Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2020-2021
AL310 - Istituzioni di Algebra Superiore
5 Gennaio 2021 - Esercitazione n. 6

Fatti generali utili per la risoluzione degli esercizi

1. (Gabelli, Corollario 9.3.2, caso $\mathbb{F} = \mathbb{Q}$) Sia $f(x) = x^3 + px + q \in \mathbb{Q}[x]$ irriducibile. Il suo discriminante à dato da $D(f) = -(4p^3 + 27q^2)$.
   - Se $D(f) < 0$ allora $f(x)$ ha una sola radice reale e il suo gruppo di Galois è isomorfo a S_3.
   - Se $D(f) > 0$ allora $f(x)$ ha tre radici reali. Il suo gruppo di Galois è isomorfo a A_3 se $\sqrt{D(f)} \in \mathbb{Q}$, a S_3 altrimenti.

2. (Gabelli, Proposizione 8.1.12) Sia $f(x) = x^4+ax^2+c \in \mathbb{Q}[x]$ un polinomio irriducibile e si ponga $t = a^2 - 4c$. Allora le radici di f sono

$$\gamma_1 = \alpha = \sqrt{-\frac{a}{2} + \frac{1}{2}\sqrt{t}},\ \gamma_2 = \beta = \sqrt{-\frac{a}{2} - \frac{1}{2}\sqrt{t}},\ \gamma_3 = -\alpha,\ \gamma_4 = -\beta.$$

   Se G indica il gruppo di Galois di f abbiamo che

   (a) $\sqrt{c} \in \mathbb{Q}$ sse G è isomorfo al gruppo di Klein $V_4 = \langle(12)(34)\rangle \oplus \langle(13)(24)\rangle$;

   (b) $\sqrt{ct} \in \mathbb{Q}$ sse G è isomorfo al gruppo ciclico $\mathbb{Z}_4 = \langle(1234)\rangle)$;

   (c) $\sqrt{c} \notin \mathbb{Q}$ e $\sqrt{tc} \notin \mathbb{Q}$ sse G è isomorfo al gruppo diedrale $D_4 = \langle(1234), (13)\rangle$.

3. (Gabelli, Teorema 5.2.6) $\mathbb{F} \subseteq \mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ è normale sse $\mathbb{K}$ contiene tutti i coniugati di $\alpha_i, i = 1, 2, \ldots, n$.

4. (Gabelli, Corollario 11.3.3.) Sia $\alpha \in \mathbb{C}$. Se $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ è pari ad una potenza di 2 e $\mathbb{Q} \subseteq Q(\alpha)$ è normale, allora α è costrubile.

5. (Gabelli, Proposizione 8.3.11) Sia p un numero primo. Allora

   (i) $\sqrt{p} \in \mathbb{Q}(\zeta_p)$ se $p \equiv 1 \bmod 4$

   (ii) $i\sqrt{p} \in \mathbb{Q}(\zeta_p)$ se $p \equiv 3 \bmod 4$

   (iii) $\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$ se $p \equiv 3 \bmod 4$

   (iv) $\sqrt{2} \in \mathbb{Q}(\zeta_8)$.

   Pertanto se $d \in \mathbb{Z}$ è privo di fattori quadratici allora $\sqrt{d} \in \mathbb{Q}(\zeta_{8|d|})$ (nota: la mia impressione è che sia sufficiente $4|d|$, vedi osservazione nell'esercizio 9).

Esercizio 1. Sia $\zeta \in \mathbb{C}$ una radice primitiva tredicesima dell'unità.

(i) Determinare una base di $\mathbb{Q}(\zeta^2)$ su $\mathbb{Q}$ che contenga l'elemento $\zeta + \zeta^3$.

(ii) Spiegare perché il reticolo dell'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$ contiene sei campi.

(iii) Esplicitare la corrispondenza di Galois per $\mathbb{Q}(\zeta)$, esibendo un elemento primitivo per ciascun sottocampo.

(iv) Individuare i sottocampi reali di $\mathbb{Q}(\zeta)$.

(v) Determinare una risolvente di Galois per l'estensione

$$\mathbb{Q}(\zeta + \zeta^3 + \zeta^4 + \zeta^9 + \zeta^{10} + \zeta^{12}) \subseteq \mathbb{Q}(\zeta + \zeta^3 + \zeta^9).$$

(vi) Stabilire se $\zeta + \zeta^3 + \zeta^9$ è un numero complesso costruibile. In caso affermativo, esprimerlo in forma radicale.

