We concluded the proof that:
if $\mathbf{K} \subset \mathbf{E} \subset \mathbf{L}$ are field extensions, then

$$\# Aut_{\mathbf{K}}(\mathbf{L}) \geqslant [\mathbf{L} : \mathbf{E}].$$

Cyclotomic polynomials.
(1) The inductive definition:

$$\prod_{d|n} \Phi_d = x^n - 1;$$

$\Phi_1 = x - 1;$
$\Phi_1\Phi_2 = x^2 - 1 \quad \Rightarrow \quad \Phi_2 = x + 1;$
$\Phi_1\Phi_2\Phi_3 = x^3 - 1 \quad \Rightarrow \quad \Phi_3 = x^2 + x + 1;$

(2) Alternative definition

$$\Phi_n = \prod_{\substack{\xi \ prim. \\ n^{th} \ root \ of \ 1}} (z - \xi)$$

• In definition (1), cyclotomic polynomials are rational functions; in definition (2) they are polynomials with complex coefficients. The two definitions coincide and

$$\Phi_n \in \mathbf{Q}(x) \cap \mathbf{C}[x] = \mathbf{Q}[x]$$

is a polynomial of degree $\varphi(n)$.

• (Kronecker $\sim$ 1880) $\Phi_n(x)$ is irreducible in $\mathbf{Q}[x]$.

The construction problem.
• A complex number α is constructible with ruler and compass, starting from 0 and 1, if and only if $\mathbf{Q}(\alpha)$ is a finite extension of $\mathbf{Q}$, which is a tower of quadratic extensions

$$\mathbf{Q} = \mathbf{F}_0 \subset \mathbf{F}_1 \subset \ldots\ldots \subset \mathbf{F}_m = \mathbf{Q}(\alpha), \qquad [\mathbf{F}_{i+1} : \mathbf{F}_i] = 2.$$

In particular, $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^m$ (note however that $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^m$ is not sufficient for the existence of a tower of quadratic extensions as above).

• A regular polygon of n vertices is constructible with ruler and compass if and only if ξ_n, a primitive n^{th} root of 1, is constructible. In particular, $\varphi(n) = 2^m$ and $n = 2^k \prod p_h$, where p_h denotes a Fermat prime.