Tutoraggio di Algebra 2

Anno accademico 2026–2027

Docente del corso: Prof. Andrea Loi
Tutor: Marco Damele

Enunciati e soluzioni commentate

Esercizi 1.2, 1.6, 1.7 e 1.10

Testo di riferimento: Andrea Loi, *Appunti sulla teoria elementare dei gruppi*, capitolo 1, sezione 1.4, pp. 24–26 dell'edizione fornita.

Esercizio 1.2 Un monoide di coppie

Enunciato

Sia $G = \mathbb{Q} \times \mathbb{Z}^*$, dove $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Definiamo su G l'operazione

$$(q, m) \cdot (q', m') = (q + mq', mm').$$

Si provi che $(G, \cdot)$ è un monoide e si calcolino gli elementi invertibili. Si dica se G è un gruppo e se G è abeliano.

Soluzione

Idea della soluzione. Verifichiamo chiusura, associatività ed esistenza del neutro. Poi imponiamo che il prodotto di una coppia con il suo eventuale inverso sia il neutro: la seconda coordinata darà una restrizione decisiva.

1. L'operazione è ben definita su G. Se $q, q' \in \mathbb{Q}$ e $m, m' \in \mathbb{Z}^*$, allora $q + mq' \in \mathbb{Q}$ e $mm' \in \mathbb{Z}^*$. Infatti il prodotto di due interi non nulli è un intero non nullo. Quindi il risultato appartiene ancora a G.

2. L'operazione è associativa. Siano $(q, m), (q', m'), (q'', m'') \in G$. Calcoliamo le due possibili parentesizzazioni:

$$\begin{aligned}((q, m) \cdot (q', m')) \cdot (q'', m'') &= (q + mq', mm') \cdot (q'', m'') \\ &= (q + mq' + mm'q'', mm'm''), \\ (q, m) \cdot ((q', m') \cdot (q'', m'')) &= (q, m) \cdot (q' + m'q'', m'm'') \\ &= (q + m(q' + m'q''), m(m'm'')) \\ &= (q + mq' + mm'q'', mm'm'').\end{aligned}$$

Le coppie ottenute coincidono. Non abbiamo scambiato l'ordine dei fattori: abbiamo soltanto applicato la definizione e le proprietà delle usuali operazioni numeriche.

3. Esiste un elemento neutro. La coppia $e = (0, 1)$ appartiene a G e, per ogni $(q, m) \in G$,

$$(0, 1) \cdot (q, m) = (q, m), \qquad (q, m) \cdot (0, 1) = (q, m).$$

Dunque e è neutro sia a sinistra sia a destra. I tre controlli dimostrano che G è un monoide.

4. Gli elementi invertibili. Supponiamo che (q, m) ammetta un inverso $(r, n) \in G$. Deve valere

$$(q, m) \cdot (r, n) = (0, 1),$$

ossia, uguagliando le coordinate,

$$q + mr = 0, \qquad mn = 1.$$

Poiché m e n sono *interi*, la seconda uguaglianza è possibile soltanto per $m = n = 1$ oppure $m = n = -1$. Inoltre $r = -q/m$.

Viceversa, se $m \in \{1, -1\}$, la coppia $(-q/m, m)$ appartiene a G e verifica entrambe le uguaglianze richieste:

$$\begin{aligned}(q, m) \cdot (-q/m, m) &= (0, 1),\\ (-q/m, m) \cdot (q, m) &= (-q/m + mq, 1) = (0, 1).\end{aligned}$$

Nell'ultimo passaggio usiamo $m^{-1} = m$. Pertanto

$$\boxed{G^\times = \mathbb{Q} \times \{1, -1\}, \qquad (q, m)^{-1} = (-q/m, m) \quad (m = \pm 1).}$$

In particolare $(q, 1)^{-1} = (-q, 1)$ e $(q, -1)^{-1} = (q, -1)$.

5. G non è un gruppo. Per esempio $(0, 2) \in G$ non è invertibile: un suo inverso dovrebbe avere seconda coordinata $1/2$, che non appartiene a $\mathbb{Z}^*$.

