

ESERCIZI TUTORATO ALGEBRA 2
22 NOVEMBRE 2019 - LEZIONE 5
SOLUZIONI

MARCO ABBADINI

Di seguito si trovano le soluzioni degli esercizi svolti in classe. Non sono soluzioni complete, ma solo dei veloci riassunti.

Data una permutazione $\sigma \in S_n$, definiamo

$$\text{supp } \sigma := \{i \in \{1, \dots, n\} \mid \sigma(i) \neq i\},$$

ovvero gli elementi di $\{1, \dots, n\}$ che sono “mossi” da σ .

Inoltre ricordiamo che, dati due elementi g ed h in un gruppo, si definisce il commutatore $[g, h] := g^{-1}h^{-1}gh$.

Esercizio 1. Sia n un intero nonnegativo. Provare le seguenti affermazioni.

- (a) Per ogni coppia di elementi $\sigma, \tau \in S_n$ tali che $\text{supp } \sigma \cap \text{supp } \tau = \emptyset$, si ha che $[\sigma, \tau]$ è l'identità.
- (b) Non esistono $\sigma, \tau \in S_n$ tali che $[\sigma, \tau]$ è uno scambio.
- (c) Per ogni coppia di elementi $\sigma, \tau \in S_n$ tali che $|\text{supp } \sigma \cap \text{supp } \tau| = 1$, si ha che $[\sigma, \tau]$ è un tre-ciclo.

Soluzione. Per mostrare i passaggi mancanti qui di seguito, i seguenti fatti possono tornare utili: se $\rho \in S_n$, allora $\text{supp } (\rho^{-1}) = \text{supp } \rho$, ed inoltre $i \in \text{supp } \rho \Rightarrow \rho(i) \in \text{supp } \rho$.

- (a) ...
- (b) Ogni commutatore è pari, ma uno scambio non lo è.
- (c) Denotando con k l'unico elemento di $\text{supp } \sigma \cap \text{supp } \tau$, si ha $[\sigma, \tau] = (k, \tau(k), \sigma(k))$.

Esercizio 2. Siano G ed H due gruppi. Sia g un elemento di G di periodo finito n e sia h un elemento di H di periodo finito m . Provare che il periodo dell'elemento (g, h) nel prodotto diretto esterno $G \times H$ è $\text{mcm}(n, m)$.

Soluzione. Si usa il fatto che $(g, h)^n = (g^n, h^n)$.

Esercizio 3. $\mathbb{Z}_2 \times \mathbb{Z}_3$ è ciclico¹? Se sì, trovare tutti i generatori, altrimenti stabilire se è isomorfo a S_3 .

Soluzione. È ciclico, come si deduce dal fatto che $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm} \iff \text{MCD}(n, m) = 1$. I generatori sono $([1]_2, [1]_3)$ e $([1]_2, [2]_3)$.

Esercizio 4. (a) Stabilire quali tra i seguenti gruppi sono tra loro isomorfi.

- (a) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.
- (b) $\mathbb{Z}_2 \times \mathbb{Z}_6$.
- (c) $\mathbb{Z}_4 \times \mathbb{Z}_3$.
- (d) \mathbb{Z}_{12} .

Ultimo aggiornamento: 23 novembre 2019. Non esitate a segnalare eventuali errori a marco.abbadini@unimi.it.

¹Quando consideriamo \mathbb{Z}_n come gruppo, diamo sempre per sottinteso che l'operazione in questione è la somma. Si noti che, per ogni $n > 1$, il prodotto non costituisce un'operazione di gruppo su \mathbb{Z}_n , in quanto 0 non è invertibile.

(b) Quanti sono, a meno di isomorfismo, i gruppi di ordine 12 che si ottengono come prodotto diretto di un numero finito di gruppi ciclici²?

Soluzione. (a) Si ha che (a) e (b) sono isomorfi, e (c) e (d) sono isomorfi. Non ci sono altre coppie di gruppi isomorfi. Queste affermazioni si deducono dal fatto che $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm} \iff \text{MCD}(n, m) = 1$. Una soluzione alternativa potrebbe usare l'esercizio 8.

(b) Sono 2: $\mathbb{Z}_2 \times \mathbb{Z}_6$ e \mathbb{Z}_{12} .

