ARITMETICA 8 NOV 2017

Note Title 11/8/2017

Sottogruppi generati da un insieme

$S \subseteq G$ gruppo.

Cerco il più piccolo sottogrupp. di G che contiene S.

Esiste: si può prendere

$$K = \bigcap_{\substack{H < G \\ H \supseteq S}} H$$

(intersezione non vuota c'è $H = G$)

- K è un sottogruppo perché è l'intersezione di sottogruppi
- K è il più piccolo perché $K \subseteq H \ \forall H$.

Come si costruisce?

1° caso: $S = \{x\}$.

Proposizione. Il sottogruppo generato da x è $\langle x \rangle = \{ x^m \mid m \in \mathbb{Z} \}$.

Dim. Chiamiamo $H = \{ x^m \mid m \in \mathbb{Z} \}$ e dimostriamo che $\langle x \rangle = H$

- $H \subseteq \langle x \rangle$.

Se un sottogruppo contiene x, allora contiene anche $x \cdot x = x^2$ ... $\underbrace{x \cdot x \cdot x \cdots x}_{n \text{ volte}} = x^n$ con n positivo.

e anche $x^{-n} = \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{n \text{ volte}}$

$\rightarrow H \ni x^n \quad \forall n \in \mathbb{Z}$.

- $H \supseteq \langle x \rangle$ Basta vedere che $H < G$.

- $e \in H \qquad e = x^0$

① $a, b \in H \Rightarrow ab \in H$

$a = x^n, \quad b = x^m \qquad ab = x^{n+m}$

(se $n, m > 0$ $\quad x^n = \underbrace{x \cdot x \cdots x}_{n \text{ volte}}$, $\quad x^m = \underbrace{x \cdot x \cdots x}_{m \text{ volte}}$)

$x^n \cdot x^m = \underbrace{x \cdots x}_{n \text{ volte}} \cdot \underbrace{x \cdots x}_{m \text{ volte}} = \underbrace{x \cdots x}_{n+m \text{ volte}}$

Se $n > 0 \quad m < 0$

$\underbrace{x \cdots x}_{n \text{ volte}} \quad \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1}}_{m \text{ volte}} = \underbrace{x \cdots x}_{n-m \text{ volte}}$ $\quad (n \geq m)$

$a \in H \quad a^{-1} \in H$

$x^n \in H \Rightarrow x^{-n} \in H$

Concludendo: $\langle x \rangle = \{ x^n \mid n \in \mathbb{Z} \}$

con l'operazione $+$

$\langle x \rangle = \{ nx \mid n \in \mathbb{Z} \}$

Più in generale, se $S = \{x_1, \dots, x_n\}$ è un insieme finito, consideriamo

$$T = S \cup S^{-1} = \{x_1, \dots, x_n, x_1^{-1}, x_2^{-1}, \dots, x_n^{-1}\}.$$

Allora il sottogruppo generato da S è l'insieme

$$H = \{ t_1 \dots t_k \mid k \in \mathbb{N}, t_i \in T \}$$

- Certamente $\forall k \ \forall t_i$ $t_1 \dots t_k$ deve appartenere al sottogruppo generato da S.

- D'altra parte H è un sottogruppo.

  - $e \in H$ (prodotto vuoto)
  - $x, y \in H \Rightarrow xy \in H$
    $x = t_1 \dots t_k \quad y = t'_1 \dots t'_h$
    $xy = t_1 \dots t_k t'_1 \dots t'_h$
  - $x \in H \Rightarrow x^{-1} \in H$
    $x = t_1 \dots t_k \quad x^{-1} = t_k^{-1} t_{k-1}^{-1} \dots t_2^{-1} t_1^{-1}$

    Se $t_i = x_i \quad t_i^{-1} = x_i^{-1} \in T$
    Se $t_i = x_i^{-1} \quad t_i^{-1} = x_i \in T$.

Caso particolare: G commutativo.

I prodotti $t_1 t_2 \dots t_k$ si possono riordinare ottenendo $x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$ $\quad a_i \in \mathbb{Z}$

Se l'operazione è l'addizione
si ottiene $a_1x_1 + a_2x_2 + \dots + a_nx_n$.

Classi laterali di un sottogruppo

$H < G$

Relazioni di equivalenza in G

$a \sim b \iff a^{-1}b \in H$ | $a \sim b \iff ba^{-1} \in H$

Controlliamo che siano relazioni di equivalenza (per la prima relazione).

- riflessiva: $a \sim a$ cioè $a^{-1}a \in H$. $e \in H$ OK.
- transitiva: $a \sim b, b \sim c \Rightarrow a \sim c$
  $a^{-1}b \in H, b^{-1}c \in H \Rightarrow a^{-1}c \in H$
  $a^{-1}c = a^{-1}b \cdot b^{-1}c$
- simmetrica: $a \sim b \Rightarrow b \sim a$
  $a^{-1}b \in H \Rightarrow b^{-1}a \in H$
  $b^{-1}a = (a^{-1}b)^{-1}$ OK.

(Lo stesso ragionamento porta a verificare che anche la seconda relazione è una rel. di equivalenza)

CLASSI DI EQUIVALENZA

Prima relazione $a \sim b \iff a^{-1}b \in H$

$Cl(a) = \{b \in G \mid b \sim a\}$

$b \sim a \Rightarrow a^{-1}b = h \in H$

moltiplicando a sinistra per a,

$b = ah$

$b \in aH = \{ah \mid h \in H\}$.

