ALGEBRA 1 – 19 OTT 2018

Note Title 10/19/2018

G gruppo abeliano finito, $\text{ord}(G) = n$
Operazione $+$

Sia d un divisore di n.

$$G_d = \{x \in G \mid dx = 0\}$$

$$dG = \{dx \in G \mid x \in G\}$$

$$\varphi_d : G \to G \qquad \varphi_d(x) = dx$$

$$\ker \varphi_d = G_d \qquad \operatorname{Im} \varphi_d = dG.$$

Oss. I sottogruppi G_d e dG sono anche sottogruppi CARATTERISTICI di G.
(G_d è car: Se $\varphi : G \to G$ è un automorfismo e $x \in G_d$ $\quad d\varphi(x) = \varphi(dx) = \varphi(0) = 0$.
dG è simile)

Oss. 2 Sia $k > 0$ qualsiasi. Allora

$$G_k = G_{(k,n)} \qquad e \qquad kG = (k,n)G$$

$x \in G_k \Rightarrow kx = 0$ Ma anche $nx = 0$.

$$akx + bnx = (k,n)x = 0.$$

(e similmente per kG)

Abbiamo anche $|G_d| \cdot |dG| = |G| = n$.

Teorema Ogni gruppo abeliano finito è isomorfo a un prodotto diretto di gruppi ciclici.

Dim. 1° passo:

Lemma Se $a \cdot b = n$ e $(a,b) = 1$ allora $G \cong G_a \times G_b$.

Dim. lemma $G_a \cap G_b = \{0\}$

$x \in G_a \cap G_b \Rightarrow ax = bx = 0$.

$\exists\, s,t$ tali che $sa + tb = 1$

$$x = (sa+tb)x = s\underline{ax} + t\underline{bx} = 0 + 0 = 0.$$

$G_a + G_b = G$: $\quad \subseteq$ ovvio

$\supseteq \quad x \in G \qquad x = \underbrace{sax}_{\in G_b} + \underbrace{tbx}_{\in G_a}$

Cor. Se $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, allora

$$G \cong \underbrace{G_{p_1^{a_1}} \times \cdots \times}\, G_{p_k^{a_k}}. \quad (*)$$

Traccia della dim. Induzione su k.

$k=1$ banale $\qquad G = G_{n/p_k^{a_k}} \times G_{p_k^{a_k}}$

Ora basta dimostrare che un p-gruppo finito è isomorfo a un prodotto diretto di gruppi ciclici.

(*) Osserviamo che $|G_{p_i^{a_i}}| = p_i^{a_i}$

(Infatti, la cardinalità è una potenza di p_i per il teorema di Cauchy: $|G_{p_i^{a_i}}| \leq p_i^{a_i}$
(sgr $\Rightarrow$ ordine che divide l'ordine del gruppo)
Ma se fosse $|G_{p_i^{a_i}}| < p_i^{a_i}$ per qualche i, avrei $|G| = \prod |G_{p_i^{a_i}}| < \prod p_i^{a_i} = |G|$, assurdo).

Lemma 2 $|G| = p^a$. Sia $x \in G$ di ordine massimo possibile ($\text{ord}(x) = p^k$).
Sia $H = \langle x \rangle$. e sia $\pi : G \to G/H$ la proiezione canonica.
Allora $\forall z \in G/H$ esiste $y \in G$ tale che $\pi(y) = z$ e $\boxed{\text{ord}(y) = \text{ord}(z)}$.

Dim lemma 2 Innanzitutto scelgo un elemento $y_0 \in G$ tale che $\pi(y_0) = z$.
Gli elementi la cui immagine è z sono tutti e soli della forma $y_0 + sx$
(due el hanno la stessa immagine $\Leftrightarrow$ la differenza $\in$ ker)

Sia $\text{ord}(z) = p^c$. Vorrei trovare s tale che $\text{ord}(y_0 + sx) = p^c$.
Basta trovare s tale che $p^c(y_0 + sx) = 0$.
($\text{ord}(y_0 + sx) \mid p^c$ e $p^c \mid \text{ord}(y_0 + sx)$).
(in un omo. $\text{ord}\, f(a) \mid \text{ord}(a)$)

So che $\pi(p^c y_0) = p^c z = 0$
Quindi $p^c y_0 \in H$ $\boxed{p^c y_0 = tx}$
e anche

$0 = p^k y_0 = p^{k-c} \cdot p^c y_0 = p^{k-c} t x$

(perché tutti gli el. hanno ordine $\leq p^k$).