Esercizio 5. Sia G un gruppo finito di ordine 15, e supponiamo che G abbia un sottogruppo normale H di ordine 3 e un sottogruppo normale K di ordine 5.³

(a) Provare che G è prodotto diretto interno di H e K .

(b) Provare che G è isomorfo a \mathbb{Z}_{15} .

Soluzione. (a) $H \cap K = \{1\}$ per coprimalità di 3 e 5. $|HK| = \frac{|H||K|}{|H \cap K|} = 15$. Perciò $HK = G$. Segue che G è prodotto diretto interno di H e K .

(b) Per (a), G è isomorfo al prodotto diretto esterno di H e K . H e K sono ciclici di ordine coprimo. Quindi $H \times K$ è ciclico, e perciò anche G .

Esercizio 6. Per ciascuno dei seguenti gruppi si trovi un gruppo “famoso” a lui isomorfo⁴:

$$\text{Aut}(\{1\}), \text{Aut}(\mathbb{Z}_2), \text{Aut}(\mathbb{Z}_3), \text{Aut}(\mathbb{Z}_4), \text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2), \text{Aut}(\mathbb{Z}_5), \text{Aut}(\mathbb{Z}_6), \text{Aut}(S_3), \text{Aut}(\mathbb{Z}_7), \text{Aut}(\mathbb{Z}_8).$$

Soluzione. $\text{Aut}(\{1\}) \simeq \{1\}$,

$$\text{Aut}(\mathbb{Z}_2) \simeq \{1\},$$

$$\text{Aut}(\mathbb{Z}_3) \simeq \mathbb{Z}_2,$$

$$\text{Aut}(\mathbb{Z}_4) \simeq \mathbb{Z}_2,$$

$$\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq S_3,$$

$$\text{Aut}(\mathbb{Z}_5) \simeq \mathbb{Z}_4,$$

$$\text{Aut}(\mathbb{Z}_6) \simeq \mathbb{Z}_2,$$

$$\text{Aut}(S_3) \simeq S_3,$$

$$\text{Aut}(\mathbb{Z}_7) \simeq \mathbb{Z}_6,$$

$$\text{Aut}(\mathbb{Z}_8) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Per ottenerle, ecco qualche risultato.

Per ogni intero positivo n , $\text{Aut}(\mathbb{Z}_n)$ è isomorfo a $U(\mathbb{Z}_n)$, cioè il gruppo moltiplicativo degli elementi invertibili (=coprimi con n) di \mathbb{Z}_n . Inoltre, per i *primi* p , si ha un risultato non banale: $\text{Aut}(\mathbb{Z}_p)$ è ciclico; in particolare, $\text{Aut}(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$. Questo segue dal fatto che, per p primo, $(\mathbb{Z}_p, +, \cdot)$ è un campo, e, per ogni campo finito K , il gruppo moltiplicativo $K \setminus \{0\}$ è ciclico; perciò $U(\mathbb{Z}_p)$ è ciclico e perciò anche $\text{Aut}(\mathbb{Z}_p) \simeq U(\mathbb{Z}_p)$ lo è.

Per quanto riguarda $\mathbb{Z}_2 \times \mathbb{Z}_2$, si osservi che ogni permutazione dei 3 elementi di periodo 2 induce un automorfismo.

Per quanto riguarda S_3 , si noti che S_3 è isomorfo a $\text{Inn}(S_3)$, per il teorema $G/\mathbf{Z}(G) \simeq \text{Inn}(G)$. Ma $\text{Aut}(G) = \text{Inn}(G)$ per questione di cardinalità. Infatti, considerato che un automorfismo mappa il trecciclo $(1, 2, 3)$ in un elemento di periodo 3, e mappa $(1, 2)$ in un elemento di periodo 2, e che $(1, 2, 3)$ e $(1, 2)$ generano

²Vedremo che questi sono precisamente i gruppi abeliani di ordine 12; infatti ogni prodotto di un numero finito di gruppi ciclici finiti è un gruppo abeliano finito e, viceversa, ogni gruppo abeliano finito è isomorfo a un prodotto di un numero finito di gruppi ciclici finiti.

³Vedremo che le ipotesi di esistenza di H e K normali di ordine 3 e 5 in realtà non sono necessarie, in quanto garantite dai teoremi di Sylow. Questo vuol dire che \mathbb{Z}_{15} è, a meno di isomorfismo, l'unico gruppo di ordine 15 (vedi il punto (b)).

