Assignment 23

Galois extensions. Constructions with ruler and compass.

1. Let E/k be a finite field extension, write $G := \mathrm{Gal}(E/k)$ and consider an element $\alpha \in E$. Consider the polynomial

$$q := \prod_{\sigma \in G/\mathrm{Stab}_G(\alpha)} (X - \sigma(\alpha)) \in E[X].$$

Prove that $q \in E^G[X]$.

2. Let E/k be a finite Galois extension with Galois group $G = \mathrm{Gal}(E/k)$ of degree $n = [E : k]$. Define the *trace* $T : E \longrightarrow E$ by

$$T(x) = \sum_{\sigma \in G} \sigma(x).$$

One can prove that this map coincides with the trace defined in Assignment 12, Exercise 7.

(a) Prove that $\mathrm{im}(T) \subseteq k$ and that T is k-linear.

(b) Show that T is not identically zero and deduce that $\dim(\ker(T)) = n - 1$. [*Hint:* Independence of characters].

(c) Now suppose that $\mathrm{Gal}(E/k)$ is cyclic and generated by an automorphism σ. Consider the linear map $\tau = \sigma - \mathrm{id}_E$. Prove that

$$\ker(T) = \mathrm{im}(\tau) = \{\sigma(u) - u : u \in E\}.$$

3. Define the set $S \subset \mathbb{R}^2$ of *constructible points* as the smallest subset S of the Euclidean plane containing O, $(1, 0)$ and such that:

- if $A, B, C, D \in S$ and the line through A and B is not parallel to the one through C and D, then the intersection point is in S;
- if $A, B, C, D, E \in S$, then all points of intersection between the line through A and B and the circle centered at C with radius equal to $d(D, E)$ are in S.
- if $A, B, C, D, E, F \in S$, then all points of intersection between the circle centered at C with radius equal to $d(D, E)$ and the circle centered at F with radius equal to $d(A, B)$ are in S.

(a) Suppose that the points A, B, C, D, E, F have coordinates in a common field $K \subset \mathbb{R}$. Explain why if a point X can be constructed by performing one of the two steps above, then its coordinates belong to a field extension K'/K such that $[K' : K] \leqslant 2$.

We say that a real number $r \in \mathbb{R}$ is *constructible* if the point $(r, 0) \in \mathbb{R}^2$ is constructible.

(b) Prove that the point $(a, b) \in \mathbb{R}^2$ is constructible if and only if a and b are constructible.

(c) Prove that a real number $r \in \mathbb{R}$ is constructible if and only if there are field extensions

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$$

such that $[K_i : K_{i-1}] \leqslant 2$ and $r \in K_n$.

(d) Prove that the real numbers π, $\sqrt[3]{2}$ and $\cos(20°)$ are not constructible. Explain what this means in terms of classical ruler-and-compass construction problems. [*Hint:* What is the degree of $\mathbb{Q}(z)/\mathbb{Q}$ if z is a constructible number? You may need the trigonometric identity $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$].