Workshop 9

Algebra 2

2026 Semester 1

The goal of this workshop is to use Galois theory to settle the question of ruler/compass constructions. We say that $x \in \mathbf{C}$ is *constructible* if it lies in a tower of quadratic extensions. That is, if there exist fields

$$\mathbf{Q} \subset K_1 \subset K_2 \subset \cdots \subset K_n,$$

where each $K_i \subset K_{i+1}$ is a degree 2 extension and $\alpha \in K_n$. Let us prove the following.

Theorem. A number $x \in \mathbf{C}$ is constructible if and only if its Galois group (= the Galois group of the splitting field of its minimal polynomial) has order 2^m for some m.

Let us prove the if part. Suppose z is constructible. It is enough to construct a Galois extension (= splitting field) that contains z and whose degree over $\mathbf{Q}$ is a power of 2.

1. Suppose $z = \sqrt{2+\sqrt{3}}$. Construct a Galois extension (= splitting field) that contains z and whose degree over $\mathbf{Q}$ is a power of 2.
2. Do the same for $\sqrt{2+\sqrt{3+\sqrt{5}}}$.
3. Try to formalise the pattern you see. This is a bit tricky. One clean way is to prove the following by induction: there exists field K_i' containing K_i such that (a) $K_i'/\mathbf{Q}$ is Galois and (b) the degree of $K_i'/\mathbf{Q}$ is a power of 2.

Let us now try the converse. Suppose z lies in a Galois extension of degree 2^m over $\mathbf{Q}$. Let G be the Galois group.

1. Here is a fact from group theory: a group of order 2^m has a subgroup of order 2^{m-1}. Use it to produce a chain of subgroups of size $1, 2, \cdots, 2^m$.
2. Apply the main theorem of Galois theory.