Solutions of exercise sheet 3

1. Let L/K be a Galois extension, and $G = \mathrm{Gal}(L/K)$. Fix $x \in L$ and let $f(X) = \mathrm{Irr}(x, K)(X)$. Show that we have the following equality of subsets in L:

$$\{\sigma(x) | \sigma \in G\} = \{\alpha \in L : f(\alpha) = 0\}.$$

Solution: Let $S_x := \{\alpha \in L : f(\alpha) = 0\}$ be the set of roots of x's minimal polynomial. Then for $\sigma \in G$ and $\alpha \in S_x$ we get, writing $f(X) = \sum_{i=0}^{l} a_i X^i$ and using that σ is a field endomorphism fixing K,

$$f(\sigma(\alpha)) = \sum_{i=0}^{l} a_i \sigma(\alpha)^i = \sum_{i=0}^{l} \sigma(a_i)\sigma(\alpha^i) = \sigma\left(\sum_{i=0}^{l} a_i \alpha^i\right) = \sigma(f(\alpha)) = \sigma(0) = 0,$$

so that $\sigma(\alpha) \in S_x$ as well. This means that the action of G on L restricts to an action on the set S_x. The orbit of $x \in S_x$ via this action is $O(x) := \{\sigma(x) | \sigma \in G\}$, so that the result will follow immediately if we prove that the action of G on S_x is transitive.

This transitivity is equivalent to check that $\sigma(x)$ attains all the roots of f for σ varying in G. For $\alpha \in S_x$, the association $x \mapsto \alpha$ gives an embedding $K(x) \mapsto \bar{K}$, which as seen in class extends to an embedding $L \mapsto \bar{K}$, which gives an elements $\sigma \in G$ such that $\sigma(x) = \alpha$.

2. Let L be a field, $G \subseteq \mathrm{Aut}(L)$ a finite subgroup of cardinality n, and consider the subfield $K = L^G$ of L. Prove:

1. L/K is a finite extension of degree n [*Hint:* Exercise 1.9 from Exercise sheet 1].
2. L/K is Galois with group G.

Solution: Let $x \in L$. Then $O(x) := \{\sigma(x) | \sigma \in G\}$ is the orbit of x under the action of G on L, and $|O(x)| \leq |G| < \infty$. Notice that the polynomial

$$f_x(Y) = \prod_{y \in O(x)} (Y - y)$$

has x as a root. Moreover, it is stable under the action of G on the ring $L[Y]$ (defined by letting G act trivially on Y and imposing additivity and multiplicativity), since each $\tau \in G$ restricts to a bijection of $O(x)$, so that

$$\tau \cdot f_x(Y) = \prod_{y \in O(x)} (Y - \tau(y)) = \prod_{y \in \tau^{-1}O(x)} (Y - y) = \prod_{y \in O(x)} (Y - y) = f_x(Y).$$

Please turn over!

Looking at the coefficients of f_x, this means that $f_x(Y) \in L^G[Y] = K[X]$, so that x satisfies a polynomial of degree smaller than $|G| = n$ over K. This polynomial splits completely in L and has distinct roots by construction (meaning that it is a separable polynomial), so that L/K is a Galois extension by the arbitrarity of $x \in L$ (Part 2.).

To conclude, notice that since the extension L/K is separable we are in position to apply Exercise 1.9 from Exercise sheet 1 (which consisted of a true statement). Since $\deg(f_x) \leq n$ for all $x \in L$, that statement tells us that L/K is finite and $[L : K] \leq n$. Now $G \leq \mathrm{Aut}_K L$ by definition of K, so that

$$[L : K] \leq n = |G| \leq |\mathrm{Aut}_K L| \leq [L : K],$$

as seen in class. In conclusion, $[L : K] = n$ (Part 1.).

3. Let L/K be a finite extension. Prove that L/K is Galois if and only if $|\mathrm{Aut}_K(L)| = [L : K]$. [You can apply the primitive element theorem]

Solution: Suppose that L/K is a finite Galois extension. Then we can apply the primitive element theorem and write $L = K(x)$ for some $x \in L$. By normality and separability, the minimal polynomial of x has $[L : K]$ roots, and then exercise 1 implies that $\sigma(x)$ attains $[L : K]$ distinct values for $\sigma(x) \in \mathrm{Aut}_K(L)$, and since here σ is uniquely determined by $\sigma(x)$, we obtain $|\mathrm{Aut}_K(L)| = [L : K]$.

Conversely, suppose that $|\mathrm{Aut}_K(L)| = [L : K]$. Then $G := \mathrm{Aut}_K(L) \subseteq \mathrm{Aut}(L)$ is a subgroup of cardinality $[L : K]$, so that L/L^G is a Galois extension of degree $[L : K]$. Since $K \subseteq L^G$, the multiplicativity of the degree forces $K = L^G$ and we can conclude that L/K is Galois.

4. Let K be an infinite field, and V a K-vector space over K. Prove that if $V_1, \ldots, V_m$ are vector subspaces in V such that $V_i \neq V$ for all i, then $\bigcup_{i=1}^m \neq V$. [*Hint:* Induction on n].

Solution: See Lemma 3.3.4 in Chambert-Loir, *A field guide to algebra*.

5. In this exercise, we will show how to prove the primitive element theorem using Galois theory. This is useful because it is possible to prove the Galois correspondence without the primitive element theorem, see Section 4.3 in Reid's notes.

Let L/K be a finite separable field extension.

1. Prove that there exist only finitely many intermediate field extensions $K \subseteq E \subseteq L$. [You can use the fact that L embeds in a Galois closure L^g, that is, a smallest finite extension of L such that $K \subseteq L^g$ is Galois]
2. Deduce that if K is an infinite field, then $L = K(x)$ for some $x \in L$. [*Hint:* Previous exercise]

See next page!

3. Suppose that K is finite. Prove that $L = K(x)$ for some $x \in L$.

Solution:

1. Let L^g be a Galois closure of L with respect to K as in the hint. Then any intermediate extension $K \subseteq E \subseteq L$ is an intermediate extension $K \subseteq E \subseteq L^g$, and those are in 1-1 correspondence with subgroups of $\mathrm{Gal}(L^g/K)$ by the Galois correspondence. Since L^g is a finite extension of K, $\mathrm{Gal}(L^g/K)$ is finite and has finitely many subgroups.
2. By previous point there are only finitely many primitive extensions of K, which we call $L_1, \ldots, L_n$. Then $L = \bigcup_i L_i$ because each element $x \in L$ belongs to the primitive extension $K(x)$. Then by the previous exercise the only possibility is that $L_i = L$ for some i, which means that L is itself primitive.
3. As seen in the first semester, the multiplicative group of a finite field is cyclic. Since L is also a finite field (containing $|K|^{[L:K]}$ elements), there exists $x \in L$ such that $L^\times = \langle x \rangle$. Then $L = K(x)$ as desired.