ALGEBRA 1 – 23 OTT 2018

Note Title 10/23/2018

Ricordo che se G è un p-gruppo abeliano finito, $G \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_r}\mathbb{Z}$,

allora r è il MIN numero di generatori di G.

Se invece G non è un p-gruppo, facciamo un esempio.

$a_1 \geq a_2$ $\quad$ $b_1 \geq b_2 \geq b_3$

$$G \cong \left(\mathbb{Z}/p^{a_1}\mathbb{Z} \times \mathbb{Z}/p^{a_2}\mathbb{Z}\right) \times \left(\mathbb{Z}/q^{b_1}\mathbb{Z} \times \mathbb{Z}/q^{b_2}\mathbb{Z} \times \mathbb{Z}/q^{b_3}\right) \times \mathbb{Z}/r^{c}\mathbb{Z}$$

La "forma canonica" di G come prodotto diretto di sottogruppi ciclici è:

$$\mathbb{Z}/p^{a_1}q^{b_1}r^{c}\mathbb{Z} \times \mathbb{Z}/p^{a_2}q^{b_2}\mathbb{Z} \times \mathbb{Z}/q^{b_3}\mathbb{Z}$$

$$\cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \mathbb{Z}/d_3\mathbb{Z} \quad \text{dove}$$

$$d_3 \mid d_2 \mid d_1.$$

Il n° minimo di generatori in questo caso è 3.

- 3 bastano: $(\bar{1},\bar{0},\bar{0})$, $(\bar{0},\bar{1},\bar{0})$, $(\bar{0},\bar{0},\bar{1})$
- 3 sono necessari:

$$G/pG \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

che è uno s.v. su $\mathbb{F}_q$ di dimensione 3

Oss. In un gruppo abeliano finito di ordine n esistono sottogruppi di ordine d per ogni $d \mid n$.

Esempio: $\mathbb{Z}/p^6\mathbb{Z} \times \mathbb{Z}/q^4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$

un sottogruppo di ordine p^{11} è, per esempio,

$$\mathbb{Z}/p^6\mathbb{Z} \times \mathbb{Z}/p^4\mathbb{Z} \times p^2\mathbb{Z}/p^3\mathbb{Z}$$

In generale, se $G \cong G_{p_1^{a_1}} \times \dots \times G_{p_r^{a_r}}$

e cerco un sottogruppo di ordine $p_1^{b_1} \cdots p_r^{b_r}$ (con $b_i \le a_i$) basta fare il prodotto diretto dei sottogruppi di ordine $p_i^{b_i}$ dentro $G_{p_i^{a_i}}$.

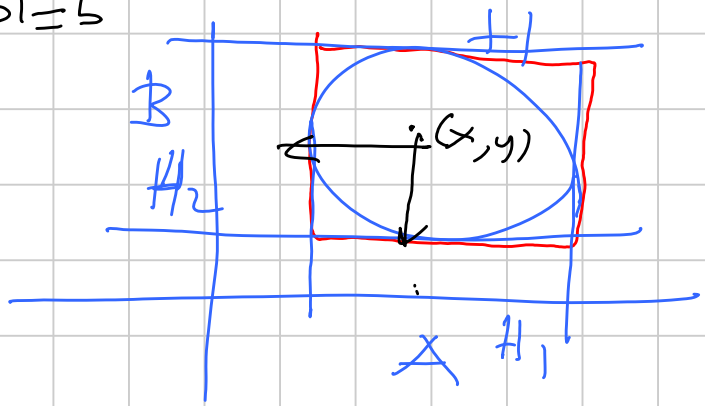
Problema Se $G = A \times B$ è vero che ogni sottogruppo H di G si scrive nella forma $H = H_1 \times H_2$ dove $H_1 < A$ e $H_2 < B$?

No: $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ $\quad H = \{(x,x) \mid x \in \mathbb{Z}/p\mathbb{Z}\}$

Invece è vero se A, B hanno ordini primi fra loro, $|A| = a$, $|B| = b$

Infatti: $H < A \times B$

Considero le due proiezioni di H su A e su B.



$\pi_1 : H \to A \qquad \pi_1(H) = H_1$

$\pi_2 : H \to B \qquad \pi_2(H) = H_2$

Abbiamo che $H \subseteq H_1 \times H_2$

Vediamo che in realtà $H = H_1 \times H_2$.

Prendo $(x,y) \in H$

Quindi $x \in H_1$, $y \in H_2$.

Considero le potenze di (x,y) . $(x,y)^k = (x^k, y^k)$

Se $k \equiv 1 \pmod a$ allora $x^k = x$

Se $k \equiv 0 \pmod b$ allora $y^k = e$

$\rightarrow$ in H c'è (x,e)

Similmente c'è (e,y)

e quindi ci sono tutti i prodotti

$(x,e)(e,y) = (x,y) \qquad \forall x \in H_1, \forall y \in H_2$

<u>Conseguenza:</u> $G \cong G_{p_1}^{a_1} \times G_{p_2}^{a_2} \times \dots \times G_{p_r}^{a_r}$

$H < G \Rightarrow H \cong H_1 \times H_2 \times \dots \times H_r$.

Però gli H_i NON SONO NECESSARIAMENTE prodotti diretti dei sottogruppi che compaiono nella decomposizione

$G_{p_i}^{a_i} = \prod \mathbb{Z}/p_i^{c_i}\mathbb{Z}$.

Esercizio G gruppo abeliano finito di ordine n

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

Allora d divide l'ordine di G_d.

