Esercizio 1.

1. Calcolare il numero dei 7-cicli in S_7.
2. Calcolare il numero dei 7-Sylow in S_7.
3. Dimostrare che S_7 ha un sottogruppo H di ordine 42.
4. Dire se H può essere abeliano.

Risoluzione:

1) I 7-cicli sono $\frac{7!}{7} = 6!$

2) Un 7-Sylow è ciclico di ordine 7, e contiene 6 elementi di ordine 7, che sono necessariamente 7-cicli. Pertanto il numero n_7 di 7-Sylow è $n_7 = \frac{6!}{6} = 5!$

3) Se S è un 7-Sylow, $n_7 = [S_7 : N_G(S)] = \frac{|S_7|}{|N_G(S)|}$

Pertanto $|N_G(S)| = \frac{7!}{n_7} = \frac{7!}{5!} = 7 \cdot 6 = 42$

4) Poiché $42 = 2 \cdot 3 \cdot 7$, il teorema di Cauchy garantisce l'esistenza di elementi di ordine 2, 3, 7. Se H fosse abeliano, il loro prodotto avrebbe ordine 42 ma in S_7 non esiste un elemento ~~[illegible]~~ tale ordine

Esercizio 2. Sia ϕ la funzione di Eulero

1. Dimostrare che se $MCD(n, \phi(n)) = 1$, allora n è privo di quadrati.
2. Dimostrare che se C_n è l'unico gruppo di ordine n allora n è privo di quadrati.
3. Dimostrare che se G è un gruppo di ordine $p_1 \cdots p_s$ ove $p_1, \ldots, p_s$ sono primi distinti, allora G è risolubile, assumendo che G ha un Sylow normale.

Risoluzione:

1. Se $n = p^m k$, $(p, k) = 1$, allora

$$\phi(n) = p^{m-1}(p-1)\phi(k),$$

per cui se $m > 1$, $(\phi(n), n) \neq 1$

2. Per il teorema fondamentale dei gruppi abeliani finiti, se n essere è privo di quadrati, esistono quei gruppi di ordine n: precisamente, se $n = p_1^{k_1} \cdots p_s^{k_s}$, esistono $\pi(k_1) \cdots \pi(k_s)$ tali gruppi, ove $\pi(r)$ è il numero di partizioni di r.

3. Per induzione su s. Se $s = 1$ G è ciclico di ordine primo, quindi abeliano, quindi risolubile.

Se H è un p_i-Sylow normale, G/H ha ordine $p_1 \cdots p_{i-1} p_{i+1} \cdots p_s$ e per induzione è risolubile.

H è abeliano, quindi è risolubile e si conclude ricordando che estensioni di gruppi risolubili con gruppi risolubili sono risolubili.

Esercizio 3. Siano $E/F, K/F$ estensioni finite di Galois. Dimostrare che EK/F ed $E \cap K/F$ sono estensioni finite di Galois. Identificare $Gal(EK/F)$ come sottogruppo di $Gal(E/F) \times Gal(K/F)$.

Risoluzione:

1. Sia $p(x) \in F[x]$ è irriducibile con una radice α in $E \cap K$. Poiché $\alpha \in E$ e E/F è galois, tutte le radici di $p(x)$ appartengono a K. Ripetendo l'argomento per F ottengo che $E \cap F$ è normale. Essendo ovviamente separabile è di Galois.

2. Sia E il campo di spezzamento di $f_1(x)$, K il campo di spezzamento di $f_2(x)$. Allora EK è il campo di spezzamento di $f_1(x) f_2(x)$. Poiché $f_1(x), f_2(x)$ sono separabili, tale è $f_1(x) f_2(x)$ (infatti i fattori irriducibili di $f_1 f_2$ sono l'unione di quelli di f_1, f_2)

Sia $\Phi : Gal(EK/F) \longrightarrow Gal(E/F) \times Gal(K/F)$,

$\Phi(\sigma) = (\sigma|_E, \sigma|_K)$; è chiaramente un omomorfismo.

$\ker \Phi = \{\sigma \in Gal(EK/F) \mid \sigma|_E = \sigma|_F = id\} = \{id\}$

Sia $H = \{(\sigma_1, \sigma_2) \in Gal(E/F) \times Gal(K/F) \mid \sigma_1|_{E \cap F} = \sigma_2|_{E \cap F}\}$.

Allora $\operatorname{Im} \Phi \subset H$, perché $(\sigma|_E)|_{E \cap F} = \sigma|_{E \cap F} = (\sigma|_F)|_{E \cap F}$

Inoltre

$$|H| = |Gal(E/F)| \cdot |Gal(K/E \cap F)| = |Gal(E/F)| \frac{|Gal(K/F)|}{|Gal(E \cap K/F)|}$$

Ma $[EK:F] = \dfrac{[E:F][K:F]}{[E \cap K : F]}$

Dunque $|H| = |\operatorname{Im} \Phi|$ e $H = \operatorname{Im} \Phi$

Esercizio 4. Sia $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

1. Mostrare che $a = \sqrt{2} + \sqrt[3]{2}$ è un elemento primitivo per K; determinare il grado di K su $\mathbb{Q}$, e il polinomio minimo $m_a(x)$ di a (può essere utile ricordare che il polinomio minimo di un'elemento α di un'estensione galoisiana è il prodotto dei fattori lineari $x - \beta$ al variare di β tra i coniugati di α);
2. il gruppo di Galois di $K/\mathbb{Q}$;
3. l'ordine del gruppo di Galois del campo di spezzamento di $m_a(x)$.

Risoluzione:

1. Chiaramente $\mathbb{Q}(a) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$

Ma $(a-\sqrt{2})^3 = 2$, dunque $a^3 - 3a^2\sqrt{2} + 6a - 2\sqrt{2} = 2$

$a^3 + 6a - 2 = \sqrt{2}(3a^2+2)$, dunque $\sqrt{2} = \dfrac{a^3+6a-2}{3a^2+2} \in \mathbb{Q}(a)$

Dunque $\sqrt[3]{2} = a - \sqrt{2} \in \mathbb{Q}(a)$ e quindi $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$

La chiusura normale N di K è $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \omega)$ ove ω è una radice primitiva cubica dell'unità. Un N

$$m_a(x) = (x - (\sqrt{2}+\sqrt[3]{2}))(x - (-\sqrt{2}+\sqrt[3]{2}))(x - (\sqrt{2}+\omega\sqrt[3]{2}))(x - (-\sqrt{2}+\omega\sqrt[3]{2}))\cdot$$
$$\cdot (x - (\sqrt{2}+\omega^2\sqrt[3]{2}))(x - (-\sqrt{2}+\omega^2\sqrt[3]{2})) =$$
$$= x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4$$

(Tale polinomio è certamente irriducibile perché $[\mathbb{Q}(a):\mathbb{Q}] = 6$).

Dall'analisi precedente segue che

$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2$

$|\mathrm{Gal}(N/\mathbb{Q})| = 12$