

**A.A. 2015-2016. CORSO DI ALGEBRA 1.**  
**PROFF. P. PIAZZA, E. SPINELLI.**  
**SOLUZIONE ESERCIZI FOGLIO 6.**

**Esercizio 6.1.** Studiare la compatibilità e risolvere quando possibile il seguente sistema di equazioni congruenziali lineari al variare di  $k \in \mathbb{Z}$ :

$$\begin{cases} 22(X+k) \equiv 2 \pmod{17} \\ 4X \equiv 3k \pmod{11} \\ kX \equiv 2 \pmod{5} \end{cases}$$

*Soluzione.* Cominciamo osservando che i moduli sono tra loro coprimi (si tratta infatti di numeri primi distinti). Pertanto per verificare la compatibilità del sistema al variare di  $k$  ci è sufficiente studiare la compatibilità delle singole equazioni. Partiamo dalla prima  $22(X+k) \equiv 2 \pmod{17}$ . Riducendo 22 modulo 17 e moltiplicando otteniamo quindi che l'equazione è equivalente a  $5X + 5k \equiv 2 \pmod{17}$ . Portando  $5k$  dall'altro lato dell'equazione otteniamo quindi l'equazione  $5X \equiv 2 + 12k \pmod{17}$ . Osserviamo che  $\text{MCD}(5, 17) = 1 \mid 2 + 12k$ , qualsiasi sia  $k$ , e dunque la prima equazione del nostro sistema è compatibile. Riscriviamo il sistema tenendo in considerazione le trasformazioni apportate alla prima equazione:

$$\begin{cases} 5X \equiv 2 + 12k \pmod{17} \\ 4X \equiv 3k \pmod{11} \\ kX \equiv 2 \pmod{5} \end{cases}$$

Consideriamo la seconda equazione  $4X \equiv 3k \pmod{11}$ .  $\text{MCD}(4, 11) = 1 \mid 3k$ , qualsiasi sia  $k \in \mathbb{Z}$  e pertanto anche la seconda equazione è compatibile qualsiasi sia il valore di  $k$ .

Andiamo quindi a studiare la compatibilità della terza equazione. In questa terza equazione  $k$  compare come coefficiente della  $X$ . Essendo 5 primo osserviamo che  $k$  è invertibile a meno che esso non sia congruo a 0 modulo 5. In questo secondo caso l'equazione risulta non compatibile e dunque per i valori  $k = 5j$  il sistema non ammette soluzione.

Dallo studio appena fatto risulta che il sistema ammette un'unica soluzione modulo 935 se e soltanto se  $k \neq 5j$ .

Andiamo a risolvere il sistema per  $k \not\equiv 0 \pmod{5}$ . Denoteremo con  $k'$  l'inverso aritmetico modulo 5 di  $k$ . Per risolvere il sistema ci riportiamo ad un sistema cinese moltiplicando ogni equazione per l'inverso aritmetico rispetto all'opportuno modulo del coefficiente della variabile  $X$ . L'inverso di 5 modulo 17 è 7 ( $1 = 7 \cdot 5 - 2 \cdot 17 = 35 - 34$ ), mentre l'inverso di 4 modulo 11 è 3. Per quanto riguarda l'inverso di  $k$ , sappiamo che esiste e lo denoteremo per il momento  $k'$ . Una volta determinata la soluzione del sistema in funzione di  $k$  e  $k'$  andremo poi a sostituire a  $k$  e  $k'$  gli opportuni valori per scrivere in modo completamente esplicito l'insieme delle soluzioni al variare di  $k$ . Un modo alternativo per rispondere alla domanda è risolvere 4 sistemi distinti sostituendo alla variabile  $k$  la quantità  $i + 5\ell$  con  $i = 1, 2, 3, 4$ .

Dalla discussione precedente segue che per  $k \not\equiv 0 \pmod{5}$  il nostro sistema è equivalente al seguente sistema cinese:

$$\begin{cases} X \equiv 14 + 16k \pmod{17} \\ X \equiv 9k \pmod{11} \\ X \equiv 2k^{-1} \pmod{5} \end{cases}$$

Risolviamo per sostituzione: la generica soluzione della prima equazione è  $x_Y = (14 + 16k) + 17Y$ . Sostituiamo nella seconda equazione e troviamo (riducendo modulo 11 i coefficienti):

$$3 + 5k + 6Y \equiv 9k \pmod{11} \Leftrightarrow 6Y \equiv 4k + 8 \pmod{11}$$

L'inverso aritmetico di 6 modulo 11 è 2 e dunque l'equazione diventa:  $Y \equiv 8k + 5 \pmod{11}$ . La soluzione generica di tale equazione è  $y_Z = (8k + 5) + 11Z$ . Andando a sostituire ad  $Y$  la soluzione

generica  $y_Z$  otteniamo:  $x_Z = (14 + 16k) + 17(8k + 5) + 187Z = (152k + 99) + 187Z$ . Andiamo a sostituire nell'ultima equazione ed otteniamo, una volta ridotti i coefficienti modulo 5:

$$2k + 4 + 2Z \equiv 2k^{-1} \pmod{5} \Leftrightarrow 2Z \equiv 1 + 2k^{-1} + 3k \pmod{5} \Leftrightarrow Z \equiv 3 + k^{-1} + 4k \pmod{5}$$

La soluzione generica è dunque:  $z_j = (3 + k^{-1} + 4k) + 5j$ . Andiamo a sostituire tale valore a  $Z$  in  $x_Z$  e troviamo così:  $x_j = (660 + 900k + 187k^{-1}) + 935j$ .

Sostituiamo ora a  $k$  i valori  $1 + 5\ell$ ,  $2 + 5\ell$ ,  $3 + 5\ell$ ,  $4 + 5\ell$ ; come loro inversi aritmetici modulo 5 possiamo prendere rispettivamente 1, 3, 2 e 4. Andiamo quindi a sostituire i seguenti valori per la coppia  $(k, k')$  nella formula trovata nel precedente paragrafo:

• se  $k = 1 + 5\ell$  abbiamo detto che possiamo scegliere  $k' = 1$ ; andando a sostituire nella formula trovata per  $x_j$  (e riducendo modulo 935) abbiamo quindi:

$$x_j^{1,\ell} = (812 + 760\ell) + 935j$$

• se  $k = 2 + 5\ell$  possiamo scegliere  $k' = 3$ ; andando a sostituire nella formula che definisce  $x_j$  (e riducendo modulo 935) otteniamo:

$$x_j^{2,\ell} = (216 + 760\ell) + 935j$$

• se  $k = 3 + 5\ell$  possiamo scegliere  $k' = 2$ ; sostituiamo nella formula per  $x_j$  e riduciamo modulo 935:

$$x_j^{3,\ell} = (929 + 760\ell) + 935j$$

• se  $k = 4 + 5\ell$  abbiamo  $k' = 4$  sostituiamo dunque nella formula per  $x_j$  e riduciamo modulo 935:

$$x_j^{4,\ell} = (333 + 760\ell) + 935j$$

Questo risolve il primo esercizio.  $\square$

**Esercizio 6.2.** Consideriamo  $\mathbb{Z}_{15}$  e consideriamo l'insieme degli invertibili  $\mathcal{U}(\mathbb{Z}_{15})$ .

(A) Determinare  $\mathcal{U}(\mathbb{Z}_{15})$ .

(B) Per ciascun elemento di  $g \in \mathcal{U}(\mathbb{Z}_{15})$  calcolare  $g^{1347}$ .

*Soluzione.* Cominciamo dal punto (A). Si chiede di determinare l'insieme degli invertibili di  $\mathbb{Z}_{15}$ . Sappiamo dalla teoria che il gruppo moltiplicativo degli invertibili modulo 15 è formato dalle classi resto modulo 15 i cui rappresentanti sono coprimi con 15. Per rispondere dunque alla domanda dobbiamo determinare tutti gli interi  $0 \leq k \leq 14$  tali che  $\text{MCD}(k, 15) = 1$ . I rappresentanti delle classi resto in questione sono quindi: 1, 2, 4, 7, 8, 11, 13, 14. Pertanto il gruppo moltiplicativo degli invertibili di  $\mathbb{Z}_{15}$  è:

$$\mathcal{U}(\mathbb{Z}_{15}) = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$$

dove si è deciso di denotare con  $\bar{k}$  la classe resto di  $k$  modulo 15.

