ALGEBRA SUPERIORE: SOLUZIONI LEZIONE 1

esercizio 1. *Sia $n \geq 2$ e D_{2n} il gruppo diedrale di ordine $2n$. Si provi che le seguenti condizioni sono equivalenti:*

(1) *n è dispari;*
(2) *le involuzioni di D_{2n} sono a due a due coniugate.*

SOLUZIONE. Scriviamo il gruppo diedrale $D := D_{2n} = \langle y \rangle \rtimes \langle x \rangle$, con $|y| = n$ e $|x| = 2$.
Se n è pari, allora $u = y^{n/2}$ è una involuzione, e non è coniugata all'involuzione x, dato che (poiché $\langle y \rangle \trianglelefteq D$) tutti i coniugati di a sono contenuti in $\langle y \rangle$ (di fatto $a \in Z(D)$). Quindi (2) $\Rightarrow$ (1).
Viceversa, se n è dispari, $\langle y \rangle$ non contiene involuzioni, e dunque, per quanto visto a lezione, l'insieme delle involuzioni di D è $D \setminus \langle y \rangle = \{y^i x \mid 0 \leq i \leq n-1\}$. Dato $0 \leq i \leq n-1$, sia $0 \leq t \leq n-1$ tale che $2t \equiv i \pmod{n}$ (esiste perché n è dispari); allora

$$x^{y^t} = y^t x y^{-t} = y^t x y^{-t} x^2 = y^t (x y^{-t} x) x = y^t (y^{-t})^x x = y^t y^t x = y^{2t} x = y^i x.$$

Dunque, tutte le involuzioni sono coniugate a x (quindi tra di loro). ■

esercizio 2. *Sia G un gruppo infinito tale che esiste $A \trianglelefteq G$ con A ciclico e $|G : A| = 2$. Si provi che G è isomorfo ad uno dei seguenti gruppi: $\mathbb{Z}$, $\mathbb{Z} \times C_2$, D_∞.*

SOLUZIONE. Poiché G è infinito $A = \langle a \rangle$ è un gruppo ciclico infinito. Sia $b \in G \setminus A$, allora $b^2 \in A$, quindi $b^2 = a^z$ per qualche $z \in \mathbb{Z}$.
Inoltre, poiché $A \trianglelefteq G$, b agisce per coniugio come un automorfismo di A. Poiché gli automorfismi di un gruppo ciclico infinito so 1 (l'identità) e -1 (l'inversione), si ha

$$a^b = a \quad \text{oppure} \quad a^b = a^{-1}.$$

Nel primo caso, G è abeliano. Se $z = 2m$ è pari, posto $u = a^{-m}$ si ha

$$u^2 = a^{-2m} b^2 = a^{-2m} a^{2m} = 1,$$

inoltre $\langle a \rangle \cap \langle u \rangle = 1$ e quindi $G = \langle a \rangle \times \langle u \rangle \simeq \mathbb{Z} \times C_2$; se $z = 2m+1$ è dispari, posto $c = a^{-m} b$ si trova

$$c^2 = a^{-2m} b^2 = a^{-2m} a^{2m+1} = a.$$

quindi $G = \langle c \rangle$ è ciclico, cioè isomorfo a $\mathbb{Z}$.

Nel secondo caso, abbiamo

$$a^z = b^2 = (b^2)^b = (a^z)^b = (a^z)^{-1},$$

quindi $b^2 = a^z = 1$, e dunque $G = \langle a \rangle \rtimes \langle b \rangle \simeq D_\infty$. ■

esercizio 3. *Sia $\{G_i\}_{i \in \Lambda}$ una famiglia di gruppi, e $W = Car_{i \in \Lambda} G_i$ il suo prodotto cartesiano. Per ogni $i \in \Lambda$ si denoti con π_i la proiezione $W \to G_i$.*
Sia H un gruppo e per ogni $i \in \Lambda$ sia assegnato un omomorfismo

$$\phi_i : H \to G_i.$$

Si provi che esiste un unico omomorfismo $\phi : H \to W$ tale che $\pi_i \phi = \phi_i$ per ogni $i \in \Lambda$.

