**SOLUZIONI DEL COMPITO DI ALGEBRA 1**
21 gennaio 2013

**Esercizio 1.** Contare le soluzioni $\sigma \in S_{10}$ dell'equazione $\sigma^4 = (1,2,3)(4,5,6)$.

**Soluzione esercizio 1.**PRIMA SOLUZIONE Dalla relazione $3 = \mathrm{ord}(\sigma^4) = \mathrm{ord}(\sigma) \cdot (\mathrm{ord}(\sigma), 4)$ otteniamo che $3|\mathrm{ord}(\sigma)|12$, quindi che $\sigma$ può avere ordine 3,6 o 12. Da questo segue che i cicli che compongono $\sigma$ possono avere solo ordine 2,3,4,6 (in $S_{10}$ non ci sono 12-cicli!!) e che almeno uno ha ordine 3 o 6.
Sia $\sigma = \rho_1 \cdots \rho_r$ la decomposizione di $\sigma$ in cicli disgiunti, allora $\sigma^4 = \rho_1^4 \cdots \rho_r^4 = (1,2,3)(4,5,6)$. Osserviamo anche che se $\rho$ è un 3-ciclo $\rho^4 = \rho$, mentre se $\rho = (a,b,c,d,e,f)$ allora $\rho^4 = (a,e,c)(b,f,d)$; da ciò possiamo dedurre che $\sigma$ ha una scrittura unica come:
i) $\sigma = (1,2,3)(4,5,6)\gamma$ con $\gamma \in S\{7,8,9,10\}$ e $\gamma^4 = id$.
ii) $\sigma = (a,b,c,d,e,f)\gamma$ con $(a,b,c,d,e,f)^4 = (a,e,c)(b,f,d) = (1,2,3)(4,5,6)$, $\gamma \in S\{7,8,9,10\}$ e $\gamma^4 = id$.
Le permutazioni di tipo (i) sono tante quante le permutazioni di ordine divisore di 4 in $S\{7,8,9,10\} \cong S_4$ e queste sono, oltre all'identità, le permutazioni di tipo 2, 2+2, 4, quindi sono $1 + \binom{4}{2} + \binom{4}{2}\binom{2}{2}\frac{1}{2} + \binom{4}{4}3! = 16$.
Per contare le permutazioni di tipo (ii), poiché abbiamo già contato le permutazioni $\gamma$ che sono 16, rimangono da contare i 6 cicli $(a,b,c,d,e,f)$ tali che $(a,e,c)(b,f,d) = (1,2,3)(4,5,6)$. Possiamo chiaramente supporre $a = 1$, allora necessariamente $e = 2$ e $c = 3$; $b$ può invece essere 4,5,6 e di conseguenza si ottengono univocamente i valori di $f$ e $d$. I 6-cicli sono quindi 3 e le permutazioni del caso (ii) sono $3 \cdot 16 = 48$.
In tutto le soluzioni dell'equazione assegnata sono 64.

SECONDA SOLUZIONE Ricordiamo che il quadrato di un ciclo di lunghezza dispari è un ciclo della stessa lunghezza, mentre per un ciclo di lunghezza pari abbiamo $(a_1, b_1, a_2, b_2, \ldots, a_n, b_n)^2 = (a_1, \ldots, a_n)(b_1, \ldots, b_n)$. Da questo segue che l'equazione $\sigma^4 = (1,2,3)(4,5,6)$ è equivalente a $\sigma^2 = (1,3,2)(4,6,5)\gamma$ o $\sigma^2 = (1,a,2,b,3,c)\gamma$ con con $a = 4, b = 5, c = 6$ oppure $a = 5, b = 6, c = 4$ o $a = 6, b = 4, c = 5$ e $\gamma \in S\{7,8,9,10\}$ e $\gamma^2 = id$. Osserviamo però che $\sigma^2 = (1,a,2,b,3,c)\gamma$ non ha soluzione perchè al secondo membro compare un solo 6-ciclo, quindi l'equazione assegnata è equivalente a $\sigma^2 = (1,3,2)(4,6,5)\gamma$ con $\gamma \in S\{7,8,9,10\}$ e $\gamma^2 = id$. Con lo stesso argomento di prima si ha che questa equazione è equivalente a $\sigma = (1,2,3)(4,5,6)\gamma$ con $\gamma \in S\{7,8,9,10\}$ e $\gamma^4 = id$ oppure $\sigma = (1,a,3,b,2,c)\gamma$ con con $a = 4, b = 6, c = 5$ oppure $a = 5, b = 4, c = 6$ o $a = 6, b = 5, c = 4$ e $\gamma \in S\{7,8,9,10\}$ e $\gamma^2 = id$. Il numero delle permutazioni cercate è quindi $4 \cdot \#\{\gamma \in \S_4 \,|\, \gamma^4 = id\} = 4 \cdot (1 + \binom{4}{2} + \binom{4}{2}\binom{2}{2}\frac{1}{2} + \binom{4}{4}3!) = 64$.