⁴Per gruppi famosi si intendono ad esempio gli \mathbb{Z}_n , gli S_n , gli A_n , i D_{2n} , prodotti diretti di questi...

S_3 , allora il numero di automorfismi non può superare $6 = 2 \cdot 3 = (\text{numero di elementi di periodo } 3) \cdot (\text{numero di elementi di periodo } 2)$.

- Esercizio 7.** (1) Trovare due sottogruppi non banali A e B di S_3 tali che $S_3 = A \rtimes B$ (prodotto semidiretto interno)⁵. Descrivere il corrispondente omomorfismo $\varphi: B \rightarrow \text{Aut}(A)$.
- (2) Trovare due sottogruppi A e B di \mathbb{Z}_6 di cardinalità rispettivamente 3 e 2 tale che $\mathbb{Z}_6 = A \rtimes B$ (prodotto semidiretto interno). Descrivere il corrispondente omomorfismo $\varphi: B \rightarrow \text{Aut}(A)$.
- (3) Descrivere tutti gli omomorfismi $\varphi: \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}_3)$ e, per ciascuno di questi, trovare un gruppo “famoso” isomorfo al corrispondente prodotto semidiretto $\mathbb{Z}_3 \rtimes_{\varphi} \mathbb{Z}_2$.

Soluzione. (a) Come A bisogna prendere obbligatoriamente A_3 (unico sottogruppo normale di S_3 diverso da S_3 e $\{\text{Id}\}$). Come B bisogna prendere un sottogruppo di ordine 2, ad esempio $B = \{\text{Id}, (1, 2)\}$. φ è l'unico omomorfismo non banale.

- (b) Bisogna prendere necessariamente $A = \{0, 2, 4\}$ e $B = \{0, 3\}$. φ è l'omomorfismo banale.
- (c) $\text{Aut}(\mathbb{Z}_3) \simeq \mathbb{Z}_2$ (l'elemento neutro di $\text{Aut}(\mathbb{Z}_3)$ è l'identità, mentre l'altro elemento è l'automorfismo che scambia i due elementi di periodo 3). Perciò ci sono 2 automorfismi da \mathbb{Z}_2 a $\text{Aut}(\mathbb{Z}_3)$. Quello banale e l'altro. Quello banale corrisponde a \mathbb{Z}_6 , mentre l'altro corrisponde a S_3 . Per verificare questa affermazione, possono essere utili i seguenti fatti.

Fatto. Siano H, K, H', K' gruppi, siano $\varphi: H \rightarrow \text{Aut}(K)$ e $\varphi': H' \rightarrow \text{Aut}(K')$ omomorfismi. Supponiamo che esistano $\beta: H \rightarrow H'$ e $\alpha: K \rightarrow K'$ isomorfismi tali che il seguente diagramma commuti,

$$\begin{array}{ccc} H & \xrightarrow{\varphi} & \text{Aut}(K) \\ \downarrow \beta & & \downarrow \alpha^{-1}[-]\alpha \\ H' & \xrightarrow{\varphi'} & \text{Aut}(K') \end{array}$$

dove $\alpha^{-1}[-]\alpha: \text{Aut}(K) \rightarrow \text{Aut}(K')$ è la funzione che associa a $f \in \text{Aut}(K)$ la composizione $\alpha^{-1}f\alpha$ (da sinistra verso destra).

$$\begin{array}{ccc} K & \xrightarrow{f} & K \\ \alpha^{-1} \uparrow & & \downarrow \alpha \\ K' & \xrightarrow{\alpha^{-1}f\alpha} & K' \end{array}$$

Allora $K \rtimes_{\varphi} H \simeq K' \rtimes_{\varphi'} H'$.

(Nota: in classe è stata fatta questa osservazione nel caso specifico $H = H', K = K'$, in cui quindi $\beta \in \text{Aut}(H)$ e $\alpha \in \text{Aut}(K)$.)

Fatto. Sia G un gruppo, siano H e N sottogruppi di G tali che $G = N \rtimes H$ (prodotto semidiretto interno). Sia $\varphi: H \rightarrow \text{Aut}(N)$ l'omomorfismo corrispondente, e sia G' il gruppo che si costruisce come prodotto semidiretto esterno corrispondente a tale omomorfismo. Allora G e G' sono isomorfi.

