Note di Algebra (versione preliminare)

Michele Grassi

Indice

CAPITOLO 1

Nozioni di base

1. Nozione di insieme

La nozione di insieme è usualmente considerata un *concetto primitivo* in matematica, ovvero un concetto che non si cerca di definire ma si prende come dato intuitivamente. Per procedere in modo rigoroso dovremmo però elencare le proprietà che ci aspettiamo che gli insiemi debbano soddisfare. Per i fini di questo corso sarà invece sufficiente la nozione intuitiva di insieme.
Notazione *Appartenenza di elementi ad insiemi* Quando l'elemento x appartiene all'insieme S, si scrive $x \in S$
Definizione *Uguaglianza e disuguaglianza di insiemi* Due insiemi sono uguali se e solo se contengono gli stessi elementi: in notazione matematica,

$$S = T \iff (\forall x \; x \in S \iff x \in T)$$

Quando due insiemi non sono uguali scriviamo $S \neq T$.
Notazione Per descrivere un insieme è necessario descrivere i suoi elementi. Quando questi elementi sono pochi, si possono semplicemente elencare. La notazione matematica per l'insieme formato dai numeri $2, 4$ e 6 è la seguente:

$$S = \{2, 4, 6\}$$

Si noti che gli elementi ripetuti vengono contati solo una volta, per cui $\{2, 4, 6\} = \{2, 2, 4, 6\}$.
Esempio
$\emptyset$ *l'insieme vuoto*
$\mathbb{N} = \{0, 1, 2, 3, ...\}$ (numeri naturali),
$\mathbb{Z} = \{-2, -1, 0, 1, 2, ...\}$ (numeri interi),
$\mathbb{Q} = \{0, 1, \frac{2}{5}, -\frac{7}{3}, ...\} = \{\frac{p}{q} \mid p \in \mathbb{Z}, \; q \in \mathbb{N}\}$ (numeri razionali)

Dato un insieme, possiamo individuare un certo numero di suoi elementi che soddisfano una qualche proprietà, e considerarli come elementi di un nuovo insieme, che sarà incluso in quello iniziale, nel senso che tutti i suoi elementi sono anche elementi di quello iniziale. In notazione matematica, diciamo che
Definizione S è incluso in T, e scriviamo $S \subset T$ quando vale quanto segue:

$$S \subset T \iff (\forall x \; x \in S \implies x \in T)$$

È chiaro che quando un insieme è incluso in un altro e a sua volta lo include, deve coincidere con esso. Questa affermazione ovvia può essere formalizzata in una proposizione matematica, che necessita di una dimostrazione rigorosa
Proposizione $S = T \iff S \subset T$ e $T \subset S$
Dimostrazione Dimostriamo prima che $S = T \implies S \subset T \wedge T \subset S$. Se $S = T$, per

la definizione della sezione 1 sappiamo che deve valere $\forall x\ x \in S \iff x \in T$. Da questo seguono le due proprietà:

$$\forall x\ x \in S \implies x \in T,\ \ \forall x\ x \in T \implies x \in S$$

che dicono esattamente (per definizione) che $S \subset T$ e $T \subset S$.
Viceversa, supponiamo di sapere che $S \subset T \wedge T \subset S$. Allora per definizione questo vuol dire che

$$\forall x\ x \in S \implies x \in T,\ \ \forall x\ x \in T \implies x \in S$$

da cui segue che $\forall x\ x \in S \iff x \in T$, che di nuovo per definizione vuol dire che $S = T$. □
Questa dimostrazione dovrebbe rendere chiara la differenza fra affermare "è chiaro" e "dimostrare". Molto spesso in matematica cose che sembrano "chiare" si rivelano non così chiare (o magari false) quando si prova a dimostrarle.
Definizione S è un *sottoinsieme proprio* di T se $S \subset T$ e $S \neq T$
Esempio $\{2, 3\} \subset \{2, 3, 5\}$ Quando vogliamo individuare degli elementi specifici di un insieme per definire un sottoinsieme, usando la proprietà P, usiamo la seguente notazione
Notazione $T = \{x \in S \mid x \text{ soddisfa } P\}$
Esempio $\{2, 3\} = \{x \in \{2, 3, 5\} \mid x \neq 5\}$
La notazione semplificata $\{x \mid \ x \text{ soddisfa } P\}$ si usa quando e' chiaro da dove prendiamo gli elementi x. Ad esempio, se stiamo parlando di numeri interi, possiamo scrivere $\{x \mid \ x \text{ è pari}\}$ invece del più corretto $\{x \ \in \mathbb{N} \mid \ x \text{ è pari}\}$.
Definizione Dati gli insiemi S, T, possiamo definire dei nuovi insiemi:
$S \cup T = \{x \mid x \in S \ \vee \ x \in T\}$ (unione di S e T)
$S \cap T = \{x \mid x \in S \ \wedge \ x \in T\}$ (intersezione di S e T) $S \setminus T = \{x \mid x \in S \wedge \ \notin T\}$ (differenza di S e T)
Esempio $\{1, 4, -3\} \cup \{4, 5, 7\} = \{1, 4, -3, 5, 7\}$ $\{1, 4, -3\} \cap \{4, 5, 7\} = \{1\}$), $\{1, 4, -3\} \cap \{5, 7\} = \emptyset$)
Teorema Dati gli insiemi R, S, T, valgono le seguenti proprietà:
a) (commutativa) $S \cap T = T \cap S$, $S \cup T = T \cup S$.
b) (associativa) $S \cap (T \cap U) = (S \cap T) \cap U$, $S \cup (T \cup U) = (S \cup T) \cup U$.
c) (distributiva) $R \cap (S \cup T) = (R \cap S) \cup (R \cap T)$, $R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$
Dimostrazione a) Esercizio
b) Esercizio
c) $R \cap (S \cup T) = (R \cap S) \cup (R \cap T)$: dimostriamo la doppia inclusione.
Dimostrazione di $R \cap (S \cup T) \subset (R \cap S) \cup (R \cap T)$: Sia $x \in R \cap (S \cup T)$. Allora deve essere $x \in R$ e $x \in S \cup T$. Quindi $x \in S$ o $x \in T$. Nel primo caso, $x \in R \cap S$, mentre nel secondo caso $x \in R \cap T$. Quindi $x \in (R \cap S) \cup (R \cap T)$.
Dimostrazione di $(R \cap S) \cup (R \cap T) \subset R \cap (S \cup T)$:Sia $x \in (R \cap S) \cup (R \cap T)$. Allora deve essere o $(R \cap S)$ oppure $x \in (R \cap T)$. Quindi si ha in ogni caso $x \in R$, e inoltre o $x \in S$ o $x \in T$, ovvero $x \in S \cup T$.
L'altra proprietà distributiva si dimostra in modo simile. La dimostrazione è lasciata come esercizio. □
Gli elementi di un insieme possono essere a loro volta insiemi.
Esempio $\{\mathbb{N}, \mathbb{Q}, \mathbb{Z}\}$ è un insieme con tre elementi.
Definizione Dato un insieme S, l'*insieme delle parti* di S, indicato con $\mathcal{P}(S)$, è definito come

