ESERCIZI TUTORATO ALGEBRA 2
18 OTTOBRE 2019 - LEZIONE 2
SOLUZIONI

MARCO ABBADINI

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

Prima di passare agli esercizi, ricordo il seguente fatto, che può essere utile per elencare gli elementi dei gruppi ciclici. Tale fatto risponde alla domanda: quali sono gli elementi di un gruppo ciclico?

Fatto. Sia G un gruppo ciclico, e sia $g \in G$ un suo generatore.

(a) Nel caso in cui il periodo di g è finito (cioè esiste un intero positivo k tale che $g^k = 1$), denotando con n tale periodo (= il più piccolo intero positivo k tale che $g^k = 1$), gli elementi di G sono precisamente $1, g, g^2, \dots, g^{n-2}, g^{n-1}$ e questi sono a due a due distinti.

(b) Nel caso in cui il periodo di g non è finito, allora gli elementi di G sono precisamente

$$\dots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^1, g^2, g^3 \dots,$$

e questi sono a due a due distinti.

In particolare, G è finito se e solo se il periodo di g lo è, e in tal caso l'ordine di G e il periodo di g coincidono.

Esercizio 1. Sia G un gruppo, generato da un elemento g il cui ordine è 12.

(a) Determinare, per ogni $h \in G = \{1, g, g^2, \dots, g^{10}, g^{11}\}$, il sottogruppo generato da h.

(b) Determinare il sottogruppo di G generato da $\{g^4, g^6\}$.

Soluzione. Si ricorda il seguente

Teorema (Identità di Bezout)**.** Dati $a, b, d \in \mathbb{Z}$, si ha

$$[\exists x \in \mathbb{Z}\ \exists y \in \mathbb{Z} : ax + by = d] \iff [\text{MCD}(a, b) \text{ divide } d.]$$

Si ricorda inoltre la versione analoga per $\mathbb{Z}/n\mathbb{Z}$.

Teorema (Identità di Bezout, versione modulo n)**.** Dati un intero positivo n, e dati $a, b \in \mathbb{Z}_n$, si ha

$$[\exists x \in \mathbb{Z} : ax \equiv_n b] \iff [\text{MCD}(a, n) \text{ divide } b.]$$

L'identità di Bezout ha un analogo per un qualsiasi numero (finito o infinito) di variabili.

Teorema (Identità di Bezout, versione generale)**.** Data una famiglia $\{a_i\}_{i \in I}$ di elementi di $\mathbb{Z}$, e dato $b \in \mathbb{Z}$, si ha

$$[\exists k \in \mathbb{N}_{\geq 0}\ \exists i_1, \dots, i_k \in I\ \exists x_1, \dots, x_n \in \mathbb{Z} : a_1 x_1 + \dots + a_n x_n = b] \iff [\text{MCD}(\{a_i \mid i \in I\}) \text{ divide } b.]$$

L'ultimo teorema si può anche esprimere così:

Teorema. Dato $S \subseteq \mathbb{Z}$, il sottogruppo di $\mathbb{Z}$ generato da S è $k\mathbb{Z}$, con $k := \text{MCD}(S)$.

Ultimo aggiornamento: 28 ottobre 2019. Non esitate a segnalare eventuali errori a marco.abbadini@unimi.it.

Quest'ultimo teorema ci sta dicendo che ogni sottogruppo H di $\mathbb{Z}$ è ciclico, e ci dice, a partire da un qualsiasi insieme di generatori di H, qual è un singolo generatore per tutto H. (Ricordando che sottogruppi e ideali di $\mathbb{Z}$ coincidono, il teorema precedente ci dice che $\mathbb{Z}$ è PID, e "come".)

Abbiamo anche la versione "modulo n":

Teorema. Dato n un intero positivo, e dato $S \subseteq \mathbb{Z}$, il sottogruppo di $\mathbb{Z}_n$ generato da $\{[x]_n : x \in S\}$ è costituito dai multipli di $[\mathrm{MCD}(S \cup \{n\})]_n$.

Usando quest'ultimo teorema, otteniamo quanto segue.

(a) $\langle 1\rangle = \{1\}$.
$\langle g\rangle = G$.
$\langle g^2\rangle = \{1, g^2, g^4, g^6, g^8, g^{10}\}$.
$\langle g^3\rangle = \{1, g^3, g^6, g^9\}$.
$\langle g^4\rangle = \{1, g^4, g^8\}$.
$\langle g^5\rangle = G$.
$\langle g^6\rangle = \{1, g^6\}$.
$\langle g^7\rangle = G$.
$\langle g^8\rangle = \{1, g^4, g^8\}$.
$\langle g^9\rangle = \{1, g^3, g^6, g^9\}$.
$\langle g^{10}\rangle = \{1, g^2, g^4, g^6, g^8, g^{10}\}$.
$\langle g^{11}\rangle = G$.

(b) $\langle g^2, g^4\rangle = \{1, g^2, g^4, g^6, g^8, g^{10}\}$.

