$(G, +)$ gruppo (abeliano)

ALLORA $(G^n, +^n)$ é un gruppo (abeliano)

$$G^n = \{(g_1, g_2, \dots g_n) \mid g_i \in G\}$$

$$(g_1, g_2 \dots g_n) +^n (h_1, h_2, \dots h_n) := (g_1+h_1 \; g_2+h_2 \dots g_n+h_n)$$

operazione definita componente per componente

El. neutro di G $= 0$

El. neutro di $(G^n, +^n)$ $\quad 0^n := (0, 0 \dots 0)$

$$(g_1, g_2 \dots g_n) +^n (-g_1, -g_2 \dots, -g_n) = (0 0 \dots 0)$$

$(g_1 \dots g_n), (h_1 \dots h_n), (l_1 \dots l_n) \in G^n$

$\Rightarrow (g_1 \dots g_n) +^n ((h_1 \dots h_n) +^n (l_1 \dots l_n)) =$

$= (g_1 \dots g_n) +^n (h_1 + l_1 \dots h_n + l_n) =$

$= (g_1 + (h_1 + l_1) \dots g_n + (h_n + l_n)) =$

$= ((g_1 + h_1) + l_1 \dots (g_n + h_n) + l_n) =$

$= \dots = ((g_1 \dots g_n) +^n (h_1 \dots h_n)) +^n (l_1 \dots l_n)$

associativa

IDEM per commutativa.

Si può mostrare che pure $(G \times H, * \times \Delta)$ ove $(G, *)$ e (H, Δ) sono gruppi è un gruppo rispetto le operazione

$$(* \times \Delta) : (G \times H) \times (G \times H) \longrightarrow (G \times H)$$
$$(g, h), (g', h') \rightarrow (g * g', h \Delta h')$$

è un gruppo.

Il prodotto cartesiano di 2 gruppi è un gruppo rispetto le operazioni definite componente per componente.

NOZIONE DI CAMPO. → proprietà degli insiemi numerici su cui si può studiare e risolvere l'equazione

$$\boxed{a \cdot x + b = 0} \qquad a \neq 0$$

$$ax+b+(-b) = 0+(-b)$$

$$ax = -b \qquad a \neq 0$$

$$a^{-1}(ax) = a^{-1}(-b)$$

$$\begin{gathered} a^{-1}(ax) \\ \parallel \\ x \end{gathered}$$

$$x = a^{-1}(-b)$$

Un campo $\mathbb{K}$ é una struttura algebrica $(\mathbb{K}, +, \cdot)$ con 2 operazioni binarie tale che

1) $(\mathbb{K}, +)$ é un gruppo abeliano con el. neutro 0
2) $(\mathbb{K} \setminus \{0\}, \cdot)$ é un gruppo (abeliano)
3) valgono le prop. distributive $a(b+c) = ab+ac$
   $(a+b)c = ac+bc$

<u>OSS</u>: quando consideriamo il prodotto diciamo

$$(\mathbb{K} \setminus \{0\}, \cdot)$$

é un gruppo (abeliano).

<u>OSS</u>: 0 non può essere un elemento invertibile in $\mathbb{K}$ rispetto il prodotto.

$\forall k \in \mathbb{K}$: $\quad 0 \cdot k = k \cdot 0 = 0$

$$0 \cdot k = (0+0) \cdot k = 0 \cdot k + 0 \cdot k$$

sommando a dx e sx $\quad - 0 \cdot k$

si ottiene

$$0 = (-0 \cdot k) + 0 \cdot k = (-0 \cdot k) + 0 \cdot k + 0 \cdot k = 0 \cdot k$$

Vale la legge di annullamento del prodotto

$$a \cdot b = 0 \quad \text{in } \mathbb{K} \Rightarrow a = 0 \text{ oppure } b = 0$$

$a \cdot b = 0 \Rightarrow$

se $a = 0$ non c'è nulla da verificare in più.

se $a \neq 0 \Rightarrow \exists\, a^{-1} \in \mathbb{K} : a^{-1} a = 1$

$$\Rightarrow \quad a^{-1}(ab) = a^{-1} 0 = 0$$

$$a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$$

$(\mathbb{Q}, +, \cdot)$
$(\mathbb{R}, +, \cdot)$
$(\mathbb{C}, +, \cdot)$
CAMPI

$(\mathbb{Z}, +, \cdot)$
NON È UN CAMPO

gli unici el. invertibili sono $+1, -1$!!

