SOLUZIONI DEL COMPITINO DEL 16/11/2017

Esercizio 1. Si consideri il polinomio $f(X) = X^3 - 9 \in \mathbb{Q}[X]$ e sia $E \subset \mathbb{C}$ il suo campo di spezzamento.

(1) Determinare il grado di $[E : \mathbb{Q}]$. Esibire una base di E come $\mathbb{Q}$-spazio vettoriale.
(2) Dimostrare che $\mathbb{Q} \subset E$ è una estensione di Galois. Descrivere tutti gli elementi del gruppo di Galois $G_{E/\mathbb{Q}}$ di E su $\mathbb{Q}$.
(3) Trovare $\eta \in E$ tale che $E = \mathbb{Q}(\eta)$.
(4) Esibire un generatore di $E \cap \mathbb{R}$ come estensione di $\mathbb{Q}$.

Soluzione: (1) Avendo grado 3, sappiamo che $X^3 - 9$ è irriducibile in $\mathbb{Q}[X]$ se e solo se non ha radici radici in $\mathbb{Q}$ e sappiamo anche che, se $x = \frac{r}{s}$ con $r, s \in \mathbb{Z}$ tali che $(r, s) = 1$ è una radice, allora $r \mid 9$ ed $s \mid 1$, ovvero $x \in \{\pm 1, \pm 3, \pm 9\}$. Abbiamo

$$f(1) = -8,\ f(-1) = -10,\ f(3) = 18,\ f(-3) = -36,\ f(9) = 9^3 - 9 \text{ ed } f(-9) = -9^3 - 9.$$

Dunque $X^3 - 9$ è irriducibile in $\mathbb{Q}[X]$, coincide con il polinomio minimo di α su $\mathbb{Q}$ e, pertanto,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg\left(X^3 - 9\right) = 3.$$

D'altra parte

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\Phi_3) = 2.$$

Essendo i gradi coprimi deduciamo che

$$[E : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}]\,[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$$

e che, poiché $\left\{1, \alpha, \alpha^2\right\}$ (risp. $\{1, \zeta\}$) è base di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$ (risp. $\mathbb{Q}(\zeta)$ su $\mathbb{Q}$),

$$\left\{1, \alpha, \alpha^2, \zeta, \alpha\zeta, \alpha^2\zeta\right\}$$

è base di E su $\mathbb{Q}$.

(2) Abbiamo che, posto $R_f := \left\{\alpha, \alpha\zeta, \alpha\zeta^2\right\}$, il campo di spezzamento di $f \in \mathbb{Q}[X]$ è $\mathbb{Q}(R_f)$. Ovviamente $\mathbb{Q}(R_f) \subset \mathbb{Q}(\alpha, \zeta)$ ma vale anche l'altra inclusione, essendo $\alpha \in \mathbb{Q}(R_f)$ e $\zeta = \frac{\alpha\zeta}{\alpha} \in \mathbb{Q}(R_f)$. Dunque $E = \mathbb{Q}(R_f)$ è di Galois su $\mathbb{Q}$, essendo campo di spezzamento di un polinomio separabile su $\mathbb{Q}$. Sappiamo anche che

$$G_{E/\mathbb{Q}} \longrightarrow Aut(R_f) \simeq S_3$$

dove l'identificazione si ottiene identificando $\left\{\alpha, \alpha\zeta, \alpha\zeta^2\right\}$ ed $\{1, 2, 3\}$ come insiemi ordinati. L'applicazione è infatti iniettiva e, poichè

$$\#G_{E/\mathbb{Q}} = [E : \mathbb{Q}] = 6,$$

si trattadi un isomorfismo di gruppi. Dunque

$$G_{E/\mathbb{Q}} = \left\langle \rho := \left(\alpha, \alpha\zeta, \alpha\zeta^2\right), \sigma := \left(\alpha\zeta, \alpha\zeta^2\right) \right\rangle \simeq \langle (123), (23) \rangle.$$

