercizio. L'intersezione di tutti i sottocampi è un campo, detto *sottocampo primo* di F. Poiché i campi sono particolari anelli, il sottocampo primo deve contenere il sottoanello fondamentale di K. Se quest'ultimo è un campo, allora coincide col sottocampo primo, altrimenti è più piccolo. Se X è un sottoinsieme di K, il *sottocampo generato da* X è l'intersezione di tutti i sottocampi che lo contengono. Il sottocampo primo è generato da $X = \{1_K\}$.

Nel caso del campo razionale **Q**, non ci sono sottocampi propri, perciò il sottocampo primo di **Q** è **Q** stesso, mentre il suo sottoanello fondamentale è **Z**. Poiché **Q** è un campo incluso in **R**, anche per **R** il sottocampo primo è **Q** ed il sottoanello fondamentale è **Z**.

§ 2 – IDEALI, OMOMORFISMI E CONGRUENZE

Riprendiamo il caso dell'anello **Z** degli interi. Non ha sottoanelli propri, in quanto 1 genera tutto **Z**. E i numeri pari allora che cosa costituiscono? Formano il sottogruppo 2**Z** di (**Z**, +), ed il prodotto di numeri pari è pari. Ma, in più, hanno la proprietà di assorbire il prodotto: se in un prodotto c'è un numero pari, il prodotto è pari. Questa proprietà dell'insieme 2**Z** è analoga a quella dello zero di assorbire il prodotto. Ma anche m**Z** ha la stessa proprietà: è un sottogruppo rispetto a + e se in un prodotto c'è un multiplo di m, il prodotto è multiplo di m a sua volta. Simili sottogruppi del gruppo additivo sono detti ideali dell'anello. Più precisamente:

Sia $(A,+,\cdot,1_A)$ un anello. Un suo sottoinsieme I prende il nome di *ideale* (bilatero) se è un sottogruppo del gruppo additivo ed inoltre, per ogni $i\in I$, per ogni $a\in A$ i prodotti $a\cdot i$ ed $i\cdot a$ appartengono ad I.

Ogni anello A ha come ideali almeno $\{0_A\}$ e se stesso. Tali ideali sono detti rispettivamente *ideale nullo* e *improprio*, e talora sono detti *ideali banali*.

Come al solito, si dimostra facilmente che l'intersezione di una famiglia $\Im$ di ideali è sempre un ideale. Di conseguenza, ogni sottoinsieme X di A genera un ideale, come intersezione della famiglia di ideali che contengono X. Lo denoteremo con (X), riservando la scrittura $\langle X\rangle$ al sottoanello generato da X.

Un ideale di A si dice *principale* se è generato da un solo elemento. Chiaramente, $\{0_A\}=(0_A)$ è principale, ma anche A lo è; infatti per ogni $a\in A$ si ha $a=a\cdot 1_A\in(1_A)\Rightarrow A=(1_A)$. Vediamo numerosi esempi, ma prima alcune proprietà.

PROPOSIZIONE 2.1. Sia A un anello.

a) Se un ideale I di A contiene un elemento invertibile, allora I = A

b) Se A è un campo, allora i soli ideali di A sono $\{0_A\}$ ed A.

Dimostrazione. a) Sia I un ideale e sia $u\in I$, invertibile, allora $1_A=u^{-1}\cdot \underset{\in I}{\underbrace{u}}\in I$, quindi per ogni $a\in A$, $a=a\cdot 1_A\in I\Rightarrow A\subseteq I$, ossia I = A.

b) Se I non è l'ideale banale, allora contiene un elemento non nullo, quindi invertibile, ed allora per a) si ha I = A.

PROPOSIZIONE 2.2. Sia A un anello commutativo.

a) Per ogni a∈A si ha $(a)=\{a\cdot x \mid x\in A\}$

b) A è un campo se e solo se gli unici ideali di A sono $\{0_A\}$ ed A.

Dimostrazione. a) Si tratta di dimostrare che l'insieme $I=\{a\cdot x \mid x\in A\}$ coincide con l'ideale (a) generato da a, ossia che vale la doppia inclusione. L'inclusione $I\subseteq(a)$ è immediata, perché $a\in(a)\Rightarrow \forall x\in A,\ a\cdot x\in(a)$ per definizione di ideale. L'altra inclusione si dimostra in maniera indiretta: poiché (a) è l'intersezione della famiglia $\Im$ degli ideali che contengono a, se dimostriamo che I è un ideale che contiene a, ossia che I∈$\Im$, automaticamente I conterrà (a). Ora, I contiene a perché $a=a\cdot 1_A$. Inoltre, poiché la funzione $\sigma_a : A\to A,\ \sigma_a(x)=a\cdot x$, è un endomorfismo del gruppo additivo (A, +) avente I per immagine, allora per il teorema fondamentale di omomorfismo per i gruppi, I è un sottogruppo di (A, +) (ma si può anche verificare direttamente, per esercizio provando che I è chiuso rispetto al + e contiene lo zero e gli opposti dei suoi elementi). Infine, tenendo presente che A è commutativo, per ogni y∈a, per ogni i = a·x∈I si ha:

$$y\cdot i = i\cdot y = (a\cdot x)\cdot y = a\cdot(x\cdot y) \in I$$

e quindi I è un ideale contenente a. Dunque, per quanto detto, $(a)\subseteq I$ ed allora, valendo la doppia inclusione, si ha $(a)=I$.

b) Abbiamo già visto che un campo ha solo gli ideali banali. Inversamente, sia A un anello commutativo nel quale i soli ideali siano quelli banali. Sia a un qualunque elemento non nullo, allora l'ideale $(a)=\{a\cdot x \mid x\in A\}$ non è l'ideale nullo, perciò coincide con tutto A. Ne segue che $1_A\in(a)$, quindi esiste $\bar{x}\in A$ tale che $a\cdot\bar{x}=1_A$. Ma allora a è invertibile, quindi A è un campo.

ESEMPI 2.3.

2.3.A. – Troviamo gli ideali dell'anello **Z**. Innanzi tutto, poiché sono sottogruppi di (**Z**,+) devono essere della forma m**Z**. Basta provare che questi sono tutti ideali. Ma questo è immediato: per ogni x∈**Z**, per ogni mk∈m**Z** si ha x(mk) = m(kx)∈m**Z**. Perciò tutti i sottogruppi di (**Z**,+) sono ideali dell'anello.

2.3.B. – Abbiamo visto che nel prodotto diretto di due anelli A e B, i due sottoinsiemi $\overline{A} = \{(a, 0_B) \mid a \in A\}$, $\overline{B} = \{(0_A, k) \mid b \in B\}$ sono sottogruppi di $(A \times B, +)$, sono chiusi rispetto alla moltiplicazione di A×B, ma non sono sottoanelli di A×B, perché non contengono l'unità $(1_A, 1_B)$ di A×B. Sono invece ideali. Infatti, per ogni $(x, y) \in A \times B$, per ogni $(a, 0_B) \in \overline{A}$ si ha $\begin{cases} (x, y) \cdot (a, 0_B) = (x \cdot a, 0_B) \in \overline{A} \\ (a, 0_B) \cdot (x, y) = (a \cdot x, 0_B) \in \overline{A} \end{cases}$, quindi $\overline{A}$ è un ideale. Analogamente, lo è $\overline{B}$.

C'è un'analogia tra ideali di un anello e sottogruppi normali di un gruppo, ed è costituita dalle congruenze. Una congruenza ~ di un anello A è una congruenza del gruppo additivo (A, +) compatibile anche con la moltiplicazione: per ogni a, b, a', b'∈A, dall'essere a~a', b~b' segue a·b~a'·b'.

Nel gruppo quoziente (A/~,+) costituito dalle classi di equivalenza definiamo anche la seguente moltiplicazione: per ogni a,b∈A,

$$[a]_{\sim} \cdot [b]_{\sim} = [a \cdot b]_{\sim} .$$

Essa risulta associativa, distributiva rispetto al + ed ha per elemento neutro la classe $[1_A]_{\sim}$. Otteniamo così un nuovo anello $(A/\sim, +, \cdot, [1_A]_{\sim})$, l'*anello quoziente* di A rispetto alla congruenza ~.

Se l'anello A è commutativo, lo è anche il quoziente. Inoltre, se a∈A ha inverso a^{-1} allora la classe $[a]_{\sim}$ ha per simmetrica la classe $[a^{-1}]_{\sim}$.

PROPOSIZIONE 2.4. Sia dato un anello $(A, +, \cdot, 1_A)$

a) Sia I un ideale. La relazione $x \sim_I y \Leftrightarrow x-y \in I$ è una congruenza in A, nella quale $[0_A]_{\sim} = I$ e le altre classi sono i suoi laterali.

b) Data una congruenza ~ in A, posto $I = [0_A]_{\sim}$, I è un ideale e si ha $\sim = \sim_I$.

Dimostrazione. a) Poiché (A,+) è abeliano, allora (I,+) è un sottogruppo normale e la relazione $\sim_I$ è una congruenza rispetto al +. Proviamone la compatibilità con

la moltiplicazione. Siano $a \sim_I a'$, $b \sim_I b'$, ossia esistono $i, j \in I$ tali che $\begin{cases} a' = a + i \\ b' = b + j \end{cases}$,

allora $a' \cdot b' = (a+i)\cdot(b+j) = a \cdot b + \overbrace{\left(\underbrace{a \cdot j}_{\in I} + \underbrace{i \cdot b}_{\in I} + \underbrace{i \cdot j}_{\in I} \right)}^{\in I} \Rightarrow a' \cdot b' \sim_I a \cdot b$.

b) Inversamente, sia $\sim$ una congruenza e sia $I = [0_A]_\sim$. Allora I è un sottogruppo di (A,+) e le altre classi sono i suoi laterali I+a, ossia $\sim = \sim_I$. Resta da dimostrare che I è un ideale. $\forall a \in A, \forall i \in I, \begin{cases} a \sim a \\ i \sim 0_A \end{cases} \Rightarrow a \cdot i \sim a \cdot 0_A = 0_A \Rightarrow a \cdot i \in I$.

Analogamente si prova che $i \cdot a \in I$. Quindi, I è un ideale di A.

Pertanto, le congruenze negli anelli sono completamente descritte dagli ideali. L'anello quoziente di A rispetto alla congruenza associata all'ideale I si denota con A/I .

ESEMPIO 2.5. Le congruenze dell'anello $\mathbf{Z}$ sono dunque tutte e sole quelle associate agli ideali $m\mathbf{Z}$, perciò sono le congruenze mod m, $m \geq 0$. Gli anelli quoziente sono dunque gli $\mathbf{Z}/m\mathbf{Z}$. La moltiplicazione quoziente associa a due classi $[r]_m, [s]_m$ la classe $[rs]_m$, rappresentata canonicamente dal resto della divisione di rs per m, ossia da $r \cdot_m s = \mathrm{mod}(rs, m)$. Allora in definitiva anche i gruppi $(\mathbf{Z}_m, +)$ sono davvero anelli rispetto alla moltiplicazione $\cdot_m$, come affermato in 1.1.C.

Si osservi che anche se un anello è integro, non è detto che un suo anello quoziente lo sia. Per esempio, l'anello $\mathbf{Z}$ è integro ma, se m non è primo, $\mathbf{Z}_m$ non lo è. Per altro, se m è primo, è ben noto che $\mathbf{Z}_m$ è addirittura un campo.

Una struttura algebrica si dice *semplice* se le sole congruenze che possiede sono quelle banali, ossia l'identità, nella quale ogni elemento è in relazione solo con se stesso, ed il prodotto cartesiano, nel quale ogni elemento è in relazione con ogni altro. Come già detto per i gruppi, la determinazione delle strutture semplici è solitamente un problema assai complesso e di grande importanza.

Nel caso dei un anello A, l'essere semplice equivale a non possedere altri ideali all'infuori di $\{0_A\}$ e A stesso. Abbiamo dimostrato che i soli anelli commutativi semplici sono i campi. Altri esempi sono gli anelli di matrici quadrate d'ordine n ad elementi in un campo.

Date due strutture algebriche $(X,*)$ e $(Y,\cdot)$, si chiama *omomorfismo* una funzione $f : X \to Y$ tale che per ogni coppia a, b di elementi di X sia $f(a * b) = f(a) \cdot f(b)$.

Se le operazioni sono più di una, come nel caso degli anelli, occorre che la funzione f sia omomorfismo rispetto a tutte le operazioni. Le operazioni da considerare, però, non sono solo il + ed il ·, ma anche gli elementi neutri, gli opposti, ecc. Nel caso dei gruppi una funzione che sia omomorfismo rispetto all'operazione binaria lo è automaticamente rispetto all'elemento neutro e agli opposti, come visto nel capitolo dei gruppi. Nel caso dei monoidi, invece, un omomorfismo rispetto all'operazione binaria non porta necessariamente l'elemento neutro del dominio nell'elemento neutro del codominio. Un omomorfismo tra due monoidi $(M,\cdot,1_M)$ ed $(H,*,1_H)$ è di conseguenza una funzione $f : M \to H$ tale che $\begin{cases} \forall x,y \in M, f(x \cdot y) = f(x) * f(y) \\ f(1_M) = 1_H \end{cases}$.

Un anello è la sovrapposizione del gruppo additivo e del monoide moltiplicativo, pertanto un *omomorfismo* f:A→B tra gli anelli A e B deve soddisfare le condizioni sui gruppi e sui monoidi:

$$\begin{cases} \forall x,y \in A, \begin{cases} f(x+y) = f(x) + f(y) \\ f(x \cdot y) = f(x) \cdot f(y) \end{cases} \\ f(1_A) = 1_B \end{cases}$$

Così come per i gruppi, un omomorfismo biiettivo si chiama *isomorfismo*. In tal caso, anche l'inversa f^{-1} di f è un isomorfismo e i due anelli differiscono solo per il nome degli oggetti ed i simboli usati per descriverli, ma sono essenzialmente coincidenti.

Un omomorfismo suriettivo si chiama *epimorfismo* e in tal caso si dice che B è *immagine omomorfa* di A. Un omomorfismo iniettivo si chiama *monomorfismo* o immersione di A in B, e B si chiama *estensione* di A.

ESEMPI 2.6.

2.6.A. – Sia A un anello. Sia f:**Z**→A un omomorfismo. Allora $f(1) = 1_A$, quindi per ogni n∈**Z** si ha $f(n) = n1_A$. Questo è anche omomorfismo di anelli, perché per

ogni $m,n \in \mathbf{Z}$ si ha $f(mn) = \underbrace{(mn)1_A = (m1_A)\cdot(n1_A)}_{\text{prop. distrib.}} = f(m)\cdot f(n)$. Allora questo è il solo omomorfismo tra i due anelli, e la sua immagine è il sottoanello fondamentale di A. Se A ha caratteristica 0 allora im(f) è infinito, quindi f è un monomorfismo, ed il sottoanello fondamentale è isomorfo a **Z**.

2.6.B. - Sia ~ una congruenza nell'anello A e sia $I = [0_A]_\sim$, che sappiamo essere un ideale. Denotiamo con A/I l'anello quoziente. La funzione π:A→A/I, definita da $\pi(x) = [x]_\sim = x + I$, è un epimorfismo, detto *epimorfismo canonico*. Infatti, è un omomorfismo di gruppi, essendo $\pi(x+y) = [x+y]_\sim = [x]_\sim + [y]_\sim = \pi(x) + \pi(y)$, ed inoltre $\pi(x\cdot y) = [x\cdot y]_\sim = [x]_\sim \cdot [y]_\sim = \pi(x)\cdot\pi(y)$ e $\pi(1_A) = [1_A]_\sim = 1_{A/I}$.
La suriettività è ovvia.

2.6.C. - Il monoide degli endomorfismi ed il gruppo degli automorfismi. Gli omomorfismi tra un anello e se stesso si chiamano *endomorfismi,* e formano il monoide (End(A), ∘, id_A). Gli isomorfismi tra l'anello A e se stessa si chiamano *automorfismi*, formano il gruppo Aut(A) e viene detto *automorfo* di A. In particolare, mentre Aut(**Z**, +) possiede due elementi: l'identità e la funzione che ad ogni x associa l'opposto –x, invece, Aut(**Z**, +, ·, 1) è costituito solo dall'identità, dato che l'elemento unità 1 deve andare in 1.