6. G non è abeliano. Basta trovare due elementi il cui prodotto dipenda dall'ordine:

$$(0, 2) \cdot (1, 1) = (2, 2), \qquad (1, 1) \cdot (0, 2) = (1, 2).$$

Poiché $(2, 2) \neq (1, 2)$, l'operazione non è commutativa.

Da ricordare. Un inverso deve appartenere all'insieme su cui stiamo lavorando. Il numero $1/m$ esiste in $\mathbb{Q}$, ma la seconda coordinata delle coppie di G deve essere un intero non nullo.

Esercizio 1.6 Il neutro può cambiare restringendo l'insieme

Enunciato

Sia $(M, \cdot, 1)$ un monoide e sia $S \subseteq M$ tale che $(S, \cdot)$ sia un semigruppo e $1 \notin S$. Si può affermare che $(S, \cdot)$ non è un monoide?

Soluzione

Idea della soluzione. Il neutro di M deve agire come identità su tutti gli elementi di M. Un eventuale neutro di S deve farlo soltanto sugli elementi di S: le due richieste sono diverse.

La risposta è **no**. L'assenza del neutro di M non impedisce a S di avere un proprio elemento neutro.

Un controesempio. Prendiamo il monoide $M = (\mathbb{Z}, \cdot, 1)$, con la moltiplicazione usuale, e il sottoinsieme $S = \{0\}$. Allora:

- $1 \notin S$;
- S è chiuso rispetto al prodotto, perché $0 \cdot 0 = 0$;
- il prodotto su S è associativo, essendo la restrizione di un prodotto associativo;
- 0 è neutro *in* S: per ogni $s \in S$, necessariamente $s = 0$, dunque $0 \cdot s = s = s \cdot 0$.

Quindi $(S, \cdot, 0)$ è un monoide. È perfino il gruppo con un solo elemento: il suo neutro è 0 e 0 è il proprio inverso.

Perché non c'è contraddizione con l'unicità del neutro? L'unicità vale per una stessa operazione *su uno stesso insieme*. Qui 0 non è neutro in $\mathbb{Z}$, perché, ad esempio, $0 \cdot 2 = 0 \neq 2$. È neutro soltanto quando restringiamo l'insieme a $\{0\}$.

Un esempio con più di un elemento. Nel monoide $M = \mathbb{Z} \times \mathbb{Z}$ con prodotto componente per componente,

$$(a, b) \cdot (c, d) = (ac, bd),$$

il neutro è $(1, 1)$. Il sottoinsieme $S = \mathbb{Z} \times \{0\}$ è chiuso rispetto al prodotto e ha neutro $(1, 0)$, poiché

$$(1, 0) \cdot (a, 0) = (a, 0) = (a, 0) \cdot (1, 0).$$

Dunque S è un monoide infinito, pur non contenendo il neutro di M.

Da ricordare. Se si richiede che un *sottomonoide* contenga il neutro del monoide ambiente, questi esempi non sono sottomonoidi in quel senso. L'esercizio chiede invece se la struttura $(S, \cdot)$ possa essere un monoide con un proprio neutro: può esserlo.

Esercizio 1.7 Accoppiare un elemento con il suo inverso

Enunciato

Sia G un gruppo finito e sia

$$S = \{x \in G \mid x \neq x^{-1}\}.$$

Dimostrare che:

1. S ha un numero pari di elementi;
2. $|G| \equiv |G \setminus S| \pmod 2$;
3. se $|G|$ è pari, esiste $x \in G \setminus S$ con $x \neq 1$. Quindi un gruppo di ordine pari ha almeno un elemento di ordine 2.

Soluzione

Idea della soluzione. Gli elementi che non coincidono con il proprio inverso si possono suddividere in coppie $\{x, x^{-1}\}$. Gli elementi rimasti sono precisamente quelli che soddisfano $x^2 = 1$.

1. La cardinalità di S è pari.

Ricordiamo che G è un gruppo finito e che

$$S = \{x \in G \mid x \neq x^{-1}\}.$$

L'idea è definire su S una relazione di equivalenza le cui classi contengano esattamente due elementi: un elemento e il suo inverso.

Se $S = \varnothing$, allora $|S| = 0$, che è pari. Supponiamo dunque $S \neq \varnothing$.

