Corso di Algebra - a.a. 2006-2007

Prova scritta del 24.9.2007

1. Dimostrare che un gruppo G è abeliano se e solo se per ogni sottogruppo H di G si ha $Z(H) = H \cap Z(G)$ (ricordiamo che, per ogni gruppo Γ, $Z(\Gamma)$ denota il centro di Γ).

2. Per quali n esiste un elemento di ordine n in S_7?

3. Sia A un dominio, e siano (a) e (b) ideali principali in A. Supponiamo che a non divida b e che b non divida a. Mostrare che $(a) \cap (b)$ non è un ideale primo.

4. Un anello A si dice *ridotto* se per ogni elemento non nullo $a \in A$ e per ogni intero positivo n si ha $a^n \neq 0$.

   Sia A un dominio a fattorizzazione unica, siano $p_1, \ldots, p_k$ elementi irriducibili distinti di A ed $e_1, \ldots, e_k$ interi positivi. Dimostrare che l'anello quoziente $A/(\prod_{i=1}^k p_i^{e_i})$ è ridotto se e solo se $e_1 = \cdots = e_k = 1$.

5. Sia P il polinomio $X^5 + 6X^3 - 15X^2 - 3$.

   (a) Fattorizzare P in $\mathbb{Q}[X]$.

   (b) Detta α una radice di P, determinare il grado di α su $\mathbb{Q}[\sqrt{2}]$.

Soluzioni

1. Se G è abeliano, $Z(G) = G$, quindi $H \cap Z(G) = H$ per ogni sottogruppo H. D'altra parte, $Z(H) = H$ perchè H è abeliano. Viceversa, supponiamo che $H \cap Z(G) = Z(H)$ per ogni sottogruppo H di G. Se $g \in G$ e H è il sottogruppo ciclico da esso generato, l'ipotesi dice che $H \cap Z(G) = H$ perchè H è abeliano, e quindi uguale al suo centro. In altre parole, $H \subset Z(G)$. Dato che g 'è arbitrario, questo mostra che $G \subset Z(G)$, cioè che G è abeliano.

2. 1, 2, 3, 4, 5, 6, 7 (cicli di lunghezza 1, ..., 7), 10 (prodotto di cicli disgiunti di lunghezze 2 e 5), 12 (prodotto di cicli disgiunti di lunghezze 3 e 4).

3. Il prodotto ab appartiene a $(a) \cap (b)$. D'altra parte $a \notin (b)$ perchè non è divisibile per b, e quindi non appartiene a $(a) \cap (b)$, mentre $b \notin (a)$ perchè non è divisibile per a, e quindi non appartiene a $(a) \cap (b)$. Quindi $(a) \cap (b)$ non è primo.

4. Se $e = \max\{e_i : i = 1, \ldots, k\} > 1$, $\prod_{i=1}^k p_i \notin (\prod_{i=1}^k p_i^{e_i})$, ma $\prod_{i=1}^k p_i^e \in (\prod_{i=1}^k p_i^{e_i})$, quindi, indicando con a la classe di $\prod_{i=1}^k p_i$ in $A/(\prod_{i=1}^k p_i^{e_i})$, $a \neq 0$ ma $a^e = 0$. Se $e_i = 1$ per ogni i e $x \in A$ non è nullo, possiamo scrivere $x = \prod_{i=1}^k p_i^{d_i} \prod_{j=1}^h q_j^{f_j}$, dove i q_j sono primi diversi dai p_i, $d_i \geq 0$ per ogni i, e $f_j \geq 0$ per ogni j. Allora $x^n = \prod_{i=1}^k p_i^{nd_i} \prod_{j=1}^h q_j^{nf_j}$ è nullo modulo $(\prod_{i=1}^k p_i^{e_i})$ se e solo se $nd_i \geq e_i = 1$ per ogni i, cioè se e solo se $d_i \geq 1 = e_i$ per ogni i, cioè se e solo se x è nullo modulo $(\prod_{i=1}^k p_i^{e_i})$.

5. La riduzione di P modulo 2 è uguale a $X^5 + X^2 + 1$. Questo polinomio non ha radici in $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ e non è divisibile per l'unico polinomio irriducibile di grado 2 in $\mathbb{F}_2[X]$, cioè per $X^2 + X + 1$, e dunque è irriducibile. Quindi P è irriducibile in $\mathbb{Z}[X]$, e dunque in $\mathbb{Q}[X]$. Ne segue che $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 5$. D'altra parte

$$\begin{aligned}
\left[\mathbb{Q}\left[\alpha, \sqrt{2}\right] : \mathbb{Q}\right] &= \left[\mathbb{Q}\left[\alpha, \sqrt{2}\right] : \mathbb{Q}\left[\sqrt{2}\right]\right] \left[\mathbb{Q}\left[\sqrt{2}\right] : \mathbb{Q}\right] \\
&= 2\left[\mathbb{Q}\left[\alpha, \sqrt{2}\right] : \mathbb{Q}\left[\sqrt{2}\right]\right] \\
&= \left[\mathbb{Q}\left[\alpha, \sqrt{2}\right] : \mathbb{Q}[\alpha]\right] \left[\mathbb{Q}[\alpha] : \mathbb{Q}\right] \\
&= 5\left[\mathbb{Q}\left[\alpha, \sqrt{2}\right] : \mathbb{Q}[\alpha]\right]
\end{aligned}$$

Dunque il doppio di $\left[\mathbb{Q}\left[\alpha, \sqrt{2}\right] : \mathbb{Q}\left[\sqrt{2}\right]\right]$ è divisibile per 5. Dato che $\left[\mathbb{Q}\left[\alpha, \sqrt{2}\right] : \mathbb{Q}\left[\sqrt{2}\right]\right]$ è minore o uguale a 5, la sola possibilità è che sia uguale a 5.