

TRENTO, A.A. 2022/23
CORSO DI ALGEBRA B
FOGLIO DI ESERCIZI # 2

Esercizio 2.1. Sia $n \geq 3$. Con le notazioni dell'esercizio 1.8, si consideri l'insieme

$$D_n = \{ f_{\varepsilon,b} : \varepsilon \in \{1, -1\}, b \in \mathbf{Z}/n\mathbf{Z} \}.$$

- (1) Si mostri che D_n è un gruppo rispetto alla composizione, detto il *gruppo diedrale*.
- (2) Si mostri che $f_{1,1}^k = f_{1,k}$.
- (3) Si mostri che l'elemento $f_{1,1}$ ha periodo n , e dunque

$$\langle f_{1,1} \rangle$$

è un gruppo di ordine n , e che i suoi elementi sono

$$1, f_{1,1}, f_{1,2}, \dots, f_{1,n-1}.$$

- (4) Si trovi il periodo di ogni $f_{1,b} = f_{1,1}^b$, per $b \in \mathbf{Z}/n\mathbf{Z}$.
(SUGGERIMENTO: Questo è svolto nel prossimo Esercizio 2.2.)
- (5) Si mostri che ogni elemento $f_{-1,b}$, per $b \in \mathbf{Z}/n\mathbf{Z}$, ha periodo 2.
- (6) Si mostri che

$$f_{-1,0} \circ f_{-1,1} = f_{1,1}$$

(con la composizione fatta da sinistra a destra), dunque il prodotto di due elementi di periodo 2 può avere periodo n arbitrario.

- (7) Si mostri che

$$f_{-1,1} \circ f_{-1,0} = f_{1,-1}.$$

Esercizio 2.2 (Forse l'ho già fatto ad Algebra A).

Sia G un gruppo, e $a \in G$ un elemento di periodo finito n .

Sia $k \in \mathbf{Z}$. Allora il periodo della potenza a^k è

$$\frac{n}{\gcd(n, k)}.$$

(SUGGERIMENTO: Anzi, svolgimento. Il periodo di a^k è il più piccolo intero positivo t tale che $(a^k)^t = 1$. Ora sappiamo da Algebra A che $a^{tk} = (a^k)^t = 1$ se e solo se $n \mid tk$, e per il Lemma Aritmetico 3, questo implica $\frac{n}{\gcd(n, k)} \mid t$, dunque

il periodo di a^k è un multiplo di $\frac{n}{\gcd(n, k)}$. D'altra parte

$$(1) \quad (a^k)^{n/\gcd(n, k)} = (a^n)^{k/\gcd(n, k)} = 1$$

perché n è il periodo di a . Notate che $\frac{k}{\gcd(n, k)}$ è un intero. Un altro modo di vedere questo fatto è che l'esponente di a in (1) è

$$\frac{nk}{\gcd(n, k)},$$

che sappiamo essere il minimo comune multiplo di n e k , dunque in particolare un multiplo di n , per cui la potenza è 1. (Riguardatevi quello che abbiamo detto sul periodo in Algebra A in caso.)

Esercizio 2.3 (Facoltativo, ma utile). Consideriamo $\Omega = \mathbf{Z}$. Per $a \in \{1, -1\}$, e $b \in \mathbf{Z}$, consideriamo la funzione

$$f_{a,b} : \mathbf{Z} \rightarrow \mathbf{Z} \\ x \mapsto ax + b.$$

Si consideri l'insieme

$$D_\infty = \{ f_{\varepsilon,b} : \varepsilon \in \{1, -1\}, b \in \mathbf{Z} \}.$$

- (1) Si mostri che D_∞ è un gruppo rispetto alla composizione, detto il *gruppo diedrale infinito*.
- (2) Si mostri che $f_{1,1}^k = f_{1,k}$.
- (3) Si mostri che l'elemento $f_{1,1}$ ha periodo infinito (cioè le sue potenze sono tutte distinte).
- (4) Si mostri che ogni elemento $f_{-1,b}$, per $b \in \mathbf{Z}$, ha periodo 2.
- (5) Si mostri che

$$f_{-1,0} \circ f_{-1,1} = f_{1,1}$$

(con la composizione fatta da sinistra a destra), dunque il prodotto di due elementi di periodo 2 può avere anche periodo infinito.

