Esercizio 1. Consideriamo $\mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$ ed il sottogruppo $n\mathbb{Z}$. Spiegare perché il gruppo quoziente $\mathbb{Z}/n\mathbb{Z}$ è ben definito ed isomorfo (di fatto, uguale) a $\mathbb{Z}_n$.

Si ricordi che $n\mathbb{Z} = \{n \cdot a \mid a \in \mathbb{Z}\}$, definiamo $\mathbb{Z}/n\mathbb{Z}$ come il gruppo quoziente per un sottogruppo normale, formato dalle classi laterali $= \{0\mathbb{Z}, 1\mathbb{Z}, 2\mathbb{Z} \dots, (n-1)\mathbb{Z}\}$. La relazione che definisce ciò è $a \rho b \Leftrightarrow b - a \in n\mathbb{Z}$. definisco un applicazione $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ tale che $f(a\mathbb{Z}) = [a]$, tale applicazione è ben definita

$$f(a\mathbb{Z} + b\mathbb{Z}) = f((a+b)\mathbb{Z}) = [a+b] = [a] + [b] = f(a\mathbb{Z}) + f(b\mathbb{Z})$$

è quindi f un omomorfismo. Inoltre, f è suriettiva, perché $\forall [a] \in \mathbb{Z}_n, \exists\, a\mathbb{Z} \mid f(a\mathbb{Z}) = [a]$, so poi che la cardinalità di $\mathbb{Z}_n$ è n, e noto che $\mathbb{Z}/n\mathbb{Z} = \{0\mathbb{Z}, 1\mathbb{Z}, 2\mathbb{Z} \dots, (n-1)\mathbb{Z}\}$ ha precisamente n elementi, essendo l'applicazione suriettiva su due gruppi della stessa cardinalità, è anche biettiva, quindi f è un isomorfismo. NON SONO SICURO DELLA CORRETTEZZA

Esercizio 2. Sia G il gruppo affine della retta affine numerica $\mathbb{R}$: **per definizione** $G = \{f_{a,c}, a \in \mathbb{R} \setminus \{0\}, c \in \mathbb{R}\}$ con $f_{a,c}(x) = ax + c$ e prodotto in G uguale alla composizione di applicazioni. Dopo aver verificato che G è effettivamente un sottogruppo del gruppo di tutte le bigezioni di $\mathbb{R}$ e che non è commutativo, dimostrare che il sottoinsieme delle traslazioni $T = \{f_{1,c}, c \in \mathbb{R}\}$ è un sottogruppo normale e che G/T è isomorfo al gruppo $(\mathbb{R} \setminus \{0\}, \cdot)$.
Suggerimento: definire un opportuno omomorfismo surgettivo $G \to \mathbb{R} \setminus \{0\}$ ed applicare il teorema fondamentale di omomorfismo fra gruppi.....

$ax+c$

Chiamiamo B il gruppo di tutte le bigezioni su $\mathbb{R}$

$B = \{f,\ f \text{ biettiva}\}$, e dimostro che $G \leq B$:

$\forall f'_{a,c}, f''_{a,c} \in G$ ho che $f'_{a,c} \circ \left(f''_{a,c}\right)^{-1} = f'_{a,c} \circ f''^{-1}_{a,c} = {}^{*}$ (la funzione inversa di $ax+c$ e' $\frac{x-c}{a}$)

$= (a'x+c') \circ \left(\frac{x-c''}{a''}\right) = a'\left(\frac{x-c''}{a''}\right) + c' = \frac{a'x - c''a'}{a''} + c'$

$= \left(\frac{a'x}{a''} - \frac{c''a'}{a''}\right) + c' = \left(x\frac{a'}{a''} - \frac{c''a'}{a''}\right) + c' = x\left(\frac{a'}{a''} - \frac{c''a'}{a''}\right) + c' \in G$ ✓

quindi G e' un sottogruppo, ma non e' commutativo:

$(a'x+c') \circ (a''x+c'') = a'(a''x+c'') + c' \neq a''(a'x+c') + c'' = (a''x+c'') \circ (a'x+c')$.

