SOLUZIONI DELL' ESAME DI FINE SEMESTRE

---

1. Dopo aver dato la definizione di sottogruppo transitivo di S_n, si elenchino i sottogruppi transitivi di S_4 descrivendone gli elementi come permutazioni.

Un sottogruppo H di S_n si dice transitivo se per ogni $i, j \in \{1, 2, \ldots, n\}$ esiste $\sigma \in H$ tale che $\sigma(i) = j$. I sottogruppi transitivi di S_4 sono isomorfi a uno dei seguenti:

$$S_4,\ A_4, V = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$

$$C_4 = \{(1), (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 2\ 3)\} \quad e \quad D_4 = C_4 \cup \{(1\ 2)(3\ 4), (1\ 3), (2\ 4), (1\ 4)(2\ 3)\}.$$

---

2. Descrivere gli elementi del gruppo di Galois del polinomio $x^5 - 2$ mostrando che ha 20 elementi.

Si osservi che il campo di spezzamento del polinomio è $\mathbf{Q}(2^{1/5}, \zeta_5 2^{1/5}, \zeta_5^2 2^{1/5}, \zeta_5^3 2^{1/5}, \zeta_5^4 2^{1/5}) = \mathbf{Q}(2^{1/5}, \zeta_5)$. Quindi la dimensione $[\mathbf{Q}(2^{1/5}, \zeta_5) : \mathbf{Q}] = [\mathbf{Q}(2^{1/5}, \zeta_5) : \mathbf{Q}(2^{1/5})][\mathbf{Q}(2^{1/5}) : \mathbf{Q}] = 20$ visto che 4 non divide $[\mathbf{Q}(2^{1/5}) : \mathbf{Q}]$. Ciò mostra che il gruppo di Galois del polinomio ha esattamente 20 elementi che sono esattamente:

$$\mathbf{Q}(2^{1/5}, \zeta_5) \longrightarrow \mathbf{Q}(2^{1/5}, \zeta_5),\ 2^{1/5} \mapsto \zeta_5^j 2^{1/5},\ \ \zeta_5 \mapsto \zeta_5^i, \qquad con\ \ i = 1, 2, 3, 4\ \ e\ \ j = 1, 2, 3, 4, 5.$$

---

3. Dimostrare che il gruppo di Galois de polinomio (che si può assumere irriducibile) $x^5 + x^4 + x^3 + 2x^2 + 3x + 4$ non ha 20 elementi né 10 mostrando che contiene un 3 ciclo.

Il polinomio ottenuto riducendo il polinomio modulo 2 è $x^5 + x^4 + x^3 + x = x(x^4 + x^3 + x^2 + 1) = x(x + 1)(x^3 + x^2 + 1)$. Osserviamo che il terzo fattore è irriducibile perchè non ha radici e ha grado tre. Possiamo applicare il Teorema di Dedekind che implica che il gruppo di Galois contiene un elemento che ammette una rappresentazione come permutazione di S_5 del tipo $(c_1)(c_1)(c_3)$ cioè un 3 ciclo. Infine sia un gruppo con 20 elementi che un gruppo con 10 elementi non possono contenere un elemento di ordine 3.

---

4. Calcolare quanti sono i polinomi irriducibili (monici) di grado 8 su $\mathbf{F}_2$.

Partiamo dalla formula $\sum_{d|n} dN_d(q) = q^n$ (dove $N_d(q)$ indica il numero dei polinomi irriducibili di grado d in $\mathbf{F}_q[x]$). Nel caso $q = 2$ e $n = 8$ otteniamo:

$$8N_8(2) + 4N_4(2) + 2N_2(2) + N_1(2) = 2^8 = 256.$$

D'altronde $N_1(2) = 2$ (x e $x + 1$ sono i polinomi irriducibili di grado 1) $N_2(2) = 1$ ($x^2 + x + 1$ è l'unico polinomio irriducibile di grado 2) e $N_4(2) = 3$ ($x^4 + x + 1$, $x^4 + x^3 + 1$ e $x^4 + x^3 + x^2 + x + 1$ sono i polinomi irriducibili di grado 4). Quindi

$$N_8(2) = \frac{1}{8}\left(256 - 4N_4(2) - 2N_2(2) - N_1(2)\right) = \frac{256 - 12 - 2 - 2}{8} = 30.$$

---

5. Calcolare il gruppo di Galois del polinomio $x^4 + 8x + 12$ (assumendo che è irriducibile).

La risolvente cubica del polinomio è $x^3 - 48x - 64 = 64((\frac{x}{4})^3 - 3(\frac{x}{4}) - 1)$. Pertanto la risolvente è irriducibile e il suo gruppo di Galois è lo stesso di $y^3 - 3y - 1$. Quest'ultimo polinomio ha discriminante pari a $43^3 - 27 = 3^4$ (un quadrato perfetto) e quindi il suo gruppo di Galois è A_3. Infine il polinomio di grado 4 di partenza ha gruppo di Galois di typo A_4.