2.6.D - Anche il campo reale ha solo l'automorfismo banale. Infatti, se f è un automorfismo del campo **R**, allora f(1) = 1, quindi per ogni $m \in \mathbf{N}$ si ha $f(m) = f\left(\sum_{i=1}^{m} 1\right) = \sum_{i=1}^{m} f(1) = m\cdot 1 = m$.

Ma allora si ha anche f(-m) = -m e, in definitiva, per ogni numero razionale $\frac{m}{n}$ si ha $f\left(\frac{m}{n}\right) = \frac{f(m)}{f(n)} = \frac{m}{n}$ e quindi f induce l'identità sui razionali. Inoltre, $\forall x > 0 \Rightarrow \exists y \in \mathbf{R}$ tale che $x = y^2$, quindi $f(x) = f\left(y^2\right) = \left(f(y)\right)^2 \Rightarrow f(x) > 0$. Pertanto, f conserva l'ordinamento di R. Ne viene che, essendo **Q** *denso in* **R**, allora f è l'identità anche su **R**. Dunque, Aut(**R**) = {id}.

C'è una connessione tra omomorfismi e congruenze, come prova il seguente teorema, detto *teorema fondamentale d'omomorfismo*, nella versione per gli anelli. Chiamiamo *nucleo* Ker f dell'omomorfismo f:A→B l'insieme degli elementi di A che f porta nello zero di B.

TEOREMA 2.7. Siano A e B due anelli ed f un omomorfismo tra di essi. Sia poi $I = \operatorname{Ker} f = \{x \in A \mid f(x) = 0_B\}$ il nucleo di f.

a) l'immagine Im f è un sottoanello di B;

b) I è un ideale di A;

c) A/I è isomorfo ad Im f. (L'isomorfismo è definito da: $F : x + I \mapsto f(x)$).

d) f è un monomorfismo se e solo se $I = \operatorname{Ker} f = \{0_G\}$.

Dimostrazione. a) Innanzi tutto, $0_B = f(0_A) \in \operatorname{Im} f$, $1_B = f(1_A) \in \operatorname{Im} f$. Per ogni $b_1, b_2 \in \operatorname{Im} f$ esistono $a_1, a_2 \in A$ tali che $\begin{cases} f(a_1) = b_1 \\ f(a_2) = b_2 \end{cases}$, allora

$$\begin{cases} b_1 + b_2 = f(a_1) + f(a_2) = f(a_1 + a_2) \in \operatorname{Im} f \\ b_1 \cdot b_2 = f(a_1) \cdot f(a_2) = f(a_1 \cdot a_2) \in \operatorname{Im} f \end{cases}$$

e quindi Im f è un sottoanello di B.

b) Per cominciare, $0_A \in I$ perché $f(0_A) = 0_B$. Per ogni $x_1, x_2 \in I$, $f(x_1 + x_2) = f(x_1) + f(x_2) = 0_B + 0_B = 0_B \Rightarrow x_1 + x_2 \in I$. Inoltre, per ogni y∈A, $f(x_1 \cdot y) = f(x_1) \cdot f(y) = 0_B \cdot f(y) = 0_B \Rightarrow x_1 \cdot y \in I$. Analogamente, $y \cdot x_1 \in I$. Pertanto, I è un ideale.

c) La funzione $F : x + I \mapsto f(x)$ è ben definita, perché per ogni x' tale che x'+I = x+I si ha x' = x+i, i∈I, allora f(x') = f(x+i) = f(x)+f(i) = f(x), perché f(i) è nullo, dunque F(x+I) = F(x'+I). E' anche iniettiva, perché si ha:

$$F(x + I) = F(x' + I) \Leftrightarrow f(x) = f(x') \Leftrightarrow f(x - x') = 0_B \Leftrightarrow x - x' \in I \Leftrightarrow x + I = x' + I$$

Ha per immagine Im f, per come è costruita, ed inoltre è un omomorfismo di anelli. Infatti, per ogni x+I, y+I appartenenti ad A/I si ha:

$$F((x + I) + (y + I)) = F((x + y) + I) = f(x + y) = f(x) + f(y) = F(x + I) + F(y + I),$$

$$F((x + I) \cdot (y + I)) = F((x \cdot y) + I) = f(x \cdot y) = f(x) \cdot f(y) = F(x + I) \cdot F(y + I),$$

$$F(1_A + I) = f(1_A) = 1_B$$

d) f è iniettiva se e solo se per ogni $y \in \mathrm{Im}\, f$ esiste un solo x_0 tale che $f(x_0) = y$, ossia se e solo se, $f^{-1}(y) = \{x \in A \mid f(x) = y\} = x_0 + I = \{x_0\}$, e ciò è possibile se e solo se $I = \{0_A\}$.

Un ideale I di un anello A è detto *massimale* se per ogni ideale J di A tale che $I \subseteq J \subseteq A$ segue $J = I$ oppure $J = A$.

ESEMPIO 2.8. Troviamo gli ideali massimali dell'anello $\mathbf{Z}$. Sappiamo che gli ideali non banali sono tutti della forma $m\mathbf{Z}$, con $m \geq 2$. Un ideale $I = m\mathbf{Z}$ è incluso in un ideale $J = n\mathbf{Z}$ se e solo se $m \in J$, ossia se e solo se m è multiplo di n. Allora, I è un ideale massimale se e solo se m non ha divisori propri, ossia se e solo se m è un numero primo. In tal caso, l'anello quoziente $\mathbf{Z}/m\mathbf{Z}$ è un campo, come già sappiamo. Se invece m è composto, allora $m\mathbf{Z}$ non è massimale e sappiamo che $\mathbf{Z}/m\mathbf{Z}$ non è un campo. Sarà sempre così in tutti gli anelli?

TEOREMA 2.9. Sia A un anello commutativo. Un suo ideale I è massimale se e solo se A/I è un campo.

Dimostrazione. Sia I un ideale massimale di A. Per dimostrare che A/I è un campo dimostriamo che ogni suo elemento non nullo $\bar{a}$ ha l'inverso rispetto alla moltiplicazione quoziente. L'essere $\bar{a} \neq I = 0_{A/I}$ implica che esiste $a \in A$, $a \notin I$, tale che $\bar{a} = a + I$. Sia $J \subseteq A$, $J = \{ax + i \mid x \in A,\ i \in I\}$. Dimostriamo che J è un ideale di A che contiene propriamente I. Innanzi tutto, $\forall i \in I,\ i = a \cdot 0_A + i \in J \Rightarrow I \subseteq J$. In particolare, $0_A \in J$. Inoltre, siano $j_1 = a \cdot x_1 + i_1$, $j_2 = a \cdot x_2 + i_2$ due elementi di J. Allora, $\begin{cases} j_1 + j_2 = (a \cdot x_1 + i_1) + (a \cdot x_2 + i_2) = a \cdot \underbrace{(x_1 + x_2)}_{\in A} + \underbrace{(i_1 + i_2)}_{\in I} \in J \\ -j_1 = a \cdot (-x_1) + (-i_1) \in J \end{cases}$, quindi (J, +) è un sottogruppo di (A, +). Infine, $\forall j = a \cdot x + i \in J$, $\forall y \in A$, si ha:

$$y \cdot j = j \cdot y = a \cdot \underbrace{(x \cdot y)}_{\in A} + \underbrace{(i \cdot y)}_{\in I} \in J$$

e quindi J è un ideale. Poiché $a = a \cdot 1_A + 0_A \in J$ ma non ad I, allora I è incluso propriamente in J. Ora, per l'ipotesi, I è ideale massimale di A, perciò J = A. Ne

segue che $1_A \in J$, quindi esistono $x_0 \in A$, $i_0 \in I$ tali che $1_A = a \cdot x_0 + i_0$. Allora, in A/I si ha: $1_{A/I} = 1_A + I = a \cdot x_0 + \underbrace{i_0 + I}_{=I} = a \cdot x_0 + I = (a+I)\cdot(x_0+I) = \bar{a} \cdot \overline{x_0}$, ossia $\bar{a}$ ha l'inverso. Pertanto, A/I è un campo.

Viceversa, supponiamo che A/I sia un campo. Per dimostrare che I è massimale, sia J un ideale di A contenente propriamente I, e dimostriamo che J = A. Poiché J contiene propriamente I, esiste $a \in J \setminus I$. Nel quoziente A/I, allora, $\bar{a} = a + I$ è invertibile, ossia esiste $\bar{b} = b + I$ tale che $1_A + I = 1_{A/I} = \bar{a} \cdot \bar{b} = a \cdot b + I$. Ne segue che esiste $i \in I$ tale che $1_A = a \cdot b + i$. Ma $a \in J \Rightarrow a \cdot b \in J$, $i \in I \subset J$, quindi $1_A = a \cdot b + i \in J$. Pertanto, J = A ed I è massimale in A.

Il teorema precedente ha vaste applicazioni, ed alcune le vedremo in seguito. Si osservi che avendo dimostrato che gli ideali di **Z** sono tutti e soli quelli della forma p**Z**, p primo, ritroviamo, per questa via, che **Z**/p**Z** è un campo. Concludiamo il capitolo con lo studio degli ideali di un prodotto diretto.

TEOREMA 2.10. Siano A e B due anelli e sia A×B il loro prodotto diretto.

a) Siano I un ideale di A e J un ideale di B, allora U = I×J è un ideale di A×B
b) Sia U un ideale di A×B, allora esistono un ideale I di A ed un ideale J di B tali che U = I×J.

Dimostrazione. a) $U = I \times J = \{(i,j) \mid i \in I,\ j \in J\}$. Dimostriamo che è un ideale di A×B. Per cominciare, $0_{A\times B} = (0_A, 0_B) \in I \times J$. Poi, $\forall (i,j),\ (i',j') \in U$, $(i,j) + (i',j') = (i+i', j+j') \in U$, $-(i,j) = (-i,-j) \in U$, quindi (U,+) è un sottogruppo di (A×B,+). Infine, dato che I e J sono ideali, $\forall (i,j) \in U, \forall (a,b) \in A \times B, \begin{cases} (i,j)\cdot(a,b) = (i\cdot a, j\cdot b) \in U \\ (a,b)\cdot(i,j) = (a\cdot i, b\cdot j) \in U \end{cases}$, quindi U è un ideale.

b) Inversamente, sia U un ideale di A×B. Sia $I \subseteq A$, $I = \{i \in A \mid \exists b \in B,\ (i,b) \in U\}$. Allora I è un ideale di A. Infatti, Poiché $(0_A, 0_B) = 0_{A\times B} \in U$, allora $0_A \in I$. Inoltre, per ogni i, i'∈I esistono b, b'∈B tali che (i, b)∈U, (i', b')∈U, quindi essendo (i+i', b+b') = (i, b)+(i', b')∈U, allora i+i'∈I. Analogamente, (-i, -b) = -(i, b)∈U, segue -i∈I. Pertanto, (I, +) è un sottogruppo di (A, +). Infine, per ogni a∈A si ha: $(a\cdot i, 0_B) = \underbrace{(a, 0_B)}_{\in A\times B} \cdot \underbrace{(i,b)}_{\in U} \in U$, quindi a·i∈I, ed analogamente, i·a∈I, quindi I è un ideale

di A. Allo stesso modo si dimostra che $J \subseteq B$, $J = \{j \in B \mid \exists a \in a,\ (a,j) \in U\}$ è un ideale di B. Dimostriamo che U = I×J. Per questo osserviamo che per ogni i∈I, dal fatto che per un opportuno b∈B si abbia (i,b)∈U segue che anche $(i,0_B) = (1_A,0_B)\cdot(i,b) \in U$. Allo stesso modo si prova che per ogni j∈J, si ha $(0_A,j) \in U$. Allora, $\forall i \in I,\ \forall j \in J,\ (i,j) = (i,0_B) + (0_A,j) \in U \Rightarrow I \times J \subseteq U$. Inversamente, per ogni $u \in U,\ u = (a,b)$, dall'essere b∈B segue a∈I, e dall'essere a∈A segue b∈J, quindi $u = (a,b) \in I \times J \Rightarrow U \subseteq I \times J$. Pertanto, U = I×J.

ESEMPIO 2.11. Consideriamo il prodotto diretto del campo $\mathbf{Z}_2$ per se stesso. Gli ideali di $\mathbf{Z}_2$ sono solo quelli banali {0} e $\mathbf{Z}_2$. Pertanto, l'anello $\mathbf{Z}_2 \times \mathbf{Z}_2$ ha in tutto quattro ideali:

$$\{0\} \times \{0\} = \{(0,0)\},\ \{0\} \times \mathbf{Z}_2 = \{(0,0),(0,1)\},\ \mathbf{Z}_2 \times \{0\} = \{(0,0),(1,0)\},\ \mathbf{Z}_2 \times \mathbf{Z}_2$$

Si osservi che il gruppo additivo dell'anello $\mathbf{Z}_2 \times \mathbf{Z}_2$, oltre a questi quattro sottogruppi, ha un ulteriore sottogruppo d'ordine 2, $\{(0,0),(1,1)\}$, che non è un ideale, ma costituisce il sottoanello fondamentale, in quanto è il sottogruppo generato da (1,1), che è l'unità del prodotto diretto.

§ 3 – DIVISIBILITA'

Ricordiamo che, dati a, b∈**N**, si dice che a divide b (o che b è multiplo di a) se esiste q∈**N** tale che b = aq. Si usa talvolta scrivere a | b. L'unità 1 di **N** divide ogni altro numero naturale, mentre lo zero è multiplo di ogni altro numero naturale. Ogni numero naturale è inoltre divisore di se stesso.

Per estendere questa definizione ad altri contesti algebrici occorrono un insieme X ≠ ø ed una operazione · su X, ossia un *gruppoide* (X, ·). La definizione è allora trasferibile così com'è:

per ogni a, b∈X, a | b se esiste q∈X tale che b = a·q

Perché non pretendere invece: a | b se esiste q∈X tale che b = q·a? Se l'operazione · non è commutativa, ovviamente le cose si complicano. Perciò:

PRIMA RIDUZIONE: (X, ·) gruppoide *commutativo*.

Se (X, ·) è un gruppo, per ogni a, b∈X esiste sempre q∈X tale che b = aq e si ha quindi a | b per ogni a, b∈X. Perciò:

SECONDA RIDUZIONE: (X, ·) gruppoide *commutativo* ma non un gruppo.

La relazione "divide" ha in **N** varie ben note proprietà, sia algebriche sia "relazionali". Vediamo alcune proprietà "relazionali". Siano a, b, c∈**N**:

i. Riflessiva: a | a
ii. Antisimmetrica: se a | b e b | a allora a = b
iii. Transitiva: se a | b e b | c allora a | c

In altre parole, la relazione "divide" è una relazione d'ordine in **N**, cioè (**N**, |) è un *insieme ordinato.* Poiché esistono coppie di numeri nessuno dei quali divide l'altro allora tale ordine non è totale. L'unità 1 è il minimo e lo zero è il massimo di (**N**, |).

Osservazione. L'analoga definizione "additiva": per ogni a, b∈**N**,

$$a \le b \text{ se esiste } d \in \mathbf{N} \text{ tale che } b = a+d$$

produce invece un ordine totale in **N**. In esso, 0 è il minimo e non c'è il massimo.

Vediamo quali proprietà deve avere il gruppoide commutativo $(X, \cdot)$ perché la relazione | abbia qui proprietà simili a quelle della relazione "divide" in **N**.

I) L'*elemento neutro* 1_X assicura la proprietà riflessiva: $a = a\cdot 1_X \Rightarrow a \mid a$

II) La *proprietà associativa* assicura la proprietà transitiva di |, infatti

$$b = a\cdot q,\ c = b\cdot p \Rightarrow c = (a\cdot q)\cdot p = a\cdot(q\cdot p)$$

TERZA RIDUZIONE: $(X, \cdot, 1_X)$ *monoide* commutativo (ma non un gruppo).