Primo passo: S è chiuso rispetto all'inversione. Sia $x \in S$. Per definizione, $x \neq x^{-1}$. Poiché $(x^{-1})^{-1} = x$, abbiamo

$$x^{-1} \neq (x^{-1})^{-1},$$

quindi anche x^{-1} appartiene a S.

Secondo passo: definiamo una relazione di equivalenza. Per $x, y \in S$, poniamo

$$x \sim y \quad \Longleftrightarrow \quad y = x \text{ oppure } y = x^{-1}.$$

Verifichiamo le tre proprietà.

- **Riflessività.** Per ogni $x \in S$ vale $x = x$, quindi $x \sim x$.
- **Simmetria.** Supponiamo $x \sim y$. Se $y = x$, allora anche $x = y$. Se invece $y = x^{-1}$, passando agli inversi otteniamo
  $$y^{-1} = (x^{-1})^{-1} = x.$$
  In entrambi i casi $x = y$ oppure $x = y^{-1}$, dunque $y \sim x$.
- **Transitività.** Supponiamo $x \sim y$ e $y \sim z$. Dalla prima relazione sappiamo che $y = x$ oppure $y = x^{-1}$; dalla seconda sappiamo che $z = y$ oppure $z = y^{-1}$.
  Se $y = x$, allora $z = x$ oppure $z = x^{-1}$. Se invece $y = x^{-1}$, allora $z = x^{-1}$ oppure
  $$z = y^{-1} = (x^{-1})^{-1} = x.$$
  In ogni caso $z = x$ oppure $z = x^{-1}$, quindi $x \sim z$.

Pertanto $\sim$ è una relazione di equivalenza su S.

Terzo passo: determiniamo le classi di equivalenza. Per ogni $x \in S$, la sua classe è

$$[x]_\sim = \{y \in S \mid x \sim y\} = \{x, x^{-1}\}.$$

Entrambi gli elementi appartengono a S, come verificato nel primo passo, e sono distinti per definizione di S. Dunque

$$|[x]_\sim| = 2 \qquad \text{per ogni } x \in S.$$

Quarto passo: contiamo gli elementi di S. Le classi di una relazione di equivalenza formano una partizione dell'insieme su cui la relazione è definita: ogni elemento appartiene a una classe e due classi distinte sono disgiunte.

Consideriamo quindi l'insieme quoziente

$$S/\sim = \{[x]_\sim \mid x \in S\},$$

cioè l'insieme delle classi di equivalenza distinte. Poiché $S \subseteq G$ e G è finito, S è finito; di conseguenza anche $S/\sim$ è finito.

Indichiamo con $r = |S/\sim|$ il numero delle classi e denotiamole con $C_1, \dots, C_r$. Essendo una partizione,

$$S = C_1 \sqcup \cdots \sqcup C_r,$$

dove $\sqcup$ indica un'unione disgiunta. Possiamo quindi sommare le cardinalità delle classi senza contare alcun elemento più di una volta:

$$|S| = \sum_{i=1}^{r} |C_i| = \sum_{i=1}^{r} 2 = 2r.$$

Pertanto $|S|$ è pari. **2. Confronto delle parità.** La decomposizione disgiunta $G = S \sqcup (G \setminus S)$ dà

$$|G| = |S| + |G \setminus S|.$$

Poiché $|S|$ è pari, riducendo modulo 2 otteniamo

$$\boxed{|G| \equiv |G \setminus S| \pmod 2.}$$

3. Esistenza di un elemento di ordine 2. Supponiamo $|G|$ pari. Dal punto precedente anche $|G \setminus S|$ è pari. Inoltre $1 \in G \setminus S$, perché $1^{-1} = 1$: questo insieme è non vuoto e quindi, avendo cardinalità pari, contiene almeno due elementi.

Esiste allora $x \in G \setminus S$ con $x \neq 1$. Per definizione $x = x^{-1}$; moltiplicando per x si ottiene $x^2 = 1$. Poiché $x \neq 1$, la prima potenza positiva che dà il neutro è la seconda: l'ordine di x è esattamente 2.

