

PS4

Sasha Redden

February 10, 2026

1. Let F be the splitting field of $x^p - 1$ over $\mathbb{Q}$.
 - (a) Using results from the previous problem sets, show that $[F : \mathbb{Q}] = p - 1$.
 - (b) Prove that $\text{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/(p-1)$. [Hint: show that an element of the Galois group is determined by the image of ζ_p .]
 - (c) Consider the case $p = 7$. Find all subgroups of $\text{Gal}(F/\mathbb{Q})$ and the corresponding intermediate subfields.

- (a) From PS1, $x^p - 1 = \Phi_p(x)(x - 1)$ and we know $\zeta_p^k \notin \mathbb{Q}, k \in \{1, \dots, p-1\}$ are the roots of $\Phi_p(x)$, so then $F = \mathbb{Q}(\zeta_p)$, where $\Phi_p(x)$ is the minimal polynomial for ζ_p which is of degree $p - 1$, so $[F : \mathbb{Q}] = p - 1$.
- (b) Let $\theta_m \in \text{Gal}(F/\mathbb{Q})$, then for $\zeta_p^k, k \in \{1, \dots, p-1\}$, $\theta_m(\zeta_p^k) = \theta_m(\zeta_p)^k$, so every $\theta_m \in \text{Gal}(F/\mathbb{Q})$ is determined by $\theta_m(\zeta_p)$. We can construct a bijection $\varphi : \text{Gal}(F/\mathbb{Q}) \rightarrow (\mathbb{Z}/p)^\times$ defined by $\varphi(\theta_m) \mapsto m$ (where $\theta_m(\zeta_p) = \zeta_p^m$). This is a bijection because there exists an inverse $\phi = \varphi^{-1} : (\mathbb{Z}/p)^\times \rightarrow \text{Gal}(F/\mathbb{Q})$ defined by $\phi(m) = \theta_m$ for all $m \in \{1, \dots, p-1\}$. And φ is a homomorphism: for some $\theta_m, \theta_n : n, m \in \{1, \dots, p-1\}$,

$$\theta_m \circ \theta_n(\zeta_p) = \theta_m(\theta_n(\zeta_p)) = \theta_m(\zeta_p^n) = \zeta_p^{nm} = \theta_{mn}(\zeta_p)$$

Then

$$\varphi(\theta_m \circ \theta_n) = \varphi(\theta_{mn}) = mn = \varphi(\theta_m)\varphi(\theta_n).$$

And since $(\mathbb{Z}/p)^\times \cong \mathbb{Z}/(p-1)$ we have that $\text{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/(p-1)$.

- (c) $p = 7$, then F is the splitting field of $x^7 - 1$, $F = \mathbb{Q}(\zeta_7)$, and $\text{Gal}(F/\mathbb{Q}) \cong (\mathbb{Z}/7)^\times$. The (non-trivial) subgroups of $(\mathbb{Z}/7)^\times$ are $H = \{1, 6\} \cong \mathbb{Z}/2$ and $K = \{1, 2, 4\} \cong \mathbb{Z}/3$ (because these are the only subgroups of order dividing 6). These subgroups will correspond to subgroups of $\text{Gal}(F/\mathbb{Q})$ via φ : $H \cong \{\varphi^{-1}(1), \varphi^{-1}(6)\} = \{\theta_1, \theta_6\} = H'$ and $K \cong \{\varphi^{-1}(1), \varphi^{-1}(2), \varphi^{-1}(4)\} = \{\theta_1, \theta_2, \theta_4\} = K'$. The corresponding intermediate subfield for H' and K' is $\mathbb{Q}(\zeta_7^6)$ and $\mathbb{Q}(\zeta_7^2)$ respectively.
2. A subgroup $H \leq S_n$ is called **transitive** if its action on $\{1, \dots, n\}$ is transitive.
 - (a) Find all transitive subgroup of S_4 . [Hint: first show that $4 \mid |H|$.]