Per una spiegazione più approfondita della corrispondenza tra prodotto semidiretto interno e prodotto semidiretto esterno, si guardi la Sezione 2 (ma non è necessario farlo).

Esercizio 8. Siano G, H, G' e H' gruppi finiti tali che $|G| = |G'|, |H| = |H'|$ e $G \times H \simeq G' \times H'$.

- (a) Mostrare che, con le date ipotesi, *non* necessariamente si ha $G \simeq G'$.
- (b) Dimostrare che, se $|G|$ e $|H|$ sono coprimi, allora $G \simeq G'$ e $H \simeq H'$.

Soluzione. (a) $S_3 \times \mathbb{Z}_6 \simeq \mathbb{Z}_6 \times S_3$, ma $S_3 \not\simeq \mathbb{Z}_6$.

⁵Ricordiamo che il sottogruppo normale è A . Se avete delle note, controllate che siano conformi a questa notazione.

- (b) Sia $\varphi: G \times H \rightarrow G' \times H'$ un isomorfismo. Ogni elemento del tipo $(g, 1)$ deve essere mandato da φ in un elemento di tipo $(g', 1)$ per questione di ordine (usando la coprimalità). Allora la composizione $G \xrightarrow{\iota_1} G \times H \xrightarrow{\varphi} G' \times H' \xrightarrow{\pi_1} G'$ è un omomorfismo iniettivo, quindi anche suriettivo (dato che $|G| = |G'| < \infty$), quindi isomorfismo. Analogamente per H e H' .

1. CORRISPONDENZA TRA PRODOTTO DIRETTO INTERNO E PRODOTTO DIRETTO ESTERNO.

Dato un prodotto diretto interno $G = H \times K$, a questi sono associati due gruppi H e K . Viceversa, dati due gruppi H e K , ad essi è associato un gruppo $G = H \times K$ (prodotto diretto esterno). Questi due processi sono l'uno l'inverso dell'altro, e qui cercherò di chiarire in che senso.

Per l'occasione, userò delle definizioni che non vanno prese come standard.

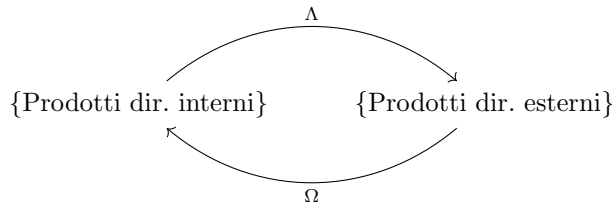
Definizione 1. Chiamiamo *prodotto diretto interno* una tripla (G, H, K) dove G è un gruppo, H e K sono sottogruppi normali di G tali che $H \cap K = 1$, e $G = HK$.

Definizione 2. Chiamiamo *prodotto diretto esterno* una coppia (H, K) dove H e K sono gruppi.

Dato un prodotto diretto interno (G, H, K) , si ha che (H, K) è un prodotto diretto esterno.

Ad ogni prodotto diretto esterno (H, K) , associamo un prodotto diretto interno $(H \times K, \overline{H}, \overline{K})$, dove l'operazione di gruppo su $H \times K$ è definita così: $(h_1, k_1) \cdot (h_2, k_2) = (h_1 h_2, k_1 k_2)$, ed inoltre $\overline{H} = \{(h, 1) \mid h \in H\}$, e $\overline{K} = \{(1, k) \mid k \in K\}$.

Quindi abbiamo due applicazioni



dove $\Lambda(G, H, K) = (H, K)$, e $\Omega(H, K) = (H \times K, \overline{H}, \overline{K})$, come sopra.

Le due applicazioni Λ e Ω sono, in un senso che dobbiamo specificare meglio, una l'inversa dell'altra: se partiamo da un prodotto diretto interno (G, H, K) , allora $\Omega(\Lambda(G, H, K))$ è "strutturalmente simile" a (G, H, K) . Ugualmente, se partiamo da un prodotto diretto esterno (H, K) , allora $\Lambda(\Omega(H, K))$ è "strutturalmente simile" a (H, K) . Definiamo cosa vuol dire strutturalmente simile.

Definizione 3. Due prodotti diretti interni (G, H, K) e (G', H', K') si dicono *simili* se esiste un isomorfismo di gruppi $\varphi: G \rightarrow G'$ tale che $\varphi(H) = H'$ e $\varphi(K) = K'$.