$\mathbb{Z}_3 = \{-1, 0, 1\}$

rispetto somma e prodotto con $\left(\begin{array}{l} 1+1=-1 \\ -1-1=1 \end{array} \right.$

AFFERMO CHE $(\mathbb{Z}_3, +, \cdot)$ è un campo.

+	-1	0	1
-1	1	-1	0
0	-1	0	1
1	0	1	-1

$\cdot$	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

operazioni ovvero

verifichiamo che vale la legge di annullamento del prodotto. e che + e $\cdot$ sono operazioni di gruppo su $\mathbb{Z}_3$ e $\mathbb{Z}_3 \setminus \{0\}$.

valgono anche le distributive.

a	b	c	$b+c$	$a(b+c)$	$ab+ac$
1	0	0	0	0	$0+0=0$
1	0	1	1	1	$0+1=1$
1	1	0	1	+1	$1+0=1$
1	1	1	-1	-1	$1+1=-1$
1	1	-1	0	0	$1-1=0$
1	-1	0	-1	-1	$1\cdot -1+1\cdot 0=-1$
1	-1	1	0	0	$1\cdot -1+1\cdot 1=0$
1	-1	-1	1	1	$1\cdot -1+1\cdot -1=1$
1	0	-1	-1	-1	$1\cdot 0+1\cdot -1=-1$

con $a=-1$ si cambiano tutti i segni

→ valgono le prop. distributive.

$\mathbb{Z}_2 = \{0, 1\}$

bits

+	0	1
0	0	1
1	1	0

XOR

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

AND

$(\mathbb{Z}_2, +, \cdot)$ CAMPO CON 2 ELEMENTI

$(\mathbb{Z}_n, +, \cdot)$ con $n \geq 2$ intero.

$a, b \in \{0, 1, \ldots, n-1\}$.

$a + b := (a+b) \% n$

$a b := (a \cdot b) \% n$

resto della divisione per n del numero precedente.

$(\mathbb{Z}_5, +, \cdot)$

$3+3 = 6 \,\%\, 5 = 1$

$(\mathbb{Z}_2, +, \cdot)$

$1+1 = 2 \,\%\, 2 = 0$ $\quad$ $1+0 = 1 \,\%\, 2 = 1$

$1 \cdot 1 = 1 \,\%\, 2 = 1$

$\{0, 1, 2\}.$ $\quad$ $1+1 = 2 \,\%\, 3 = 2$

$2+1 = 3 \,\%\, 3 = 0$ $\quad$ "2" = "-1"

Quando $\mathbb{Z}_n$ è un campo?

In generale 1) $(\mathbb{Z}_n, +)$ è un gruppo abeliano

2) valgono sempre le proprietà distributive

3) Il prodotto è commutativo, associativo ed ha el. neutro 1

MA

AFFINCHÉ OGNI ELEMENTO DI $\mathbb{Z}_n$ DIVERSO DA 0 ABBIA INVERSO SERVE CHE n SIA UN NUMERO PRIMO (E BASTA)

$(\mathbb{Z}_n, +, \cdot)$ CAMPO $\Leftrightarrow$ n primo.

In $\mathbb{Z}_4$

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

$2 \cdot 2 = 0$

MA $2 \neq 0$

$\Rightarrow$ 2 NON È INVERTIBILE

$(\mathbb{Z}_4, +, \cdot)$ NON È UN CAMPO.

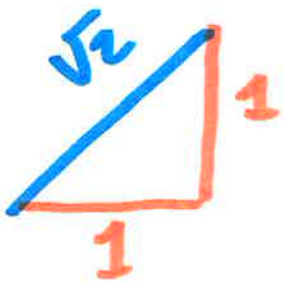
Tutta la teoria sviluppata per campi arbitrari (algebra lineare) si applica anche ai campi $\mathbb{Z}_p$ p primo o a campi più complicati.

$(\mathbb{Q}, +, \cdot)$ NUMERI RAZIONALI

$(\mathbb{R}, +, \cdot)$ NUMERI REALI

$(\mathbb{C}, +, \cdot)$ CAMPO DEI NUMERI COMPLESSI.

$x^2+1=0$ in $\mathbb{R}$ non ha soluzione.



