Corso di Algebra 1 - a.a. 2024-2025

Prova scritta del 17/09/2025

1. Sia G il gruppo $A_4 \times D_4$.
   (a) Dato un intero positivo n, dimostrare che G contiene un elemento di ordine n se e solo se n divide 12.
   (b) Dimostrare che gli elementi il cui ordine è una potenza di 2 formano un sottogruppo normale di G.
   (c) Dimostrare che G non contiene un sottogruppo isomorfo a S_3.
   (d) Esiste un sottogruppo normale di ordine 6 di G?
2. Sia $f := 6X^3 + 2$.
   (a) Stabilire se $\mathbb{Z}[X]/(f)$ è un dominio.
   (b) Trovare un numero primo p tale che $\mathbb{Z}[X]/(p, f)$ sia un dominio ma non un campo.
   (c) Trovare un numero primo p tale che $\mathbb{Z}[X]/(p, f)$ sia un campo.
   (d) Trovare un numero primo p tale che $\mathbb{Z}[X]/(p, f)$ sia isomorfo al prodotto di due campi.

Soluzioni

1. Ricordiamo che gli elementi non banali di A_4 sono i 3-cicli (di ordine 3) e le coppie di 2-cicli disgiunti (di ordine 2); inoltre l'insieme V_4 costituito dalle 3 coppie di 2-cicli disgiunti e dall'elemento neutro è un sottogruppo normale di A_4. In D_4, invece, R e R^3 hanno ordine 4, mentre tutti gli altri elementi non banali (cioè R^2 e R^iS per $i = 0, 1, 2, 3$) hanno ordine 2.

   (a) Dato $g = (a, b) \in G$, si ha $\mathrm{ord}(g) = \mathrm{mcm}(\mathrm{ord}(a), \mathrm{ord}(b))$. Poiché i possibili valori di $\mathrm{ord}(a)$ (con $a \in A_4$) sono 1, 2 e 3, mentre quelli di $\mathrm{ord}(b)$ (con $b \in D_4$) sono 1, 2 e 4, i possibili valori di $\mathrm{ord}(g)$ sono 1, 2, 3, 4, 6 e 12, che sono tutti e soli i divisori di 12.

   (b) Indicando con D l'insieme degli elementi di G il cui ordine è una potenza di 2, per quanto visto nel punto precedente è chiaro che $g = (a, b) \in H$ se e solo se $\mathrm{ord}(a) = 1$ o 2, se e solo se $a \in V_4$. Dunque $D = V_4 \times D_4$ è un sottogruppo normale di G perché V_4 lo è di A_4 e D_4 di D_4.

   (c) Per assurdo sia $H \cong S_3$ un sottogruppo di G. Ricordiamo che S_3 contiene 2 elementi di ordine 3 (i 3-cicli), mentre gli altri 3 elementi non banali (i 2-cicli) hanno ordine 2. Dunque esistono $g = (a, b), g' = (a', b') \in H$ tali che $\mathrm{ord}(g) = \mathrm{mcm}(\mathrm{ord}(a), \mathrm{ord}(b)) = 3$ e $\mathrm{ord}(g') = \mathrm{mcm}(\mathrm{ord}(a'), \mathrm{ord}(b')) = 2$. Se ne deduce che $\mathrm{ord}(a) = 3$ e $\mathrm{ord}(a') = 1$ o 2, per cui $a \in A_4 \setminus V_4$ e $a' \in V_4$. Dato che V_4 è un sottogruppo di A_4, questo implica $aa' \in A_4 \setminus V_4$, e pertanto $\mathrm{ord}(aa') = 3$. Essendo $gg' = (aa', bb')$, si ottiene allora $3 \mid \mathrm{ord}(gg') = \mathrm{mcm}(\mathrm{ord}(aa'), \mathrm{ord}(bb'))$. Questo contraddice il fatto che invece dovrebbe essere $\mathrm{ord}(gg') = 2$ (in S_3 il prodotto di un 3-ciclo e di un 2-ciclo è un 2-ciclo).

