Corso di Algebra - a.a. 2008-2009

Prova scritta del 2.2.2009

1. (a) Sia G un gruppo finito. Dimostrare che l'ordine di ogni elemento di $G \times G$ divide l'ordine di G.
   (b) Dimostrare che $D_n \times D_n$ contiene un elemento di ordine $2n$ se e solo se n è dispari.
2. Dimostrare che i gruppi D_{12} e S_4 non sono isomorfi.
3. Sia $f\colon A \to B$ un omomorfismo di anelli e siano I e J due ideali di B.
   (a) Dimostrare che $f^{-1}(I) + f^{-1}(J) \subset f^{-1}(I + J)$.
   (b) Dimostrare che $f^{-1}(I) + f^{-1}(J) = f^{-1}(I + J)$ se f è suriettivo.
4. Sia A un anello commutativo finito. Dimostrare che ogni ideale primo di A è massimale.
5. Sia $F(X)$ il polinomio $X^3 + 12$.
   (a) Trovare un numero primo p tale che $F(X)$ sia irriducibile in $\mathbb{Z}/p\mathbb{Z}[X]$.
   (b) Determinare il grado del campo di spezzamento di $F(X)$ su $\mathbb{Q}$.

Soluzioni

1. (a) Detto m l'ordine di G, per il teorema di Lagrange $g^m = 1$ per ogni $g \in G$. Allora per ogni $(g_1, g_2) \in G \times G$ si ha
   $$(g_1, g_2)^m = (g_1^m, g_2^m) = (1, 1),$$
   per cui l'ordine di (g_1, g_2) divide m.
   (b) D_n contiene un sottogruppo ciclico di ordine n generato da una rotazione ρ, mentre tutti gli altri elementi sono riflessioni di ordine 2. Dunque se n è pari $\mathrm{ord}(g)|n$ per ogni $g \in G$, e quindi anche
   $$\mathrm{ord}((g_1, g_2)) = \mathrm{mcm}(\mathrm{ord}(g_1), \mathrm{ord}(g_2))|n$$
   per ogni $(g_1, g_2) \in D_n \times D_n$; questo mostra in particolare che $D_n \times D_n$ non contiene elementi di ordine $2n$ in questo caso. Se invece n è dispari, indicando con σ una riflessione di D_n, si ha
   $$\mathrm{ord}((\rho, \sigma)) = \mathrm{mcm}(\mathrm{ord}(\rho), \mathrm{ord}(\sigma)) = \mathrm{mcm}(n, 2) = 2n.$$
2. D_{12} contiene un sottogruppo ciclico di ordine 12, e quindi elementi di ordine 12. Gli elementi di S_4 invece, oltre all'identità, sono le trasposizioni, i prodotti di due trasposizioni disgiunte, i 3-cicli e i 4-cicli; essi hanno ordini 2, 2, 3, 4.
3. (a) Un elemento di $f^{-1}(I) + f^{-1}(J)$ è della forma $a + b$ con $a \in f^{-1}(I)$ (cioè $f(a) \in I$) e $b \in f^{-1}(J)$ (cioè $f(b) \in J$). Essendo $f(a + b) = f(a) + f(b) \in I + J$, concludo che $a + b \in f^{-1}(I + J)$.

(b) Resta da vedere che, se f è suriettivo, $f^{-1}(I+J) \subset f^{-1}(I)+f^{-1}(J)$. Se $a \in f^{-1}(I+J)$ (cioè $f(a) \in I+J$), per definizione esistono $b' \in I$ e $c' \in J$ tali che $f(a) = b'+c'$. Per la suriettività di f esiste $b \in A$ tale che $f(b) = b'$, e pongo $c = a-b \in A$. Allora $a = b+c \in f^{-1}(I)+f^{-1}(J)$, dato che $b \in f^{-1}(I)$ (perché $f(b) = b' \in I$) e $c \in f^{-1}(J)$ (perché $f(c) = f(a)-f(b) = c' \in J$).

4. Sia A un anello commutativo finito e sia P un suo ideale. Allora A/P è un dominio. Ma ogni dominio finito è un campo. Quindi P è massimale.

5. (a) Essendo $\deg(F) = 3$, F è irriducibile se e solo se non ha radici nel campo $\mathbb{Z}/p\mathbb{Z}$. Un numero primo p per cui questo accade è $p = 7$. Infatti, indicando con $\bar{a}$ la classe di resto modulo 7 di $a \in \mathbb{Z}$, si verifica immediatamente che $F(\bar{0}) = \bar{5}$, $F(\bar{1}) = F(\bar{2}) = F(\bar{4}) = \bar{6}$ e $F(\bar{3}) = F(\bar{5}) = F(\bar{6}) = \bar{4}$.

   (b) Osservo intanto che F è irriducibile in $\mathbb{Z}[X]$ e quindi in $\mathbb{Q}[X]$: questo segue dal fatto che la riduzione di F modulo 7 è irriducibile (in alternativa si può dimostrare usando il criterio di Eisenstein rispetto al primo 3, o verificando direttamente che nessun divisore di 12 è radice di F). Dunque, detta $\alpha = -\sqrt[3]{12}$ la radice reale di F, si ha $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(F) = 3$. Inoltre, indicando con $\zeta \neq 1$ una radice (complessa) terza di 1, le altre radici di F sono $\alpha\zeta$ e $\alpha\zeta^2$. Il campo di spezzamento di F su $\mathbb{Q}$ è pertanto

$$K = \mathbb{Q}(\alpha, \alpha\zeta, \alpha\zeta^2) = \mathbb{Q}(\alpha, \zeta).$$

   Poiché il polinomio minimo di ζ su $\mathbb{Q}$ è $(X^3-1)/(X-1) = X^2+X+1$, si ha $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$. Essendo $\mathrm{mcd}(3,2) = 1$, possiamo concludere che

$$[K : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta) : \mathbb{Q}] = 3 \cdot 2 = 6.$$