Esercizio 2.4 (Diciamo facoltativo, ma almeno leggetelo per favore).

Vediamo alcuni casi particolari dell'Esercizio 2.1, in cui vogliamo scrivere gli elementi, che sono permutazioni dell'insieme

$$\Omega = \mathbf{Z}/n\mathbf{Z} = \{0, 1, \dots, n-1\},$$

come prodotti di cicli disgiunti.

- (1) Le rotazioni nel caso generale. Per n qualsiasi si vede che $f_{1,1}$ si scrive come $(0, 1, 2, \dots, n-1)$. È un pochino più complicato vedere come si scrivono le potenze $f_{1,1}^k = f_{1,k}$. Comunque l'Esercizio 2.2 ci dice che $f_{1,k}$ ha ordine $\frac{n}{\gcd(n,k)}$, e si può vedere che $f_{1,k}$ si scrive come prodotto di un numero $\gcd(n,k)$ di cicli lunghi $\frac{n}{\gcd(n,k)}$.
- (2) Esempi del punto precedente.
 - (a) Per $n = 3$ si ha $f_{1,1} = (0, 1, 2)$, $f_{1,1}^2 = (0, 2, 1)$, e infine $f_{1,1}^3 = (0)(1)(2)$ è la funzione identica.
 - (b) Per $n = 4$ si ha $f_{1,1} = (0, 1, 2, 3)$, $f_{1,1}^2 = (02)(13)$, $f_{1,1}^3 = (0, 3, 2, 1)$ e infine $f_{1,1}^4 = (0)(1)(2)(3)$ è la funzione identica.
 - (c) Provate a fare i casi $n = 5$ e $n = 6$.
- (3) Le riflessioni $f_{-1,k}$ sono un tantino più complicate. Sappiamo che hanno periodo 2, dunque per il punto (2) dell'Esercizio 1.7. come scrittura in cicli disgiunti dovranno essere prodotti di 1-cicli (che corrispondono a *punti fissi*) e 2-cicli (anche detti trasposizioni).

Contiamo quindi quanti punti fissi ha una rotazione $f_{-1,k}$. Sia $x = xf_{-1,k} = -x + k$. Ricordiamoci che stiamo calcolando in $\mathbf{Z}/n\mathbf{Z}$, dunque questo equivale a $2x \equiv k \pmod{n}$, ovvero $2x + ny = k$ per qualche $x, y \in \mathbf{Z}$. Sappiamo da Algebra A che questa equazione è risolubile se e solo se $\gcd(2, n) \mid k$. Distinguiamo due casi.

- (a) n è dispari. Allora $\gcd(2, n) = 1$, dunque ogni $f_{-1,k}$ ha un punto fisso, e vi lascio da vedere che ne ha uno solo. Due esempi.
- (i) Per $n = 3$ si ha $f_{-1,0} = (12)$, $f_{-1,1} = (01)$, $f_{-1,2} = (02)$.
- (ii) Per $n = 5$ si ha $f_{-1,0} = (1234)$, provate a finite voi.
- (b) n è pari. Allora $\gcd(2, n) = 2$, e dunque ci sono punti fissi (e si può vedere che ce ne sono due) se e solo se k è pari. Vediamo il caso $n = 4$, vi lascio da fare il caso $n = 6$. Per $n = 4$ si ha $f_{-1,0} = (13)$, $f_{-1,1} = (01)(23)$, $f_{-1,2} = (02)$, $f_{-1,3} = (03)(12)$.

