ARITMETICA 13 NOV 2017

Note Title 11/13/2017

G gruppo finito. $H < G$, $x \in G$

$\text{ord}(H) \mid \text{ord}\, G$

$\text{ord}(x) \mid \text{ord}\, G$ e, se $|G| = n$. $x^n = e$

$\text{ord}(H)$ = n° di elementi di H

$\text{ord}(x)$ = n° di elementi del sottogruppo generato da x $\{e, x, \dots, x^{d-1}\}$ dove d è il più piccolo esponente positivo per cui $x^d = e$.

$G = \mathbb{Z}/m\mathbb{Z}$ + $\forall x \in G$ $\text{ord}(x) = d$, $d \mid m$, $mx = \bar{0}$

$G = (\mathbb{Z}/m\mathbb{Z})^*$. $\forall x \in G$ $\text{ord}(x) \mid \phi(m)$, $x^{\phi(m)} = \bar{1}$.

Gruppi ciclici.

Def. Un gruppo G si dice ciclico se esiste un elemento $x \in G$ tale che $G = \langle x \rangle$ (sottogruppo generato da x)

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

Esempi $G = \mathbb{Z}/m\mathbb{Z}$ +

$\mathbb{Z}/m\mathbb{Z} = \langle \bar{1} \rangle$.

Oss. Se p è un numero primo e G

è un gruppo con p elementi, allora G è un gruppo ciclico.
Infatti, se $x \in G$, $x \neq e$

$$\text{ord}(x) \mid p \qquad \text{ord}(x) = \begin{cases} 1 \\ p \end{cases}$$ NO perché $x \neq e$

Quindi $\langle x \rangle$ ha p elementi $\Rightarrow = G$.

Oss. 2 Un gruppo G di ordine n è ciclico se e solo se esiste $x \in G$ tale che $\text{ord}(x) = n$.

Prodotto diretto di gruppi.

Siano G_1, G_2 due gruppi.
Il prodotto diretto di G_1 per G_2, $G = G_1 \times G_2$ è il prodotto cartesiano di G_1 per G_2 con l'operazione

$$(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2)$$
(in G_1, in G_2)

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} \qquad (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

Caso particolare: G_1, G_2 gruppi finiti
$|G_1| = m \qquad |G_2| = n$
$|G| = |G_1 \times G_2| = mn$

$\text{ord}(x_1, x_2)$: come dipende da $\text{ord}(x_1)$ e $\text{ord}(x_2)$?

$= \text{mcm}\{\text{ord}(x_1), \text{ord}(x_2)\}$

Se $\text{ord}(x_1) = d_1$, $\text{ord}(x_2) = d_2$

abbiamo che $x_1^k = e_1 \iff d_1 | k$.
$x_2^k = e_2 \iff d_2 | k$

e quindi $(x_1, x_2)^k = (x_1^k, x_2^k) = (e_1, e_2)$
$\iff d_1 | k$ e $d_2 | k$ cioè $[d_1, d_2] | k$.

Proposizione $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ è un gruppo ciclico $\iff (m,n) = 1$.

Dim. Supponiamo $(m,n) = 1$. Allora la coppia $(\bar{1}_m, \bar{1}_n)$ ha ordine mcm fra m ed n $= mn$.
Se invece $(m,n) = d > 1$, allora, preso $(x,y) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$\text{ord}(x) | m$ $\quad \text{ord}(y) | n$
$\text{ord}(x,y) = [\text{ord}(x), \text{ord}(y)] \mid [m,n) < mn$.
e quindi non c'è una coppia (x,y) tale che
$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} = \langle (x,y) \rangle$

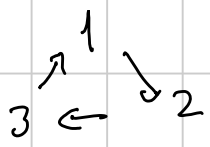
Oss. (da dimostrare in seguito)
p primo $\Rightarrow (\mathbb{Z}/p\mathbb{Z})^*$ è ciclico.

Sottogruppi normali

Def. Un sottogruppo H di un gruppo G si dice

un sottogruppo NORMALE di G se $xH = Hx$ $\forall x \in G$. (Notazione: $H \triangleleft G$)

Esempio $G = S_3$ $\quad H = \langle (123) \rangle$



$H = \{ e, (123), (123)^2 = (132) \}$

$x = (12)$ $\quad (1 \mapsto 2)$, $3 \mapsto 3$

xH $\qquad\qquad$ Hx

$x e = (12)$ $\qquad$ $e (12) = (12)$

$(12)(123) = (23)$ $\qquad$ $(123)(12) = (13)$

$(12)(132) = (13)$ $\qquad$ $(132)(12) = (23)$

$xH = Hx$

GLI INSIEMI SONO UGUALI, MA NON ELEMENTO PER ELEMENTO

$H \triangleleft G$ NOTAZIONE

Oss. Se G è un gruppo commutativo (= abeliano) allora tutti i sottogruppi di G sono automaticamente normali.

Come verificare che un certo sottogruppo H di un gruppo G è un sottogruppo normale.