Passiamo quindi al punto (B). Si chiedeva di calcolare la potenza 1347-sima di ciascun elemento  $g \in \mathcal{U}(\mathbb{Z}_{15})$ . Osserviamo che calcolare  $\bar{k}^{1347}$ , dove  $\bar{k} \in \mathcal{U}(\mathbb{Z}_{15})$  è equivalente a risolvere  $k^{1347} \equiv X \pmod{15}$  con  $\text{MCD}(k, 15) = 1$ . La domanda quindi si riduceva ad un'equazione congruenziale da risolvere utilizzando il Teorema di Eulero-Fermat; utilizzando tale risultato (per definizione abbiamo infatti che per ogni  $\bar{k} \in \mathcal{U}(\mathbb{Z}_{15})$  risulta  $\text{MCD}(k, 15) = 1$ ) il nostro problema si riduce a calcolare  $\bar{k}^3$  in  $\mathcal{U}(\mathbb{Z}_{15})$ , infatti sappiamo che per ogni  $\bar{k} \in \mathcal{U}(\mathbb{Z}_{15})$  risulta  $\bar{k}^{\varphi(15)} = \bar{k}^8 \equiv 1 \pmod{15}$ , pertanto osservando che  $1347 \equiv 3 \pmod{8}$  abbiamo provato la precedente affermazione.

Il resto dell'esercizio è un banale conto modulo 15. Per completezza scriveremo i risultati:

$$\bar{1}^3 = \bar{1}; \bar{2}^3 = \bar{8}; \bar{4}^3 = \bar{4}; \bar{7}^3 = \bar{13}; \bar{8}^3 = \bar{2}; \bar{11}^3 = \bar{11}; \bar{13}^3 = \bar{7}; \bar{14}^3 = \bar{14}.$$

*Curiosità.* Osserviamo che per  $\bar{k} = \bar{4}, \bar{11}, \bar{13}$  risulta  $\bar{k}^3 = \bar{k}$ . Ragionando per induzione è possibile provare che  $\bar{k}^{3+2j} = \bar{k}$ , per ogni  $j \in \mathbb{N}$ .  $\square$

**Esercizio 6.3.** Denotiamo con  $i$  l'unità immaginaria di  $\mathbb{C}$ . Consideriamo le seguenti matrici:

$$\pm \underline{1} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad \pm \underline{i} = \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}; \quad \pm \underline{j} = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \quad \pm \underline{k} = \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

(A) Verificare che l'insieme  $Q = \{\pm \underline{1}, \pm \underline{i}, \pm \underline{j}, \pm \underline{k}\}$  ha una struttura di gruppo rispetto all'usuale prodotto tra matrici a coefficienti complessi. A tal scopo scrivere una tabella moltiplicativa che descriva l'operazione di prodotto su  $Q$ .

(B) Determinare tutti i sottogruppi di  $Q$ . Stabilire se vi sono sottogruppi normali ed in caso esibirli. Determinare il centro del gruppo  $Q$ .

(C) Denotiamo con  $\mathcal{Z}(Q)$  il centro del gruppo  $Q$ . Descrivere il gruppo quoziente  $Q/\mathcal{Z}(Q)$  scrivendone una tavola moltiplicativa.

(D) Descrivere tutti gli omomorfismi da  $Q$  in  $\mathbb{Z}_4$ .

*Soluzione.* Cominciamo dal punto (A). Per verificare che  $Q$  è un gruppo rispetto all'usuale prodotto righe per colonne ricordiamo che bisogna verificare che  $Q$  è chiuso rispetto all'operazione di prodotto righe per colonne (tale operazione infatti è a priori definita su un gruppo più grande ovvero  $GL(2, \mathbb{C})$ , bisogna quindi verificare che la restrizione di tale operazione al sottoinsieme  $Q \subset GL(2, \mathbb{C})$  definisca un'operazione su  $Q$ ). Verificheremo quindi scrivendo una tabella dei prodotti (1) che il prodotto di elementi di  $Q$  è in  $Q$ ; (2) che ogni elemento di  $Q$  ha un inverso in  $Q$ . Il fatto che l'identità sia in  $Q$  e che tale prodotto sia associativo sono ereditate dal fatto che stiamo restringendo un'operazione definita su un gruppo più grande,  $GL(2, \mathbb{C})$ , ad un sottoinsieme  $Q$  che contiene l'identità. La tabella dei prodotti è la seguente:

$\cdot$	$\underline{1}$	$\underline{-1}$	$\underline{i}$	$\underline{-i}$	$\underline{j}$	$\underline{-j}$	$\underline{k}$	$\underline{-k}$
$\underline{1}$	$\underline{1}$	$\underline{-1}$	$\underline{i}$	$\underline{-i}$	$\underline{j}$	$\underline{-j}$	$\underline{k}$	$\underline{-k}$
$\underline{-1}$	$\underline{-1}$	$\underline{1}$	$\underline{-i}$	$\underline{i}$	$\underline{-j}$	$\underline{j}$	$\underline{-k}$	$\underline{k}$
$\underline{i}$	$\underline{i}$	$\underline{-i}$	$\underline{-1}$	$\underline{1}$	$\underline{-k}$	$\underline{k}$	$\underline{-j}$	$\underline{j}$
$\underline{-i}$	$\underline{-i}$	$\underline{i}$	$\underline{1}$	$\underline{-1}$	$\underline{k}$	$\underline{-k}$	$\underline{j}$	$\underline{-j}$
$\underline{j}$	$\underline{j}$	$\underline{-j}$	$\underline{-k}$	$\underline{k}$	$\underline{-1}$	$\underline{1}$	$\underline{-i}$	$\underline{i}$
$\underline{-j}$	$\underline{-j}$	$\underline{j}$	$\underline{k}$	$\underline{-k}$	$\underline{1}$	$\underline{-1}$	$\underline{k}$	$\underline{-k}$
$\underline{k}$	$\underline{k}$	$\underline{-k}$	$\underline{-j}$	$\underline{j}$	$\underline{-i}$	$\underline{i}$	$\underline{-1}$	$\underline{1}$
$\underline{-k}$	$\underline{-k}$	$\underline{k}$	$\underline{j}$	$\underline{-j}$	$\underline{i}$	$\underline{-i}$	$\underline{1}$	$\underline{-1}$

TABELLA 1. Tavola moltiplicativa di  $Q$

In particolare risulta che  $Q$  è chiuso rispetto al prodotto righe per colonne, e che la restrizione di tale operazione a  $Q$  è tale che per ogni elemento di  $Q$  vi è un inverso in  $Q$ :  $(\pm \underline{1})^{-1} = \pm \underline{1}$ ,  $(\pm \underline{i})^{-1} = \mp \underline{i}$ ,  $(\pm \underline{j})^{-1} = \mp \underline{j}$ ,  $(\pm \underline{k})^{-1} = \mp \underline{k}$ .

Nel punto (B) si chiedeva di determinare tutti i sottogruppi di  $Q$  e di stabilire se vi fossero sottogruppi normali ed in caso esibirli.

Cominciamo osservando che, grazie al Teorema di Lagrange, sappiamo che se  $H$  è un sottogruppo di  $Q$  allora  $|H| \mid |Q|$ . Questo in particolare significa che se  $H < Q$  allora  $|H|$  è uguale a 1, 2, 4, o 8.

Chiaramente se  $|H| = 1$ ,  $H = \{1\}$  e se  $|H| = 8$  allora  $H = Q$ . Dobbiamo quindi preoccuparci unicamente dei sottogruppi di ordine 2 e 4. Osserviamo a tal scopo che se  $H$  contiene uno qualsiasi tra i seguenti elementi  $\pm \underline{i}$ ,  $\pm \underline{j}$ ,  $\pm \underline{k}$  allora  $|H| \geq 4$ , infatti ciascuno di questi elementi genera un sottogruppo ciclico<sup>1</sup> di ordine 4, come si può verificare direttamente utilizzando la tabella. Non resta dunque che verificare l'ordine dell'elemento  $-1$ . L'ordine di tale elemento è evidentemente 2 (infatti, come

<sup>1</sup>Per futura referenza, dato un gruppo  $G$  e dato  $g \in G$  denoteremo con  $\langle g \rangle$  il sottogruppo ciclico generato da  $g$ .

si evince dalla tabella,  $(-\underline{1})^2 = \underline{1}$ ). Abbiamo pertanto un unico sottogruppo di ordine due (dunque necessariamente ciclico)  $H = \langle -\underline{1} \rangle = \{\pm\underline{1}\} \simeq \mathbb{Z}_2$ .

Supponiamo ora  $|H| = 4$ . Osservando la tabella ci possiamo accorgere che i sottogruppi ciclici generati rispettivamente da  $\underline{i}$ ,  $\underline{j}$ ,  $\underline{k}$ , ovvero  $\langle \underline{i} \rangle = \{\pm\underline{1}, \pm\underline{i}\}$ ,  $\langle \underline{j} \rangle = \{\pm\underline{1}, \pm\underline{j}\}$ ,  $\langle \underline{k} \rangle = \{\pm\underline{1}, \pm\underline{k}\}$  sono tre sottogruppi ciclici di ordine 4 che ammettono, ciascuno, due generatori, rispettivamente  $\pm\underline{i}$ ,  $\pm\underline{j}$ ,  $\pm\underline{k}$ . Questi sottogruppi esauriscono la lista dei sottogruppi di ordine 4: infatti se  $H$  è di ordine 4 esso deve contenere almeno uno dei generatori dei tre gruppi ciclici introdotti poco sopra, e dunque tutte le sue potenze. Poiché il sottogruppo ciclico generato da un tale elemento avrebbe cardinalità uguale a  $|H|$  esso deve essere  $H$  stesso. Questo esaurisce la lista dei sottogruppi di  $Q$ . Qui di sotto il reticolo dei sottogruppi di  $Q$  secondo l'analisi da noi portata avanti.

