Politecnico di Milano Anno accademico 2005–2006
Secondo anno di Laurea Foglio 3

Algebra e Logica Matematica

Gruppi, classi di resto

Esercizio 3.1. Calcolare il MCD e il mcm delle coppie seguenti:

1) $(12, 35)$;

2) $(231, 152)$;

3) $(1200, 17)$;

4) $(2301, 45)$.

Esercizio 3.2. a) Mostrare che $((-1; 1), *)$ è un gruppo ove $*$ è definita da

$$x * y = \frac{x + y}{1 + xy}.$$

Indicazione: è molto utile la tangente iperbolica.

b) Sia $(\mathbb{R}, *)$ dove $*$ è definita da

$$\forall x, y \in \mathbb{R},\ x * y = \sqrt[n]{x^n + y^n},$$

per un certo intero $n > 0$ dispari. Mostrare che $(\mathbb{R}, *)$ è un gruppo. Esibire un isomorfismo col gruppo $(\mathbb{R}, +)$.

Esercizio 3.3. a) Sie E un insieme finito munito di una legge interna associativa $*$ per la quale tutti gli elementi di E sono regolari. Stabillire che $(E, *)$ è un gruppo.

b) Sia $(E, *)$ un gruppo finito. Mostrare che se si costruisce la tavola dell'operazione $*$, ogni elemento di E compare una e un'unica volta in ogni riga e ogni colonna della tavola. Costruire una tavola con tale proprietà che non sia la tavola moltiplicativa di un gruppo.

c) Mostrare che se $(E, *)$ e $(E', .)$ sono due gruppi di ordine tre, esiste un isomorfismo tra questi due gruppi. Mostrare che è falso per quattro elementi.

Esercizio 3.4. Mostrare che i gruppi $(\mathbb{Q}, +)$ e $(\mathbb{Q}_+^*, \times)$ non sono isomorfi.
Mostrare che $(\mathbb{R}^*, \times)$ e $(\mathbb{C}^*, \times)$ non sono isomorfi.
Indicazione: in $\mathbb{Q}$, l'equazione $x^2 = p$, dove p è primo, non ha soluzione.

Esercizio 3.5. Determinare gli elementi di ordine 3 in $(\mathbb{C}^*, \times)$.

Esercizio 3.6. a) Mostrare che l'intersezione di una famiglia di sottogruppi di un gruppo G è un sottogruppo di G.

b) Sia G un gruppo. Dare una condizione necessaria e sufficente affinché due sottogruppi H e K di G siano tali che $H \cup K$ sia un sottogruppo di G.

c) Dedurne una condizione necessaria e sufficente affinché $H \cup K = G$.

Esercizio 3.7. Siano $(G, *)$ un gruppo, x e y due elementi di ordine finito di G tali che $x * y = y * x$.

a) Mostrare che $x * y$ è di ordine finito.

b) Supponiamo che $\mathrm{MCD}(o(x), o(y)) = 1$, mostrare che $o(x * y) = o(x)o(y)$.

c) Nel caso generale, mostrare che $o(x * y) = \mathrm{mcm}(o(x), o(y))$.

Esercizio 3.8. Siano $(G, *)$ un gruppo, x e y in G. Mostrare che

1) Se $o(x) = o(y) = o(x * y) = 2$, allora $x * y = y * x$.

2) Se $o(x)$ è finito, calcolare $o(x^{-1})$.

3) Se $o(x)$ è finito, calcolare $o(y * x * y^{-1})$.

4) Se $o(x * y)$ è finito, mostrare che $o(y * x)$ è finito e calcolarlo.

Esercizio 3.9. Mostrare che se tutti gli elementi di un gruppo G diversi dell'unità hanno ordine 2 allora G è abeliano.

Esercizio 3.10. Sia $(G, *)$ un gruppo con identità e. Sia $\mathcal{S}$ il sottoinsieme di G costituito dagli elementi di ordine 2, cioè

$$\mathcal{S} = \{g \in G / g * g = e \wedge g \neq e\}.$$

1) Mostrare che la relazione definita su G da

$$x \mathcal{R} y \iff x = y \text{ o } x = y^{-1}$$

è una relazione di equivalenza (questo è vero per tutti i gruppi, non solo per quelli di ordine pari).

2) Descrivere le classi di equivalenza della relazione.

3) Dire quanti elementi ha una classe di equivalenza (attenzione: ci sono due casi !).

4) Dedurre della domanda precedente che se il gruppo G è di ordine pari, allora $\mathcal{S}$ ha un numero dispari di elementi.

Esercizio 3.11. Fissiamo un intero $n \geqslant 1$.

