Algebra I - Soluzioni 3

12 Aprile

1 Esercizi

Esercizio 1. Ogni ideale di un anello $(R, +, \cdot)$ è in primis un sottogruppo del gruppo $(R, +)$. Siccome il gruppo $\mathbb{Z}/21\mathbb{Z}$ è ciclico, gli unici sottogruppi sono della forma $d\mathbb{Z}/21\mathbb{Z}$ con $d \mid 21$, cioè

$$\mathbb{Z}/21\mathbb{Z}, \quad 3\mathbb{Z}/21\mathbb{Z}, \quad 7\mathbb{Z}/21\mathbb{Z}, \quad 21\mathbb{Z}/21\mathbb{Z}.$$

Sono tutti degli ideali, e gli unici non banali sono $3\mathbb{Z}/21\mathbb{Z}$ e $7\mathbb{Z}/21\mathbb{Z}$. Siccome per $p = 3, 7$,

$$\mathbb{Z}/21\mathbb{Z}\big/p\mathbb{Z}/21\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$$

che è un campo, i due ideali sono massimali.

Esercizio 2. Siccome $\mathbb{Z}/5\mathbb{Z}$ è un dominio (in realtà è anche un campo), allora $\mathbb{Z}/5\mathbb{Z}[x]$ è un dominio. Essendo i polinomi seguenti di grado 2 o 3, per verificarne l'irriducibilità basta verificare che non abbiano radici in $\mathbb{Z}/5\mathbb{Z}$.

Siano p_1, p_2, p_3 e p_4 i polinomi dell'esercizio.

$\mathbb{Z}/5\mathbb{Z}$	p_1	p_2	p_3	p_4
0	1	3	2	2
1	3	4	3	1
2	1	2	1	1
3	1	2	1	3
4	4	4	3	3

Siccome nessun polinomio si annulla in neanche un elemento di $\mathbb{Z}/5\mathbb{Z}$, segue che sono tutti irriducibili.

Esercizio 3. Per esempio il gruppo $(\mathbb{Z}/720\mathbb{Z}, +)$ è un gruppo ciclico di ordine 720. Il gruppo essendo ciclico possiede sottogruppi per ogni $d \mid 720$, ed essendo abeliano ogni suo sottogruppo è normale. Segue che non è semplice.

Un altro esempio può essere $\mathcal{S}_6$. Il sottogruppo alterno A_6 è normale in $\mathcal{S}_6$ perché è il nucleo dell'omomorfismo *segno della permutazione*. Infine

$$|\mathcal{S}_6| = 6! = 720.$$

Esercizio 4. Un sottogruppo di $\mathcal{S}_4$ di ordine 8 è un 2-Sylow. Per il secondo teorema di Sylow, tutti i 2-Sylow sono coniugati, dunque un sottogruppo di ordine 8 è abeliano se e solo se lo sono tutti i sottogruppi di ordine 8. Il coniugio infatti è un omomorfismo, e quindi preserva l'abelianità.

L'esercizio quindi può essere risolto trovando un sottogruppo di ordine 8 e mostrando che non è abeliano. Ricordiamo la struttura degli elementi di $\mathcal{S}_4$. Nella seguente tabella abbiamo la struttura ciclica delle permutazioni e il numero di elementi aventi quella struttura ciclica.

()	1
(xx)	6
(xx)(xx)	3
(xxx)	8
(xxxx)	6

Costruiamo il sottogruppo H partendo da (1234).

- $(1234) \in H \implies$
$$(13)(24), (1432) \in H.$$
- Se $(12)(34) \in H$, allora
$$(1234) \circ (12)(34) = (24) \in H.$$
- Se $(14)(23) \in H$, allora
$$(1234) \circ (14)(23) = (13) \in H.$$

Siccome
$$\{e, (13), (24), (12)(23), (14)(23), (13)(24), (1234), (1432)\}$$
sono 8 elementi, e (si può verificare a mano facilmente che) questo sottoinsieme rispetta gli assiomi di gruppo, allora H è un sottogruppo di $\mathcal{S}_4$ di ordine 8.

Ma H non è abeliano, infatti

$$(13) \circ (1234) = (14)(23) \neq (12)(34) = (1234) \circ (13).$$

Da questo segue la tesi.

