CAPITOLO QUINTO

ANELLI E CORPI

1 Anelli

Definizione 1. *Un* **anello** *è un gruppo abeliano additivo A, dotato di una ulteriore legge di composizione $(a, b) \longrightarrow ab$ detta* **moltiplicazione** *(ed ab è detto il* **prodotto** *di a e b), che soddisfa le relazioni seguenti, per a, b, $c \in A$:*

associatività: $(ab)c = a(bc)$;

distributività: $a(b + c) = ab + ac$ $[= (ab) + (ac)]$, $(b + c)a = ba + ca$.

L'associatività permette di scrivere abc in luogo di $(ab)c$; analogamente per più fattori.

Lemma 1. *Se a, b sono elementi di un anello, e se 0 ne è lo zero, si ha*
$0a = a0 = 0$, $(-a)b = a(-b) = -ab$ $\quad [ossia = -(ab)]$.

Dim.
Da $0a = (0 + 0)a = 0a + 0a$ si ricava $0a = 0$; analogamente per $a0$.
Poi, $(-a)b + ab = (-a + a)b = 0b = 0$, onde $(-a)b = -(ab)$; analogamente per $a(-b)$.

Un anello è **commutativo** se $ab = ba$ per ogni coppia $\{a, b\}$ di suoi elementi.

Definizione 2. *Un elemento $u \neq 0$ dell'anello A è una* **identità sinistra** *(risp.* **destra***) di A se $ua = a$ (risp. $au = a$) per ogni $a \in A$; $u \neq 0$ è una* **identità** *se è identità destra e sinistra.*

Lemma 2. *Se un anello ha una identità sinistra u ed una destra v, allora $u = v$ è l'unica identità dell'anello, e questo non possiede altre identità nè sinistre nè destre.*

Dim.
Si ha $v = uv = u$; se poi u' è un'altra identità sinistra allora si deve avere $v = u'v = u'$.

Se a appartiene ad un anello, ed n è intero positivo, a^n (**potenza** $n-$esima) di a; a ne è la **base**, n l'**esponente**) significa il prodotto di n fattori uguali ad a.

Quando un anello A ha identità, esso di solito (ma non sempre) viene indicato con 1 o 1_A.

Un insieme B di un anello A è un **sottoanello** di A (ed A è un **sopranello** di B), se B è un anello rispetto alle leggi di composizione indotte da quelle di A; si noti che può darsi benissimo che esistano tanto 1_A quanto 1_B, ma che esse siano distinte.

Esempio. Nel precedente capitolo abbiamo definito sul gruppo additivo degli interi una moltiplicazione: in questo modo abbiamo ottenuto un anello la cui identità è 1.

Definizione 3. *Un elemento $a \neq 0$ di un anello A è un* **divisore sinistro** *(risp.* **destro***)* **dello zero** *in A se esiste un $b \neq 0$ di A tale che $ab = 0$ (risp. $ba = 0$). È un* **divisore dello zero** *in A se è un divisore sinistro o destro dello zero in A.*

Definizione 4. *Un anello commutativo, privo di divisori dello zero, e dotato di identità, è chiamato* **campo di integrità**.

Lemma 3. *Sia A un anello con l'identità 1; allora l'insieme degli $a \in A$ per ciascuno dei quali esistono dei b, $c \in A$ tali che $ba = ac = 1$ è un gruppo moltiplicativo; inoltre $b = c$, e b è unico.*

Dim. Si ha
$b = b\,(ac) = (ba)\,c = c$;
sia G l'insieme descritto; se a_1, $a_2 \in G$, e se
$b_1\,a_1 = a_1\,b_1 = 1$, $b_2\,a_2 = a_2\,b_2 = 1$
è anche
$(b_2b_1)(a_1a_2) = 1$ e $(a_1a_2)(b_2b_1) = 1$,
onde $a_1a_2 \in G$.
Poi, $1 \in G$; inoltre se $a \in G$ anche $b \in G$, in quanto $ba = 1$ e $ab = 1$. Ciò mostra che G è un gruppo. L'unicità di b deriva dal teorema sui gruppi dimostrato nel capitolo precedente.

Il b del Lemma 3 si indica con a^{-1} e si chiama reciproco di a. Si ha ovviamente: $(a_1a_2)^{-1} = a_2^{-1}a_1^{-1}$. Un elemento che soddisa alla condizione espressa nel Lemma 3 si chiama una **unità** di A. Se a è unità, ed n è intero positivo, a^{-n} significa $(a^{-1})^n$, ed a^0 significa 1.