Sol. In G esiste un sottogruppo H di ordine d.

$$H < G_d$$

$$d = \mathrm{ord}(H) \mid \mathrm{ord}(G_d).$$

(Esercizi: contare gli elementi di ordine d e i sottogruppi di ordine d in un gruppo abeliano finito. Il caso importante è $d = p^\alpha$.)

TEOREMI DI SYLOW

Primo teorema di Sylow: Sia G un gruppo (non necessariamente abeliano) di ordine $n = p^a m$ con $(m, p) = 1$.
Allora G ha un sottogruppo di ordine p^a (detto sottogruppo di Sylow).

Dim. Consideriamo l'insieme X dei sottoinsiemi di G di cardinalità p^a.

$$|X| = \binom{n}{p^a} = \binom{p^a m}{p^a}$$

$$\binom{p^a m}{p^a} = \frac{p^a m \,(p^a m - 1) \cdots (p^a m - (p^a - 1))}{p^a \cdot 1 \cdot 2 \cdot \cdots \cdot (p^a - 1)}$$

$p^{am} - p^b$ → non divisibile per p.

11

m non divisibili per p.

In totale, $\binom{p^a m}{p^a}$ NON È DIVISIBILE per p.

Alternativamente, $\binom{p^a m}{p^a}$ è un coefficiente del binomio $(x+y)^{p^a m}$

Congruenza modulo p:

$$(x+y)^{p^a m} \equiv \left[(x+y)^{p^a}\right]^m \equiv (x^{p^a}+y^{p^a})^m$$

$$\equiv x^{p^a m} + \binom{p^a m}{p^a} x^{(p^a)(m-1)} y^{p^a} + \dots$$

$$= x^{p^a m} + m\, x^{p^a(m-1)} y^{p^a}$$

$$\Rightarrow \binom{p^a m}{p^a} \equiv m \pmod p \qquad (\not\equiv 0 \pmod p)$$

Considero l'azione del gruppo G sull'insieme X data da

$$G \xrightarrow{\varphi} S(X) \qquad A \in X$$

$$g \longmapsto \varphi_g \qquad \varphi_g(A) = gA.$$

Siccome X ha una cardinalità NON MULTIPLA DI p, allora esiste un'orbita di questa azione che ha una cardinalità non multipla di p.

Sia A un insieme con tale orbita. Allora

$|\mathrm{Orb}(A)|$ divide m.

$$|\mathrm{Stab}(A)| \cdot |\mathrm{Orb}(A)| = p^a m$$

$$\Rightarrow \boxed{p^a \mid \mathrm{ord}(\mathrm{Stab}(A))}.$$

$$\mathrm{Stab}(A) = \{g \in G \mid gA = A\}$$

$$A = \{x_1, x_2, \dots, x_{p^a}\}$$

Se $g \in \mathrm{Stab}(A)$ allora $gx_1 = x_i$ per qualche i.

$g = x_i' x_1$

Quando $\boxed{|\mathrm{Stab}(A)| \leq p^a}$

$\Rightarrow |\mathrm{Stab}(A)| = p^a$.

QUESTO È IL GRUPPO CERCATO.

Secondo teorema di Sylow

Teo Sia H un p-gruppo contenuto in G. Allora H è contenuto in un sottogruppo P di Sylow di G (relativo a p; cioè $|P| = p^a$). Inoltre, due sottogruppi di Sylow di G (relativi allo stesso primo p) sono coniugati.

Dim Consideriamo P un p-Sylow di G.

1° caso: $H \subseteq N(P)$ (normalizzatore di P).

Allora $HP < G$ $\quad (hp \cdot h'p' = hh'p''p' \in HP)$

$\uparrow$ $ph' = h'p$

Vale la formula:

$$|HP| \cdot |H \cap P| = |H| \cdot |P|$$

potenza di p ← potenza di p

$\Rightarrow HP = P$ e $H \subseteq P$.

2° caso Considero l'insieme X dei sottogruppi coniugati a P.

G agisce su X per coniugio. (una sola orbita)

$$Stab(P) = \{g \in G \mid gPg^{-1} = P\} = N(P)$$

$N(P) \geq P$. Quindi

$X = Orb(P) = [G : Stab(P)] = [G : N(P)]$
ha cardinalità non divisibile per p.

Sia H un p-gruppo contenuto in G.
Anche H agisce su X per coniugio.
→ Le orbite dell'azione di H hanno per cardinalità una potenza di p.

$p \nmid |X| \Rightarrow$ esiste un'orbita con 1 elemento.

Chiamiamo quest'orbita $\mathrm{Orb}(Q) = \{Q\}$.

Abbiamo che, se $h \in H$,

$$hQh^{-1} = Q \quad \forall h \in H$$

$$H \subseteq N(Q)$$

1° caso : $H \subseteq Q$.

In particolare, se H è un p-Sylow
H è contenuto in un coniugato di P,
e per cardinalità sono uguali.
(quando tutti i p-Sylow sono coniugati)

3° teorema di Sylow Il numero dei coniugati di P è congruo a 1 modulo p.

Dim Se H è un p-Sylow, allora
$\exists Q$ tale che $H \subseteq Q \Rightarrow H = Q$.
Questo dice che nell'azione di H su X
c'è una sola orbita con 1 elemento
(orbita di Q).
(Il ragionamento del teo. 2 dice che
orbita di un elemento $\Rightarrow H \subseteq Q$, $H = Q$
1 possibilità)
Quindi 1 orbita con 1 elemento e tutte le
altre orbite di ordine potenza di p.
Sommando, si ottiene un numero
congruo a 1 mod p.