Corso di Algebra 1 - a.a. 2023-2024

Prova scritta del 10/06/2024

1. Dato un gruppo finito G, sia

$$t(G) := \min\{k > 0 : G \text{ non contiene elementi di ordine } k\}.$$

   (a) Trovare $n > 0$ tale che $t(\mathbb{Z}/n\mathbb{Z}) = 5$.

   (b) Dimostrare che, se G è ciclico, allora $t(G)$ è una potenza di un numero primo.

   (c) Dimostrare che non esiste $n > 0$ tale che $t(S_n) = 6$.

   (d) Esiste $n > 0$ tale che $t(A_n) = 6$?

2. Dato un intero $n > 1$, sia $f_n := X^n - 2nX - 5$.

   (a) Dimostrare che solo un numero finito di ideali di $\mathbb{Q}[X]$ contiene f_n.

   (b) Trovare tutti gli ideali di $\mathbb{Q}[X]$ contenenti f_3.

   (c) Trovare un valore di n tale che $\mathbb{Q}[X]/(f_n)$ sia un campo.

   (d) Dimostrare che ci sono infiniti ideali di $\mathbb{Z}[X]$ contenenti f_n.

Soluzioni

1. (a) Si può prendere per esempio $n = 12$. Infatti, poiché $\mathbb{Z}/n\mathbb{Z}$ contiene elementi di ordine k se e solo se $k \mid n$, va bene qualunque n tale che $1, 2, 3, 4 \mid n$ ma $5 \nmid n$.

   (b) Indicando con n l'ordine di G (quindi $G \cong \mathbb{Z}/n\mathbb{Z}$), come già detto nel punto precedente G contiene elementi di ordine k se e solo se $k \mid n$, e dunque $t(G) = \min\{k > 0 : k \nmid n\}$. Se per assurdo $t(G)$ non fosse una potenza di un numero primo, esisterebbero due interi coprimi a e b tali che $t(G) = ab$ e $1 < a, b < t(G)$. Si avrebbe allora $a \mid n$ e $b \mid n$, da cui segue l'assurdo $\mathrm{mcm}(a, b) = ab = t(G) \mid n$.

   (c) Ricordiamo preliminarmente che l'ordine di una permutazione è il minimo comune multiplo delle lunghezze dei cicli che compaiono nella sua scrittura come prodotto di cicli disgiunti. Chiaramente $t(S_n) \leq 5$ per $n \leq 4$, dato che in tal caso S_n non contiene elementi di ordine 5. D'altra parte $t(S_n) \geq 7$ per $n \geq 5$, perché in tal caso S_n contiene elementi di ordine k sia per $k = 1, \ldots, 5$ (per esempio il k-ciclo $(1, \ldots, k)$) che per $k = 6$ (per esempio $(1, 2, 3)(4, 5)$).

   (d) Sì, si ha $t(A_6) = 6$. Infatti, ricordando che una permutazione è pari se e solo se nella sua scrittura come prodotto di cicli disgiunti ci sono un numero pari di cicli di lunghezza pari, si trova che A_6 contiene elementi di ordine 1 (l'elemento neutro), 2 (per esempio $(1, 2)(3, 4)$), 3 (per esempio $(1, 2, 3)$), 4 (per esempio $(1, 2, 3, 4)(5, 6)$) e 5 (per esempio $(1, 2, 3, 4, 5)$). Per concludere basta osservare che invece A_6 non contiene elementi di ordine 6, perché gli unici elmenti di ordine 6 di S_6 sono i 6-cicli e i prodotti di un 3-ciclo e di un 2-ciclo disgiunti, ed entrambi sono dispari.

