ALGEBRA
CANALE A-L

ESAME PRIMA PARTE
27 GENNAIO 2012

C. MALVENUTO

Istruzioni.

- Completare subito la parte inferiore di questa pagina con il proprio nome, cognome e firma.
- Scrivere solamente su questi fogli, anche dietro se occorre, a penna o a matita. Non sono ammessi libri, quaderni, altri fogli né calcolatrici.
- Tutte le risposte vanno **motivate**.
- **Non parlare** pena il ritiro immediato del compito.

ESERCIZIO	PUNTEGGIO
1	/ 7
2	/ 7
3	/ 7
4	/ 7
5	/ 2 (+3)
TOTALE	/30 (+3)

Nome e Cognome ↓	**Firma** ↓

Esercizio 1. (7 punti) Risolvere l'equazione congruenziale $14x \equiv 2 \pmod{25}$.

Soluzione. L'equazione congruenziale $ax \equiv b \pmod{n}$ ammette soluzioni se e solo se $(a, n)|b$. In questo caso il massimo comune divisore tra 14 e 25 è 1, (che divide qualunque numero): si dovrà dunque cercare l'inverso moltiplicativo di $\overline{14}$ in $\mathbb{Z}_{25}$ mediante un'identità di Bézout.

Calcoliamo intanto il massimo comune divisore tra 14 e 25 mediante l'algoritmo di Euclide delle divisioni successive:

- $25 = 14 \cdot 1 + 11$
- $14 = 11 \cdot 1 + 3$
- $11 = 3 \cdot 3 + 2$
- $3 = 2 \cdot 1 + 1$
- $2 = 1 \cdot 2 + 0$

Il massimo comune divisore è l'ultimo resto non nullo, quindi $(25, 14) = 1$. Ricaviamo ora dalle relazioni del tipo $a = bq + r$ (tranne l'ultima) i resti non nulli $r = a - bq$:

- $11 = 25 + 14(-1)$
- $3 = 14 + 11(-1)$
- $2 = 11 + 3(-3)$
- $1 = 3 + 2(-1)$

Sostituendo a ritroso si ricava:

$$\begin{aligned} 1 &= 3 + 2(-1) \\ &= 3 + [11 + 3(-3)](-1) \\ &= 11(-1) + 3(4) \\ &= 11(-1) + [14 + 11(-1)](4) \\ &= 14(4) + 11(-5) \\ &= 14(4) + [25 + 14(-1)](-5)) \\ &= 25(-5) + 14(9) \end{aligned}$$

Passando la relazione $1 = 25(-5) + 14(9)$ all'insieme quoziente $\mathbb{Z}_{25}$ si ottiene $\overline{1} = \overline{25}(\overline{-5}) + \overline{14}(\overline{9}) = \overline{0} + \overline{14} \cdot \overline{9}$: quindi $\overline{9}$ è l'inverso moltiplicativo di $\overline{14}$: l'equazione $14x \equiv 2 \pmod{25}$ in $\mathbb{Z}$ è equivalente all'equazione $\overline{14}x = \overline{2}$ di $\mathbb{Z}_{25}$: per risolverla si moltiplicano ambo i membri di quest'ultima equazione per l'inverso di $\overline{14}$ e si ottiene: $\overline{9} \cdot \overline{14}x = \overline{9} \cdot \overline{2}$, da cui $\overline{1}x = x = \overline{18}$ è la soluzione in $\mathbb{Z}_{25}$: le soluzioni dell'equazione congruenziale di partenza sono quindi tutti e soli gli elementi della progressione aritmetica

$$\overline{18} = \{x : x = 18 + 25k, k \in \mathbb{Z}\}.$$

Esercizio 2. (7 punti)

Sia τ_0 una fissata permutazione di S_n. Sia $f : S_n \to S_n$ l'applicazione così definita: $f(\sigma) = \tau_0^{-1}\sigma\tau_0, \ \ \forall \sigma \in S_n$.
Si dimostri che f è un automorfismo di S_n.