Definizione 4. Due prodotti diretti esterni (H, K) e (H', K') si dicono *simili* se $H \simeq H'$ e $K \simeq K'$.

Ed ecco il teorema che stabilisce che prodotti diretti interni ed esterni sono "la stessa cosa", cioè danno la stessa informazione. (Si veda Teorema 2 più sotto per una riformulazione più immediata.)

Teorema 1. (a) Se (G, H, K) e (G', H', K') sono prodotti diretti interni simili, allora $\Lambda(G, H, K)$ e $\Lambda(G', H', K')$ sono prodotti diretti esterni simili.

(b) Se (H, K) e (H', K') sono prodotti diretti esterni simili, allora $\Omega(G, H, K)$ e $\Omega(G', H', K')$ sono prodotti diretti interni simili.

(c) Ogni prodotto diretto interno (G, H, K) è simile a $\Omega(\Lambda(G, H, K))$.

(d) Ogni prodotto diretto esterno (H, K) è simile a $\Lambda(\Omega(H, K))$.

(Si deduce che vale anche il viceversa in (a) e (b).)

Il Teorema 1 dice che Λ e Ω stabiliscono una biiezione tra i quozienti delle due classi dei prodotti diretti interni e dei prodotti diretti esterni per la relazione di similitudine.

Il Teorema 1 si può riformulare in modo più immediato così.

Teorema 2. (a) Se (G, H, K) e (G', H', K') sono prodotti diretti interni simili, allora $H \simeq H'$ e $K \simeq K'$.

(b) Siano H, K, H', K' gruppi con $H \simeq H'$ e $K \simeq K'$; allora i prodotti diretti interni $(H \times K, \overline{H}, \overline{K})$ e $(H' \times K', \overline{H'}, \overline{K}')$ sono simili.

(c) Ogni prodotto diretto interno (G, H, K) è simile a $(H \times K, \overline{H}, \overline{K})$.

(d) Dati due gruppi H e K , si ha che $H \simeq \overline{H}$ e $K \simeq \overline{K}$.

2. CORRISPONDENZA TRA PRODOTTO SEMIDIRETTO INTERNO E PRODOTTO SEMIDIRETTO ESTERNO.

Dato un prodotto semidiretto interno $G = N \rtimes H$, a questo è associata una mappa $\varphi: H \rightarrow \text{Aut}(N)$. Viceversa, dati due gruppi H e N , ed una mappa $\varphi: H \rightarrow \text{Aut}(N)$, abbiamo un gruppo $G = N \rtimes H$ (prodotto semidiretto esterno). Questi due processi sono l'uno l'inverso dell'altro, e qui cercherò di chiarire in che senso.

Per l'occasione, userò delle definizioni che non vanno prese come standard.

Definizione 5. Chiamiamo *prodotto semidiretto interno* una tripla (G, N, H) dove G è un gruppo, $N \trianglelefteq G$, $H \leq G$ con $H \cap N = 1$, e $G = HN$.

Definizione 6. Chiamiamo *prodotto semidiretto esterno* una tripla (N, H, φ) , dove N e H sono gruppi e φ è un omomorfismo di gruppi da H a $\text{Aut}(N)$.

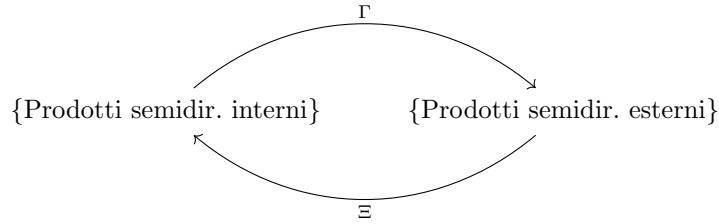
Dato un prodotto semidiretto interno (G, N, H) , a partire da questo possiamo costruire il prodotto semidiretto esterno (N, H, φ) , dove

$$\begin{aligned} \varphi: H &\longrightarrow \text{Aut}(N) \\ h &\longmapsto t_h: N \rightarrow N; g \mapsto h^{-1}gh. \end{aligned}$$

Denotiamo con $\Gamma(G, N, H)$ il prodotto semidiretto esterno costruito a partire dal prodotto semidiretto interno (G, N, H) .