Da ricordare. In generale $G \setminus S$ contiene il neutro e tutti gli elementi di ordine 2, non soltanto questi ultimi. Se $|G|$ è pari, il numero di elementi di ordine 2 è dispari, perché è $|G \setminus S| - 1$.

Esercizio 1.10 Il problema dei cappelli

Enunciato

Dieci uomini vengono condannati a morte e rinchiusi nella stessa cella la notte precedente all'esecuzione. Viene data loro una possibilità di salvarsi: la mattina verranno messi in fila indiana e sulla testa di ciascuno sarà posto un cappello bianco oppure nero.

Nessuno può vedere il proprio cappello; ciascuno può vedere soltanto i cappelli delle persone davanti a lui. A turno, ognuno può pronunciare soltanto la parola "nero" oppure "bianco". Chi indica il colore del proprio cappello viene graziato; chi sbaglia viene ucciso.

Quale strategia possono concordare la notte prima per essere sicuri che almeno nove siano graziati? Generalizzare a n persone e k colori.

Soluzione

Convenzione sullo svolgimento. Si parla iniziando dalla persona in fondo alla fila, che vede i cappelli di tutte le altre, e si procede verso la persona in testa, che non vede alcun cappello. Tutti sentono le risposte precedenti e non si usano segnali aggiuntivi. Questo è lo svolgimento necessario alla strategia descritta sotto.

Idea della soluzione. La prima risposta comunica una sola informazione collettiva: la parità del numero di cappelli neri visibili. Combinando questa informazione con ciò che vedono e con le risposte già ascoltate, tutte le altre persone ricavano il proprio colore.

1. La strategia per dieci persone e due colori. Etichettiamo le persone $P_1, \dots, P_{10}$ nell'ordine in cui parlano. Quindi P_1 è in fondo alla fila e P_{10} è in testa. Codifichiamo i colori con

$$\text{bianco} = 0, \qquad \text{nero} = 1.$$

Sia $c_i \in \{0, 1\}$ il colore del cappello di P_i.

La prima persona vede $c_2, \dots, c_{10}$ e calcola

$$s \equiv c_2 + \cdots + c_{10} \pmod 2.$$

Dice "bianco" se $s = 0$ e "nero" se $s = 1$. In altre parole, comunica se il numero di cappelli neri davanti a lei è pari o dispari.

La sua risposta non è necessariamente il colore del suo cappello. Può salvarsi oppure no; la strategia garantisce invece la salvezza di tutte le altre nove persone.

La seconda persona sente s e vede $c_3, \dots, c_{10}$. Perciò ricava il proprio colore da

$$\boxed{c_2 \equiv s - (c_3 + \cdots + c_{10}) \pmod 2.}$$

Tra 0 e 1 c'è un solo valore che soddisfa questa congruenza. La seconda persona può quindi dire con certezza il proprio colore.

La terza persona conosce s, sente la risposta corretta c_2 e vede $c_4, \dots, c_{10}$. Calcola allora

$$c_3 \equiv s - c_2 - (c_4 + \cdots + c_{10}) \pmod 2.$$

Lo stesso procedimento continua lungo tutta la fila.

2. Perché ogni persona successiva alla prima risponde correttamente. Quando tocca a P_i, con $2 \leq i \leq 10$, supponiamo che le persone $P_2, \ldots, P_{i-1}$ abbiano risposto correttamente. La persona P_i conosce allora i colori $c_2, \ldots, c_{i-1}$ dalle risposte e i colori $c_{i+1}, \ldots, c_{10}$ perché li vede.

L'unico termine ignoto nella somma comunicata da P_1 è c_i. Dunque

$$\boxed{c_i \equiv s - \sum_{j=2}^{i-1} c_j - \sum_{j=i+1}^{10} c_j \pmod 2.} \tag{1}$$

Per $i = 2$ la prima somma è vuota e vale 0, e abbiamo già verificato che la risposta è corretta. La formula prova il passo successivo: per induzione, tutti da P_2 a P_{10} rispondono correttamente. Per P_{10} è la seconda somma a essere vuota.

3. Un esempio concreto. Supponiamo che i cappelli di $P_2, \ldots, P_{10}$ siano, nell'ordine,

$$(1, 0, 1, 1, 0, 0, 1, 0, 1).$$

Ci sono cinque cappelli neri, quindi P_1 comunica $s = 1$ dicendo "nero". Il colore c_1 non influisce su questa comunicazione.