Soluzione. Ricordiamo che $f : (G, \cdot) \to (G', *)$ è un morfismo del gruppo G nel gruppo G' se è verificata la condizione:

$$\forall \sigma, \rho \in S_n : f(\sigma\rho) = f(\sigma)f(\rho).$$

In questo caso $G = G' = S_n$, l'operazione è la composizione di permutazioni. Prese comunque $\sigma, \rho \in S_n$ si ha:

$$\begin{aligned} f(\sigma)f(\rho) &= (\tau_0^{-1}\sigma\tau_0)(\tau_0^{-1}\rho\tau_0) \\ \text{(associatività)} &= \tau_0^{-1}\sigma(\tau_0\tau_0^{-1})\rho\tau_0 \\ &= \tau_0^{-1}\sigma(\text{id})\rho\tau_0 \\ &= \tau_0^{-1}(\sigma\rho)\tau_0 \\ &= f(\sigma\rho). \end{aligned}$$

Dunque f è un morfismo. Esso è inoltre biiettivo, in quanto l'applicazione $g : S_n \to S_n$ definita da $g(\sigma) = \tau_0\sigma\tau_0^{-1}$ è l'applicazione inversa di f:

$(f \circ g)(\sigma) = f(g(\sigma)) = f(\tau_0\sigma\tau_0^{-1}) = \tau_0^{-1}(\tau_0\sigma\tau_0^{-1})\tau_0 = (\tau_0^{-1}\tau_0)\sigma(\tau_0^{-1}\tau_0) = (\text{id})\sigma(\text{id}) = \sigma$. (Analogamente si verifica che $g \circ f = id$.)

N.B. Il fatto che l'applicazione f (che è il coniugio per un elemento fissato τ_0 sia un automorfismo, non dipende dal gruppo che si è analizzato qui, il gruppo delle permutazioni, ma vale per ogni gruppo.

Esercizio 3. (7 punti)

Determinare il periodo dell'elemento x^{321} del gruppo ciclico

$$C_{15} =< x : x^{15} = 1 > .$$

Descrivere gli elementi del sottogruppo $< x^{321} >$ ed elencare tutti i suoi generatori.

Soluzione. Eseguendo la divisione col resto si ha $321 = 15 \cdot 21 + 6$: pertanto $x^{321} = x^{15 \cdot 21 + 6} = x^{15 \cdot 21} \cdot x^6 = (x^{15})^{21} \cdot x^6 = (1)^{21} \cdot x^6 = x^6$.

Dunque $< x^{321} >=< x^6 >= \{(x^6)^h : h \in \mathbb{Z}\} = \{x^6, x^{12}, \}$

Calcoliamo le potenze di x^6:
$(x^6)^1 = x^6$;
$(x^6)^2 = x^{12}$;
$(x^6)^3 = x^{18} = x^3$;
$(x^6)^4 = x^3 \cdot x^6 = x^9$;
$(x^6)^5 = x^9 \cdot x^6 = x^{15} = 1$,
da cui $< x^6 >= \{1, x^3, x^6, x^9, x^{12}\}$, che è un gruppo ciclico a 5 elementi, isomorfo pertanto a $\mathbb{Z}_5$: per questo, dalla teoria sappiamo che tutti gli elementi non identici sono generatori di $< x^6 >$: ognuna delle potenze x^3, x^6, x^9, x^{12} è un generatore (si calcoli - solo a guisa di esempio - $< x^{12} >$ per vedere che in esso vi sono gli stessi elementi di $< x^6 >$).

Esercizio 4. (7 punti)

Studiare il gruppo moltiplicativo $U(\mathbb{Z}_9)$ (tavola moltiplicativa, inversi e ordine degli elementi). Stabilire se è isomorfo a $\mathbb{Z}_6$ oppure a S_3, nel qual caso descrivere esplicitamente un isomorfismo.

Soluzione. In $U(\mathbb{Z}_9)$ ci sono le classi resto mod(9) invertibili rispetto al prodotto di classi: queste sono rappresentate dagli interi coprimi con il modulo 9: dunque

$$U(\mathbb{Z}_9) = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}.$$

La tavola moltiplicativa degli elementi è:

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{5}$	$\overline{7}$	$\overline{8}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{5}$	$\overline{7}$	$\overline{8}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{1}$	$\overline{5}$	$\overline{7}$
$\overline{4}$	$\overline{4}$	$\overline{8}$	$\overline{7}$	$\overline{2}$	$\overline{1}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{2}$	$\overline{7}$	$\overline{8}$	$\overline{4}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{1}$	$\overline{8}$	$\overline{4}$	$\overline{2}$
$\overline{8}$	$\overline{8}$	$\overline{7}$	$\overline{5}$	$\overline{4}$	$\overline{2}$	$\overline{1}$

(Si noti che poiché la moltiplicazione del gruppo $U(\mathbb{Z}_9)$ è commutativa, è sufficiente calcolare i prodotti del tipo $\overline{i} \cdot \overline{j}$ con $i \leq j$, la tavola è simmetrica rispetto alla diagonale.)