**Esercizio 2.** Classificare, a meno di isomorfismo, i gruppi di ordine 2013.
**Soluzione esercizio 2.** Sia $G$ un gruppo di ordine $2013 = 3 \cdot 11 \cdot 61$.
Per $p \in \{3, 11, 61\}$ indichiamo con $H_p$ un $p$-Sylow di $G$, che nel nostro caso ha ordine $p$ e quindi è ciclico. Dal Teorema di Sylow sappiamo che, detto $n_p$ il numero dei $p$-Sylow di $G$

si ha $n_p \equiv 1 \pmod p$ e $n_p \big| |G|$. Queste condizioni danno $n_{61} = 1$ e $n_{11} = 1$ quindi $H_{61}$ e $H_{11}$ sono normali in $G$. Da questo segue che il prodotto $H_{61}H_{11}$ è un sottogruppo normale di $G$ ( in quanto entrambi i sottogruppi sono normali, o, se volete, anche perché ha indice 3 che è il piú piccolo primo che divide l'ordine di $G$); inoltre tale sottogruppo è anche ciclico, in quanto ha ordine il prodotto di due primi e $11 \nmid 61 - 1$, quindi $H_{61}H_{11} = \langle x \rangle$. Fissato un 3-Sylow $H_3$ e posto $H_3 = \langle y \rangle$, abbiamo che $G \cong \langle x \rangle \rtimes_{\varphi} \langle y \rangle$ dove $\varphi : \langle y \rangle \to \mathrm{Aut}(\langle x \rangle)$ e $\varphi_y(x) = yxy^{-1} = x^k$. Ora $\mathrm{Aut}(\langle x \rangle) \cong (\mathbb{Z}/671\mathbb{Z})^* \cong (\mathbb{Z}/11\mathbb{Z})^* \times (\mathbb{Z}/60\mathbb{Z})^*$ contiene esattamente due elementi di ordine 3 ($x \mapsto x_0^k$ e $x \mapsto x^{k_0^2}$), quindi ci sono 3 omomorfismi $\varphi$ possibili che sono definiti da $\varphi_{0y}(x) = yxy^{-1} = x$, $\varphi_{1y}(x) = yxy^{-1} = x^{k_0}$ e $\varphi_{2y}(x) = yxy^{-1} = x^{k_0^2}$.
L'omomorfismo $\varphi_0$ è quello banale e corrisponde al prodotto diretto, cioè al gruppo $G \cong \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}/11 \cdot 61\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2013\mathbb{Z}$. Gli altri due omomorfismi danno gruppi non abeliani $G_1 = \langle x \rangle \rtimes_{\varphi_1} \langle y \rangle$ e $G_2 = \langle x \rangle \rtimes_{\varphi_2} \langle y \rangle$. Vediamo che questi due gruppi sono isomorfi. Per evitare confusione usiamo per il gruppo $G_2$ le lettere maiuscole: si ha $G_1 = \langle x, y | x^{671} = 1, y^3 = 1, yxy^{-1} = x^{k_0} \rangle$ e $G_2 = \langle X, Y | X^{671} = 1, Y^3 = 1, YXY^{-1} = X^{k_0^2} \rangle$; definiamo $\Phi : G_2 \to G_1$ ponendo $\Phi(X) = x$ e $\Phi(Y) = y^2$: tale assegnamento conserva l'ordine degli elementi e inoltre $\Phi(X^{k_0^2}) = x^{k_0^2}$ e $\Phi(YXY^{-1}) = y^2xy^{-2} = x^{k_0^2}$, cioè conserva la regola di commutazione, quindi si estende ad un isomorfismo.
Possiamo concludere un gruppo di ordine 2013 è ciclico oppure è isomorfo al gruppo $G_1$.