Osserviamo per prima cosa che $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^2)$. L'inclusione $\supseteq$ è ovvia, mentre l'inclusione $\subseteq$ segue dal fatto che $\zeta = (\zeta^2)^7 \in \mathbb{Q}(\zeta^2)$. Una base di $Q(\zeta)$ è data da $\{1, \zeta, \zeta^2, \zeta^3, \dots, \zeta^{11}\}$. D'altra parte si può sempre rimpiazzare un elemento di una base con la somma dello stesso elemento con un altro elemento della stessa base e quindi $\{1, \zeta, \zeta^2, \zeta + \zeta^3, \dots, \zeta^{11}\}$ è un'altra base di $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^2)$.

Il gruppo di Galois G di $\mathbb{Q}(\zeta)$ è ciclico di ordine 12 e generato dall'automorfismo Ψ_2 (si ricorda che $\Psi_k(\zeta) = \zeta^k$). Un gruppo ciclico di ordine n possiede un unico sottogruppo (ciclico) di ordine d per ogni divisore d di n (e non vi sono altri sottogruppi). I sottogruppi non banali sono

1. $\langle \Psi_2^2 = \Psi_4 \rangle \cong \mathbb{Z}_6$
2. $\langle \Psi_2^3 = \Psi_8 \rangle \cong \mathbb{Z}_4$
3. $\langle \Psi_2^4 = \Psi_3 \rangle \cong \mathbb{Z}_3 \leq \mathbb{Z}_6$
4. $\langle \Psi_2^6 = \Psi_{12} \rangle \cong \mathbb{Z}_2 \leq \mathbb{Z}_6, \mathbb{Z}_4$.

Di conseguenza abbiamo i seguenti sottocampi non banali di $\mathbb{Q}(\zeta)$ (ovviamente tutti normali, essendo G Abeliano).

1. $\mathbb{Q}(\zeta)^{\langle \Psi_4 \rangle}$ che ha grado 2 su $\mathbb{Q}$
2. $\mathbb{Q}(\zeta)^{\langle \Psi_8 \rangle}$ che ha grado 3 su $\mathbb{Q}$
3. $\mathbb{Q}(\zeta)^{\langle \Psi_3 \rangle}$ che ha grado 4 su $\mathbb{Q}$
4. $\mathbb{Q}(\zeta)^{\langle \Psi_{12} \rangle}$ che ha grado 6 su $\mathbb{Q}$.

Determiniamo un elemento primitivo per ciascun sottocampo.

Consideriamo l'orbita di ζ sotto l'azione di Ψ_4: $\zeta \to \zeta^4 \to \zeta^3 \to \zeta^{12} \to \zeta^9 \to \zeta^{10} \to \zeta$. Pertanto, $\mathbb{Q}(\zeta + \zeta^4 + \zeta^3 + \zeta^{12} + \zeta^9 + \zeta^{10}) \subseteq \mathbb{Q}(\zeta)^{\langle \Psi_4 \rangle}$. Poiché $[\mathbb{Q}(\zeta)^{\langle \Psi_4 \rangle} : \mathbb{Q}]$ è un primo, abbiamo che $\mathbb{Q}(\zeta)^{\langle \Psi_4 \rangle}$ non contiene sottocampi non banali; d'altra parte $\zeta + \zeta^4 + \zeta^3 + \zeta^{12} + \zeta^9 + \zeta^{10} \notin \mathbb{Q}$ in quanto $\{1, \zeta, \zeta^2, \zeta^3, \dots, \zeta^{11}\}$ è una base di $\mathbb{Q}(\zeta)$ ($\zeta^{12} = -1 - \zeta - \cdots - \zeta^{11}$) e quindi possiamo concludere che

$$\mathbb{Q}(\zeta)^{\langle \Psi_4 \rangle} = \mathbb{Q}(\zeta + \zeta^4 + \zeta^3 + \zeta^{12} + \zeta^9 + \zeta^{10}).$$

In maniera perfettamente analoga si dimostra che

$$\mathbb{Q}(\zeta)^{\langle \Psi_8 \rangle} = \mathbb{Q}(\zeta + \zeta^8 + \zeta^{12} + \zeta^5).$$