2. (a) Poiché $\mathbb{Q}[X]$ è un dominio a ideali principali (essendo $\mathbb{Q}$ un campo), gli ideali di $\mathbb{Q}[X]$ contenenti f_n sono tutti e soli della forma (g) con $g \in \mathbb{Q}[X]$ tale che $g \mid f_n$. Inoltre due elementi di $\mathbb{Q}[X]$ generano lo stesso ideale se e solo se sono associati (dato che $\mathbb{Q}[X]$ è un dominio). Se ne deduce che gli ideali di $\mathbb{Q}[X]$ contenenti f_n sono in corrispondenza biunivoca con i divisori di f_n a meno di associati. Tenendo conto che $\mathbb{Q}[X]$ è anche un dominio a fattorizzazione unica (come ogni dominio a ideali principali) e $f_n \neq 0$, è chiaro che tali divisori sono in numero finito. Più esplicitamente, se $f_n = \prod_{i=1}^{k} p_i^{l_i}$ con i p_i elementi irriducibili a due a due non associati e gli l_i interi positivi, allora a meno di associati ci sono

$\prod_{i=1}^{k}(l_i+1)$ divisori di f_n (cioè quelli della forma $\prod_{i=1}^{k} p_i^{l'_i}$ con $0 \leq l'_i \leq l_i$ per ogni $i = 1, \ldots, k$).

(b) Come spiegato nel punto precedente basta trovare la fattorizzazione di $f_3 = X^3 - 6X - 5$ in $\mathbb{Q}[X]$. Per il criterio della radice razionale le eventuali radici razionali di f_3 possono essere solo $\pm 1, \pm 5$. Dato che $f_3(-1) = 0$, $f_3(1), f_3(5), f_3(-5) \neq 0$, l'unica radice razionale di f_3 è -1 e risulta $f_3 = (X+1)(X^2 - X - 5)$ con $X^2 - X - 5$ irriducibile (perché di secondo grado e senza radici razionali). Dunque gli ideali di $\mathbb{Q}[X]$ contenenti f_3 sono $(1) = \mathbb{Q}[X]$, $(X+1)$, $(X^2 - X - 5)$ e (f_3).

(c) L'anello $\mathbb{Q}[X]/(f_n)$ è un campo se e solo se l'ideale (f_n) è massimale in $\mathbb{Q}[X]$ se e solo se (essendo $\mathbb{Q}[X]$ un dominio a ideali principali) f_n è irriducibile in $\mathbb{Q}[X]$. Si può allora prendere per esempio $n = 5$, dato che $f_5 = X^5 - 10X - 5$ è irriducibile in $\mathbb{Z}[X]$ (quindi anche in $\mathbb{Q}[X]$) per il criterio di Eisenstein relativo al numero primo 5.

(d) Per ogni numero primo p sia $I_p := (p, f_n)$ in $\mathbb{Z}[X]$. Poiché i numeri primi sono infiniti, basta dimostrare che tali ideali di $\mathbb{Z}[X]$ sono a due a due distinti. Supponiamo per assurdo che esistano due numeri primi p e q tali che $p \neq q$ e $I_p = I_q$. In particolare $p, q \in I_p = I_q$, e quindi, dato che esistono $a, b \in \mathbb{Z}$ tali che $pa + qb = 1$ (essendo p e q due interi coprimi), si avrebbe $1 = pa + qb \in I_p$, cioè $I_p = \mathbb{Z}[X]$. L'anello quoziente $\mathbb{Z}[X]/I_p$ sarebbe allora banale, ma, per il terzo teorema di isomorfismo,

$$\mathbb{Z}[X]/I_p \cong \big(\mathbb{Z}[X]/(p)\big)/(\overline{f}_n) \cong \mathbb{Z}/p\mathbb{Z}[X]/(\overline{f}_n)$$

e si otterrebbe $(\overline{f}_n) = \mathbb{Z}/p\mathbb{Z}[X]$, cioè $\overline{f}_n \in \mathbb{Z}/p\mathbb{Z}[X]^* = \mathbb{Z}/p\mathbb{Z}^*$. Questo però non è vero, visto che $\deg(\overline{f}_n) = \deg(f_n) = n > 0$ (essendo f_n monico).