- (b) Suppose that $f \in K[x]$ is an irreducible separable degree n polynomial. Let F be its splitting field. Prove that $\text{Gal}(F/K)$ is a transitive subgroup of S_n .
- (c) Suppose that $f \in \mathbb{Q}[x]$ is an irreducible degree 4 polynomial with exactly 2 real roots. Which groups are possible for $\text{Gal}(F \setminus \mathbb{Q})$?
- (a) Let $H \leq S_4$ be transitive, then size of the orbit of an element $a \in \{1, 2, 3, 4\}$ is 4, then $|H| = |O_a| |Stab_H(a)| = 4 |Stab_H(a)|$ so $4 \mid |H|$, and $|H| \mid 24 = |S_4|$ so $|H| = 4, 8, 12$ thus we could have $H \cong \mathbb{Z}/2 \times \mathbb{Z}/2 = V_4, \mathbb{Z}/4, D_4, A_4$. For $H \cong V_4 = \{(), (12)(34), (13)(24), (14)(23)\}$ so every $a \in \{1, 2, 3, 4\}$ is moved by every element of H , thus $|Stab_H(a)| = 1 \implies |O_a| = 4$ and H is transitive. For $H \cong \mathbb{Z}/4 = \langle (1234) \rangle = \{(), (1234), (13)(24), (1432)\}$, similarly $|Stab_H(a)| = 1$ so H is transitive. For $H \cong D_4 = \langle (1234), (13) \rangle$ here $Stab_H(1) = \{(24), ()\}$ so $|O_1| = 4$ and H is transitive. For $H \cong A_4 = \langle (123), (12)(34) \rangle$, and $Stab_H(4) = \{(123), (132), ()\}$, so $|O_4| = 4$ so H is transitive. Then $V_4, \mathbb{Z}/4, D_4$, and A_4 are all of the transitive subgroups of S_n .
- (b) Let $A = \{\alpha : f(\alpha) = 0\}$, $|A| = n$, by Orbit-Stabilizer, $|\text{Gal}(F/K)| = |A| |Stab_{\text{Gal}(F/K)}(\alpha)|$. Suppose $\theta(\alpha) = \alpha$ for $\theta \in \text{Gal}(F/K)$, then $H = \{c \in F : \theta(c) = c\} \leq F$ contains α thus $H = F$ and $\theta = id$ so $Stab_{\text{Gal}(F/\mathbb{Q})}(\alpha) = \{id\}$ and so $\text{Gal}(F/K)$ is a transitive subgroup of S_n .
- (c) First assume f is inseparable. Let $\alpha, \beta \in \mathbb{R}$ be the (real) roots of $f(x) = (x - \alpha)^2(x - \beta)^2$, then there are only 2 distinct roots, so $\text{Gal}(F/\mathbb{Q}) \cong S_2$. Now assume f is separable, then $f(x)$ has 2 imaginary roots, γ, τ , (and then $\text{Gal}(F/\mathbb{Q})$ is Galois if F is the splitting field of f). $\theta \in \text{Gal}(F/\mathbb{Q})$ has to send γ to τ and vice versa because if $\theta(i) = c \in \mathbb{R}$, then $\theta(-1) = \theta(i^2) = \theta(i)^2 = c^2 \neq -1$. So let $\theta_1(\alpha) = \beta, \theta_1(\beta) = \alpha$ and $\theta_2(\gamma) = \tau, \theta_2(\tau) = \gamma$, then $\text{Gal}(F/\mathbb{Q}) = \{id, \theta_1, \theta_2, \theta_1 \circ \theta_2\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.
3. Let $F \setminus K$ be a Galois extension of degree 4. Prove that there exists an intermediate field $K \subsetneq L \subsetneq F$.
 F/K is a Galois extension so it is simple, $\exists \delta \in F : F = K(\delta)$, and there is a separable irreducible polynomial $f(x) \in K[x]$ such that F is the splitting field of f . f is separable so it can be factored into two quadratic polynomials $g(x), h(x)$. Let $\alpha, \beta \in F$ be the roots of $g(x)$ and let $\gamma, \tau \in F$ be the roots of $h(x)$, then let L be the splitting field for $g(x)$, $L = K(\alpha, \beta)$ is an intermediate field such that $K \subsetneq L \subsetneq F$.
4. Let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
- (a) Prove that $F \setminus \mathbb{Q}$ is Galois.
- (b) Find $\text{Gal}(F \setminus \mathbb{Q})$.
- (c) Find all subgroups of $\text{Gal}(F \setminus \mathbb{Q})$ and the corresponding intermediate fields.
- (a) Let $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$, the roots of $f(x)$ are $\pm\sqrt{2} \pm \sqrt{3}$, so F is the splitting field of a separable polynomial $f(x) \in \mathbb{Q}[x]$ and thus $F/\mathbb{Q}$ is Galois.
- (b) $|\text{Gal}(F/\mathbb{Q})| = [F : \mathbb{Q}] = 4$ so $\text{Gal}(F/\mathbb{Q})$ is either $\mathbb{Z}/4$ or $\mathbb{Z}/2 \times \mathbb{Z}/2$. If we consider the map $\phi_1 : F \rightarrow F$ such that $\phi_1(\pm\sqrt{2} \pm \sqrt{3}) = \mp\sqrt{2} \pm \sqrt{3}$ and $\phi_2 : F \rightarrow F$ such

