Esercizio 1.
Sia $(S(X), \circ)$ il gruppo delle permutazioni di un insieme X e sia A un sottoinsieme di X. Poniamo

$$J(A) = \{\sigma \in S(X) \mid \sigma(A) = A\}$$

e

$$F(A) = \{\sigma \in S(X) \mid \sigma(a) = a \ \forall a \in A\}.$$

a) Mostrare che $J(A)$ è un sottogruppo di $S(X)$.
b) Mostrare che $F(A)$ è un sottogruppo normale di $J(A)$.
c) Calcolare $[J(A) : F(A)]$ nel caso $X = \{1, 2, \ldots, 10\}$ e $A = \{1, \ldots, 4\}$.

---

a) $J(A) < S(X)$

$Id \in J(A) \Rightarrow J(A) \neq \emptyset$

$\sigma, \tau \in J(A) \Rightarrow \sigma \circ \tau \in S(X)$ e $\sigma\circ\tau(A) = \sigma(A) = A$

$\Rightarrow \sigma\circ\tau \in J(A)$

$\sigma \in J(A) \Rightarrow \sigma^{-1} \in J(A) \Rightarrow J(A) < S(X)$

b) $F(A) \lhd J(A)$ Chiaramente $F(A) \subset J(A)$.

$Id \in F(A) \Rightarrow F(A) \neq \emptyset$

$\alpha, \beta \in F(A) \Rightarrow \alpha\circ\beta(a) = \alpha(\beta(a)) = \alpha(a) = a \quad \forall a \in A$

$\alpha \in F(A) \Rightarrow \alpha^{-1}$ è una permutazione di X e

$\alpha^{-1}a = a \quad \forall a \in A$

Ne segue che $F(A) < J(A)$

Vediamo che è normale.

Sia $\sigma \in J(A)$ e sia $\alpha \in F(A) \Rightarrow \sigma\alpha\sigma^{-1}(a)$

Sia $\sigma^{-1}(a) = a' \quad a' \in A \Rightarrow \sigma\alpha\sigma^{-1}(a) = \sigma\alpha(a') =$

$= \sigma(a') = a$

quindi $\forall \sigma \in J(A), \forall \alpha \in F(A)$ si ha

$\sigma \alpha \sigma^{-1} \in F(A)$ cioè $F(A) \lhd J(A)$.

c) $[J(A) : F(A)] = \dfrac{|J(A)|}{|F(A)|}$

$\# X = 10$
$\# A = 4$

$\Rightarrow \# J(A) = 6!\,4!$

$\# F(A) = 6!$

$\Rightarrow [J(A) : F(A)] = 4!$

Esercizio 2

Esercizio 2.
Sia $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.
a) Determinare il numero do sottogruppi di G di ordine 4.
b) Contare gli omomorfismi da $\mathbb{Z}/4\mathbb{Z}$ in G.
c) Contare gli omomorfismi da $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in G.

Svolgimento:

a) Un gruppo di ordine 4 è isomorfo a $\mathbb{Z}/4\mathbb{Z}$ oppure a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$\#$ sgr ciclici di ordine $4 = \dfrac{\#\text{ el di ordine } 4}{\phi(4)}$ *

Conto $\#$ el di ordine 4 : questi sono ~~quelli~~ gli $(a,b) \in G$ tali che

$4(a,b) = (0,0)$

ma $2(a,b) \neq (0,0)$

$(4a, 4b) = (0,0) \iff 4a \equiv 0 \ (6) \quad a \equiv 0 \ (3)$
$4b \equiv 0 \ (12) \quad b \equiv 0 \ (3)$

quindi ci sono 2 possibili valori di a e
4 possibili valori di b $\rightarrow$ 8 coppie
$(\#G_4 = 8)$

Di queste vanno tolte le coppie
(a,b) tali che $2(a,b) = 0$

$2a \equiv 0 \ (6) \quad a \equiv 0 (3) \rightarrow$ 2 soluzioni
$2b \equiv 0 \ (12) \quad b \equiv 0 (6) \rightarrow$ 2 soluzioni

$\Rightarrow$ In tutto 4 coppie $(\#G_2 = 4)$

$\Rightarrow$ # el di ordine $4 = 8 - 4 = 4$

sgr ciclici di ordine $4 = \frac{4}{\varphi(4)} = 2$

(Si possono determinare esplicitamente e sono i gruppi $H_1 = \langle (\bar{0}, \bar{3}) \rangle$, $H_2 = \langle (\bar{3}, \bar{3}) \rangle$