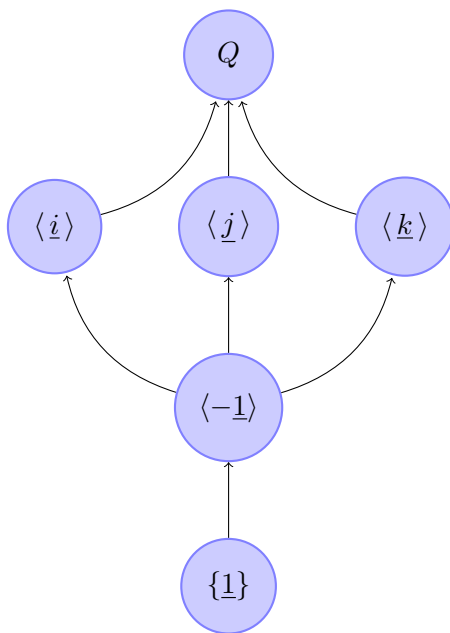


FIGURA 1. Reticolo dei sottogruppi di  $Q$ .

Torniamo dunque alla seconda parte della domanda (B). Vi sono dei sottogruppi normali? Chiaramente abbiamo i due sottogruppi normali banali ovvero  $\{\underline{1}\}$  e  $Q$ . Ve ne sono degli altri?

Consideriamo il sottogruppo  $\langle -\underline{1} \rangle$ . Dalla tabella dei prodotti di  $Q$  risulta evidente che gli elementi  $\pm\underline{1}$  commutano con tutti gli altri elementi del gruppo, mentre gli elementi  $\pm\underline{i}$  non commutano con  $\{\pm\underline{j}, \pm\underline{k}\}$ , gli elementi  $\pm\underline{j}$  non commutano con  $\{\pm\underline{i}, \pm\underline{k}\}$ , gli elementi  $\pm\underline{k}$  non commutano con  $\{\pm\underline{i}, \pm\underline{j}\}$ . Poiché gli elementi del sottogruppo  $\langle \pm\underline{1} \rangle$  commutano con tutti gli elementi di  $Q$  in particolare il sottogruppo è normale. Inoltre, poiché ogni altro elemento di  $Q$  non commuta con tutti gli elementi di  $Q$ , possiamo concludere che il sottogruppo  $\langle \pm\underline{1} \rangle$  è proprio il centro del gruppo  $Q$ , denotato anche  $\mathcal{Z}(Q)$ <sup>2</sup>.

Per quanto riguarda gli altri tre sottogruppi,  $\langle \underline{i} \rangle$ ,  $\langle \underline{j} \rangle$ ,  $\langle \underline{k} \rangle$ , sono anch'essi normali. Possiamo procedere in due modi: utilizzando la tabella e dunque verificando direttamente che verificano la condizione data nella definizione di sottogruppo normale, altrimenti si può osservare il seguente fatto, ovvero che ciascuno di questi gruppi ha indice 2 in  $Q$  e concludere utilizzando la seguente:

*Affermazione.* Sia  $G$  un gruppo finito. Ogni sottogruppo  $H$  di indice 2 in  $G$  è normale.

<sup>2</sup>Sia  $G$  un gruppo. Il centro del gruppo  $G$  è, per definizione, il sottogruppo  $\mathcal{Z}(G) = \{g \in G \mid gh = hg, \forall h \in G\}$ .

*Dimostrazione.* Sia  $g \in G \setminus H$ . Siano  $H, Hg$  le due classi laterali sinistre di  $G$  modulo  $H$ , e siano  $H, gH$  le classi laterali destre. Supponiamo che  $gH \neq Hg$ . Esisterebbe allora un elemento  $g_0 \in G$  tale che  $g_0 \in gH$  ma  $g_0 \notin Hg$  o viceversa  $g_0 \in Hg$  ma  $g_0 \notin gH$ . Supponiamo che valga la prima. Per definizione  $gH \cap H = \emptyset$  (l'insieme delle classi laterali destre, così come l'insieme delle classi laterali sinistre costituisce infatti una partizione di  $G$ ) e dunque avremmo  $g_0 \in G = H \cup Hg$  ma  $g_0 \notin H$  e  $g_0 \notin Hg$  che è assurdo. Il secondo caso può essere trattato in analogia. Concludiamo quindi che  $gH = Hg$  e dunque le classi laterali destre e sinistre coincidono, dunque il sottogruppo  $H$  è normale.  $\square$

Passiamo alla domanda (C). Abbiamo visto nel punto (B) che il sottogruppo  $\langle \pm 1 \rangle$  è il centro del gruppo  $Q$ , in particolare esso è normale e possiamo dunque considerare il gruppo quoziente  $Q/\langle \pm 1 \rangle = Q/\mathcal{Z}(Q)$ .

Vogliamo determinare il gruppo quoziente. Cominciamo osservando che  $|Q/\mathcal{Z}(Q)| = \frac{|Q|}{|\mathcal{Z}(Q)|} = 4$  e che di gruppi di ordine 4, a meno di isomorfismi, ne esistono solamente due, ovvero il gruppo ciclico di ordine 4,  $\mathbb{Z}_4$ , e il gruppo di Klein,  $\mathbb{Z}_2 \times \mathbb{Z}_2$ ; possiamo quindi limitarci a verificare se in  $Q/\mathcal{Z}(Q)$  vi siano o meno elementi di ordine 4 in caso affermativo il gruppo quoziente sarebbe isomorfo a  $\mathbb{Z}_4$ , in caso negativo il gruppo quoziente sarebbe isomorfo al gruppo di Klein.

Ricordiamo che dato un gruppo  $G$  e un sottogruppo normale  $H$ , denotate con  $H = Hg_1, Hg_2, \dots, Hg_n$  è ben definita il seguente prodotto tra classi laterali sinistre:

$$Hg_i \cdot Hg_j = H(g_i \cdot g_j)$$

l'identità di tale prodotto è data dalla classe  $H$ , mentre l'inversa della classe  $Hg$  è la classe  $Hg^{-1}$ .

Possiamo quindi descrivere esplicitamente il gruppo quoziente  $Q/\mathcal{Z}(Q)$ , descrivendo le classi laterali sinistre di  $Q$  modulo  $\mathcal{Z}(Q)$  e utilizzando la tabella moltiplicativa di  $Q$ .

Cominciamo quindi elencando le classi laterali di  $Q$  modulo  $\langle \pm 1 \rangle$ . Da un punto di vista insiemistico esse sono:  $\{\pm 1\}$ ,  $\{\pm 1\}i$ ,  $\{\pm 1\}j$ ,  $\{\pm 1\}k$ . Scriviamo ora la tabella moltiplicativa di  $Q/\mathcal{Z}(Q)$  utilizzando quella di  $Q$ :

$\cdot$	$\{\pm 1\}$	$\{\pm 1\}i$	$\{\pm 1\}j$	$\{\pm 1\}k$
$\{\pm 1\}$	$\{\pm 1\}$	$\{\pm 1\}i$	$\{\pm 1\}j$	$\{\pm 1\}k$
$\{\pm 1\}i$	$\{\pm 1\}i$	$\{\pm 1\}$	$\{\pm 1\}k$	$\{\pm 1\}j$
$\{\pm 1\}j$	$\{\pm 1\}j$	$\{\pm 1\}k$	$\{\pm 1\}$	$\{\pm 1\}i$
$\{\pm 1\}k$	$\{\pm 1\}k$	$\{\pm 1\}j$	$\{\pm 1\}i$	$\{\pm 1\}$

TABELLA 2. Tavola moltiplicativa di  $Q/\mathcal{Z}(Q)$

Osservando la diagonale della tabella concludiamo che ciascun elemento di  $Q/\mathcal{Z}(Q)$  differente dall'identità è l'inverso di sé stesso, in particolare ha ordine 2. Il gruppo è quindi isomorfo a  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , ovvero il gruppo di Klein.