Dato un prodotto semidiretto esterno (N, H, φ) , a partire da questo possiamo costruire il prodotto semidiretto interno $(G, \overline{N}, \overline{H})$, dove il gruppo G ha come insieme soggiacente $H \times N$, e l'operazione è definita così: $(h_1, n_1) \cdot (h_2, n_2) = (h_1 h_2, (\varphi(h_2)(n_1))n_2)$, ed inoltre $\overline{H} = \{(h, 1) \mid h \in H\}$, e $\overline{N} = \{(1, n) \mid n \in N\}$. Denotiamo con $\Xi(N, H, \varphi)$ il prodotto semidiretto interno costruito a partire dal prodotto semidiretto esterno (N, H, φ) .

Quindi abbiamo due applicazioni



Le due applicazioni Γ e Ξ sono, in un senso che dobbiamo specificare meglio, una l'inversa dell'altra: se partiamo da un prodotto semidiretto interno (G, N, H) , allora $\Xi(\Gamma(G, N, H))$ è "strutturalmente simile" a (G, N, H) . Ugualmente, se partiamo da un prodotto semidiretto esterno (N, H, φ) , allora $\Gamma(\Xi(N, H, \varphi))$ è "strutturalmente simile" a (N, H, φ) . Definiamo cosa vuol dire strutturalmente simile.

Definizione 7. Due prodotti semidiretti interni (G, N, H) e (G', N', H') si dicono *simili* se esiste un isomorfismo di gruppi $\varphi: G \rightarrow G'$ tale che $\varphi(N) = N'$ e $\varphi(H) = H'$.

Definizione 8. Due prodotti semidiretti esterni (N, H, φ) e (N', H', φ') si dicono *simili* se esiste una coppia (α, β) , con $\alpha: N \rightarrow N'$ isomorfismo di gruppi e $\beta: H \rightarrow H'$ isomorfismo di gruppi tali che il seguente diagramma commuta

$$\begin{array}{ccc} H & \xrightarrow{\varphi} & \text{Aut}(N) \\ \downarrow \beta & & \downarrow \alpha^{-1}[-]\alpha \\ H' & \xrightarrow{\varphi'} & \text{Aut}(N') \end{array}$$

dove $\alpha^{-1}[-]\alpha: \text{Aut}(N) \rightarrow \text{Aut}(N')$ è la funzione che associa a $f \in \text{Aut}(N)$ la composizione $\alpha^{-1}f\alpha$ (da sinistra verso destra).

$$\begin{array}{ccc} N & \xrightarrow{f} & N \\ \alpha^{-1} \uparrow & & \downarrow \alpha \\ N' & \xrightarrow{\alpha^{-1}f\alpha} & N' \end{array}$$

- Teorema 3.** (a) Se (G, N, H) e (G', N', H') sono prodotti semidiretti interni simili, allora i prodotti semidiretti esterni $\Gamma(G, N, H)$ e $\Gamma(G', N', H')$ sono simili.
- (b) Se (N, H, φ) e (N', H', φ') sono prodotti semidiretti esterni simili, allora i prodotti semidiretti esterni $\Xi(G, N, H)$ e $\Xi(G', N', H')$ sono simili.
- (c) Ogni prodotto semidiretto interno (G, N, H) è simile $\Xi(\Gamma(G, N, H))$.
- (d) Ogni prodotto semidiretto esterno (N, H, φ) è simile a $\Gamma(\Xi(N, H, \varphi))$.

(Si deduce che vale anche il viceversa in (a) e (b).)

Il Teorema 3 dice che Γ e Ξ stabiliscono una biiezione tra i quozienti delle due classi dei prodotti diretti interni e dei prodotti diretti esterni per la relazione di similitudine.

3. COSA RICORDARE

- In S_n ogni commutatore è una permutazione pari. (Esercizio 1)
- Il periodo di (g, h) in $G \times H$ è $\text{mcm}(o(g), o(h))$. (Esercizio 2)
- $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm} \iff \text{MCD}(n, m) = 1$. In tal caso un generatore è $([1]_n, [1]_m)$. (Esercizi 3, 4, 5)
- $\text{Aut}(\mathbb{Z}_n) \simeq U(\mathbb{Z}_n)$, cioè $\text{Aut}(\mathbb{Z}_n)$ è isomorfo al gruppo moltiplicativo degli elementi invertibili (cioè coprimi con n) di \mathbb{Z}_n . (Esercizio 6)
- $\text{Aut}(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$ per p primo. (Esercizio 6)