Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2008/2009
AL2 - Algebra 2: Gruppi, Anelli e Campi
Esercitazione 2 (14 ottobre 2008)

Esercizio 1. Siano $\sigma, \sigma' \in S_n$. σ e σ' si dicono *coniugate* (in simboli $\sigma \sim \sigma'$) se esiste $\tau \in S_n$ tale che $\sigma' = \tau\sigma\tau^{-1}$. Mostrare che $\sigma \sim \sigma'$ se e soltanto se σ e σ' hanno la stessa struttura ciclica.

Soluzione. Proposizione 5.3.2 del Piacentini-Cattaneo.

Esercizio 2. Sia G un gruppo di ordine 6. Mostrare che se G non è abeliano allora G è isomorfo a S_3.

Soluzione. Se G ha ordine 6 ogni $x \in G$ può avere ordine 2, 3 o 6. Poiché G non è abeliano nessun elemento ha ordine 6. Se ogni elemento avesse ordine 2, G sarebbe abeliano e dunque esiste almeno un elemento y di ordine 3. Inoltre non è possibile che ogni elemento abbia ordine 3, perché un gruppo finito non banale di ordine pari ha almeno un elemento di ordine 2 (verificare). Dunque:

$$\left\{e, x, y, y^2, xy, xy^2\right\}.$$

$yx \in G$, dunque $yx = xy$ oppure $yx = xy^2$, nel primo caso però G è abeliano quindi necessariamente $yx = xy^2$. L'isomorfismo di G con S_3 cercato è dunque dato da: $x \mapsto (12)$ e $y \mapsto (123)$. $\square$

Esercizio 3. Siano $(G, *), (G', *')$ gruppi abeliani. Mostrare che:

(a)
$$\mathrm{Hom}(G, G') := \{\varphi : G \longrightarrow G' \mid \varphi \text{ omomorfismo}\}$$
è un gruppo con l'operazione di somma puntuale, ovvero se $\varphi, \psi \in \mathrm{Hom}(G, G')$ allora $(\varphi + \psi)(x) := \varphi(x) *' \psi(x)$.

(b) Determinare esplicitamente gli elementi di $\mathrm{Hom}(\mathbb{Z}_{15}, \mathbb{Z}_3)$.

(c) Dimostrare che $\mathrm{Hom}(\mathbb{Z}_{12}, \mathbb{Z}_5) = \left\{\overline{0}\right\}$ dove $\overline{0}$ è l'omomorfismo nullo.

(d) Per n, m generici, quanti sono gli elementi di $\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$?

Soluzione. Siano φ e $\psi \in \mathrm{Hom}(G, G')$, facciamo vedere che $\varphi + \psi \in \mathrm{Hom}(G, G')$.

$$\begin{aligned}(\varphi + \psi)(x * y) &= \varphi(x * y) *' \psi(x * y) = \\ &= \varphi(x) *' \varphi(y) *' \psi(x) *' \psi(y) = \\ &= \varphi(x) *' \psi(x) *' \varphi(y) *' \psi(y) = (\varphi + \psi)(x) *' (\varphi + \psi)(y).\end{aligned}$$

Dunque $\varphi + \psi \in \mathrm{Hom}(G, G')$. Non è difficile poi dimostrare che:

(-) l'elemento neutro di Hom è: $\varphi_e : G \to G'$, $x \mapsto e$, dove e è l'elemento neutro di G'.

(-) Dato $\varphi \in \mathrm{Hom}(G, G')$, l'inverso di φ, ovvero φ^{-1} è l'elemento di Hom tale che $x \mapsto (\varphi(x)^{-1})$. (Far vedere che $\varphi^{-1} \in \mathrm{Hom}$).

Poiché $\mathbb{Z}_n$ è ciclico un omomorfismo φ di $\mathbb{Z}_n$ in G è completamente determinato quando si conosce $\varphi(\overline{1})$.

