Exercise sheet 10

1. Let $d \geq 2$ be an integer, and $H \leq S_d$ be a subgroup generated by a set of transpositions, such that H acts transitively on $\{1, \ldots, d\}$. Prove that $H = S_d$. [*Hint:* It is enough to show that H contains, for some fixed i, all permutations $(i\ k)$ with $k \neq i$. Start with a permutation $(i\ j) \in H$, and for k arbitrary construct a "path" of transpositions from j to k. Then...]

2. Let K be a field, and let L_1/K, L_2/K be two finite extensions lying in a fixed algebraic closure $\bar{K}$ of K.

1. Let $L_1L_2 \subseteq \bar{K}$ be the smallest extension of K containing L_1 and L_2. Show that L_1L_2 is a finite extension of K.
2. Assume that L_1 and L_2 are normal extensions of K. Show that L_1L_2 is also a normal extension of K.
3. Assume that L_1 and L_2 are separable extensions of K. Show that L_1L_2 is also a separable extension of K.
4. Now assume that L_1 and L_2 are Galois extensions of K with Galois groups $G_i := \mathrm{Gal}(L_i/K)$. Show that restriction of automorphisms induces an injective group homomorphism
$$\varphi : \mathrm{Gal}(L_1L_2/K) \longrightarrow G_1 \times G_2.$$
5. Assume that $L_1 \cap L_2 = K$. Show that φ is surjective.
6. Construct a field extension $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. [Gauss sums] Let p be an odd prime and define the Legendre symbol as follows for $x \in \mathbb{F}_p^\times$:

$$\left(\frac{x}{p}\right) = \begin{cases} 1 \text{ if } x \text{ is a square in } \mathbb{F}_p^\times \\ -1 \text{ if } x \text{ is a not square in } \mathbb{F}_p^\times \end{cases}$$

Recall that the association $x \mapsto \left(\frac{a}{p}\right)$ defines a group homomorphism $\mathbb{F}_p^\times \longrightarrow \{\pm 1\}$. (See last semester's - Algebra I, HS 2014 - Exercise sheet 13, Exercise 2).

Let

$$\tau := \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \exp\left(\frac{2\pi i a}{p}\right).$$

Please turn over!

Prove directly by Galois theory that $\tau^2 \in \mathbb{Q}^\times$, but $\tau \notin \mathbb{Q}^\times$.

[*Hint:* Compute the action of the Galois group of $\mathbb{Q}(\xi_p)/\mathbb{Q}$, where $\xi_p = \exp\left(\frac{2\pi i}{p}\right)$. Recall that $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1$.]