$$\mathcal{P}(S) = \{X \mid X \subset S\}$$

Esempio

$$\mathcal{P}(\{1,2,3\}) = \{\{\emptyset, \{1,2,3\}, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}\}$$

Esempio Dato $i \in \mathbb{N}$, sia $T_i = \{x \in \mathbb{Z} \mid x = ni \text{ per qualche } y \in \mathbb{Z}\}$. Al variare di $i \in \mathbb{N}$ si ottengono sottoinsiemi diversi di $\mathbb{Z}$. Possiamo costruire allora l'insieme $\{T_i \mid i \in \mathbb{N}\}$, che contiene tutti i T_i come elementi. Si ha chiaramente che $\{T_i \mid i \in \mathbb{N}\} \subset \mathcal{P}(\mathbb{Z})$
Definizione Dato un insieme S i cui elementi sono a loro volta insiemi, definiamo:
$\bigcup S = \{x \mid \exists T \in S : x \in T\}$ (unione di S)
$\bigcap S = \{x \mid \forall T \in S : x \in T\}$ (intersezione di S)
Esempio Per ogni insieme X, si ha $\bigcup \mathcal{P}(X) = X$.
Esempio $\bigcup\{\{2,3\},\{3,4\}\} = \{2,3,4\}$.
Esempio $\bigcap\{\{2,3\},\{3,4\}\} = \{3\}$.
Esempio Prendendo $S = \{T_i \mid i \in \mathbb{N}\}$, si ha che $\bigcup S = \mathbb{Z}, \bigcap S = \{0\}$.
Dimostrazione Dato che $T_1 = \mathbb{Z}$, si ha che $\mathbb{Z} \subset \bigcup S$, e inoltre dato che $\forall i\ T_i \subset \mathbb{Z}$ deve anche essere $\bigcup S \subset \mathbb{Z}$. Unendo questi due fatti si ha che $\bigcup S = \mathbb{Z}$.
Supponiamo ora per assurdo che esista $x \in \bigcap S$, con $x > 0$. Si dovrebbe avere per definizione di intersezione che $\forall i\ x \in T_i$, e quindi in particolare $x \in T_{2x}$. Questo significherebbe però che esiste $y \in \mathbb{Z}$ con $x = 2xy$, e questo è assurdo. Se invece fosse $x \in \bigcap S$ con $x < 0$, si dovrebbe avere analogamente che $x \in T_{-2x}$, e quindi dovrebbe esistere $y \in \mathbb{Z}$ con $x = -2xy$ che è assurdo. Dato che chiaramente $0 \in \bigcap S$, ne segue che deve essere $\bigcap S = \{0\}$.
Definizione Una *funzione* con *dominio* A e *codominio* B è una regola per associare ad ogni elemento di A uno ed un solo elemento di B. In tal caso scriviamo $f : A \to B$. Se indichiamo con f una funzione, allora il suo dominio si indica con $Dom(f)$, il suo codominio si indica con $Cod(f)$, e il valore della funzione sull'elemento $x \in Dom(f)$ si indica con $f(x) \in Cod(f)$
Definizione Una funzione f da un insieme A ad un insieme B si dice:
Iniettiva se $\forall x_1, x_2 \in A\ f(x_1) = f(x_2) \implies x_1 = x_2$
Surgettiva se $\forall y \in B\ \exists x \in A\ :\ f(x) = y$.
Bigettiva se è sia iniettiva che bigettiva.
Definizione Date due funzioni $f : A \to B$ e $g : B \to A$, diciamo che g è *inversa* di f se vale che

$$\forall x \in A\ g(f(x)) = x \quad \forall y \in B\ f(g(y)) = y$$

2. Principio del buon ordinamento e principio di induzione

Principio del buon ordinamento *Ogni insieme non vuoto di numeri naturali contiene un elemento minimo*
Il principio del buon ordinamento è equivalente al seguente
Principio di induzione *Sia S un insieme di numeri naturali con le seguenti proprietà:*
a) $1 \in S$
b) Se $x \in S$, allora $x + 1 \in S$.
Allora $S = \mathbb{N}$.
Teorema Il principio di induzione ed il principio del buon ordinamento sono equivalenti.