(a) Tutti e soli gli elementi di $\mathrm{Hom}(\mathbb{Z}_{15}, \mathbb{Z}_3)$ sono: $\varphi_0(\overline{1}) = \overline{0}$, $\varphi_1(\overline{1}) = \overline{1}$ e $\varphi_2(\overline{1}) = \overline{2}$.

(b) Supponiamo esista un elemento non nullo $\varphi \in \mathrm{Hom}(\mathbb{Z}_{12}, \mathbb{Z}_5)$, allora $\varphi(\overline{1})$ genera un sottogruppo (ciclico) di $\mathbb{Z}_5$ che necessariamente è tutto $\mathbb{Z}_5$. Per il teorema fondamentale di Omomorfismo si ha che $\mathbb{Z}_{12}/\ker(\varphi)$ è isomorfo al gruppo ciclico generato da $\varphi(\overline{1})$. Per il Teorema di Lagrange però tale sottogruppo di $\mathbb{Z}_5$ ha per ordine un divisore di 12, dunque $5 \mid 12$ che è assurdo.

(c) Facciamo vedere che $\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$ ha d elementi dove d è il $\gcd(n, m)$. Denotiamo con $\overline{a}_n$ gli elementi di $\mathbb{Z}_n$ e con $\overline{a}_m$ quelli di $\mathbb{Z}_m$.
È chiaro che se $\varphi \in \mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$ allora $\mathrm{Im}(\varphi)$ è il sottogruppo di $\mathbb{Z}_m$ generato da $\varphi(\overline{1}_n)$. Inoltre φ è suriettivo se e solo se $\varphi(\overline{1}_n) \in \mathcal{U}(\mathbb{Z}_m)$. Sia ora $\overline{a}_m \in \mathbb{Z}_m$, se l'ordine di $\overline{a}_m$ divide n, l'applicazione: $\psi : \mathbb{Z}_n \to \mathbb{Z}_m$, $\overline{x}_n \mapsto \overline{ax}_m$ è ben definita ed è un omomorfismo di gruppi (verificare).
Definiamo $f : (\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m), +) \to (\mathbb{Z}_m, +)$, $\varphi \mapsto \varphi(\overline{1}_n)$. Si dimostra facilmente che f è un omomorfismo, inoltre:

$$\varphi \in \ker(f) \iff f(\varphi) = \overline{0}_m \iff \varphi(\overline{a}_n) = \overline{0}_m,\ \forall \overline{a}_n \in \mathbb{Z}_n,$$

dunque f è iniettivo.
$\mathrm{Im}(f) = \{\varphi(\overline{1}_n) \,|\, \varphi \in \mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)\}$. Osserviamo che, in quanto sottogruppo di $\mathbb{Z}_m$, $\mathrm{Im}(f)$ è ciclico di ordine un divisore di m. Sia $k := \frac{m}{d}$, l'ordine di $\overline{k}_m$, che è uguale a d, divide n, dunque $\overline{k}_m \in \mathrm{Im}(f)$. Se $\overline{a}_m \in \mathrm{Im}(f)$ allora l'ordine di $\overline{a}_m$ divide sia m che n, e dunque divide d, ne segue che $\mathrm{Im}(f) = \overline{k}_m\mathbb{Z}_m$ in quanto $\mathrm{Im}(f)$ contiene un elemento di ordine d. Dunque $\mathrm{Im}(f)$ è isomorfo a $\mathbb{Z}_d$ e applicando il Teorema fondamentale di Omomorfismo si ha che $\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$ è isomorfo a $\mathbb{Z}_d$. □

Esercizio 4. Classificare, a meno di isomorfismi, tutti i gruppi di ordine 8.

