19/06/19

1) a) • $m \in M$ t.c. $\exists\, m_1, m_2 \in M$ t.c. $m m_1 = m_1 \cdot m = e$
$m m_2 = m_2 m = e$

$e = m m_1$, moltiplico a sinistra per m_2

$m_2 = m_2 m m_1 = (m_2 m) m_1 = e m_1 = m_1$

b) • u_1, u_2 invertibili $\Rightarrow \exists\, u_1^{-1}, u_2^{-1} \in M$

$u_1 u_2 (\overbrace{u_2^{-1} u_1^{-1}}^{\in M}) = u_1 e u_1^{-1} = e$
$(u_2^{-1} u_1^{-1}) u_1 u_2 = e$
$\Big\} \Rightarrow u_1 u_2$ è invertibile

• e è invertibile

• u invertibile $\Rightarrow \exists\, u^{-1}$ t.c. $u u^{-1} = u^{-1} u = e \Rightarrow u^{-1}$ invertibile

c) $\mathbb{Z}_7$ è un campo $\Rightarrow$ ogni suo el. è invertibile

$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\bar{1}$? $\exists\, \bar{x} \in \mathbb{Z}_6$ t.c. $\bar{1} \cdot \bar{x} = \bar{x} \cdot \bar{1} = \bar{1}$? Sì, $\bar{1}$
$\bar{2}$? ∄ inverso (provarli tutti! $\bar{2} \cdot \bar{1} \neq \bar{1}$ $\bar{2} \cdot \bar{2} \neq \bar{1}$, $\bar{2} \cdot \bar{3} \neq \bar{1}$, ...)
$\bar{3}$? ∄ inverso
$\bar{4}$? ∄ inverso
$\bar{5}$? il suo inverso è $\bar{5}$ ($\bar{5} \cdot \bar{5} = \overline{25} = \overline{6 \cdot 4 + 1} = \bar{1}$)

TIP: $\bar{m}$ invertibile in $\mathbb{Z}_m \iff \exists\, \bar{a} \in \mathbb{Z}_m$ t.c. $am = 1 + mk$
$\iff MCD(m, m) = 1$

2) b) $H \leq G$ sottogr. unico nel suo ordine $\Rightarrow$ normale.

Sol. $\forall g \in G$ considero gHg^{-1}. É un sottogruppo di G, infatti

- $e \in gHg^{-1}$ perché $e = geg^{-1}$ $(e \in H)$
- $\forall x, y \in gHg^{-1} \Rightarrow xy \in gHg^{-1}$

$$x = ghg^{-1}, h \in H \quad y = gkg^{-1}, k \in H \Rightarrow xy = gh\overbrace{g^{-1}g}^{e}kg^{-1} = g\underbrace{(hk)}_{\in H}g^{-1} \in gHg^{-1}$$

Vediamo che ~~[illegible]~~ gHg^{-1} ha lo stesso ordine di H:

costruisco $f: H \to gHg^{-1}$
$h \mapsto ghg^{-1}$

è iniettiva:

$f(h_1) = f(h_2) \Rightarrow gh_1g^{-1} = gh_2g^{-1}$
$gh_1 = gh_2$
$h_1 = h_2$ ✓

è suriettiva (ovvio)

$\Rightarrow gHg^{-1}$ e H, essendo finiti e in biiezione, hanno lo stesso ordine $\Rightarrow gHg^{-1} = H$ cioè H è normale.

3), e 4) : già visto (credo!)

26/02/'18

1) $f: G \to H$ omom. G, H finiti

a) $o(f(g))$ divide $o(g)$:

$$g^{o(g)} = e \qquad f(g^{o(g)}) = f(e) = e = (f(g))^{o(g)}$$

$o(g)$ è un "candidato" ordine di $f(g)$. In generale, dato che il minimo n t.c. $(f(g))^n = e$ è $o(f(g))$, si ha che $o(g) = o(f(g)) \cdot k$.

b) $o(f(g)) = o(g)$ $\forall g \in G \Rightarrow f$ iniettivo:

Basta dim. che $\ker f = \{e\}$ (banale)

$\ker f = \{g \in G \text{ t.c. } f(g) = e\}$

cioè $g \in G$ t.c. $o(f(g)) = 1$
$\qquad\qquad\qquad\qquad \| $
$\qquad\qquad\qquad\quad o(g)$

L'unico el. di G che ha ordine 1 è $g = e$.

Scansionato con CamScanner

26/02/18 Esercizio 1 c) (e anche d)...)

1) Lagrange: $S \leq T$ sottogr., T finito
$\Rightarrow |T| = |S| \cdot n$ dove n = numero di classi laterali sinistre $x S$ (o destre)

2) 1° teor. di omomorfismo:
$f: G \to H$ omom. di gruppi $\Rightarrow f(G) \simeq G/\ker f$

Esercizio

$f: G \to H$ omom. suriettivo di gruppi finiti $\Rightarrow |H|$ divide $|G|$

Soluzione

Ricordare che $|T/S|$ (cioè l'ordine del gruppo quoziente) è il numero di classi laterali (sinistre o destre) per definizione di T/S.
In simboli: $|T/S| = \frac{|T|}{|S|}$ ←

So che $f(G) \simeq G/\ker f$ quindi hanno lo stesso ordine:

$$|f(G)| = |G/\ker f| = \frac{|G|}{|\ker f|}$$

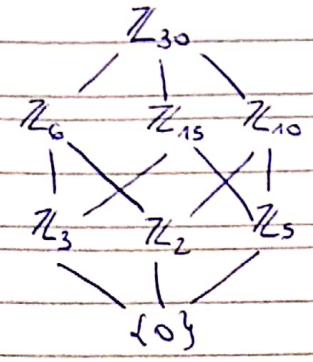
Ora, poiché f è suriettiva si ha $f(G) = H$, quindi

$$|H| \cdot |\ker f| = |G|$$

ovvero l'ordine di H divide l'ordine di G.

(ho usato che $|\ker f| \neq 0$. ~~Per esercizio test~~ Infatti $\ker f$ contiene sempre almeno un elemento, il neutro)

4) Sottogruppi di $(\mathbb{Z}_{30}, +)$: $\{0\}, \mathbb{Z}_{30}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_6, \mathbb{Z}_{10}, \mathbb{Z}_{15}$



Complementi:

$\mathbb{Z}_6$	$\mathbb{Z}_5$
$\mathbb{Z}_{15}$	$\mathbb{Z}_2$
$\mathbb{Z}_{10}$	$\mathbb{Z}_3$
$\{0\}$	$\mathbb{Z}_{30}$

È distributivo perché non contiene i sottoreticoli "problematici"
$\Rightarrow$ è di Boole (notando che ha "0" e "1")

Esercizio d'esame / teorema

Gli ideali di un anello formano un reticolo modulare

Dim. Definiamo, per ogni I, J ideali di A

$\inf(I,J) := I \cap J$

$\sup(I,J) := I + J$ (N.B.: sono ancora ideali di A)

$\Rightarrow L = \{ I \text{ ideale di } A \}$ è un reticolo $\vee$

Modulare:

$\forall\ I \subseteq J$, K tutti ideali di A, si ha $(I+K) \cap J \subseteq I + (K \cap J)$?

Sia $x \in (I+K) \cap J \Rightarrow x \in I+K$ e $x \in J$

$\Downarrow$

$x = \underset{\uparrow I}{i} + \underset{\uparrow K}{k}$

Vediamo che $k \in J$: $k = x - i$, $x \in J$, $i \in I \subseteq J \Rightarrow k \in J$

$\Rightarrow x \in I + (K \cap J)$