GRUPPI (ANCORA)

Note Title 11/29/2017

Sia G un sottogp finitamente generato di $(\mathbb{Q}, +)$. Dimostrare che G e' ciclico

Oss • $(\mathbb{Q}, +)$ non e' isomorfo a $(\mathbb{Z}, +)$

$\underbrace{x + \ldots + x}_{n} = a$ si risolve sempre in $\mathbb{Q}$, ma non in $\mathbb{Z}$

• $\{$Razionali con denominatore $| 2\} \simeq (\mathbb{Z}, +)$

$$\frac{1}{2} \longleftarrow\!\shortmid\ 1$$

Sia $G = \langle q_1, \ldots, q_r \rangle$. Posso scegliere $M \in \mathbb{N}$ che sia un denominatore comune per $q_1, \ldots, q_r$.

Allora $\forall x \in G$ si ha $x \in \left\{ \frac{a}{M} \mid a \in \mathbb{Z} \right\} = \frac{1}{M}\mathbb{Z}$

$\left(\frac{1}{M}\mathbb{Z}, +\right)$ e' un gruppo, isomorfo a $(\mathbb{Z}, +)$

$$f : (\mathbb{Z}, +) \longrightarrow \left(\frac{1}{M}\mathbb{Z}, +\right)$$
$$1 \longmapsto \frac{1}{M}$$

f è un isomorfismo : → omo di gp
→ iniettivo
→ surgettivo } l'inversa è $\times M$

$$\frac{1}{M}x + \frac{1}{M}y = \frac{1}{M}(x+y) \qquad \forall x, y \in \mathbb{Z}$$

Conclusione: $G < \frac{1}{M}\mathbb{Z} \simeq \mathbb{Z}$

Sappiamo dalla teoria che tutti i sottogp. di $\mathbb{Z}$ sono ciclici (quindi $f^{-1}(G)$ è ciclico $\Rightarrow G$ cicl.)

$$q_1 = \frac{a_1}{M}, \quad \dots, \quad q_r = \frac{a_r}{M}$$

$f^{-1}(G)$ è il sottogp di $\mathbb{Z}$ generato da $(a_1, \dots, a_r)$, ovvero il sottogp generato dal $MCD(a_1, \dots, a_r)$

Teorema di Sylow per gruppi abeliani

$(G,+)$ abel. finito, p primo, $a \in \mathbb{N}$ t.c.

$$p^a \,\|\, |G| \qquad (p^a \mid |G|,\ p^{a+1} \nmid |G|)$$

(i) $H = \{x \in G : p^a x = 0\}$ è un sottogp.

(ii) Dim. che G/H non ha elem. di ordine p

(iii) $\# H = p^a$

(i) $x \in H \quad y \in H \overset{?}{\Longrightarrow} x+y \in H$

$$p^a(x+y) = (\underbrace{x + \dots + x}_{p^a}) + (\underbrace{y + \dots + y}_{p^a})$$

$$= 0 + 0 = 0$$

Questo basta per dire che H e' un sottogruppo
[stiamo usando che G e' finito]

(ii) Sia $x + H \in G/H$ di ordine p $(x \in G)$

$$\Longrightarrow \begin{cases} x \notin H \\ px \in H \Longrightarrow p^a(px) = 0 \end{cases}$$

$\uparrow px \in H$

$\left(x^{p^{a+1}} = 1\right)$ in notaz. moltiplicativa

$$\Longrightarrow \operatorname{ord}_G(x) \mid p^{a+1}$$

$$\operatorname{ord}_G(x) \mid \# G$$

$$\Longrightarrow \operatorname{ord}_G(x) \mid (p^{a+1}, \# G) = p^a$$

$\Rightarrow \quad p^a x = 0 \quad \Rightarrow \quad x \in H$, assurdo

(iii) G/H non ha elementi di ordine p

$$\Rightarrow \quad \left| G/H \right| \not\equiv 0 \ (p)$$

contronominale di Cauchy

$$\left| G/H \right| = |G|/|H|$$

$\Rightarrow \quad ord(H) \equiv 0 \ (p^a)$ (tutti i fattori p nel rapporto $|G|/|H|$ si cancellano)

Inoltre $ord(H)$ è una potenza di p.

