Scritto di Algebra 1 del 10 luglio 2020.

(1) **grp-finiti-v1**
Chiamiamo $\mathrm{SL}_2(\mathbb{Z}_3)$ il gruppo delle matrici 2×2 a coefficienti in $\mathbb{Z}_3$ e con determinante 1.
Calcolare il numero di elementi di ordine 3 in $\mathrm{SL}_2(\mathbb{Z}_3)$.
- 8 ✓

(2) **grp-finiti-v2**
Chiamiamo $\mathrm{SL}_2(\mathbb{Z}_5)$ il gruppo delle matrici 2×2 a coefficienti in $\mathbb{Z}_5$ e con determinante 1.
Calcolare il numero di elementi di ordine 5 in $\mathrm{SL}_2(\mathbb{Z}_5)$.
- 24 ✓

(3) **omomor-v1**
Determinare il numero di sottogruppi di S_6 isomorfi al gruppo diedrale D_5.
- 36 ✓

(4) **omomor-v1**
Determinare il numero di sottogruppi di S_8 isomorfi al gruppo diedrale D_7.
- 960 ✓

(5) **campi-finiti-v1**
Calcolare il numero di elementi di ordine massino nel gruppo moltiplicativo $(\mathbb{Z}_3[x]/(x^3 + 2x + 1))^*$
- 12 ✓

(6) **campi-finiti-v2**
Calcolare il numero di elementi di ordine massino nel gruppo moltiplicativo $(\mathbb{Z}_5[x]/(x^3+x+1))^*$
- 60 ✓

(7) **est-campi-v1**
Quante sono le sotto-estensioni del campo di spezzamento di x^3-2 su $\mathbb{Q}$ che <u>non</u> sono estensioni normali di $\mathbb{Q}$?
- 3 ✓

(8) **est-campi-v2**
Quante sono le sotto-estensioni del campo di spezzamento di x^4-2 su $\mathbb{Q}$ che <u>non</u> sono estensioni normali di $\mathbb{Q}$?
- 4 ✓

(9) **galois-v1**
Sia $\mathbb{F}$ il campo di spezzamento di $x^4 + 1$ su $\mathbb{Q}$. Determinare quanti sono gli automorfismi di $\mathbb{F}$ che hanno come campo fisso $\mathbb{Q}$.
- 0 ✓

(10) **galois-v2**
Sia $\mathbb{F}$ il campo di spezzamento di $x^6 + x^3 + 1$ su $\mathbb{Q}$. Determinare quanti sono gli automorfismi di $\mathbb{F}$ che hanno come campo fisso $\mathbb{Q}$.
- 2 ✓

(11) **es-gruppi**
Sia p un numero primo. Sia G un sottogruppo di S_p. Sia $N(G)$ il numero di distinti omomorfismi

$$f : G \to \mathbb{Z}_p$$

Determinare il valore di $N(G)$ al variare di G fra tutti i sottogruppi di S_p.

(12) **es-campi**
(a) Calcolare il polinomio minimo di $\alpha = \sqrt[8]{2}$ su $\mathbb{Q}$.
(b) Sia $\mathbb{F}$ la più piccola estensione di Galois di $\mathbb{Q}$ che contiene $\alpha = \sqrt[8]{2}$, calcolare $[\mathbb{F} : \mathbb{Q}]$.
(c) Data $\mathbb{F}$ come sopra, dire se il gruppo $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ è isomorfo al gruppo diedrale D_n, per qualche $n \in \mathbb{N}$.

Soluzione:
(a) α soddisfa il polinomio $x^8 - 2$, che è irriducibile su $\mathbb{Z}$ grazie al Criterio di Eisenstein, e conseguentemente su $\mathbb{Q}$ per il Lemma di Gauss.
(b) L'estensione $\mathbb{F}$ è il campo di spezzamento di x^8-2. Le radici (complesse) di tale polinomio sono $\zeta_8^i\alpha$, e quindi $\mathbb{F}$ contiene sicuramente sia α che le potenze di ζ_8. In particolare, $i \in \mathbb{F}$ e quindi $\mathbb{F}$ contiene $\mathbb{Q}(\alpha, i)$. Poiché $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$, dal momento che $i \notin \mathbb{Q}(\alpha) \in$

