Campi

Def Un campo è un insieme non vuoto K munito di due operazioni binarie $+$ e $\cdot$ t.c.

1) K è un gruppo abeliano rispetto a $+$ con elemento neutro $0 \in K$
2) $K - \{0\}$ è un gruppo abeliano rispetto a $\cdot$ con elemento neutro $1 \in K$ e t.c. $1 \neq 0$
3) $\cdot$ è distributiva rispetto a $+$, cioè $a(b+c) = ab + ac \quad \forall\, a, b, c \in K$

Oss La proprietà distributiva collega $+$ e $\cdot$.

$+$ è detta addizione e $\cdot$ moltiplicazione di K

Si noti che $0 \cdot a = (0+0)a = 0a + 0a \Rightarrow 0a = 0$ $\forall\, a \in K$

Pertanto $+$ e $\cdot$ sono associative, commutative, ammettono elementi neutri 0 e 1 (ma chiediamo che $0 \neq 1$) e $\cdot$ è distributiva rispetto a $+$.

Esempi 1) $\mathbb{Q}$ = insieme dei numeri razionali è un campo rispetto alle usuali addizione e moltiplicazione $+$ e $\cdot$.

2) $\mathbb{R}$ = insieme dei numeri reali con le usuali addizione e moltiplicazione $+$ e $\cdot$.

Oss K campo, $a, b \in K$: $ab = 0 \Rightarrow a = 0$ o $b = 0$.

Numeri complessi

Def I numeri complessi sono le espressioni formali del tipo $a+ib$, con $a,b \in \mathbb{R}$.
La lettera i rappresenta l'unità immaginaria.
Poniamo $\mathbb{C} \stackrel{def}{=} \{a+bi \mid a,b \in \mathbb{R}\}$, l'insieme dei numeri complessi.

OSS I numeri complessi sono essenzialmente coppie ordinate di numeri reali $a+bi \longleftrightarrow (a,b)$.

Le operazioni di addizione e moltiplicazione di numeri complessi sono definite estendendo per distributività, associatività e commutatività le analoghe operazioni sui numeri reali, e con

$$i^2 = -1.$$

In questo modo $\mathbb{C}$ diventa un campo:
il campo dei numeri complessi.
Si noti che $\mathbb{R} \subset \mathbb{C}$ come sottocampo.

Si ha: $(a+bi)+(a'+b'i) = a+a'+(b+b')i$
(per definizione)
$$(a+bi)(a'+b'i) = aa'-bb'+(ab'+ba')i$$

Se $c = a+bi \in \mathbb{C}$, con $a,b \in \mathbb{R}$, poniamo
$\bar{c} \stackrel{def}{=} a-bi \in \mathbb{C}$ (coniugato di c)

Si ha $c\bar{c} = a^2-(bi)^2 = a^2-b^2i^2 = a^2+b^2 \in \mathbb{R}$

Poniamo anche $|c| \stackrel{\text{def}}{=} \sqrt{c\bar{c}} = \sqrt{a^2+b^2}$ (modulo di c)

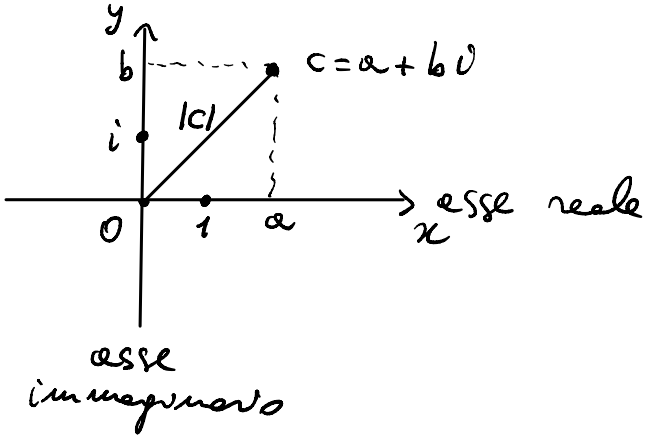
Quindi se $c \neq 0$, abbiamo

$$c^{-1} = \frac{\bar{c}}{c\bar{c}} = \frac{\bar{c}}{|c|^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}\, i$$

Si osservi che se $c \in \mathbb{R}$ allora $|c|$ coincide col valore assoluto di c.

<u>Piano di Gauss</u>:

numeri complessi identificati con punti del piano cartesiano.