Considero il sottogruppo $T = \{f_{1,c}, c \in \mathbb{R}\} = \{x+c,\ c \in \mathbb{R}\}$, dimostro che e' un sottogruppo: $(x+c') \circ (x+c'')^{-1} = (x+c') \circ (x-c'') = (x-c'') + c' = x + (c'-c'') \in T$,

inoltre noto che T e' commutativo:

$(x+c') \circ (x+c'') = (x+c'') + c' = x + (c'+c'') = x + (c''+c') = (x+c') + c'' = (x+c'') \circ (x+c')$

Le classi laterali sinistre $gT = \{g \circ t,\ g \in G,\ t \in T\}$ che sono tutte le funzioni del tipo:

$g = ax+c \Rightarrow \{(ax+c) \circ (x+c'), (ax+c) \circ (x+c''), (ax+c) \circ (x+c''') \ldots\}$

le classi laterali destre sono:

$g = ax+c \Rightarrow \{(x+c')\circ(ax+c), (x+c'')\circ(ax+c)\dots\}$ noto che, $\forall ax+c \in G$ e $\forall x+c' \in T \Rightarrow (x+c')\circ(ax+c) = (ax+c)+c' = ax+c+c'$ e che $(ax+c)\circ(x+c') - a(x+c')+c = x+c'+\frac{c}{a} \Rightarrow$ le classi laterali sono uguali, T è normale! Definisco adesso il gruppo di tutte le classi laterali $G/T = \{gT\ , c\in\mathbb{R}, g\in G\}$ con l'operazione $gT\cdot hT = (g\circ h)T = \begin{cases} g = ax+c \\ h = a'x+c' \end{cases} = ((ax+c)\circ(ax+c'))T$.

Definisco adesso un applicazione $f: G \to \mathbb{R}\setminus\{0\}$ tale che $f(ax+c) = a$. $\quad G \xrightarrow{f} \mathbb{R}\setminus\{0\}$

Noto che, $\ker f = \{ax+c \mid f(ax+c) = 1\} = \{x+c\} = T$

Il gruppo T definito prima è il nucleo di f!

definisco la proiezione canonica $\pi: G \to G/T$ tale che $\pi(ax+c) = (ax+c)T$. per il teorema fondamentale di omomorfismo di gruppi, esiste un ISOMORFISMO $F: G/T \to \mathbb{R}\setminus\{0\}$

quindi G/T è isomorfo ad $\mathbb{R}\setminus\{0\}$.

Esercizio 3. Determinare il gruppo degli automorfismi del gruppo ciclico $(\mathbb{Z}_n,+)$. (Suggerimento: basta determinare gli omomorfismi di $\mathbb{Z}_n$ in sé stesso che sono suriettivi; osserviamo anche che un omomorfismo di $\mathbb{Z}_n$ is sé stesso è determinato dall'immagine di [1]....).

Esercizio svolto in classe

prendo un qualsiasi automorfismo f, e so che $f([1])=[1]$, quindi un automorfismo $f(n)=n\cdot h$ dove h deve essere un unita', ossia deve generare $\mathbb{Z}_n$, quindi gli automorfismi sono del tipo $f(n)=n\cdot a$, $a\in M(\mathbb{Z}_n)$, considero l'applicazione $\Psi: Aut(\mathbb{Z}_n)\to M(\mathbb{Z}_n)$ tale che $\Psi(n\cdot a)=[a]$. noto che preserva l'op. $\Psi(na+nb)=[a]+[b]=\Psi(na)+\Psi(nb)$, e' un omomorfismo, inoltre, e' suriettivo, $\forall [a]\in\mathbb{Z}_n$, $\exists na \mid f(na)=[a]$, inoltre $|M(\mathbb{Z}_n)|=\varphi(n)$, dove φ e' la funzione di eulero, e $Aut(\mathbb{Z}_n)$ ha la stessa cardinalita' di $M(\mathbb{Z}_n)$, i gruppi sono isomorfi. NON SONO SICURO DELLA CORRETTEZZA