Questo vuol dire che $p^k \mid p^{k-c} t$

cioè $p^c \mid t$ $\quad t = p^c u$

Sostituisco, e trovo $p^c y_0 = p^c u x$

$p^c (y_0 - ux) = 0$.

$s = -u$ FUNZIONA

Continuiamo la dimostrazione, per induzione sull'ordine di $|G| = p^a$. (caso $a=1$ ovvio)

Nelle notazioni precedenti, ho

$$G/H \cong C_1 \times \dots \times C_m \qquad C_i \text{ ciclici}.$$

$$C_i = \langle y_i \rangle$$

Prendo x_i come nel lemma 2

$\pi(x_i) = y_i \qquad \text{ord}(x_i) = y_i$

e voglio dimostrare che

$$G \cong \underset{H}{\langle x \rangle} \times \langle x_1 \rangle \times \dots \langle x_m \rangle$$

Chiamo $K = \langle x_1, \dots, x_m \rangle$

<u>Lemma 3</u> $G = H + K$;

$H \cap K = \{0\}$: infatti

$g \in H \cap K \qquad g = tx = t_1x_1 + \dots + t_m x_m$

$\downarrow \qquad \qquad \downarrow \pi$

$\pi(g) = 0$

$t_1 y_1 + \dots + t_m y_m = 0$

$\Rightarrow t_i y_i = 0 \ \forall i$ (G/H è prod diretto)

$\Leftarrow$

$t_i x_i = 0 \ \forall i$

$\Downarrow$

$tx = 0$.

$H + K = G \qquad g \in G \qquad \pi(g) = t_1 y_1 + \dots + t_m y_m$

$\pi(g) = \pi(t_1 x_1 + \dots + t_m x_m)$

$g - (t_1 x_1 + \dots + t_m x_m) = tx \in H$.

$g = tx + t_1 x_1 + \dots + t_m x_m$.

<u>Lemma 4</u>. $K \cong \langle x_1 \rangle \times \dots \times \langle x_m \rangle$.

<u>Dim</u> Induzione su m. $m = 1$ banale

Per il passo induttivo basta dimostrare

$K \cong \underset{A}{\langle x_1, \dots, x_{m-1} \rangle} \times \underset{B}{\langle x_m \rangle}$

$A \cap B = \{0\}$

$g \in A \cap B \qquad g = t_1 x_1 + \dots + t_{m-1} x_{m-1} = t_m x_m$

$\pi(g) = t_1 y_1 + \dots + t_{m-1} y_{m-1} = t_m y_m$

$t_1 y_1 + \dots + t_{m-1} y_{m-1} - t_m y_m = 0$.

$\to$ prod diretto $\to t_i y_i = 0 \to t_i x_i = 0$.

$A+B=K$

$g\in K \quad g=(t_1x_1+\dots+t_{m-1}x_{m-1})+t_mx_m$

$\in A+B.$

$\square$.

UNICITÀ? In generale <u>NO</u>

$$\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

$$(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}) \cong$$

$$\mathbb{Z}/36\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}.$$

<u>Prop.</u> Sia G un p-gruppo abeliano finito. Allora la sua decomposizione come prodotto diretto di gruppi ciclici è unica a meno dell'ordine.

<u>Dim.</u> Scrivo G in due modi diversi

$$G\cong\mathbb{Z}/p^{a_1}\mathbb{Z}\times\dots\times\mathbb{Z}/p^{a_r}\mathbb{Z}\cong\mathbb{Z}/p^{b_1}\mathbb{Z}\times\dots\times\mathbb{Z}/p^{b_s}\mathbb{Z}$$

con $a_1\geq a_2\geq\dots\geq a_r>0$, $b_1\geq b_2\geq\dots\geq b_s>0$.

