Corso di Algebra - a.a. 2008-2009

Prova scritta del 17.2.2009

1. Sia G un gruppo e $A = \{g^2 : g \in G\}$.
   (a) Dimostrare che, se G è abeliano, allora A è un sottogruppo di G.
   (b) Dimostrare che, se G è finito di ordine dispari, allora $A = G$.

2. Esiste un sottogruppo del gruppo diedrale D_6 che sia isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?

3. Sia A un anello commutativo non nullo. Poniamo

$$D(A) = \{a \in A : a = 0 \text{ oppure } a \text{ è divisore di zero}\}.$$

   Dato un intero $n > 1$, dimostrare che $D(\mathbb{Z}/n\mathbb{Z})$ è un ideale di $\mathbb{Z}/n\mathbb{Z}$ se e solo se n è una potenza di un numero primo.

4. Dimostrare che $\mathbb{Q}$ è l'unico sottocampo di $\mathbb{Q}[X]$.

5. Fattorizzare il polinomio $X^3 - X + 6$ in $\mathbb{Q}[X]$ e determinare il grado del suo campo di spezzamento K su $\mathbb{Q}$. Si dica inoltre se il polinomio $X^2 - 2$ è irriducibile in $K[X]$.

Soluzioni

1. (a) Se G è abeliano, $g \mapsto g^2$ è un omomorfismo, dato che $(gh)^2 = ghgh = gghh = g^2h^2$. L'insieme A è l'immagine di questo omomorfismo, e quindi è un sottogruppo.
   (b) Sia g un elemento di G. Il suo ordine divide quello di G, e quindi è dispari, diciamo uguale a $n = 2k+1$ per qualche intero k. Allora $g = gg^n = g^{2k+2} = (g^{k+1})^2$.

2. Sì. Il gruppo D_6 è generato da elementi α e β, dove α ha ordine 6, β ha ordine 2, e $\alpha\beta = \beta\alpha^5$. Ne segue che $\gamma = \alpha^3$ ha ordine 2 e commuta con β. Il sottogruppo generato da β e γ è dunque $\{1, \beta, \gamma, \beta\gamma\}$, che ha ordine 4. Dato che β, γ e $\beta\gamma$ hanno ordine 2, questo sottogruppo è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. Notiamo intanto che $D(A)$ è l'insieme degli $a \in A$ tali che esista $b \in A$, $b \neq 0$, tale che $ab = 0$. Ora poniamo $A = \mathbb{Z}/n\mathbb{Z}$. Per ogni intero h indichiamo con $\overline{h}$ la sua classe in A. Se $n = p^r$, con r primo, $\overline{h}$ appartiene dunque a $D(A)$ se e solo se c'è un intero k, non divisibile per p^r, ma tale che lo sia hk. Questo significa che $\overline{h} \in D(A)$ se e solo se h è divisibile per p, cioè che $D(A)$ è l'ideale principale generato da $\overline{p}$. Supponiamo invece che n non sia potenza di un primo. Possiamo dunque scrivere $n = km$, dove k e m sono primi fra loro e diversi da ± 1. Notiamo che $\overline{k}$ e $\overline{m}$ non sono nulli, ma lo è il loro prodotto; sono dunque divisori di zero. Se mostriamo che $\overline{k} + \overline{m}$ non appartiene a $D(A)$ avremo mostrato che quest'ultimo non è un ideale. Supponiamo che $\overline{\ell}(\overline{k} + \overline{m}) = 0$, cioè che $\ell(k+m)$ sia divisibile per km. Ne segue che k divide ℓm, e dunque divide ℓ, e allo stesso modo che m divide ℓ. Dato che k e m sono primi fra loro, ne concludiamo che km divide ℓ, cioè che $\overline{\ell} = 0$.

4. Se $P(X) \in \mathbb{Q}[X]$ è invertibile deve avere grado nullo. Quindi ogni sottocampo K di $\mathbb{Q}[X]$ è sottocampo di $\mathbb{Q}$. Dato che $1 \in K$, ogni intero positivo $n = 1 + 1 + \cdots + 1$ appartiene a K, e lo stesso vale per il suo opposto $-n$. Quindi $\mathbb{Z} \subset K$. Poi, dato che K è un campo, $n^{-1} \in K$ per ogni intero $n \neq 0$, e anche ogni frazione mn^{-1} appartiene a K. Dunque $K = \mathbb{Q}$.

5. $X^3 - X + 6 = (X+2)(X^2-2X+3)$. Il polinomio X^2-2X+3 ha discriminante negativo, quindi non ha radici reali. In particolare è irriducibile in $\mathbb{Q}[X]$. Ne concludiamo che $[K : \mathbb{Q}] = 2$. Il polinomio $X^2 - 2$ è irriducibile se e solo se non ha radici in K. Dunque se fosse riducibile $\sqrt{2}$ apparterrebbe a K. In altre parole K conterrebbe $\mathbb{Q}[\sqrt{2}]$. D'altra parte $K \neq \mathbb{Q}[\sqrt{2}]$ perchè $X^2 - 2X + 3$ non ha radici reali. Quindi

$$[K : \mathbb{Q}] = \big[K : \mathbb{Q}[\sqrt{2}]\big]\big[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\big] = \big[K : \mathbb{Q}[\sqrt{2}]\big] \cdot 2 > 2\,,$$

un assurdo.