Come sopra si vede facilmente che $\mathbb{Q}(\zeta+\zeta^{12}) \subseteq \mathbb{Q}(\zeta)^{\langle\Psi_{12}\rangle}$. Per mostrare che vale l'uguaglianza è sufficiente mostrare che

$$[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta+\zeta^{12})] = 2 \ (= [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta)^{\langle\Psi_{12}\rangle}]).$$

Osserviamo che Ψ_{12} coincide con il coniugio: $\zeta^{12} = \zeta^{-1} = \overline{\zeta}$. Quindi

$$\mathbb{Q}(\zeta+\zeta^{12}) = \mathbb{Q}(\zeta+\overline{\zeta}) = \mathbb{Q}(\zeta+\overline{\zeta}, \zeta\overline{\zeta})$$

(dove l'ultima uguaglianza segue dal fatto che $\zeta\overline{\zeta} = 1$). Il polinomio $x^2 - (\zeta + \overline{\zeta})x + \zeta\overline{\zeta} \in \mathbb{Q}(\zeta+\zeta^{12})[x]$ ha come radici ζ e $\overline{\zeta}$ e quindi

$$\mathbb{Q}(\zeta)^{\langle\Psi_{12}\rangle} = \mathbb{Q}(\zeta+\zeta^{12}).$$

Come sopra si verifica facilmente che $\mathbb{Q}(\zeta+\zeta^3+\zeta^9) \subseteq \mathbb{Q}(\zeta)^{\langle\Psi_3\rangle}$. D'altra parte $\zeta+\zeta^3+\zeta^9 \notin \mathbb{R}$ e pertanto $\mathbb{Q}(\zeta+\zeta^3+\zeta^9)$ non può coincidere con nessuno dei sottocampi precedenti (che sono reali) e quindi deve necessariamente coincidere con $\mathbb{Q}(\zeta)^{\langle\Psi_3\rangle}$. Ovviamente i campi reali sono quelli contenuti in $\mathbb{Q}(\zeta+\zeta^{12})$.

Poniamo $\beta = \zeta+\zeta^3+\zeta^9$ ed $\alpha = \zeta+\zeta^4+\zeta^3+\zeta^{12}+\zeta^9+\zeta^{10}$. Abbiamo visto che $\mathbb{Q}(\beta) \supseteq \mathbb{Q}(\alpha)$ e che $[\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)] = 2$. Inoltre segue dalla teoria di Galois che

$$\mathrm{Gal}_{\mathbb{Q}(\alpha)}(\mathbb{Q}(\beta)) = \frac{\langle\Psi_4\rangle}{\langle\Psi_3\rangle} = \langle\Psi_4\langle\Psi_3\rangle\rangle \cong \mathbb{Z}_2.$$

Pertanto il polinomio minimo di β su $\mathbb{Q}(\alpha)$ è dato da

$$m_\beta(x) = x^2 - (\beta + \Psi_4(\beta))x + \beta\Psi_4(\beta) = x^2 - \alpha x + (2-\alpha)$$

(ho fatto una correzione: Errata: $4-\alpha$ Corrige: $2-\alpha$). Questo permette di esprimere β attraverso radicali di α:

$$\beta = \frac{\alpha \pm \sqrt{\alpha^2 - 4(2-\alpha)}}{2}.$$

β è costruibile in quanto $\mathbb{Q}(\beta)$ è normale e $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. Ragionando come nel caso del calcolo di m_β, otteniamo che il polinomio minimo di α su $\mathbb{Q}$ è dato da $m_\alpha(x) = x^2 + x - 3$. Se $\zeta = \exp(2\pi i/13)$ si ha che

$$\alpha = \frac{-1+\sqrt{13}}{2} \text{ e } \beta = \frac{1}{4}\left(-1+\sqrt{13}+2i\sqrt{\frac{13}{2} - \frac{3\sqrt{13}}{2}}\right).$$

Osservazione. Nell'analisi di questa estensione abbiamo utilizzato pesantemente il fatto che 13 è un numero primo.

Esercizio 2. Mostrare che un campo finito non può avere ampliamenti biquadratici.

Dato un campo $\mathbb{F}$, un suo ampliamento biquadratico $\mathbb{F}(\alpha,\beta)$ è un ampliamento di grado 4 su $\mathbb{F}$ che contiene i due ampliamenti distinti quadratici $\mathbb{F}(\alpha)$ e $\mathbb{F}(\beta)$. Pertanto il suo gruppo di Galois non può essere ciclico. D'altra parte il gruppo di Galois di un'estensione finita di un campo finito è sempre ciclico e pertanto non possono esistere ampliamenti biquadratici di un campo finito (esistono però amplimenti biquadratici di campi di caratteristica p).