$\mathbb{R}$ soddisfa un polinomio di grado 2, abbiamo $[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = 16$, e $\mathbb{F} \supset \mathbb{Q}(\alpha, i)$ ha almeno grado 16 su $\mathbb{Q}$. Mostriamo che $\mathbb{F} = \mathbb{Q}(\alpha, i)$. Ora, sappiamo che $\mathbb{F} = \mathbb{Q}(\alpha, \zeta_8)$, e sicuramente $\mathbb{Q}(\alpha, i) \subset \mathbb{Q}(\alpha, \zeta_8)$ poiché $i = \zeta_8^2$. L'altra inclusione segue immediatamente da $\zeta_8 = (1+i)/\sqrt{2} = (1+i)/\alpha^4 \in \mathbb{Q}(\alpha, i)$.

(c) Due osservazioni preliminare: poiché l'estensione $[\mathbb{F} : \mathbb{Q}]$ ha grado 16, il gruppo $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ ha 16 elementi e dunque può eventualmente essere isomorfo al gruppo diedrale D_8 e a nessun altro gruppo diedrale; inoltre se $\varphi \in \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$, allora $\varphi(\sqrt[8]{2})$ è una delle 8 radici complesse di $x^8 - 2$, e quindi $\varphi(\alpha) = \zeta_8^j \alpha$ per qualche $j = 0, \dots, 7$. Fissata l'immagine di α, φ è allora determinato dall'immagine di i che può solo essere $\pm i$, poiché $\mathbb{Q}(i)$ è un'estensione normale di $\mathbb{Q}$. L'automorfismo φ è anche determinato dalla sua azione sulle 8 radici ottave di 2, che potrebbe essere quella del diedrale D_8. In effetti, se $\varphi(\alpha) = \zeta_8^j \alpha$, allora

$$\varphi(\sqrt{2}) = \varphi(\alpha^4) = \zeta_8^{4j} \alpha^4 = (-1)^j \sqrt{2}.$$

Consideriamo i due automorfismi

$$c : \begin{cases} \alpha \mapsto \alpha \\ i \mapsto -i \end{cases} \qquad \rho : \begin{cases} \alpha \mapsto \zeta_8 \alpha \\ i \mapsto i \end{cases}$$

Se numeriamo le radici di $x^8 - 2$ in senso antiorario a partire da α con i numeri da 0 a 7, la coniugazione complessa c induce la permutazione $(1\ 7)(2\ 6)(3\ 5)$. L'azione di ρ è lievemente più complicata da calcolare. Iniziamo notando che $\rho(\sqrt{2}) = -\sqrt{2}$. Ricordando che $\zeta_8 = (1+i)/\sqrt{2}$, si ottiene $\rho(\zeta_8) = -(1+i)/\sqrt{2} = -\zeta_8 = \zeta_8^5$. Si puó quindi calcolare che $\rho(\zeta_8 \alpha) = \zeta_8^6 \alpha$, $\rho(\zeta_8^2 \alpha) = \zeta_8^3 \alpha$,... e in generale ρ induce la permutazione $(0\ 1\ 6\ 7\ 4\ 5\ 2\ 3)$. Nessuna potenza di tale permutazione è prodotto di tre trasposizioni disgiunte. Possiamo concludere che ρ genera un sottogruppo (normale) di ordine 8, c uno di ordine 2, e $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ è prodotto semidiretto di tali due sottogruppi. Per determinare completamente la struttura, calcoliamo $c\rho c^{-1}$; la sua azione come permutazione è $(0\ 7\ 2\ 1\ 4\ 3\ 6\ 5)$ che è la stessa di ρ^3. Pertanto c coniuga ρ in ρ^3, e ρ^j in ρ^{3j}. Questo prodotto semidiretto NON É isomorfo a il gruppo diedrale D_8: infatti gli elementi della forma $\rho^j c$ hanno ordine 2 se j è pari, e 4 se j è dispari e dunque il gruppo contiene 5 elementi di ordine 2, non 9 come il gruppo D_8.