ALGEBRA

PRIMO ESONERO CANALE A-L
18 NOVEMBRE 2011

C. MALVENUTO

Esercizio 1. (8 punti) Sia $\mathcal{H}$ la famiglia di tutti i sottogruppi del gruppo additivo $\mathbb{Z}_{20}$ delle classi resto modulo 20.

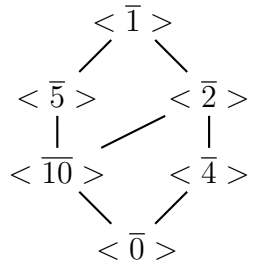
1. Elencare tutti gli elementi di $\mathcal{H}$. Determinare almeno un generatore per ogni sottogruppo $S \in \mathcal{H}$.
2. Disegnare il diagramma di Hasse dell'ordine parziale $(\mathcal{H}, \leq)$ dove per ogni $S, T \in \mathcal{H}$ si definisce:

$$S \leq T \Leftrightarrow \text{S è sottogruppo di } T.$$

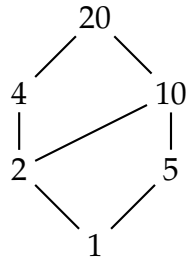
Soluzione Il gruppo additivo $\mathbb{Z}_{20}$ delle classi resto modulo 20 è ciclico e finito, generato da $\overline{1}$: pertanto in esso tutti i sottogruppi sono ciclici, ed esiste uno e un solo sottogruppo per ogni divisore d di 20, generato dalla classe $\overline{20/d}$. I divisori di 20 sono $\{1, 2, 4, 5, 10, 20\}$; per ognuno di essi il sottogruppo corrispondente è generato, nell'ordine, da $\overline{20}(= \overline{0}), \overline{10}, \overline{5}, \overline{4}, \overline{1}$.

Divisore d di 20	**Generatore**	**Sottogruppo** di ordine d
1	$\overline{20} = \overline{0}$	$< \overline{0} >= \{\overline{0}\}$
2	$\overline{10}$	$< \overline{10} >= \{\overline{0}, \overline{10}\}$
4	$\overline{5}$	$< \overline{5} >= \{\overline{0}, \overline{5}, \overline{10}, \overline{15}\}$
5	$\overline{4}$	$< \overline{4} >= \{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}\}$
10	$\overline{2}$	$< \overline{2} >= \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}\}$
20	$\overline{1}$	$< \overline{1} >= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \ldots, \overline{17}, \overline{18}, \overline{19}\}$

Dunque il diagramma di Hasse dei sottogruppi di $\mathbb{Z}_{20}$, ordinati rispetto alla relazione d'ordine $H \leq K$ se e solo se H è sottogruppo di K è



Si osservi che, per il teorema sulla struttura dei sottogruppi dei gruppi ciclici finiti, esso è lo stesso che il diagramma di Hasse dei divisori di 20, ordinati rispetto alla relazione d'ordine della divisibilità è:



Esercizio 2. (6 punti) Dati i numeri $m = 375$ ed $n = 123$:

1. trovare (m, n) il massimo comune divisore tra m ed n mediante l'algoritmo di Euclide;
2. Scrivere un'identità di Bézout per (m, n);
3. dire se l'equazione diofantea $375x + 123y = 6$ ammette o no soluzioni intere $x_0, y_0 \in \mathbb{Z}$: in caso negativo motivare perché non ne ha, in caso affermativo trovarle.

Soluzione Eseguiamo le divisioni euclidee successive:

- $375 = 123 \cdot 3 + 6$
- $123 = 6 \cdot 20 + 3$
- $6 = 3 \cdot 2 + 0$

Il massimo comune divisore è l'ultimo resto non nullo, quindi $(m, n) = 3$. Ricaviamo ora dalle relazioni del tipo $a = bq + r$ (tranne l'ultima) i resti non nulli $r = a - bq$:

- $6 = 375 + 123(-3)$
- $3 = 123 + 6(-20)$

Sostituendo a ritroso si ricava:

$$\begin{aligned} 3 &= 123 + 6(-20) \\ &= 123 + [375 + 123(-3)](-20) \\ &= 375(-20) + 123(61) \end{aligned}$$

L'equazione diofantea $mx+ny = c$ ammette soluzioni se e solo se il massimo comune divisore tra m ed n divide il termine noto c, come in questo caso.