(3) Notiamo che

$$\rho(\zeta) = \rho\left(\frac{\alpha\zeta}{\alpha}\right) = \frac{\rho(\alpha\zeta)}{\rho(\alpha)} = \frac{\alpha\zeta^2}{\alpha\zeta} = \zeta$$
$$\sigma(\zeta) = \sigma\left(\frac{\alpha\zeta}{\alpha}\right) = \frac{\sigma(\alpha\zeta)}{\sigma(\alpha)} = \frac{\alpha\zeta^2}{\alpha} = \zeta^2.$$

Mostriamo che l'orbita di $\eta := \alpha + \zeta$ ha 6 elementi, da cui segue che $E = \mathbb{Q}(\eta)$. Abbiamo che:

$$\begin{array}{cc|l}
\sigma^i\rho^j & \sigma^i\rho^j(\eta) & \\
1 & \alpha+\zeta, & \\
\rho & \rho(\alpha+\zeta) & = \rho(\alpha)+\rho(\zeta) = \alpha\zeta+\zeta, \\
\rho^2 & \rho^2(\alpha+\zeta) & = \rho^2(\alpha)+\rho^2(\zeta) = \rho(\zeta\alpha)+\zeta = \rho(\zeta)\rho(\alpha)+\zeta = \zeta^2\alpha+\zeta \\
 & & = -\alpha(\zeta+1)+\zeta = \zeta-\alpha-\alpha\zeta, \\
\sigma & \sigma(\alpha+\zeta) & = \alpha+\zeta^2 = -1-\zeta+\alpha, \\
\sigma\rho & \sigma(\rho(\alpha+\zeta)) & = \sigma(\zeta\alpha+\zeta) = \sigma(\zeta)\sigma(\alpha)+\sigma(\zeta) = \zeta^2\alpha+\zeta^2 \\
 & & = -(\zeta+1)\alpha + -(\zeta+1) = -1-\zeta-\alpha-\alpha\zeta, \\
\sigma\rho^2 & \sigma\left(\rho^2(\alpha+\zeta)\right) & = \sigma\left(\zeta^2\alpha+\zeta\right) = \sigma(\zeta)^2\sigma(\alpha)+\sigma(\zeta) = \zeta^4\alpha+\zeta^2 = \zeta\alpha+\zeta^2 \\
 & & = \zeta\alpha-(\zeta+1) = -1-\zeta+\alpha\zeta.
\end{array}$$

Avendo questi elementi differenti espressioni nella base di $E/\mathbb{Q}$ trovata in (1), sono a due a due distinti e, dunque, l'orbita di $\eta := \alpha + \zeta$ ha 6 elementi.

(4) Poichè $\overline{\alpha} = \alpha$ e $\overline{\zeta} = \zeta^2$, il coniugio complesso si restringe a σ in E. Pertanto, s $x \in E$,

$$x \in \mathbb{R} \;\Leftrightarrow\; \sigma(x) = \overline{x} = x,$$

i.e.

$$E \cap \mathbb{R} = E^{\langle c \rangle}.$$

Notiamo che $\mathbb{Q}(\alpha) \subset E \cap \mathbb{R}$ e, d'altra parte,

$$\begin{aligned}
\left[E^{\langle c\rangle} : \mathbb{Q}\right] &= \left[E^{\langle c\rangle} : E^{G_{E/\mathbb{Q}}}\right] \\
&= \left[G_{E/\mathbb{Q}} : \langle c\rangle\right] = \frac{6}{3} = 2.
\end{aligned}$$

Poichè $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, segue che $\mathbb{Q}(\alpha) = E \cap \mathbb{R}$.

Esercizio 2. Sia dato il polinomio

$$f(X) = \left(X^2+1\right)\left(X^2-3\right) \in \mathbb{Q}[X],$$

(1) Si espliciti il campo di spezzamento E di $f(X)$ su $\mathbb{Q}$ trovandone dei generatori ed il grado come estensione di $\mathbb{Q}$.
(2) Si determinino tutti i sottocampi K di E, esibendone un generatore α come estensione di $\mathbb{Q}$, ovvero tale che $K = \mathbb{Q}(\alpha)$. Si dica quali di queste estensioni sono contenute in $\mathbb{R}$.
(3) Per ogni sottocampo K di E , determinare il polinomio minimo su $\mathbb{Q}$ del generatore α trovato in (2).