SOLUZIONE. Si pone, per ogni $x \in H$,

$$\phi(x) = (\phi_i(x))_{i\in\Lambda}.$$

Poiché ogni ϕ_i è un omomorfismo. $\phi : H \to W$ è un omomorfismo, e chiaramente, per ogni $x \in H$, ed ogni $i \in \Lambda$, $\pi_i\phi(x) = \pi_i((\phi_i(x))_{i\in\Lambda}) = \phi_i(x)$; quindi $\pi_i\phi = \phi_i$.
L'unicità è ovvia. ■

esercizio 4. *Si provino le seguenti affermazioni.*

(1) *ogni prodotto cartesiano di gruppi finiti è residualmente finito;*
(2) *la classe dei gruppi residualmente finiti è chiusa per sottogruppi, cioè ogni sottogruppo di un gruppo residualmente finito è residualmente finito.*

SOLUZIONE. (1) Sia $\{G_i\}_{i\in\Lambda}$ una famiglia di gruppi finiti, $W = Car_{i\in\Lambda}G_i$, e per ogni $i \in \Lambda$ sia π_i la proiezione $W \to G_i$. Per ogni $i \in \Lambda$ sia $G_i^* = \ker(\pi_i)$; allora $G_i^* \trianglelefteq W$ e $W/G_i^* \simeq G_i$ è un gruppo finito. Poiché $\bigcap i \in \Lambda G_i^* = 1$, si conclude che W è residualmente finito.

(2) Siano G un gruppo, $H \leq G$ e N un sottogruppo normale di G di indice finito; allora $N \cap H \trianglelefteq H$ e, per il secondo teorema di omomorfismo,

$$\frac{H}{N\cap H} \simeq \frac{NH}{N} \leq \frac{G}{N}$$

è un gruppo finito. Supponiamo ora che G sia residualmente finito. Per ogni $1 \neq h \in H$ esiste $N \trianglelefteq G$ tale che G/N è finito e $h \notin N$; ma allora $h \notin H \cap N$ e $H/(H \cap N)$ è finito. Dunque H è residualmente finito. ■

esercizio 5. *Fissato un numero primo p, sia*

$$\mathbb{Z}[1/p] = \{n/p^m \in \mathbb{Q} \mid n \in \mathbb{Z},\ m \geq 0\}.$$

Si dimostrino i seguenti fatti:

(1) $\mathbb{Z}[1/p]$ *è residualmente finito:*
(2) $\mathbb{Z}[1/p]/\mathbb{Z} \simeq C_{p^\infty}$ *non è residualmente finito.*

SOLUZIONE. (1) Sia q un numero primo, $q \neq p$, e sia $0 \leq t \leq q-1$ tale che $pt \equiv 1 \pmod p$. Consideriamo l'applicazione $\pi_q : \mathbb{Z}[1/p] \to \mathbb{Z}/q\mathbb{Z}$ definita da

$$n/p^m \mapsto nt^m + q\mathbb{Z}.$$

È ben definita: infatti, se $n/p^m = n_1/p^{m_1}$ allora $np^{m_1} = n_1p^m$, quindi

$$nt^m \equiv nt^m(p^{m_1}t^{m_1}) = n_1p^mt^{m_1}t^m = n_1(p^mt^m)p^{m_1} \equiv n_1t^{m_1} \pmod q.$$

π_q è chiaramente suriettiva; ed è un omomorfismo. Siano infatti $n/p^m, n_1/p^{m_1} \in \mathbb{Z}[1/p]$, con $m_1 \geq m$, allora

$$\pi_q\Big(\frac{n}{p^m} + \frac{n_1}{p^{m_1}}\Big) = \pi_q\Big(\frac{np^{m_1-m} + n_1}{p^{m_1}}\Big) = np^{m_1-m}t^{m_1} + n_1t^{m_1} + q\mathbb{Z} =$$

$$= nt^m + n_1t^{m_1} + q\mathbb{Z} = \pi_q\Big(\frac{n}{p^m}\Big) + \pi_q\Big(\frac{n_1}{p^{m_1}}\Big).$$

Abbiamo $\mathbb{Z}[1/p]/\ker(\pi_q) \simeq \mathbb{Z}/q\mathbb{Z}$, inoltre

$$\ker(\pi_q) = \{n/p^m \in \mathbb{Z}[1/p] \mid q \text{ divide } n\}.$$

Quindi

$$\bigcap_{p\neq q\in\mathbb{P}} \ker(\pi_q) = 1$$

e dunque $\mathbb{Z}[1/p]$ è residualmente finito.