$\forall h \in H \quad ord(h) \mid p^a$

Se $ord(H)$ non fosse una potenza di p, esisterebbe un primo $q \neq p$ t.c. $q \mid ord(H)$

$\overset{\text{Cauchy}}{\Longrightarrow}$ H avrebbe un elemento di ordine q, assurdo. $\Rightarrow ord(H) = p^k$, $k \geq a$

Infine $|H| \mid |G|$, quindi $k \leq a$ $\boxed{\text{FINE}}$

Altri quozienti

G gruppo abeliano, $K, H < G$

$m = [G : H]$ $\qquad$ $n = [G : K]$ $\leftarrow$ indice di K in G $= \left| G/K \right|$

$d = [G : K \cap H]$

(b) $d \mid mn$

(c) $d = mn \iff K + H = G$

(b) Basta trovare $f : G/_{K \cap H} \hookrightarrow G/K \times G/H$

$$\varphi : G \longrightarrow G/K \times G/H \quad \text{omomorfismo}$$
$$x \longmapsto (x + K, x + H)$$

$$\ker(\varphi) = \{x : x + K = K \text{ e } x + H = H\}$$
$$= \{x \in G : x \in K \text{ e } x \in H\} = K \cap H$$

Per il 1° teo di omomorfismo,

$$\frac{G}{\ker \varphi} = \frac{G}{K \cap H} \simeq \mathrm{Im}(\varphi) < G/K \times G/H$$

quindi $d = \left|\frac{G}{K\cap H}\right| = |\mathrm{Im}\,\varphi| \;\Big|\; \mathrm{ord}\left(G/_K \times G/_H\right)$

$\Rightarrow d \mid mn$

(c) $d = mn \iff |\mathrm{Im}\,\varphi| = |G/_K \times G/_H|$

$\iff \mathrm{Im}\,\varphi = G/_K \times G/_H$

$\iff \varphi$ e' surgettiva

$\overset{?}{\iff} K + H = G$

$\boxed{\Leftarrow}$ Sia $G = K+H$, dim. φ surgettiva

Voglio: $\forall a,b \in G$ $\exists x \in G$ $(x+K, x+H) = (a+K, b+H)$

$x + K = a + K \iff \exists k \in K$ t.c. $x - a = k$

$x + H = b + H \iff \exists h \in H$ t.c. $x - b = h$

$\Rightarrow b - a = k - h$

Siccome $K + H = G$, esistono $k \in K$ e $h \in H$ t.c. $b - a$ (che e' un elem. di G) si scriva come $k - h = k + (-h)$

Prendo $x := a + k = a + (b-a) + h = b + h$

$$\varphi(x) = (a + k + K,\ a + k + H)$$

$$= (a + K,\ b + h + H) = (a + K,\ b + H)$$

$\boxed{\Longrightarrow}$ Supponiamo φ surgettiva, dim $G = K + H$

$\forall g \in G \quad \exists x \in G$ t.c.

$$\underset{\displaystyle (x+K,\ x+H)}{\underset{\|}{\varphi(x)}} = (g + K,\ H)$$

$$\Longrightarrow \begin{cases} g - x \in K \\ x \in H \end{cases} \qquad g = \underset{K}{\underset{\cap}{(g-x)}} + \underset{H}{\underset{\cap}{x}}$$

CENTRO, CENTRALIZZATORE, NORMALIZZATORE

G gruppo. Il suo CENTRO è

$$Z(G) = \{ g \in G \mid \forall h \in G \quad gh = hg \}$$

PROP $Z(G)$ è un sottogruppo (normale) di G

Dim
- $e_G \in Z(G)$ ok $e_G \cdot h = h \cdot e_G \quad \forall h \in G$
- $x, y \in Z(G) \overset{?}{\Longrightarrow} xy \in Z(G)$

$$(xy) \cdot h = x \cdot (yh) = (yh) \cdot x$$
$$= (h \cdot y) \cdot x = h \cdot (y \cdot x) = h \cdot (xy)$$