---

6. Calcolare una formula per il discriminante di $x^4 + ax + b$.

La derivata del polinomio $f = x^4 + ax + b$ è $f' = 4x^3 + a$. Utilizzando la formula $D = disc(x^4 + ax + b) = \prod_{i=1}^4 f'(\alpha_i)$ e il fatto che $\gamma = (4\alpha^3 + a) = -4(a + b/\alpha) + a$, otteniamo che $\alpha = -4b/(\gamma + 3a)$. Dunque $f(-4b/(\gamma + 3a)) = 0$ e quindi $256b^3 - 4a(\gamma + 3a)^3 + (\gamma + 3a)^4 = 0$. Da cui il polinomio minimo $f_\gamma = 256b^3 - 4a(x + 3a)^3 + (x + 3a)^4 = 0$ e infine $D = f_\gamma(0) = \gamma_1 \cdot \gamma_2 \cdot \gamma_3 \cdot \gamma_4 = -27a^4 + 256b^3$

---

7. Spiegare come si fa a costruire un polinomio il cui gruppo di Galois ha 13 elementi. *Pensare al numero primo 53.*

Consideriamo il campo ciclotomico $\mathbf{Q}(\zeta_{53})$. Sappiamo che il gruppo di Galois $Gal(\mathbf{Q}(\zeta_{53})/\mathbf{Q}) = U(\mathbf{Z}/53\mathbf{Z}) \cong \mathbf{Z}/52\mathbf{Z}$. Dal fatto che $52 = 13 \cdot 4$ segue che il gruppo di Galois contiene un sottogruppo con indice 13. Si tratta del sottogruppo $\{\mathrm{id}, \sigma_{-1}, \sigma_{23}, \sigma_{-23}\} = \langle\sigma_{23}\rangle$. Poniamo $\eta = \zeta_{53} + \zeta_{53}^{-1} + \zeta_{53}^{23} + \zeta_{53}^{-23}$. Vogliamo prima mostrare che $\mathbf{Q}(\eta) = \mathbf{Q}(\zeta_{53})^{\langle\sigma_{23}\rangle}$ e poi calcolare il polinomio minimo di η su $\mathbf{Q}$ il cui gruppo di Galois sarà ciclico con 13 elementi (perchè grazie al Teorema di corrispondenza di Galois è isomorfo a $H = Gal(\mathbf{Q}(\zeta_{53})/\mathbf{Q})/\langle\sigma_{23}\rangle$. che è ciclico con 13 elementi).

Per quanto riguarda la prima affermazione, si osservi che siccome $\sigma_{23}(\eta) = \eta$, si ha $\mathbf{Q}(\eta) \subseteq \mathbf{Q}(\zeta_{53})^{\langle\sigma_{23}\rangle}$. D'altronde se l'inclusione sopra fosse propria, si avrebbe un sottogruppo che contiene propriamente $\langle\sigma_{23}\rangle$ i cui elementi fissano η. Ciò è impossibile perchè l'indice di $\langle\sigma_{23}\rangle$ è 13 e quindi non ci sono sottogruppi propri del gruppo di Galois che contengono propriamente $\langle\sigma_{23}\rangle$.

Per quanto riguarda la seconda affermazione, osservare che $\eta = 2(\cos\frac{2\pi}{53} + \cos\frac{46\pi}{53}) \approx 0.15567095754099698115120114 52$ e che il polinomio minimo

$$f_\eta(x) = \prod_{\sigma\in H}(x - \sigma(\eta)) = \prod_{j=1}^{13}(x - \sigma_{2^j}(\eta)) = \prod_{j=1}^{13}\left(x - 2\left(\cos\frac{2\cdot 2^j\pi}{53} + \cos\frac{46\cdot 2^j\pi}{53}\right)\right) =$$

$$= x^{13} + x^{12} - 24x^{11} - 19x^{10} + 190x^9 + 116x^8 - 601x^7 - 246x^6 + 738x^5 + 215x^4 - 291x^3 - 68x^2 + 10x + 1$$

