Corso di Algebra 1 – a.a. 2012-2013

Prova scritta del 22.1.2013

1. Siano $I_1 = \{1,2,3\}$, $I_2 = \{4,5,6\}$, $I_3 = \{7,8,9\}$ e consideriamo

$$H = \{\sigma \in S_9 : \sigma(I_i) = I_i,\ i = 1,2,3\}\ , \quad K = \{\sigma \in S_9 : \sigma(I_i) \in \{I_1, I_2, I_3\},\ i = 1,2,3\}\,.$$

   (a) Verificare che H e K sono sottogruppi di S_9.

   (b) Mostrare che H è un sottogruppo normale di K.

   (c) Mostrare che K/H è isomorfo a S_3.

2. (a) Verificare che il gruppo $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ è isomorfo a $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

   (b) Contare i possibili isomorfismi $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

3. Sia $A = \mathbb{Z}\big[\sqrt{-p^3}\big]$, dove p è un numero primo. Dato $z = a + b\sqrt{-p^3} \in A$ poniamo

$$v(z) = a^2 + b^2p^3\,.$$

   (a) Verificare che $v(xy) = v(x)v(y)$.

   (b) Mostrare che $x \in A^*$ se e solo se $v(x) = 1$. Determinare A^*.

   (c) Mostrare che p e $\sqrt{-p^3}$ sono irriducibili in A.

4. Sia $m \in \mathbb{Z}$.

   (a) Verificare che il grado $\big[\mathbb{Q}[\sqrt{2}, \sqrt{m}] : \mathbb{Q}\big]$ può valere solo 2 o 4.

   (b) Determinare i valori di m per cui $\big[\mathbb{Q}[\sqrt{2}, \sqrt{m}] : \mathbb{Q}\big] = 2$.

   (c) Verificare che $\mathbb{Q}[\sqrt{2} + \sqrt{m}] = \mathbb{Q}[\sqrt{2}, \sqrt{m}]$.

Soluzioni

1. (a) L'identità appartiene a H, che quindi non è vuoto. Lo stesso è vero per K, che contiene H. Se $\sigma, \tau \in K$, allora $\sigma\tau(I_i) = \sigma(I_j) = I_k$ per qualche j e qualche k, dunque $\sigma\tau \in K$; se in più $\sigma, \tau \in H$ allora $k = j = i$ e quindi $\sigma\tau \in H$. Dato che S_9 è un gruppo **finito** questo basta a concludere che H e K sono suoi sottogruppi. Infatti se $\sigma \in S_9$ allora $\sigma^{-1} = \sigma^{n-1}$, dove n è l'ordine di σ, e quindi se $\sigma \in H$ (o $\sigma \in K$) allora $\sigma^{-1} = \sigma^{n-1}$ appartiene a H (o a K) per quanto mostrato prima.

   (b) Supponiamo che $\sigma \in H$ e $\tau \in K$. Allora $\tau^{-1}(I_i) = I_j$ per qualche j, e di conseguenza $\tau(I_j) = I_i$. Dunque $\tau\sigma\tau^{-1}(I_i) = \tau\sigma(I_j) = \tau(I_j) = I_i$. Questo mostra che $\tau\sigma\tau^{-1} \in H$. Dunque H è normale in K. Alternativamente si può ragionare come segue. Ogni elemento di K permuta tra loro I_1, I_2, I_3. Questo dà un omomorfismo $\alpha : K \to S(\{I_1, I_2, I_3\}) \simeq S_3$. Il nucleo di questo omomorfismo è costituito da tutti quei $\sigma \in K$ tali che $\sigma(I_i) = I_i$ per ogni i, cioè dagli elementi di H. Ne segue in particolare che H è normale in K.

   (c) Visto il punto precedente basta mostrare che α è suriettivo. Sia $\rho \in S(\{I_1, I_2, I_3\})$. Dunque $\rho(I_1) = I_i$, $\rho(I_2) = I_j$ e $\rho(I_3) = I_k$, dove naturalmente $\{i, j, k\} = \{1, 2, 3\}$ e i, j e k sono distinti. Esistono applicazioni biunivoche $\beta_1 : I_1 \to I_i$, $\beta_2 : I_2 \to I_j$ e $\beta_3 : I_3 \to I_k$, perché I_1, I_2, I_3 hanno tutti tre elementi. Sia $\sigma \in S_9$ l'applicazione che coincide con β_ℓ su I_ℓ, $\ell = 1, 2, 3$. È chiaro che $\alpha(\sigma) = \rho$. Dunque α è suriettiva.

2. (a) $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ è isomorfo a $\mathbb{Z}/15\mathbb{Z}$ perché 3 e 5 sono primi fra loro. Quindi $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.

   (b) Se α e β sono isomorfismi $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, allora $\alpha^{-1}\beta$ è un automorfismo di $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Quindi dobbiamo contare gli automorfismi di $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Se τ_1, τ_2, τ_3 sono automorfismi, rispettivamente, di $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ e $\mathbb{Z}/4\mathbb{Z}$, allora l'applicazione $\sigma : \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ data da $\sigma(a,b,c) = (\tau_1(a), \tau_2(b), \tau_3(c))$ è un automorfismo. D'altra parte, dato che 3, 5 e 4 sono a due a due primi fra loro, ogni automorfismo di $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ è di questo tipo. Gli automorfismi di $\mathbb{Z}/k\mathbb{Z}$ sono in corrispondenza biunivoca con $(\mathbb{Z}/k\mathbb{Z})^*$. Ora, $(\mathbb{Z}/3\mathbb{Z})^*$ consta di 2 elementi, $(\mathbb{Z}/5\mathbb{Z})^*$ di 4 e $(\mathbb{Z}/4\mathbb{Z})^*$ di 2. Dunque il numero cercato è $2\cdot 4\cdot 2 = 16$.