**Esercizio 3.** Sia $A$ il sottoanello di $\mathbb{Q}(x)$ definito da

$$A = \Big\{ \frac{f(x)}{g(x)} \,|\, f(x), g(x) \in \mathbb{Q}[x],\ g(0)g(-1) \neq 0 \Big\}.$$

a) Determinare gli elementi invertibili di $A$.

b) Dimostrare che $A$ è un dominio a ideali principali.

c) Determinare gli ideali primi di $A$.

**Soluzione esercizio 3. (a)** Osserviamo per prima cosa che la scrittura degli elementi di $\mathbb{Q}(X)$ non è unica perchè $\frac{f(x)}{g(x)} = \frac{f(x)h(x)}{g(x)h(x)}$ per ogni $h(x) \in \mathbb{Q}[x] \setminus \{0\}$. La scrittura degli elementi di $\mathbb{Q}(x)$ è però unica come frazione ridotta ai minimi termini, cioè con numeratore e denominatore coprimi. Sia $\frac{f(x)}{g(x)} \in A \setminus \{0\}$ e supponiamo che la scrittura considerata sia ridotta ai minimi termini: tale elemento è invertibile in $A$ se e solo se il suo inverso nel campo $\mathbb{Q}(x)$, $\frac{g(x)}{f(x)}$, appartiene ad $A$, cioè se e solo se esiste un scrittura di tale frazione con denominatore che non si annulla in 0 e -1. D'altra parte, poiché $\frac{g(x)}{f(x)}$ è ridotta ai minimi termini, questo vale se e solo se $f(0)f(-1) \neq 0$.
**(b)** Sicuramente $A$ è un dominio d'integrità perché è sottoanello del campo $\mathbb{Q}(x)$. Osserviamo che dalla proprietà di fattorizzazione unica di $\mathbb{Q}[x]$ segue che ogni polinomio $f(x) \in \mathbb{Q}[x] \setminus \{0\}$ ammette una scrittura unica come $f(x) = x^a(x+1)^b u(x)$ con $a, b \in \mathbb{N}$ e $u(x) \in \mathbb{Q}[x]$ tale che $u(0) \neq 0$ e $u(-1) \neq 0$. Ne segue che per ogni elemento $\frac{f(x)}{g(x)} \in A \setminus \{0\}$ si ha

$$\frac{f(x)}{g(x)} = x^a(x+1)^b \frac{u(x)}{g(x)}$$

con $a, b \in \mathbb{N}$ univocamente determinati e $\frac{u(x)}{g(x)}$ invertibile in $A$, quindi ogni elemento di $A$ è associato ad un polinomio del tipo $x^a(x+1)^b$.
Sia $I \subset A$ un ideale non banale, per quanto appena detto $I = (x^{a_l}(x+1)^{b_l})_{l\in\Lambda}$. Sia $x^{a_0}(x+1)^{b_0}$ il massimo comune divisore in $\mathbb{Q}[x]$ dei polinomi $\{x^{a_l}(x+1)^{b_l}\}_{l\in\Lambda}$, tale mcd esiste perchè $Q[X]$ è un dominio euclideo ed è una combinazione finita del polinomi $x^{a_l}(x+1)^{b_l}$. Questo assicura che $I = (x^{a_0}(x+1)^{b_0})$, quindi $A$ è un PID.
**(c)** Poichè $A$ è un PID gli ideali primi di $A$ sono $(0)$ e gli ideali massimali, che sono generati dagli elementi irriducibili di $A$. Abbiamo visto che ogni elemento di $A$ è associato ad un polinomio del tipo $x^a(x+1)^b$ e che $x$ e $x+1$ non sono invertibili, quindi $x$ e $x+1$ sono gli irriducibili di $A$ e generano gli ideali massimali di $A$.