Soluzione. Sia G di ordine 8. Per ogni $a \in G$ a può avere ordine $2, 4, 8$. Dato che G ha ordine pari esiste sempre almeno un elemento di ordine 2. Se esiste $a \in G$ con ordine 8 allora $G \cong \mathbb{Z}_8$, supponiamo dunque che nessuna elemento di G abbia ordine 8. Se per ogni $a \in G$, $a \neq e$ si ha $a^2 = e$ necessariamente G è abeliano ed è della forma: $\{e, a, b, c, ab, bc, abc\}$. Si verifica facilmente allora che l'applicazione:

$$\begin{array}{rcl} \varphi : G & \longrightarrow & \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\ e & \longmapsto & (\overline{0}, \overline{0}, \overline{0}) \\ a & \longmapsto & (\overline{1}, \overline{0}, \overline{0}) \\ b & \longmapsto & (\overline{0}, \overline{1}, \overline{0}) \\ c & \longmapsto & (\overline{0}, \overline{0}, \overline{1}) \end{array}$$

è un isomorfismo.
Supponiamo dunque che esista almeno un elemento a di ordine 4. Il sottogruppo ciclico generato da a è normale in G avendo indice 2, dunque se $b \in G$ e $b \notin \langle a \rangle$

si ha $bab^{-1} = a^k$ per qualche $k \in \{0,1,2,3\}$.
Supponiamo b abbia ordine 2: (si noti che, avendo a ordine 4, a^2 ha ordine 2, dunque non necessariamente in G c'è un altro elemento di ordine 2). Se b ha ordine 2 allora $bab^{-1} = bab = a^k$, chiaramente $k \neq 0$, altrimenti $b^2 = a = e$. Se $bab = a$ allora $ab = ba$, $a^2b = ba^2$ e $a^3b = ba^3$, G è abeliano ed è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_4$ (tramite l'isomorfismo che associa a a $(\overline{0}, \overline{1})$ e b a $(\overline{1}, \overline{0})$.
Se $bab = a^2$, allora $ab = ba^2$ e $ba = ba^2$, inoltre $a = ba^2b$, da cui $a^2 = a(ba^2b) = (ab)(a^2b) = (ba^2)(a^2b) = e$ contro l'ipotesi che a abbia ordine 4. Dunque il caso $bab = a^2$ è da escludere.
Facciamo vedere che se $bab = a^3$ allora $G \cong D_4$. È sufficiente dimostrare che G contiene 2 elementi a, b tali che $a^4 = b^2 = e$ ed $(ab)^2 = e$, in quanto già sappiamo che in G due siffatti elementi generano D_4. Per questioni di ordine G sarà isomorfo a D_4. Per ipotesi sappiamo che $a^4 = b^2 = e$. $(ab)^2 = abab = aa^3 = e$, dunque $G \cong D_4$.
Supponiamo b abbia ordine 4: sia $\langle a \rangle$ che $\langle b \rangle$ sono normali in G. $aba^{-1} = b^s$ e $bab^{-1} = a^t$ con $s, t \in \{0,1,2,3\}$. $s = 1$ (o $t = 1$) è da escludere; in questo caso infatti non è difficile dimostrare che G ha 16 elementi ed è isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_4$. Facciamo vedere che necessariamente $bab^{-1} = a^3 = a^{-1}$. Chiaramente $bab^{-1} \neq a, e$, dobbiamo escludere anche il caso in cui $bab^{-1} = a^2$. Supponiamo che si abbia $bab^{-1} = a^2$, allora $ba = a^2b$ e $b = a(aba^{-1}) = ab^t$ perché anche $\langle b \rangle$ è normale in G. Dunque $b^{t-1} = a^{-1}$. Facciamo vedere che questo non è possibile per alcun valore di t: se $t = 0$ allora $b^{-1} = a^{-1}$ ovvero $a = b$, se $t = 1$, allora $a^3 = e$, se $t = 2$ invece $b = a^3$, se $t = 3$ allora $b^2 = a^3$. È chiaro che nessuno dei precedenti casi può verificarsi, dunque $bab^{-1} = a^3$. Allo stesso modo si verifica che $aba^{-1} = b^3$.
Mostriamo che $a^2 = b^2$. Dalle relazioni precedenti si ha: $a^2 = (ab^{-1}a^{-1})b = b^s$; per questioni di ordine deve essere necessariamente $s = 2$, dunque $a^2 = b^2$.
Possiamo concludere quindi che G contiene un sottogruppo $\langle a, b \rangle$ tale che $a^4 = 1$, $a^2 = b^2$ e $bab^{-1} = a^3$. Un tale sottogruppo è però isomorfo a Q_8, dunque, per questione di ordine $G \cong Q_8$. $\square$

Esercizio 5. Sia Q_8 il gruppo dei quaternioni:

(a) Determinare un sottogruppo di S_8 isomorfo a Q_8.