(2) Sia T il gruppo moltiplicativo dei numeri complessi di modulo 1, e consideriamo l'applicazione $\Phi : \mathbb{Z}[1/p] \to T$ definita da

$$\Phi\Big(\frac{n}{p^m}\Big) = e^{2\pi i \cdot \frac{n}{p^m}}$$

che si verifica facilmente essere un omomorfismo. Come facilmente si vede che $Im(\Phi) = C_{p^\infty}$ e $\ker(\Phi) = \mathbb{Z}$. Dunque, per il Teorema di omomorfismo

$$\frac{\mathbb{Z}[1/p]}{\mathbb{Z}} \simeq C_{p^\infty}.$$

Infine, C_{p^∞} non ha sottogruppi propri di indice finito, e pertanto $\mathbb{Z}[1/p]/\mathbb{Z}$ non è residualmente finito. ■

esercizio 6. *Siano $W = Car_{i\in\Lambda} G_i$ e $D = Car_{i\in\Lambda} G_i$.*

(1) *Si provi che D è periodico se e solo se ogni G_i è periodico;*
(2) *Si provi che W è periodico se e solo se ogni G_i è periodico ed esiste $n \geq 1$ tale che l'insieme dei gruppi G_i il cui esponente non divide n è finito.*

SOLUZIONE. Poichè per ogni $\in \Lambda$, G_i è isomorfo a un sottogruppo di D, se W o D sono periodici allora G_i è periodico.

(1) Supponiamo che ogni G_i sia periodico e sia $g = (g_i)_{i\in\Lambda} \in D$. Per ogni $i \in \Lambda$ sia $n_i = |g_i|$; poiché il supporto di g è finito, tutti tranne un numero finito di n_i sono uguali a 1. Quindi esiste $n = m.c.m.\{n_i \mid i \in \Lambda\}$ e chiaramente $g^n = (g_i)^n_{i\in\Lambda} = (g_i^n)_{i\in\Lambda} = 1$.

(2) Supponiamo che ogni G_i sia periodico ed esista $n \geq 1$ tale che l'insieme

$$I = \{i \in \Lambda \mid \text{esponente di } G_i \text{ non divide } n\}$$

sia finito. Posto $\Lambda_1 = \Lambda \setminus I$, possiamo scrivere $W = W_1 \times H$, dove

$$W_1 = Car_{i\in\Lambda_1} G_i, \qquad H = Car_{i\in I} G_i = Dir_{i\in I} G_i.$$

Se $g = (g_i)_{i\in\Lambda_1} \in W_1$ allora $g^n = (g_i)^n_{i\in\Lambda_1} = (g_i^n)_{i\in\Lambda_1} = 1$, e dunque W_1 è periodico, mentre H è periodico per il punto precedente. Quindi W è periodico.
Viceversa, assumendo sempre che ogni G_i sia periodico, supponiamo che per ogni $n \geq 1$ esistano infiniti gruppi G_i tali che il loro esponente non divide n. Possiamo allora selezionare un sottoinsieme infinito $\Delta = \{i_1, i_2, i_3, \dots\}$ di Λ in modo che per ogni $n \geq 1$ esiste $g_{i_n} \in G_{i_n}$ tale che $g_{i_n}^n \neq 1$. Ma allora

$$(g_{i_n})_{i_n\in\Delta} \in Car_{j\in\Delta} G_j \leq W$$

è un elemento di ordine infinito. ■

esercizio 7. *Si provi che un prodotto cartesiano di gruppi non-banali è finitamente generato se e soltanto se è il prodotto diretto di un insieme finito di gruppi finitamente generati.*

SOLUZIONE. Il prodotto cartesiano di una famiglia infinita di gruppi non-banali è non-numerabile, mentre ogni gruppo finitamente generato è numerabile.
Quindi, se $W = Car_{i\in\Lambda} G_i$ (con $G_i \neq 1$ per ogni $i \in \Lambda$) è finitamente generato, Λ deve essere finito (dunque$W$ coincide con il prodotto diretto); inoltre, poiché ogni G_i è isomorfo ad un quoziente di W, ogni G_i è finitamente generato.
Il viceversa è facile. ■

esercizio 8. *Si provi che un gruppo abeliano divisibile non ha alcun sottogruppo proprio di indice finito.*