that $\phi_2(\pm\sqrt{2} \pm \sqrt{3}) = \pm\sqrt{2} \mp \sqrt{3}$ it is clear that $\text{Gal}(F/\mathbb{Q}) = \{id, \phi_1, \phi_2, \phi_1 \circ \phi_2\} \cong \{(0,0), (1,0), (0,1), (1,1)\} = \mathbb{Z}/2 \times \mathbb{Z}/2$

- (c) The subgroups of $\text{Gal}(F/\mathbb{Q})$ are $H = \{id, \phi_1\}$ and $K = \{id, \phi_2\}$ corresponding to $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{2})$ respectively.

5. Let $F \setminus K$ be an extension, not necessarily finite or Galois. Let $G = \text{Gal}(F \setminus K)$.

- (a) Let $K \subseteq L \subseteq F$ be an intermediate field. Consider $\text{Fix}(\text{Gal}(F \setminus L))$ and L . One is always contained inside the other. Which way does the containment go?
- (b) Let $H \subseteq G$. Consider $\text{Gal}(F \setminus \text{Fix}(H))$ and H . One is always contained inside the other. Which way does the containment go?
- (c) Pick one of the containments that you found above and give an example where the containment is strict. [One is much easier than the other one.]

- (a) $\text{Fix}(\text{Gal}(F/L)) = \{c \in F : \sigma(c) = c \forall \sigma \in \text{Gal}(F/L)\}$ so $L \subseteq \text{Fix}(\text{Gal}(F/L))$ because for all $c \in L, \theta \in \text{Gal}(F/L), \theta(c) = c$.

- (b) Let $A = \text{Fix}(H) = \{c \in F : \sigma(c) = c \forall \sigma \in H\}$. Let $\theta \in H$, then $\theta : F \rightarrow F$ is an automorphism, let $c \in F$ such that for all $\sigma \in H, \sigma(c) = c$, then $\theta(c) = c$ because $\theta \in H$, so $\theta \in \text{Gal}(F/A) \implies H \subseteq \text{Gal}(F/A)$.

- (c) Consider the containment found in (a) and let $L = \mathbb{Q}, F = \mathbb{Q}(\sqrt[4]{2})$ ($K = \mathbb{F}_p$) or something. Then $\text{Gal}(F/L) = \{id, \varphi\}$ where φ sends $\pm\sqrt[4]{2} \mapsto \mp\sqrt[4]{2}$. Then $\text{Fix}(\text{Gal}(F/L)) = \mathbb{Q} \cup \{\sqrt{2}\}$.