~~Abbiamo visto che~~
I sgr isomorfi a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sono tutti
contenuti in $G_2 = \{(a,b) \mid 2(a,b) = 0\}$
Abbiamo appena visto che $|G_2| = 4$
quindi # $G_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (è chiaro che
G_2 non è ciclico) $\Rightarrow$ c'è un unico sgr
che è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

b) $\#\,\mathrm{Hom}(\mathbb{Z}/4\mathbb{Z}, G)$

Un omomorfismo $\varphi: \mathbb{Z}/4\mathbb{Z} \to G$ è sempre univocamente determinato dal valore di $\varphi(\bar{1})$ con la condizione che

$\mathrm{ord}\,\varphi(\bar{1}) \mid \mathrm{ord}(\bar{1}) = 4$ (questo è vero perché il dominio è ciclico)

Ne segue che $\#\mathrm{Hom}(\mathbb{Z}/4\mathbb{Z}, G) = \#\, G_4 = 8$.

c) $\#\,\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, G)$

In questo caso il dominio non è ciclico, ma è generato da $(\bar{1}, \bar{0})$ e da $(\bar{0}, \bar{1})$

~~Assegnamo i valori~~

Per definire $\varphi: \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to G$

assegnamo i valori di $\varphi(\bar{1}, \bar{0}) = x$ (*)

$\varphi(\bar{0}, \bar{1}) = y$

Sappiamo che necessariamente deve essere

$\mathrm{ord}\, x \mid \mathrm{ord}(\bar{1}, \bar{0}) = 2$

$\mathrm{ord}\, y \mid \mathrm{ord}(\bar{0}, \bar{1}) = 2$ $\Rightarrow x, y \in G_2$

D'altra parte ogni assegnamento delle immagini di $(\bar{1}, \bar{0})$ e di $(\bar{0}, \bar{1})$ che rispetti la condizione data si estende in modo unico ad un omo di tutto $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Infatti $\forall (\bar{a}, \bar{b}) \in \mathbb{Z}/2 \times \mathbb{Z}/2$ si ~~dispone~~ se φ è un omomorfismo che estende (*) necessariamente $\varphi(\bar{a}, \bar{b}) = a\varphi(\bar{0}, \bar{1}) + b\varphi(\bar{1}, \bar{0}) = ax + by$ $\quad a \in \bar{a}$, $b \in \bar{b}$

Poniamo quindi $\varphi(\bar{a}, \bar{b}) = ax + by$

~~φ cosi definita~~

φ è ben definita: infatti $a \equiv a' \quad b \equiv b' \quad (2)$

$\Rightarrow a'x = (a+2k)x = ax$ perché $2x = 0$

$b'y = (b+2h)y = by$ perché $2y = 0$

φ è omo $\Rightarrow \quad \varphi((\bar{a},\bar{b}) + (\bar{c},\bar{d})) =$

$= \varphi((\bar{a}+\bar{c}, \bar{b}+\bar{d})) = (a+c)x + (b+d)y =$

$= ax + by + cx + dy = \varphi(\bar{a},\bar{b}) + \varphi(\bar{c},\bar{d})$

$\Rightarrow \#\,\mathrm{Hom}(\mathbb{Z}_{2\mathbb{Z}} \times \mathbb{Z}_{2\mathbb{Z}}, G) = 4 \cdot 4 = 16$

2° metodo: Ognuno degli omomorfismi cercati corrisponde ad un unico omomorfismo

$$f : \mathbb{Z} \times \mathbb{Z} \longrightarrow G$$

t.c. $\ker f \supset 2\mathbb{Z} \times 2\mathbb{Z}$

Posto $f(1,0) = x$ e $f(0,1) = y$

sappiamo che $\exists$ un unico omo compatibile con questo assegnando, ed è quello definito da $f(a,b) = ax + by$

(quello dato è l'unica estensione possibile e si verifica che è un omo)

Si ha $2\mathbb{Z} \times \bar{2}\mathbb{Z} \subset \ker f \iff$

$f(2,0) = 2x = 0, \; f(0,2) = 2y = 0 \iff$ ord $x \mid 2$, ord $y \mid 2$

$\Rightarrow \#\,\mathrm{Hom}(\mathbb{Z}_{2\mathbb{Z}} \times \mathbb{Z}_{2\mathbb{Z}}, G) = 4 \cdot 4 = 16$

Esercizio 3.
Sia $f(x) = x^4 - 4$.
a) Determinare la fattorizzazione e il grado del campo di spezzamento del polinomio $f(x)$ su K per $K = \mathbb{Q}, \mathbb{F}_7, \mathbb{F}_{13}$.
b) Determinare il tipo di fattorizzazione e il campo di spezzamento di $f(x)$ su $\mathbb{F}_{503^k}$ per $k \geq 1$.