Per quanto riguarda la proprietà antisimmetrica, vediamo come esprimerla:

$a \mid b$ e $b \mid a \Leftrightarrow$ esistono $p, q \in X$ tali che $a = b\cdot p$ e $b = a\cdot q$, quindi $a = a\cdot(q\cdot p)$.

Tenendo presente che si ha anche $a = a\cdot 1_X$, allora:

III) Se a è *cancellabile*, da $a = b\cdot p$ e $b = a\cdot q$ segue $p\cdot q = 1_X$ e quindi p e q sono invertibili.

QUARTA RIDUZIONE: $(X,\cdot)$ monoide commutativo (ma non un gruppo) *in cui ogni elemento sia cancellabile,* escluso al più l'eventuale *elemento assorbente*.

Nella maggior parte dei casi, le condizioni poste non bastano ad assicurare la antisimmetria della relazione |. Per esempio, in $(\mathbf{Z}, \cdot, 1)$ si ha: $-3 \mid 3$ e $3 \mid (-3)$. Si può osservare, a questo punto che:

IV) La proprietà antisimmetrica vale se e solo se *il gruppo delle unità* del monoide contiene solo 1_X.

Quest'ultima condizione, tuttavia, non è verificata negli esempi consueti, come visto per $(\mathbf{Z}, \cdot, 1)$. Lo è invece in $(\mathbf{N}, \cdot, 1)$ (e anche in $(\mathbf{N}, +, 0)$). Dove non è

verificata possiamo definire *associati* due elementi a, b se a | b e b | a. La relazione "essere associati" è di equivalenza nel monoide, come è immediato verificare. Chiaramente, questa relazione è *compatibile* con la relazione |, nel senso che se a | b e a', b' sono associati ad a e b rispettivamente, allora a' | b'. Ne segue la possibilità di definire la relazione | fra le classi d'equivalenza di elementi associati e allora l'insieme quoziente risulta un insieme ordinato.

Vediamo ora alcune proprietà "algebriche": siano a, b, c∈**N**:

iv. Unicità del quoziente: se b = a·c ed (a, b) ≠ (0, 0) allora c è l'unico numero che moltiplicato per a dia b.
v. Se a | b e a | c allora a | (b+c) ed a | (bc).

La iv) è verificata anche nel monoide (X, ·, 1_X) in cui ora lavoriamo dopo la quarta riduzione. La v) implica la presenza in X di un'altra operazione, +, rispetto alla quale l'operazione · sia distributiva. Ma allora:

QUINTA RIDUZIONE: (X, +,·, 1_X) *dominio d'integrità*.

Certamente (**N**, +,·, 1_X) non lo è, ma possiamo *simmetrizzarlo* aggiungendo i segni ed ottenere (**Z**, +,·, 1), che lo è.

Sappiamo dalla sezione precedente che ogni dominio d'integrità finito (X, +,·, 1_X) è un campo. In un campo, la moltiplicazione · forma un gruppo sugli elementi non nulli, quindi rende non interessante, come già rilevato, il nostro studio. Pertanto:

SESTA ED ULTIMA RIDUZIONE. (X, +,·, 1_X) dominio d'integrità *infinito e non campo*.

In questo ambiente si sviluppa quindi una teoria della divisibilità, che mantiene le proprietà elementari valide in **N**, a parte l'antisimmetria della relazione "divide". Per quest'ultima si ha:

PROPOSIZIONE 3.1. In ogni dominio d'integrità $(X, +,\cdot, 1_X)$, per ogni $a, b \in X$, non entrambi nulli, si ha:

a e b sono associati $\Leftrightarrow$ esiste un elemento invertibile u tale che $b = a\cdot u$.

Dimostrazione. Se $b = a\cdot u$, con u invertibile (rispetto al prodotto), allora $a = b\cdot u^{-1}$ e quindi a e b sono associati. Inversamente, supponiamo che a e b siano associati. Allora, se $a = 0_X$ allora $b = 0_X$ e viceversa. Se $a \neq 0_X$, allora a è cancellabile e quindi, come già osservato, ne segue $b = a\cdot q$, con q invertibile.

E' interessante quindi sapere chi siano gli elementi invertibili dell'anello. Nel caso di **Z** sono solo 1 e -1. Talora è possibile effettuare una scelta "canonica" dei rappresentanti delle classi di elementi associati: nel caso di **Z**, fra due numeri a e -a si sceglie quello positivo.

Sia dato un dominio d'integrità $(X, +,\cdot, 1_X)$ e siano $a, b \in X$. Un elemento $d \in X$ si dice *massimo comune divisore* di a e b se:

i. è un divisore di a e di b (*divisore comune*)
ii. è multiplo di ogni altro divisore comune (*massimo)*

Un elemento $m \in X$ si dice *minimo comune multiplo* di a e b se:

i. è un multiplo di a e di b (*multiplo comune*)
ii. è divisore di ogni altro multiplo comune (*minimo)*

In **N** per ogni a, b esistono entrambi e sono unici, per cui si scrive $d = \mathrm{MCD}(a, b)$, $m = \mathrm{mcm}(a, b)$ e queste due, MCD e mcm, sono operazioni in **N**, le quali possiededono varie proprietà, che elenchiamo rinviando la dimostrazione agli esercizi.

PROPOSIZIONE 3.2. Siano $a, b, c \in \mathbf{N}$. Allora valgono le seguenti proprietà

a) associativa:

MCD(MCD(a, b),c) = MCD(a, MCD(b, c)),

mcm(mcm(a, b),c) = mcm(a, mcm(b, c))

b) commutativa:

MCD(a, b) = MCD(b, a),

mcm(a, b) = mcm(b, a)

c) idempotenza:

MCD(a, a) = a = mcm(a, a)

d) assorbimento:

MCD(mcm(a, b),a) = a = mcm(MCD(a, b),a)

e) distributività reciproca:

MCD(mcm(a, b),c) = mcm(MCD(a, c), MCD(b, c))

mcm(MCD(a, b),c) = MCD(mcm(a, c), mcm(b, c))

f) elementi neutri/assorbenti:

MCD(a, 0) = a = mcm(a, 1)

MCD(a, 1) = 1, mcm(a, 0) = 0

La struttura algebrica (**N**, mcm, MCD) così ottenuta è un *reticolo*. Si noti che, rispetto alla relazione d'ordine "divide", si ha:

$$\begin{cases} MCD(a, b) = \inf\{a, b\} \\ mcm(a, b) = \sup\{a, b\} \end{cases}$$

Inoltre, 1 e 0 sono, rispettivamente, il minimo ed il massimo di (**N**, |). Pertanto, il reticolo così ottenuto su **N** è distributivo ed ha minimo e massimo.

Se ci poniamo ora in un dominio d'integrità qualsiasi $(X, +, \cdot, 1_X)$, non è detto che ogni coppia di elementi $a, b \in X$ possieda un massimo comune divisore o un minimo comune multiplo.

Inoltre, se d' è associato a d e d è un massimo comune divisore di a e b, anche d' lo è. Inoltre, d è massimo comune divisore anche di a', b', se a' e b' sono associati rispettivamente ad a e b. Lo stesso dicasi per il minimo comune multiplo. Pertanto, l'unicità non è assicurata, ma lo è a meno di elementi associati. Scriveremo perciò d = MCD(a, b) (o anche d = (a, b)) e m = mcm(a, b) anche se ciò non sarebbe del tutto corretto.

Si pone quindi il problema di trovare condizioni che assicurino l'esistenza di MCD ed mcm.

ESEMPIO 3.3. - Vediamo in **N** come si trova il MCD di due numeri.

3.3.A. - In **N** sovente si definisce MCD(a, b) come "il più grande" dei divisori comuni di a e b, dove l'espressione "il più grande" non si riferisce all'ordine parziale | ma a quello totale ≤. Quest'ultimo è legato all'altro dal fatto che, per ogni a, b∈**N**\{0},

$$a \mid b \text{ implica } a \le b.$$

Pertanto, ogni divisore comune di a e b è ≤ d. Ne segue che basta determinare l'insieme D(a) dei divisori di a e quello, D(b), dei divisori di b, entrambi finiti, farne l'intersezione D(a) ∩ D(b) e prenderne il massimo:

$$D(12) = \{1, 2, 3, 4, 6, 12\},\ D(18) = \{1, 2, 3, 6, 9, 18\},$$
$$D(a) \cap D(b) = \{1, 2, 3, 6\} \Rightarrow MCD(12, 18) = 6.$$

Si ha inoltre: mcm(12, 18) = 12·18/6 = 36, come si può verificare.

In modo simile, il minimo comune multiplo mcm(a,b) è il minimo dei multipli comuni. Come sopra, si considerano l'insieme dei multipli di a e quello dei multipli di b, se ne fa l'intersezione e si prende il minimo. In questo caso, però, i multipli di a e b sono infiniti e non si possono scrivere tutti, ma poiché tra di essi c'è il prodotto a·b, che è un multiplo comune, allora basta considerare per entrambi i multipli minori o uguali al prodotto.

Il vantaggio di questo approccio è che la dimostrazione delle proprietà di MCD e mcmc è facile, perché è ricondotta alle proprietà dell'intersezione di insiemi.

Ma tutto ciò è esportabile al massimo in **Z**, in cui c'è l'ordine totale come in **N**, ma non per esempio fra i polinomi.

3.3.B. - Il *procedimento euclideo delle divisioni successive*: sappiamo che in **N** si può eseguire la *divisione col resto*: per ogni a, b∈**N**, b ≠ 0, esistono e sono unici q∈**N** (quoziente) ed r∈**N** (resto) tali che a = b·q + r, 0 ≤ r < b. Sappiamo che si ha:

a) Ogni divisore comune di a e b è anche divisore comune di b ed r, e viceversa.

b) MCD(a, b) = MCD(b, r)

Ne segue il seguente algoritmo: supposto a ≥ b e posto d = MCD(a, b),

$a = b\cdot q_1 + r_1$, $0 \le r_1 < b$: se $r_1 = 0$ allora $d = b$

$b = r_1\cdot q_2 + r_2$, $0 \le r_2 < r_1$: se $r_2 = 0$ allora $d = r_1$

$r_1 = r_2\cdot q_3 + r_3$, $0 \le r_3 < r_2$: se $r_3 = 0$ allora $d = r_2$

....

Il procedimento termina dopo un numero finito di passi, poiché i resti decrescono ad ogni passo. Per esempio:

$18 = 12\cdot 1 + 6$

$12 = 6\cdot 2 + 0 \Rightarrow \text{MCD}(18, 12) = 6$

Per trovare poi mcm(a, b) si usa il fatto che mcm(a,b)·MCD(a,b) = a·b. Per esempio, mcm(18,12) = 18·12/6 = 36.

Anche in alcuni dominii d'integrità è definita una funzione a valori reali non negativi, detta modulo, e si può eseguire la divisione col resto, col modulo del resto minore del modulo del divisore, individuati a meno di elementi associati. Per esempio, in **Z**, posto |x| = valore assoluto di x, per ogni a, b, $b \neq 0$, esistono e sono unici q, r∈**Z** tali che $a = b\cdot q + r$, $0 \leq r < |b|$.

Essi sono detti *anelli euclidei*. Con l'analogo algoritmo si trovano quindi MCD ed mcm anche in questi anelli. In generale, tuttavia, in un dominio d'integrità non c'è questa possibilità.

3.3.C. - La *scomposizione in fattori irriducibili*. In **N** si definisce *primo* o *irriducibile* un numero p maggiore di 1 e divisibile solo per 1 e per se stesso. Una sua proprietà rilevante, e che lo caratterizza, è:

per ogni a, b∈**N**, $p \mid a\cdot b \Rightarrow p \mid a$ oppure $p \mid b$.

Esistono infiniti numeri primi, come ha dimostrato Euclide. Inoltre, vale il:

Teorema fondamentale dell'aritmetica: ogni numero naturale > 1 si può scrivere in uno ed un solo modo come prodotto di fattori primi, a parte l'ordine dei fattori stessi.

Sia Π l'insieme dei numeri primi. Per ogni a∈**N**, $a \neq 0$, accorpando con l'uso delle potenze i fattori primi uguali e ponendo = 0 gli esponenti dei primi mancanti nella sua scomposizione, possiamo rappresentare a nella forma:

$$a = \prod_{p\in\Pi} p^{\alpha_p}$$

dove gli esponenti sono nulli per tutti i primi p tranne un numero finito.

Ciò posto, se $b = \prod_{p\in\Pi} p^{\beta_p}$, si ha:

$$b \mid a \text{ se e solo se per ogni } p\in\Pi,\ \beta_p \le \alpha_p.$$

Questa proprietà è nota come *criterio generale di divisibilità*, e dipende dalle proprietà delle potenze: posto $\theta_p = \alpha_p - \beta_p$ e $q = \prod_{p\in\Pi} p^{\theta_p}$, segue $a = b\cdot q$. Il viceversa è immediato.

Ne segue la regola che usualmente si insegna nella scuola secondaria: per ogni a, b non nulli, scritti come prodotto di primi, si ha:

$$\mathrm{MCD}(a,b) = \prod_{p\in\Pi} p^{\min\{\alpha_p,\beta_p\}},\ \mathrm{mcm}(a,b) = \prod_{p\in\Pi} p^{\max\{\alpha_p,\beta_p\}}.$$

Per esempio: $12 = 2^2\cdot 3 = 2^2\cdot 3^1\cdot 5^0\cdot 7^0\cdot \ldots$, $18 = 3^2\cdot 2 = 2^1\cdot 3^2\cdot 5^0\cdot 7^0\cdot \ldots$

$$\mathrm{MCD}(12, 18) = 2^1\cdot 3^1\cdot 5^0\cdot 7^0\cdot \ldots = 6,\ \mathrm{mcm}(12, 18) = 2^2\cdot 3^2\cdot 5^0\cdot 7^0\cdot \ldots = 36$$

Questo procedimento, con qualche variante, funziona anche in altri anelli. Innnanzitutto, in un anello ogni elemento è multiplo di tutti gli elementi invertibili e di tutti i suoi associati; lo diremo *irriducibile* (o *indecomponibile*) se questi sono i soli suoi divisori. Per esempio, -3 in **Z** ha come divisori 1, -1, 3, -3, quindi è irriducibile; non avremo quindi l'unicità della fattorizzazione, ma solo una *unicità essenziale*, cioè a meno di elementi associati, oltre che dell'ordine dei fattori:

$$12 = 2\cdot 2\cdot 3 = (-2)\cdot 2\cdot (-3) = (-2)\cdot (-2)\cdot 3$$

Inoltre, la proprietà dei numeri primi di dividere necessariamente un fattore tutte le volte che dividono un prodotto non è sempre vera in ogni dominio d'integrità. Un elemento p di un dato dominio $(A, +,\cdot, 1_A)$, non nullo e non invertibile, si dice *primo* se

$$\text{per ogni } a, b\in X,\ p \mid a\cdot b \Rightarrow p \mid a \text{ oppure } p \mid b.$$

Si vede facilmente che se p è primo in A è anche irriducibile: se $p = m\cdot n$, allora p ovviamente divide il prodotto $m\cdot n$, quindi divide m oppure n; ma questi sono suoi divisori, quindi se per esempio $p \mid n$, allora p ed n sono associati ed m è invertibile; ossia, p è irriducibile. Esistono però dominii d'integrità con elementi irriducibili che non sono primi.

Un dominio d'integrità $(A, +,\cdot, 1_A)$ si dice *fattoriale* se ogni $a\in A$, non nullo e non invertibile, è esprimibile come prodotto di fattori irriducibili ed in modo essenzialmente unico, cioè se vale in esso il teorema fondamentale

dell'aritmetica. Chiaramente, in un tal dominio ogni coppia di elementi possiede MCD ed mcm. Inoltre, ogni irriducibile è primo. Infatti, se p è irriducibile e divide il prodotto a·b, allora esiste q tale che: a·b = p·q. I due membri sono uguali, p è irriducibile e compare nella fattorizzazione del II membro, quindi deve comparire anche nella fattorizzazione del I membro, o fra i fattori di a (ed allora p divide a) o fra quelli di b (ed allora p divide b) o in entrambi.

A questo punto, in un dominio fattoriale si pongono due problemi:

a) Classificare gli elementi irriducibili (= primi)

b) Scomporre un dato elemento in un prodotto di irriducibili.