SOLUZIONE. Siano A un gruppo abeliano divisibile e $B \leq A$ un sottogruppo di indice finito $n \geq 1$. Allora per ogni $a \in A$, si ha (notazione additiva):

$$B = 0_{A/B} = n(a + B) = na + B,$$

quindi $na \in B$. Ma l'ipotesi di divisibilità implica $A = \{na \mid a \in A\}$. Pertanto $B = A$ e $n = 1$. ■

esercizio 9. *Sia p un numero primo e, per ogni $n \geq 1$, sia $H_n = C_{p^n}$ un gruppo ciclico di ordine p^n. Siano*

$$G = Car_{n\geq1}H_n, \quad D = Dir_{n\geq1}H_n, \ e \ \ T = \{x \in G \mid |x| < \infty\}.$$

Si provi che $D \leq T \leq G$, che T è un p-gruppo (cioè ogni suo elemento ha ordine una potenza di p), e che T/D è un gruppo abeliano radicabile (divisibile).

SOLUZIONE. Cominciamo osservando che se A è un gruppo abeliano e $a, b \in A$ sono elementi di ordine finito, $|a| = n$ e $|b| = n$, allora $(ab)^{nm} = a^{nm}b^{nm} = 1$, quindi ab ha ordine finito. Dunque $\{a \in A \mid |a| < \infty\}$ è un sottogruppo di A.
Questo si applica al gruppo $G = Car_{n\geq1}H_n$, che è abeliano, e quindi $T \leq G$. Inoltre $D \leq T$ per il punto (1) dell'esercizio 6. Inoltre $D \trianglelefteq G$ (questo in generale) e dunque $D \trianglelefteq T$.

Sia $g = (g_i)_{i\geq1} \in T$ e $n = |g|$; allora $g_i^n = 1$ per ogni $i \geq 1$. Poiché gli elementi g_i hanno tutti ordine una potenza di p si deduce che anche n è tale, ovvero $n = p^m$ per qualche $m \geq 0$. Dunque $gD^{p^m} = g^{p^m}D = D = 1_{T/D}$, e questo prova che T/D è un p-gruppo.

Per il punto conclusivo, facciamo un'altra osservazione generale:
un p-gruppo H è radicabile se per ogni $x \in H$ esiste $y \in H$ tale che $y^p = x$.
Infatti, sia H un p-gruppo con tale proprietà, allora con una ovvia induzione si vede che per ogni $x \in H$ ed ogni $m \geq 1$, esiste $y \in H$ tale che $y^{p^m} = x$. Se n è un intero positivo qualsiasi, scriviamo $n = p^m k$ con k coprimo con p. Per ogni $x \in H$, poiché $|x|$ è una potenza di p, si ha $\langle x \rangle = \langle x^k \rangle$ e dunque $x = (x^k)^t$, per qualche $t \geq 1$. Per ipotesi, esiste $y \in H$ tale che $y^{p^m} = x^t$, e dunque

$$y^n = y^{p^m k} = (y^{p^m})^k = (x^t)^k = (x^k)^t = x.$$

Quindi H è radicabile.

Torniamo all'esercizio. Sia $g = (g_i)_{i\geq1} \in T$ con $|g| = p^m$. Allora $g_i^{p^m} = 1$ per ogni $i \geq 1$. Questo implica che per per ogni indice $t > m$, $\langle g_t \rangle$ è un sottogruppo proprio di H_t, il che significa, dato che H_t è un gruppo ciclico di ordine $p^t > p^m$, che $g_t = h_t^p$ con $h_t \in H_t$. Osserviamo che $h_t^{p^{m+1}} = 1$.
Sia $y = (y_i)_{i\geq1}$ l'elemento di G definito da $y_i = 1$ se $i \leq m$ e $y_i = h_i$ se $i > m$. Allora $y^{p^{m+1}} = 1$ e dunque $y \in T$. Abbiamo inoltre $y_i^p g_i^{-1} = 1$ per ogni $i > m$, e dunque

$$y^p g^{-1} = (y_i^p g_i^{-1})_{i\geq1} \in D,$$

da cui $(yD)^p = gD$. Per quanto osservato sopra, T/D è radicabile. ■