1 True / False

Label each statement as true or false and give a short reason. (A single sentence or counterexample is sufficient.)

(a) If K/F is a Galois extension, and $F \subseteq L \subseteq K$ is an intermediate field, then $\mathrm{Gal}(K/L)$ is a subgroup of $\mathrm{Gal}(K/F)$.

True. If an automorphism of K fixes L, then it also fixes F.

(b) Every Galois extension $K/\mathbb{Q}$ of degree 6 has exactly one intermediate field of degree 3 over $\mathbb{Q}$.

False. S_3 is a group of order 6 with 3 subgroups of order 2, so any extension with Galois group S_3, such as the splitting field of x^3-2, has 3 intermediate fields of degree 3 over $\mathbb{Q}$. (In this example, they are $\mathbb{Q}(\alpha_i)$, where α_i are the 3 cube roots of 2.)

(c) The finite field $\mathbb{F}_{27}$ is a degree 3 extension of $\mathbb{F}_9$.

False. The degree 3 extension of $\mathbb{F}_9$ should have $9^3 = 729$ elements. $\mathbb{F}_9$ is not a subfield of $\mathbb{F}_{27}$.

(d) Let $f \in \mathbb{Q}[x]$ be a degree n irreducible polynomial. The splitting field of f over $\mathbb{Q}$ has degree n over $\mathbb{Q}$.

False. For example, $x^3 - 2$ again.

(e) Let K/F be a field extension with finite degree. Then every element of K is algebraic over F.

True. Since K is a finite dimensional F-vector space, for any $\alpha \in K$, there is an F-linear dependence among the elements

$$1, \alpha, \alpha^2, \alpha^3, \ldots$$

which gives a polynomial in $F[x]$ with α as a root.

2 Examples

Provide an example for each of the following. (No further explanation needed.)

(a) A Galois extension with Galois group isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

$\mathbb{Q}(\zeta_7)/\mathbb{Q}$, where $\zeta_7 = e^{2\pi i/7}$.

(b) A Galois extension with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

(c) A Galois extension with Galois group isomorpic to $\mathbb{Z}/4\mathbb{Z}$.

$\mathbb{Q}(\zeta_5)/\mathbb{Q}$, where $\zeta_5 = e^{2\pi i/5}$.

(d) A primitive element of the extension $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$.

$\sqrt{3} + \sqrt{5}$.

(e) A primitive element of the splitting field of $x^3 - 2$ over $\mathbb{Q}$.

$\sqrt[3]{2} + \omega$, where $\omega = e^{2\pi i/3}$.

3 Short answer

For Problems 3.1 and 3.2, provide a short explanation with your answer.

3.1 Galois group of cubic

Let K be the splitting field of $x^3 - 3x - 1$ over $\mathbb{Q}$. What is the degree $[K : \mathbb{Q}]$?

Solution. The discriminant of this cubic is

$$-4 \cdot (-3)^3 - 27(-1)^2 = 108 - 27 = 81,$$

which is a square in $\mathbb{Q}$, so $\mathrm{Gal}(K/\mathbb{Q}) \simeq A_3$, and $\boxed{[K : \mathbb{Q}] = 3}$.

3.2 Number of intermediate fields

According to Problem 4.1 below, the field $K = \mathbb{Q}(\cos(2\pi/41))$ is a Galois extension of $\mathbb{Q}$, with Galois group isomorphic to $\mathbb{Z}/20\mathbb{Z}$. How many subfields does K have?

Solution. Intermediate fields correspond to subgroups of $\mathbb{Z}/20\mathbb{Z}$. There are 6 subgroups:

$$\mathbb{Z}/20\mathbb{Z}, \quad \langle\overline{2}\rangle, \quad \langle\overline{4}\rangle, \quad \langle\overline{5}\rangle, \quad \langle\overline{10}\rangle, \quad \{\overline{0}\}.$$

Thus, there are $\boxed{6}$ subfields of K.

4 Proof-based problems

For Problems 4.1 and 4.2, you should write a complete proof.

4.1 Subfield of $\mathbb{Q}(\zeta_{41})$

Let $K = \mathbb{Q}(\cos(2\pi/41))$. Show that $K/\mathbb{Q}$ is a Galois extension, and that $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of order 20.

Solution. Let $\zeta = e^{2\pi i/41}$. Note that $\zeta + \zeta^{-1} = 2\cos(2\pi/41)$, so $K = \mathbb{Q}(\zeta + \zeta^{-1})$.

Let $K' = \mathbb{Q}(\zeta)$. The Galois group $G = \mathrm{Gal}(K'/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/41\mathbb{Z})^\times \simeq \mathbb{Z}/40\mathbb{Z}$. It has a 2-element subgroup $H = \{\sigma_1, \sigma_{-1}\}$, where σ_1 is the identity automorphism, and σ_{-1} is defined by

$$\sigma_{-1}(\zeta) = \zeta^{-1}.$$

By the Main Theorem, its fixed field is a degree 20 extension of $\mathbb{Q}$.

Note that $\zeta + \zeta^{-1}$ is fixed by H. Furthermore, the G-orbit of $\zeta + \zeta^{-1}$ consists of the 20 elements

$$\zeta^j + \zeta^{-j}, \quad 1 \leq j \leq 20,$$

so $\zeta + \zeta^{-1}$ has degree 20 over $\mathbb{Q}$, and $K = \mathbb{Q}(\zeta + \zeta^{-1})$ is the fixed field of H.

Since G is abelian, every subgroup is normal. By the Main Theorem, this means that $K/\mathbb{Q}$ is Galois, and $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to G/H.

Since G is isomorphic to $\mathbb{Z}/40\mathbb{Z}$, the subgroup H corresponds to the subgroup $\{\overline{0}, \overline{20}\}$ of $\mathbb{Z}/40\mathbb{Z}$, and the quotient group G/H is isomorphic to $\mathbb{Z}/20\mathbb{Z}$.

4.2 Please remember to review the bonus problems

Prove that the polynomial $x^4 - 2x^2 + 9$ is reducible in $\mathbb{F}_p[x]$ for every prime p.

Solution. The roots of this polynomial are $\pm\sqrt{1 \pm \sqrt{-8}}$. Note that $\sqrt{1 + \sqrt{-8}} = \sqrt{2} + i$. (There is some ambiguity with signs in this statement. However, we don't actually need to worry about the square roots of complex numbers when we factor the polynomial over $\mathbb{F}_p$.)

The proof is the same as the solution to the second bonus problem, with 2 and 3 replaced by 2 and -1.