Passiamo all'ultimo punto dell'esercizio, il punto (D). Si chiedeva di individuare tutti gli omomorfismi da  $Q$  in  $\mathbb{Z}_4$ . La prima osservazione da fare è che non esistono omomorfismi suriettivi da  $Q$  in  $\mathbb{Z}_4$ : sia infatti  $\varphi : Q \rightarrow \mathbb{Z}_4$  un tale omomorfismo allora  $|\ker(\varphi)| = |Q|/|\mathbb{Z}_4| = 2$ ; poiché  $\ker(\varphi)$  è un sottogruppo normale di  $Q$  di cardinalità 2 esso deve essere il sottogruppo  $\langle \pm 1 \rangle = \mathcal{Z}(Q)$ . Per il Teorema fondamentale di omomorfismo esisterebbe dunque un omomorfismo  $\bar{\varphi} : Q/\mathcal{Z}(Q) \rightarrow \mathbb{Z}_4$  iniettivo e suriettivo. Ma abbiamo visto nel punto (C) che  $Q/\mathcal{Z}(Q)$  è isomorfo a  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , dunque abbiamo un assurdo.

Dalla discussione precedente segue che non esistono omomorfismi suriettivi da  $Q$  in  $\mathbb{Z}_4$ .

Ricordiamo che l'immagine di un omomorfismo  $\varphi : G \rightarrow G'$  è un sottogruppo di  $G'$ .  $\mathbb{Z}_4$  ha tre sottogruppi:  $\{\bar{0}\}$  e  $\mathbb{Z}_4$  e il sottogruppo  $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}\}$ . Vi è un unico isomorfismo avente per immagine il

sottogruppo banale di  $\mathbb{Z}_4$ , ovvero  $\varphi_{\bar{0}} : Q \rightarrow \mathbb{Z}_4$ ,  $\varphi(\pm\bar{1}) = \varphi(\pm\bar{i}) = \varphi(\pm\bar{j}) = \varphi(\pm\bar{k}) = \bar{0}$ . Abbiamo escluso con l'osservazione iniziale l'esistenza di omomorfismi suriettivi, non ci resta quindi che determinare gli omomorfismi  $\varphi : Q \rightarrow \mathbb{Z}_4$  aventi per immagine il sottogruppo  $\langle \bar{2} \rangle$ . Sia ora  $\varphi : Q \rightarrow \mathbb{Z}_4$  un isomorfismo tale che  $Im(\varphi) = \langle \bar{2} \rangle$ . Il nucleo di un tale isomorfismo deve avere cardinalità 4. Vi sono dunque tre scelte possibili. Supponiamo che  $\ker(\varphi) = \langle \bar{i} \rangle$ , allora per il Teorema fondamentale di omomorfismo  $\varphi$  induce un isomorfismo  $\bar{\varphi} : Q/\langle \bar{i} \rangle \rightarrow \langle \bar{2} \rangle$  tale isomorfismo invia  $\{\pm\bar{1}, \pm\bar{i}\}$  in  $\bar{0}$  e  $\{\pm\bar{j}, \pm\bar{k}\}$  in  $\bar{2}$ . Da tale discussione segue che esiste un unico omomorfismo  $\varphi_{\bar{i}} : Q \rightarrow \mathbb{Z}_4$  che ha come nucleo  $\langle \bar{i} \rangle$  e come immagine  $\langle \bar{2} \rangle$ . In modo completamente analogo si può osservare che esiste un unico omomorfismo  $\varphi_{\bar{j}} : Q \rightarrow \mathbb{Z}_4$  il cui nucleo è  $\langle \bar{j} \rangle$  e la cui immagine sia  $\langle \bar{2} \rangle$  ed un unico omomorfismo  $\varphi_{\bar{k}}$  che abbia come nucleo  $\langle \bar{k} \rangle$  e come immagine  $\langle \bar{2} \rangle$ . Abbiamo quindi determinato tutti gli omomorfismi da  $Q$  in  $\mathbb{Z}_4$ :  $\varphi_{\bar{0}}, \varphi_{\bar{i}}, \varphi_{\bar{j}}, \varphi_{\bar{k}}$ .  $\square$

**Esercizio 6. 4.** Sia  $(G, \cdot)$  un gruppo abeliano di cardinalità  $n < +\infty$  e siano  $1_G = g_1, g_2, \dots, g_n$  gli elementi di  $G$ . Senza fare uso del Teorema di Lagrange, ma utilizzando la definizione di gruppo abeliano:

(A) Mostrare che  $g_1^2 \cdots g_n^2 = 1_G$ .

(B) Mostrare che  $g^n = 1_G$  per ogni  $g \in G$ . (*Suggerimento. Osservare che per ogni fissato  $g \in G$  l'applicazione  $L_g : G \rightarrow G$ ,  $L_g : h \mapsto g \cdot h$  è biettiva*)

(C) Utilizzando l'Esercizio 3.6 del Foglio 3, osservare che l'ordine di un elemento<sup>3</sup>  $g \in G$  divide  $|G| = n$ . Se non si è svolto l'Esercizio precedentemente citato dimostrare che l'ordine di un elemento  $g \in G$  divide ogni numero  $k$  tale che  $g^k = 1_G$ .

*Soluzione.* Sappiamo che uno dei corollari del Teorema di Lagrange è il seguente:

*Sia  $G$  un gruppo finito e sia  $g \in G$ . Denotiamo con  $o(g)$  l'ordine dell'elemento  $g$ , allora  $o(g) \mid |G|$ .*

Scopo di questo esercizio era dimostrare questo risultato sotto l'ipotesi addizionale che il gruppo  $G$  fosse abeliano, senza far uso del Teorema di Lagrange.

Cominciamo dal punto (A). Vogliamo dimostrare che  $g_1^2 \cdots g_n^2 = 1_G$ . Ricordiamo che in  $G = \{1_G = g_1, g_2, \dots, g_n\}$  vi sono due tipi di elementi. Quelli di ordine 2 o inferiore (cioè l'identità di  $G$  -l'unico elemento che ha ordine 1- e tutti gli elementi di ordine 2) e quelli il cui ordine è superiore a 2. Essendo il gruppo  $G$  abeliano l'ordine nel prodotto  $g_1^2 \cdots g_n^2$  è ininfluenza; possiamo quindi supporre di aver ordinato gli elementi di  $G$  in modo tale che tutti gli elementi di ordine minore o uguale a due siano i primi  $k$  (qui  $k \geq 1$ ). Osserviamo che se l'insieme degli elementi di ordine  $> 2$  in un gruppo finito  $G$  è sempre pari. Infatti se  $g^2 \neq 1_G$  (e dunque  $g^{-2} \neq 1_G$ ) allora  $g \neq g^{-1}$ . Poiché in un gruppo ogni elemento ha un unico inverso ne segue che l'insieme degli elementi di ordine maggiore di due ha cardinalità pari infatti esso è unione disgiunta dei sottoinsiemi formati dalle coppie di inversi. Ne segue dunque che  $n = k + 2m$ . Supponiamo quindi di aver numerato i restanti  $2m$  elementi in modo tale che  $g_{k+2i} = g_{k+2i-1}^{-1}$  dove  $i = 1 \dots m$ ; il punto (A) è allora banale:

$$g_1^2 \cdots g_n^2 = 1_G^2 \cdot (g_1^2 \cdots g_k^2)(g_{k+1}^2 g_{k+1}^{-2}) \cdots (g_{k+2m-1}^2 g_{k+2m-1}^{-2}) = 1_G$$

Passiamo al punto (B). Veniva chiesto di dimostrare che per ogni elemento  $g \in G$  risulta  $g^n = g^{|G|} = 1_G$ . Consideriamo come prima una numerazione degli elementi di  $G = \{1_G = g_1, \dots, g_n\}$ . Dato  $g \in G$  consideriamo la seguente applicazione  $L_g : G \rightarrow G$ ,  $L_g : g_j \mapsto g \cdot g_j$ . Osserviamo che tale mappa è biettiva: esiste infatti un'inversa che è data da  $L_{g^{-1}} : G \rightarrow G$ ,  $L_{g^{-1}} : g_j \mapsto g^{-1} \cdot g_j$ . Andiamo quindi a scrivere

$$g^n = g^n \cdot g_1^2 \cdots g_n^2 = (g \cdot g_1) \cdots (g \cdot g_n) \cdot g_1 \cdots g_n = g_{j_1} \cdots g_{j_n} \cdot g_1 \cdots g_n = g_1^2 \cdots g_n^2 = 1_G$$

dove nella penultima disuguaglianza abbiamo utilizzato l'abelianità del gruppo per riordinare il prodotto e il fatto che la moltiplicazione per  $g$  in  $G$  induce una permutazione degli indici della numerazione.

<sup>3</sup>Ricordiamo che l'ordine di un elemento  $g \in G$  è il più piccolo intero positivo  $k$  tale che  $g^k = 1_G$ .