Moltiplicando ambo i membri dell'identità di Bézout $375(-20)+123(61) = 3$ per $c/(m,n) = 6/3 = 2$, si ottiene

$$2 \cdot [375(-20) + 123(61)] = 2 \cdot 3,$$

ovvero

$$375(-40) + 123(122) = 6,$$

da cui si ricava la soluzione $(x_0, y_0) = (-40, 122)$

Esercizio 3. (2 punti) Determinare le soluzioni dell'equazione congruenziale

$$4x \equiv 3 \pmod{385}.$$

Scrivere l'insieme delle soluzioni come elemento di $\mathbb{Z}_{385}$ (anello delle classi resto modulo 385), scegliendo opportunamente il rappresentante tra 0 e 384, ed eseguire la verifica.

Soluzione Detta equazione ha soluzioni se e solo se 4 e 285 sono coprimi, come in questo caso (2 è il solo fattore di 4, ed evidentemente non divide 285 che è dispari). Il massimo comune divisore si ricava subito tramite l'algoritmo euclideo con un'unica divisione: $385 = 4 \cdot 96 + 1$, da cui si ricava immediatamente un' identità di Bézout per $1 = (385, 4)$ come $1 = 385(1) + 4(-96)$: quando essa venga letta nell'insieme quoziente $\mathbb{Z}/385\mathbb{Z}$, tale relazione diventa $\overline{1} = \overline{385} \cdot (\overline{1}) + \overline{4} \cdot (\overline{-96})$: l'inverso moltiplicativo di $\overline{4}$ è $\overline{-96} = \overline{385 - 96} = \overline{289}$. L'equazione congruenziale

$$4x \equiv 3 \pmod{385}$$

diventa l'equazione

$$\overline{4}x = \overline{3} \text{ in } \mathbb{Z}_{385},$$

che si risolve moltiplicando ambo i membri per l'inverso moltiplicativo del coefficiente dell'incognita:

$$\overline{289} \cdot \overline{4}x = \overline{289} \cdot \overline{3}$$

ovvero

$$\overline{1}x = \overline{867} = \overline{97} :$$

si ha quindi che le soluzioni dell'equazione congruenziale sono tutti e soli gli interi dell'insieme

$$\overline{97} = \{385k + 97 : k \in \mathbb{Z}\}.$$

Esercizio 4. (3 punti)

1. Studiare il gruppo moltiplicativo $U(\mathbb{Z}_{10})$ degli invertibili di $\mathbb{Z}_{10}$.

2. (Facoltativo) A quale gruppo è isomorfo e perché?

Soluzione Ricordiamo che una classe resto $\overline{x} \in \mathbb{Z}_{10}$ è invertibile se e solo se x è coprimo col modulo n: in questo caso gli invertibili di $\mathbb{Z}_{10}$ sono $\{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$, risulta che l'ordine di $U(\mathbb{Z}_{10})$ è $\varphi(10) = 4$ (dove φ denota la funzione di Eulero, che conta il numero di interi compresi tra 1 ed n coprimi con n).

L'unità di tale gruppo è chiaramente $\overline{1}$. Il gruppo è abeliano, perché eredita come prodotto di classi la moltiplicazione usuale tra numeri interi, che è commutativa. Scriviamo la tavola moltiplicativa per $U(\mathbb{Z}_{10})$:

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
$\overline{3}$	$\overline{3}$	$\overline{9}$	$\overline{1}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{1}$	$\overline{9}$	$\overline{3}$
$\overline{9}$	$\overline{9}$	$\overline{7}$	$\overline{3}$	$\overline{1}$

Dalla tavola, di ogni elemento si può dedurre l'inverso:

$\overline{x}$	$\overline{x}^{-1}$
$\overline{1}$	$\overline{1}$
$\overline{3}$	$\overline{7}$
$\overline{7}$	$\overline{3}$
$\overline{9}$	$\overline{9}$

Calcoliamo l'ordine di ogni elemento diverso dall'unità (che ha sempre ordine 1). Si ha $\overline{3}^2 = \overline{9}$, $\overline{3}^3 = \overline{7}$, $\overline{3}^4 = \overline{1}$, cosi' pure $\overline{7}^2 = \overline{9}$, $\overline{7}^3 = \overline{3}$, $\overline{7}^4 = \overline{1}$, mentre $\overline{9}^2 = \overline{1}$, da cui $o(\overline{3}) = o(\overline{7}) = 4$ e $o(\overline{9}) = 2$. In particolare $< \overline{3} >= U(\mathbb{Z}_{10}) =< \overline{7} >$ risulta essere un gruppo ciclico, di ordine 4, isomorfo a $(Z_4, +)$ (oppure, in notazione moltiplicativa, a $(C_4, \cdot)$.) Il solo sottogruppo non banale è $< \overline{9} >$, sottogruppo di ordine 2. Esso è anche normale, come ogni sottogruppo di un gruppo abeliano.