Esercizio 3. Mostrare che il gruppo di Galois su $\mathbb{Q}$ del polinomio $f(x) = x^3 - 3x + 1$ è isomorfo ad A_3.

$f(x)$ è irriducibile su $\mathbb{Q}$,in quanto non ha radici razionali. Il discriminante di f è dato da $D(f) = -(4(-27) + 27) = 81 > 0$. Poich'e' $9 = \sqrt{81} \in \mathbb{Q}$ possiamo concludere (Fatto 1) che il gruppo di Galois è isomorfo ad A_3. Se $\alpha_1 = \alpha \in \mathbb{R}$ è una radice, le altre sono $\alpha_2 = \alpha^2 - 2$ e $\alpha_3 = -\alpha - \alpha^2 + 2$. Il campo di spezzamento è dato quindi da $\mathbb{Q}(\alpha)$. I tre automorfismi sono dati dall'identità, da $\Psi_1 : \alpha \to \alpha_2$ e $\Psi_2 : \alpha \to \alpha_3$. Ψ_1 corrisponde al ciclo (123), mentre Ψ_2 corrisponde a (132).

Esercizio 4. Mostrare che se $c > 0$ il gruppo di Galois su $\mathbb{Q}$ del polinomio $f(x) = x^3 + cx + 1$ è isomorfo ad S_3 ed esplicitare tale isomorfismo.

$f(x)$ è irriducibile su $\mathbb{Q}$,in quanto non ha radici razionali. In questo caso il discriminante di f è dato da $D(f) = -(4c^4 + 27) < 0$. Quindi (Fatto 1) il suo gruppo di Galois è isomorfo a S_3. Considerate le tre radici $\alpha_1, \alpha_2, \alpha_3$ (delle quali una sola è reale), ad una permutazione $\sigma \in S_3$, corrisponde l'automorfismo Ψ_σ di $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ definito da $\Psi_\sigma(\alpha_i) = \alpha_{\sigma(i)}$.

Esercizio 5. Determinare il gruppo di Galois su $\mathbb{Q}$ del polinomio $f(x) = x^4 - 3$ ed un sottogruppo di S_4 ad esso isomorfo.

Il polinomio è irriducibile, in quanto è 3-Eisenstein. Abbiamo $a = 0$ $c = -3$, $t = a^2 - 4c = 12$, e quindi $\sqrt{c} = \sqrt{-3} \notin \mathbb{Q}$ e $\sqrt{ct} = \sqrt{-36} \notin \mathbb{Q}$. Quindi se ordiniamo le radici come

$$\gamma_1 = \sqrt[4]{3}, \gamma_2 = i\sqrt[4]{3}, \gamma_3 = -\sqrt[4]{3}, \gamma_4 = -i\sqrt[4]{3},$$

otteniamo, in virtù del Fatto 2, che il gruppo di Galois di f è isomorfo a $D_4 = \langle (1234), (13) \rangle$.

Esercizio 6. Mostrare che il gruppo di Galois su $\mathbb{Q}$ del polinomio $f(x) = x^4 + x^2 - 1$ è un gruppo diedrale di grado 4. Determinare tutti i sottocampi normali del campo di spezzamento di $f(x)$.

$f(x)$ non ha radici razionali. D'altra parte si vede facilmente che

$$f(x) = \left(x^2 + \frac{1}{2} - \frac{\sqrt{5}}{2}\right)\left(x^2 + \frac{1}{2} + \frac{\sqrt{5}}{2}\right)$$

e pertanto f non ha neanche fattori razionali di secondo grado e deve essere quindi irriducibile. Come nel caso precedente si verifica che siamo nel caso c) del Fatto 2. Le radici sono

$$\gamma_1 = \alpha = \sqrt{-\frac{1}{2} + \frac{\sqrt{5}}{2}},\ \gamma_2 = \beta = i\sqrt{\frac{1}{2} + \frac{\sqrt{5}}{2}},\ \gamma_3 = -\alpha, \gamma_4 = -\beta.$$