Soluzione: Poichè $X^2+1, X^2-3 \in \mathbb{Q}[X]$ sono irriducibili (il primo poichè $i \notin \mathbb{R}$ ed il secondo per il criterio di Eisenstein con $p = 3$),

$$\left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = [\mathbb{Q}(i) : \mathbb{Q}] = 2.$$

Inoltre $i \notin \mathbb{Q}\left(\sqrt{3}\right) \subset \mathbb{R}$, pertanto $X^2+3 \in \mathbb{Q}(i)[X]$ è irriducibile,

$$\left[\mathbb{Q}\left(\sqrt{3}, i\right) : \mathbb{Q}(i)\right] = 2$$

e

$$\left[\mathbb{Q}\left(\sqrt{3}, i\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{3}, i\right) : \mathbb{Q}(i)\right][\mathbb{Q}(i) : \mathbb{Q}] = 4.$$

Notiamo inoltre che $\mathbb{Q}\left(\sqrt{3}, i\right) = \mathbb{Q}\left(\pm\sqrt{3}, \pm i\right) = E$. Poichè $G_{E/\mathbb{Q}}$ è un gruppo di ordine 4, abbiamo $G_{E/\mathbb{Q}} \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$, oppure $G_{E/\mathbb{Q}} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$. Ma abbiamo notato che $X^2+3 \in \mathbb{Q}(i)[X]$ è irriducibile, pertanto $\overline{\psi_{\pm\sqrt{3}}} : \frac{\mathbb{Q}(i)[X]}{(X^2+3)} \xrightarrow{\sim} \mathbb{Q}\left(i, \sqrt{3}\right)$ è un isomorfismo e $\sigma := \overline{\psi_{-\sqrt{3}}} \circ \overline{\psi_{\sqrt{3}}}^{-1}$ è un

automorfismo di E che fissa $\mathbb{Q}(i)$ e che manda $\sqrt{3}$ in $-\sqrt{3}$. D'altra parte, poichè $E/\mathbb{Q}$ è di Galois, il coniugio complesso c agisce su questo campo fissando $\mathbb{Q}\left(\sqrt{3}\right) \subset \mathbb{R}$ e mandando i in $-i$. Notiamo che

$$\begin{aligned}(\sigma c)\left(\sqrt{3}\right) &= \sigma\left(\sqrt{3}\right) = -\sqrt{3},\\ (\sigma c)(i) &= -\sigma(i) = -i,\end{aligned}$$

da cui vediamo che σ, c e σc sono tre elementi di $G_{E/\mathbb{Q}}$ di ordine 2. Segue che $G_{E/\mathbb{Q}} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$, che ha 3 sottogruèèi propri, ovvero:

$$H \in \{\langle\sigma\rangle, \langle c\rangle, \langle\sigma c\rangle\}.$$

Poichè $\mathbb{Q}\left(\sqrt{3}\right)$, $\mathbb{Q}(i)$ e $\mathbb{Q}\left(\sqrt{3}i\right)$ sono tre sottocampi propri di $E/\mathbb{Q}$, sono tutti. Infatti $\mathbb{Q}\left(\sqrt{3}\right) \subset E^{\langle c\rangle}$ (rispettivamente $\mathbb{Q}(i) \subset E^{\langle\sigma\rangle}$), da cui l'uguaglianza e, per differenza, necessariamente $\mathbb{Q}\left(\sqrt{3}i\right) = E^{\langle\sigma c\rangle}$. I polinomi minimi di $\alpha = \sqrt{3}$ ed $\alpha = i$ sono già stati calcolati, mentre X^2+3 è il polinomio minimo di $\alpha = \sqrt{3}i$. Notiamo che, posto $\alpha := \sqrt{3}+i$, abbiamo

$$\begin{aligned}\alpha^2 &= 3 + 2i\sqrt{3} - 1 = 2 + 2i\sqrt{3}\\ &\Leftrightarrow\ 2i\sqrt{3} = \alpha^2 - 2\\ &\Rightarrow\ -12 = \left(\alpha^2-2\right)^2 = \alpha^4 - 4\alpha^2 + 4.\end{aligned}$$