Nell'Esercizio 3.6 del Foglio 3 vi era stato chiesto di dimostrare che in un gruppo  $G$  l'ordine di un elemento  $g \in G$  divide sempre ogni intero  $k$  tale che  $g^k = 1_G$ . Per mostrare tale risultato si procede per contraddizione utilizzando la minimalità dell'ordine dell'elemento  $g$  rispetto alla proprietà  $g^k = 1_G$  (vedere le Soluzioni del Foglio 3). Poiché in (B) abbiamo provato che  $g^n = 1_G$  il punto (C) è dimostrato.  $\square$

**Esercizio 6.5.** Consideriamo il seguente insieme di applicazioni da  $\mathbb{R}$  in  $\mathbb{R}$ :

$$\mathcal{A}(\mathbb{R}) = \{x \mapsto ax + b \mid a \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R}\}$$

(A) Mostrare che tale insieme è un gruppo rispetto alla composizione di applicazioni (denoteremo con  $\circ$  l'operazione di composizione).

(B) Sia  $T_y \in \mathcal{A}(\mathbb{R})$  la traslazione di  $y$ , ovvero l'applicazione definita da  $T_y : x \mapsto x + y$ . Mostrare che il sottoinsieme delle traslazioni  $\mathcal{T}_{\mathbb{R}} = \{T_y \mid y \in \mathbb{R}\}$  è un sottogruppo normale di  $\mathcal{A}(\mathbb{R})$ .

(C) Mostrare che  $\varphi : (\mathbb{R}, +) \rightarrow (\mathcal{A}(\mathbb{R}), \circ)$ ,  $\varphi : y \mapsto T_y$  dove  $T_y(x) = x + y$  è un omomorfismo iniettivo.

(D) Determinare il sottoinsieme  $\mathcal{A}^+$  delle applicazioni in  $\mathcal{A}(\mathbb{R})$  che manda  $\mathbb{R}_+$  in sé biettivamente. Mostrare che si tratta di un sottogruppo di  $(\mathcal{A}(\mathbb{R}), \circ)$ .

(E) Mostrare che esiste una mappa  $F : \mathbb{R}_+ \rightarrow \mathbb{R}$  ed un isomorfismo  $\varphi : \mathcal{A}^+ \rightarrow \mathcal{T}_{\mathbb{R}}$  tale che, se  $g \in \mathcal{A}^+$  (e dunque  $\varphi(g) \in \mathcal{T}_{\mathbb{R}}$ )  $(\varphi(g) \circ F)(x) = (F \circ g)(x)$ .

*Soluzione.* Cominciamo dal punto (A). Si chiede di mostrare che l'insieme  $\mathcal{A}(\mathbb{R})$  è un gruppo rispetto all'operazione di composizione delle applicazioni. Si tratta di verificare quindi che l'operazione di composizione è associativa, che esiste l'identità in  $\mathcal{A}(\mathbb{R})$  rispetto a tale operazione e che per ogni trasformazione in  $\mathcal{A}(\mathbb{R})$  esiste un'inversa.

Denoteremo con  $T_{a,b}$  la trasformazione  $T_{a,b} \in \mathcal{A}(\mathbb{R})$  definita da  $T_{a,b}(x) = ax + b$ . Osserviamo che  $T_{1,0}$  è tale che  $(T_{a,b} \circ T_{1,0})(x) = T_{a,b}(x) = (T_{1,0} \circ T_{a,b})(x)$ ,  $\forall x \in \mathbb{R}$ . Con questa notazione la formula di composizione diventa:  $T_{c,d} \circ T_{a,b} = T_{ac,d+cb}$  (verificate!). Utilizziamo tale formula per verificare l'associatività dell'operazione:

$$(T_{e,f} \circ T_{c,d}) \circ T_{a,b} = T_{ec,f+ed} \circ T_{a,b} = T_{eca,f+ed+ecb} = T_{e,f} \circ T_{ca,d+cb} = T_{e,f} \circ (T_{c,d} \circ T_{a,b})$$

Osserviamo infine che per ogni elemento  $T_{a,b} \in \mathcal{A}(\mathbb{R})$  vi è un inverso:  $T_{a^{-1}, -a^{-1}b}$ .

Nel punto (B) si restringeva l'attenzione a quelle trasformazioni  $T_{a,b} \in \mathcal{A}(\mathbb{R})$  il cui coefficiente moltiplicativo,  $a$ , fosse uguale ad 1. Per brevità denoteremo  $T_y = T_{1,y}$ . Chiamiamo  $\mathcal{T}_{\mathbb{R}}$  il sottoinsieme di queste mappe. Verifichiamo che è un sottogruppo. Dalla legge di composizione osserviamo che esso è chiuso rispetto al prodotto:  $T_y \circ T_z = T_{1,y} \circ T_{1,z} = T_{1,y+z} = T_{y+z}$ ; per ogni elemento  $T_y \in \mathcal{T}_{\mathbb{R}}$  l'inversa  $T_y^{-1} \in \mathcal{A}(\mathbb{R})$  è anch'essa in  $\mathcal{T}_{\mathbb{R}}$ :  $T_y^{-1} = T_{-y}$ . Infine  $\text{id}_{\mathcal{A}(\mathbb{R})} = T_{1,0} = T_0 \in \mathcal{T}_{\mathbb{R}}$ . Questo dimostra che  $\mathcal{T}_{\mathbb{R}}$  è un sottogruppo. Mostriamo che esso è normale. Faremo vedere questo fatto verificando che per ogni  $T_{a,b} \in \mathcal{A}(\mathbb{R})$  risulta  $T_{a,b} \circ \mathcal{T}_{\mathbb{R}} \circ T_{a,b}^{-1} = \mathcal{T}_{\mathbb{R}}$ :

$$T_{a,b} \circ T_y \circ T_{a,b}^{-1} = T_{a,b} \circ T_{1,y} \circ T_{a^{-1}, -a^{-1}b} = T_{a,b} \circ T_{a^{-1}, -a^{-1}b+y} = T_{1,ay} = T_{ay} \in \mathcal{T}_{\mathbb{R}}$$

Consideriamo  $\varphi : (\mathbb{R}, +) \rightarrow (\mathcal{T}_{\mathbb{R}}, \circ)$ ,  $\varphi(x) = T_x$ . Mostriamo che è un isomorfismo. Sappiamo che si tratta, per definizione di una mappa biettiva. Mostriamo che si tratta di un omomorfismo:

$$\varphi(x+y) = T_{x+y} = T_{1,x+y} = T_{1,x} \circ T_{1,y} = T_x \circ T_y = \varphi(x) \circ \varphi(y)$$

Il punto (D) è composto in realtà di due domande: (1) determinare l'insieme  $\mathcal{A}^+$ , (2) verificare che si tratta di un sottogruppo.

Osserviamo che se  $T_{a,b}$  deve mandare  $\mathbb{R}_+$  in  $\mathbb{R}_+$  biettivamente deve risultare  $b = 0$  e  $a > 0$ . Se fosse  $a < 0$  per valori di  $x > |a|^{-1}b$  avremmo infatti  $T_{a,b}(x) < 0$ . Supponiamo ora che  $b \neq 0$  allora  $T_{a,b}(\mathbb{R}_+) = T_{a,b}((0, +\infty)) = (b, +\infty) \neq (0, +\infty) = \mathbb{R}_+$ . Viceversa se  $a > 0$  consideriamo  $T_{a,0}$ ; osserviamo che  $T_{a,0}(x) = ax$  è una mappa biettiva da  $\mathbb{R}_+$  in  $\mathbb{R}_+$  (verificate!).

Per mostrare che si tratta di un sottogruppo osserviamo che  $T_{a,0} \circ T_{a',0} = T_{aa',0}$ , dunque l'insieme  $\mathcal{A}^+$  è chiuso rispetto alla composizione. D'altra parte lo stesso conto ci dice che  $T_{a,0}^{-1} = T_{a^{-1},0}$  e che il sottogruppo  $\mathcal{A}^+$  è abeliano.

Conosciamo un celebre isomorfismo tra il gruppo moltiplicativo dei numeri reali positivi  $(\mathbb{R}_+, \cdot)$  e il gruppo additivo dei reali  $(\mathbb{R}, +)$ : il logaritmo. Sia quindi  $F = \log$  e  $\varphi$  la mappa che invia  $T_{a,0}$  in  $T_{0,\log(a)} = T_{1,\log(a)}$ . Mostriamo che  $\varphi$  è un isomorfismo. Innanzitutto la biettività: osserviamo che dato  $T_y$  esso è immagine tramite  $\varphi$  di  $T_{e^y,0}$ , il che prova la suriettività di  $\varphi$ , mentre l'iniettività segue dall'iniettività del logaritmo come mappa da  $\mathbb{R}_+$  in  $\mathbb{R}$ .