Esercizio 2.5. Sia G un gruppo, $H \leq G$. Si mostri che la relazione su G data per $a, b \in G$ da

$$aSb \quad \text{se e solo se} \quad a^{-1}b \in H$$

è una relazione di equivalenza, e che la classe di $a \in G$ è

$$[a] = aH = \{ah : h \in H\}.$$

Esercizio 2.6 (Facoltativo). Sia G un gruppo, $\emptyset \neq X \subseteq G$.

Si mostri che se la relazione su G data per $a, b \in G$ da

$$aSb \quad \text{se e solo se} \quad a^{-1}b \in X$$

è una relazione di equivalenza, allora X è un sottogruppo di G .

Esercizio 2.7. Sia G un gruppo, $H \leq G$. Si mostri che la relazione su G data per $a, b \in G$ da

$$aDb \quad \text{se e solo se} \quad ab^{-1} \in H$$

è una relazione di equivalenza, e che la classe di $a \in G$ è

$$[a] = Ha = \{ha : h \in H\}.$$

Esercizio 2.8. Si enunci e si dimostri il Teorema di Lagrange, nelle due forme

- (1) Sia G un gruppo finito, H un sottogruppo di G . Sia d il numero di classi laterali destre di H in G . Allora

$$|G| = |H| \cdot d.$$

- (2) Sia G un gruppo finito, H un sottogruppo di G . Sia s il numero di classi laterali sinistre di H in G . Allora

$$|G| = |H| \cdot s.$$

Se ne deduca che $s = |G|/|H| = d$. Questo numero viene indicato $|G : H|$, e chiamato l'*indice di H in G* .

Esercizio 2.9. Si mostri che un gruppo G di ordine primo è ciclico, nel senso che per ogni $a \in G \setminus \{1\}$ si ha $G = \langle a \rangle$.

Esercizio 2.10. Sia G un gruppo finito, $a \in G$. Si mostri che il periodo di a divide l'ordine di G .

(SUGGERIMENTO: Sappiamo che l'insieme $\langle a \rangle = \{a^n : n \in \mathbf{Z}\}$ delle potenze di a è un sottogruppo di G , che ha per ordine proprio l'ordine (o periodo) di a . Ora si usi il Teorema di Lagrange.)

Esercizio 2.11.

- (1) Si elenchino gli elementi di D_3 e D_4 .
- (2) Si elenchino i sottogruppi di D_3 .
- (3) Si elenchino i sottogruppi di ordine 2 di D_4 .

Facoltativo Si elenchino (alcuni de)i sottogruppi di ordine 4 di D_4 .

Esercizio 2.12.

- (1) Si dia la definizione di sottogruppo normale.
- (2) Si mostri che il sottogruppo $\langle (12) \rangle$ di D_3 non è normale in D_3 , mentre $\langle (123) \rangle$ lo è.

Esercizio 2.13. Sia G un gruppo, $H \leq G$, $a \in G$.

Si mostri che sono equivalenti:

- (1) $a \in H$,
- (2) $aH = H$,
- (3) $Ha = H$.

(SUGGERIMENTO: Ricordiamo che aH è la classe di equivalenza $[a]$ di a rispetto alla relazione di equivalenza S data da aSb se e solo se $a^{-1}b \in H$. Ora $[1] = 1H = H$. Dunque $a \in H = [1]$ se e solo se $aH = [a] = [1] = H$.)

Esercizio 2.14 (Facoltativo). Sia G un gruppo, $H \leq G$. Mostrate che esiste una biiezione fra l'insieme delle classi laterali sinistre e l'insieme di quelle destre di H in G , data da

$$aH \mapsto Ha^{-1}.$$

(SUGGERIMENTO: Sia $\mathfrak{D} = \{Hb : b \in G\}$ l'insieme delle classi laterali destre di H in G . Si consideri la funzione $G \rightarrow \mathfrak{D}$ data da $x \mapsto Hx^{-1}$. Si applichi il primo teorema di isomorfismo per insiemi, mostrando che la relazione di equivalenza su G indotta da questa funzione è proprio la S del foglio precedente.)