Voglio dimostrare

1. $r=s$
2. $a_i=b_i \quad \forall i$.

Conto gli elementi di ordine divisore di p. G_p

$$p^r=p^s \quad\Rightarrow r=s.$$

② Induzione su ord G. ($|G| = p$ banale).

Se ho un isomorfismo $\varphi : G \to G$
e H è un sottogruppo caratteristico di G,
allora φ induce un isomorfismo

$$\bar{\varphi} : G/H \to G/H$$

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"] \arrow[dr, dashed, "\psi"] & G \arrow[d, "\pi"] \\ G/H \arrow[r, dashed, "\bar{\varphi}"] & G/H \end{tikzcd}$$

($\ker \pi \circ \varphi = H$)

Prendo $H = G_p$

$$G/H \cong \mathbb{Z}/p^{a_1-1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{a_r-1}\mathbb{Z}$$

$$\cong \mathbb{Z}/p^{b_1-1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{b_r-1}\mathbb{Z}$$

$a_k - 1 = 0$ lo stesso numero di volte per cui $b_k - 1 = 0$. $a_k = 1$ tante volte $b_k = 1$

Per gli altri, induzione: $a_i - 1 = b_i - 1 > 0$

$a_i = b_i$.

Se $G = \left(\mathbb{Z}/p^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{a_r}\mathbb{Z}\right) \times \left(\mathbb{Z}/q^{b_1}\mathbb{Z} \times \dots \times \mathbb{Z}/q^{b_s}\mathbb{Z}\right)$

$a_1 \geq a_2 \geq \dots \geq a_r > 0$ $\quad b_1 \geq b_2 \geq \dots \geq b_s > 0$

Con ev. fattori banali

e faccio il prodotto dei $\mathbb{Z}/p^{a_i}\mathbb{Z}$ e $\mathbb{Z}/q^{b_j}\mathbb{Z}$

in ordine, ottengo

$$\mathbb{Z}/_{p^{a_1}q^{b_1}\mathbb{Z}} \times \mathbb{Z}/_{p^{a_2}q^{b_2}\mathbb{Z}} \times \dots \times \mathbb{Z}/_{p^{a_r}q^{b_r}\mathbb{Z}}$$

dove

$$p^{a_r}q^{b_r} \mid p^{a_{r-1}}q^{b_{r-1}} \mid \dots \mid p^{a_2}q^{b_2} \mid p^{a_1}q^{b_1}.$$

e questo è vero $\iff$ li prendo in ordine

Quindi ottengo l'unicità con una fattorizzazione del tipo

$$\mathbb{Z}/_{d_1\mathbb{Z}} \times \mathbb{Z}/_{d_2\mathbb{Z}} \times \dots \times \mathbb{Z}/_{d_r\mathbb{Z}}$$

dove $d_r \mid d_{r-1} \mid \dots \mid d_2 \mid d_1$.

Numero sul numero di generatori.

p-gruppi. $G = \mathbb{Z}/_{p^{a_1}\mathbb{Z}} \times \dots \times \mathbb{Z}/_{p^{a_r}\mathbb{Z}}$

$(1,0,\dots,0), (0,1,\dots,0), \dots, (0,0,\dots,1)$
sono r generatori.

$\pi: G \to G/H$

$G = \langle x_1, \dots, x_k \rangle$
$\pi(G) = \langle \pi(x_1), \dots, \pi(x_k) \rangle$
n° min. di gen di $G/H \leq$ n° min. gen di G

$$H = p\mathbb{Z}/_{p^{a_1}\mathbb{Z}} \times \dots \times p\mathbb{Z}/_{p^{a_r}\mathbb{Z}} = pG$$

$$G/H = \underbrace{\mathbb{Z}/_{p\mathbb{Z}} \times \dots \times \mathbb{Z}/_{p\mathbb{Z}}}_{r \text{ volte}}$$

$\to$ sp. vettoriale ci vogliono r generatori.