Corso di Algebra - a.a. 2008-2009

Prova scritta del 23.9.2009

1. Sia G un gruppo non banale. Dimostrare che G è ciclico di ordine un numero primo se e solo se gli unici sottogruppi di G sono $\{1\}$ e G.
2. Dimostrare che A_4 non contiene sottogruppi di ordine 6.
3. Sia $f\colon A \to B$ un omomorfismo di anelli commutativi e siano a, b, c elementi di A tali che valga $(a, b) = (c)$ come ideali di A. Dimostrare che allora $(f(a), f(b)) = (f(c))$ come ideali di B.
4. Sia A un anello commutativo con $1 \neq 0$. Dimostrare che esistono $a, b \in A$ tali che $a \neq 0$, $b \neq 1$ e $ab = a$ se e solo se A non è un dominio di integrità.
5. Sia α una radice del polinomio $X^4 - 9X + 3 \in \mathbb{Q}[X]$.
   (a) Si dimostri che $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$;
   (b) si determini $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Soluzioni

1. Se G è ciclico di ordine p primo e H è un suo sottogruppo, l'ordine di H divide l'ordine di G, cioè p. Quindi l'ordine di H può essere 1 o p. Nel primo caso $H = \{1\}$, nel secondo $H = G$.

   Supponiamo ora che G non abbia sottogruppi tranne $\{1\}$ e G. Se $G = \{1\}$ non c'è niente da dimostrare. Se invece G contiene un elemento $g \neq 1$, indichiamo con H il sottogruppo generato da g. Dato che $H \ni g$, $H \neq \{1\}$. Quindi, per ipotesi, $H = G$. Questo mostra che G è ciclico. Se G fosse infinito sarebbe isomorfo a $\mathbb{Z}$, e quindi avrebbe sottogruppi di qualsiasi indice. Dunque G deve essere finito. Se l'ordine di G, cioè l'ordine di g, non fosse primo, e fosse quindi della forma hk con $h, k > 1$, g^h genererebbe un sottogruppo di G di ordine k, quindi diverso sia da $\{1\}$ che da G, contro l'ipotesi.

2. Un eventuale sottogruppo H di ordine 6 avrebbe indice 2, quindi sarebbe normale. Inoltre, H dovrebbe essere isomorfo a S_3 o ciclico, e quindi conterrebbe easttamente due elementi di ordine 3. Gli elementi di ordine 3 in A_4 sono i 3-cicli. Supponiamo che $\tau = (a\ b\ c) \in H$, e sia d l'elemento di $\{1, 2, 3, 4\}$ diverso da a, b, c. La permutazione $\sigma = (a\ b)(c\ d)$ appartiene a A_4, e
$$\sigma^{-1}\tau\sigma = (a\ b)(c\ d)(a\ b\ c)(a\ b)(c\ d) = (a\ d\ b)$$
   Dato che H è normale, $(a\ d\ b)$ appartiene a H. Ma $(a\ d\ b)$ è diversa sia da τ che da $\tau^{-1} = (a\ c\ b)$. Dunque H contiene almeno tre elementi di ordine 3, in contraddizione con quanto visto sopra.

3. Esistono $\alpha, \beta \in A$ tali che $c = \alpha a + \beta b$. Quindi $f(c) = f(\alpha)f(a) + f(\beta)f(b)$ e dunque $f(c) \in (f(a), f(b))$ o, che è lo stesso, $(f(c)) \subset (f(a), f(b))$. Viceversa, esiste $r \in A$ tale che $a = rc$. Ne segue che $f(a) = f(r)f(c) \in (f(c))$. Allo stesso modo si mostra che $f(b) \in (f(c))$. Dunque $(f(a), f(b)) \subset (f(c))$.

4. Se esistono a e b come nell'enunciato, $0 = ab - a = a(b-1)$. Dato che a e $b-1$ non sono nulli per ipotesi, sono divisori di zero. Viceversa, supponiamo che A non sia un dominio di integrità, cioè che esistano $e, f \in A$ tali che $e \neq 0$, $f \neq 0$, ma $ef = 0$. Allora $e(f+1) = ef + e = e$. Dato che $e \neq 0$ e $f + 1 \neq 1$ poiché $f \neq 0$, basta prendere $a = e$ e $b = f + 1$.

5. (a) $\alpha^4 - 9\alpha + 3 = 0$, quindi $\alpha = \frac{1}{9}\big((\alpha^2)^2 + 3\big) \in \mathbb{Q}[\alpha^2]$.

   (b) Il polinomio $X^4 - 9X + 3$ è irriducibile in $\mathbb{Q}[X]$ o, equivalentemente, in $\mathbb{Z}[X]$. Questo segue immediatamente dal criterio di Eisenstein. In alternativa si può ridurre il polinomio modulo 2, e osservare che il polinomio ottenuto, cioè $X^4 + X + 1$, è irriducibile in $\mathbb{Z}/2\mathbb{Z}[X]$. Infatti questo polinomio non ha radici in $\mathbb{Z}/2\mathbb{Z}$ e non è divisibile per il solo polinomio irriducibile di grado 2 in $\mathbb{Z}/2\mathbb{Z}$, cioè per $X^2 + X + 1$, dato che $(X^2 + X + 1)^2 = X^4 + X^2 + 1$. Dunque $X^4 - 9X + 3$ è il polinomio minimo di α su $\mathbb{Q}$, e quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ è pari al suo grado, cioè a 4.