È sufficiente vedere che $xH \subseteq Hx$ $\forall x \in G$

Infatti, se $xH \subseteq Hx$ $\forall x \in G$, allora

$xHx^{-1} \subseteq Hxx^{-1} = He = H \quad \forall x \in G$

e anche

$Hx^{-1} = x^{-1}xHx^{-1} \subseteq x^{-1}H$

Poiché x è qualsiasi, x^{-1} è qualsiasi, e quindi varia fra tutti gli elementi di G.

Alternativamente, si può dimostrare che

$xHx^{-1} = H \quad \forall x \in G$

o anche $xHx^{-1} \subseteq H \quad \forall x \in G$

Gruppo quoziente

G gruppo, $H \lhd G$

Insieme quoziente: G/H $\left(\mathbb{Z}/m\mathbb{Z}\right)$

Definiamo un'operazione in G/H come segue

$xH \cdot yH \overset{\text{def}}{=} xyH$

Buona definizione $\quad x \sim x' \iff x^{-1}x' \in H$

$\iff x' \in xH$

Supponiamo $x \sim x'$, $y \sim y'$

$x' \in xH \qquad y' \in yH$

$x' = xh_1 \qquad y' = yh_2$

$h_1 \in H \qquad h_2 \in H$

$x'y' = xh_1yh_2 = xyh_3h_2 \in xyH$

$h_1y \in Hy = yH$; $h_3 \in H$

$\Rightarrow x'y' \sim xy$.

Oss. Se G è un gruppo finito e $H \trianglelefteq G$, allora

$$|G| = |H| \cdot |G/H|.$$

$$|G/H| = |G|/|H|.$$

OMOMORFISMI

Def. Siano G e G' due gruppi.
Un omomorfismo da G in G' è una funzione

$f : G \to G'$

tale che $f(xy) = f(x) \cdot f(y) \quad \forall x, y \in G$

NOTA xy è un'operazione in G
$f(x)f(y)$ è un'operazione in G'.

$$f : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$$

$$f(x) = e^x$$

$$f(x+y) = f(x)f(y)$$
$$e^{x+y} = e^x \cdot e^y$$

Altro esempio G gruppo, $H \trianglelefteq G$

Allora $\pi : G \to G/H$ (proiezione canonica)

definita da $\pi(x) = xH$
è un omomorfismo.
($\pi(xy) = xyH = xH \cdot yH = \pi(x) \cdot \pi(y)$)

Def. Se $f: G \to G'$ è un omomorfismo, si dice NUCLEO di f ($\ker f$)
$\{x \in G \mid f(x) = e'\}$

Proprietà degli omomorfismi.

① $f(e) = e'$
Infatti $e' \cdot f(e) = f(e \cdot e) = f(e) \cdot f(e)$
CANCELLAZIONE $\Rightarrow e' f(e)$

② $f(x^{-1}) = [f(x)]^{-1} \quad \forall x \in G$

Infatti $f(x) f(x^{-1}) = f(x x^{-1}) = f(e) = e'$
e lo stesso succede anche se scambio l'ordine

PROPOSIZIONE Il nucleo di un omomorfismo $f: G \to G'$ è un sottogruppo normale di G.

DIM. Sia $K = \ker f$.

(sgr)
$e \in K$ $\quad f(e) = e'$ (v. sopra)
$x, y \in K \Rightarrow xy \in K \quad f(x) = e' \; f(y) = e' \; f(xy) = f(x) f(y) = e' e' = e'$
$x \in K \Rightarrow x^{-1} \in K$
$\downarrow$
$f(x) = e \quad f(x^{-1}) = (e')^{-1} = e'$.

normale Dimostro che $xkx^{-1} \subseteq K \quad \forall x \in G$.

Sia $k \in K \qquad xkx^{-1} \in xKx^{-1}$

$$f(xkx^{-1}) = f(x)\underbrace{f(k)}_{e'}f(x^{-1}) = f(x)f(x^{-1})$$
$$= f(x)[f(x)]^{-1} = e'.$$

PROP. 2 I nuclei degli omomorfismi $f: G \to G'$, dove G' è un qualsiasi gruppo, sono TUTTI E SOLI i sottogruppi normali di G.

DIM. Visto la prop. precedente dato un sottogruppo normale H di G', basta trovare un omomorfismo che abbia nucleo H.

$$\pi : G \to G/H$$

$$\ker \pi = \{x \in G \mid xH = eH = H\}$$
$$= H$$

OSS Allora $f: G \to G'$ omomorfismo.
$f(x) = f(y) \iff xK = yK$
(dove $K = \ker f$)

Dim Se $xK = yK$ allora $x \in yK$
$x = yk \quad (k \in K)$

e quindi

$$f(x) = f(yk) = f(y)\cdot\underbrace{f(k)}_{e'} = f(y)$$

Se $f(x) = f(y)$
allora $f(x)f(y)^{-1} = e'$

$$f(xy^{-1}) = e'$$
$$xy^{-1} \in K$$
$$x \in Ky$$