Corso di Algebra 1 - a.a. 2013-2014

Prova scritta dell'11.9.2014

1. Determinare gli interi positivi x che verificano il seguente sistema di congruenze:
$$\begin{cases} 2^x \equiv 3 \mod 5 \\ 3x \equiv 2 \mod 5 \end{cases}$$

2. Siano G e H due gruppi.

   (a) Se $f\colon H \to G$ è un omomorfismo con immagine contenuta nel centro di G, allora la funzione
   $$\begin{aligned} G \times H &\to G \\ (g,h) &\mapsto gf(h) \end{aligned}$$
   è un omomorfismo suriettivo con nucleo $\{(f(h^{-1}),h) : h \in H\}$.

   (b) Nel caso in cui $G = D_{2n}$ per qualche intero positivo n e $H = \mathbb{Z}/2\mathbb{Z}$, dimostrare che il sottogruppo K di $G \times H$ generato da $(R^n, \overline{1})$ è normale e $(G \times H)/K$ è isomorfo a G.

3. Sia A un anello commutativo e B un suo sottoanello.

   (a) Dimostrare che per ogni $a \in A$ l'insieme $I_a = \{b \in B : ab \in B\}$ è un ideale di B.

   (b) Supponiamo ora $A = \mathbb{Q}$, $B = \mathbb{Z}$ e sia J un ideale di $\mathbb{Z}$. Dimostrare che esiste $a \in \mathbb{Q}$ tale che $J = I_a$ se e solo se $J \neq \{0\}$.

4. Sia P il polinomio $X^4 + 2X^3 + X^2 - X - 1$.

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

   (b) Sia $\alpha \in \mathbb{C}$ una radice non razionale di P e sia $\beta \in \mathbb{Q}(\alpha) \setminus \mathbb{Q}$. Determinare $[\mathbb{Q}(\beta) : \mathbb{Q}]$.

Soluzioni

1. Essendo $\mathrm{mcd}(2,5) = \mathrm{mcd}(3,5) = 1$, per x positivo la prima congruenza è equivalente a $\overline{2}^x = \overline{3}$ in $\mathbb{Z}/5\mathbb{Z}^*$. Poiché $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{3}$ e $\overline{2}^4 = \overline{1}$, troviamo che $\overline{2}$ ha ordine 4, e quindi $\overline{2}^x = \overline{3} = \overline{2}^3$ se e solo se $x \equiv 3 \mod 4$.

   Essendo $\mathrm{mcd}(3,5) = 1$, la seconda congruenza ha un'unica soluzione modulo 5, che si vede facilmente essere $x \equiv 4 \mod 5$.

   Dunque per x positivo il sistema di partenza è equivalente al sistema

$$\begin{cases} x \equiv 3 \equiv -1 \mod 4 \\ x \equiv 4 \equiv -1 \mod 5 \end{cases}$$

   Essendo $\mathrm{mcd}(4,5) = 1$, per il teorema cinese del resto tale sistema ha un'unica soluzione modulo $4 \cdot 5 = 20$, che è chiaramente $x \equiv -1 \equiv 19 \mod 20$.

2. (a) La funzione $\alpha\colon G \times H \to G$ definita da $(g,h) \mapsto gf(h)$ è un omomorfismo di gruppi perché per ogni $g, g' \in G$ e per ogni $h, h' \in H$ si ha (usando il fatto che $g'f(h) = f(h)g'$ perché $f(h) \in Z(G)$ per ipotesi)

$$\begin{aligned} \alpha((g,h)(g',h')) &= \alpha((gg',hh')) = gg'f(hh') \\ &= gg'f(h)f(h') = gf(h)g'f(h') = \alpha((g,h))\alpha((g',h')). \end{aligned}$$

   α è suriettiva perché per ogni $g \in G$ si ha $\alpha((g,1_H)) = gf(1_H) = g1_G = g$. Infine, dato $(g,h) \in G \times H$, si ha $(g,h) \in \ker(\alpha)$ se e solo se $1_G = \alpha((g,h)) = gf(h)$ se e solo se $g = f(h)^{-1} = f(h^{-1})$. Concludiamo pertanto che $\ker(\alpha) = \{(f(h^{-1}),h) \,:\, h \in H\}$.