Viceversa, supponiamo che $b \in aH$, cioè $b = ah$ per qualche $h \in H$.

Allora

$a^{-1}b = a^{-1}ah = h \in H$ cioè $\boxed{a \sim b}$.

$Cl_1(a) = aH \rightarrow$ classe laterale sinistra di a

Si può vedere, in modo totalmente analogo, che se si usa la seconda relazione di equivalenza, si ottiene

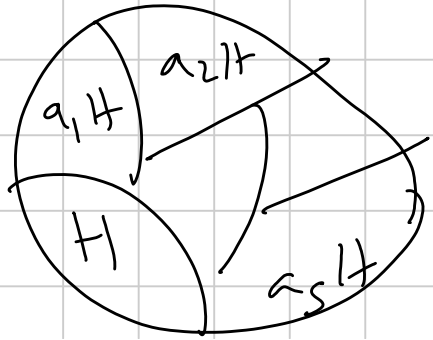
$$Cl_2(a) = Ha = \{ha \mid h \in H\}$$

In particolare, la classe di equivalenza di a è in corrispondenza biunivoca con gli elementi di H

$h \leftrightarrow ah$

$H \leftrightarrow aH$

Se G è un gruppo finito (e quindi H è finito) tutte le classi laterali hanno LO STESSO NUMERO DI ELEMENTI (= n° di elementi di H).



Supponiamo che ci siano s classi di equivalenza (classi laterali sinistre)

$$|G| = |H| \cdot s$$

Teorema (Lagrange) Se G è un gruppo finito e H è un sottogruppo di G, allora $|H|$ è un DIVISORE di $|G|$ (l'ordine di H è un divisore dell'ordine di G)

CASI PARTICOLARI

$$H = \langle x \rangle = \{ x^m \mid m \in \mathbb{Z} \}$$

$$e, x, x^2, \dots, x^d = e \qquad |H| = d$$

$$|G| = n \Rightarrow d \mid n.$$

$\mathbb{Z}/m\mathbb{Z}$

$a \in \mathbb{Z}/m\mathbb{Z}$

$d = \text{ord}(a) \quad d \mid m$

$$ax \equiv b \pmod m$$

si risolve sempre se $(a, m) \mid b$

$(a,m) = d$

Divido per d

$$\frac{a}{d} x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

$(\mathbb{Z}/m\mathbb{Z})^*$

$a \in (\mathbb{Z}/m\mathbb{Z})^*$

$d = \text{ord}(a)$

$d \mid \phi(m)$

e ottengo una soluzione

$$x \equiv x_0 \pmod{\frac{m}{d}}$$

$\frac{m}{d}$ è l'ordine dell'elemento a

(cioè il più piccolo multiplo di a $\equiv 0$ in $\mathbb{Z}/m\mathbb{Z}$)

Infatti:

(1) $\frac{m}{d} a \equiv 0 \pmod{m}$

Questo è chiaro, perché

$d = (a, m) \Rightarrow d \mid a$

$a = a_1 d$

$\frac{m}{d} a = \frac{m}{d} a_1 d = m a_1 \equiv 0 \pmod{m}$

(2) $\frac{m}{d}$ è il minimo

Supponiamo che $ka \equiv 0 \pmod{m}$

Quindi $m \mid ka$

Dividendo per d, ottengo

$$\frac{m}{d} \mid k \frac{a}{d}$$

Siccome $(a, m) = d$

abbiamo $\left(\frac{m}{d}, \frac{a}{d}\right) = 1$

$\Rightarrow \frac{m}{d} \mid k$

Osservazione finale

G gruppo finito di ordine n.
$H = \langle x \rangle = \{e, x, x^2, \dots, x^{d-1}\} < G$
(d è il minimo esponente positivo per cui $x^d = e$ e quindi le potenze di x si ripetono con periodo d ossia $x^i = x^j \iff i \equiv j \pmod d$)

So che $d \mid n$. $\quad n \equiv 0 \pmod d$

$\Rightarrow x^n = e$

Corollario Se $|G| = n$ e $x \in G$, allora $x^n = e$

$G = \left(\mathbb{Z}/p\mathbb{Z}\right)^* \quad |G| = p-1 \quad x^{p-1} = 1 \quad$ (p.t.F.)

$G = \left(\mathbb{Z}/n\mathbb{Z}\right)^* \quad x \in G \quad x^{\phi(n)} = 1 \quad$ (Eulero)
$(x, n) = 1$

Esercizi proposti vecchi

Carte (26+26)

- Il rimescolamento corrisponde alla moltiplicazione della posizione della carta per 2 mod 53.

- Periodo di $1/p$. $\quad (2n) \quad$ ↗ $p-1$

$10^{2n} \equiv 1 \pmod p \Rightarrow 10^n \equiv -1 \pmod p$

$\frac{1}{p} = \overline{a_1 \dots a_n b_1 \dots b_n} \qquad A = \overline{a_1 \dots a_n} \quad B = \overline{5, \dots 5}$

$$\frac{10^n}{p} = A + \frac{p-1}{p}$$

$$p-1 \quad \frac{10^n}{p} = B + \frac{1}{p}$$

SOMMARE →