$\mathbb{C} = \{(a,b) \mid a,b \in \mathbb{R}\}.$

$(a,b) = a+ib$

$\boxed{(a,b)+(c,d)=(a+c,\ b+d)}$ $\qquad i^2=-1$

$(a+ib)+(c+id) = a+c + i(b+d)$

$(a,b)\cdot(c,d) = (ac-bd,\ bc+ad)$

$(a+ib)(c+id) = ac + iad + ibc + i^2bd =$
$= (ac-bd)+i(ad+bc).$

$(a,b) \in \mathbb{C} \quad \exists \quad (x,y) \in \mathbb{C}$ tale che

(*) $\boxed{(a,b)\cdot(x,y) = (1,0)}$ $\quad (a,b) \neq (0\,0)$.

$(1,0)\cdot(a,b) = (a,b)\cdot(1,0) = (a,b)$

altra $\quad (a+ib)(x+iy) = 1 + i\cdot 0 = 1$

$$(*) \begin{cases} ax - by = 1 \\ ay + bx = 0 \end{cases} \qquad (a,b)\cdot(x,y) = (ax-by,\, ay+bx)$$

2 equazioni in 2 incognite.

~~[illegible]~~ $a=0$, $b\neq 0$ $\quad \begin{cases} -by = 1 \\ bx = 0 \end{cases} \rightarrow \quad x=0, \quad y = -\frac{1}{b}$

$\cancel{(\alpha,\beta)}$ $\quad (0,b)\cdot\left(0,-\frac{1}{b}\right) =$

$= (0 - -1, 0+0) = (1,0) = 1$ ✓

$a\neq 0$ $\quad \begin{cases} ax - by = 1 \\ ay = -bx \end{cases} \qquad \begin{cases} y = -\frac{b}{a}x \\ \frac{a^2+b^2}{a}x = 1 \end{cases}$

$x = \frac{a}{a^2+b^2} \qquad y = \frac{-b}{a^2+b^2}$

N.B. $a^2+b^2>0$ in quanto $a\neq 0$.

Teorema fondamentale dell'algebra.

Il campo $(\mathbb{C}, +, \cdot)$ è algebricamente chiuso.

$\rightarrow$ OGNI EQUAZIONE $f(x) = 0$ con $f(x) \in \mathbb{C}[x]$ (cioè $f(x)$ polinomio in x a coeff. in $\mathbb{C}$) e $\deg f(x) \geq 1$ AMMETTE ALMENO UNA SOLUZIONE IN $\mathbb{C}$

($\Rightarrow$ $f(x) = 0$ AMMETTE $n = \deg f(x)$ soluzioni in $\mathbb{C}$ contate con le debite molteplicità).

Supponiamo che ogni equazione $f(x)=0$ con $\deg(x)=n\geq 1$ ammetta almeno una sol. in $\mathbb{C}$ $\Rightarrow$ $\exists \beta, \alpha_1 \dots \alpha_n \in \mathbb{C}$ tali che

$$f(x)=\beta(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$$

con $\beta\neq 0$

$f(x)$ <u>si spezza</u> in termini di grado 1
$\Rightarrow f(x)$ ha n radici $\alpha_1, \alpha_2 \dots \alpha_n$

- Se $\deg f(x)=1 \Rightarrow f(x)=\beta(x-\alpha_1)$ $\square$

Se $\deg f(x)=n \Rightarrow$ per ipotesi $\exists\, \alpha_n$ tale che $f(\alpha_n)=0 \Rightarrow$ per Ruffini $\exists\, g_{n-1}(x)\in\mathbb{C}[x]$

tale che

$$f(x) = g_{n-1}(x)(x-\alpha_n) \quad e$$

$\deg g_{n-1}(x) = n-1$.

iteriamo...

$$f(x) = \boxed{g_{n-1}(x)}(x-\alpha_n) =$$

$$= \boxed{g_{n-2}(x)(x-\alpha_{n-1})}(x-\alpha_n)$$

$= \dots$ fino a che non si ha $g_1(x) = \beta(x-\alpha_1)$

Dato $(\mathbb{C}, +, \cdot)$ e $z \in \mathbb{C}$ con $z = a+ib$

$$\overline{z} := a - ib$$

(coniugato di z).

1) $z = \bar{z} \iff a+ib = a-ib \iff b=0$

in particolare identifichiamo i numeri complessi con $b=0$ con i numeri reali.

$a + i \cdot 0 = a$

2) $z + \bar{z} = (a+ib) + (a-ib) = 2a \in \mathbb{R}$

$Re(z) := \frac{1}{2}(z+\bar{z})$ parte reale di z.