In **N** entrambi i problemi sono aperti e sono tuttora oggetto di ricerche, a causa delle applicazioni alla crittografia e quindi alla tutela della segretezza nella trasmissione di informazioni bancarie, militari, politiche. Si hanno numerosi criteri di primalità e di divisibilità, alcuni dei quali sono ben noti ed elementari, ma ce ne sono di ben più sofisticati, alcuni dei quali sono implementati sui programmi matematici più comuni (Mathematica, Maple, Derive, ...)
Vedremo nella prossima sezione quel che accade con i polinomi sui campi reale, complesso e razionale.

3.3.D. - C'è infine un ulteriore aspetto algebrico da considerare, che lega in un certo senso addizione e MCD: *l'identità di Bézout*: se d = MCD(a, b) in **Z**, esistono u, v∈**Z** tali che $au + bv = d$.

Per esempio, 6 = MCD(12, 18) = -1·12 + 1·18.

Non in tutti i dominii fattoriali vale questa identità. Essa è legata alla nozione di *ideale principale* di un anello: in un anello commutativo un ideale I si dice *principale* se esiste m∈I tale che I = {m·a | a∈A}, cioè è costituito dai multipli di m. In tal caso I si dice *generato* da m. Si usa scrivere I = (m). La nozione di divisore si traduce in termini di ideali osservando che, per ogni m, n∈A si ha:

$$m \mid n \text{ se e solo se } (n) \subseteq (m).$$

Un dominio d'integrità i cui ideali siano tutti principali è detto *dominio ad ideali principali* (P.I.D.). Un esempio è costituito dagli anelli euclidei: se I è un ideale non nullo, esso ha elementi non nulli di modulo minimo: se m è uno di essi, ogni altro suo elemento x, diviso per m dà x = mq+r, con $0 \le |r| < |m|$, ma

allora $r = x - mq \in I$ e per la minimalità di m segue r = 0 ed x = mq. Dunque, I = (m). Ma non tutti i dominii ad ideali principali sono euclidei.

In un dominio ad ideali principali vale l'identità di Bézout: siano a, b non nulli e consideriamo l'ideale I generato dall'insieme $\{a, b\}$. Si vede facilmente che $I = \{a \cdot x + b \cdot y \mid x, y \in A\}$, dato che ogni ideale contenente a e b, I compreso, deve contenere tutti gli elementi $a \cdot x + b \cdot y$ e che, viceversa, $\{a \cdot x + b \cdot y \mid x, y \in A\}$ è un ideale contenente a e b e quindi deve contenere I. Poiché A è ad ideali principali, esiste $d \in A$, $(d) = I$. Allora esistono u,v in A tali che d = au+bv. Segue subito che ogni divisore comune di a e b divide anche d. Inoltre, da $(d) = I = (\{a, b\}) \supseteq (a)$ segue $a \in (d) \Rightarrow d \mid a$; analogamente, d divide b. Ma allora d è un MCD di a e b.
Se però A non è euclideo, non c'è un algoritmo semplice per trovare i coefficienti u, v. Per quanto riguarda il minimo comune multiplo di a e b, si consideri l'ideale $(a) \cap (b)$: i suoi elementi sono i multipli comuni ad a e b. Poiché A è un P.I.D. anche questo ideale è principale, quindi esiste $m \in A$, $(m) = (a) \cap (b)$. Allora m = mcm(a,b), dato che tutti gli altri multipli comuni appartengono ad (m) e dunque sono suoi multipli. Abbiamo così dimostrato il seguente risultato:

PROPOSIZIONE 3.4. Sia A un dominio d'integrità ad ideali principali. Allora ogni coppia $\{a,b\}$ di elementi di A possiede MCD ed mcm. Più precisamente,

a) $(\{a,b\}) = \{ax + by \mid x,y \in A\} = (MCD(a,b))$

b) $(a) \cap (b) = (mcm(a,b))$

Giuochiamo ancora un poco con i P.I.D. per dimostrare che sono fattoriali ed hanno altre proprietà.

PROPOSIZIONE 3.5. Sia A un dominio d'integrità ad ideali principali.

a) Siano a, b, c ∈A, tali che $\begin{cases} a \text{ divide } b \cdot c \\ MCD(a,b) = 1_A \end{cases}$, allora a divide c

b) Ogni elemento irriducibile è primo

c) Ogni successione crescente di ideali è finita.

Dimostrazione. a) Per l'ipotesi, esiste q∈A tale che bc = aq. Poiché siamo in un P.I.D., l'ipotesi $\mathrm{MCD}(a,b)=1_A$ implica che esistono u,v∈A tali che $au+bv=1_A$. Allora, se moltiplichiamo per c ambo i membri:

$$c\cdot(au+bv)=c\cdot 1_A \Rightarrow a\cdot(cu)+(bc)v=c \Rightarrow a\cdot(cu+qv)=c$$

e quindi a divide c.

b) Sappiamo che un primo è sempre irriducibile. Viceversa, sia p irriducibile, e siano b, c∈A tali che p divida il prodotto bc. Se p divide b siamo a posto. Se p non divide b, allora essendo MCD(p,b) divisore di p e non uguale (o meglio, non associato) a p, allora deve essere uguale ad 1_A, dato che p è irriducibile. Ma allora, per la parte a), p deve dividere c. Pertanto, p divide almeno uno dei due fattori e quindi è primo.

c) Sia $I_1\subseteq I_2\subseteq\ldots\subseteq I_k\subseteq\ldots$ una successione crescente di ideali di A, e poniamo $I=\bigcup_{k\geq 1} I_k$. Allora anche I è un ideale di A. Infatti, $0_A\in I_1\subseteq I\Rightarrow 0_A\in I$. Inoltre, $\forall x,y\in I\ \exists I_h,I_k \mid x\in I_h,\ y\in I_K$. Uno dei due tra h e k è più grande, per esempio sia h ≤ k. Allora $I_h\subseteq I_k\Rightarrow x,y\in I_k\Rightarrow\begin{cases}x+y\in I_k\\ -x\in I_k\end{cases}\Rightarrow\begin{cases}x+y\in I\\ -x\in I\end{cases}$ e quindi (I,+) è un sottogruppo di (A,+); infine, per ogni a∈A, $a\cdot x\in I_h\Rightarrow a\cdot x\in I$ e quindi I è un ideale. Poiché A è un P.I.D., anche I è principale, quindi esiste u∈I tale che $I=(u)$. Allora esiste n ≥ 1 tale che $u\in I_n$, dunque $I=(u)\subseteq I_n$, ma $I_n\subseteq I$, $\Rightarrow I_n=I$. Perciò la successione ha al più n elementi distinti: $I_1\subseteq I_2\subseteq\ldots\subseteq I_k\subseteq\ldots\subseteq I_n=I_n=I_n=\ldots$

TEOREMA 3.6. Ogni dominio d'integrità ad ideali principali è fattoriale.

Dimostrazione. Sia A un P.I.D. Dobbiamo dimostrare che ogni elemento a∈A, non nullo e non invertibile, o è irriducibile oppure è prodotto di fattori irriducibili, e la fattorizzazione è essenzialmente unica, a prescindere da riordini dei fattori o dalla presenza di fattori associati. Procediamo per passi. Sia a∈A, non nullo e non invertibile.

i) Dimostriamo che a è multiplo di almeno un elemento irriducibile. Se a lo è, siamo a posto. Altrimenti, è multiplo di un elemento a_1 non invertibile e non associato ad a. Procedendo ricorsivamente, si ottiene una successione $a=a_0,a_1,a_2,\ldots$ di elementi ciascuno dei quali è multiplo del successivo. $\forall j\geq 0$ sia $I_j=(a_j)$: allora $I_0\subset I_1\subset I_1\subset\ldots$ Ma A è un P.I.D., quindi la successione è finita: esiste quindi n ≥ 0 tale che a_n è multiplo solo di associati ed invertibili, ossia è irriducibile; inoltre, per la transitività della divisibilità, è divisore di a.

ii) Dimostriamo che a è scomponibile in un prodotto di elementi irriducibili. Se è irriducibile, siamo a posto. Altrimenti, per il passo i) precedente, esistono un irriducibile p_1 ed un elemento

q_1 tali che $a = p_1 q_1$. Possiamo ripetere il discorso a partire da q_1 ed ottenere ricorsivamente una successione $p_1, p_2, \ldots$ di irriducibili ed una successione $q_0 = a, q_1, q_2, \ldots$ di elementi tali che $q_i = p_{i+1} q_{i+1}$ con q_{i+1} divisore di q_i. Come sopra, posto $\forall i \geq 0,\ I_i = (q_i)$, abbiamo una successione $I_0 \subset I_1 \subset I_1 \subset \ldots$di ideali, che deve essere finita. Allora deve esistere n ≥ 0 tale che q_n è irriducibile, e quindi $a = p_1 p_2 \cdots p_n q_n$, con i fattori tutti irriducibili.

iii) Proviamo l'unicità della fattorizzazione di a in irriducibili. Sappiamo che ogni irriducibile è primo. Sia $a = p_1 \cdots p_r = q_1 \cdots q_s$, con i fattori tutti primi. Procediamo per induzione rispetto ad r. Se r = 1 allora $a = p_1$ ed ognuno dei q_j è divisore di $p_1 \Rightarrow s = 1$ e $q_1 = p_1$. Sia r > 1. Poiché p_1 divide il prodotto $q_1 \cdots q_s$, essendo primo ne divide uno dei fattori, che possiamo supporre sia q_1; ma q_1 è irriducibile, quindi q_1 e p_1 sono associati. L'eventuale fattore invertibile possiamo conglobarlo in un altro dei q_j e quindi supporre $q_1 = p_1$. Posto allora $a = p_1 a'$, segue $a' = p_2 \cdots p_r = q_2 \cdots q_s$. Per ipotesi induttiva si ha s-1 = r-1, quindi r = s e, a meno di riordini, p_i e q_i sono associati anche per per ogni i > 1.

TEOREMA 3.8. Sia A un P.I.D. Un ideale I è massimale se e solo se $I = (p)$, con p irriducibile.

Dimostrazione. Si procede come in Z. Siano I, J due ideali. Poiché sono principali, esistono a, b∈A tali che $I = (a),\ J = (b)$. Si ha $I \subseteq J \Leftrightarrow b \mid a$, quindi I è massimale se e solo se a non ha altri divisori che quelli che generano I, e sono i suoi associati, e quelli che generano A, e sono gli elementi invertibili, quindi se e solo se a è irriducibile.

§ 4 – POLINOMI A COEFFICIENTI REALI O COMPLESSI

Chiamiamo *funzione polinomiale* (o più brevemente *polinomio*) in una variabile una funzione f:**R**→**R**, per la quale esistono a_0, a_1, ..., $a_n \in \mathbf{R}$, tali che per ogni $x \in \mathbf{R}$ si ha $f(x) = \sum_{i=0}^{n} a_i x^i$. I numeri a_0, a_1, ... sono detti *coefficienti*. Tra queste funzioni c'è la costante nulla **0**, ottenibile ponendo = 0 tutti i coefficienti.

Denotiamo con **R**[x] l'insieme dei polinomi. Il modo di sommare e moltiplicare i polinomi è ben noto dal calcolo letterale: si considerano le operazioni punto per punto tipiche delle funzioni di una variabile reale, già definite nell'esempio 1.1.A. Si ha:

PROPOSIZIONE 4.1. L'insieme **R**[x] dei polinomi costituisce un sottoanello dell'anello delle funzioni da **R** ad **R**.

Dimostrazione. Sappiamo già che la costante nulla si può scrivere come polinomio, quindi appartiene ad **R**[x]. Siano f, g due polinomi, $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$. Se per esempio m < n, possiamo porre $b_{m+1} = \ldots = b_n = 0$. Allora, $g(x) = \sum_{i=0}^{n} b_i x^i$. Usando le proprietà delle operazioni in **R**, si ha:

$$(f+g)(x) = f(x) + g(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

quindi $f+g \in \mathbf{R}[x]$. Inoltre, $(-f)(x) = -f(x) = \sum_{i=0}^{n} (-a_i) x^i$ implica $-f \in \mathbf{R}[x]$.

Per la moltiplicazione si ha innanzi tutto che la costante **1**, che ad ogni x associa 1, si può scrivere come polinomio $1 + \sum_{i=1}^{n} 0x^i$, $n \geq 1$. Inoltre, per il prodotto di due polinomi si ha:

$$(f\cdot g)(x)=f(x)\cdot g(x)=\sum_{i=0}^{n}a_ix^i\cdot\sum_{j=0}^{m}b_jx^j=\sum_{i=0}^{n}\sum_{j=0}^{m}(a_ib_j)x^{i+j}=\sum_{k=0}^{m+n}\left(\sum_{i+j=k}(a_ib_j)\right)x^k,$$

avendo posto k = i+j e raccolto i termini simili. Dunque, anche $f\cdot g\in\mathbf{R}[x]$.

Pertanto, $\mathbf{R}[x]$ è un sottoanello dell'anello $\left(\mathbf{R}^{\mathbf{R}},+,\cdot,1\right)$.

Occupiamoci ora della espressione di un polinomio $f(x)=\sum_{i=0}^{n}a_ix^i$: è unica?

TEOREMA 4.2. (Principio d'identità dei polinomi a coefficienti reali).

a) Il solo modo di rappresentare la costante nulla come polinomio è con i coefficienti tutti nulli.

b) Siano f, g due polinomi, $f(x)=\sum_{i=0}^{n}a_ix^i$, $g(x)=\sum_{i=0}^{m}b_ix^i$. Si ha f = g (ossia, per ogni $x\in\mathbf{R}$ si ha f(x) = g(x)) se e solo se per ogni $i\geq 0$ si ha $a_i=b_i$.

Dimostrazione. a) Tra le molte dimostrazioni esistenti, ne propongo una che fa uso di ben note nozioni di Analisi Matematica. La costante nulla **0** è tale che per ogni $x\in\mathbf{R}$ si ha **0**(x) = 0, perciò $\lim_{x\to+\infty}\mathbf{0}(x)=0$. Per assurdo supponiamo che si possa scrivere $\mathbf{0}(x)=\sum_{i=0}^{n}a_ix^i$, $n\geq 0$, $a_n\neq 0$. Allora:

$$0=\lim_{x\to+\infty}\mathbf{0}(x)=\lim_{x\to+\infty}\sum_{i=0}^{n}a_ix^i=\lim_{x\to+\infty}\left(\begin{array}{c}x^n\\ \downarrow\\ +\infty\end{array}\cdot\sum_{i=0}^{n}\frac{a_i}{x^{n-i}}\begin{array}{c}\\ \downarrow\\ a_n\end{array}\right)=\begin{cases}+\infty & \text{se } a_n>0\\ -\infty & \text{se } a_n<0\end{cases},$$

assurdo. Pertanto, l'unico modo di scrivere la funzione nulla come polinomio è con i coefficienti tutti nulli.

b) per ogni $x\in\mathbf{R}$ si ha f(x) = g(x) se e solo se f(x) – g(x) = 0 ossia se e solo se f-g è la costante nulla **0**. Allora, ponendo come sopra, $b_{m+1}=\ldots=b_n=0$ se m < n,

$$\mathbf{0}(x)=f(x)-g(x)=\sum_{i=0}^{n}(a_i-b_i)x^i\Rightarrow a_i-b_i=0\ \forall i\geq 0$$

quindi per ogni $x\in\mathbf{R}$ si ha f(x) = g(x) se e solo se per ogni $i\geq 0$ si ha $a_i=b_i$.

Il principio d'identità ci consente di definire il *grado* di un polinomio non nullo.

Sia f un polinomio non nullo, allora si ha $f(x)=\sum_{i=0}^{n} a_i x^i$, con almeno uno dei coefficienti non nullo. Sia $n \geq 0$ il massimo indice tale che $a_n \neq 0$. Allora n si dice grado di f, e si denota con gr(f), mentre a_n si chiama *coefficiente direttore* di f. Se $a_n = 1$ il polinomio si dice *monico*.