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

$\overline{x}$	$\overline{x}^{-1}$
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{7}$
$\overline{5}$	$\overline{2}$
$\overline{7}$	$\overline{4}$
$\overline{8}$	$\overline{8}$

così come l'ordine (o periodo) degli elementi, calcolandone le potenze:

$\overline{x}$	$o(x)$
$\overline{1}$	1
$\overline{2}$	6
$\overline{4}$	3
$\overline{5}$	6
$\overline{7}$	3
$\overline{8}$	2

Ad esempio si ha:
$(\overline{2})^1 = \overline{2}$;
$(\overline{2})^2 = \overline{4}$;
$(\overline{2})^3 = \overline{4} \cdot \overline{2} = \overline{8}$;
$(\overline{2})^4 = \overline{8} \cdot \overline{2} = \overline{7}$;
$(\overline{2})^5 = \overline{7} \cdot \overline{2} = \overline{5}$;
$(\overline{2})^6 = \overline{5} \cdot \overline{2} = \overline{1}$.

Allo stesso modo si calcolano i periodi degli altri elementi. Abbiamo trovato un elemento di ordine $6 = |U(\mathbb{Z}_9)|$ pari all'ordine del gruppo: questo vuol dire che $U(\mathbb{Z}_9) =< \overline{2} >$ è un gruppo ciclico di ordine 6: esso è perciò isomorfo a $(\mathbb{Z}_6, +)$.Un isomorfismo esplicito si trova mandando un generatore di $U(\mathbb{Z}_9)$ in un generatore di $\mathbb{Z}_6$, e gli altri elementi di conseguenza. Per evitare ambiguità, avendo denotato con $\overline{x}$ la classe resto di x modulo 9, scriveremo $[a]_6$ per indicare la classe resto di a modulo 6. In questo caso si può definire un isomorfismo f tra $U(\mathbb{Z}_9)$ in $\mathbb{Z}_6$ tramite $f(\overline{2}) := [1]_6$, e mappando $(\overline{2})^h$ in $[h]_6$:

$$\begin{array}{rccc} f: & U(\mathbb{Z}_9) & \to & \mathbb{Z}_6 \\ & \overline{2} & \mapsto & [1]_6 \\ & \overline{4} & \mapsto & [2]_6 \\ & \overline{8} & \mapsto & [3]_6 \\ & \overline{7} & \mapsto & [4]_6 \\ & \overline{5} & \mapsto & [5]_6 \\ & \overline{1} & \mapsto & [0]_6 \end{array}$$

A priori si può affermare che $U(\mathbb{Z}_9)$ non è isomorfo a S_3, perchè esso (pur avendo cardinalità 6) non è abeliano.

Esercizio 5. (2 punti)

Dimostrare che l'insieme $H = \{\pi \in S_4 : \pi(1) = 1\}$ è un sottogruppo di S_4. (Facoltativo) (3 punti) Descrivere l'insieme delle classi laterali destre di H in S_4. H è normale in S_4?

Soluzione. Gli elementi di H sono permutazioni del tipo $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & a & b & c \end{pmatrix}$, con $\{a, b, c\} = \{2, 3, 4\}$. Per la condizione di sottogruppo si deve verificare che:

(a) l'identità $id = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ del gruppo S_4 sta in H: infatti si ha $id(1) = 1$;

(b) per ogni $\pi, \rho \in H$, anche $\pi \circ \rho \in H$: ora se $\pi(1) = 1, \rho(1) = 1$, allora per definizione di funzione composta si ottiene $(\pi \circ \rho)(1) = \pi(\rho(1)) = \pi(1) = 1$, quindi $\pi \circ \rho \in H$;

(c) se $\pi \in H$ allora $\pi^{-1} \in H$: ma $\pi(1) = 1 \leftrightarrow \pi^{-1}(1) = 1$.

Ne segue che H è un sottogruppo.

Poiché H ha ordine 6, vi sono $|S_4|/|H| = 4$ classi laterali: si noti che se $\sigma(1) = a$, allora $\sigma\pi(1) = a$ per ogni $\pi \in H$, e dunque

$$\sigma H = \{\sigma\pi : \pi \in H\} = \{\rho \in S_4 : \rho(1) = a\}.$$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

H non è normale in S_4: difatti basta coniugare un elemento di H tramite una permutazione che manda 1 in un elemento diverso da 1 per uscire fuori

dal sottogruppo stesso: ad esempio se $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1,2,4,3)$ in notazione ciclica, e $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (1)(2,4,3)$, allora $\sigma^{-1}\pi\sigma = (1,2,4)(3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \notin H$. (Si ricordi che quando si coniuga una permutazione π tramite un'altra σ, se $(a_1, a_2, \ldots, a_k)$ è un ciclo di π allora $(\sigma^{-1}(a_1), \sigma^{-1}(a_2), \ldots, \sigma^{-1}(a_k))$ è un ciclo di $\sigma^{-1}\pi\sigma$.)