---

8. Si enunci nella completa generalità il Teorema di corrispondenza di Galois.

Teorema. *Sia E/F un estensione di Galois (cioè E è il campo di spezzamento di un polinomio separabile in $F[x]$) e sia $G = Gal(E/F)$. Allora c'è una corrispondenza biunivoca tra ti sottogruppi di G e i sottocampi di E che contengono F. Se $H \leq G$ e $F \subseteq M \subseteq E$, allora la corrispondenza è data da:*

$$H \mapsto E^H, \quad M \mapsto \mathrm{Gal}(E/M).$$

Inoltre

i G *corrisponde a* F *e* $\{1\}$ *corrisponde a* E*;*

ii $H_1 \leq H_2 \Leftrightarrow E^{H_1} \supseteq E^{H_2}$.

iii Per ogni $\sigma \in G$,

- $E^{\sigma H\sigma^{-1}} = \sigma E^H$;
- $Gal(E/\sigma M) = \sigma Gal(E/M)\sigma^{-1}$.

iv $H \triangleleft G \Leftrightarrow E^H/F$ *è un estensione normale. In tal caso inoltre* $Gal(E^H/F) \cong G/H$.

---

9. Definire il discriminante di un polinomio $\mathbf{F}[x]$ e dimostrare che è un elemento di $\mathbf{F}$.

La definizione in questione è nelle note di Milne a pagina 42. Mentre la proprietà da dimostrare è il primo punto del Corollario 4.2.

---

10. Quali sono le radici di $x^{16} + x^{12} + 1$ in $\mathbf{F}_2[\alpha]$, con $\alpha^4 = \alpha + 1$? *Provare con* $\alpha^3 + 1$.

Si ha la seguente fattorizzazione unica in $\mathbf{F}_2[x]$: $x^{16} + x^{12} + 1 = (x^4 + x^3 + 1)^4$. Infine le radici del polinomio $x^4 + x^3 + 1$ in $\mathbf{F}_2[\alpha]$ sono: $\alpha^3 + \alpha + 1$, $\alpha^3 + 1$, $\alpha^3 + \alpha^2 + 1$ e $\alpha^3 + \alpha^2 + \alpha$. Quindi

$$x^{16} + x^{12} + 1 = (x + \alpha^3 + \alpha + 1)^4(x + \alpha^3 + 1)^4(x + \alpha^3 + \alpha^2 + 1)^4(x + \alpha^3 + \alpha^2 + \alpha)^4.$$

---

11. Si calcoli il numero di elementi nel campo di spezzamento del polinomio $(x^4 + x + 1)(x^4 + x^3 + 1)(x^2 + x + 1)(x^3 + x + 1)$ su $\mathbf{F}_2$.

Il numero di elementi del campo di spezzamento è 2^{12}. Infatti se F è un campo di spezzamento, allora $[F : \mathbf{F_2}]$ è divisibile per 4 in quanto contiene un sottocampo isomorfo a $\mathbf{F}_2[\tau], \tau^4 = \tau + 1$. È anche divisibile per tre infatti contiene un sottocampo isomorfo a $\mathbf{F}_2[\rho], \rho^3 = \rho + 1$. Quindi $12 \mid [F : \mathbf{F}_2]$.

Infine ogni campo con 2^{12} elementi contiene tutte le radici del polinomio e quindi contiene un campo di spezzamento.

---

12. Dopo aver enunciato il teorema di caratterizzazione per i numeri reali costruibili, si dimostri che $\sqrt{1 + \sqrt{3 - 2^{1/8}}}$ esibendone una costruzione nel senso della teoria dei campi. Dimostrare anche che $2^{1/5}$ non è costruibile.

Teorema. *$x \in \mathbf{R}$ è costruibile se e solo se esiste un torre di campi $\mathbf{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$ tali che $[K_i : K_{i-1}] = 2$ per ogni $i = 1, 2, \ldots, n$ e $K_n = \mathbf{Q}(x)$.*

$\sqrt{1 + \sqrt{3 - 2^{1/8}}}$ è costruibile in quanto una sua è data da

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt{\sqrt{2}}) \subset \mathbf{Q}(\sqrt{\sqrt{\sqrt{2}}}) \subset \mathbf{Q}(\sqrt{3 - 2^{1/8}}) \subset \mathbf{Q}(\sqrt{1 + \sqrt{3 - 2^{1/8}}}).$$

Infine $2^{1/5}$ non è costruibile perchè $[\mathbf{Q}(2^{1/5}) : \mathbf{Q}] = 5$ non è una potenza di 2 e pertanto è impossibile soddisfare il teorema di caratterizzazione.
