**COMPITO DI ALGEBRA 3, 2/5/2013**

COGNOME e Nome .....

MATRICOLA .....

**Esercizio 1.** Sia $f(X) = X^4 - 2X^2 - 10 \in \mathbb{Q}[X]$. Sia $K$ il campo di spezzamento di $f(X)$ su $\mathbb{Q}$.

(1) Determinare le radici di $f(X)$
(2) Determinare il grado $\big[K : \mathbb{Q}\big]$
(3) Descrivere il gruppo di Galois $G$ di $K$ su $\mathbb{Q}$

**Soluzione 1.** (i) Il polinomio $f(X)$ è irriducibile per il criterio di Eisenstein applicato al primo 2. Le sue soluzioni sono le soluzioni di $X^2 = y$ con $y$ radice di $Y^2 - 2Y - 10$, ovvero $y = 1 \pm \sqrt{11}$. Le radici di $f(X)$ sono quindi $\{\pm\alpha, \pm\beta\}$ con $\alpha = \sqrt{1+\sqrt{11}}$ e $\beta = \sqrt{1-\sqrt{11}}$.

(ii) Visto che $f(X)$ è irriducibile, le estensioni $L_1 = \mathbb{Q}(\alpha)$ e $L_2 = \mathbb{Q}(\beta)$ sono di grado 4 su $\mathbb{Q}$. Esse contengono $\mathbb{Q}(\sqrt{11})$ in quanto $\sqrt{11} = \alpha^2 - 1 = 1 - \beta^2$ e per moltiplicatività dei gradi sono di grado 2 su $\mathbb{Q}(\sqrt{11})$. Poichè $\alpha \in \mathbb{R}$ e $\beta \in \mathbb{C}\backslash\mathbb{R}$, concludiamo che $L_1 \cap L_2 = \mathbb{Q}(\sqrt{11})$ altrimenti $L_1 = L_2$. Visto che $K$ è il campo composto $L_1 \cdot L_2$, segue che $K$ ha grado 4 su $\mathbb{Q}(\sqrt{11})$ e quindi ha grado 8 su $\mathbb{Q}$.

(iii) Osserviamo che $\mathbb{Q} \subset \mathbb{Q}(\sqrt{11})$ è una estensione quadratica, e quindi di Galois, contenuta in $K$. L'applicazione $\pi\colon G \to \mathrm{Gal}\big(\mathbb{Q}(\sqrt{11})/\mathbb{Q}\big)$ definita da $\sigma \mapsto \sigma|_{\mathbb{Q}(\sqrt{11})}$ è quindi ben definita e suriettiva. Sia $\sigma \in G$. Se $\pi(\sigma) = \mathrm{Id}$, allora $\sigma(\alpha)^2 = \pi(\sigma)\big(1+\sqrt{11}\big) = 1 + \sqrt{11}$ e quindi $\sigma(\alpha) = \pm\alpha$. Similmente $\sigma(\beta) = \pm\beta$. Ho quindi le seguenti possibilità per $\sigma$:

1) $\sigma(\alpha) = \alpha$, $\sigma(\beta) = \beta$;
2) $\sigma(\alpha) = -\alpha$, $\sigma(\beta) = \beta$,
3) $\sigma(\alpha) = \alpha$, $\sigma(\beta) = -\beta$,
4) $\sigma(\alpha) = -\alpha$, $\sigma(\beta) = -\beta$.

Se $\pi(\sigma)$ è non banale, invia $\sqrt{11} \mapsto -\sqrt{11}$ e quindi $\sigma(\alpha)^2 = \pi(\sigma)\big(1+\sqrt{11}\big) = 1 - \sqrt{11}$, Deduco che $\sigma(\alpha) = \pm\beta$ e similmente $\sigma(\beta) = \pm\alpha$. Ho quindi le seguenti possibilità per $\sigma$:

5) $\sigma(\alpha) = \beta$, $\sigma(\beta) = \alpha$,
6) $\sigma(\alpha) = -\beta$, $\sigma(\beta) = \alpha$,
7) $\sigma(\alpha) = \beta$, $\sigma(\beta) = -\alpha$,
8) $\sigma(\alpha) = -\beta$, $\sigma(\beta) = -\alpha$.

Visto che $K = \mathbb{Q}(\alpha, \beta)$ ogni $\sigma \in G$ è univocamente determinato da dove invia $\alpha$ e $\beta$. Visto che $G$ ha cardinalità uguale a $[K : \mathbb{Q}] = 8$, concludo che per ognuno dei casi (i), con $1 \leq i \leq 8$, esiste ed è unico un automorfismo $\sigma_i \in G$ che soddisfa le condizioni del caso (i).

**Esercizio 2.** Sia $p > 2$ un numero primo. Sia $K_p$ il $p$-esimo campo ciclotomico, ovvero il campo di spezzamento del polinomio $X^p - 1$ su $\mathbb{Q}$.