(b) Calcolare il gruppo degli automorfismi interni $\mathbf{I}(Q_8)$ e determinare a quale gruppo noto è isomorfo.

Soluzione.

1. $S_8 \cong S(Q_8)$, dunque un sottogruppo S_8 isomorfo a Q_8 è dato da:

$$H := \langle (1\, i\, -1\, -i)(j\, k\, -j\, -k\,), (1\, j\, -1\, -j)(k\, i\, -k\, -i) \rangle\,.$$

2. Poiché $Z(Q_8)$ ha 2 elementi $\mathbf{I}(Q_8)$ ha 4 elementi (utilizzando l'isomorfismo $G/Z(G) \cong \mathbf{I}(G)$). Allora $\mathbf{I}(Q_8)$ può essere $\mathbb{Z}_4$ oppure V_4. I quattro automorfismi interni di Q_8 sono l'identità e γ_x, per $x = i, j, k$. Allora per ogni $g \in Q_8$, $\gamma_i^2(g) = \gamma_i(ig(-i)) = (-1)g(-1) = g$. Ripetendo lo stesso per γ_j e γ_k si deduce che ogni elemento di $\mathbf{I}(Q_8)$ ha ordine 2 3 dunque $\mathbf{I}(Q_8) \cong V_4$. $\square$

Esercizio 6. Determinare per ogni $n \geq 2$:

(a) $Z(D_n)$;

(b) $\mathbf{I}(D_n)$.

Soluzione.

1. $$Z(D_n) = \begin{cases} \langle \rho^{\frac{n}{2}} \rangle & \text{se } n = 2k, \\ \{\mathrm{id}\} & \text{se } n = 2k+1. \end{cases}$$

2. Se n è dispari $\mathbf{I}(D_n) \cong D_n$, se n è pari $\mathbf{I}(D_n)$ avrà ordine n. Gli automorfismi del tipo γ_ρ costituiscono un sottogruppo ciclico di ordine $k := \frac{n}{2}$, mentre γ_σ ha ordine 2. Inoltre $\gamma_\rho \gamma_\sigma(g) = \rho\sigma g(\rho\sigma)^{-1} = \gamma_{\rho\sigma}(g) = \gamma_{\sigma\rho^{n-1}}(g) = \gamma_\sigma \gamma_{\rho^{n-1}}(g)$. Si verifica subito che $(\gamma_\rho\gamma_\sigma)^2 = \gamma_{(\rho\sigma)^2} = \gamma_{\mathrm{id}} = \mathrm{id}$. Dunque $\mathbf{I}(D_n) \cong D_{\frac{n}{2}}$. □

Esercizio 7. Un sottogruppo H di un gruppo G si dice *caratteristico* se $\alpha(H) = H$ per ogni $\alpha \in \mathrm{Aut}(G)$. Mostrare che il centro di G, $Z(G)$, è un sottogruppo caratteristico.

Soluzione. Sia $\alpha \in \mathrm{Aut}(G)$ e $x \in G$, vogliamo far vedere che $x \in Z(G) \iff \alpha(x) \in Z(G)$.
Sia $g \in G$ un elemento qualsiasi.

$$x \in Z(G) \iff xg = gx \iff \alpha(xg) = \alpha(gx) \iff \alpha(x)\alpha(g) = \alpha(g)\alpha(x).$$

Poiché α è un automorfismo, per ogni $y \in G$, $y = \alpha(z)$ per qualche $z \in G$, dunque, facendo variare $g \in G$, $x \in Z(G) \iff \alpha(x) \in Z(G)$. □