Esercizio 4. Sia $(G,\cdot)$ un gruppo. Il Centro di G è l'insieme

$$Z(G) := \{z \in G \mid z \cdot g = g \cdot z \ \forall g \in G\}$$

Consideriamo l'applicazione $\Phi : G \to \mathrm{Aut}(G)$ che associa a $x \in G$ l'automorfismo γ_x. Abbiamo incontrato questa applicazione nell'Esercizio 8 del compito dell'8/11/23.

- Verificare che $Z(G) = \mathrm{Ker}\Phi$
- cosa deduciamo da questa informazione ?
- Cosa ci dice questo risultato sul sottogruppo $\mathrm{Im}\Phi$ degli automorfismi interni ?

$Z(G)$ e' il gruppo di tutti gli elementi di G che commutano.
L'automorfismo γ_x e' definito nel seguente modo: $\gamma_x(a)=x\cdot a\cdot x^{-1}$.
Considero $\Phi: G\to Aut(G)$ tale che $\Phi(x)=\gamma_x$, adesso, definisco il nucleo: $Ker\Phi=\{a\in G \mid \gamma_x(a)=$ Identita$\}$

↳ elemento neutro di $Aut(G)$

Oss. $\gamma_x(a)=$ Identita' $\iff \gamma_x(a)=a \iff xax^{-1}=axx^{-1} \iff ax=xa \iff a\in Z(G)$
ne concludiamo che, $a\in Ker\Phi \iff a$ commuta $\iff a\in Z(G) \Rightarrow Ker\Phi=Z(G)$.
ne deduco che, se G e' commutativo, $Z(G)=G$, quindi, se G e' commutativo, $G=Ker\Phi$, inoltre, $\forall x\in G$, $\Phi(x)=\gamma_x=$ funzione identita' $\Rightarrow \forall x,y\in G$, $\Phi(x)=\Phi(y)\Rightarrow \Phi$ mappa tutti gli elementi di G nella funzione identita'. $Im(\Phi)=\{$FUNZIONE IDENTITA'$\}$, $|Im(\Phi)|=1$, tale funzione inoltre e' l'elemento neutro di $Aut(G)$.

Esercizi di ripasso.

1. Svolgere l' esercizio 2.12 alla fine del Capitolo 2 in Campanella.
2. Svolgere l'esercizio 3 p. 83 in Piacentini-Cattaneo.
3. Risolvere, se possibile, il sistema

$$\begin{cases} 3x \equiv 9 \bmod 21 \\ 2x \equiv 3 \bmod 5 \end{cases}$$

4. Calcolare le ultime due cifre di 81^{82}.

2 $\begin{cases} X \equiv 7 \pmod 9 \\ X \equiv 3 \pmod 5 \end{cases}$

è un sistema di tipo cinese, essendo $MCD(9,5)=1$, ammette un unica soluzione (mod $9 \cdot 5$).

$R = 45, \quad R_1 = 5, \quad R_2 = 9,$

(i) $5 \cdot t_1 + 9 \cdot 9_1 = 1 \Rightarrow 5(-7) + 9(4) = 1 \Rightarrow t_1 = -7 \Rightarrow \tilde{x}_1 = -7 \cdot 7 = -49$

(ii) $9 \cdot t_2 + 5 \cdot 9_2 = 1 \Rightarrow 9 \cdot (4) + 5(-7) = 1 \Rightarrow t_2 = 4 \Rightarrow \tilde{x}_2 = 4 \cdot 3 = 12$

$SOL = -49 \cdot 5 + 12 \cdot 9 = -137 \pmod{45} = 43 \pmod{45}$