Pertanto α è radice del polinomio

$$f(X) := X^4 - 4X^2 + 16 \in \mathbb{Q}[X].$$

Mostriamo che il polinomio minimo di α su $\mathbb{Q}$ ha grado 4, da cui seguirà che è $f(X)$ è il polinomio minimo e che $\mathbb{Q}\left(\sqrt{3}, i\right) = \mathbb{Q}(\alpha)$. Infatti, il grado del polinomio minimo è la cardinalità dell'orbita di α sotto l'azione del gruppo di Galois. Abbiamo

$$\begin{aligned}&\alpha = \sqrt{3}+i, \sigma(\alpha) = -\sqrt{3}+i,\\ &c(\alpha) = \sqrt{3}-i,\ \sigma(c(\alpha)) = \sigma\left(\sqrt{3}-i\right) = -\sqrt{3}-i\end{aligned}$$

che sono quattro elementi distinti (essendo $\left\{1, \sqrt{3}, i, i\sqrt{3}\right\}$ una base di E su $\mathbb{Q}$). Infine, evidentemente solo $\mathbb{Q}$ e $\mathbb{Q}\left(\sqrt{3}\right)$ sono sottocampi reali di E.

Esercizio 3. Si dimostrino le seguenti affermazioni.

(1) Se E/F è una estensione finita di campi ed $\alpha \in E$, allora detto $f_{\alpha,F}(X) \in F[X]$ il polinomio minimo di α su F,
$$[F(\alpha) : F] = \deg(f_{\alpha,F})$$
(2) Per ogni $n \in \mathbb{N}$, esiste una estensione di campi $\mathbb{Q} \subset E$ tale che $[E : \mathbb{Q}] = n$.
(3) Sia F una estensione quadratica di $\mathbb{Q}$. Allora, per ogni $n \in \mathbb{N}$, esiste una estensione di campi $F \subset E$ tale che $[E : F] = n$.

Soluzione: (1) Infatti $\overline{\psi_\alpha} : \frac{F[X]}{(f_{\alpha,F}(X))} \to F(\alpha)$ è ben definita poichè $f_{\alpha,F}(\alpha) = 0$, suriettiva poichè $F(\alpha) = F[\alpha]$ (poichè un dominio di dimensione finita su un campo è un campo) ed iniettiva poichè $\frac{F[X]}{(f_{\alpha,F}(X))}$ è campo (per lo stesso motivo essendo $f_{\alpha,F}(X) \neq 0$, o poichè $0 \neq f_{\alpha,F}(X)$ è irriducibile ed $F[X]$ è PID). Segue che $\overline{\psi_\alpha}$ è isomorfismo, dunque

$$[F(\alpha) : F] = \dim_F\left(\frac{F[X]}{(f_{\alpha,F}(X))}\right) = \deg(f_{\alpha,F})$$

(la seconda uguaglianza grazie all'esistenza del resto con divisione per $f_{\alpha,F}(X) \neq 0$).

Poichè $[F(\alpha):F]=\deg(f_{\alpha,F})$ (per (1)) per verificare (2) e (3) basta mostrare che, per ogni $n\in\mathbb{N}$, esiste un polinomio $f(X)\in F[X]$ irriducibile in $F[X]$ di grado n (ed infatti, per il teorema dell'elemento primitivo, questa affermazione è equivalente alla tesi).

(2) Possiamo considerare la famiglia di polinomi

$$f_n(X)=X^n+2X^{n-1}+...+2\in\mathbb{Q}[X],$$

che è irriducibile per il criterio di Eisenstein.

(3) Diamo due possibili soluzioni.

Prima soluzione (assumedo $F\neq\mathbb{Q}(i)$) Poichè F è quadratica, si ha $F=\mathbb{Q}\left(\sqrt{D}\right)$ con $D\in\mathbb{Z}$ privo di quadrati e supponiamo $D\neq-1$. Come nella risoluzione del punto (2) del precedente esercizio, vediamo che $X^{2n}-D\in\mathbb{Q}[X]$ è irriducibile per Eisenstein applicato ad un primo $p\mid D$, essendo $D\neq-1$, ed una sua radice α genera una estensione tale che $[\mathbb{Q}(\alpha):\mathbb{Q}]=2n$. Ma, poichè $\alpha^n=\pm\sqrt{D}$, si ha $F=\mathbb{Q}\left(\sqrt{D}\right)\subset\mathbb{Q}(\alpha)=:E$ e, per moltiplicatività dei gradi,