Dimostrazione Dimostriamo che il principio di induzione implica il principio del buon ordinamento:
Sia $S \subset \mathbb{N}$, $S \neq \emptyset$, e prendiamo $T = \{n \in \mathbb{N} \mid \forall t \in S \; n < t\}$ Si dimostra allora che $1 \in T$ e $x \in t \implies x + 1 \in T$, e quindi per il principio di induzione $T = \mathbb{N}$, contraddicendo $S \neq \emptyset$.
Viceversa, dimostriamo che il principio del buon ordinamento implica il principio di induzione:
Sia S un insieme di numeri naturali tale che $1 \in S$ e se $x \in S$, allora $k + 1 \in S$. Vogliamo dimostrare che $S = \mathbb{N}$ usando il principio del buon ordinamento. Supponiamo per assurdo che $S \neq \mathbb{N}$. Allora $T = \mathbb{N} \setminus S \neq \emptyset$. T ammette quindi un minimo, chiamiamolo m. Deve esssere $m > 1$, perche' $1 \in S$ per ipotesi. Ma allora si ha che $m - 1 \in \mathbb{N}$, e inoltre $m - 1 \notin T$ perchè m è il minimo di T e $m - 1 < m$. Deve essere quindi $m-1 \in S$, e quindi per ipotesi $m = (m-1)+1 \in S$, assurdo. □

Per definire una espressione $F(n)$ che dipende da $n \in \mathbb{N}$, possiamo usare un metodo induttivo, nel senso che definiamo $F(1)$ e poi diamo un modo per dire quanto vale $F(n + 1)$ sapendo quanto vale $F(n)$. In questo modo l'insieme S degli $n \in \mathbb{N}$ per cui $F(n)$ è definito contiene 1, e se contiene n allora contiene $n + 1$. Per il principio di induzione, deve essere $S = \mathbb{N}$, e quindi abbiamo definito $F(n)$ per tutti gli N.
Esempio Potenza di un numero razionale: $F(n) = x^n$ per un qualche (fissato) $x \in \mathbb{Q}$. Definiamo $F(1) = x$, e $F(n + 1) = xF(n)$. In altre parole, per definire x^n diciamo che $x^1 = x$, e $x^{n+1} = x(x^n)$. È chiaro che in questo modo definiamo x^n er tutti gli $n \in \mathbb{N}$.
Esempio Simbolo di sommatoria: $F(n) = \sum_{i=1}^{n} f(i)$, per qualche funzione $f = f(i)$ nota.
Definiamo $F(1) = f(1)$, e $F(n + 1) = F(n) + f(n + 1)$. Questa è una buona definizione per induzione, e la funzione F che si ottiene si indica con $\sum_{i=1}^{n} f(i)$.
Usando il principio di induzione si possono fare le cosiddette dimostrazioni per induzione, in cui si dimostrano in genere (ma non esclusivamente) proprietà di quantità che sono stade a loro volta definite in modo induttivo. Vediamo di seguito due esempi.
Proposizione $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
Dimostrazione Faremo una *dimostrazione per induzione*: Sia $\subset \mathbb{N}$ l'insieme dei numeri naturali per cui l'affermazione "$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$" è vera. Vogliamo dimostrare che $S = \mathbb{N}$. Intanto $1 \in S$, perche' l'affermazione per $n = 1$ è semplicemente $1 = 1$. Supponiamo di sapere che $n \in S$, e cerchiamo di dimostrare che $n+1 \in S$. In effetti $\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n + 1)$ che è uguale, per ipotesi induttiva, a $\frac{n(n+1)}{2} + (n + 1)$. Quest'ultima espressione è però chiaramente

$$\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

□
Proposizione Per qualunque numero (razionale) $x \neq 1$ e qualunque $n \in \mathbb{N}$, vale $\sum_{i=0}^{n} x^i = \frac{1-x^{n+1}}{1-x}$
Dimostrazione Dimostriamo il teorema per induzione su n. Per $n = 1$ la proposizione dice che $\sum_{i=0}^{1} x^i = \frac{1-x^2}{1-x}$, e questo si verifica direttamente, osservando che $\sum_{i=0}^{n} x^i = 1 + x$ per definizione (usiamo la convenzione $x^0 = 1$.

Supponiamo di sapere la proposizione per $n = h$, e dimostriamola per $n = h + 1$. Vogliamo dimostrare che $\sum_{i=0}^{h+1} x^i = \frac{1-x^{h+2}}{1-x}$. Per definizione di sommatoria sappiamo che

$$\sum_{i=0}^{h+1} x^i = \sum_{i=0}^{h} x^i + x^{h+1}$$

Per ipotesi induttiva, questo si può riscrivere:

$$\sum_{i=0}^{h} x^i + x^{h+1} = \frac{1 - x^{h+1}}{1 - x} + x^{h+1}$$

e una semplice manipolazione algebrica di questa espressione la rende uguale a $\frac{1-x^{h+2}}{1-x}$. Per il principio di induzione, abbiamo dimostrato la tesi del teorema. □

3. Campi ed Anelli

Per definire cosa intendiamo per un campo in generale, elenchiamo le operazioni che si possono fare fra i suoi elementi (somma e prodotto) e le proprietà fondamentali di queste operazioni, dalle quali tutte le altre si possono dedurre.

Definizione Dato un insieme K con due operazioni binarie $+, \cdot$ e due elementi $0, 1$ diciamo che $(K, +, \cdot, 0, 1)$ è un *anello* se valgono le seguenti proprietà:

a) Proprietà *associativa*

$$\forall x, y, z \in K \; x + (y + z) = (x + y) + z, \; x(yz) = (xy)z$$

b) Proprietà *commutativa*

$$\forall x, y \in K \; x + y = y + x, \; xy = yx$$

c) Proprietà *distributiva*

$$\forall x, y, z \in K \; x(y + z) = (xy) + (yz)$$

d) *Elementi neutri* ed *esistenza degli inversi*:

$$\forall x \in K \; x + 0 = x, \; x1 = x, \quad \forall x \in K \; \exists y \in K \; : \; x + y = 0$$

Se in più vale anche la proprietà:

$$\forall x \in K \setminus \{0\} \; \exists y \in K \; : \; xy = 1$$

diciamo che $(K, +, \cdot, 0, 1)$ è un *campo*.

Notazione Nelle espressioni, il simbolo di moltiplicazione ha priorità maggiore rispetto a quello di addizione, e quindi ad esempio $(xy) + (zw)$ si può anche scrivere $xy + zw$ senza rischio di ambiguità.

Un avvertimento: quello che noi chiamiamo "anello" in realtà andrebbe chiamato "anello commutativo con identità". Visto però che noi considereremo sempre e soltanto anelli commutativi con identità, ometteremo sempre l'ultima parte del nome e parleremo più semplicemente di anelli.

