Solutions of 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...]

Solution: Suppose that H contains all the permutations of the kind $(i\ k)$ for fixed i. Then for each k', k'' we have $H \ni (i\ k')(i\ k'')(i\ k') = (k'\ k'')$, so that H contains all transpositions and hence $H = S_d$.

By hypothesis there is a transposition $\tau = (i\ j) \in H$ (since H is non-trivial as it is non-transitive). Suppose that k differs from both i and j. Then by transitivity of H there exists transpositions $\tau_0, \ldots, \tau_l$ such that the composite $\tau_0 \cdots \tau_l$ sends j to k. Without loss of generality we may assume that τ_l does not fix j (else, we can remove and use induction on l). Moreover, without loss of generality we may assume that two $\tau_s \neq \tau_{s+1}$ for each s (else, we can remove them both, and again use induction on l). Furthermore, we can also assume that τ_s switches the image of j via $\tau_{s+1} \cdots \tau_l$ (else, we can take s maximal such that τ_s and τ_{s+1} are disjoint and notice that the image of j through $\sigma_{s+1} \cdots \sigma_l$ is fixed by τ_s, which can then be removed), and prove with an easy induction that this allows to write $\tau_l = (i_s\ i_{s+1})$ where $i_0 := k$, $i_{l+1} := j$ and $i_1, \ldots, i_l$ are some other elements. Then $k = ((k\ i_1)(i_1\ i_2) \cdots (i_l\ j))(j)$ where all the transposition lie in H. We can also assume, without loss of generality, that the i_s are all different for $s = 0, \ldots, l+1$ (else, if $i_s = i_{s'}$, then one can remove the transpositions $\tau_s, \ldots, \tau_{s'-1}$ and use induction).

Now we have $k = (k\ i_1\ i_2\ \cdots\ i_l\ j)(j)$ for distinct i_s. There are now two cases:

- Suppose that $i \neq i_s$ for each s. Let $\gamma = (k\ i_1\ i_2\ \cdots\ i_l\ j)$. Then
$$H \ni \gamma^{-1}(i\ j)\gamma^{-1} = (i\ k)$$
- Suppose that $i = i_s$ for some s. We have $\sigma := (k\ i_1\ i_2\ \cdots\ i_{s-1}\ i) \in H$, so that
$$H \ni \tau(\sigma\tau\sigma^{-1})\tau^{-1} = \tau(j\ k)\tau^{-1} = (i\ k)$$

In both cases, we have proved that $(i\ k) \in H$, so that our initial considerations allow us to conclude.

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.

Please turn over!

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 $\mathrm{Gal}(L/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Solution:

1. Since $L_1L_2 \subseteq \bar{K}$, the extension L_1L_2/K is algebraic, and we are only left to prove that it is finitely generated. By hypothesis both the extensions L_i/K are finitely generated. Adjoining to K some chosen generators of L_1/K together with some chosen generators of L_2/K we get a finitely generated extension of K which contains both L_1 and L_2, and has then to coincide with L_1L_2 by definition. Hence L_1L_2 is finitely generated over K.
2. Let $\sigma : L_1L_2 \longrightarrow \bar{K}$ be a K-embedding, and let us prove that $\sigma(L_1L_2) = L_1L_2$ to conclude normality of L_1L_2/K. This is quite straightforward: $\sigma(L_1L_2)$ contains $\sigma(L_i)$ for both i, which is L_i by hypothesis. Then $\sigma(L_1L_2) \supseteq L_1L_2$ by hypothesis, and equality is immediate by equality of the dimensions of the two sides as K-vector space (and injectivity of σ).
3. Write $L_1 = K(\alpha_1, \ldots, \alpha_t)$. All the α_i's are separable over K. Then $L_1L_2 = L_2(\alpha_1, \ldots, \alpha_t)$, and all the α_i's are separable over L_2 (because their minimal polynomials L_2 are factors of their minimal polynomials over K), so that L_1L_2/L_2 is separable. Since separability is preserved in towers of extensions, L_1L_2/K is a separable extension.
4. Clearly L_1L_2/K is Galois by the two previous points. Define

$$\begin{aligned}\varphi : \mathrm{Gal}(L_1L_2/K) &\longrightarrow G_1 \times G_2\\ \sigma &\mapsto (\sigma|_{L_1}, \sigma|_{L_2}).\end{aligned}$$

   This is clearly a group homomorphism. Suppose $\sigma \in \ker(\varphi)$. Then $\sigma|_{L_i} = \mathrm{id}_{L_i}$ for $i = 1, 2$. Then applying σ to generators of the extensions L_i/K, the procedure used in Point 1 to construct L_1L_2 proves that $\sigma = \mathrm{id}_{L_1L_2}$, so that φ is injective.
5. Let $H_1 = \mathrm{Gal}(L_1L_2/L_2)$ and $H_2 = \mathrm{Gal}(L_1L_2/L_1)$. They are subgroups of ϕ. Moreover, $\phi(H_1) = K_1 \times 1$ and $\phi(H_2) = 1 \times K_2$ for some subgroups K_i of G_i, so that we can identify $H_i \leq G_i$ for $i = 1, 2$. To conclude, we just need to show that $H_1 \times H_2 = \mathrm{Gal}(L_1L_2/K)$, which is quite straightforward by Galois correspondence. Indeed, $L^{H_1 \times H_2} \subseteq L^{H_i} = L_i$, so that $L^{H_1 \times H_2} \subseteq L_1 \cap L_2 = K$.

See next page!

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

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

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 $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1$.]

Solution:

By definition, $\tau \in \mathbb{Q}(\xi_p)$, and we know that $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, where the class $b + p\mathbb{Z}$, with $p \nmid b$, acts via $\xi_p \mapsto \xi_p^b$. Hence, we have

$$\begin{aligned}(b + p\mathbb{Z}) \cdot \tau = (b + p\mathbb{Z}) \cdot \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \exp\left(\frac{2\pi i a}{p}\right) &= \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \exp\left(\frac{2\pi i a b}{p}\right) \\ = \left(\frac{b}{p}\right) \sum_{a \in \mathbb{F}_p^\times} \left(\frac{ab}{p}\right) \exp\left(\frac{2\pi i a b}{p}\right) &= \left(\frac{b}{p}\right) \tau.\end{aligned}$$

Then it's clear that τ^2 is fixed by all automorphisms of $\mathbb{Q}(\xi_p)/\mathbb{Q}$, while τ is not (as $\mathbb{F}_p^\times$ contains non-squares). By Galois theory, this means that $\tau \notin \mathbb{Q}^\times$ and $\tau^2 \notin \mathbb{Q}^\times$.