(1) Determinare il grado $[K_p : \mathbb{Q}]$
(2) Descrivere il gruppo di Galois $G_p = \mathrm{Gal}\big(K_p/\mathbb{Q}\big)$,

(3) Mostrare che esiste un'unica estensione quadratica $L_n = \mathbb{Q}(\sqrt{d})$ di $\mathbb{Q}$ contenuta in $K_p$. Determinare $d$.

**Soluzione 2.** (i) Sia $f(X) = \frac{X^p-1}{X-1}$. Si mostra che $f(Y+1)$ è un polinomio di Eisenstein per il primo $p$ e quindi è irriducibile su $\mathbb{Q}$. Segue che $f(X)$ è irriducibile su $\mathbb{Q}$ di grado $p-1$. Sia $\zeta_p$ una radice. Allora $\zeta_p^i \neq \zeta_p^j$ per $1 \leq i < j \leq p-1$, altrimenti $\zeta_p^{j-i} = 1$ e $\zeta_p$ sarebbe soluzione del polinomio $X^{j-i} - 1$ che ha grado strettamente minore di $p-1$ (assurdo). Inoltre $\zeta_p^i \neq 1$ per $1 \leq i \leq p-1$: per $i < p-1$ è lo stesso argoento, per $i = p-1$ se avessimo $\zeta_p^{p-1} = 1$ allora $\zeta_p$ sarebbe zero di $X^{p-1} - 1$ e quindi $f(X) = X^{p-1} - 1$ (assurdo). Segue che $\zeta_p^i$, per $i = 1, \ldots, p-1$, sono tutti e soli gli zeri di $f(X)$. In particolare, $K_p = \mathbb{Q}(\zeta_p)$ ha grado $p-1$ su $\mathbb{Q}$.

(ii) Ogni $\sigma \in G_p$ invia $\zeta_p$ in una radice di $f(X)$. Quindi esiste un unico intero $1 \leq \rho(\sigma) \leq p-1$ tale che $\sigma(\zeta_p) = \zeta_p^{\rho(\sigma)}$. Sia $\rho\colon G_p \to \left(\mathbb{Z}/p\mathbb{Z}\right)^*$ l'applicazione appena definita. Si mostra che è un omomorfismo di gruppi. È iniettivo visto che $K_p = \mathbb{Q}(\zeta_p)$ e quindi ogni $\sigma \in G_p$ è univocamente determinato da dove invia $\zeta_p$. Per ragioni di cardinalità, concludiamo che $\rho$ è un isomorfismo.

(iii) Le estensioni quadratiche di $\mathbb{Q}$ contenute in $K_p$ corrispondono ai sottogruppi di $G_p$ di indice 2 per la teoria di Galois. Sappiamo dal punto (ii) che $G_p \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Basta mostrare che esiste un unico sottogruppo di indice 2 in $\mathbb{Z}/(p-1)\mathbb{Z}$. Ogni tale sottogruppo contiene la classe [2] di 2 e [2] ha ordine $\frac{p-1}{2}$. Quindi esiste un unico sottogruppo di ordine $\frac{p-1}{2}$ in $\mathbb{Z}/(p-1)\mathbb{Z}$, quello generato dalla classe di 2.

Ricordiamo ora che $\mathrm{disc}(\zeta_p) = \epsilon p^{p-2}$ dove $\epsilon = 1$ se $p \equiv 1 \bmod 4$ mentre $\epsilon = -1$ se $p \equiv -1 \bmod 4$. D'altra parte, il discriminante è per definizione il quadrato del determinante $\delta$ di una matrice a coefficienti in $K_p$; perciò $\delta \in K_p$ con $\delta^2 = \epsilon p \left(p^{(p-1)/2}\right)^2$ quindi $\sqrt{\epsilon p} \in K_p$. Possiamo pertanto concludere che se $p \equiv 1 \bmod 4$ allora $\mathbb{Q}(\sqrt{p})$ è l'unica sottoestensione quadratica di $K_p$, mentre se $p \equiv -1 \bmod 4$ allora $\mathbb{Q}(\sqrt{-p})$ è l'unica sottoestensione quadratica di $K_p$.

**Esercizio 3.** Sia $\alpha = \sqrt{-3} + \sqrt[3]{7}$.

(1) Si descriva una chiusura normale $K$ di $\mathbb{Q} \subset \mathbb{Q}(\alpha)$.
(2) Si calcoli il grado $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.
(3) Si calcoli il polinomio minimo di $\alpha$ su $\mathbb{Q}(\sqrt[3]{7})$, su $\mathbb{Q}(\sqrt{-3})$ e su $\mathbb{Q}$.
(4) Il polinomio minimo di $\alpha$ su $\mathbb{Q}(\sqrt{3})$ coincide col polinomio minimo di $\alpha$ su $\mathbb{Q}$?