I numeri interi soddisfano quasi tutte le proprietà dei campi, se li dotiamo della somma e della moltiplicazione standard. Qualcosa però manca, e non otteniamo un campo. Più precisamente,

Esempio $(\mathbb{Z}, +, \cdot, 0, 1)$ è un anello.

Dimostrazione Assumeremo questi fatti come conosciuti, così come le altre proprietà standard dei numeri interi. □

Definizione *I numeri razionali* L'insieme $\mathbb{Q}$ dei numeri razionali è stato definito in precedenza,

$$\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z},\ q \neq 0\}$$

Le operazioni di somma e di prodotto fra numeri razionali sono definite come segue:

$$\frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs},\ \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$$

Ovviamente è sottintesa la regola per cui $\frac{p}{q} = \frac{pr}{qr}$ per tutti gli $r \in \mathbb{Z}$ diversi da zero.
Teorema $(\mathbb{Q}, +, \cdot, 0, 1)$ è un campo.
Dimostrazione Per dimostrare l'associatività della somma, espandiamo le due espressioni coinvolte usando la definizione di somma data in precedenza.

$$\frac{p}{q} + \left(\frac{r}{s} + \frac{t}{u}\right) = \frac{p}{q} + \frac{ru + st}{su} = \frac{p(su) + q(ru + st)}{q(su)}$$

$$\left(\frac{p}{q} + \frac{r}{s}\right) + \frac{t}{u} = \frac{ps + qr}{qs} + \frac{t}{u} = \frac{(ps + qr)u + (qs)t}{(qs)u}$$

Usando associativi'a, distributività e commutatività di somma e prodotto su $\mathbb{Z}$ si ottiene che le due espressioni rappresentano lo stesso numero razionale. Il resto della dimostrazione è una verifica diretta, che è lasciata come esercizio. □
Abbiamo visto che le proprietà associativa, commutativa e distributiva valgono anche per un tipo completamente diverso di operazioni, ovvero le operazioni di intersezione e di unione di insiemi. In effetti, il seguente esempio mostra come a partire da queste operazioni si possa costruire un oggetto che assomiglia ad un campo, ma in effetti non lo è
Esempio Se X è un insieme, allora $(\mathcal{P}(X), \cup, \cap, \emptyset, X)$ soddisfa le proprietà a, b, c della definizione di campo, e la prima delle proprietà d. Non soddisfa però le restanti proprietà del punto d.
Dimostrazione Esercizio □
A partire dagli assiomi di anello, si possono dimostrare proprietà generali che valgono in tutti gli anelli. Questo è uno dei vantaggi dell'identificare degli assiomi generali, che valgono in tutti gli anelli.
Proposizione *Possibilità della sottrazione* $\forall a, b \exists c : a + c = b$ In tal caso scriviamo $c = b - a$. Se $b = 0$, scriviamo semplicemente $-a$
Dimostrazione Sia d tale che $a + d = 0$. Prendiamo $c = b + d$. Si ha che $a + c = a + (b + d) = b + (a + d) = b + 0 = b$.
Proposizione *Legge di semplificazione per* $+$ $a + b = a + c \implies b = c$:
Dimostrazione Aggiungiamo $-a$ ad entrambi i membri. □
Quando l'anello è anche un campo valgono anche altre proprietà, come ad esempio:
Proposizione *Possibilità della divisione* Se $b \neq 0$, allora $\forall a \exists c\ :\ bc = a$. In tal caso scriviamo $c = \frac{a}{b} = ab^{-1}$. Se $a = 1$ scriviamo semplicemente b^{-1}.
Dimostrazione Esiste d tale che $db = 1$. Allora prendiamo $c = ad$. si ha che $bc = b(ad) = a(db) = a1 = a$. □
Proposizione *Legge di semplificazione per il prodotto* Se $b \neq 0$, $ba = bc \implies a = c$.
Dimostrazione Moltiplichiamo entrambi i membri per b^{-1}. □

4. I numeri complessi

Definizione $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, e inoltre si hanno due operazioni di somma e di prodotto, $\cdot, +$ definite come:

$(a+bi)+(c+di) = a+c+(b+d)i$,
$(a+bi)(c+di) = ac-bd+(ad+bc)i$.

Teorema Con gli elementi $1 = 1+0i$ e $0 = 0+0i$ si ha che $(\mathbb{C}, +, \cdot, 0, 1)$ è un campo

Dimostrazione La dimostrazione è lasciata come esercizio. □

I numeri complessi si possono rappresentare come punti del piano $\mathbb{R}^2$, mandando il numero $a+bi$ nel punto (a,b).

Definizione Dato $a+bi \in \mathbb{C}$, definiamo la sua *norma* come $|a+bi| = \sqrt{a^2+b^2}$, e il suo *coniugato* come $a+bi = a-bi$.

Proposizione Per ogni numero complesso z si ha che $|z|^2 = z\bar{z}$, e inoltre $\left|\frac{z}{|z|}\right| = 1$.

Dimostrazione La dimostrazione è lasciata come esercizio. □

Definizione Dato un numero complesso z di norma uguale a 1, l'angolo corrispondente al punto sulla circonferenza unitaria associato a z in $\mathbb{R}^2$ si chiama *argomento* di z, ed è definito a meno di aggiungere multipli di 2π. L'argomento è definito anche come quell'angolo per il quale vale (per z di norma unitaria)

$$z = cos(arg(z)) + isin(arg(z))$$

Se z è un numero complesso qualsiasi diverso da 0, definiamo $arg(z)$ come $arg(z) = arg\left(\frac{z}{|z|}\right)$.