Definizione 5. *Un anello in cui ogni elemento non nullo è una unità dicesi* **anello divisorio** *o* **quasi-corpo**. *Un anello divisorio commutativo dicesi* **corpo**, *ed i suoi elementi si chiamano* **numeri**.

Lemma 4. *Un anello divisorio non ha divisori dello zero; un corpo è un campo di integrità. In altre parole: un corpo non ha divisori di zero.*

Dim. Sia A divisorio; se $ab = 0$, con $a \neq 0$, si ha $b = a^{-1}ab = 0$; quindi A non ha divisori sinistri dello 0; analogamente per i destri. La seconda parte dell'enunciato non fa che ripetere la prima con l'aggiunta della commutatività.

Esempio 1. Gli interi formano un anello commutativo (vedi capitolo precedente); è un campo di integrità per la *legge di annullamento del prodotto* sui numeri interi vista nel capitolo precedente. Non è un corpo perché le sue uniche unità sono 1 e -1.

Esempio 2. Il gruppo additivo dei razionali, con la moltiplicazione descritta nel Capitolo quarto, è un corpo, il **corpo dei razionali**.

Esempio 3. Il gruppo additivo dei reali, con la moltiplicazione descritta nel Capitolo quarto, è un corpo, il **corpo reale**, ed è un sopracorpo (ossia sopranello che è anche corpo) del corpo razionale.

2 I numeri primi

Una proprietà fondamentale di $\mathbb{Z}$ è quella descritta dal seguente teorema.

Teorema 1. (Teorema di divisione)
Dati gli interi $a > 0$ e $b \geq 0$ esistono interi unicamente determinati $q \geq 0$ ed r, $0 \leq r < a$, tali che $b = qa + r$.

Dim.
Dato un divisore $a \neq 0$ dimostreremo che per ogni $b \geq 0$ esistono q ed r con $0 \leq r < a$ tali che $b = qa + r$.
Intanto, $0 = a \cdot 0 + 0$, quindi quando $b = 0$ possiamo porre $q = r = 0$.
Per $b > 0$ usiamo il *Principio di Induzione* II (vedi Appendice). Supponiamo che per ogni c, $0 \leq c < b$, esistano q_0, r_0 con $0 \leq r_0 < a$ e $c = q_0\, a + r_0$. Consideriamo ora b. Vogliamo rappresentare b come $b = qa + r$ con $0 \leq r < a$.
Se $b < a$ allora $b = 0 \cdot a + b$; poiché $0 \leq b < a$ possiamo porre $q = 0$, $r = b$.
Se $b \geq a$, sia $c = b - a$. Allora $0 \leq c < b$. Per induzione, $c = a \cdot q_0 + r_0$ per opportuni q_0 ed r_0 con $0 \leq r_0 < a$. Ma allora

$$b = a + c = a + a \cdot q_0 + r_0 = a(q_0 + 1) + r_0$$

e $0 \leq r_0 < a$. Possiamo porre $q = q_0 + 1$, $r = r_0$.
Per il *Principio di Induzione* II, deduciamo allora che ogni $b > 0$ può essere scritto come $b = a \cdot q + r$, con $0 \leq r < a$.

Per quanto riguarda l'unicità, supponiamo di avere q, r con $b = aq + r$ e $0 \leq r < a$, e supponiamo anche di avere $b' = aq' + r'$ con q', r' eventualmente diversi, e sempre con $0 \leq r' < a$. Vogliamo dimostrare che $r = r'$ e che $q = q'$.
Per farlo, supponiamo $r' \geq r$ e sottraiamo $b = aq' + r'$ da $b = aq + r$, ottenendo $a(q - q') + (r - r') = 0$ ossia $a(q - q') = r' - r$. Poiché $r' - r \geq 0$ ed $a > 0$, risulta $q - q' \geq 0$. Ora $r' - r \leq r' < a$, quindi $a(q - q') < a$ e quindi $q - q' < 1$. Essendo $q - q'$ un intero, abbiamo necessariamente $q - q' = 0$, e $q = q'$. Quindi anche $r' - r = a(q - q') = 0$ e $r' = r$. Questo completa la dimostrazione di unicità, e con ciò il teorema di divisione.