Verifichiamo che si tratta di un omomorfismo:

$$\varphi(T_{a,0} \circ T_{b,0}) = \varphi(T_{ab,0}) = T_{1,\log(ab)} = T_{1,\log(a)+\log(b)} = T_{1,\log(a)} \circ T_{1,\log(b)} = \varphi(T_{a,0}) \circ \varphi(T_{b,0})$$

L'ultima cosa che ci resta da controllare è l'equivarianza di  $\varphi$  rispetto al logaritmo:

$$\varphi(T_{a,0})(\log(x)) = T_{1,\log(a)}(\log(x)) = \log(x) + \log(a) = \log(ax) = \log(T_{a,0}(x))$$

Questo conclude la dimostrazione dell'esercizio.  $\square$

**Esercizio 6.6.** Consideriamo  $\mathbb{N}$ . Consideriamo l'insieme

$$\mathcal{B}_1 = \{f : \mathbb{N} \rightarrow \mathbb{N} \mid f(0) = 0, f \text{ è biettiva e } |f(k) - k| \leq 1\}$$

(A) Sia  $k \geq 2$ . Mostrare che se  $f(k) = k - 1$  allora  $f(k - 1) = k$ .

(B) Siano  $n$  e  $k$  tali che  $f(n) = n$  e  $k \in \mathbb{N}$  è il primo intero positivo per cui  $f(n + k) = n + k$ . Allora  $k - 1 = 2m$  è pari e per ogni  $i = 1, \dots, m$  risulta che  $(f(n + 2i - 1), f(n + 2i)) = (n + 2i, n + 2i - 1)$ .

(C) Dedurre da (B) che ogni elemento di  $\mathcal{B}_1$  è tale che  $f \circ f = \text{Id}_{\mathbb{N}}$ .

(D) Osservare che per ogni  $k \in \mathbb{N}^*$  la trasformazione  $T_k$  definita come  $T_k(m) = m$  se  $m \neq \{2k - 1, 2k\}$  e  $T_k(2k - 1) = 2k$ ,  $T_k(2k) = 2k - 1$  è nell'insieme  $\mathcal{B}_1$ . Verificare che le trasformazioni ottenute come composizione eventualmente numerabile delle applicazioni  $T_k$  è ancora in  $\mathcal{B}_1$ . Dedurre che la cardinalità di  $\mathcal{B}_1$  è  $|\mathbb{R}|$ .

*Soluzione.* Rispondiamo al quesito (A). Consideriamo  $f \in \mathcal{B}_1$ . Supponiamo quindi che  $k \geq 2$  e che  $f(k) = k - 1$ . Vogliamo mostrare che  $f(k - 1) = k$ . Supponiamo per assurdo che  $f(k - 1) = k - 2$ . Mostriamo che allora  $f$  non è biettiva. Utilizzeremo a tal scopo l'induzione dimostrando che se  $f \in \mathcal{B}_1$  e se  $f(k) = k - 1$  e  $f(k - 1) = k - 2$ , allora  $f(k - j) = k - j - 1$  per ogni  $j \in \mathbb{N}$ ,  $j \leq k - 2$ . Per  $j = 0$  osserviamo che dall'ipotesi segue che  $f(k - 2) = k - 3$ , infatti  $f(k - 2) \in \{k - 1, k - 2, k - 3\}$  ma  $f(k) = f(k - 1)$  e  $f(k - 1) = k - 2$  ed  $f$  deve essere iniettiva. Dunque  $f(k - 2) = k - 3$ . Sia quindi  $j \geq 2$  e supponiamo che  $f(k - i) = k - i - 1$  per  $i = 0, \dots, j$  vogliamo far vedere che  $f(k - (j + 1)) = k - (j + 1) - 1$ . Per ipotesi sappiamo che  $f(k - j + 1) = k - j$  e che  $f(k - j) = k - (j + 1)$ . D'altra parte per definizione dell'insieme  $\mathcal{B}_1$  deve risultare  $f(k - (j + 1)) \in \{k - j, k - (j + 1), k - (j + 2)\}$  e dunque deve essere per forza  $f(k - (j + 1)) = k - (j + 2) = k - (j + 1) - 1$ . Abbiamo dunque dimostrato per induzione che se  $f(k) = k - 1$  e  $f(k - 1) = k - 2$  allora  $f(k - j) = k - j - 1$  per ogni  $0 \leq j \leq k$ . Ma  $f : \mathbb{N} \rightarrow \mathbb{N}$ , è biettiva e manda 0 in 0, mentre dal ragionamento precedente dovrebbe risultare  $f(1) = f(k - (k - 1)) = k - k = 0$  e dunque  $f$  non sarebbe iniettiva.

Rispondiamo al punto (B). Siano  $n$  e  $k$  due interi positivi tali che  $f(n) = n$  e  $k$  è il più piccolo intero (strettamente) positivo per cui  $f(n + k) = n + k$ . Vogliamo usare il punto (A) per concludere che:

(1)  $k = 2m + 1$ ;

(2) per ogni  $i = 1, \dots, m$   $f(k + 2i - 1) = k + 2i$ ,  $f(k + 2i) = k + 2i - 1$ .

Dimostreremo (1) e (2) simultaneamente. Consideriamo  $n + k - 1$ ; sappiamo che deve risultare  $f(n + k - 1) \in \{n + k - 2, n + k - 1, n + k\}$ , poiché  $f \in \mathcal{B}_1$ ; d'altra parte essendo  $f \in \mathcal{B}_1$  essa è biettiva e visto che  $f(n + k) = n + k$  possiamo escludere che valga  $f(n + k - 1) = n + k$ ; inoltre per minimalità di  $k$  non può risultare nemmeno  $f(n + k - 1) = n + k - 1$  e dunque obbligatoriamente deve risultare  $f(n + k - 1) = n + k - 2$ . Ci chiediamo quindi dove vada a finire  $n - k - 2$  attraverso l'applicazione  $f$ . Sappiamo che  $f(n + k - 2) \in \{n + k - 3, n + k - 2, n + k - 1\}$ . Per il punto (A) sappiamo che non può essere  $f(n + k - 2) = n + k - 3$ , altrimenti dovrebbe risultare  $f(n) = n - 1$  mentre sappiamo che  $f(n) = n$ ; d'altra parte per minimalità di  $k$  non può risultare  $f(n + k - 2) = n + k - 2$  (a meno che non fosse  $k = 2$  ma in tal caso avremmo  $f(n) = n$  e



$f(n+1) = n$  e questo contraddirebbe la biiettività di  $f$ ). Abbiamo dunque scoperto che deve risultare  $f(n+k-2) = n+k-1$ . Supponiamo quindi di aver scoperto che  $f(n+k-(2i-1)) = n+k-2i$  e  $f(n+k-2i) = n+k-(2i-1)$  per ogni  $1 \leq i \leq j$ ,  $2j < k$ . Mostriamo che  $2(j+1)-1 = k$  oppure  $f(n+k-(2(j+1)-1)) = n+k-2(j+1)$  e  $f(n+k-2(j+1)) = n+k-2(j+1)+1$ . Supponiamo che sia  $2(j+1) < k$  così che  $n \leq n-2(j+1) \leq n-2(j+1)+1 \leq n+k$ . Ricordiamo che per ogni  $i \leq j$  abbiamo dimostrato che risulta  $f(n+k-(2i-1)) = n+k-2i$  e  $f(n+k-2i) = n+k-(2i-1)$ . In particolare quindi risulta che  $f(k-(2j-1)) = k-2j$  ed  $f(k-2j) = k-(2j-1)$ . Osserviamo che in tal caso risulta  $f(n+k-(2(j+1)-1)) = n+k-2j$  infatti  $f(n+k-(2(j+1)-1)) = f(n+k-(2j+1)) \in \{n+k-(2j+2), n+k-(2j+1), n+k-2j\}$  tuttavia per biiettività possiamo escludere  $f(n+k-(2(j+1)-1)) = n+k-2j$ , sappiamo infatti dal passo precedente che  $f(n+k-(2j-1)) = n+k-2j$ , mentre per minimalità di  $k$  possiamo concludere che  $f(n+k-(2(j+1)-1)) \neq n+k-(2(j+1)-1)$ . Dunque  $f(n+k-(2(j+1)-1)) = n+k-2(j+1)$ . Osserviamo ora che per minimalità di  $k$  non possiamo avere  $f(n+k-2(j+1)) = n+k-2(j+1)$  mentre grazie al punto (A) possiamo escludere il caso  $f(n+k-2(j+1)) = n+k-2(j+1)-1$ ; deve quindi risultare  $f(n+k-2(j+1)) = n+k-(2(j+1)-1)$ .

Supponiamo allora che  $2(j+1) \geq k$ ; vogliamo mostrare che  $k = 2j+1$ . Poiché  $2j < k$  possiamo avere  $k = 2(j+1)$  oppure  $k = 2(j+1)-1$ . Per assurdo assumiamo che valga  $k = 2(j+1)$  allora  $n < n+k-(2(j+1)-1) < n+k$ . Dal passo precedente sappiamo che  $f(n+k-(2j-1)) = n+k-2j$ , e dunque  $f(n+k-(2(j+1)-1)) \neq n+k-2j$  mentre per minimalità di  $k$  sappiamo che  $f(n+k-(2(j+1)-1)) \neq n+k-(2(j+1)-1)$ . D'altra parte, essendo  $k = 2(j+1)$  dovrebbe allora risultare  $f(n+k-(2(j+1)-1)) = n+k-2(j+1) = n = f(n)$ , contraddicendo la biiettività di  $f$ . Dunque  $k = 2(j+1)-1 = 2j+1$ .

