

# Questions

Hui Sun

May 2, 2025

**Problem 0.1.** To see whether a polynomial is irreducible over  $\mathbb{Q}$ , is it sufficient to test whether  $f \pmod p$  is irreducible over any prime  $p$ ?  
For example,  $x^5 - 5x^3 + 1$ .

*Proof.* Yes. The converse is not true, consider the minimal polynomial for  $\sqrt{2} + \sqrt{3}$ . □

**Problem 0.2.** In the above example, how do we know that the Galois group contains an element of order 5? (It is clear why it contains a transposition because there exists complex roots).

*Proof.* This is because the Galois group  $G$  acts transitively on the set of roots, by the Orbit stabilizer theorem, we know

$$|G| = |\text{Orbit}(\alpha)| \cdot |\text{Stab}(\alpha)| = 5 \cdot |\text{Stab}(\alpha)|$$

i.e., 5 divides  $|G|$ . By Cauchy's theorem, there exists an element of order 5 in  $G$ , i.e., a 5-cycle. □

**Problem 0.3.** The Galois action on the set of roots implies for any root  $r$  of the irreducible polynomial (where  $G$  is the splitting field of), we must have

$$\text{Orbit}(r) = \{ \text{set of all roots} \}$$

*Proof.* Yes, by definition of a transitive action. □

**Problem 0.4.** Is it true that if  $I, J$  are ideals of a ring  $R$ , then

$$\frac{R}{I} \otimes_R \frac{R}{J} = \frac{R}{(I+J)}$$

in the case where  $R = \mathbb{Q}[x]$ , and  $I, J$  are irreducible polynomials, we have

$$\frac{R}{(f)} \otimes_R \frac{R}{(g)} = \frac{R}{(f)+(g)} = \frac{R}{\gcd(f,g)}$$

**Problem 0.5.** Fall 2014 Q2,  $\text{Hom}_R(M, N)$ .

**Problem 0.6.**  $\mathbb{Z}/55\mathbb{Z}$ .

*Proof.* We have  $n_{11} = 1$ , and we can write  $G$  as a semidirect product

$$G = \frac{\mathbb{Z}}{11\mathbb{Z}} \rtimes_{\theta} \frac{\mathbb{Z}}{5\mathbb{Z}}$$

where  $\theta : \frac{\mathbb{Z}}{5\mathbb{Z}} \rightarrow \left( \frac{\mathbb{Z}}{11\mathbb{Z}} \right)^{\times}$ . We know  $\theta(1)$  needs to be sent to an element of order 5, which includes 3, 4.

$$G = \langle g, h : g^{11} = h^5 = e, hgh^{-1} = g^3 \rangle$$

and

$$G = \langle g, h : g^{11} = h^5 = e, hgh^{-1} = g^4 \rangle$$

□

**Problem 0.7.** Is cyclotomic extension cyclic.

*Proof.* No, consider  $\mathbb{Q}(\zeta_8)$ , then the Galois group is  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . □

**Problem 0.8.** If an intermediate field extension of a Galois extension has order  $a$ ,  $k \subset E \subset K$  has  $[E : k] = a$ , then the subgroup that fixes  $E$  has index  $a$ .

**Problem 0.9.** Find all intermediate fields when the Galois group is  $\mathbb{Q}(\zeta_9)$ .

**Problem 0.10.** Find all the intermediate fields when the Galois group is  $D_8$ .

**Problem 0.11.** S2013-Q6(b)(c), S2016-Q3