NOTA. Al polinomio nullo non si può attribuire il grado, poiché i suoi coefficienti sono tutti nulli. In qualche testo si pone però gr(0) = -∞

Il termine a_0 è detto *termine noto*. I *polinomi costanti* sono quelli di grado zero, insieme con il polinomio nullo. Si ha:

TEOREMA 4.3. (Teorema dei gradi). Siano f, g due polinomi non nulli, di gradi n, m rispettivamente. Allora

a) gr(f+g) ≤ max{gr(f), gr(g)}

b) gr(f·g) = gr(f)+gr(g)

c) **R**[x] è un dominio d'integrità

Dimostrazione. a) Siano $f(x)=\sum_{i=0}^{n} a_i x^i$, $g(x)=\sum_{i=0}^{m} b_i x^i$ e sia per esempio m < n. Allora, dalla proposizione 4.1. segue:

$$(f+g)(x)=(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\ldots+(a_m+b_m)x^m+a_{m+1}x^{m+1}+\ldots+a_n x^n$$

Quindi f+g ha il grado di f. Se m = n può accadere che sia $b_n = -a_n$, quindi il grado della somma può essere minore di quello degli addendi.

b) Da 4.1 si ha poi che $(f\cdot g)(x)=\sum_{k=0}^{m+n}\left(\sum_{i+j=k}(a_i b_j)\right)x^k$ ha grado m+n, poiché

$a_n \neq 0,\ b_m \neq 0 \Rightarrow a_n \cdot b_m \neq 0$.

c) Da b) segue che se f e g non sono nulli, anche f·g non è il polinomio nullo.

PROPOSIZIONE 4.4.

a) $(\mathbf{R}[x])^*$ è costituito dall'insieme dei polinomi di grado 0

b) L'insieme dei polinomi costanti costituisce un sottoanello di $\mathbf{R}[x]$, isomorfo ad $\mathbf{R}$.

Dimostrazione. a) Un polinomio f di grado 0 è una costante c non nulla, ossia si ha f(x) = c per ogni x, quindi ha per reciproca la funzione $\frac{1}{f}(x) = \frac{1}{c} = \frac{1}{c} + 0x + 0x^2 + \dots$, che è ancora un polinomio di grado 0. Ogni altro polinomio non è invertibile. Infatti, avendo grado ≥ 1, il suo prodotto con l'inverso dovrebbe dare da un lato la costante 1, di grado zero, mentre dall'altro avrebbe grado uguale alla somma dei gradi, cioè ≥ 1, assurdo.

b) La funzione $\Phi: \mathbf{R} \to \mathbf{R}[x]$, tale che $\Phi(a) = a + 0x + 0x^2 + \dots$, ossia che al numero reale a associa la costante a, è un monomorfismo di anelli: infatti,

$$\Phi(a+b) = a + b + 0x + 0x^2 + \dots = \left(a + 0x + 0x^2 + \dots\right) + \left(b + 0x + 0x^2 + \dots\right) = \Phi(a) + \Phi(b)$$

$$\Phi(a \cdot b) = a \cdot b + 0x + 0x^2 + \dots = \left(a + 0x + 0x^2 + \dots\right) \cdot \left(b + 0x + 0x^2 + \dots\right) = \Phi(a) \cdot \Phi(b)$$

$$\Phi(1) = 1 + 0x + 0x^2 + \dots = \mathbf{1}.$$

Ovviamente è anche iniettiva, dato che il nucleo è un ideale di $\mathbf{R}$ che, essendo un campo, oltre a se stesso ha solo l'ideale nullo.

Nell'anello $\mathbf{R}[x]$ si può eseguire anche la *divisione col resto*:

TEOREMA 4.5. Dati due polinomi f, g, con g diverso dal polinomio nullo (cioè dalla funzione costante 0), esistono e sono unici due polinomi q ed r, con r = 0 oppure di grado minore del grado di g, tali che f = gq + r.

Dimostrazione. Se f = 0 allora q = 0, r = f. Se g è una costante c, allora $q = \frac{1}{c} \cdot f$ ed r = 0. Procediamo ora per induzione rispetto al grado di f. Se gr(f) < gr(g) allora q = 0, r = f. Siano ora $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$, $n = gr(f) \geq gr(g) = m > 0$.

Allora il polinomio $h(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$ ha il coefficiente del termine x^n uguale a zero. Dunque, ha grado $\leq$ n-1. Allora, per ipotesi induttiva esistono due polinomi k, r tali che h(x) = g(x)·k(x) + r(x), con r = 0 oppure gr(r) < gr(g). Ne

segue $f(x) = h(x) + \frac{a_n}{b_m} x^{n-m} g(x) = g(x) \cdot \underbrace{\left(\frac{a_n}{b_m} x^{n-m} + k(x) \right)}_{q(x)} + r(x)$. L'unicità segue da questo: se $f(x) = g(x) \cdot q(x) + r(x) = g(x) \cdot p(x) + s(x)$, allora $g(x) \cdot (q(x) - p(x)) = s(x) - r(x)$. Il II membro, se non è nullo, ha grado minore del grado di g, mentre il primo membro, che in tal caso non è nullo a sua volta, ha grado ≥ gr(g), pertanto si ha un assurdo. Allora il II membro è nullo, ossia r = s, ed allora lo è anche il primo. Dall'essere g non nullo, segue che deve essere nullo il fattore q-p, ossia q = p.

COROLLARIO 4.6. L'anello **R**[x] è un dominio ad ideali principali, quindi è fattoriale.

Dimostrazione. In ogni ideale non nullo I di **R**[x] si consideri un polinomio di grado minimo p; allora per ogni altro polinomio f esistono q, r tali che $f = p \cdot q + r$, con r = 0 oppure di grado minore di quello di p. Poiché $r = f - p \cdot q \in I$, allora per la minimalità del grado di p si ha r = 0 e quindi f multiplo di p. Dunque, $I = (p)$. La fattorialità segue dal teorema 3.8.

OSSERVAZIONE. Nella scuola secondaria si introducono anche i polinomi in n variabili, come somme (punto per punto) di monomi, che sono funzioni $f: \mathbf{R}^n \to \mathbf{R}$, della forma $f(x_1, ..., x_n) = a x_1^{k_1} \cdot ... \cdot x_n^{k_n}$, dove gli esponenti sono interi non negativi ed a è un numero razionale, detto *coefficiente* del monomio. Se $a \neq 0$, il *grado* del monomio è il numero $k_1 + ... + k_n$. Il grado di un polinomio non nullo è il massimo dei gradi dei suoi monomi. L'insieme dei polinomi in n variabili si denota con $\mathbf{R}[x_1, ..., x_n]$ ed è un dominio d'integrità fattoriale, ma non ad ideali principali Se $f \in \mathbf{R}[x_1, ..., x_n]$, l'equazione $f(x_1, ..., x_n) = 0$ è detta *equazione algebrica (intera) in n incognite*. Ci occupiamo qui però solo del caso n = 1.

Le *equazioni algebriche in un'incognita* sono quelle che hanno al primo membro un polinomio f di una sola variabile. Chiamiamo *zeri* o *radici* di f le soluzioni dell'equazione f(x) = 0.

Se per ogni i si ha $a_i = 0$, allora ogni x è soluzione e si ha un'*identità*. Escludiamo questo caso. Allora il *grado* dell'equazione è il grado di f.

Le *equazioni di grado 0* sono ottenute uguagliando a zero una costante non nulla e non hanno soluzioni.

Le *equazioni di primo grado* hanno la forma $ax+b = 0$, con $a \neq 0$, ed hanno una ed una sola soluzione: $x = -b/a$.

Le *equazioni di secondo grado* hanno la forma: $ax^2+bx+c = 0$, con $a \neq 0$. Non è detto che abbiano soluzioni: per esempio:

$x^2-4 = 0$ ha due soluzioni: 2 e -2.

$x^2+2x+1 = 0$ ha la sola soluzione -1.

$x^2+3 = 0$ non ha soluzioni: infatti, dalle proprietà dell'ordinamento di **R** segue, per ogni $x \in \mathbf{R}$, $x^2 \geq 0$ per cui $3+x^2 \geq 3 > 0$ per ogni $x \in \mathbf{R}$.

OSSERVAZIONE. L'equazione $x^2 - 2 = 0$ ha soluzione in **R**, ma non in **Q**. Non esiste infatti in **Q** un numero il cui quadrato sia 2: se ci fosse, si potrebbe rappresentare con la frazione p/q ridotta ai minimi termini, ma allora sarebbe $p^2 = 2q^2$, quindi p sarebbe pari, $p = 2p'$, e allora si avrebbe $4p'^2 = 2q^2$, da cui, semplificando per 2, seguirebbe $2p'^2 = q^2$, cioè anche q pari, assurdo. Ecco uno dei motivi per introdurre i numeri reali.

Osserviamo innanzitutto che l'equazione $ax^2+bx+c = 0$, $a \neq 0$, diventa:

$$(x+b/2a)^2 - \Delta/4a^2 = 0,$$

dove $\Delta = b^2-4ac$ è detto *discriminante*. Se $\Delta \geq 0$ l'equazione ha per soluzioni $\frac{-b \pm \sqrt{\Delta}}{2a}$. Se $\Delta < 0$, l'equazione è impossibile, perché si ha $(x+b/2a)^2 - \Delta/4a^2$ somma di due numeri, il primo ≥ 0 ed il secondo > 0.

Prima di procedere oltre, esaminiamo un poco le proprietà dei polinomi. Consideriamo un polinomio $f \in \mathbf{R}[x]$, di grado $n \geq 1$. Se f è prodotto (punto per punto) di due polinomi g, h di grado > 0 allora l'equazione $f(x) = 0$ diventa $g(x)h(x) = 0$, e, per la *legge di annullamento del prodotto*, si ha $g(x) = 0$ oppure $h(x) = 0$. Le soluzioni delle due nuove equazioni ottenute sono soluzioni anche dell'equazione data, e viceversa.

Un polinomio f di grado ≥ 1 si dice *irriducibile* se non è possibile ottenerlo come prodotto di due polinomi di grado inferiore al suo.

I polinomi irriducibili occupano fra i polinomi il ruolo dei numeri primi in **N**. In particolare, la fattorialità dell'anello $\mathbf{R}[x]$ significa che ogni polinomio di

grado ≥ 1 e non irriducibile si può scomporre in uno ed un solo modo (a meno dell'ordine dei fattori) in un prodotto di fattori monici irriducibili, moltiplicato per il suo coefficiente direttore.

Pertanto potremmo spezzare il problema delle equazioni algebriche in due sottoproblemi:

a) scomporre un polinomio in fattori irriducibili;

b) risolvere l'equazione $f(x) = 0$ quando f è un polinomio irriducibile.

Entrambi i sottoproblemi sono però difficili come il problema di partenza.

TEOREMA 4.7 (Ruffini) Dato il polinomio $f \in \mathbf{R}[x]$, di grado $n \geq 1$, l'equazione $f(x) = 0$ ha una soluzione $x = a$ se e solo se esiste un polinomio q tale che per ogni $x \in \mathbf{R}$ si abbia $f(x) = (x-a)q(x)$.

Dimostrazione. Si divida f per $(x-a)$: si ottiene $f = (x-a)q + r$, dove $r = 0$ oppure r ha grado minore del grado di $(x-a)$, cioè ha grado 0: in ogni caso, dunque, r è una costante. Ma allora $f(a) = (a-a)q(a)+r = r$. Ecco che si ha $r = 0$ se e solo se $f(a) = 0$.

Conseguenze:

- Se si riesce a trovare una radice a, l'equazione $f(x) = 0$ si scinde nelle due equazioni $x-a = 0$ e $q(x) = 0$: la seconda ha grado inferiore di 1 a quello dell'equazione data.
- Il numero delle soluzioni dell'equazione algebrica $f(x) = 0$ non supera il grado di f. Ciò si dimostra per induzione rispetto al grado n di f: se $n = 0$, non ci sono soluzioni e siamo a posto; se $n > 0$, e non ci sono soluzioni siamo pure a posto; altrimenti, data una radice a di f, si ha $f(x) = (x-a)\cdot q(x)$ e, per la legge d'annullamento del prodotto, ogni altra radice di f è radice di q. Poiché q ha grado n-1, per l'ipotesi induttiva ha al massimo n-1 radici, quindi fd ne ha al massimo n.
- Un polinomio irriducibile di grado $n > 1$ non ha mai radici.
- Per un polinomio di grado 2 o 3, l'essere irriducibile equivale a non avere radici. Per gli altri gradi non è vero: per esempio il polinomio $f(x) = x^4+5x^2+6$ non ha radici, essendo somma di numeri positivi, ma si ha $f(x) = (x^2+2)(x^2+3)$.

Si osservi che il risultato sul grado del polinomio e sul numero delle radici dipende dalla legge d'annullamento del prodotto. Se consideriamo le equazioni algebriche in un anello commutativo che non sia un dominio d'integrità, anziché nel campo reale, la situazione è assai diversa. Per esempio, abbiamo visto gli anelli $\mathbf{Z}_m$: per m = 12 (l'*aritmetica dell'orologio*) si consideri l'equazione di secondo grado $6x^2 = 6x$: essa ha sorprendentemente 12 soluzioni! Infatti

- Per ogni x pari, si ha $6x^2 = 0 = 6x$.
- Per ogni x dispari si ha $6x^2 = 6 = 6x$.

Si noti che $\mathbf{Z}_{12}$ non è un dominio d'integrità, poiché $6\cdot 2 = 0$.

EQUAZIONI A COEFFICIENTI RAZIONALI. Sia f(x) = 0 un'equazione algebrica sul campo razionale, con f di grado maggiore di 1. Come trovarne una eventuale radice razionale? Innanzi tutto, si riducono i coefficienti allo stesso denominatore e poi si elimina il denominatore comune, ottenendo una equazione a coefficienti interi. Si raccoglie poi a fattor comune e si elimina il massimo comune divisore dei coefficienti. Il polinomio ottenuto è detto *primitivo*.

TEOREMA 4.7. (Ruffini?) Le eventuali radici razionali del polinomio primitivo f di grado ≥ 1, col temine noto diverso da zero, sono della forma p/q, dove p è un divisore (positivo o negativo) del termine noto, mentre q è un divisore (positivo) del coefficiente direttore.

Dimostrazione. Sia $f(x) = \sum_{k=0}^{n} a_k x^k$ a coefficienti interi e primi tra loro. Sia $\frac{p}{q}$ una sua radice razionale con MCD(p,q) = 1. Sostituiamo $\frac{p}{q}$ al posto di x e riduciamo allo stesso denominatore: $0 = f\left(\frac{p}{q}\right) = \sum_{k=0}^{n} a_k \left(\frac{p}{q}\right)^k \Rightarrow 0 = \sum_{k=0}^{n} a_k p^k q^{n-k}$.

Riduciamo modulo p questo numero intero: tutte le potenze di p si azzerano e rimane solo: $a_0 q^n \equiv 0 \pmod{p}$. Poiché MCD(p, q) = 1 e p divide il prodotto

a_0q^n, allora p deve dividere il termine noto a_0. Se invece si riduce modulo q, si ottiene che q deve dividere il coefficiente direttore a_n.

ESEMPI 4.8 .

4.8.A. $3x^2 + 4x + 1 = 3(x + 1)(x + \frac{1}{3})$.

4.8.B. $x^4 + x^2 + 1$ non ha ovviamente radici, ma è uguale a $(x^2+x+1)(x^2-x+1)$.

4.8.C. $x - 2$ è irriducibile, pur avendo una radice.

4.8.D. Data l'equazione $5x^4 - 24x^3 + x = 0$, raccogliamo x a fattor comune ed otteniamo le due equazioni $x = 0$ e $5x^3 - 24x^2 + 1 = 0$. Quest'ultima ha i coefficienti interi coprimi. Le eventuali radici razionali sono da ricercarsi nell'insieme $\left\{1, -1, \frac{1}{5}, -\frac{1}{5}\right\}$. Oltre a 0, si verifica così che $-\frac{1}{5}$ è l'unica altra radice razionale.

Torniamo ora alle equazioni a coefficienti reali. In qualche caso si possono risolvere, eventualmente con qualche artificio.