Identità di Bézout*Se d è il MCD di a e b, allora $d = ax + by$ per opportuni interi x e y.*

Per dimostrare questa identità si utilizza il cosiddetto **algoritmo di Euclide**, ovvero dati due numeri naturali a e b, applichiamo il *Teorema di divisione* 1 nel modo seguente:

$$\begin{array}{rcll}
a & = & bq + r_0 & \text{(dividendo } a \text{ per } b \text{)} \\
b & = & r_0 q_0 + r_1 & \text{(dividendo } b \text{ per } r_0 \text{)} \\
r_0 & = & r_1 q_1 + r_2 & \text{(dividendo } r_0 \text{ per } r_1 \text{)} \\
r_1 & = & r_2 q_2 + r_3 & \text{(dividendo } r_1 \text{ per } r_2 \text{)} \\
\cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots \\
r_{n-2} & = & r_{n-1} q_{n-1} + r_n & \text{(dividendo } r_{n-2} \text{ per } r_{n-1} \text{)} \\
r_{n-1} & = & r_n q_n + 0 &
\end{array}$$

Il seguente teorema ci permette di dimostrare che r_n è il MCD di a e b.

Teorema 2. *Se r_n è l'ultimo resto non zero dell'algoritmo di Euclide per a e b, allora r_n è il MCD di a e b, e $r_n = ax + by$ per opportuni x e y.*

Dim. Se r_n è l'ultimo resto non zero dell'algoritmo di Euclide per a e b, allora l'algoritmo comporta $n + 1$ passi. Dimostriamo il teorema per induzione su n.
Se $n = 0$, allora a divide b, ed il teorema è banale. Se $n = 1$ allora l'algoritmo di Euclide ha la forma

$$\begin{array}{rcl}
b & = & aq_1 + r_1 \\
a & = & r_1 q_2 + 0
\end{array}$$

In tal caso è facile vedere che r_1 è il MCD di a e b; inoltre $r_1 = b \cdot 1 + a \cdot (-q_1)$, quindi l'identità di Bézout è verificata.
Supponiamo ora il Teorema vero per $n-1$. Quindi il teorema è vero per ogni coppia di numeri per cui l'algoritmo di Euclide richiede n passi.
Supponiamo quindi che l'algoritmo di Euclide richieda $n+1$ passi per la coppia (a,b). Sia $b = aq_1 + r_1$ la divisone di b per a, che è il primo passo dell'algoritmo di Euclide. Allora il resto dell'algoritmo per (a,b) coincide con l'algoritmo di Euclide per (r_1, a). Dall'ipotesi induttiva sappiamo quindi che r_n è il MCD di a ed r_1, e $r_n = au + r_1 v$, per opportuni interi u, v. Poiché $b = aq_1 + r_1$, si vede facilmente che essendo r_n il MCD di a ed r_1, è anche il MCD di b ed a. Inoltre, sostituendo $b - aq_1$ al posto di r_1 nell'eguaglianza $r_n = au + r_1 v$ si ottiene $r_n = a(u - vq_1) + bv$. Quindi l'identità di Bézout è valida. Il teorema è dimostrato per induzione.

Ricordiamo che un numero naturale $p > 1$ si definisce **primo** se l'unico divisore di p che sia maggiore di 1 è p stesso.([1])
Ricordiamo ora il seguente teorema sui numeri primi

Teorema 3. (Teorema fondamentale dell'aritmetica) *Ogni numero naturale > 1 è o primo o prodotto di primi.*
Ogni numero naturale ≥ 2 si fattorizza **unicamente** *come prodotto di primi.*

Dim. Dimostriamo l'esistenza di una fattorizzazione per induzione (Utilizziamo il Principio di induzione II). Sia $P(n)$ l'affermazione "n è un prodotto di primi".
$P(2)$ è vera in quanto 2 è primo.
Supponiamo che $P(m)$ sia vera per ogni $m < n$. Se n è primo, allora $P(n)$ è vera. Altrimenti si avrà $n = ab$ per opportuni interi $a < n$, $b < n$. Quindi $P(a)$ e $P(b)$ saranno vere, perciò a e b saranno prodotto di primi, ed anche $n = ab$ lo sarà, quindi, Per il principio di induzione II, $P(n)$ sarà vera.