Persona	Informazioni disponibili	Calcolo modulo 2	Risposta
P_2	Vede quattro neri	$1 - 4 \equiv 1$	nero
P_3	Ha sentito $c_2 = 1$; vede quattro neri	$1 - 1 - 4 \equiv 0$	bianco
P_4	Ha sentito $1, 0$; vede tre neri	$1 - 1 - 0 - 3 \equiv 1$	nero

Gli altri proseguono nello stesso modo. Alla fine P_{10} ha ascoltato i colori corretti di $P_2, \ldots, P_9$: tra loro ci sono quattro neri, quindi calcola $c_{10} \equiv 1 - 4 \equiv 1 \pmod 2$ e dice "nero".

Generalizzazione a n persone e k colori

Siano $n \geq 1$ e $k \geq 2$. Associamo in anticipo ai k colori le classi

$$0, 1, \ldots, k-1 \quad \text{in } \mathbb{Z}_k.$$

La corrispondenza è nota a tutti. Scriviamo $c_i \in \mathbb{Z}_k$ per il colore della persona P_i, sempre numerando nell'ordine in cui si parla.

La prima risposta. La persona P_1 vede $c_2, \ldots, c_n$ e calcola

$$s = c_2 + \cdots + c_n \quad \text{in } \mathbb{Z}_k.$$

Pronuncia il nome del colore corrispondente a s. Così, pur dicendo soltanto un nome di colore, comunica a tutti la somma modulo k dei cappelli davanti a lei.

Le risposte successive. Per $i = 2, \ldots, n$, la persona P_i pronuncia il colore corrispondente a

$$\boxed{c_i = s - \sum_{j=2}^{i-1} c_j - \sum_{j=i+1}^{n} c_j \quad \text{in } \mathbb{Z}_k.}$$

La prima somma è nota dalle risposte precedenti, la seconda dai cappelli visibili. Come nel caso di due colori, un'induzione su i dimostra che ciascuna di queste risposte è corretta. Pertanto la strategia garantisce

$$\boxed{\text{almeno } n-1 \text{ persone salve, per qualunque assegnazione dei cappelli.}}$$

Esempio con tre colori. Codifichiamo bianco $= 0$, nero $= 1$, rosso $= 2$. Con quattro persone, supponiamo $(c_2, c_3, c_4) = (2, 1, 2)$. La prima comunica

$$s \equiv 2 + 1 + 2 \equiv 2 \pmod 3$$

dicendo "rosso". La seconda vede $1, 2$ e calcola $c_2 \equiv 2 - 1 - 2 \equiv 2$, quindi dice "rosso". La terza ha sentito $c_2 = 2$, vede $c_4 = 2$ e calcola $c_3 \equiv 2 - 2 - 2 \equiv 1$, quindi dice "nero". Infine la quarta calcola $c_4 \equiv 2 - 2 - 1 \equiv 2$, quindi dice "rosso".

Perché non si possono garantire n salvezze? Fissiamo i cappelli di $P_2, \ldots, P_n$ e consideriamo due configurazioni che differiscono soltanto per il colore del cappello di P_1. Prima di rispondere, P_1 vede esattamente la stessa situazione nei due casi e non ha ancora ascoltato alcuna risposta. Quindi una strategia concordata gli fa pronunciare lo stesso colore in entrambi i casi. Non può avere ragione in entrambi.

Di conseguenza, se ci sono almeno due colori, nessuna strategia può assicurare che tutti siano salvi in ogni configurazione. La garanzia di $n - 1$ salvezze è quindi ottimale. Se $n = 1$ garantisce zero salvezze; se invece $k = 1$, il problema è immediato e si salvano tutti.

Da ricordare. Si usa soltanto la struttura di *gruppo additivo* di $\mathbb{Z}_k$: si possono sommare e sottrarre le classi. Non occorre dividere, quindi k non deve essere primo. Inoltre la prima risposta va interpretata come informazione sulla somma, non come il valore di c_1: per questo c_1 non compare nelle formule.