   (b) Poiché R^n ha ordine 2 in D_{2n}, la funzione

$$\begin{aligned} f\colon \mathbb{Z}/2\mathbb{Z} &\to D_{2n} \\ \overline{k} &\mapsto (R^n)^k = R^{nk} \end{aligned}$$

   è ben definita ed è un omomorfismo di gruppi. Essendo inoltre $R^n \in Z(D_{2n})$, l'immagine di f risulta chiaramente contenuta in $Z(D_{2n})$. Applicando la prima parte troviamo allora un omomorfismo suriettivo $\alpha\colon D_{2n} \times \mathbb{Z}/2\mathbb{Z} \to D_{2n}$ con nucleo

$$\begin{aligned} \{(f(-\overline{k}),\overline{k}) \,:\, \overline{k} \in \mathbb{Z}/2\mathbb{Z}\} &= \{(f(-\overline{0}),\overline{0}),(f(-\overline{1}),\overline{1})\} \\ &= \{(f(\overline{0}),\overline{0}),(f(\overline{1}),\overline{1})\} = \{(1,\overline{0}),(R^n,\overline{1})\} = K. \end{aligned}$$

Concludiamo che $(D_{2n} \times \mathbb{Z}/2\mathbb{Z})/K$ è isomorfo a D_{2n} per il primo teorema di isomorfismo.

3. (a) $0 \in I_a$ perché $a0 = 0 \in B$.
   Dati $b, b' \in I_a$ (cioè $b, b' \in B$ tali che $ab, ab' \in B$), si ha $b + b' \in B$ e $a(b + b') = ab + ab' \in B$ (perché B è chiuso rispetto alla somma, essendo un sottoanello di A), il che dimostra che $b + b' \in I_a$.
   Infine, dati $b \in I_a$ e $c \in B$, si ha $bc \in B$ e $a(bc) = (ab)c \in B$ (perché B è chiuso rispetto al prodotto, essendo un sottoanello di A), il che dimostra che $bc \in I_a$.

   (b) Se esiste $a = \frac{m}{n} \in \mathbb{Q}$ (con $m, n \in \mathbb{Z}$ e $n \neq 0$) tale che $J = I_a$, allora $n \in \mathbb{Z}$ e $na = m \in \mathbb{Z}$, quindi per definizione $n \in I_a$, il che dimostra che $J \neq \{0\}$.
   Viceversa, se $J \neq \{0\}$, allora esiste $0 \neq n \in \mathbb{Z}$ tale che $J = n\mathbb{Z}$, e si può dimostrare per esempio che $J = I_{\frac{1}{n}}$. Infatti, dato $m \in \mathbb{Z}$, si ha $m \in I_{\frac{1}{n}}$ se e solo se $\frac{m}{n} \in \mathbb{Z}$, il che è vero se e solo se $m \in n\mathbb{Z}$.

4. (a) Il polinomio $P(X)$ ammette la radice -1, come è immediato verificare. Si ottiene così $P(X) = (X + 1)(X^3 + X^2 - 1)$. Se il fattore $Q(X) = X^3 + X^2 - 1$ fosse riducibile in $\mathbb{Q}[X]$, essendo di grado 3 esso dovrebbe avere un fattore di grado 1 e quindi una radice in $\mathbb{Q}$: ma, in tal caso, per il criterio della radice razionale, tale radice dovrebbe essere 1 o -1, che però non lo annullano. Se ne deduce che $Q(X)$ è irriducibile e quindi i soli fattori irriducibili di $P(X)$ sono $(X + 1)$ e $Q(X)$ (ciascuno con molteplicità 1).

   (b) Se α è una radice non razionale di $P(X)$, evidentemente $\alpha \neq -1$ e quindi α è anche radice di $Q(X)$. Come abbiamo visto, $Q(X)$ è irriducibile (e monico) e quindi esso è anche il polinomio minimo di α, che ha così grado 3 su $\mathbb{Q}$. Gli elementi di $\mathbb{Q}(\alpha)$, come β, generano quindi su $\mathbb{Q}$ una sottoestensione di $\mathbb{Q}(\alpha)$; ma poiché $\mathbb{Q} \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$, il grado $[\mathbb{Q}(\beta) : \mathbb{Q}]$ di tale sottoestensione può solo essere 1 o 3. Ma se fosse 1, si avrebbe $\mathbb{Q}(\beta) = \mathbb{Q}$ e quindi $\beta \in \mathbb{Q}$, il che è escluso per ipotesi; perciò $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$.