$$[E:F]=\frac{[E:\mathbb{Q}]}{[F:\mathbb{Q}]}=\frac{2n}{2}=n.$$

Seconda soluzione Se n è dispari, detta α una radice di $f_n(X)$, abbiamo che $([F:\mathbb{Q}],[\mathbb{Q}(\alpha):\mathbb{Q}])=1$, da cui si deduce facilmente che

$$[F(\alpha):F]=[\mathbb{Q}(\alpha):\mathbb{Q}]=n.$$

Se $n=2^m$ ed $F=\mathbb{Q}\left(\sqrt{D}\right)$ (con $D\in\mathbb{Z}$ privo di quadrati), possiamo considerare una famiglia $\{p_1,...,p_m\}$ di primi coprimi con D e tra loro distinti. Mostreremo sotto per induzione che, posto $F_0=F$ ed $F_i=F_{i-1}\left(\sqrt{p_i}\right)$ per $i\geq1$, si ha che F_i/F_{i-1}è una estensione di grado due e, dunque,

$$[F_m:F]=2^m=n.$$

Mostrato ciò, in generale scriviamo $n=2^mn_0$ in modo tale che $(2,n_0)=1$. Detta F_1/F (risp. F_2/F) una estensione di grado 2^m (risp. n_0), abbiamo che, poichè

$$([F_1:F],[F_2:F])=(2^m,n_0)=1,$$

l'estensione E_1E_2/F ha grado

$$[F_1F_2:F]=[F_1:F][F_2:F]=2^mn_0=n.$$

Per verificare la tesi induttiva mostriamo più precisamente che $F_m/\mathbb{Q}$ è una estensione di Galois grado 2^{m+1} e $G_{F_m/\mathbb{Q}}\simeq\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{m+1}$ in modo tale che la 0-esima copia di $\frac{\mathbb{Z}}{2\mathbb{Z}}$ si identifica con $G_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}$ e la i-esima copia di $\frac{\mathbb{Z}}{2\mathbb{Z}}$ con $G_{\mathbb{Q}(\sqrt{p_i})/\mathbb{Q}}$ nella decomposizione $G_{F_{m+1}/\mathbb{Q}}\simeq\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{m+1}$. Se $m=0$ la tesi segue dal fatto che $X^2-D\in\mathbb{Q}[X]$ è irriducibile. Supponiamo ora di conoscere la tesi per m e mostriamola per $m+1$. Poichè $\mathbb{Q}\left(\sqrt{p_{m+1}}\right)/\mathbb{Q}$ è di Galois e di grado due ed $F_m/\mathbb{Q}$ è una estensione di Galois tale che $G_{F_m/\mathbb{Q}}\simeq\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{m+1}$, una volta verificato che $F_m\cap\mathbb{Q}\left(\sqrt{p_{m+1}}\right)=\mathbb{Q}$ seguirà

$$G_{F_{m+1}/\mathbb{Q}}\simeq\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{m+1}\times\frac{\mathbb{Z}}{2\mathbb{Z}}=\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{m+2}.$$

Resta da mostrare che $\sqrt{p_{m+1}}\notin F_m=\mathbb{Q}\left(\sqrt{D},\sqrt{p_1},...,\sqrt{p_m}\right)$. In caso contrario, $\mathbb{Q}\left(\sqrt{p_{m+1}}\right)\subset F_m$ è una sottoestensione di grado due, che corrisponde ad un sottogruppo di indice 2, ovvero ad un sottospazio di $G_{F_m/\mathbb{Q}}\simeq\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{m+1}$ di codimensione 1. Ma questi sottospazi sono definiti da una equazione lineare $a_0X_0+...+a_mX_m$ a coefficienti $a_i\in\frac{\mathbb{Z}}{2\mathbb{Z}}$ non tutti nulli e due stringhe di coefficienti definiscono lo stesso sottospazio se e solo se differiscono per moltiplicazione per uno scalare λ non-nullo, ovvero $\lambda=1$: ci sono dunque $2^{m+1}-1$ sottogruppi di indice 2.