Proposizione Dati due numeri complessi z, w diversi da 0, si ha che

$$|zw| = |z||w|,\ arg(zw) = arg(z) + arg(w)$$

Dimostrazione Se $s = arg(z)$ e $t = arg(w)$,, possiamo scrivere

$$z = |z|(cos(s) + isin(s)),\quad w = |w|(cos(t) + isin(t))$$

Si ha che

$$zw = |z||w|(cos(s) + isin(s))(cos(t) + isin(t)) =$$
$$|z||w|\left((cos(s)cos(t) - sin(s)sin(t)) + (cos(s)sin(t) + sin(s)cos(t))i\right)$$

Non dimostriamo il fatto (standard) che per ogni s, t vale

$$cos(s)cos(t) - sin(s)sin(t) = cos(s+t),\quad cos(s)sin(t) + sin(s)cos(t) = sin(s+t)$$

da cui seguono immediatamente le uguaglianze cercate (esercizio). □

La proposizione precedente permette di rappresentare graficamente il prodotto di numeri complessi: dati due numeri, il loro prodotto si ottene ruotando di un angolo pari alla somma degli angoli relativi ai due numeri iniziali, e allontanandosi dall'origine di una lunghezza pari al prodotto delle lunghezze relative ai due numeri iniziali.

Esempio Dato un numero complesso $z = a+bi$ diverso da zero, il numero complesso $z^{-1} = x+iy$ può essere trovato risolvendo il problema

$$(a+bi)(x+iy) = 1$$

Questo implica le condizioni $ax - by = 1$ e $ay + bx = 0$. Queste due condizioni determinano un sistema

$$\begin{cases} ax - by = 1 \\ bx + ay = 0 \end{cases}$$

Se $a \neq 0$, dalla prima equazione ricaviamo $x = \frac{1}{a}(1+by)$, e andando a sostituire nella seconda equazione $\frac{b}{a}(1+by) + ay = 0$, da cui$y = -(a + \frac{b^2}{a})^{-1}\frac{b}{a}$ e sostituendo

nella equazione per x si ottiene anche il valore di x. Se invece $a = 0$, allora deve essere $x = 0$ e $y = -\frac{1}{b}$.

CAPITOLO 2

Polinomi e algoritmo di Euclide

1. Polinomi

I polinomi sono somme formali, a cui possono essere associate delle funzioni.
Definizione Un polinomio nella variabile x a coefficienti nel campo K è una espressione del tipo $p(x) = \sum_{i=1}^{n} a_i x^i$, con $\{a_0, ..., a_n\} \subset K$. Se inoltre per qualche $m \leq n$ si ha che $a_m \neq 0$ e $\forall k > m \quad a_k = 0$ diciamo che p è di grado m, e scriviamo $deg(p) = m$. L'insieme dei polinomi nella variabile x a coefficienti nel campo K si indica con $K[x]$.
Definizione Un polinomio p determina una funzione da K a K, associando al numero c il valore $p(c) = \sum_{i=1}^{n} a_i c^i$.
Definizione Diciamo che due polinomi sono uguali se sono uguali tutti i loro coefficienti.
Proposizione Se le funzioni associate ai due polinomi p, q sono uguali, allora i due polinomi sono uguali.
Dimostrazione Dimostreremo questo fatto più avanti, quando avremo a disposizione le derivate. □
Definizione Dati due polinomi $p(x) = \sum_{i=1}^{n} a_i x^i, q(x) = \sum_{j=1}^{m} b_i x^i$ si definiscono la loro somma ed il loro prodotto come

$$(p+q)(x) = \sum_{i=0}^{max(m,n)} (a_i + b_i)x^i, \quad pq(x) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j x^{i+j}$$

Teorema $(K[x], +, \cdot, 0, 1)$ è un anello.
Dimostrazione esercizio. □
Teorema Dati due polinomi non nulli $p, q \in K[x]$, si ha che

$$deg(pq) = deg(p) + deg(q)$$

Dimostrazione Siano $h = deg(p)$, $k = deg(q)$. Si ha allora che $p = \sum_{i=0}^{h} a_i x^i$ e $q = \sum_{j=0}^{k} b_j x^j$, con $a_h \neq 0$ e $b_k \neq 0$. Si ha allora per definizione $pq = \sum_{i=0}^{h}\sum_{k=0}^{k} a_i b_j x^{i+j}$. Il massimo esponente per x in questa somma è $h+k$, e il suo coefficiente e' $a_h b_k$, che è diverso da zero in quanto sia che a_h che b_k sono diversi da zero. Quindi per definizione di grado, il grado di pq è esattamente $h+k$. □
Teorema Dati due polinomi $p(x) = \sum_{i=1}^{n} a_i x^i, q(x) = \sum_{j=1}^{m} b_i x^i$ e $c \in \mathbb{R}$, si ha che

$$(p+q)(c) = p(c) + q(c), \quad pq(c) = p(c)q(c)$$

Dimostrazione Esercizio. □
Esercizio: Dato il polinomio $p(x) = x^2 - 2$, si determinino i $c \in \mathbb{R}$ per cui $p(c) \geq 0$.

Definizione Diciamo che $\lambda \in K$ è una *radice* del polinomio $p(x)$ se $p(\lambda) = 0$.
Teorema *Teorema fondamentale dell'algebra* Ogni polinomio in $\mathbb{C}[x]$ di grado maggiore di zero ha almeno una radice in $\mathbb{C}$.
Dimostrazione Omettiamo la dimostrazione di questo teorema. □
Esempio Sia $p(x) = x^2 + 1 \in \mathbb{R}[x] \subset \mathbb{C}[x]$. Il polinomio p non ha radici in $\mathbb{R}$: se $\lambda \in \mathbb{R}$, si ha che $p(\lambda) = 1 + \lambda^2 \geq 1 > 0$. In $\mathbb{C}$ invece p ha due radici, i e $-i$.

