Corso di Algebra - a.a. 2005-2006

Prova scritta del 6.2.2006 – soluzioni

1. Siano C un gruppo ciclico, c un suo generatore, e G un gruppo. Gli omomorfismi $C \to G$ sono in corrispondenza biunivoca con gli elementi di G il cui ordine divide l'ordine di C; l'omomorfismo α corrispondente a $g \in G$ è dato da $\alpha(c^n) = g^n$. Visto che l'ordine di ogni elemento di S_3 divide 6, gli omomorfismi $\mathbb{Z}/6\mathbb{Z} \to S_3$ sono dunque in corrispondenza biunivoca con gli elementi di S_3.

   Un omomorfismo $\alpha : S_3 \to \mathbb{Z}/6\mathbb{Z}$ non può essere iniettivo perchè $\mathbb{Z}/6\mathbb{Z}$ è abeliano e S_3 no. Poiché i soli sottogruppi normali di S_3 sono $\{1\}$, S_3 e il gruppo alterno A_3, il nucleo di α deve contenere A_3. Dunque α è la composizione dell'omomorfismo quoziente $S_3 \to S_3/A_3 = C$ e di un omomorfismo $\beta : C \to \mathbb{Z}/6\mathbb{Z}$. Dato che C ha ordine 2, vi è un omomorfismo β per ogni elemento di $\mathbb{Z}/6\mathbb{Z}$ il cui ordine divida 2. Questi elementi sono solo due, cioè le classi di 0 e di 3. Il primo corrisponde all'omomorfismo nullo, il secondo all'omomorfismo α tale che $\alpha(g) = [0]$ se g è l'identità o un 3-ciclo, e $\alpha(g) = [3]$ se g è una trasposizione.

2. Se $g, g' \in Z_G(H)$ e $h \in H$, $gg'h = ghg' = hgg'$, quindi $gg' \in Z_G(H)$. Inoltre $g^{-1}h = (h^{-1}g)^{-1} = (gh^{-1})^{-1} = hg^{-1}$, quindi $g^{-1} \in Z_G(H)$. Se $\gamma \in G$, $g \in Z_G(H)$ e $h \in H$, $\gamma^{-1}g\gamma h = \gamma^{-1}g\gamma h\gamma^{-1}\gamma$. Poiché H è normale, $k = \gamma h\gamma^{-1} \in H$. Dunque $\gamma^{-1}g\gamma h = \gamma^{-1}gk\gamma = \gamma^{-1}kg\gamma = h\gamma^{-1}g\gamma$. Questo significa che $\gamma^{-1}g\gamma \in Z_G(H)$.

3. Se f è suriettiva e X è un sottinsieme di B, allora $f(f^{-1}(X)) = X$ (questo è un fatto puramente insiemistico). Dunque, se I, J sono ideali distinti di B, $f^{-1}(I) \neq f^{-1}(J)$ perchè $f(f^{-1}(I) = I \neq J = f(f^{-1}(J))$.

   Se φ è suriettiva, in particolare c'è un ideale I di B tale che $f^{-1}(I) = \{0\}$ (questo ideale non può che essere l'ideale $\{0\}$). Ne segue che $\ker(f) = \{0\}$, e quindi che f è iniettiva.

4. La riduzione di $P(X)$ modulo 2 è $Q(X) = X^4 + X^3 + 1$. Basta mostrare che $Q(X)$ è irriducibile in $F[X]$, dove F è il campo $\mathbb{Z}/2\mathbb{Z}$. In primo luogo, $Q(X)$ non ha fattori di grado 1, dato che non ha radici in F; infatti $Q(0) = 1 = Q(1)$. Se $Q(X)$ non fosse irriducibile, dovrebbe dunque essere $Q(X) = S(X)T(X)$, dove S e T sono irriducibili di grado 2. I polinomi riducibili di grado 2 sono X^2, $X(X+1) = X^2 + X$ e $(X+1)^2 = X^2 + 1$. Quindi il solo polinomio irriducibile di grado 2 in $F[X]$ è $R(X) = X^2 + X + 1$. D'altra parte $R(X)$ non divide $Q(X)$. Questo si può vedere direttamente o ragionando come segue. Sia ξ una radice di $R(X)$ in una estensione L di F. Dato che $(X-1)R(X) = X^3 - 1$, deve essere $\xi^3 = 1$. Ne segue che $Q(\xi) = \xi + 1 + 1 = \xi \neq 0$. Dunque ξ non è radice di $Q(X)$, e di conseguenza $R(X)$ non divide $Q(X)$.

5. Indichiamo con L il campo di spezzamento di f. Almeno uno dei fattori irriducibili di f ha grado > 1, altrimenti L coinciderebbe con K. Sia p uno di questi fattori, e sia $\xi \in L$ una sua radice. Dato che $4 = [L : K] = [L : K[\xi]] \cdot [K[\xi] : K]$ e che $\deg(p) = [K[\xi] : K]$, il grado di p può essere 2 o 4. Nel secondo caso $\deg(f) \geq 4$. Se p ha grado 2, si spezza in un prodotto di due fattori di grado 1 in $K[\xi][X]$; dunque $K[\xi]$ è il campo di spezzamento di p, e quindi $f \neq p$. Scriviamo $f = pq$; il polinomio q non può avere grado 1, perchè in questo caso $K[\xi]$ sarebbe il campo di spezzamento di f. Dunque $\deg(f) = \deg(p)\deg(q) = 2\deg(q) \geq 4$. Se f è irriducibile ha grado 4 poiché, come si è mostrato, il grado di ogni fattore irriducibile di f non può superare 4.