D'altra parte, consideriamo l'insieme ordinato di $m+1$ elementi $\left\{\sqrt{D}, \sqrt{p_1}, ..., \sqrt{p_m}\right\}$ e, per l'i-esimo elemento sia $a_i \in \frac{\mathbb{Z}}{2\mathbb{Z}}$ uguale a zero se non lo scegliamo oppure 1 se lo scegliamo; posto $\alpha := \sqrt{D}^{a_0}\sqrt{p_1}^{a_1}..., \sqrt{p_m}^{a_m}$ abbiamo che $\mathbb{Q}(\alpha)$ è una estensione di grado due a patto che gli a_i non siano tutti nulli. Abbiamo dunque esibito $2^{m+1}-1$ sottoestensioni quadratiche di $F_m/\mathbb{Q}$ ed inoltre, se identifichiamo la 0-esima copia di $\frac{\mathbb{Z}}{2\mathbb{Z}}$ con $G_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}$ e la i-esima copia di $\frac{\mathbb{Z}}{2\mathbb{Z}}$ con $G_{\mathbb{Q}(\sqrt{p_i})/\mathbb{Q}}$ nella decomposizione $G_{F_{m+1}/\mathbb{Q}} \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{m+1}$ come da ipotesi induttiva, vediamo che $\mathbb{Q}(\alpha) \subset F_{m+1}^{\left\langle \sigma_0^{a_0'}...\sigma_m^{a_m'} \right\rangle}$, dove σ_i genera la i-esima copia di $\frac{\mathbb{Z}}{2\mathbb{Z}}$ nella decomposizione $G_{F_{m+1}/\mathbb{Q}} \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{m+1}$ ed $a_i' = a_i + 1$ è 0 oppure 1 a seconda che a_i sia 1 o, rispettivamente, 0. Poichè $\left\langle \sigma_0^{a_0'}...\sigma_m^{a_m'} \right\rangle$ corrisponde al sottospazio di codimensione 1 definito dall'equazione $a_0X_0+...+a_mX_m$, vediamo che $\mathbb{Q}(\alpha) = F_{m+1}^{\left\langle \sigma_0^{a_0'}...\sigma_m^{a_m'} \right\rangle}$ e che tutte le sottoestensioni quadratiche sono ottentute in questo modo. Segue che $\mathbb{Q}\left(\sqrt{p_{m+1}}\right) \subset F_m$ implica $\mathbb{Q}\left(\sqrt{p_{m+1}}\right) = \mathbb{Q}(\alpha)$ con $\alpha := \sqrt{D}^{a_0}\sqrt{p_1}^{a_1}..., \sqrt{p_m}^{a_m}$. Ma allora possiamo scrivere

$$\sqrt{p_{m+1}} = a + b\sqrt{D}^{a_0}\sqrt{p_1}^{a_1}..., \sqrt{p_m}^{a_m} \text{ con } a, b \in \mathbb{Q},$$

da cui prendendo il quadrato

$$p_{m+1} = a^2 + b^2 D^{a_0} p_1^{a_1}...p_m^{a_m} + 2ab\sqrt{D}^{a_0}\sqrt{p_1}^{a_1}..., \sqrt{p_m}^{a_m}.$$

Se $ab \neq 0$ si ottiene la contraddizione $\sqrt{D}^{a_0}\sqrt{p_1}^{a_1}..., \sqrt{p_m}^{a_m} \in \mathbb{Q}$ (per Eisenstein, notando che gli a_i non sono tutti nulli, per esempio). Dunque $ab = 0$, ma se $b = 0$ si ottiene la contraddizione $\sqrt{p_{m+1}} \in \mathbb{Q}$ (ancora per Eisenstein, per esempio). Pertanto $a = 0$, da cui $\frac{\sqrt{p_{m+1}}}{\sqrt{D}^{a_0}\sqrt{p_1}^{a_1}..., \sqrt{p_m}^{a_m}} \in \mathbb{Q}$, che non è possibile per Eisenstein che si applica, grazie al fatto che p_{m+1} è coprimo con D, p_1,..., p_m, al polinomio

$$D^{a_0}p_1^{a_1}...p_m^{a_m}X^2 - p_{m+1} \in \mathbb{Z}[X].$$