   (d) No, non esiste. Sia infatti K un sottogruppo di G di ordine 6. Grazie al punto precedente (e ricordando la classificazione dei gruppi di ordine 6, a meno di isomorfismo) K è ciclico, cioè esiste $g = (a, b) \in G$ tale che $K = \langle g \rangle$. Poiché

   $$6 = \#K = \mathrm{ord}(g) = \mathrm{mcm}(\mathrm{ord}(a), \mathrm{ord}(b)),$$

   deve essere $\mathrm{ord}(a) = 3$ (e $\mathrm{ord}(b) = 2$). Quindi a è un 3-ciclo, diciamo $a = (i, j, k)$ con $i, j, k \in \{1, 2, 3, 4\}$ distinti. Posto $a' := (i, j)(k, l)$ (dove l è tale che $\{i, j, k, l\} = \{1, 2, 3, 4\}$), e $g' := (a', 1)$, si ha $g'gg'^{-1} = (a'aa'^{-1}, b) \notin \langle g \rangle = K$ (dunque K non è normale) perché $a'aa'^{-1} = (j, i, l) \notin \langle a \rangle$.

2. (a) $\mathbb{Z}[X]/(f)$ non è un dominio. Infatti l'ideale (f) non è primo perché $f = 2(3X^3 + 1)$ non è irriducibile nel dominio $\mathbb{Z}[X]$ (dato che $2, 3X^3 + 1 \notin \mathbb{Z}[X]^* = \mathbb{Z}^* = \{\pm 1\}$).

   Si osservi che, come conseguenza del terzo teorema di isomorfismo, per ogni numero primo p si ha $\mathbb{Z}[X]/(p, f) \cong \mathbb{Z}/p\mathbb{Z}[X]/(\overline{f})$, dove $\overline{f}$ indica l'immagine di f in $Z/p\mathbb{Z}[X]$.

   (b) Si può prendere $p = 2$. Infatti in tal caso risulta $\overline{f} = \bar{0}$, per cui $\mathbb{Z}[X]/(2, f) \cong \mathbb{Z}/2\mathbb{Z}[X]/(\bar{0}) \cong \mathbb{Z}/2\mathbb{Z}[X]$ è un dominio (essendo $\mathbb{Z}/2\mathbb{Z}$ un dominio) ma non un campo.

   (c) Si può prendere $p = 7$. Infatti in generale $\mathbb{Z}/p\mathbb{Z}[X]/(\overline{f})$ è un campo se e solo se l'ideale $(\overline{f})$ è massimale in $\mathbb{Z}/p\mathbb{Z}[X]$. Poiché $\mathbb{Z}/p\mathbb{Z}[X]$ è un dominio a ideali principali (essendo $\mathbb{Z}/p\mathbb{Z}$ un campo), $(\overline{f})$ è massimale se e solo se $\overline{f}$ è irriducibile in $\mathbb{Z}/p\mathbb{Z}[X]$. Per $p = 7$ si ha $\overline{f} = -X^3 + \bar{2}$, che è irriducibile in $\mathbb{Z}/7\mathbb{Z}[X]$ perché di terzo grado e senza radici in $\mathbb{Z}/7\mathbb{Z}$ (come è immediato verificare).

   (d) Si può prendere $p = 5$. Infatti in tal caso $\overline{f} = X^3 + \bar{2}$ ha la radice $\bar{2}$ in $\mathbb{Z}/5\mathbb{Z}$. Per il teorema di Ruffini $\overline{f}$ è allora divisibile per $g := X - \bar{2}$, e si trova $\overline{f} = gh$ con $h := X^2 + \bar{2}X + \bar{4}$. Sia g (essendo di primo grado) che h (essendo di secondo grado e senza radici in $\mathbb{Z}/5\mathbb{Z}$, come è immediato verificare) sono irriducibili in $\mathbb{Z}/5\mathbb{Z}[X]$, e chiaramente non sono tra loro associati. Dunque (dato che $\mathbb{Z}/5\mathbb{Z}[X]$ è un dominio a ideali principali) (g) e (h) sono ideali massimali distinti, e pertanto $(g) + (h) = \mathbb{Z}/5\mathbb{Z}[X]$. Poiché chiaramente $(\overline{f}) = (g)(h)$, per il teorema cinese del resto generalizzato si ottiene allora $\mathbb{Z}/5\mathbb{Z}[X]/(\overline{f}) \cong K \times L$, dove sia $K := \mathbb{Z}/5\mathbb{Z}[X]/(g)$ che $L := \mathbb{Z}/5\mathbb{Z}[X]/(h)$ sono campi, perché g e h sono irriducibili in $\mathbb{Z}/5\mathbb{Z}[X]$.