Alla dimostrazione dell'unicità premettiamo il seguente Lemma

Lemma 5. *Se p è primo e p divide ab, allora p divide a oppure p divide b.*

Dim.(del Lemma) Sia d il MCD di p e a. Se $d > 1$ allora $d = p$ essendo p primo. I questo caso p divide a. Se $d = 1$, per l'identità di Bézout possiamo scrivere

$$1 = ax + py$$

per opportuni interi x e y. Quindi $b = bax + bpy$. Allora p divide ab ed anche bpy, quindi divide $bax + bpy = b$, completando la dimostrazione del lemma.

Ritorniamo alla dimostrazione del Teorema.
Unicità. Dimostriamo anche questo risultato per induzione. Supponiamo che esista $a \in \mathbb{N}$ che abbia due fattorizzazioni come prodotto di primi:
$a = p_1 \cdots p_n$ e $b = q_1 \cdots q_m$. Vogliamo dimostrare che le due fattorizzazioni coincidono.
Per il Lemma 5 si avrà che esiste j tale che $p_1 = q_j$. Allora

$$\frac{a}{p_1} = p_2 \cdots p_n \; = \; q_1 \cdots q_{j-1} \cdot q_{j+1} \cdots q_m.$$

Poiché $\dfrac{a}{p_1} < a$, per ipotesi di induzione le due fattorizzazioni di $\dfrac{a}{p}$ coincidono:
cioé l'insieme (con ripetizioni) $\{p_2, \cdots, p_n\} = \{q_1, \cdots, q_{j-1}, q_{j+1}, \cdots, q_m\}$. Ma essendo $p_1 = q_j$ ne segue che $p_1, \cdots, p_n$ coincide con $q_1, \cdots, q_m$. Quindi le fattorizzazioni sono le stesse ed il teorema è verificato per a.

[1] Ricordiamo che 1 non è primo per convenzione.

3 Esempi ed esercizi svolti

Esempio 1. Ricordiamo la relazione di equivalenza definita in $\mathbb{Z}$ nel Capitolo terzo:
dati $m, n \in \mathbb{Z}$ e $p \in \mathbb{N}$ diremo che m è congruo n (o equivalente ad n) modulo p se la differenza $m - n$ è un multiplo di p.
In simboli:

$$m \cong n \pmod{p} \iff \exists h \in \mathbb{Z} \quad \text{tale che } m - n = hp. \tag{1}$$

Indichiamo con $\mathbb{Z}_p$ l'insieme quoziente così determinato e con $[a]_p$ la classe di equivalenza di a. .
$\mathbb{Z}_p$ è un anello commutativo se su di esso definiamo le seguenti operazioni:

$$\begin{aligned} [a]_p + [b]_p &= [a+b]_p \\ [a]_p\,[b]_p &= [ab]_p\,. \end{aligned} \tag{2}$$

Verifichiamo per prima cosa che è una buona definizione. Ovvero se $c \cong a$ allora
$[c]_p + [b]_p = [a+b]_p$.
Infatti sia $h \in \mathbb{Z}$ tale che $c - a = hp$. Dalla (2) segue
$[c]_p + [b]_p = [c+b]_p$ Osserviamo che
$[c+b]_p = [a+b]_p$, perché $(c+b) - (a+b) = hp$.
Per quanto riguarda il prodotto dobbiamo verificare che
$[c]_p\ [b]_p = [ab]_p$.
Anche in questo caso
$[c]_p\ [b]_p = [cb]_p$.
e quindi deve essere
$[cb]_p = [ab]_p$.
ovvero
$(cb) - (ab) = bhp$.
La verifica del fatto che si tratta di un anello commutativo è semplice. Osserviamo in particolare che $[0]_p = [p]_p$. Mentre $[p+1]_p = [1]_p$. L'unità dell'anello è $[1]_p$.
Dato che $card\mathbb{Z}_p$ è finita si ha che anche il suo ordine è finito.
(dimostrare)
Diamo due esempi di due anelli commutativi di questo tipo.