Esercizio 2. (a) Sia $\sigma := (1\ 2) \in S_4$. Trovare $\tau \in S_4$ tale che $\tau^{-1}\sigma\tau = (3\ 4)$.
(b) Sia $\alpha := (1\ 2)(3\ 4\ 5) \in S_5$. Trovare $\beta \in S_5$ tale che $\beta^{-1}\alpha\beta = (1\ 4)(3\ 5\ 2)$.
(c) Sia $\gamma := (1\ 2) \in S_3$. Esiste $\delta \in S_3$ tale che $\delta^{-1}\gamma\delta = (1\ 2\ 3)$?

Soluzione. (a) Si consideri

$$\begin{aligned} \tau\colon \{1,2,3,4\} &\longrightarrow \{1,2,3,4\} \\ 1 &\longmapsto 3 \\ 2 &\longmapsto 4 \\ 3 &\longmapsto 1 \\ 4 &\longmapsto 2. \end{aligned}$$

Questa scelta funziona. Non era l'unica. L'importante è che

- 3 venga mandato in 1 e 4 in 2, oppure
- 3 in 2 e 4 in 1

(è condizione necessaria e sufficiente).

(b) Si scrivano α e β uno sotto l'altro in modo tale che le sequenze di lunghezze dei cicli siano uguali, e si prenda la mappa che manda ogni elemento che compare in α nel corrispettivo sottostante elemento che compare in β. Cioè

$(1\ 2)(3\ 4\ 5)$
$\downarrow\downarrow\ \downarrow\downarrow\downarrow$
$(1\ 4)(3\ 5\ 2)$

ovvero

$1 \mapsto 1,\ 2 \mapsto 4,\ 3 \mapsto 3,\ 4 \mapsto 5,\ 5 \mapsto 2.$

(c) No, perchè (1 2) e (1 2 3) non hanno la stessa struttura ciclica.

Esercizio 3 (Prova scritta, 14 Settembre 2017, eserc. 1)**.** Sia $G = S_6$ il gruppo simmetrico su 6 oggetti.

(a) Quante sono le classi di coniugio di elementi di ordine 6 in G?

(b) Quante sono le classi di coniugio di elementi di ordine 12 in G?

(c) È vero che ogni elemento di ordine 3 di G è il quadrato di un elemento di ordine 6?

Soluzione. Si ricorda che due elementi sono coniugati se e solo se hanno la stessa struttura ciclica (a.k.a. tipo), e che l'ordine di un elemento di tipo $(n_1, \dots, n_k)$ è $\mathrm{mcm}(n_1, \dots, n_k)$.

(a) 2: $[(1\ 2\ 3\ 4\ 5\ 6)]$ e $[(1\ 2\ 3)(4\ 5)]$.

(b) 0.

(c) Sì. Gli elementi di ordine 3 sono trecicli e doppi trecicli. Un doppio treciclo è il quadrato di un seiciclo, mentre un treciclo è il quadrato di un elemento che si scrive come prodotto di un treciclo e uno scambio disgiunti.

Esercizio 4. [1] Sia H l'insieme dei numeri razionali rappresentabili con frazioni della forma $\frac{m}{7^\epsilon}$, con $\epsilon \in \{0, 1\}$.

(a) Si provi che H è un sottogruppo di $(\mathbb{Q}, +)$ contenente $\mathbb{Z}$.

(b) Si provi che $\mathbb{Z}$ è un sottogruppo normale di H.

(c) Si determini $[H : \mathbb{Z}]$, mostrando esplicitamente un insieme di rappresentanti per i laterali di $\mathbb{Z}$ in H.

(d) Si stabilisca se il gruppo quoziente $H/\mathbb{Z}$ è ciclico.

Soluzione. (a) Lo si provi.

(b) H è abeliano perché sottogruppo di $\mathbb{Q}$ abeliano. Ogni sottogruppo di un abeliano è normale.

(c) Insieme di rappresentanti: $\{\frac{i}{7} \mid i \in \{0, \dots, 6\}\}$. $[H : \mathbb{Z}] = 7$.

(d) Sì. H è ciclico (generato da $\frac{1}{7}$), perciò ogni suo quoziente è ciclico.

1. Cosa ricordare

- Dato un gruppo ciclico G, ogni suo sottogruppo è ciclico. Dato $S \subseteq G$, un generatore di $\langle S \rangle$ si trova facendo un'opportuno MCD. (Esercizio 1)
- Due elementi di S_n sono coniugati se e solo se hanno lo stesso tipo (=struttura ciclica). (Esercizi 2 e 3.)
- Il periodo (anche detto ordine) di un elemento di S_n di tipo $(m_1, \dots, m_k)$ è $\mathrm{mcm}(m_1, \dots, m_k)$. (Esercizio 3.)
- Ogni sottogruppo di un gruppo abeliano è normale. (Esercizio 4.)
- Un quoziente di un gruppo ciclico è ciclico. (Esercizio 4.)

[1] L'esercizio 4, nella forma presente, coincide con l'esercizio 2 della prova scritta del 22 Novembre 2018, ad eccezione dei punti (b) e (d), che sono stati introdotti per questa esercitazione.