TEOREMA 4.9. a) Per ogni $a\in\mathbf{R}^+$, per ogni intero $n > 1$, esiste uno ed un solo $u\in\mathbf{R}^+$ tale che $u^n = a$. Tale elemento si denota con $\sqrt[n]{a}$.

b) Per ogni intero pari $n = 2k$, l'equazione "binomia" $x^n = a$ se $a > 0$ ha due soluzioni, opposte tra loro; se $a < 0$ è impossibile.

c) Per ogni $a\in\mathbf{R}$, per ogni intero dispari $n = 2k+1$, l'equazione "binomia" $x^n = a$ ha una ed una sola soluzione.

Schema della dimostrazione. a) Supponiamo dapprima $a > 1$. Definiamo due insiemi E ed F nel modo seguente:

$$E = \{x\in\mathbf{R} \mid x \geq 1, x^n < a\}, F = \{x\in\mathbf{R} \mid x \geq 1, x^n > a\}.$$

I due insiemi E ed F sono *separati* e fra di essi vi è un solo *elemento di separazione*, che denoteremo con u. Si ha necessariamente $u^n = a$.

Se invece $a < 1$, si consideri $a' = 1/a$, che è > 1: trovato u' tale che $u'^n = a'$, si può porre infine $u = 1/u'$.

b) Se $a > 0$ si ha $x = \pm\sqrt[n]{a}$. Se $a < 0$, l'equazione è impossibile, dato che per ogni $x \in \mathbf{R}$, $x^n = x^{2k} \geq 0$.

c) Sia $n = 2k+1$. La funzione $f(x) = x^n$ ha per derivata $f'(x) = n \cdot x^{n-1} = (2k+1) \cdot x^{2k}$. Tale derivata è positiva sui due intervalli $]-\infty, 0[$ e $]0, +\infty[$, pertanto f è crescente su ciascuno di essi. Dato poi che per $x < 0$ f è negativa e per $x > 0$ è positiva, allora f è crescente su tutto **R**, dunque è iniettiva. Ne segue che l'equazione $x^n = a$ ha un'unica soluzione. Più precisamente, applicando a), segue che se $a > 0$, $x = \sqrt[n]{a}$, se $a = 0$ si ha $x = 0$ e se $a < 0$, si ha $x = -\sqrt[n]{|a|}$. È però consuetudine indicare con $\sqrt[n]{a}$ la soluzione in ogni caso.

OSSERVAZIONE 4.10. Si consideri l'equazione "trinomia" $a \cdot x^{2n} + b \cdot x^n + c = 0$, $a \neq 0$. Si ponga $y = x^n$, in modo da ottenere *l'equazione ausiliaria* $a \cdot y^2 + b \cdot y + c = 0$, di II grado. Se il suo discriminante è < 0, è impossibile. Se è ≥ 0, si otterranno due soluzioni (eventualmente uguali) y_1, y_2. Si arriva dunque alla coppia di equazioni binomie $x^n = y_1$, $x^n = y_2$, da risolvere come ricordato nel teorema 4.9.

Riassumendo: esistono formule risolutive per equazioni algebriche di primo e secondo grado col discriminante ≥ 0; esiste una soluzione per l'equazione binomia $x^n = a$; con qualche artificio si possono risolvere alcuni tipi di equazioni di grado maggiore di 2, riconducibili a equazioni di II grado o binomie. Se i coefficienti sono interi e coprimi, si ha un numero finito di possibilità per trovare almeno le soluzioni razionali. Ma **R** non risolve tutti i problemi: l'equazione $x^2+1 = 0$ non ha soluzione, e siamo da capo. Pertanto, passiamo decisamente al campo complesso.

LEMMA 4.11. L'ideale generato dal polinomio x^2+1 è massimale in $\mathbf{R}[x]$, perciò il quoziente $\mathbf{R}[x]/(x^2+1)$ è un campo.

Dimostrazione. Poiché questo polinomio è di II grado e non ha radici, allora è irriducibile. Ne segue che l'ideale $I = (x^2+1)$ deve essere massimale, per il teorema 3.8. ed allora il quoziente è un campo, per il teorema 2.7.

Il quoziente $\mathbf{R}[x]/(x^2+1)$ ha per elementi i laterali dell'ideale $I = (x^2+1)$, quindi del tipo $I + f$. Se dividiamo f per x^2+1, otteniamo il quoziente q ed il resto r, che ha la forma a+bx, con a, b reali opportuni, eventualmente nulli. Allora:

$$I + f = I + \underbrace{\left(x^2+1\right)\cdot q}_{\in I} + \left(a+bx\right) = I + \left(a+bx\right) = \left(I+a\right) + \left(I+b\right)\left(I+x\right).$$

Osserviamo che l'applicazione $\Phi:\mathbf{R}\to \mathbf{R}[x]/(x^2+1)$, che associa ad ogni numero reale a il laterale I+a è un monomorfismo di anelli, perciò l'immagine è un campo isomorfo ad **R**, e possiamo identificare il numero reale a col laterale I+a. Inoltre, denotiamo con i il laterale I+x; si ha:

$$i^2 = \left(I+x\right)^2 = I + x^2 = I + \left(x^2+1\right) - 1 = I + \left(-1\right) = -1$$

Dunque, gli elementi del campo quoziente si scrivono nella forma $a+bi$, con a e b reali ed i tale che $i^2 = -1$. Tale campo si denota con **C** ed è chiamato *campo complesso*. L'elemento i si chiama *unità immaginaria*. Si osservi che la scrittura $a+bi$ per un numero complesso è unica: per l'unicità del resto della divisione, in ogni laterale I+f c'è un solo polinomio della forma a+bx. Dunque,

$$a + bi = a' + b'i \Leftrightarrow \begin{cases} a = a' \\ b = b' \end{cases}$$

Per altre costruzioni si veda il capitolo sugli insiemi numerici. Ricordiamo solo le regole di calcolo, ricavate dalla costruzione precedente:

$$\begin{cases} \left(a+bi\right) + \left(c+di\right) = \left(a+c\right) + \left(b+d\right)i \\ \left(a+bi\right)\cdot\left(c+di\right) = \left(ac-bd\right) + \left(ad+bc\right)i \end{cases}.$$

Lo zero è 0+0i, l'unità è 1+0i, mentre l'inverso di un numero complesso non nullo è $\left(a+bi\right)^{-1} = \dfrac{a}{a^2+b^2} - \dfrac{b}{a^2+b^2}i$. Si osservi che il denominatore è nullo se e solo se a = b = 0, ossia solo per lo zero.

Il numero $\overline{a+bi} = a - bi$ è detto *complesso coniugato* di a+bi. Si ha:

PROPOSIZIONE 4.12. Denotiamo con $\overline{z}$ il coniugato del numero complesso z = a+bi. Allora:

a) $z + \overline{z}$ e $z\cdot\overline{z}$ sono numeri reali

b) La funzione che a z associa $\overline{z}$ è un automorfismo del campo **C**.

Dimostrazione. a) $z+\overline{z}=2a$, $z\cdot\overline{z}=a^2+b^2$ sono numeri reali.

b) Intanto, $\overline{1}=\overline{1+0i}=1-0i=1$. Poi, per ogni $z=a+bi$, $w=c+di$ si ha:

$$\overline{z+w}=\overline{(a+c)+(b+d)i}=(a+c)-(b+d)i=(a-bi)+(c-di)=\overline{z}+\overline{w},$$

$$\overline{z\cdot w}=\overline{(ac-bd)+(ad+bc)i}=(ac-bd)-(ad+bc)i=\overline{z}\cdot\overline{w}$$

Pertanto, il coniugio è un omomorfismo di anelli. Il solo numero complesso che ha 0 per coniugato è 0 stesso, quindi il coniugio è iniettivo. Inoltre, $z=\overline{(\overline{z})}$ dice che il coniugio è anche suriettivo, ed è quindi un automorfismo di **C**. Inoltre, è inverso di se stesso.

Un *polinomio*, o *funzione polinomiale*, sul campo complesso è una funzione $f:\mathbf{C}\to\mathbf{C}$, per la quale esistono $\alpha_0, \alpha_1, \ldots, \alpha_n\in\mathbf{C}$, tali che per ogni $z\in\mathbf{C}$ si ha $f(z)=\sum_{k=0}^{n}\alpha_k z^k$. I numeri $\alpha_0, \alpha_1, \ldots$ sono detti *coefficienti*. Tra queste funzioni c'è la costante nulla **0**, ottenibile ponendo = 0 tutti i coefficienti.

Denotiamo con **C**[z] (o con **C**[x]) l'insieme dei polinomi a coefficienti complessi. Il modo di sommare e moltiplicare i polinomi è come in **R**[x]: si considerano le operazioni punto per punto già descritte per **R** nella Proposizione 4.1. Esse danno luogo ad un anello commutativo costruito sui complessi.

TEOREMA 4.13. (Principio d'identità dei polinomi a coefficienti complessi).

a) Il solo modo di rappresentare la costante nulla come polinomio è quello con i coefficienti tutti nulli.

b) Siano f, g due polinomi, $f(z)=\sum_{k=0}^{n}\alpha_k z^k$, $g(z)=\sum_{k=0}^{m}\beta_k z^k$. Si ha f = g (ossia, per ogni $z\in\mathbf{C}$ si ha f(z) = g(z)) se e solo se per ogni $k\geq 0$ si ha $\alpha_k=\beta_k$.

Dimostrazione. Sia $\mathbf{0}(z) = \sum_{k=0}^{n} \alpha_k z^k$, $n \geq 0$. Per ogni k, $0 \leq k \leq n$, sia $\alpha_k = a_k + b_k i$.

Allora, $\forall z \in \mathbf{C}$, $0 + 0i = \mathbf{0}(z) = \sum_{k=0}^{n} a_k z^k + i \sum_{k=0}^{n} b_k z^k \Rightarrow \begin{cases} \sum_{k=0}^{n} a_k z^k = 0 \\ \sum_{k=0}^{n} b_k z^k = 0 \end{cases}$.

Queste due uguaglianze tra polinomi a coefficienti reali in particolare devono valere per ogni $z = x+0i$, cioè per ogni numero reale, ed allora per il principio d'identità in $\mathbf{R}[x]$ segue $\begin{cases} a_k = 0 \\ b_k = 0 \end{cases}$, ossia $\alpha_k = 0$ per ogni $k \geq 0$.

Torniamo ora alle equazioni algebriche. **Il *teorema fondamentale dell'algebra***, enunciato e provato (quasi completamente) dall'enciclopedista *D'Alembert*, afferma che **in C ogni equazione algebrica f(x) = 0 di grado ≥ 1 ha almeno una soluzione.** Di questo teorema non si riporta la dimostrazione. Pertanto, i soli polinomi irriducibili in $\mathbf{C}[x]$ sono quelli di I grado.

Come corollario, applicando il teorema di Ruffini, si ottiene che **ogni polinomio di grado n ≥ 1 si scompone in C[x] in n fattori di primo grado.** Si esprime questa proprietà dicendo che il campo complesso è *algebricamente chiuso*.

Vediamo ora i polinomi a coefficienti reali come caso particolare di polinomi a coefficienti complessi. Il teorema fondamentale dell'algebra ha come conseguenza la classificazione dei polinomi irriducibili in $\mathbf{R}[x]$.

COROLLARIO 4.14.

a) Se un polinomio a coefficienti reali ha una radice complessa, allora ha anche la radice complessa coniugata.
b) I soli polinomi irriducibili a coefficienti reali sono quelli di I grado e quelli di II grado col discriminante negativo.
c) I polinomi a coefficienti reali e di grado dispari hanno necessariamente almeno una radice reale.

Dimostrazione. a) Sia α una radice complessa del polinomio $f(z) = \sum_{k=0}^{n} a_k z^k$ a coefficienti reali. Allora, ricordando che il coniugio è un automorfismo, si ha:

$$0 = \overline{0} = \overline{\sum_{k=0}^{n} a_k \alpha^k} = \sum_{k=0}^{n} a_k \overline{\alpha}^k$$

e allora anche $\overline{\alpha}$ è radice di f.

b) Sia f un polinomio irriducibile a coefficienti reali, di grado ≥ 2. Nel campo complesso esso ha una radice $\alpha = a+bi$, quindi ha anche la coniugata $\overline{\alpha}$, dunque è multiplo del prodotto $(z-\alpha)\cdot(z-\overline{\alpha}) = z^2 - (2a)\cdot z + (a^2+b^2)$, che è di II grado ed ha i coefficienti reali. Pertanto, se f ha grado > 2 è riducibile. Poiché questo polinomio di II grado ha il discriminante $\Delta = 4a^2 - 4(a^2+b^2) = -4b^2 < 0$, è irriducibile in $\mathbf{R}[x]$.

c) La fattorialità di $\mathbf{R}[x]$ assicura che ogni polinomio di grado ≥ 1 si scompone in fattori irriducibili, che per b) sono o di I grado oppure di II grado col discriminante negativo. Allora se il grado è dispari ci deve essere almeno un fattore di I grado, quindi una radice reale.

OSSERVAZIONE. Entro $\mathbf{C}$ possiamo cercare anche le soluzioni di tutte le equazioni algebriche $f(x) = 0$, con $0 \neq f \in \mathbf{Q}[x]$. E qui si ha qualche sorpresa: queste soluzioni costituiscono solo una piccola parte del campo complesso, che denoteremo qui con $\overline{\mathbf{Q}}$. Essa costituisce un sottocampo di $\mathbf{C}$, detto *campo dei numeri algebrici*: è numerabile come $\mathbf{Q}$, a differenza di $\mathbf{C}$ che contiene anche $\mathbf{R}$ e quindi non lo è (come noto dai corsi di Analisi Matematica). Pertanto, i numeri algebrici non solo non riempiono tutto $\mathbf{C}$, ma sono un'esigua minoranza. Si ha inoltre che ogni equazione algebrica di grado > 0 a coefficienti in $\overline{\mathbf{Q}}$ ha sempre una soluzione in $\overline{\mathbf{Q}}$, quindi anche $\overline{\mathbf{Q}}$ è algebricamente chiuso. Perciò $\mathbf{C}$ è largamente sovrabbondante per le equazioni a coefficenti razionali, ma mentre è facile rappresentarlo geometricamente mediante i punti del piano cartesiano, non altrettanto accade per il campo $\overline{\mathbf{Q}}$. Dunque, l'ambiente per risolvere le equazioni algebriche resta comunque $\mathbf{C}$.

Si chiamano *numeri trascendenti* i numeri complessi non algebrici su **Q**. Come detto, la quasi totalità dei numeri complessi è trascendente, ma un problema davvero difficile è vedere se un dato numero non razionale sia trascendente o algebrico.

ESEMPIO 4.15. Sia $k = \sqrt{5-\sqrt[3]{2}}+4$: è algebrico o trascendente?

Con qualche passaggio si ha: $k-4 = \sqrt{5-\sqrt[3]{2}}$, da cui :

$$(k-4)^2 = 5-\sqrt[3]{2},$$

$$[(k-4)^2-5]^3 = -2,$$

$$(k^2 - 8k + 11)^3 + 2 = 0,$$

quindi k è soluzione dell'equazione $(x^2 - 8x + 11)^3 + 2 = 0$ e dunque è algebrico.

Ma, il numero $\pi = 3{,}14159...$ è algebrico o trascendente? Si può dimostrare che è trascendente, ed anche $e = 2{,}71...$ (il numero di Nepero), le sue potenze con esponente razionale, i logaritmi naturali di numeri razionali, seno e coseno di numeri razionali lo sono.

Radici multiple. Siano f un polinomio ed u una sua radice: u si dice *radice di molteplicità m* se f è divisibile per $(x-u)^m$ ma non per $(x-u)^{m+1}$. Allora si potrà scrivere $f(x) = (x-u)^m q(x)$, con $q(u) \neq 0$. Se $m = 1$, u si dice *radice semplice*. Se $m > 1$, u si dice *radice multipla.* Per $m = 2$, u si dice *radice doppia*.

Le equazioni di secondo grado $ax^2 + bx + c = 0$ (con $a \neq 0$), possono avere radici doppie: ciò avviene unicamente quando $\Delta = b^2 - 4ac = 0$.

In tal caso si ha: $ax^2 + bx + c = a(x + \frac{b}{2a})^2$.

