

## ESERCIZI PER CASA – PRIMA, SECONDA E TERZA SETTIMANA

Università degli Studi di Trento – Corso di Laurea in Matematica  
Corso di Teoria dei Gruppi – A.A. 2008/09  
4 marzo 2009

**I gruppi di ordine quattro.** Mostrate che ci sono, a meno di isomorfismo, esattamente due gruppi di ordine quattro, direttamente scrivendo le possibili tabelle di moltiplicazione.

[*Suggerimento:* Se il gruppo ha un elemento di ordine quattro allora è ciclico. Altrimenti il gruppo è  $1, a, b, c$  con ciascuno di  $a, b, c$  avente ordine due. Mostrate che c'è un solo modo di completare la tabella di moltiplicazione in modo da avere un gruppo.]

**Gruppi di ordine pari.** Mostrate che un gruppo di ordine pari ha sempre (almeno) un elemento di ordine due.

[*Suggerimento:* ...cioè un elemento  $g \neq 1$  tale che  $g^{-1} = g$ .]

**Sistemi di generatori per gruppi simmetrici ed alterni.** (1) Mostrate che  $S_n = \langle (12), (13), \dots, (1n) \rangle$ .

(2) Mostrate che  $S_n = \langle (12), (123 \dots n) \rangle$ .

(3) Mostrate che  $A_n$  è generato dai 3-cicli,

(4) anzi,  $A_n = \langle (123), (124), \dots, (12n) \rangle$ .

[*Suggerimenti:* (1) Si tratta di mostrare che ogni elemento di  $S_n$  si può scrivere come prodotto delle trasposizioni indicate (e i loro inversi, che sono esse stesse). Una possibilità è mostrare anzitutto che ogni trasposizione si può scrivere come prodotto delle trasposizioni indicate (conviene usare il coniugio per farlo), dopodiché ogni permutazione è prodotto di cicli, e abbiamo visto come scrivere un generico ciclo come prodotto di trasposizioni.

(2) Usate opportunamente  $(123 \dots n)$  e  $(12)$  per coniugare  $(12)$  in  $(1i)$ .

(3) Il punto cruciale è esprimere il prodotto di due arbitrarie trasposizioni come prodotto di 3-cicli. Distinguetne i due casi in cui le due trasposizioni muovono un punto in comune, o sono disgiunte.

(4) Anche qui una possibilità è usare il coniugio: mostrate che coniugando uno dei tre cicli dati sotto uno o più degli altri si riesce ad ottenere un 3-ciclo arbitrario.

**I sottogruppi di  $A_4$ .** Costruite tutti i sottogruppi di  $A_4$ .

[*Suggerimento:* Un modo per trovare tutti i sottogruppi è iniziare costruendo i sottogruppi ciclici. Poi considerate coppie di sottogruppi ciclici (o equivalentemente coppie di elementi) e trovate il sottogruppo generato da ogni coppia, ecc. Troverete dieci sottogruppi (inclusi quelli banali). Conviene rappresentarli in un diagramma che illustri le relazioni di contenimento (con  $A_4$  in cima, 1 in fondo, ecc.).]

**Classi di coniugio di  $S_6$  e  $A_6$ .** Determinate rappresentanti e lunghezze delle classi di coniugio del gruppo simmetrico  $S_6$ . Decidete quali fra quelle contenute in  $A_6$  si spezzano in due classi di coniugio di  $A_6$ , trovando quindi rappresentanti e lunghezze delle classi di coniugio di  $A_6$ . Deducetene che  $A_6$  è un gruppo semplice.

[*Suggerimenti:* Dovreste trovare che le lunghezze delle classi di coniugio di  $S_6$  sono

1, 45, 40, 40, 90, 144, 15, 15, 90, 120, 120.

Quelle contenute in  $A_6$  sono le prime sei. Per l'ultima parte usate il teorema di Lagrange come

fatto per  $A_5$  a lezione. Per semplificare la verifica potete notare, ad esempio, che tutti i divisori di 360 che superano 40 sono pari, con la sola eccezione di 45; quindi un sottogruppo normale non banale deve contenere, oltre all'elemento neutro, la classe lunga 45; inoltre, i divisori pari di 360 che superano 40 sono multipli di 4, con la sola eccezione di 90; ne segue subito che un sottogruppo normale non banale deve contenere le classi di lunghezza 1, 45 e 90.]

**Elementi di ordine finito.** (1) Mostrate che il gruppo unitario  $U(1) := \{z \in \mathbb{C} : |z| = 1\} \leq \mathbb{C}^* = \text{GL}(1, \mathbb{C})$  è isomorfo al gruppo quoziente  $\mathbb{R}/\mathbb{Z}$ .