2. Divisione fra polinomi

Così come per i numeri interi, esiste una nozione di divisione con resto fra i polinomi
Definizione Siano $p(x), s(x) \in K[x]$, con K un campo. Diciamo che $q(x), r(x) \in K[x]$ sono *quoziente* e *resto* della divisione di p per s se

$$p(x) = q(x)s(x) + r(x)$$

e $dex(r(x)) < deg(s(x))$.
Teorema Dati $p(x), s(x) \in K[x]$, con K un campo e $deg(s) > 0$, esistono e sono unici $q(x), r(x) \in K[x]$ *quoziente* e *resto* della divisione di p per s
Dimostrazione Per quanto riguarda l'unicità, supponiamo che esistano q_1, q_1, r_1, r_2 tali che

$$p(x) = q_1(x)s(x) + r_1(x), \quad p(x) = q_2(x)s(x) + r_2(x)$$

con $deg(r_1) < deg(p),\ deg(r_2) < deg(p)$. Facendo la differenza fra le due equazioni precedenti otteniamo

$$(q_1(x) - q_2(x))s(x) = -(r_1(x) - r_2(x))$$

Se $q_1 \neq q_2$, allora $q_1 - q_2 \neq 0$ e quindi il polinomio a sinistra ha grado pari a $deg(s) + deg(q_1 - q_2) \geq deg(s)$. A destra però abbiamo due polinomi di grado strettamente più piccolo del grado di s, e quindi la loro differenza ha grado strettamente più piccolo di quello di s, assurdo. Si deve quindi avere $q_1 = q_2$, e quindi anche $r_1 = r_2$.
La dimostrazione dell'esistenza è per induzione su $deg(p)$.
Se $deg(p) < deg(s)$, possiamo prendere $q = 0$ e $r = p$. Supponiamo di conoscere l'esistenza di q, r quando $deg(p) \leq n$, e sia $deg(p) = n+1$. Se $a \in K$ è il coefficiente di grado massimo di p e b è il coefficiente di grado massimo di s, il polinomio $p_1 = p - (\frac{a}{b}x^{deg(p)-deg(s)})s$ ha grado strettamente più basso del grado di p, e quindi esistono per ipotesi induttiva q_1, r_1 tali che

$$p_1(x) = q_1(x)s(x) + r_1(x)$$

con $deg(r_1) < deg(s)$. Si ha quindi che

$$p(x) = p_1(x) + (\frac{a}{b}x^{deg(p)-deg(s)})s = q_1(x)s(x) + r_1(x) + (\frac{a}{b}x^{deg(p)-deg(s)})s(x) =$$

$$\left(q_1(x) + \frac{a}{b}x^{deg(p)-deg(s)}\right)s(x) + r_1(x)$$

□
La dimostrazione del teorema fornisce anche un algoritmo per calcolare quoziente e resto in una divisione fra polinomi.
Esempio Dividere il polinomio $p(x) = 2x^4 + x^3 + -x^2 + 1$ e $s(x) = 3x^2 + 1$.
Definiamo q e r per approssimazioni successive, seguendo il metodo di dimostrazione del teorema.

$$p_1 = p - (\frac{a}{b}x^{deg(p)-deg(s)})s = 2x^4 + x^3 + -x^2 + 1 - \frac{2}{3}x^2(3x^2 + 1) = x^3 - \frac{5}{3}x^2 + 1$$

Ripetiamo il procedimento con p_1 al posto di p

$$p_2 = p_1 - \frac{1}{3}x(3x^2+1) = -\frac{5}{3}x^2 - \frac{1}{3}x + 1$$

Ripetiamo una terza volta il procedimento con p_2 al posto di p

$$p_3 = p_2 + \frac{5}{9}(3x^2+1) = -\frac{1}{3}x + \frac{14}{9}$$

Possiamo ora usare questo p_3 come r, e abbiamo

$$p = p_1 + \left(\frac{2}{3}x^2\right)s = p_2 + \left(\frac{1}{3}x + \frac{2}{3}x^2\right)s = p_3 + \left(-\frac{5}{9} + \frac{1}{3}x + \frac{2}{3}x^2\right)s$$

Riassumendo, abbiamo calcolato

$$p = \left(-\frac{5}{9} + \frac{1}{3}x + \frac{2}{3}x^2\right)(3x^2+1) + \left(-\frac{1}{3}x + \frac{14}{9}\right)$$

□

Definizione Diciamo che il polinomio s *divide* il polinomio p se esiste un polinomio q tale che $p(x) = q(x)s(x)$. In modo equivalente, s divide p se il resto della divisione di p per s è uguale a zero. In questo caso scriviamo $s|p$.

Teorema Il polinomio $p(x) \in K[x]$ ha la radice λ se e solo se il polinomio $x - \lambda$ divide p.

Dimostrazione Supponiamo che il polinomio $x - \lambda$ divida p. Per definizione, esiste q tale che $p(x) = q(x)(x - \lambda)$. Sostituendo λ in questa espressione otteniamo che $p(\lambda) = 0$.

Viceversa, supponiamo che λ sia una radice di p, e siano q, r il quoziente e il resto della divisione di p per $s = x - \lambda$. Per dimostrare che $x - \lambda$ divide p basta dimostrare che $r = 0$. Si ha

$$p(x) = q(x)(x - \lambda) + r(x)$$

con $deg(r) < 1$. Si ha quindi che deve essere $deg(r) = 0$, cioè $r \in K$, e quindi sostituendo λ nell'espressione si ha

$$p(\lambda) = 0 + r$$

e quindi deve essere $r = 0$ dato che $p(\lambda) = 0$ per ipotesi. □

Corollario Ogni polinomio $p(x) \in \mathbb{C}[x]$ di grado positivo si può scrivere come prodotto di $deg(p)$ polinomi di grado uno.