COROLLARIO 4.16. a) Nel campo complesso e nel campo $\overline{\mathbf{Q}}$ dei numeri algebrici, la somma delle molteplicità delle radici di un polinomio è uguale al grado del polinomio.

b) In **Q** ed in **R**, la somma delle molteplicità delle radici è minore o uguale al grado del polinomio.

Il seguente teorema caratterizza i polinomi reali con radici multiple e fa uso della nozione di derivata f' di un polinomio. Sia $f(x) = \sum_{i=0}^{n} a_i x^i$, di grado $n \geq 1$.

Dall'analisi matematica si sa che $f'(x) = \sum_{i=0}^{n-1}(i+1)a_{i+1}x^i$. Ricordiamo poi che il massimo comune divisore di due polinomi (non nulli) f e g è un polinomio d divisore sia di f che di g e multiplo di ogni altro divisore comune; non è unico, ma ogni altro massimo comune divisore di f e g si ottiene moltiplicando d per un numero reale non nullo. In particolare, si può sempre supporre d monico.

TEOREMA 4.17. Un polinomio $f \in \mathbf{R}[x]$ di grado ≥ 1 ha una radice multipla u se e solo se u è radice anche di f'. In tal caso, il polinomio massimo comune divisore d tra f e la sua derivata f' ha grado ≥ 1 ed ogni sua radice è radice multipla per f.

Dimostrazione. Supponiamo che f abbia la radice multipla u di molteplicità $m > 1$. Allora $f(x) = (x-u)^m q(x)$, per cui, come noto dall'Analisi matematica, si ha:

$$f'(x) = m(x-u)^{m-1}q(x)+(x-u)^m q'(x) = (x-u)^{m-1}(mq(x)+(x-u)q'(x))$$

quindi u è radice anche di f'(x) e inoltre $(x-u)^{m-1}$ è un divisore comune di f ed f', per cui $(x-u)^{m-1}$ divide $d = MCD(f, f')$.

Se invece si ha $f(x) = (x-u)q(x)$, con $q(u) \neq 0$, allora $f'(x) = q(x)+(x-u)q'(x)$ non si annulla per $x = u$.

Ne segue che u non è radice neppure di d: infatti, poiché d divide f ed f', ogni sua radice è radice comune ad f ed f' e quindi è radice multipla di f.

OSSERVAZIONE 4.18. Anche nel campo complesso si può definire la derivata di un polinomio, ponendo $\left(\sum_{k=0}^{n}\alpha_k z^k\right)' = \sum_{k=1}^{n}k\alpha_k z^{k-1}$. Si dimostra che per la derivata di un prodotto di polinomi vale la stessa regola: $(f \cdot g)' = f \cdot g' + f' \cdot g$; di conseguenza, si ricava per le radici multiple un teorema analogo a 4.15.

Il massimo comune divisore d di due polinomi f e g si può calcolare col metodo delle divisioni successive, per cui si trova senza eccessive difficoltà. Se $d \neq 1$, dividendo f per d si ottiene un polinomio h che ha tutte le radici di f, ma le ha semplici, e quindi se f ha radici multiple, h ha grado minore di quello di f.

ESEMPIO 4.19. - Sia $f(x) = x^6-x^5-11x^4+13x^3+26x^2-20x-24$. Allora

$$f'(x) = 6x^5-5x^4-44x^3+39x^2+52x-20.$$

Con un poco di calcoli segue: $d(x) = x^3-3x^2+4$. Pertanto, le radici di d(x) sono tutte e sole le radici multiple di f. Il quoziente $h(x) = f(x)/d(x) = x^3+2x^2-5x-6$ ha le stesse radici di f, ma le ha tutte semplici. Poiché i coefficienti sono interi ed h è monico, si possono cercare le radici intere di h nell'insieme $\{\pm 1, \pm 2, \pm 3, \pm 6\}$ dei divisori di 6. Con un poco di pazienza si trovano le tre radici 2, -1, -3. Poiché 2 e -1 sono radici (doppia e semplice) anche di d, allora sono multiple per f, rispettivamente tripla e doppia.

Anche nel campo complesso si possono risolvere le equazioni binomie $z^n = \alpha,\ \alpha \neq 0$. Siano $z = x + i \cdot y$ e sia $\alpha = a + i \cdot b$. Il calcolo di z^n con la formula di Newton del binomio e il successivo uguagliare le parti reale e immaginaria di z^n e di α porta ad un sistema di due equazioni di grado n nelle due incognite x, y, ma se $n > 2$ è proibitivo tentare di risolverlo. C'è tuttavia un altro approccio.

Nel capitolo degli insiemi numerici si è vista la forma trigonometrica dei numeri complessi a+i·b. Posto $\rho = \sqrt{a^2 + b^2}$, $\varphi = \operatorname{arctg}\frac{b}{a}$, si ottiene $\begin{cases} a = \rho \cdot \cos(\varphi) \\ b = \rho \cdot \operatorname{sen}(\varphi) \end{cases}$, per cui $a + i\ b = \rho\cdot(\cos\varphi + i\ \operatorname{sen}\varphi)$. Ricordiamo che ρ si chiama *modulo* e φ si chiama *argomento* del numero complesso a+ib. Tuttavia, l'argomento non è individuato, perché si ha, per ogni k intero:

$$a + i\ b = \rho\cdot(\cos\varphi + i\ \operatorname{sen}\varphi) = \rho\cdot(\cos(\varphi+2\pi k) + i\ \operatorname{sen}(\varphi+2\pi k))$$

Pertanto, si ha $a + i \cdot b = a' + i \cdot b' \Leftrightarrow \begin{cases} \rho = \rho' \\ \varphi = \varphi' + 2k\pi,\ k \in \mathbf{Z} \end{cases}$

Ricordiamo poi la formula di De Moivre, valida per ogni $n \geq 0$:

$$\left(\rho\left(\cos\varphi + i \cdot \operatorname{sen}\varphi\right)\right)^n = \rho^n\left(\cos\left(n\varphi\right) + i \cdot \operatorname{sen}\left(n\varphi\right)\right)$$

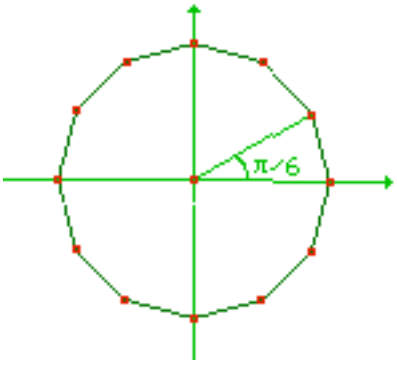
Ciò posto, scriviamo z ed α in forma trigonometrica: $\begin{cases} z = r \cdot \left(\cos\theta + i \cdot \operatorname{sen}\,\theta\right) \\ \alpha = \rho \cdot \left(\cos\varphi + i \cdot \operatorname{sen}\,\varphi\right) \end{cases}$, calcoliamo $z^n = r^n \cdot \left(\cos n\theta + i \cdot \operatorname{sen}\, n\theta\right)$ ed imponiamo $z^n = \alpha$: $\begin{cases} r^n = \rho \\ n\theta = \varphi + 2k\pi \end{cases}$. La prima equazione è binomia in **R**, e poiché r e ρ sono positivi, allora $r = \sqrt[n]{\rho}$. La

seconda equazione dà $\theta = \frac{\varphi + 2k\pi}{n}$, ma tuttavia le soluzioni non sono infinite, dato che l'equazione ha grado n. In effetti, se dividiamo k per n, ottenendo $k = n \cdot q + h$, con $0 \le h < n$, allora $\theta = \frac{\varphi + 2k\pi}{n} = \frac{\varphi + 2h\pi}{n} + 2q\pi$, dunque ci sono solo n soluzioni, e sono distinte: $z_h = \sqrt[n]{\rho}\left(\cos\frac{\varphi + 2h\pi}{n} + i \cdot \operatorname{sen}\frac{\varphi + 2h\pi}{n}\right)$, $0 \le h < n$.

TEOREMA 4.20. Per ogni $n \ge 1$, le radici complesse n-esime di 1 costituiscono un gruppo ciclico, $\mathbf{C}_n$, d'ordine n.

Dimostrazione. Trattandosi di un insieme finito con n elementi, contenente 1, basta provare che $\mathbf{C}_n$ è chiuso rispetto alla moltiplicazione. Siano u, v due radici n-esime di 1, allora $u^n = v^n = 1 \Rightarrow (u \cdot v)^n = u^n \cdot v^n = 1$. Per dimostrare che è ciclico, tenendo presente che 1 ha modulo 1 ed argomento 0, consideriamo le sue radici, che hanno la forma $\varepsilon_h = \cos\frac{2h\pi}{n} + i \cdot \operatorname{sen}\frac{2h\pi}{n}$, $0 \le h < n$. Per la formula di De Moivre, si ha $(\varepsilon_1)^h = \left(\cos\frac{2\pi}{n} + i \cdot \operatorname{sen}\frac{2\pi}{n}\right)^h = \cos\frac{2h\pi}{n} + i \cdot \operatorname{sen}\frac{2h\pi}{n} = \varepsilon_h$ per ogni h, quindi $\mathbf{C}_n$ è generato da ε_1.

OSSERVAZIONE. Le radici n-esime di 1, avendo modulo 1, appartengono alla circonferenza di centro O = (0,0) e raggio 1, e differiscono tra loro per un angolo di ampiezza $\frac{2\pi}{n}$; sono quindi, nel piano, i vertici di un poligono regolare con n lati, un vertice dei quali è (1, 0).



Le radici dodicesime di 1:

$\varepsilon_1 = \frac{\sqrt{3}}{2} + \frac{1}{2} \cdot i$

Il campo dei quozienti di un dominio d'integrità. Esiste un campo "più grande" del campo complesso? La domanda è legittima, ma la risposta sembra complicata. Infatti, la tecnica usata per passare da **R** a **C** qui non funziona, in quanto i soli polinomi irriducibili in **C**[z] sono quelli di I grado, ed il campo quoziente rispetto all'ideale da essi generato è isomorfo a **C**. Serve un'altra tecnica, che tuttavia è nelle conoscenze anche degli scolari: le frazioni, con le loro operazioni ed equivalenze: il *campo dei quozienti* di un dominio d'integrità $(A, +, \cdot, 1_A)$.

Partiamo dall'insieme F delle coppie ordinate (a,b) di elementi di A, con $b \neq 0_A$: chiameremo *frazioni* queste coppie e le indicheremo con $\frac{a}{b}$. Definiamo tra le frazioni le due operazioni seguenti: $\frac{a}{b}+\frac{c}{d}=\frac{a\cdot d+b\cdot c}{b\cdot d}$, $\frac{a}{b}\cdot\frac{c}{d}=\frac{a\cdot c}{b\cdot d}$.

La definizione è corretta perché $bd \neq 0_A$ in quanto A è un dominio d'integrità. È un esercizio provare che l'insieme F delle frazioni è un monoide commutativo rispetto ad entrambe queste operazioni. Vediamo solo la proprietà associativa dell'addizione:

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{a\cdot d+b\cdot c}{b\cdot d}+\frac{e}{f}=\frac{\left(a\cdot d+b\cdot c\right)\cdot f+\left(b\cdot d\right)\cdot e}{\left(b\cdot d\right)\cdot f}=\frac{a\cdot d\cdot f+b\cdot c\cdot f+b\cdot d\cdot e}{b\cdot d\cdot f}$$

$$\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}+\frac{c\cdot f+d\cdot e}{d\cdot f}=\frac{a\cdot\left(d\cdot f\right)+b\cdot\left(c\cdot f+d\cdot e\right)}{\left(b\cdot d\right)\cdot f}=\frac{a\cdot d\cdot f+b\cdot c\cdot f+b\cdot d\cdot e}{b\cdot d\cdot f}$$

Gli elementi neutri sono rispettivamente $\frac{0_A}{1_A}$ e $\frac{1_A}{1_A}$.

Definiamo ora in questo insieme di frazioni la seguente relazione ~:

$$\frac{a}{b}\sim\frac{a'}{b'}\Leftrightarrow a\cdot b'=b\cdot a'.$$

Si verifica facilmente che questa relazione è di equivalenza. Vediamo solo la proprietà transitiva: siano $\frac{a}{b}\sim\frac{a'}{b'}$, $\frac{a'}{b'}\sim\frac{a''}{b''}$. Allora: $\frac{a}{b}\sim\frac{a'}{b'}\Leftrightarrow a\cdot b'=b\cdot a'$, $\frac{a'}{b'}\sim\frac{a''}{b''}\Leftrightarrow a'\cdot b''=b'\cdot a''$. Ne segue: $\begin{cases}a\cdot b'=b\cdot a'\\ a'\cdot b''=b'\cdot a''\end{cases}\Rightarrow a\cdot b'\cdot a'\cdot b''=b\cdot a'\cdot b'\cdot a''$, da cui semplificando per b', che è $\neq 0_A$ segue: $a\cdot a'\cdot b''=b\cdot a'\cdot a''$. Ora, se a' $\neq 0_A$ segue $a\cdot b''=b\cdot a''\Rightarrow\frac{a}{b}\sim\frac{a''}{b''}$; se a' = 0_A segue a = a" = 0_A e di nuovo $\frac{a}{b}\sim\frac{a''}{b''}$.

Si ha $\left[\frac{0_A}{1_A}\right] = \left\{\frac{0_A}{b} \;\middle|\; b \neq 0_A\right\}$ e $\left[\frac{1_A}{1_A}\right] = \left\{\frac{b}{b} \;\middle|\; b \neq 0_A\right\}$, come si vede subito.

Questa relazione è compatibile con le due operazioni. Siano infatti $\frac{a}{b} \sim \frac{a'}{b'}$, $\frac{c}{d} \sim \frac{c'}{d'}$.

Allora, per la moltiplicazione si ha subito:

$$\begin{cases} a \cdot b' = b \cdot a' \\ c \cdot d' = d \cdot c' \end{cases} \Rightarrow a \cdot b' \cdot c \cdot d' = b \cdot a' \cdot d \cdot c' \Rightarrow \frac{a \cdot c}{b \cdot d} \sim \frac{a' \cdot c'}{b' \cdot d'}$$

Per l'addizione è più complicato:

$$(a \cdot d + b \cdot c) \cdot (b' \cdot d') = a \cdot d \cdot b' \cdot d' + b \cdot c \cdot b' \cdot d' = (a \cdot b') \cdot d \cdot d' + (c \cdot d') \cdot b \cdot b' =$$

$$= (b \cdot a') \cdot d \cdot d' + (d \cdot c') \cdot b \cdot b' = (a' \cdot d' + c' \cdot b') \cdot (b \cdot d),$$

quindi $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d} \sim \frac{a' \cdot d' + b' \cdot c'}{b' \cdot d'} = \frac{a'}{b'} + \frac{c'}{d'}$.

Consideriamo quindi la struttura quoziente F/~ : essa è un monoide rispetto ad entrambe le operazioni, con elementi neutri rispettivamente $\left[\frac{0_A}{1_A}\right]$ e $\left[\frac{1_A}{1_A}\right]$, ma, di più ogni suo elemento $\left[\frac{a}{b}\right]$ ha l'opposto $\left[\frac{-a}{b}\right]$ e, se $a \neq 0_A$, ha anche l'inverso moltiplicativo, $\left[\frac{b}{a}\right]$. Infine, la moltiplicazione quoziente è distributiva rispetto all'addizione quoziente; infatti si ha

$$\left(\frac{a}{b} + \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{a \cdot d + b \cdot c}{b \cdot d} \cdot \frac{e}{f} = \frac{a \cdot d \cdot e + b \cdot c \cdot e}{b \cdot d \cdot f}, \quad \frac{a}{b} \cdot \frac{e}{f} + \frac{c}{d} \cdot \frac{e}{f} = \frac{a \cdot e \cdot d \cdot f + c \cdot e \cdot b \cdot f}{b \cdot f \cdot d \cdot f},$$

e le due frazioni ottenute sono equivalenti, dato che

$$(a \cdot d \cdot e + b \cdot c \cdot e) \cdot (b \cdot f \cdot d \cdot f) = (a \cdot e \cdot d \cdot f + c \cdot e \cdot b \cdot f) \cdot (b \cdot d \cdot f),$$

come si vede eseguendo le due moltiplicazioni.