Il campo di spezzamento di f è dato da $\mathbb{L} = \mathbb{Q}(\alpha, \beta)$. Osserviamo che

$$\sqrt{5} = 2\alpha^2 + 1 \quad \alpha\beta = i$$

e quindi $\mathbb{Q}(i, \sqrt{5}) \subseteq \mathbb{L}$. Si verifica facilmente (Fatto 3) che $\mathbb{Q}(i, \sqrt{5})$ è normale cosi come i suoi sottocampi $\mathbb{Q}(i)$, $\mathbb{Q}(i\sqrt{5})$ e $\mathbb{Q}(\sqrt{5})$ ($Q(\alpha)$ è sempre normale se ha grado 2 su $\mathbb{Q}$.) Poiché il gruppo di Galois di f ha esattamente 4 sottogruppi normali non banali, i 4 sottocampi di $\mathbb{L}$ individuati esauriscono la lista dei sottocampi non banali di $\mathbb{L}$.

Esercizio 7. Dimostrare che i seguenti polinomi di $\mathbb{Q}[x]$, al variare di p fra i numeri primi, hanno gruppo di Galois isomorfo ad S_5: $f(x) = x^5 + px^2 - px - p$.

Utilizzeremo il fatto che se un polinomio irriducibile di quinto grado ha esattamente due radici complesse non reali allora il suo gruppo di Galois è isomorfo a S_5. Il polinomio è irriducibile in quanto è p-Eisenstein. Abbiamo $\lim_{x\to-\infty} f(x) = -\infty$,, $f(-1) > 0$, $f(0) < 0$ e $f(p) > 0$ (oppure $\lim_{x\to+\infty} f(x) = +\infty$). Quindi, per il teorema di esistenza degli zeri, la funzione ha almeno tre zeri reali. D'altra parte $f''(x) = 20x^3 + 2p$ ha un solo zero e quindi per la (nota) generalizzazione del Teorema di Rolle la funzione non può avere più di tre zeri reali (non c'è bisogno di utilizzare la regola di Cartesio!).

Esercizio 8. Costruire la chiusura normale in $\mathbb{C}$ dei seguenti campi:

(i) $\mathbb{Q}(\sqrt{3} + i)$;

(ii) $\mathbb{L} = \mathbb{Q}(\sqrt{2} - i,\ \sqrt[3]{2})$;

Poiché $(\sqrt{3} + i) = 2e^{i\pi/3}$ abbiamo che $(\sqrt{3} + i)^3 = 8i$. Pertanto $\mathbb{Q}(\sqrt{3} + i) = \mathbb{Q}(\sqrt{3}, i)$ che è normale.

Come prima si verifica che $\mathbb{Q}(\sqrt{2} - i) = \mathbb{Q}(\sqrt{2}, i)$. In questo caso però i due coniugati di $\sqrt[3]{2}$, dati da $\sqrt[3]{2}\zeta_3$ e $\sqrt[3]{2}\zeta_3^2$, non appartengono a $\mathbb{L}$. Ne deduciamo che la chiusura normale di $\mathbb{L}$ in $\mathbb{C}$ è data da $\mathbb{Q}(\sqrt{2}, i, \sqrt[3]{2}, \zeta_3)$.

Esercizio 9. Trovare un'estensione ciclotomica che contenga i seguenti radicali: $\sqrt{d}$, $d = 3, 6, 11, 12, 15$. Determinare quale estensioni quadratiche di $\mathbb{Q}$ contiene $\mathbb{Q}(\zeta_{31})$.

In virtù del Fatto 5 abbiamo

$$\sqrt{3} \in \mathbb{Q}(\zeta_{12}), \sqrt{6} \in \mathbb{Q}(\zeta_{24})(*), \sqrt{11} \in \mathbb{Q}(\zeta_{44}), \sqrt{12} = 2\sqrt{3} \in \mathbb{Q}(\zeta_{12}), \sqrt{15} \in \mathbb{Q}(\zeta_{60}).$$

Tutte le radici sono contenute in $\mathbb{Q}(\zeta_{1320})$. (*) è giustificata dal fatto che $\mathbb{Q}(\zeta_8)$ contiene anche i.

Poiché il gruppo di Galois di $\mathbb{Q}(\zeta_{31})$ è ciclico abbiamo che $\mathbb{Q}(\zeta_{31})$ contiene un unico sottocampo quadratico. Essendo $31 \equiv 3 \bmod 4$, tale sottocampo è dato da $\mathbb{Q}(i\sqrt{31})$.