$(\mathbb{Z}_3, +, \cdot)$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$(\mathbb{Z}_4, +, \cdot)$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	0	0
2	2	3	1	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Osserviamo che nel caso di $\mathbb{Z}_3$ non ci sono divisori di 0 come accade invece nel caso di $\mathbb{Z}_4$. Questo non è un fatto casuale come si vede dal seguente

Teorema 4. *$\mathbb{Z}_p$ è un corpo se e solo se p è primo.*

Dim. Iniziamo con il dimostrare che se $\mathbb{Z}_p$ è un corpo allora p è primo. Per assurdo, sia $p > 1$ non primo. Allora possiamo trovare due interi h, k, con $1 < h, k < p$ tali che $p = hk$. Osserviamo che valgono le eguaglianze
$[h]_p\,[k]_p = [h\,k]_p = [p]_p = 0.$
ma $[h]_p \neq 0$ e $[k] \neq 0$.

Viceversa, se p è primo $\mathbb{Z}_p$ è un corpo. Dobbiamo per prima cosa verificare che ogni elemento $[a]_p \in \mathbb{Z}$ ha un inverso. Se p è primo, allora il MCD tra a e p è 1. Per l'identità di Bézout esistono b ed r tali che $a \cdot b + r \cdot p = 1$ da cui $a \cdot b - 1 = -rp$ ovvero $ab \cong 1 \pmod{p}$ onde $[ab]_p = [1]_p$. Quindi in definitiva $[a]_p \cdot [b]_p = [1]_p$, ovvero $[b]_p$ è l'inverso di $[a]_p$.
Verifichiamo ora che non esistono in $\mathbb{Z}_p$ divisori di zero procedendo per assurdo: cioé, esistono h, $k \neq 0$ tali che
$[h\,k]_p = 0$ e $1 \leq h, k < p$
questo equivale a dire che $[h\,k]_p = [p]_p$.
Onde: esiste $h' \in \mathbb{Z}$ tale che $hk - p = h'p$, ovvero $hk = (h' + 1)p$, quindi la fattorizzazione di $(h' + 1)p$ contiene la fattorizzazione di hk, ovvero un prodotto di primi $<$ di p da questa segue che per l'unicità della fattorizzazione, vedi Teorema 3, che p non è primo.

Esempio 2. Consideriamo l'insieme $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ delle coppie (x, y) di numeri reali. Su questo insieme definiamo le seguenti operazioni:

$$(x, y) + (x', y') = (x + x', y + y') \tag{3}$$

$$(x, y)(x', y') = (xx' - yy', xy' + yx') \tag{4}$$

Con queste due leggi di composizione $\mathbb{R}^2$ diventa un *corpo* che viene chiameto **corpo dei numeri complessi** e si indica con $\mathbb{C}$.
È facile verificare le proprietà. In particolare si verifica facilmente che:

elemento neutro rispetto a $+$ è la coppia $(0, 0)$,

unità è la coppia $(1, 0)$,

opposto di (x, y) è $(-x, -y)$,

reciproco di (x, y) è $\left(\dfrac{x}{x^2 + y^2}, \dfrac{-y}{x^2 + y^2}\right)$.

Quest'ultima si ottiene risolvendo l'equazione:

$$(x, y)(x', y') = (1, 0)$$

che equivale, tenuto conto di (4), al sistema seguente:

$$\begin{cases} xx' - yy' = 1 \\ yx' + xy' = 0. \end{cases} \tag{5}$$

Questo sistema ammette una ed una sola soluzione che è appunto il reciproco di (x, y) scritto sopra.

Consideriamo l'insieme $\mathbb{C}_1 \subset \mathbb{C}$ costituito dai numeri complessi del tipo $(x, 0)$. Si verifica facilmente che $\mathbb{C}_1$ è un corpo con le operazioni $+$ e $\cdot$ definite da (3)(4) su $\mathbb{C}$. Quindi $\mathbb{C}_1$ è un sottocorpo di $\mathbb{C}$.

L'applicazione $\varphi : \mathbb{R} \longrightarrow \mathbb{C}$ definita da

$$\varphi(x) \;=\; (x, 0)$$

che ad ogni numero reale x associa il numero complesso $(x, 0)$ è un isomorfismo del corpo $\mathbb{R}$ sul corpo $\mathbb{C}$. Ciò significa che φ è un'applicazione biunivoca e inoltre conserva le operazioni di somma e prodotto

$$\varphi(x_1 + x_2) \quad = \quad (x_1, 0) + (x_2, 0); \tag{6}$$

$$\varphi(x_1\, x_2) \quad = \quad (x_1, 0)\,(x_2, 0). \tag{7}$$

Quindi $\mathbb{R}$ e $\mathbb{C}_1$ sono corpi isomorfi. Si dice che $\mathbb{C}_1$ è il sottocorpo dei numeri complessi reali. Possiamo scrivere x anzichè $(x, 0)$.