- $x \in Z(G) \overset{?}{\Longrightarrow} x^{-1} \in Z(G)$

$$x^{-1} \cdot h \overset{?}{=} h \cdot x^{-1} \qquad \forall h \in G$$

$$\Longleftrightarrow \quad x \cdot (x^{-1} h) \overset{?}{=} x \cdot h \cdot x^{-1}$$

$$\Longleftrightarrow \quad x\, x^{-1} h\, x \overset{?}{=} x\, h\, x^{-1} x$$

$$\Longleftrightarrow \quad hx = xh \quad \text{sì perché } x \in Z(G)$$

OSS $Z(G)$ è abeliano

Normalità: $\forall h \in G, \quad h\,Z(G) = Z(G)\,h$

che è vero perché

$$h Z(G) = \{ hz \mid z \in Z(G) \}$$
$$= \{ zh \mid z \in Z(G) \} = Z(G) h \qquad \square$$

Esempi

- $Z(\mathbb{Z}) = \mathbb{Z}$
- $Z(S_3) = \{ id_{S_3} \}$

$(1,2)$ e $(1,3)$ non commutano

$(3,2)$ e $(3,1)$ ——————

$(1,2,3)$ e $(1,2)$ ——————

- $Z(D_6) = \{1, r^3\}$

$D_6 = \{1, r, r^2, \dots, r^5;\ s, sr, sr^2, \dots, sr^5\}$

r rotaz di $\frac{2\pi}{6}$

$rs = sr^5$

$r^3 s = r^2 (rs) = r^2 s r^5$

$= r(rs) r^5$

$= r(sr^5) r^5$

$= s r^{15} = s r^3$

Def $H < G$. Il CENTRALIZZATORE di H in G è

$$Z_G(H) = \{g \in G : gh = hg \quad \forall h \in H\}$$

È un sottogruppo

Def $H < G$. Il normalizzatore di H in G è $N_G(H) = \{g : ghg^{-1} \in H \quad \forall h \in H\}$

$N_G(H)$ è il più grande sottogruppo di G in cui H è normale.

$$H < N_G(H)$$

ANELLI

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$
- $\mathbb{Z}, \quad \mathbb{Z}/n\mathbb{Z}$
- $\mathbb{Z}[x], \mathbb{R}[x], \mathbb{Z}/p\mathbb{Z}[x]$ e i loro quozienti

Polinomi

$$p(x) = x^5 + x^4 + x^3 + x^2 + x + 1$$

$\mathbb{C}[x] \qquad \mathbb{Z}/13\mathbb{Z}[x] \qquad \mathbb{R}[x] \qquad$ fattorizz. unica

$\mathbb{Z}[x]$

Fattorizz. di $p(x)$ in $\mathbb{C}[x]$

$$p(x) = \frac{x^6 - 1}{x-1} = \frac{(x^3-1)(x^3+1)}{x-1}$$

$$= \frac{\cancel{(x-1)}(x^2+x+1)(x+1)(x^2-x+1)}{\cancel{x-1}}$$

$$\begin{array}{c} x^6 - 1 \\ \| \\ (x-1)\,p(x) \end{array} = (x^2+x+1)(x+1)(x^2-x+1)(x-1)$$

$$\Rightarrow \quad (x-1)\left[p(x) - (x+1)(x^2+x+1)(x^2-x+1) \right] = 0$$

$\mathbb{C}[x]$ e' integro

$$\Longrightarrow \qquad p(x) = \underbrace{(x+1)}_{\text{irrid.}}(x^2+x+1)(x^2-x+1)$$

$$x^2+x+1 \qquad\qquad x_{1,2} = \frac{-1 \pm \sqrt{-3}}{2}$$

$$\| $$

$$\left(x - \frac{-1+\sqrt{-3}}{2}\right)\left(x - \frac{-1-\sqrt{-3}}{2}\right)$$

$$p(x) = (x+1)\left(x-\frac{-1+\sqrt{-3}}{2}\right)\left(x-\frac{-1-\sqrt{-3}}{2}\right)\left(x-\frac{1+\sqrt{-3}}{2}\right)\left(x-\frac{1-\sqrt{-3}}{2}\right)$$