(2) Mostrate che se  $G$  è un gruppo abeliano, allora gli elementi di  $G$  che hanno ordine finito formano un sottogruppo (detto il *sottogruppo di torsione*). [Suggerimento: Se  $g, h \in G$  hanno ordini  $m$  ed  $n$ , che ordine può avere  $gh$ ?]

(3) Trovate tutti gli elementi di ordine finito di  $\mathbb{C}^*$ , mostrando che appartengono a  $U(1)$ . Mostrate che il sottogruppo da essi formato (cioè il sottogruppo di torsione di  $\mathbb{C}^*$ , ovvero di  $U(1)$ ) è isomorfo a  $\mathbb{Q}/\mathbb{Z}$ .

(4) Mostrate che, per ogni intero positivo  $n$ , il gruppo  $U(1)$  ha esattamente un sottogruppo di ordine  $n$ , e questo è ciclico. [Suggerimento: Usate il teorema di Lagrange e notate che ogni elemento di ordine un divisore di  $n$  è radice dell'equazione  $z^n = 1$ .]

**Prodotto di sottogruppi.** Se  $H$  e  $K$  sono sottogruppi finiti di un gruppo  $G$  (non necessariamente finito), mostrate che il numero di elementi del prodotto  $HK = \{hk : h \in H, k \in K\}$  (che non è in generale un sottogruppo) è dato da  $|HK| = |H||K|/|H \cap K|$ .

Interpretate questa formula nel caso particolare in cui  $G = U(1)$ .

[Suggerimento: Se  $g \in G$ , quante soluzioni  $(h, k) \in G \times G$  ha l'equazione  $hk = g$ ?]

**Affinità della retta.** Se  $F$  è un campo, il *gruppo delle affinità* della retta su  $F$  (o semplicemente *gruppo affine*), indicato con  $\text{AGL}(1, F)$ , è il gruppo delle mappe  $F \rightarrow F$  della forma  $x \mapsto ax + b$  con  $a \in F^*$  e  $b \in F$ . Se rappresentiamo un punto  $x$  di  $F$  con il vettore colonna  $\begin{bmatrix} x \\ 1 \end{bmatrix}$  possiamo anche rappresentare  $\text{AGL}(1, F)$  come il sottogruppo di  $\text{GL}(2, F)$  che consiste delle matrici  $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$  con  $a \in F^*$  e  $b \in F$ .

(1) Mostrate che il sottoinsieme  $B$  di  $G$  formato da quelle matrici con  $a = 1$  è un sottogruppo normale di  $\text{AGL}(1, F)$ . Mostrate che il sottoinsieme  $A$  di  $G$  formato da quelle matrici con  $b = 1$  è un sottogruppo di  $\text{AGL}(1, F)$ , ma non un sottogruppo normale.

(2) Trovate tutti i sottogruppi finiti di  $\text{AGL}(1, \mathbb{R})$ .

(3) Trovate tutti gli elementi di ordine finito di  $\text{AGL}(1, \mathbb{C})$ . Notate che l'ordine di  $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$  dipende da  $a$  ma non da  $b$ .

(4) Se  $q$  è una potenza di un primo  $p$  indichiamo con  $\mathbb{F}_q$  l'unico campo con  $q$  elementi. In particolare  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ , il campo degli interi modulo  $p$ . Naturalmente  $\text{AGL}(1, \mathbb{F}_q)$  ha ordine  $q(q-1)$ , e quindi  $\text{AGL}(1, \mathbb{F}_2)$  è ciclico, avendo ordine 2. Mostrate che  $\text{AGL}(1, \mathbb{F}_3)$  è isomorfo al gruppo simmetrico  $S_3$ .

**Un automorfismo di  $\text{GL}(n, F)$ .** (1) Sia  $F$  un campo qualsiasi. Mostrate che la mappa di  $\text{GL}(n, F)$  in se stesso data dall'inversa trasposta, cioè  $A \mapsto (A^{-1})^\top$ , è un automorfismo di  $\text{GL}(n, F)$ . Mostrate che essa non può essere un automorfismo interno di  $\text{GL}(n, F)$ .

(2) Chiaramente la mappa  $A \mapsto (A^{-1})^\top$  manda il sottogruppo  $\text{SL}(n, F)$  in se stesso. Nel caso speciale in cui  $n = 2$  mostrate che essa è un automorfismo interno. (La mappa non è un automorfismo interno di  $\text{SL}(n, F)$  se  $n > 1$ , ma questo è meno semplice da mostrare.)

[Suggerimento: (2) Si tratta di trovare una matrice  $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}(2, F)$  tale che  $gAg^{-1} = (A^{-1})^\top$ , vale a dire, e forse meglio,  $gA = (A^{-1})^\top g$ , per ogni scelta di  $A = \begin{bmatrix} x & y \\ z & t \end{bmatrix} \in \text{SL}(2, F)$ .]