Consideriamo ora invece il sottoinsieme $\mathcal{I}$ di $\mathbb{C}$ costituito dai numeri complessi del tipo $(0, y)$. Questo non può essere un sottocorpo di $\mathbb{C}$. basta infatti osservare che il prodotto (4) deifinito in $\mathbb{C}$, non è una legge di composizione in $\mathcal{I}$.([2]) Infatti applicata a due elementi di $\mathcal{I}$ non dà in generale un elemento di $\mathcal{I}$:

$$(0, y_1)(0, y_2) \;=\; (-y_1\, y_2, 0).$$

I numeri complessi con $(0, y)$, con $y \neq 0$, si chiamano **numeri immaginari (puri)**. In particolare $(0, 1)$ si chiama **unità immaginaria** e si indica con i :

$$(0, 1) = i$$

Un numero immaginario puro si può scrivere (in modo unico) come prodotto di un numero reale e dell'unità immaginaria:

$$(0, y) = (0, 1)(0, y) = i\, y.$$

Di conseguenza ogni numero complesso si può scrivere come somma di un numero reale e di un numero immaginario puro:

$$(x, y) \;=\; (x, 0) + (y, 0) = x + iy.$$

Si dice che x è **la parte reale** e y è **il coefficiente della parte immaginaria** del numero complesso

$$z = (x, y)$$

In simboli

$$x \;=\; \mathcal{R}e\, z, \qquad y \;=\; \mathcal{I}m\, z$$

Quando il numero complesso (x, y) è scritto nella forma $x + iy$ si dice che è scritto in **forma algebrica**.

Scrivere complessi in forma algebrica è particolarmente utile ai fini del calcolo. Si seguono infatti le usuali regole del calcolo letterale tenendo conto che

$$\begin{array}{lllllllll}
i^1 & = & i & & & & & & \\
i^2 & = & i \cdot i & = & (0,1)(0,1) & = & (-1,0) & = & -1 \\
i^3 & = & i^2 \cdot i & = & (-1,0)(0,1) & = & (0,-1) & = & -i \\
i^4 & = & i^3 \cdot i & = & (0,-1)(0,1) & = & (1,0) & = & 1 \\
i^5 & = & i^4 \cdot i & = & i & & & & \\
i^6 & = & i^5 \cdot i & = & i^2 & & = & -1 & \\
\cdots & \cdots & \cdots & \cdots & \cdots & & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & & \cdots & \cdots & \cdots
\end{array} \tag{8}$$

[2]Si dice, brevemente, che $\mathcal{I}$ **non è chiuso** rispetto al prodotto definito in $\mathbb{C}$.

In generale quindi

$$i^k = \begin{cases} i & \text{se} \quad k \cong 1 \mod 4 \\ -1 & \text{se} \quad k \cong 2 \mod 4 \\ -i & \text{se} \quad k \cong 3 \mod 4 \\ 1 & \text{se} \quad k \cong 0 \mod 4 \end{cases} \tag{9}$$

Osserviamo ad esempio che
$(x+iy)+(x'+iy') = x+x'+i(y+y')$;

$(x+iy)(x'+iy') = xx'+xy'i+iyx'+i^2yy' = xx'-yy'+i(xy'+x'y)$;

Questo tipo di notazione risulta particolarmente utile nel calcolo del reciproco $(x,y)^{-1}$ di un numero complesso (x,y). Possiamo infatti scrivere
$(x,y)^{-1} = \dfrac{1}{x+iy} = \dfrac{x-iy}{(x+iy)(x-iy)} = \dfrac{x-iy}{x^2+y^2} = \dfrac{x}{x^2+y^2} + i\dfrac{-y}{x^2+y^2}$.
Sia $z = x+iy$ il numero complesso $\overline{z} = x-iy$ si chiama **complesso coniugato** di z. Si osservi che in particolare vale $z\,\overline{z} = x^2+y^2$.