Osservazione. È importante notare che questa costruzione è scritta a posteriori, e funziona perché sono stati fatti vari tentativi. Ad esempio uno poteva provare ad inserire (12) in H. Ma

$$(12) \in H \implies (1234) \circ (12) = (234) \in H$$

che è assurdo perché essendo H un 2-Sylow ha solo elementi di ordine una potenza di 2. Da cui $(12) \notin H$. E così via.

Esercizio 5. Consideriamo due elementi di D, (g, g) e (h, h). L'elemento

$$(g, g)(h, h)^{-1} = (g, g)(h^{-1}, h^{-1}) = (gh^{-1}, gh^{-1})$$

è in D, pertanto D è un sottogruppo di $G \times G$.

Mostriamo la doppia implicazione.

$$D \trianglelefteq G \times G \iff G \text{ abeliano}$$

($\Leftarrow$): Se G è abeliano, anche $G \times G$ lo è, e quindi ogni sottogruppo è normale.

($\Rightarrow$): Vogliamo mostrare che $\forall g, h \in G$,

$$gh = hg.$$

Consideriamo l'elemento $(g, g) \in D$ e coniughiamolo con l'elemento $(g, h) \in G$.

$$(g, h)^{-1}(g, g)(g, h) = (g^{-1}, h^{-1})(g, g)(g, h) = (g^{-1}gg, h^{-1}gh) = (g, h^{-1}gh).$$

Poiché D è normale, $(g, h^{-1}gh) \in D$. Segue che, per la definizione di D

$$g = h^{-1}gh.$$

E riordinando l'equazione si ottiene

$$hg = gh.$$

Dall'arbitrarietà di g e h segue la tesi.

Esercizio 6. Il terzo teorema di Sylow dice che, se $|G| = p^n m$, con p e m coprimi, valgono

- $n_p \mid m$,
- $n_p \equiv 1 \pmod{p}$,

- $n_p = [G : N_G(P)]$,

dove n_p è il numero dei p-Sylow di G e P è uno di questi p-Sylow.

Applicando questo teorema a $|G| = pq$ si ottiene che:

1) $n_p \mid q$ e $n_p \equiv 1 \pmod{p}$,

2) $n_q \mid p$ e $n_q \equiv 1 \pmod{p}$.

La condizione 1) è stringente, infatti implica $n_p = 1$. La condizione 2) invece dice solo che

$$n_q = 1 \quad \text{oppure} \quad n_q = p.$$

Supponiamo, se possibile, che n_q sia 1. Avremmo due Sylow, pS e qS, entrambi normali in G, senza intersezione e tali che $|pS| \cdot |qS| = |G|$. Ciò darebbe quindi che

$$G = pS \times qS.$$

Essendo pS e qS di ordine primo, essi sono ciclici e quindi abeliani. Ciò implicherebbe G abeliano ※.

n_q quindi non può essere 1, e deve essere p. Sempre dal punto 2) si ha quindi, per qualche k,

$$p = n_q = kq + 1.$$

Cioè $p - 1 = kq$, e quindi $q \mid p - 1$.

Esercizio 7. Bisogna scomporre i due interi di gauss e per scomporli si usa la tecnica della norma. Scomponiamo $20 + 35i$. Per prima cosa

$$20 + 35i = 5(4 + 7i) = (2 + i)(2 - i)(4 + 7i).$$

La norma di $4 + 7i$ è

$$|4 + 7i| = 16 + 49 = 65 = 5 \cdot 13.$$

Quindi si scompone nel prodotto di due numeri, uno a norma 5 e uno a norma 13. Gli interi di Gauss a norma 5 sono

$2 + i$	$2 - i$
$-1 + 2i$	$1 + 2i$
$-2 - i$	$-2 + i$
$1 - 2i$	$-1 - 2i$

mentre gli interi di Gauss a norma 13 sono

$7 + 4i$	$7 - 4i$
$-4 + 7i$	$4 + 7i$
$-7 - 4i$	$-7 + 4i$
$4 - 7i$	$-4 - 7i$

Andando per tentativi si trova che

$$20 + 35i = (2 + i)^2(2 - i)(3 + 2i).$$

Allo stesso modo si trova

$$10 - 45i = 5(2 - 9i)$$

con $|2 - 9i| = 5 \cdot 17$. Elencando ancora una volta tutti gli interi di Gauss a norma 17 e andando a tentativi si ottiene