---

a)
$f(x) = x^4 - 4 = (x^2 - 2)(x^2 + 2)$

fatt in $\mathbb{Q}[x]$ in quanto x^2-2 e x^2+2 sono irrid in $\mathbb{Z}[x]$ per il criterio di Eisenstein e quindi anche in $\mathbb{Q}[x]$ per il lemma di Gauss.

Le radici in $\mathbb{C}$ di $f(x)$ sono $\pm\sqrt{2}, \pm i\sqrt{2}$, quindi il c. di sp di f su $\mathbb{Q}$ è $F = \mathbb{Q}(\pm\sqrt{2}, \pm i\sqrt{2}) = \mathbb{Q}(\sqrt{2}, i)$

Infatti $\pm\sqrt{2}, \pm i\sqrt{2} \in \mathbb{Q}(\sqrt{2}, i)$ e $i = \frac{\sqrt{2}\, i}{\sqrt{2}} \in F$.

$\Rightarrow [F : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$

$[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] = 2$ perché il polinomio di i su $\mathbb{Q}(\sqrt{2})$ è un divisore di $x^2+1 \Rightarrow$ il grado è 1 o 2, ma $i \notin \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ $\Rightarrow$ il grado è 2.

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ perché 2 non è $\square$ in $\mathbb{Q}$ (x^2-2 è il pol min)

$\mathbb{F}_7$ $\quad f(x) = (x^2-2)(x^2+2) = (x^2-9)(x^2+2) = (x-3)(x+3)(x^2+2)$

Il pol x^2+2 è irriducibile: si può vedere per verifica diretta (ha grado 2 e non ha radici in $\mathbb{F}_7$)

C. di sp è $\mathbb{F}_{7^2}$

$\mathbb{F}_{13}$ $\quad f(x) = (x^2-2)(x^2+2)$

Poiché $13 \equiv 1 \ (4)$ $\quad$ 2 è un $\square \iff -2$ è un $\square$

$\Downarrow$

$2^{\frac{p-1}{2}} = 1 \ (13)$

$2^6 \equiv 64 \equiv -1 \ (13) \Rightarrow$ 2 non è $\square$, -2 non è $\square$

quindi quella scritta è una fattorizzazione di $f(x)$

- Il c. di sp di $f(x)$ su $\mathbb{F}_{13}$ è $\mathbb{F}_{13^2}$.

b) $503 \equiv 3 \ (4)$ ed è primo. Ne segue che

in $\mathbb{F}_{503}$ -1 non è $\square$.

$\Rightarrow$ Esattamente uno tra 2 e -2 non è un $\square$. $\Rightarrow$ Esatt 1 tra i pol (x^2-2) e (x^2+2) si spezza

$f(x) = l_1(x)\, l_2(x)\, q(x)$

con $\deg l_i = 1$ e $\deg q = 2$

Il c. di sp di $f(x)$ su $\mathbb{F}_{503}$ è $\mathbb{F}_{503^2}$

Il c di sp di $f(x)$ su $\mathbb{F}_{503^k}$ è la più piccola ext di $\mathbb{F}_{503^k}$ che contiene tutte le radici di $f(x)$. Poiché queste radici generano su $\mathbb{F}_{503}$ il campo $\mathbb{F}_{503^2}$ si ha che il c. di sp è $\mathbb{F}_{503^d}$ con d minimo tale che $\mathbb{F}_{503^d} \supset \mathbb{F}_{503^k}$ e $\mathbb{F}_{503^d} \supset \mathbb{F}_{503^2}$ cioè d minimo tale che $k \mid d$ e $2 \mid d$

$\Rightarrow d = [k, 2]$. Quindi se k pari il c di sp è $\mathbb{F}_{503^k}$ se k è dispari è $\mathbb{F}_{503^{2k}}$.