3) $z - \bar{z} = (a+ib) - (a-ib) = 2ib$

$Im(z) := \frac{1}{2i}(z-\bar{z}) \in \mathbb{R}$ parte immaginaria di z.

4) $z \cdot \overline{z} = (a+ib)(a-ib) = a^2+b^2 \geq 0 \in \mathbb{R}$

$|z| := \sqrt{z\overline{z}} \in \mathbb{R}$ modulo di z

<u>N.B</u> se $x \in \mathbb{R}$ $\quad \sqrt{x^2} = |x|$ non è x !!!

Se $z = \overline{z} \Rightarrow z = a$ con $a \in \mathbb{R}$

$$\Rightarrow \sqrt{z\overline{z}} = \sqrt{a^2} = |a| \in \mathbb{R}$$

5) $z \in \mathbb{C} \setminus \{0\} \Rightarrow \dfrac{1}{z}$ per il reciproco di z.

$$\frac{1}{z} = \frac{1}{z} \cdot 1 = \frac{1}{z} \cdot \frac{\overline{z}}{\overline{z}} = \frac{\overline{z}}{z\overline{z}}$$

$$\bar{z} = a - ib$$
$$z\bar{z} = a^2 + b^2 \Rightarrow \frac{\bar{z}}{z\bar{z}} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$$

Sia $f(x) \in \mathbb{C}[x]$ un polinomio a coeff. in $\mathbb{C}$ nell'incognita x

e sia α una sua radice $f(\alpha) = 0$

OSSERVIAMO CHE $\overline{f(\alpha)} = \bar{f}(\bar{\alpha})$

infatti

$$\overline{z+w} = \bar{z} + \bar{w}$$
$$\overline{zw} = \bar{z} \cdot \bar{w}$$

verifica con conti.

il coniugio é un automorfismo di $(\mathbb{C}, +, \cdot)$

cioè preserva le operazioni

CONIUGIO ADDENDI + SOMMA =

= SOMMA + CONIUGIO RISULTATO

CONIUGIO MOLTIPLICANDI + PRODOTTO =

PRODOTTO + CONIUGIO RISULTATO.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots$$

$$\Rightarrow \overline{f(x)} = \bar{a}_0 + \bar{a}_1 x + a_2 (\bar{x})^2 + \dots = \bar{f}(\bar{x})$$

$$f(\alpha) = 0 \Rightarrow \overline{f(\alpha)} = 0 = \bar{f}(\bar{\alpha})$$

Supponiamo $f(x) \in \mathbb{R}[x]$

polinomio a coeff. reali.

$$\bar{f}(x) = \bar{a}_0 + \bar{a}_1 x + \bar{a}_2 x^2 + \ldots =$$

$$= a_0 + a_1 x + a_2 x^2 + \ldots$$

perché $a_i \in \mathbb{R}$ e quindi $\bar{a}_i = a_i$

Sia α una radice complessa di $\bar{f}(x)$

$$\Rightarrow \quad f(\alpha) = 0 \quad \Rightarrow \quad \overline{f(\alpha)} = 0 \Rightarrow$$

$$\bar{f}(\bar{\alpha}) = 0 \Rightarrow f(\bar{\alpha}) = 0$$

α ed $\bar{\alpha}$ sono entrambe radici di

$f(x) \in \mathbb{R}[x]$

In particolare se $f(x)$ reale ed α radice di $f(x) \Rightarrow$

- $\alpha = \bar{\alpha}$ cioè $\alpha \in \mathbb{R} \Rightarrow (x-\alpha)$ divide $f(x)$
  cioè $f(x) = g(x)(x-\alpha)$
  $\deg g(x) = \deg f(x) - 1$
- $\alpha \neq \bar{\alpha} \Rightarrow$ sia $(x-\alpha)$ che $(x-\bar{\alpha})$ dividono $f(x) \Rightarrow (x-\alpha)(x-\bar{\alpha})$ divide $f(x) \Rightarrow$
  $(x^2 - (\alpha+\bar{\alpha})x + \alpha\bar{\alpha}) \in \mathbb{R}[x]$
  divide $f(x)$

OGNI POLINOMIO $f(x) \in \mathbb{R}[x]$

SI PUÒ SEMPRE SCRIVERE COME PRODOTTO DI TERMINI DI GRADO 1 o 2

(polinomi reali anche essi).

$$5 \left\langle \begin{array}{l} 1+1+1+1+1 \\ 1+1+1+2 \\ 1+2+2 \end{array} \right.$$