$\boxed{\text{OSS}}$ La fattorizzazione e' unica A MENO DI INVERTIBILI

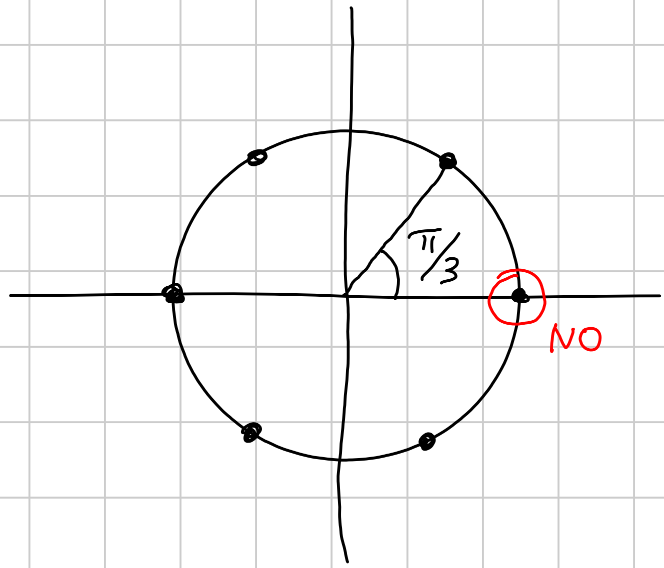
$$15 = 3 \cdot 5 = (-3)(-5)$$

INVERTIBILE: un elemento $x \in A$ per cui esiste $y \in A$ t.c. $xy = 1$

In $\mathbb{C}[x]$ tutti i numeri complessi sono invertibili!

$$(2x-1)(x-3) = \left(x-\frac{1}{2}\right)(2x-6)$$

Radici nel piano complesso: di $p(x)$



Un esempio di quoziente $A = \mathbb{Z}[x] / (x^2+6, 2x^2+17)$

In A vale $2x^3+17x = 0$

$$2x^3+17x = x\underbrace{(2x^2+17)}_{0} + x^4+6x^2$$

$p(x) \in A$ può essere rappresentato da un polinomio di 1° grado

$$x^3+7 = x^3+7 - x(x^2+6)$$

$$= -6x+7 = -x+2$$

Sia $q(x) \in \mathbb{Z}[x]$. Posso scrivere

$$q(x) = (x^2+6)\,r(x) + s(x)$$

in modo unico con $\deg(s(x)) < 2$

$$[q(x)] = [(x^2+6)\,r(x) + s(x)]$$

$$= [s(x)]$$

$[5] = 0$ $\qquad$ $[5x] = [0]$

$$5 = (2x^2+17) - 2(x^2+6)$$

Conseguenza: $|A| \leq 25$

I seguenti polinomi rappresentano tutti gli elementi di A: $\left\{ ax+b : \begin{matrix} 0 \leq a \leq 4 \\ 0 \leq b \leq 4 \end{matrix} \right\}$

$$x^3+7 = x(x^2+6) - 6x + 7$$

$$= x\left(\cancelto{0}{x^2+6}\right) + 2 + \left(\left(\cancelto{0}{2x^2+17}\right) - 2\left(\cancelto{0}{x^2+6}\right)\right)$$

$$- x - x \cdot \left[\left(\cancelto{0}{2x^2+17}\right) - 2\left(\cancelto{0}{x^2+6}\right)\right]$$

In A: $[x^3+7] = [2-x]$