Allora, la struttura quoziente è un campo, che si denota con Q(A). Il sottoinsieme $\left\{\left[\frac{a}{1_A}\right] \;\middle|\; a \in A\right\}$ costituisce un sottoanello di Q(A), come si verifica facilmente, e la funzione Φ:A→Q(A), definita da $\Phi(a) = \left[\frac{a}{1_A}\right]$, è un monomorfismo di anelli. Inoltre, per ogni $\left[\frac{a}{b}\right] \in Q(A)$ si ha $\left[\frac{a}{b}\right] = \left[\frac{a}{1_A}\right] \cdot \left[\frac{1_A}{b}\right] = \left[\frac{a}{1_A}\right] \cdot \left[\frac{b}{1_A}\right]^{-1}$. Per questa ragione Q(A) è detto *campo dei quozienti di A*.

Si può anche dimostrare che per ogni campo K che contenga l'anello A come sottoanello, l'intersezione di tutti i sottocampi contenenti A è un sottocampo isomorfo a Q(A), quindi Q(A) è in questo senso il campo "generato" da A.

Se l'anello A è fattoriale, gli elementi di Q(A) di norma si rappresentano mediante frazioni $\frac{a}{b}$ *ridotte ai minimi termini*, ossia tali che $\mathrm{MCD}(a, b) = 1_A$.

Questa costruzione, applicata all'anello **Z**, produce il campo razionale **Q**. Applicata all'anello dei polinomi **R**[x], che è un dominio d'integrità, dà luogo al *campo* **R**(x) *delle frazioni algebriche a coefficienti reali.* Naturalmente, si può applicare anche all'anello **C**[z], ed ecco un campo, **C**(z), che contiene un sottoanello isomorfo a **C**[z], il quale a sua volta contiene un sottoanello isomorfo a **C**. Ne segue che **C**(z) è un campo "più grande" di **C**.

OSSERVAZIONE. Non si confondano le frazioni algebriche $\frac{f(x)}{g(x)}$, in cui g(x) non è il polinomio nullo e che sono coppie ordinate (f(x), g(x)) di polinomi scritte in un altro modo, con le funzioni *razionali fratte*, della forma $\frac{f(x)}{g(x)}$, dove f e g sono funzioni polinomiali ed x∈**R** è tale che g(x) ≠ 0. Il loro aspetto è simile, e ciò porta a confusioni non irrilevanti, a causa principalmente del fatto che il dominio delle funzioni razionali fratte non è in generale tutto **R**, e quindi si devono imporre condizioni prima di semplificare, sommare, moltiplicare o invertire. In altre parole, i passaggi, che in **R**(x) si compiono senza problemi, nella manipolazione di funzioni razionali fratte debbono essere eseguiti con molta cautela.

Per esempio, le due frazioni algebriche $\frac{1}{1}$ e $\frac{x}{x}$ sono equivalenti e rappresentano lo stesso elemento di **R**(x), mentre le due funzioni razionali 1 e $\frac{x}{x}$ non sono uguali: la seconda è definita solo su **R**\{0} e coincide con la *restrizione* della costante 1 ad **R**\{0}.

§ 5 – ANELLI DI POLINOMI

Nel campo reale **R** abbiamo definito un *polinomio* come una particolare funzione "polinomiale" f:**R**→**R**, per la quale esistono numeri reali $a_0, a_1, \ldots, a_n \in \mathbf{R}$, detti *coefficienti*, tali che per ogni x∈**R**, $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$. Rispetto alle operazioni "punto per punto", l'insieme delle funzioni polinomiali costituisce un anello, denotato con **R**[x] e chiamato *anello dei polinomi in una variabile a coefficienti reali*. Vale in esso il *principio d'identità dei polinomi*, secondo il quale due polinomi sono uguali come funzioni se e solo se hanno gli stessi coefficienti.

Questo modello lo abbiamo applicato anche al campo complesso ed ai suoi sottocampi, compreso il campo razionale. Tuttavia, non è "esportabile" ad un anello commutativo qualsiasi, come mostra l'esempio seguente:

ESEMPIO 5.1. Nell'anello $\mathbf{Z}_{12}$ (isomorfo all'anello delle classi di resti mod 12) consideriamo la funzione polinomiale $f(x) = 6x^2 + 6x$. E' immediato verificare che si ha f(x) = 0 per ogni $x \in \mathbf{Z}_{12}$. Dunque, f non è proprio quello che vorremmo chiamare "polinomio".

Cerchiamo un'altra via, che ci farà abbandonare il ruolo di "variabile" per la x, per sostituirlo col termine "indeterminata". Sia dunque A un anello commutativo. Cerchiamo di definire l'anello A[x] dei polinomi nell'*indeterminata* x ed a coefficienti in A. Cominciamo con il considerare un anello commutativo B che contenga propriamente A come sottoanello. Si ha innanzi tutto $\begin{cases} 0_B = 0_A \\ 1_B = 1_A \end{cases}$.
Sia ora x un elemento di B non appartenente ad A. Allora B contiene tutte le potenze x^n, n∈**N**, ed i loro prodotti $a \cdot x^n$ per gli elementi di A. In particolare si ha: $\begin{cases} 0_A \cdot x^n = 0_A \\ 1_A \cdot x^n = x^n \end{cases}$. Inoltre, B contiene anche le somme di questi termini. In definitiva, B contiene tutti gli elementi della forma $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$,

dove si ha $n \geq 0$ ed i *coefficienti* a_i, $0 \leq i \leq n$, appartenenti ad A. Diremo *espressioni polinomiali* questi elementi.

Siano $f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ e $g = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$ due di queste espressioni, con $m \leq n$. Allora, posto $b_{m+1} = \ldots = b_n = 0_A$, si ha:

- $f + g = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots + (a_n + b_n)x^n$
- $f \cdot g = (a_0b_0) + (a_1b_0 + a_0b_1)x + \ldots + \left(\sum_{i=0}^{k} a_{k-i}b_i\right)x^k + \ldots + (a_nb_m)x^{m+n}$
- $-f = (-a_0) + (-a_1)x + (-a_2)x^2 + \ldots + (-a_n)x^n$
- $\forall a \in A$ si ha : $a = a + 0_A \cdot x + \ldots + 0_A \cdot x^n$

Ossia, somme, prodotti, opposti di espressioni polinomiali sono espressioni polinomiali, ed anche gli elementi di A lo sono; in particolare, anche 0_A ed 1_A sono espressioni polinomiali. Ne segue che l'insieme delle espressioni polinomiali costituisce un sottoanello di B contenente propriamente A.

Denotiamo con $\langle A, x\rangle$ tale sottoanello. Possiamo davvero identificare gli elementi di questo sottoanello con i polinomi come li abbiamo in mente, ossia somiglianti a quelli a coefficienti reali o complessi? Non ancora. Vediamo tre esempi:

ESEMPI 5.2.

5.2.A. - Siano A = **Z**, anello degli interi, e B = **Q**, anello dei numeri razionali. L'elemento $x = \frac{2}{3}$ non appartiene a **Z**. Formiamo il sottoanello $\langle A, x\rangle = \left\langle \mathbf{Z}, \frac{2}{3}\right\rangle$ delle espressioni polinomiali $a_0 + a_1 \cdot \frac{2}{3} + a_2 \cdot \left(\frac{2}{3}\right)^2 + \ldots$. Qui però accade che l'espressione polinomiale $-2 + 3 \cdot \frac{2}{3}$ coincida con l'espressione polinomiale nulla. Lo stesso accade con ogni altro numero razionale $\frac{p}{q}$. Perciò dentro **Q** non troviamo un sottoanello simile a quello che abbiamo in mente come anello dei polinomi a coefficienti interi.

5.2.B. - Siano A = **Z**, anello degli interi, e B = **R**, anello dei numeri reali. Se poniamo $x = \sqrt{2}$, che non è intero e neppure razionale, nell'anello delle espressioni polinomiali $a_0 + a_1 \cdot \sqrt{2} + a_2 \cdot \left(\sqrt{2}\right)^2 + \ldots$ si ha che $-2 + 1 \cdot \left(\sqrt{2}\right)^2$ coincide con l'espressione polinomiale nulla. Perciò $x = \sqrt{2}$ non è compatibile con quel modello che abbiamo in mente.

5.2.C. – Siano sempre A = **Z**, anello degli interi, e B = **R**, anello dei numeri reali. Se scegliamo x = π = 3,14... , allora si può dimostrare che in nessun caso una espressione polinomiale di $\langle \mathbf{Z}, \pi \rangle$ coincide con l'espressione nulla se non ha i coefficienti tutti nulli. Ciò si esprime dicendo che π è un *elemento trascendente* su **Z**. Ne segue che due di queste espressioni polinomiali danno per risultato lo stesso elemento di **R** se e solo se hanno gli stessi coefficienti: infatti siano $f = a_0 + a_1\pi + a_2\pi^2 + \ldots + a_n\pi^n$, $g = b_0 + b_1\pi + b_2\pi^2 + \ldots + b_m\pi^m$ e sia $f = g$. Allora, sostituendo e portando tutto al I membro si ottiene:

$$f = g \Leftrightarrow a_0 + a_1\pi + a_2\pi^2 + \ldots + a_n\pi^n = b_0 + b_1\pi + b_2\pi^2 + \ldots + b_m\pi^m \Leftrightarrow$$

$$\Leftrightarrow (a_0 - b_0) + (a_1 - b_1)\pi + (a_2 - b_2)\pi^2 + \ldots = 0 \Leftrightarrow$$

$$\Leftrightarrow (a_0 - b_0) = 0,\ (a_1 - b_1) = 0,\ (a_2 - b_2) = 0 \ldots \Leftrightarrow a_k = b_k\ \forall k \geq 0.$$

Allora ogni elemento di $\langle \mathbf{Z}, \pi \rangle$ si scrive in modo unico come espressione polinomiale, e ciò si avvicina di più a quel che vogliamo.

Ciò che ci serve, in sostanza, è che nel sottoanello $\langle A, x \rangle$ valga l'analogo del *principio d'identità dei polinomi: "*due espressioni polinomiali sono lo stesso elemento di B se e solo se esse hanno gli stessi coefficienti". In tal caso, diremo che x è *trascendente* rispetto ad A.

PROPOSIZIONE 5.3. Siano A e B due anelli commutativi, A ≤ B, ed esista x∈B trascendente rispetto ad A. Siano poi A' e B' due anelli commutativi, con A' isomorfo ad A, A' ≤ B', ed esista y∈B' trascendente rispetto ad A'. Allora $\langle A, x \rangle$ è isomorfo ad $\langle A', y \rangle$.

Dimostrazione. Sia $\phi : A \to A'$ l'isomorfismo tra A ed A'. Posto $a'_i = \phi(a_i)$, ad $f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in \langle A, x \rangle$ facciamo corrispondere l'elemento $f' = a'_0 + a'_1y + a'_2y^2 + \ldots + a'_ny^n \in \langle A', y \rangle$: il principio d'identità dei polinomi in $\langle A, x \rangle$ assicura che otteniamo una funzione $\Phi : \langle A, x \rangle \to \langle A', y \rangle$, $\Phi(f) = f'$.
Il principio d'identità dei polinomi in $\langle A', y \rangle$ assicura poi che Φ è iniettiva. La suriettività è ovvia. A questo punto, si verifica facilmente che Φ è anche un omomorfismo di anelli, quindi $\Phi : \langle A, x \rangle \to \langle A', y \rangle$ è un isomorfismo.

Allora, tutti gli anelli di espressioni polinomiali a coefficienti in A o in un anello isomorfo ad A, e che soddisfino il principio d'identità dei polinomi, sono isomorfi tra loro a due a due.

Denotiamo con A[x] uno qualunque di questi anelli, e lo chiamiamo *anello dei polinomi nell'indeterminata x e a coefficienti in A*.
Ma esiste sempre? Vediamo una costruzione generale.

Sia A un anello commutativo e riprendiamo l'insieme $B = A^{\mathbf{N}}$ delle *successioni*, cioè delle funzioni da $\mathbf{N}$ ad A, già visto nell'esempio 1.1.B. L'addizione è quella "punto per punto" e la moltiplicazione è la convoluzione. Ossia, per ogni $f,g \in A^{\mathbf{N}}$ si è posto per ogni $n \in \mathbf{N}$,

$(f+g)(n) = f(n)+g(n)$

$(f \cdot g)(n) = f(n)g(0)+f(n-1)g(1)+f(n-2)g(2)+\ldots+f(0)g(n)$.

Si è visto che queste operazioni sono associative, commutative ed hanno per elementi neutri rispettivamente la successione nulla $\mathbf{0} : n \mapsto 0_A$ e la successione $\mathbf{1} : n \mapsto \begin{cases} 1_A & \text{se } n = 0 \\ 0_A & \text{se } n > 0 \end{cases}$. La moltiplicazione è poi distributiva rispetto all'addizione. Infine, posto $(-f)(n) = -f(n)$, ogni successione f ha l'opposta –f.
Pertanto, $B = (A^{\mathbf{N}}, +, \cdot, \mathbf{1})$ è un anello commutativo.
Esso contiene un sottoanello isomorfo ad A: ad ogni $a \in A$ associamo la successione $\mathbf{a} : n \mapsto \begin{cases} a & \text{se } n = 0 \\ 0_A & \text{se } n > 0 \end{cases}$. Otteniamo allora una funzione $\rho : A \to B$, $\rho : a \to \mathbf{a}$, iniettiva ed omomorfismo di anelli. L'immagine $\mathbf{A} = \mathrm{Im}(\rho)$ è dunque un sottoanello di B isomorfo ad A e che possiamo identificare con A.

Ma B contiene anche un elemento x trascendente rispetto ad A: è la successione

$$x : n \mapsto \begin{cases} 1_A & \text{se } n = 1 \\ 0_A & \text{se } n \neq 1 \end{cases}.$$

Infatti, innanzi tutto per ogni $i \geq 1$ si ha $x^i : n \mapsto \begin{cases} 1_A & \text{se } n = i \\ 0_A & \text{se } n \neq i \end{cases}$. Per ogni $a \in A$ (ossia per ogni $\mathbf{a} \in \mathbf{A}$) si ha poi $a_i \cdot x^i : n \mapsto \begin{cases} a_i & \text{se } n = i \\ 0_A & \text{se } n \neq i \end{cases}$.

Pertanto, per ogni $f \in \langle A, x \rangle$, $f = \sum_{i=0}^{k} a_i x^i$, si ha

$$f(n) = \left(\sum_{i=0}^{k} a_i x^i \right)(n) = \sum_{i=0}^{k} a_i \left(x^i(n) \right) = \begin{cases} a_n & \text{se } n \leq k \\ 0_A & \text{se } n > k \end{cases}.$$

Allora, $f = \sum_{i=0}^{k} f(i) x^i$ e si ha $f(n) = 0_A \ \forall n > k$. Ne segue subito il principio d'identità dei polinomi: infatti, i coefficienti dell'espressione polinomiale che dà la successione f sono i valori f(0), f(1), f(2), ... Pertanto, ogni f si ottiene una volta sola come espressione polinomiale, e possiamo identificare A[x] con questo sottoanello di $A^{\mathbf{N}}$, che è costituito, come visto, dalle successioni in A che sono nulle da un certo n in poi.

OSSERVAZIONI **a)** Nell'anello delle funzioni da **R** ad **R** un elemento "trascendente" rispetto ad **R** è la funzione identità id: **R**→**R**, id(x) = x. In tal modo, il sottoanello delle funzioni polinomiali coincide con $\langle \mathbf{R}, \mathrm{id} \rangle$ ed è isomorfo a quello costruito con le successioni in **R** secondo lo schema appena visto.

b) Una volta costruiti i polinomi a coefficienti in un dato anello A, si pone tra gli altri il problema di definirne le radici, dato che, non essendo x una variabile su A, perché i polinomi non sono funzioni da A ad A, non è ovvio dire che cosa significhi sostituire ad x un elemento di A. Ma per ora terminiamo qui.