Questo dimostra che  $k$  è dispari e che  $f$  scambia le coppie di pari e dispari consecutivi strettamente comprese tra  $n$  e  $n+k$ .

Rispondiamo al punto (C). Nel punto (B) abbiamo sostanzialmente visto che possiamo descrivere  $f \in \mathcal{B}_1$  come segue: sia  $S_f \subset \mathbb{N}$  l'insieme su cui  $f$  non è l'identità. Allora

$$S_f = \{n_1+1, n_1+2, \dots, n_1+2k_1\} \cup \{n_2+1, \dots, n_2+2k_2\} \cup \dots \cup \{n_\ell+1, \dots, n_\ell+2k_\ell\} \cup \{n \in \mathbb{N} \mid n \geq n_{\ell+1}+1\}$$
 dove  $\ell \in \mathbb{N}$ ,  $n_i+1 > n_{i-1}+2k_{i-1}+1$  ed  $n_{\ell+1} \in \mathbb{N} \cup \{+\infty\}$  (intendendo quindi che se  $n_{\ell+1} = +\infty$  allora l'ultimo insieme dell'unione precedente è vuoto); inoltre sempre dal punto (B) sappiamo che su ciascun sottoinsieme finito della precedente partizione di  $S_f$  l'applicazione  $f$  agisce come segue:

$$f : \{n_j+1, \dots, n_{j+2k_j}\} \rightarrow \{n_j+1, \dots, n_{j+2k_j}\},$$

$$f(n_j+2i) = n_j+2i-1, \quad f(n_j+2i-1) = n_j+2i, \quad \text{dove } 1 \leq i \leq k_j$$

e analogamente, qualora l'ultimo insieme fosse non vuoto:

$$f : \{n \in \mathbb{N} \mid n \geq n_{\ell+1}+1\} \rightarrow \{n \in \mathbb{N} \mid n \geq n_{\ell+1}+1\}$$

$$f(n_{\ell+1}+2i) = n_{\ell+1}+2i-1, \quad f(n_{\ell+1}+2i-1) = n_{\ell+1}+2i, \quad \text{dove } 1 \leq i \leq +\infty$$

Da tale descrizione di  $f$  è banale osservare che  $f \circ f = \text{Id}_{\mathbb{N}}$ . Infatti fuori su  $\mathbb{N} \setminus S_f$ ,  $f \equiv \text{Id}_{\mathbb{N}}$ , mentre, per la descrizione precedente di come agisce  $f$  su  $S_f$  risulta chiaro che  $(f \circ f)|_{S_f} = \text{Id}_{\mathbb{N}}$  (verificate!).

Rispondiamo ora la punto (D) e chiudiamo così l'esercizio. La verifica che ciascun  $T_k$  è in  $\mathcal{B}_1$  è una banale verifica (che siete tuttavia invitati a fare). Utilizziamo la notazione introdotta nel punto precedente ed osserviamo che ciascuna delle trasformazioni  $T_k$  è tale che  $S_{T_k} = \{2k-1, 2k\}$ . In particolare osserviamo che se  $k \neq k'$  allora  $S_{T_k} \cap S_{T_{k'}} = \emptyset$  da cui segue (verificate!) che  $S_{T_k \circ T_{k'}} = S_{T_k} \cup S_{T_{k'}}$ . L'altra cosa da osservare è che  $T_k \circ T_{k'} = T_{k'} \circ T_k$  qualsiasi siano  $k$  e  $k'$  in  $\mathbb{N}^*$ ; possiamo assumere  $k \neq k'$  dato che dal punto (C) sappiamo che  $T_k \circ T_k = \text{Id}_{\mathbb{N}}$ . Supponiamo quindi  $k \neq k'$ ; se  $n \in \mathbb{N} \setminus (S_{T_k} \cup S_{T_{k'}})$  allora  $(T_k \circ T_{k'})(n) = n = (T_{k'} \circ T_k)(n)$ . Sia ora  $n \in S_{T_{k'}}$  (che, ricordiamo, è disgiunto da  $S_{T_k}$ ), allora  $n = 2k'$  oppure  $n = 2k'-1$ ;  $(T_k \circ T_{k'})(2k') = T_k(2k') = 2k'-1 = (T_{k'} \circ T_k)(2k')$  mentre  $(T_k \circ T_{k'})(2k'-1) = T_k(2k'-1) = 2k' = T_{k'}(2k'-1) = (T_{k'} \circ T_k)(2k'-1)$ . Un ragionamento analogo mostra che la commutatività vale anche per  $n \in S_{T_k}$ .

Consideriamo ora la composizione di trasformazioni  $T_k$  in cui ciascun  $T_k$  può comparire un numero finito di volte, denoteremo  $\mathcal{C}_T$  l'insieme di tali composizioni. Sfruttando l'abelianità e sfruttando il

fatto che per ciascuna trasformazione  $T_k$  vale  $T_k \circ T_k = \text{Id}_{\mathbb{N}}$  è possibile dimostrare che tali composizioni (eventualmente infinite) sono in biezione con le successioni  $\{0, 1\}^{\mathbb{N}}$ , e la biezione  $\{0, 1\}^{\mathbb{N}} \rightarrow \mathcal{C}_T$  è data da  $\{\delta_i\}_{i \in \mathbb{N}} \mapsto \cdots \circ T_i^{\delta_i} \circ T_{i-1}^{\delta_{i-1}} \circ \cdots \circ T_1^{\delta_1}$ .

Poiché  $\mathcal{C}_T \subset \mathcal{B}_1$  (perché?) risulta che  $|\mathcal{B}_1| \geq |\mathcal{C}_T| = |\{0, 1\}^{\mathbb{N}}| = |\mathbb{R}|$ . D'altra parte  $\mathcal{B}_1$  è un sottoinsieme delle applicazioni da  $\mathbb{N}$  in  $\mathbb{N}$  e dunque la sua cardinalità è inferiore alla cardinalità di  $\mathbb{N}^{\mathbb{N}}$ , ovvero  $|\mathbb{R}|$ .  $\square$

**Esercizio 6.7.** Stabilire la compatibilità ed eventualmente risolvere il seguente sistema di equazioni congruenziali lineari:

$$\begin{cases} 24X \equiv 6 \pmod{46} \\ 9X \equiv 42 \pmod{21} \\ 13^{2347}X \equiv 2 \pmod{15} \end{cases}$$

*Soluzione.* Cominciamo dalla prima equazione. Osserviamo innanzitutto che essa è equivalente all'equazione  $12X \equiv 3 \pmod{23}$ ; tale equazione è compatibile, poiché  $\text{MCD}(23, 12) = 1$ ; la seconda equazione del sistema è invece equivalente a  $3X \equiv 14 \pmod{7}$  ed anche in questo caso  $\text{MCD}(3, 7) = 1$  e dunque l'equazione è compatibile. Per quanto riguarda l'ultima equazione osserviamo che  $\text{MCD}(13, 15) = 1$  e dunque  $\overline{13} \in \mathcal{U}(\mathbb{Z}_{15})$ , in particolare tutte le sue potenze sono in  $\mathcal{U}(\mathbb{Z}_{15})$  e dunque  $\text{MCD}(13^{2347}, 15) = 1$ . Osserviamo infine che 7, 23 e 15 sono coprimi e dunque il sistema è compatibile ed equivalente al seguente:

$$\begin{cases} 12X \equiv 3 \pmod{23} \\ 3X \equiv 14 \pmod{7} \\ 13^{2347}X \equiv 2 \pmod{15} \end{cases}$$

Utilizzando il Teorema di Eulero-Fermat possiamo semplificare notevolmente l'ultima equazione congruenziale. Ricordiamo che, come visto nell'Esercizio 6.2,  $\varphi(15) = (5-1) \cdot (3-1) = 8$ . Scriviamo quindi la classe resto modulo 8 di 2347. Osserviamo che  $2320 = 290 \cdot 8$ . Abbiamo quindi che  $2347 \equiv 3 \pmod{8}$ . Utilizziamo quindi l'Esercizio 6.2 e calcoliamo  $13^3$  modulo 15:  $13^3 \equiv 7 \pmod{15}$ . Dunque il sistema precedente è equivalente a:

$$\begin{cases} 12X \equiv 3 \pmod{23} \\ 3X \equiv 0 \pmod{7} \\ 7X \equiv 2 \pmod{15} \end{cases}$$

Tale sistema è equivalente al seguente sistema cinese:

$$\begin{cases} X \equiv 6 \pmod{23} \\ X \equiv 0 \pmod{7} \\ X \equiv 11 \pmod{15} \end{cases}$$

Risolviamo il sistema per sostituzione. La soluzione generica della prima equazione è  $x_Y = 6 + 23Y$ . Andiamo a sostituire tale espressione nella seconda equazione e troviamo:  $2Y \equiv 1 \pmod{7}$ , ovvero  $Y \equiv 4 \pmod{7}$ . La soluzione generica di tale equazione è  $yz = 4 + 7Z$ . Andiamo a sostituire tale quantità in  $x_Y$  e troviamo così  $x_Z = 98 + 161Z$ . Sostituiamo nella terza, otteniamo quindi l'equazione  $8 + 11Z \equiv 11 \pmod{15}$  che è equivalente a  $11Z \equiv 3 \pmod{15}$ . L'inverso moltiplicativo di 11 modulo 15 è 11 stesso e dunque  $Z \equiv 3 \pmod{15}$ . La soluzione generica di tale equazione è dunque  $Z = 3 + 15j$ . Andiamo a sostituire in  $x_Z$  e troviamo la soluzione del sistema:  $x_j = 98 + 483 + 2415j = 581 + 2415j$ .  $\square$

**Esercizio 6.8.** Consideriamo l'anello degli interi modulo 26.

- (A) Determinare  $\mathcal{U}(\mathbb{Z}_{26})$ .
- (B) Stabilire se si tratta di un gruppo ciclico.
- (C) Esibire un sottogruppo ciclico di ordine 4.