Esercizio 5. (8 punti)

1. Sia $f_{a,b} : \mathbb{R} \to \mathbb{R}$ l'applicazione definita da

$$f_{a,b}(x) = ax + b;$$

detto $G = \{f_{a,b} : a, b \in \mathbb{R}, a \neq 0\}$ l'insieme delle applicazioni $f_{a,b}$ con $a \neq 0$, si dimostri che $(G, \circ)$ è un gruppo non abeliano rispetto alla composizione funzionale, determinando esplicitamente come elementi di G il suo elemento neutro, l'inverso di $f_{a,b}$ e il prodotto $f_{a,b} \circ f_{c,d}$.

2. Dire se l'insieme $H = \{f_{1,t} : t \in \mathbb{R}\} \subseteq G$ è o no sottogruppo di G.

Soluzione G è non vuoto, inoltre il prodotto di composizione funzionale è associativo. Verifichiamo l'esistenza dell'elemetno neutro, dell'inverso di ogni elemento di G e della chiusura rispetto al prodotto. Determiniamo a, b tali che per ogni $x \in \mathbb{R}$ si abbia $f_{a,b}(x) = x$, cioè $f_{a,b}$ sia l'applicazione identica di $\mathbb{R}$: $f_{a,b}(x) = ax + b = x$ se e solo se il polinomio $(a-1)x - b$ è identicamente nullo, ovvero se e solo se $a = 1, b = 0$. In questo caso $f_{1,0} = \text{id}$. Vediamo ora per quali valori $f_{a,b}$ è invertibile: posto $y = ax+b$, ricaviamo la x in funzione della y: si trova facilmente $x = \frac{y-b}{a} = \frac{1}{b}y - \frac{b}{a}$ se e solo se $a \neq 0$, i.e. se e solo se $f_{a,b} \in G$, e $(f_{a,b})^{-1} = f_{\frac{1}{b}, -\frac{b}{a}}$ è l'inversa dell'applicazione $f_{a,b}$. Calcoliamo la composizione di due tali applicazioni di G: $(f_{a,b} \circ f_{c,d})(x) = f_{a,b}(f_{c,d})(x) = f_{a,b}(cx + d) = a(cx + d) + b = ac \cdot x + (ad + b) = f_{ac,ad+b} \in G$. Se ne deduce che G è un gruppo.

Affinché H sia un sottogruppo di G, deve essere verificata la condizione seguente: $\forall x, y \in H : xy^{-1} \in H$. Nel presente caso:

$$\forall f_{1,s}, f_{1,t} : f_{1,s} \circ (f_{1,t})^{-1},$$

che per quanto precedentemente calcolato vale

$$f_{1,s} \circ (f_{1,t})^{-1} = f_{1,s} \circ f_{1,-t} = f_{1 \cdot 1 \cdot (-t)+s} = f_{1,s-t} \in H :$$

l'insieme dato è pertanto un sottogruppo di G.

Esercizio 6. (3 punti) Si dimostri la seguente identità che involve i coefficienti binomiali, vera per ogni n, k naturali, senza usare la formula del coefficiente binomiale ma in modo combinatorio:

$$\binom{n}{2} = \binom{k}{2} + \binom{n-k}{2} + k(n-k).$$

(Suggerimento: contare in due modi diversi il numero totale di coppie non ordinate di un insieme ad n elementi).

Soluzione Se S è un insieme con n elementi, si possono formare $\binom{n}{2}$ coppie non ordinate (sottoinsiemi a 2 elementi) con gli elementi di S. Supponiamo di fissare una suddivisione in due parti U ed $S \setminus I$ di S, di cui una, I, con k elementi, l'altra $S \setminus I$ coi rimanenti $n - k$ elementi. Basta dunque osservare che ogni coppia $\{x, y\}$ non ordinata di S può cadere in una sola di queste categorie, mutuamente esclusive:

- $\{x, y\}$ formata da elementi entrambi in I, quindi con $x, y \in I$: vi sono $\binom{k}{2}$ coppie di questo tipo;
- $\{x, y\}$ formata da elementi entrambi in $S \setminus I$, quindi con $x, y \in S \setminus I$: vi sono $\binom{n-k}{2}$ coppie di questo tipo;
- $\{x, y\}$ formata da elementi a cavallo tra le due pari, cioè con $x \in I$ e $y \in S \setminus I$, o viceversa: ci sono $k \setminus (n-k)$ coppie siffatte.