Dimostrazione Per induzione su $deg(p)$. Se $deg(p) = 1$ non c'è nulla da dimostrare. Se $deg(p) = n + 1 > 1$, sia $\lambda \in \mathbb{C}$ una radice di p. Per il teorema precedente, $p(x) = p_1(x)(x - \lambda)$. Per ipotesi induttiva, esistono $c \in \mathbb{C}$ e $\lambda_1, ..., \lambda_n$ tali che possiamo scrivere

$$p_1 = c\prod_{i=1}^{n}(x - \lambda_i)$$

da cui, chiamando per semplicità $\lambda = \lambda_{n+1}$,

$$p = c\prod_{i=1}^{n+1}(x - \lambda_i)$$

□

3. Algoritmo di Euclide

Definizione Dati due polinomi $p_1(x), p_2(x)$, il *massimo comun divisore* di p_1, p_2 è un polinomio $d(x)$ che ha coefficiente di grado massimo uguale a 1, che divide sia p_1 che p_2, e tale che ogni altro polinomio che divide sia p_1 che p_2 divide anche d. In massimo comun divisore si indica con $mcd(p_1, p_2)$. In formule,

$$mcd(p_1,p_2)|p_1 \wedge mcd(p_1,p_2)|p_2 \wedge (\forall s\ s|p_1 \wedge s|p_2 \implies s|mcd(p_1,p_2))$$

Proposizione Dati due polinomi, il loro massimo comun divisore quando esiste è unico.
Dimostrazione Siano d_1, d_2 due massimi comun divisori dei polinomi $p_1, p_2 \in K[x]$. Per definizione, si ha che d_1 divide d_2 e che d_2 divide d_1. Quindi deve essere $deg(d_1) = deg(d_2)$, e deve esistere $c \in K$ tale che $d_1 = cd_2$. Dato che il coefficiente di grado massimo di d_1 e di d_2 è uguale ad uno, deve essere $c = 1$ e quindi $d_1 = d_2$. □
Esempio Il massimo comun divisore di $p_1 = x^2 - 3x + 2$ e $p_2 = x^2 - 4x + 3$ è $x - 1$.
Dimostrazione Possiamo scrivere i due polinomi come $p_1 = (x-1)(x-2)$ e $p_2(x-1)(x-3)$, da cui è chiaro che $x - 1$ li divide entrambi. Se non fosse $x - 1 = mcd(p_1, p_2)$, dovrebbe esistere un polinomio $d(x) = mcd(p_1, p_2)$ di grado maggiore di uno (dato che $x - 1|d(x)$) che li divide entrambi, e dato che i due polinomi hanno grado due questo polinomio dovrebbe anch'esso avere grado due. Questo però implicherebbe che $d = p_1$ e $d = p_2$, cosa impossibile dato che $p_1 \neq p_2$. □
Teorema *(Algoritmo di Euclide)* Dati due polinomi $p, q \in K[x]$, il loro massimo comun divisore esiste, e si puo' scrivere come

$$mcd(p,q) = \alpha(x)p(x) + \beta(x)q(x)$$

per opportuni polinomi α, β.
Dimostrazione La dimostrazione dell'esistenza di d può essere fatta utilizzando l'*algoritmo di Euclide*. Per semplicità supporremo $deg(p) \geq deg(q)$ (altrimenti basta cambiare il nome ai due polinomi).
Definiamo una successione di polinomi $s_0, s_1, ..., s_t$ nel modo seguente: $s_0 = p$, $s_1 = q$. Supponiamo poi di avere definito $s_0, ..., s_n$, con $n \geq 1$, e distinguiamo i casi $deg(s_n) > 0$ e $deg(s_n) = 0$:
Se $deg(s_n) > 0$, definiamo s_{n+1} come il resto della divisione di s_{n-1} per s_n: deve quindi esistere un polinomio q_n tale che

$$s_{n-1} = q_n s_n + s_{n+1}$$

e inoltre $deg(s_{n+1}) < deg(s_n)$.
Se $deg(s_n) = 0$, o $s_n = 0$, e in questo caso definiamo $s_{n+1} = 0$, o $s_n = c \in K \setminus \{0\}$, e in questo caso definiamo $q_n = c^{-1}s_{n-1}$ e $s_{n+1} = 0$.
È chiaro che in questo modo si definisce una successione di polinomi tali che $deg(s_{n+1}) < deg(s_n)$ per tutti gli $n > 1$, e quindi da un certo punto in poi dovrà essere $s_n = 0$. Sia t un indice per cui $s_t \neq 0$ ma $s_{t+1} = 0$. Per come sono definiti gli s_n, dovrà essere $s_n = 0$ per tutti gli $n > t$ e quindi t è univocamente determinato. Se h è il coefficiente di grado massimo di s_t, definiamo $d = h^{-1}s_t$. Si ha che d può essere scritto come una combinazione del tipo

$$d = \alpha_n s_{n-1} + \beta_n s_n$$

per qualunque $n \in \{1, ..., t\}$: per $n = t$ basta prendere $\alpha_n = 0, \beta_n = h^{-1}$ e supponendo di sapere $d = \alpha_n s_{n-1} + \beta_n s_n$ per un certo $n > 1$ basta usare l'espressione

$s_n = s_{n-2} - q_{n-1}s_{n-1}$ nell'espressione per ottenere l'analoga espressione relativa all'indice $n-1$. In questo modo ci si riduce a $n = 1$, e quindi basta prendere $\alpha = \alpha_1, \beta = \beta_1$ per avere

$$d = \alpha s_0 + \beta s_1 = \alpha p + \beta q$$

come richiesto dall'enunciato del teorema.
Dimostriamo ora che questo d è effettivamente il massimo comun divisore di p e q. Supponiamo che un polinomio$r$ divida sia p che q. Per definizione, questo significa che esistono $v.w \in K[x]$ tali che $p = rv$ e $q = rw$. Sostituendo nell'espressione $d = \alpha(x)p(x) + \beta(x)q(x)$ si ottiene $d = \alpha rv + \beta rw = r(\alpha v + \beta w)$ e quindi r divide d. Per dimostrare che d divide sia p per q, dimostriamo che d divide tutti gli s_n. Chiaramente d divide s_t, e dato che $s_{t-1} = q_t s_t$ si ha che d divide anche s_{t-1}. Se però d divide due s_i consecutivi, diciamo s_n e s_{n+1}, allora d divide anche s_{n-1} in forza dell'espressione $s_{n-1} = q_n s_n + s_{n+1}$. Da questo ragionamento segue che d divide tutti gli s_n, e in particolare divide $s_0 = p$ e $s_1 = q$. Per come è stato definito, il coefficiente del termine di grado massimo di d è esattamente 1, e quindi abbiamo dimostrato che $d = (p, q)$. □
Esempio Siano $p = x^3 - 2x^2 - x + 2$ e $q = x^2 + 3x + 2$. Si calcoli il massimo comun divisore di p e q Seguendo l'algoritmo di Euclide, definiamo $s_0 = p, s_1 = q$, e dividiamo s_0 per s_1 per trovare s_2.