Osserviamo che $\mathbb{C}$ non è un corpo ordinato. Ossia non è possibile introdurre in esso un ordinamento $\preceq$ tale che

$$z \preceq w \implies z+v \preceq w+v, \qquad \forall v \in \mathbb{C} \tag{10}$$

$$0 \preceq z \ \wedge \ 0 \preceq w \implies 0 \preceq zw. \tag{11}$$

Infatti se così fosse dalla proprietà (10) seguirebbe che

$$z \preceq 0 \iff 0 \preceq -z, \qquad (z \in \mathbb{C}). \tag{12}$$

quindi è vera almeno una delle seguenti due proposizioni

$$0 \preceq i; \qquad 0 \preceq -i.$$

Essendo

$$i^2 = (-i)^2 = -1.$$

si ha in entrambi i casi, tenuto conto della proprietà (11)

$$0 \preceq -1$$

Da questa si ha l'assurdo perché per (12)

$$0 \preceq -1 \Longrightarrow 1 \preceq 0$$

mentre per la proprietà (11)

$$0 \preceq -1 \Longrightarrow 0 \preceq (-1)^2 = 1.$$

Ma dalla proprietà antisimmetrica dell'ordinamento otteniamo l'assurdo:

$$1 \preceq 0 \ \wedge \ 0 \preceq 1 \Longrightarrow 0 = 1.$$

4 APPENDICE: il Principio di Induzione.

In questa parte diamo una formulazione del Principio di Induzione diversa da quella enunciata nel primo capitolo e dimostriamo l'equivalenza tra le due. Iniziamo riportando l'enunciato visto nel primo capitolo.

Principio di Induzione I
Sia $P(n)$ definita per ogni numero naturale $n > n_0$. Se

(a) *$P(n_0)$ è vera;*

(b) *$P(n) \Longrightarrow P(n+1)$, per ogni $n \geq n_0$*

allora $P(n)$ è vera per ogni $n \geq n_0$.

L'altro enunciato che consideriamo è il seguente:

Principio di Induzione II
Sia $P(n)$ definita per ogni numero naturale $n > n_0$. Se

(a') *$P(n_0)$ è vera;*

(b') *Per ogni $n > n_0$, se $P(m)$ è vera per ogni m tale che $n_0 \leq m < n$, allora $P(n)$ è vera*

allora $P(n)$ è vera per ogni $n \geq n_0$.

Teorema 5. *Il* **Principio di Induzione I** *è valido se e solo se è valido il* **Principio di Induzione II**.

Dim.
Sia $P(n)$ una proposizione definita sui naturali e supponiamo di sapere che

(a') $P(n_0)$ è vera;

(b') Per ogni $n > n_0$, se $P(m)$ è vera per ogni m tale che $n_0 \leq m < n$, allora $P(n)$ è vera

Sia $Q(n)$ la proposizione: "$P(m)$ è vera per ogni m, $n_0 \leq m < n$."
Per dimostrare che $P(n)$ è vera per ogni $n \geq n_0$ è sufficiente dimostrare che $Q(n)$ è vera per ogni n.
Dimostreremo che $Q(n)$ è vera mediante il **Principio di Induzione I**, ovvero verificheremo che

(a) $Q(n_0)$ è vera;

(b) $Q(n-1) \Longrightarrow Q(n)$, per ogni $n \geq n_0$

L'asserzione (a) coincide con (a'), quindi è vera.
Verfichiamo (b) : supponiamo che $Q(n)$ sia vera, allora $P(m)$ è vera per ogni m, $n_0 \leq m \leq n-1$. Per (b'), $P(n)$ è vera. Quindi $P(m)$ è vera per ogni m, $n_0 \leq m \leq n$. Donde $Q(n)$ è vera. Per il **Principio di Induzione I** $Q(n)$ è vera per ogni $n \geq n_0$.

Viceversa. Sia $P(n)$ una proposizione definita sui naturali $n \geq n_0$. Come visto sopra l'ipotesi (a') equivale ad (a). Dall'induttività di $P(n)$, segue che
$P(n_0) \Longrightarrow P(n_0+1) \Longrightarrow \cdots \Longrightarrow P(n-2) \Longrightarrow P(n-1) \Longrightarrow P(n)$.
Questo vuol dire che se $P(m)$ è vera per ogni $n_0 \leq m < n$ allora è vera $P(n)$ ovvero (b').
Quindi per il **Principio di Induzione II** $P(n)$ è vera per ogni $n \geq n_0$. resta quindi verificato il **Principio di Induzione I**.