*Soluzione.* Cominciamo dal punto (A). Calcoliamoci innanzitutto la cardinalità del sottogruppo moltiplicativo degli invertibili di  $\mathbb{Z}_{26}$ : essa è uguale al numero  $\varphi(26) = \varphi(13 \cdot 2) = (13-1) \cdot (2-1) = 12$ . Sappiamo che per individuare gli elementi di  $\mathcal{U}(\mathbb{Z}_{26})$  è sufficiente trovare tutti i numeri  $k$  compresi tra

0 e 25 tali che  $\text{MCD}(k, 26) = 1$  (gli elementi di  $\mathcal{U}(\mathbb{Z}_{26})$  saranno quindi le classi resto modulo 26 di tali numeri). Quindi:

$$\{k \in \mathbb{N} \mid 0 \leq k < 26, \text{ e } \text{MCD}(k, 26) = 1\} = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

Pertanto  $\mathcal{U}(\mathbb{Z}_{26}) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \bar{11}, \bar{15}, \bar{17}, \bar{19}, \bar{21}, \bar{23}, \bar{25}\}$ .

Per rispondere a (B) è necessario verificare se esista un elemento  $\bar{k} \in \mathcal{U}(\mathbb{Z}_{26})$  tale che  $\langle \bar{k} \rangle = \mathcal{U}(\mathbb{Z}_{26})$ . Osserviamo che  $\bar{7}^2 = \bar{23}$ ,  $\bar{7}^3 = \bar{5}$  e  $\bar{7}^4 = \bar{9}$ ,  $\bar{7}^5 = \bar{11}$ ,  $\bar{7}^6 = \bar{25}$ . Per il Teorema di Lagrange (o per l'Esercizio 6.4, dato che  $\mathcal{U}(\mathbb{Z}_{26})$  è abeliano) sappiamo che  $o(\bar{7}) \mid 12 = |\mathcal{U}(\mathbb{Z}_{26})|$ , d'altra parte sappiamo dal precedente conto che  $o(\bar{7}) > 6$  e dunque deve risultare  $o(\bar{7}) = 12$  e il gruppo in questione è ciclico.

Rispondere a (C) è a questo punto molto semplice. Essendo  $\mathcal{U}(\mathbb{Z}_{26}) = \langle \bar{7} \rangle$  possiamo osservare che il sottogruppo  $\langle \bar{7}^3 \rangle = \langle \bar{5} \rangle$  è un sottogruppo ciclico di ordine 4.  $\square$

**Esercizio 6.9.** Sia  $\mathbb{R}$  la retta reale. Sia  $a \in \mathbb{R}_+$ ,  $a \neq 1$ . Consideriamo la seguente relazione:

$$x \rho y \Leftrightarrow x = a^k \cdot y \text{ per un opportuno } k \in \mathbb{Z}$$

(A) Mostrare che si tratta di una relazione di equivalenza.

(B) Esibire un modello dello spazio quoziente  $\mathbb{R}/\rho$ .

(C) Costruire, a partire da due funzioni  $f_1, f_2 : \mathbb{R} \rightarrow \mathbb{R}$  tali che  $f_i(x + k \log(a)) = f_i(x)$  per ogni  $k \in \mathbb{Z}$ , una funzione  $g : \mathbb{R} \rightarrow \mathbb{R}$  che sia costante sulle classi di equivalenza.

(D) Determinare una applicazione  $\bar{g} : \mathbb{R}/\rho \rightarrow \mathbb{R}$  tale che  $g = \bar{g} \circ \pi$  dove  $\pi : \mathbb{R} \rightarrow \mathbb{R}/\rho$  è la proiezione al quoziente.

*Soluzione.* Mostriamo che  $\rho$  è una relazione di equivalenza. La proprietà riflessiva è banalmente verificata perché  $x = 1 \cdot x = a^0 \cdot x$ . Per quanto riguarda la simmetria osserviamo che se  $y = a^k \cdot x$  allora  $x = a^{-k} \cdot y$  e viceversa; dunque  $x \rho y \Leftrightarrow y \rho x$ . Infine, per verificare la transitività osserviamo che se  $x = a^k y$  ed  $y = a^j z$  allora  $x = a^{k+j} z$ , ovvero  $x \rho y$  e  $y \rho z$  implica  $x \rho z$ .

Andiamo a descrivere le classi di equivalenza. Innanzitutto  $[0]_\rho = \{0\}$ ; sia poi  $x \in \mathbb{R}$ , osserviamo che se  $x < 0$  allora  $x$  non è in relazione  $\rho$  con nessun numero positivo, infatti  $[x]_\rho = \{a^k x\}$  ed abbiamo scelto  $a > 0$ . Simmetricamente se  $x > 0$  allora  $x$  non è in relazione con nessun numero negativo. Supponiamo ora che  $a > 1$ . Allora in  $[1, a)$  non vi sono due elementi identificati da  $\rho$ : infatti se  $x \in [1, a)$  e  $y \in [1, a)$  e  $x = a^k y$  avremmo che  $x \in [a^k, a^{k+1})$ , ma gli insiemi  $\{[a^k, a^{k+1}) \mid k \in \mathbb{Z}\}$  sono una partizione di  $\mathbb{R}_+$ ; in particolare quest'ultima affermazione implica che ogni intero positivo  $x$  cade in un opportuno  $[a^k, a^{k+1})$  pertanto  $a^{-k} x \in [1, a)$  e dunque ogni classe di equivalenza modulo  $\rho$  relativa a numeri reali positivi ammette un unico rappresentante in  $[1, a)$ . In analogia si può far vedere che, sempre nell'ipotesi  $a > 1$  ogni numero reale negativo ammette un unico rappresentante in  $(-a, -1]$ . Dunque per  $a > 1$  lo spazio quoziente (ovvero l'insieme delle classi di equivalenza modulo  $\rho$ ) è in biezione con la seguente unione:  $(-a, -1] \cup \{0\} \cup [1, a)$ .

Nel caso in cui  $a < 1$  si può concludere (sapete provarlo?) che  $\mathbb{R}/\rho$  è in biezione con il seguente sottoinsieme di  $\mathbb{R}$ :  $(-1, -a] \cup \{0\} \cup [a, 1)$ .

Abbiamo quindi risposto al punto (B).

Per quanto riguarda il punto (C) definiamo la seguente funzione  $g(0) = x_0$ ,  $g(x) = f_1(\log(x))$  se  $x > 0$  e  $g(x) = f_2(\log(-x))$  se  $x < 0$ . Si tratta a questo punto di verificare che una funzione così definita è costante sulle classi di equivalenza della relazione  $\rho$ : sia  $x > 0$  e sia  $[x]_\rho$  la sua classe di equivalenza modulo  $\rho$ . Se  $y \in [x]_\rho$  allora  $y = a^k x$  e dunque  $g(y) = g(a^k x) = f_1(\log(a^k x)) = f_1(\log(x) + k \log(a)) = f_1(\log(x)) = g(x)$ . Per  $[0]_\rho = \{0\}$  non vi è nessuna verifica da fare; infine sia  $x < 0$  e sia  $y \in [x]_\rho$ , allora  $y = a^k x$  e dunque  $g(y) = g(a^k x) = f_2(\log(-a^k x)) = f_2(\log(-x) + k \log(a)) = f_2(\log(-x)) = g(x)$ .

Sia  $g$  definita come nel punto (C) allora la restrizione di  $g$  a  $(-a, -1] \cup \{0\} \cup [1, a)$  (se  $a > 1$ ) oppure a  $(-1, -a] \cup \{0\} \cup [a, 1)$  verifica la proprietà richiesta nel punto (D).  $\square$