1) Mostrare che $(\mathbb{Z}/n\mathbb{Z}, +)$ è ciclico.

2) Sia G un gruppo ciclico di ordine n. Mostrare che è isomorfo a $(\mathbb{Z}/n\mathbb{Z}, +)$. Quanti isomorfismi ci sono ?

3) Sia G un gruppo ciclico di orgine n. Mostrare che per ogni divisore d di n, G ha un unico sottogruppo di ordine d. Mostrare che è ciclico e precisare il suo generatore.

Esercizio 3.12. Calcolare gli elementi invertibili di $(\mathbb{Z}/6\mathbb{Z})$ e $(\mathbb{Z}/12\mathbb{Z})$.

Esercizio 3.13. Determinare gli automorfismi del gruppo $(\mathbb{Z}, +)$.

Esercizio 3.14. Sia $(G, *)$ un gruppo. Si chiama centro di G e si denota $Z(G)$ l'insieme degli elementi che commutano con tutti gli altri:

$$Z(G) = \{z \in G / \forall g \in G, g * z = z * g\}.$$

Mostrare che $Z(G)$ è un sottogruppo di G, che è abeliano e che è normale in G.

Esercizio 3.15. a) Mostrare che se un gruppo è generato da un unico elemento, allora è abeliano.

b) Mostrare che un gruppo con un numero primo di elementi è ciclico.

c) Sia p un numero primo e G un gruppo con p^2 elementi. Quanti elementi può a priori avere $Z(G)$? Mostrare che se $G/Z(G)$ è ciclico allora $Z(G) = G$. Contando gli elementi nelle classi di coniugio, verificare che non è possibile che $Z(G) = 1$. Concludere che G è abeliano.

Esercizio 3.16. Si consideri la seguente proprietà di un gruppo $(G, .)$: per ogni $x \in G$ e per ogni intero $n > 0$, se $x^n = 1_G$ allora $x = 1_G$.

1) I gruppi $(\mathbb{C}, +)$ e $(\mathbb{C}^*, \times)$ hanno tale proprietà ?

2) Nel seguito, $(G, .)$ sarà un gruppo con tale proprietà. Si provi che se $x \neq 1_G$ e n e m sono interi tali che $x^n = x^m$ allora $n = m$.

3) Si definisca su G una relazione $\leqslant$ ponendo, per ogni x, y in G, $x \leqslant y$ se e solo se esiste $n \in \mathbb{N}$ tale che $x = y^n$. Mostrare che $\leqslant$ è una relazione di ordine su G.

4) Dimostrare che $\leqslant$ è un ordine totale se e solo se $G = \{1_G\}$. (Indicazione: se $x \neq 1_G$, considerare x^2 e x^3.)

Esercizio 3.17. Sia $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ l'insieme delle matrici 2×2

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{tali che } a,\, b,\, c,\, d \in \mathbb{Z}/2\mathbb{Z},\ ad - bc = [1]_2$$

In $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ definiamo la moltiplicazione nel modo solito:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

Verificare che $(\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}), \times)$ è un gruppo. Quanti elementi ha ? È abeliano ?

Esercizio 3.18. Consideriamo il gruppo $(G, *)$ dove $G = \mathbb{R}^\times \times \mathbb{R}$ e $*$ è la legge definita su G da

$$(x, y) * (x', y') = (xx', xy' + y).$$

1) Mostrare che $(G, *)$ è effettivamente un gruppo.

2) Identificare il centro $Z(G)$ di G.

3) Mostrare che $\mathbb{R}_+^\times \times \mathbb{R}$ è un sottogruppo di G.

Nota: questo tipo di costruzione si chiama prodotto semidiretto di $\mathbb{R}^\times$ e $\mathbb{R}$.

Esercizio 3.19. Consideriamo il gruppo $(G, *)$ dove $G = \mathbb{R}^\times \times \mathbb{R}$ e $*$ è la legge definita su G da

$$(x, y) * (x', y') = (xx', xy' + \frac{y}{x'}).$$

1) Mostrare che $(G, *)$ è effettivamente un gruppo.

2) Identificare il centro $Z(G)$ di G.

3) Mostrare che $\mathbb{R}^\times \times \{0\}$, $\{1\} \times \mathbb{R}$ e $\mathbb{Q}^\times \times \mathbb{Q}$ sono dei sottogruppi di G.

4) Mostrare che per ogni $k \in \mathbb{Z}$, il sottoinsieme

$$H_k = \left\{ \left(x, k\left(x - \frac{1}{x} \right) \right) \Big/ \, x \in \mathbb{R}^\times \right\}$$

è un sottogruppo abeliano di $(G, *)$.