$\text{Re}(a+bi) \stackrel{\text{def}}{=} a \in \mathbb{R}$ (<u>parte reale</u> di $a+bi$)

$\text{Im}(a+bi) \stackrel{\text{def}}{=} b \in \mathbb{R}$ (<u>parte immaginaria</u> di $a+bi$)

<u>Esempi</u> $(3+2i) + \left(4 - \frac{1}{2}i\right) = 7 + \frac{3}{2}i$

$$(3+2i)\left(4-\frac{1}{2}i\right) = 12 + 1 + \left(-\frac{3}{2}+8\right)i = 13 + \frac{13}{2}i$$

$$\overline{3+2i} = 3-2i$$

$$(3+2i)^{-1} = \frac{3-2i}{9+4} = \frac{3}{13} - \frac{2}{13}i$$

Si verifica facilmente che $\forall\, z, u \in \mathbb{C}$:

$\overline{zu} = \bar{z}\,\bar{u}$, $\overline{(z^{-1})} = (\bar{z})^{-1}$, $\overline{(\bar{z})} = z$, $\overline{(z+u)} = \bar{z} + \bar{u}$

$|zu| = |z|\,|u|$

$\mathbb{Z}_n$

Def Siano $m, n \in \mathbb{Z}$ due interi, con $n \neq 0$.

m è divisibile per n se $\exists\, q \in \mathbb{Z}$ t.c. $m = nq$ e scriviamo $n \mid m$ (n divide m).

Sia ora $n \in \mathbb{N}$, $n \geq 2$. Su $\mathbb{Z}$ definiamo la relazione

$$a \equiv_n b \iff n \mid (a-b), \text{ cioè } a-b \text{ è divisibile per } n$$

Se $a \equiv_n b$ scriviamo anche $a \equiv b \pmod n$

(si legge a congruente a b modulo n)

Mostriamo che è una relazione d'equivalenza:

1) riflessiva: $a - a = 0 = 0n \Rightarrow a \equiv_n a$

2) simmetrica: $a \equiv_n b \Rightarrow a - b = nq$ per un certo $q \in \mathbb{Z}$

$\Rightarrow b - a = n(-q) \Rightarrow b \equiv_n a$

3) transitiva: $a \equiv_n b$ e $b \equiv_n c \Rightarrow$

$a - b = nq$ e $b - c = nq'$ per certi $q, q' \in \mathbb{Z}$

$\Rightarrow a - b + b - c = nq + nq' \Rightarrow a - c = n(q+q')$

$\Rightarrow a \equiv_n c$.

Esempio Per $n = 2$, $a \equiv b \pmod 2 \iff a - b$ è pari

$\iff a$ e b entrambi pari o dispari.

Classi di equivalenza (digressione)

Supponiamo che su un insieme X sia data una relazione di equivalenza $\sim$.

$$x \in X \rightsquigarrow [x] \stackrel{\text{def}}{=} \{ y \in X \mid x \sim y \} \subset X$$

classe di equivalenza di $x \in X$.

Le classi di equivalenza hanno le seguenti proprietà:

1) $x \in [x]$ per la proprietà riflessiva
2) $[x] \cap [y] \neq \emptyset \iff x \sim y$ e $[x] = [y]$

(proprietà simmetrica e transitive)

Pertanto due classi d'equivalenza o sono disgiunte oppure sono coincidenti.

Qualunque $x' \in [x]$ è detto rappresentante della classe $[x]$.

Possiamo considerare l'insieme delle classi d'equivalenza

Def Sia X un insieme e $\sim$ una relazione d'equivalenza su X. L'insieme delle classi d'equivalenza di X rispetto a $\sim$ si denota con

$$X/\sim \stackrel{\text{def}}{=} \{ [x] \mid x \in X \}$$

e si chiama insieme quoziente.

Possiamo definire una funzione suriettiva

$$\pi : X \longrightarrow X/\sim, \quad \pi(x) \stackrel{\text{def}}{=} [x]$$

(funzione quoziente o proiezione)

Torniamo alla congruenza modulo n in $\mathbb{Z}$.

Def Sia $n \in \mathbb{N}$, $n \geq 2$, e sia $a \in \mathbb{Z}$. La classe d'equivalenza $[a]_n$ di a rispetto a $\equiv_n$ è detta <u>classe di congruenza</u> di a $(\mathrm{mod}\ n)$.

Pertanto $a \in [a]_n$ e $[a]_n \cap [b]_n \neq \emptyset \iff a \equiv_n b$
$\iff [a]_n = [b]_n$

Si osservi che $b \in [a]_n \iff \exists\, k \in \mathbb{Z}$ t.c.
$b - a = kn \iff b = a + kn$, $k \in \mathbb{Z}$.

Quindi $[a]_n = \{ a + kn \mid k \in \mathbb{Z} \}$
Per questa ragione si scrive anche

$$[a]_n = a + n\mathbb{Z} \quad (\text{notazione})$$

Def L'insieme quoziente di $\mathbb{Z}$ rispetto a $\equiv_n$ si denota con $\mathbb{Z}_n$ (oppure con $\mathbb{Z}/n$), cioè

$$\mathbb{Z}_n \overset{\text{def}}{=} \{ [a]_n \mid a \in \mathbb{Z} \} \quad (\text{interi modulo } n)$$

Teorema $\mathbb{Z}_n$ ha n elementi: $[0]_n, [1]_n, \dots, [n-1]_n$

Dim $a \in \mathbb{Z}$ div. con resto di a per n

$\rightsquigarrow \exists!\, q \in \mathbb{Z}$ e $0 \leq r < n$ t.c.
$a = nq + r \Rightarrow a \equiv r \ (\mathrm{mod}\ n)$.