3. Notiamo che $v(z)$ è il quadrato del modulo del numero complesso z, e quindi in particolare è ≥ 0. Inoltre $v(z)$ è sempre un intero.

   (a) $v(xy) = |xy|^2 = |x|^2|y|^2 = v(x)v(y)$.

   (b) Se $w \in A$ è inverso di z allora $v(z)v(w) = v(zw) = v(1) = 1$. Dato che $v(z)$ e $v(w)$ sono interi non negativi, devono essere tutti e due uguali a 1. Supponiamo viceversa che $v(z) = 1$. In questo caso $\overline{z} \in A$ e $1 = v(z) = z\overline{z}$. Dunque z è invertibile e il suo inverso è $\overline{z}$. Se $z = a + b\sqrt{-p^3}$ e $1 = v(z) = a^2 + p^3b^2 \geq p^3b^2$ deve essere $b = 0$ e $a^2 = 1$. Quindi $A^* = \{1, -1\}$.

   (c) Supponiamo che $p = xy$ oppure che $\sqrt{-p^3} = xy$. Nel primo caso $v(x)v(y) = v(p) = p^2$, nel secondo $v(x)v(y) = v(\sqrt{-p^3}) = p^3$. Se x e y non sono invertibili, cioè se $v(x) > 1$ e $v(y) > 1$, ne segue che $v(x) = p$ oppure $v(y) = p$. Ma questo è impossibile. Infatti se $z = a + b\sqrt{-p^3} \in A$, allora $v(z) \geq p^3 > p$ quando $b > 0$. Se invece $b = 0$, $v(z)$ è un quadrato, il che non è vero di p.

4. (a) $\left[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\right] = 2$. Inoltre il polinomio minimo di $\sqrt{m}$ su $\mathbb{Q}[\sqrt{2}]$ divide $X^2 - m$; quindi $\left[\mathbb{Q}[\sqrt{2}, \sqrt{m}] : \mathbb{Q}[\sqrt{2}]\right]$ vale 2 o 1. Ne segue che $\left[\mathbb{Q}[\sqrt{2}, \sqrt{m}] : \mathbb{Q}\right] = \left[\mathbb{Q}[\sqrt{2}, \sqrt{m}] : \mathbb{Q}[\sqrt{2}]\right]\left[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\right]$ vale 4 o 2.

   (b) $\left[\mathbb{Q}[\sqrt{2}, \sqrt{m}] : \mathbb{Q}\right] = 2$ se e solo se $\sqrt{m} \in \mathbb{Q}[\sqrt{2}]$, cioè se e solo se esistono interi a e b tali che $\sqrt{m} = a + b\sqrt{2}$. Ora $(a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$, che è un intero se e solo se $ab = 0$. Se $b = 0$ allora $(a + b\sqrt{2})^2$ è un quadrato; se invece $a = 0$, allora $(a + b\sqrt{2})^2$ è il doppio di un quadrato. Ne segue che $\left[\mathbb{Q}[\sqrt{2}, \sqrt{m}] : \mathbb{Q}\right] = 2$ se e solo se m è un quadrato o il doppio di un quadrato.

   (c) Distinguiamo due casi. Se $\left[\mathbb{Q}[\sqrt{2}, \sqrt{m}] : \mathbb{Q}\right] = 2$, allora $m = k^2$ oppure $m = 2k^2$ per qualche intero k, quindi $\mathbb{Q}[\sqrt{2} + \sqrt{m}] = \mathbb{Q}[\sqrt{2}, k] = \mathbb{Q}[\sqrt{2}]$ oppure $\mathbb{Q}[\sqrt{2} + \sqrt{m}] = \mathbb{Q}[\sqrt{2}, k\sqrt{2}] = \mathbb{Q}[\sqrt{2}]$. D'altra parte in questo caso $\mathbb{Q}[\sqrt{2}, \sqrt{m}] = \mathbb{Q}[\sqrt{2}]$.

   Supponiamo invece che $\left[\mathbb{Q}[\sqrt{2}, \sqrt{m}] : \mathbb{Q}\right] = 4$. Il grado di $z = \sqrt{2} + \sqrt{m}$ su $\mathbb{Q}$ può essere 2 o 4. Dobbiamo mostrare che vale 4. Dire che z è radice di un polinomio di secondo grado $X^2 + hX + k$, dove h e k sono interi, significa che $2 + m + 2\sqrt{2}\sqrt{m} + h\sqrt{2} + h\sqrt{m} + k = 0$, quindi che $\sqrt{m} \in \mathbb{Q}[\sqrt{2}]$, e quindi in definitiva che $\left[\mathbb{Q}[\sqrt{2}, \sqrt{m}] : \mathbb{Q}\right] = 2$, contro l'ipotesi.