$$s_0 - xs_1 = x^3 - 2x^2 - x + 2 - x(x^2 + 3x + 2) = -5x^2 - 3x + 2$$

$$-5x^2 - 3x + 2 + 5s_1 = -5x^2 - 3x + 2 + 5(x^2 + 3x + 2) = 12x + 12$$

e quindi $s_2 = 12x + 12$.
Dividiamo s_1 per s_2 per trovare s_3:

$$s_1 - \frac{x}{12}s_2 = x^2 + 3x + 2 - x(x + 1) = 2x + 2$$

$$2x + 2 - \frac{1}{6}s_2 = 0$$

e quindi $s_3 = 0$. In questo caso quindi $t = 2$, e $d = \frac{1}{12}s_t = x + 1$:

$$mcd(x^3 - 2x^2 - x + 2, x^2 + 3x + 2) = x + 1$$

□

Teorema Siano $p_1, p_2 \in \mathbb{C}[x]$ e supponiamo che

$$p_1 = \lambda \prod_{i=1}^{m}(x - a_i)^{\alpha_i}, \quad p_2 = \mu \prod_{j=1}^{n}(x - b_j)^{\beta_j}$$

con gli a_i diversi fra loro e i b_j diversi fra loro, e sia gli α_1 che i β_i positivi (questo si può sempre supporre, in virtù del teorema fondamentale dell'algebra). Si ha allora che, supponendo $\{a_1, ..., a_n\} \cap \{b_1, ..., b_m\} = \{a_1, ..., a_k\} = \{b_1, ..., b_k\}$, deve essere

$$mcd(p_1, p_2) = \prod_{i=1}^{k}(x - a_i)^{min(\alpha_i, \beta_i)}$$

Dimostrazione Omettiamo la dimostrazione di questo teorema. □
Esempio $p_1 = x^3 - 6x^2 + 11x - 6$ e $p_2 = x^2 + 5x + 4$.
Un metodo per trovare il $mcd(p_1, p_2)$ è l'algoritmo di Euclide (esercizio). Un altro, alla luce del teorema precedente, è *fattorizzare* i polinomi. Per fattorizzare il primo osserviamo che 1 è una radice, e quindi certamente $(x - 1)$ lo divide. Facendo la

divisione, il quoziente che si ottiene è un polinomio di secondo grado, che possiamo fattorizzare usando la formula per le radici. Si ha che in questo caso

$$p_1 = (x-1)(x-2)(x-3) \quad p_2 = (x+1)(x+4)$$

e quindi $mcd(p_1, p_2) = 1$. □

L'algoritmo di Euclide ha il pregio di essere *effettivo*, nel senso che percorrendolo si ottiene un metodo per calcolare il massimo comun divisore fra p e q. Se ci interessasse soltanto dimostrare l'esistenza di d, potremmo procedere in modo molto più spedito come segue:

Definizione Dati n polinomi $p_1, ..., p_n \in K[x]$, definiamo l'insieme $(p_1, ..., p_n) \subset K[x]$ come

$$(p_1, ..., p_n) = \{s \in K[x] \mid \exists \alpha_1, ..., \alpha_n \in K[x] \ : \ s = \alpha_1 p_1 + \cdots + \alpha_n p_n\}$$

(l'insieme di tutti i polinomi che possono essere scritti come $\alpha_1 p_1 + + \cdots + \alpha_n p_n$ per qualunque scelta di polinomi $\alpha_1, ..., \alpha_n$) Un insieme di questo tipo si chiama anche *ideale*.

Teorema Si ha che esiste il massimo comun divisore di p e q, e inoltre

$$(p, q) = (mcd(p, q))$$

Dimostrazione Definiamo $S = \{deg(s) \mid s \in (p, q) \setminus \{0\}$ (l'insieme dei gradi dei polinomi non nulli in (p, q)). L'insieme S è un sottoinsieme non vuoto di $\mathbb{N} \cup \{0\}$ (contiene almeno $deg(p)$ e $deg(q)$), e quindi per il principio del buon ordinamento ha un minimo, che indichiamo con m. Prendiamo un qualunque polinomio $s_0 \in (p, q)$ di grado m, e se h è il coefficiente del suo termine di grado massimo, definiamo $d = h^{-1} s_0$.

Dimostriamo ora che $(p, q) = (d)$. Dato che $d \in (p, q)$ per costruzione, si ha che $(d) \subset (p, q)$ (esercizio). Se $s \in (p, q)$, dalla divisione

$$s = q_1 d + r_1$$

si vede che anche r_1 deve appartenere a (p, q) (basta scrivere $r_1 = s - q_1 d$ e ricordarsi la definizione di (p, q) e il fatto che $d \in (p, q)$). Dato che se $r_1 \neq 0$ dovrebbe essere $deg(r_1) < deg(d)$, che è assurdo, deve essere $r_1 = 0$ e quindi d divide s. Quindi $(p, q) \subset (d)$ e dato che vale anche l'altra inclusione, si ha $(p, q) = (d)$.

Dimostriamo ora che questo d è il massimo comun divisore di p e q. Dal fatto che $\{p, q\} \subset (p, q) = (d)$ segue che d divide sia p che q. Inoltre, dato che $d \in (p, q)$, esistono $\alpha, \beta \in K[x]$ tali che $d = \alpha p + \beta q$, e quindi qualunque polinomio che divide sia p che q deve dividere anche d. Poichè il coefficiente del termine di grado massimo di d è uno per costruzione, si ha che $d = mcd(p, q)$ come volevamo dimostrare. □

Esempio Scrivere l'ideale $(x^2 - 3x + 2, x^2 - 4x + 3)$ nella forma (d) per un opportuno polinomio d.

Basta trovare il mcd dei due polinomi, che facendo l'algoritmo di euclide (o fattorizzandoli) risulta essere $(x - 1)$, quindi si può prendere $d = x - 1$.