**Esercizio 4.** Sia $\zeta_{15} \in \mathbb{C}$ una radice 15-esima primitiva dell'unità. Contare le sottoestensioni $K$ di grado 2 su $\mathbb{Q}$ di $\mathbb{Q}(\zeta_{15})$ e descrivere ognuna di esse come $K = \mathbb{Q}(\sqrt{m})$ con $m \in \mathbb{Z}$ libero da quadrati.
**Soluzione esercizio 4.** Dalla teoria svolta sappiamo che $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$ è un'estensione di Galois di grado $\Phi(15) = 8$ e gruppo di Galois $G$ isomorfo a $(\mathbb{Z}/15\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Le sottoestensioni di grado 2 su $\mathbb{Q}$ corrispondono ai sottogruppi del gruppo di Galois di indice 2, e quindi di ordine 4. Un gruppo di ordine 4 è ciclico oppure è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: il gruppo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ha 4 elementi di ordine 4 e 3 elementi di ordine 2, quindi ha $4/\Phi(4) = 2$ sottogruppi ciclici di ordine 4 e un solo sottogruppo isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (poiché ci sono 3 elementi di ordine 2 c'è al piú un sottogruppo di questo tipo, d'altra parte $\mathbb{Z}/2\mathbb{Z} \times 2\mathbb{Z}/4\mathbb{Z}$ è un sottogruppo del tipo cercato). I sottogruppi di $G$ di ordine 4 sono quindi 3 e ci sono 3 sottoestensioni $K$ di grado 2 su $\mathbb{Q}$.
Osserviamo che $\mathbb{Q}(\zeta_{15}) = \mathbb{Q}(\zeta_3)\mathbb{Q}(\zeta_5)$, infatti si verifica che $\zeta_3\zeta_5$ è un elemento di ordine moltiplicativo 15 e quindi una radice 15-esima primitiva di 1 e che $\zeta_{15}^5$ e $\zeta_{15}^3$ sono rispettivamente una radice terza e una radice quinta primitiva dell'unità. Ne segue che $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ è una delle sottoestensioni cercate. D'altra parte $\mathbb{Q}(\zeta_5)$ è un'estensione normale di grado 4 di $\mathbb{Q}$ e $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}$, quindi contiene una sottoestensione di grado 2. Tale sottoestensione è la sottoestensione reale $\mathbb{Q}(\zeta_5 + \zeta_5^{-1})$, vogliamo destriverla come $\mathbb{Q}(\sqrt{m})$ con $m \in \mathbb{Z}$ (chiaramente risulterà $m > 0$). I coniugati di $\alpha = \zeta_5 + \zeta_5^{-1}$ su $\mathbb{Q}$ sono le possibili immagini di $\alpha$ mediante gli elementi del $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$: ricordando che $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) = \{\sigma_i \mid i = 1,2,3,4\}$, dove $\sigma_i$ è definito da $\sigma_i(\zeta_5) = \zeta_5^i$, otteniamo che i coniugati di $\alpha$ sono $\alpha = \zeta_5 + \zeta_5^{-1}$ e $\zeta_5^2 + \zeta_5^{-2}$ e da questo troviamo che il polinomio minimo di $\alpha$ su $\mathbb{Q}$ è $\mu(x) = \left(x - (\zeta_5 + \zeta_5^{-1})\right)\left(x - (\zeta_5^2 + \zeta_5^{-2})\right) = x^2 + x - 1$. Abbiamo quindi che $\alpha = (-1 \pm \sqrt{5})/2$ da cui otteniamo $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\sqrt{5})$. Ovviamente $\mathbb{Q}(\sqrt{-3}) \neq \mathbb{Q}(\sqrt{5})$, e la terza sottoestensione è $\mathbb{Q}(\sqrt{-15})$: infatti, $\sqrt{-15} = \sqrt{-3}\sqrt{5} \in \mathbb{Q}(\zeta_{15})$, inoltre le estensioni $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{5})$ e $\mathbb{Q}(\sqrt{-15})$ sono distinte grazie al criterio che assicura che $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ se e solo se $ab$ è un quadrato in $\mathbb{Q}$.