**Soluzione 3.** Sia $K = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{7})$: è chiaro che $\alpha \in K$; d'altra parte $\alpha \notin \mathbb{Q}(\sqrt{-3})$ quindi $\mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{-3}, \sqrt[3]{7})$. Ma $[\mathbb{Q}(\sqrt{-3}, \sqrt[3]{7}) : \mathbb{Q}(\sqrt{-3})] = 3$ quindi $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{7})$ e $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. Inoltre $K = \mathbb{Q}(\zeta_3, \sqrt[3]{7})$ dove $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ è una radice terza dell'unità. Quindi $K$ è il campo di spezzamento del polinomio $X^3 - 7$ ovvero $K = \mathbb{Q}(\alpha)$ è una estensione normale di $\mathbb{Q}$.

Abbiamo che $(X - \sqrt[3]{7})^2 = -3$ è un polinomio monico in $\mathbb{Z}[\sqrt[3]{7}]$ soddisfatto da $\alpha$: poiché il suo grado è uguale a $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt[3]{7})]$, ne è necessariamente il polinomio minimo. Per lo stesso motivo $(X - \sqrt{-3})^3 = 7$ è il polinomio minimo di $\alpha$ su $\mathbb{Q}(\sqrt{-3})$.

Da quest'ultima relazione ricaviamo che $X^3 - 3\sqrt{-3}X^2 - 9X + 3\sqrt{-3} = 7$, cioè $X^3 - 9X - 7 = 3(X^2-1)\sqrt{-3}$, per cui il polinomio minimo di $\alpha$ è

$$(X^3 - 9X - 7)^2 = -27(X^2-1)^2 \tag{1}$$

Mostriamo che $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$. Supponiamo di no, allora $\mathbb{Q}(\sqrt{3})$ è una sottoestensione quadratica di $K = \mathbb{Q}(\alpha)$. Abbiamo visto che $\mathbb{Q} \subset K$ è di Galois con gruppo di Galois di ordine 6 e non abeliano in quanto $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{7})$ non è di Galois. Quindi $G \cong S_3$ e le sottoestensioni quadratiche di $K$ corrispondono ai sottogruppi di ordine 3 di $G$ o equivalentemente di $S_3$. Ma

in $S_3$ esiste un unico tale sottogruppo, generato da un 3-ciclo. Segue che $\mathbb{Q}(\sqrt{-3})$ è l'unica estensione quadratica di $\mathbb{Q}$ contenuta in $K$ (contraddizione). Quindi $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$ e il grado di $\alpha$ su $\mathbb{Q}(\sqrt{3})$ è 6 e quindi il suo polinomio minimo è quello in (1).

**Esercizio 4.** Si espliciti, al variare di $d$ fra tutti gli interi senza fattori quadrati, la fattorizzazione dell'ideale $3\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ in ideali primi. Si dia una dimostrazione delle precedenti fattorizzazioni.

**Soluzione 4.** Abbiamo

$$3\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \begin{cases} (3, \sqrt{d})^2 & \text{se } d \equiv 0 \bmod 3 \\ (3, 1+\sqrt{d})(3, 1-\sqrt{d}) & \text{se } d \equiv 1 \bmod 3 \\ \text{primo} & \text{se } d \equiv 2 \bmod 3 \end{cases}$$

Supponiamo $d \equiv 0 \bmod 3$: allora $d \in p\mathcal{O}_K$ dove $K = \mathbb{Q}(\sqrt{d})$, quindi $(p, \sqrt{d})^2 \subseteq p\mathcal{O}_K$; d'altra parte $(p, \sqrt{d})^2 \supseteq \mathrm{MCD}(d, p^2) = p$ quindi vale l'uguaglianza. Se $P$ è un ideale primo che divide $(p, \sqrt{d})$ allora $e(P/3)f(P/3)$ divide 2 quindi $(P/3) = 2$ e $P = (p, \sqrt{d})$ che quindi è primo.

Se $d \equiv 1 \bmod 3$, allora

$$(3, 1+\sqrt{d})(3, 1-\sqrt{d}) = (9, 3 \pm 3\sqrt{d}, 1-d^2)$$

Poiché $d^2 \equiv 1 \bmod 3$, abbiamo che $(3, 1+\sqrt{d})(3, 1-\sqrt{d}) \subseteq 3\mathcal{O}_K$. Ci basta osservare che

$$3 = 9 - (3 + 3\sqrt{3}) - (3 - 3\sqrt{3})$$

per concludere che i due ideali sono uguali. Ragionando come sopra, ciascuno dei due è necessariamente primo.

Supponiamo infine che $d \equiv 2 \bmod 3$, quindi in particolare $d$ non è un quadrato in $\mathbb{F}_{3\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$ mentre, ovviamente, lo è in $\mathbb{F}_P = \mathcal{O}_K/P$ dove $P$ è un primo di $\mathcal{O}_K$ su 3. Questo però implica che $\mathbb{F}_P$ sia un'estensione propria di $\mathbb{F}_{3\mathbb{Z}}$ e che quindi $f(P/3\mathbb{Z}) = 2$; perciò $e(P/3\mathbb{Z}) = 1$ ed esiste un unico primo di $\mathcal{O}_K$ su 3. In altre parole: $P = 3\mathcal{O}_K$.