$$10 - 45i = (2 + i)^2(2 - i)(-1 - 4i).$$

A questo punto, siccome $\mathbb{Z}[i]$ è un dominio a ideali principali, nello specifico euclideo, si ha che

$$I = (20 + 35i, 10 - 45i) = (MCD(20 + 35i, 10 - 45i)) = ((2 + i)^2(2 - i)).$$

Gli ideali primi che lo contengono pertanto sono

$$J_1 = (2 + i) \quad \text{e} \quad J_2 = (2 - i).$$

Esercizio 8. Seguendo il suggerimento, si cerca un omomorfismo naturale

$$\phi : N_G(H) \to \mathrm{Aut}(H)$$

Per un gruppo G qualiasi e $H \leq G$ qualsiasi. L'omomorfismo cercato è quello che prende un elemento $g \in N_G(H)$ e vi associa l'automorfismo del coniugio, i.e. per $g \in N_G(H)$ e $h \in H$,

$$\phi(g)(h) = g^{-1}hg.$$

Osservazione. Il nucleo di questo omomorfismo è esattamente il centralizzatore di H. Infatti $g \in \ker\phi$ implica che

$$\phi(g)(h) = g^{-1}hg = h \quad \forall h \in H,$$

e ciò implica

$$hg = gh \quad \forall h \in H,$$

che è la definizione di elemento del centralizzatore.

Osservazione. Dall'osservazione di prima segue che

$$N_G(H)/C_G(H) \cong \mathrm{Aut}(H).$$

Per entrare nel merito dell'esercizio ora, si considera G il gruppo nell'ipotesi e $H = N$. Poiché N è normale,

$$N_G(N) = G.$$

Da ciò, per la seconda osservazione, segue

$$G/C_G(N) \cong \mathrm{Aut}(N).$$

Osservazione. Gli elementi di $\mathrm{Aut}(N)$ sono omomorfismi bigettivi, quindi più in generale sono almeno funzioni bigettive, cioè permutazioni. Da ciò segue che

$$|\mathrm{Aut}(N)| \leq |\mathcal{S}_N|.$$

Inoltre, siccome ogni omomorfismo lascia 1_N fisso, vale anche la stima più forte

$$|\mathrm{Aut}(N)| \leq |\mathcal{S}_{N\setminus\{1_N\}}| = (|N|-1)!.$$

Ricapitolando

$$|G/C_G(N)| = |\mathrm{Aut}(N)| \leq (|N|-1)!$$

e

$$|G/C_G(N)| = |G|/|C_G(N)|.$$

Sfruttando il fatto che $C_G(N) \subseteq N$ e riordinando segue

$$|G| \leq (|N|-1)! \cdot |C_G(N)| \leq (|N|-1)! \cdot |N| = |N|!$$

Esercizio 9. La dimostrazione sarà divisa in 6 passi e l'obiettivo sarà dimostrare che ogni $x \in A$, x è centrale.

1) Per prima cosa

$$ab = 0 \implies ba = 0.$$

Infatti, $ba = (ba)^3 = b\,ab\,ab\,b = 0$.

2.a) Sia $c \in A$, se $c = cc$ allora c è centrale. Infatti, per un qualsiasi $x \in A$,

$$cx - cx = 0 \implies cx - ccx = 0 \implies c(x - cx) = 0 \implies (x - cx)c = 0 \implies xc = cxc.$$

E ancora

$$xc - xc = 0 \implies xc - xcc = 0 \implies (x - xc)c = 0 \implies c(x - xc) = 0 \implies cx = cxc.$$

2.b) Sia $x \in A$, xx è centrale. Infatti $xx = xx \cdot xx$ e la centralità segue dal punto $(2.a)$.

3.a) Sia $c \in A$, se $cc = 2c$ allora c è centrale. Infatti,

$$c = ccc = 2cc = cc + cc.$$

cc è centrale per $(2.b)$, e c è centrale perché somma di centrali.

3.b) Sia $x \in A$, $x + xx$ è centrale. Infatti,

$$(x + xx)(x + xx) = xx + xxx + xxx + xxxx = xx + x + x + xx = 2x + 2xx.$$

E per il punto $(3.a)$, $x + xx$ è centrale.

4) A questo punto, sia $x \in A$ qualsiasi,

$$x = (x + xx) - xx.$$

x è somma di elementi centrali, e quindi è centrale.