

PS5

Sasha Redden

February 23, 2026

1. Let K be a field of characteristic not equal to 2. Let $f(x) \in K[x]$ be a degree n monic separable polynomial. Let F be the splitting field of $f(x)$ and let $G = \text{Gal}(F/K)$. Let $c_1, \dots, c_n \in F$ be the roots of $f(x)$. As usual, we can regard G as a subgroup of S_n .
 - (a) Let $\Delta = \prod_{i < j} (c_i - c_j)$ and $D = \Delta^2$. Prove that $D \in K$.
 - (b) Prove that $\Delta \in K$ if and only if $G \leq A_n$.
 - (c) Suppose that $n = 2$ and $f(x) = x^2 + ax + b$. Prove that $D = a^2 - 4b$. Conclude that $f(x)$ splits over K if and only if D is a square in K .
 - (d) Suppose that $n = 3$ and $f(x) = x^3 + px + q$ (a general cubic can be brought into this form by change of variables.) Prove that $D = -4p^3 - 27q^2$. Assume that f is irreducible. Find G depending on whether or not D is a square in K .
 - (a) $K = \text{Fix}(\text{Gal}(F/K))$ because F/K is Galois. From MATH-456, worksheet 4, we know that for any permutation $\sigma \in S_n$, $\sigma \cdot \Delta = \varepsilon_\sigma \Delta$ where $\varepsilon_\sigma \in \{-1, 1\}$ so $\sigma \cdot \Delta^2 = (\varepsilon_\sigma \Delta)^2 = \Delta^2$ so $D \in \text{Fix}(\text{Gal}(F/K)) = K$
 - (b) $\Delta \in K \iff$ for any permutation $\sigma \in S_n$, $\sigma \cdot \Delta = \Delta$ ($\varepsilon_\sigma = 1$) $\iff G \leq \text{Ker}(\varepsilon) = A_n$ (where ε is the sign homomorphism).
 - (c) $c_1 = \frac{-a + \sqrt{a^2 - 4b}}{2}$, $c_2 = \frac{-a - \sqrt{a^2 - 4b}}{2}$, $\Delta = \prod_{i < j} (c_i - c_j) = (c_1 - c_2) = \frac{-a + \sqrt{a^2 - 4b} + a + \sqrt{a^2 - 4b}}{2} = \sqrt{a^2 - 4b}$, then $D = \Delta^2 = a^2 - 4b$. Assume $f(x)$ splits over K , then $c_2, \dots, c_n \in K$ so then $\Delta \in K$ so $D = \Delta^2$ is a square in K . Assume $D = \Delta^2$ is a square in K , then $\Delta = \sqrt{a^2 - 4b} \in K$, then $c_1 = \frac{-a + \sqrt{a^2 - 4b}}{2}$, $c_2 = \frac{-a - \sqrt{a^2 - 4b}}{2} \in K$ so $f(x)$ splits in K .
 - (d) Using Cardano's formula for the depressed cubic, the discriminant obtained is $D = -4p^3 - 27q^2$. Let $f(x) = x^3 + px + q$ be irreducible and suppose D is a square in K , then $\Delta \in K$, so then $G \leq A_3$ from (b), and since F is the splitting field of a separable polynomial, then $[F : K] = \text{Gal}(F/K) = G$ and $f(x)$ is irreducible so $[F : K] > 1$, so $G = A_3$. Now suppose D is not a square in K , then G is not a subgroup of A_3 , so $G = S_3$ or a transposition subgroup.
2. Let $f(x) \in K[x]$ be a separable irreducible polynomial of degree n . Let F be its splitting field. Assume that $\text{Gal}(F/K) = S_n$. Let $\alpha \in F$ be a root of $f(x)$.
 - (a) Prove that $\text{Gal}(F/K(\alpha)) = S_{n-1}$.

(b) Prove that there are no fields L such that $K \subsetneq L \subsetneq K(\alpha)$.

(a) We know $S_{n-1} \cong \text{Stab}_{S_n}(n)$, or even $\text{Stab}_{S_n}(a)$ for any $a \in \{1, \dots, n\}$. By tower theorem, $n! = [F : K] = [F : K(\alpha)][K(\alpha) : K] = [F : K(\alpha)] \cdot n$ so $[F : K(\alpha)] = (n-1)!$. Since $\text{Gal}(F/K(\alpha)) \leq \text{Gal}(F/K) = S_n$, $\text{Gal}(F/K) = S_{n-1}$.

(b) Since there are no groups between S_n and S_{n-1} , i.e. $\nexists G : S_{n-1} \subsetneq G \subsetneq S_n$, then by Galois correspondence, there is no field L such that $K \subsetneq L \subsetneq K(\alpha)$.

3. The fundamental theorem on algebra states that $\mathbb{C}$ is algebraically closed. The goal of this exercise is to prove this using Galois theory and the intermediate value theorem. From PS3, it suffices to show that every polynomial in $\mathbb{R}[x]$ splits over $\mathbb{C}$. Let $f(x) \in \mathbb{R}[x]$. Let F be the splitting field of $f(x)$ and consider the extension $F(i)/\mathbb{R}$. Let $G = \text{Gal}(F(i)/\mathbb{R})$.

(a) Show that $F(i)/\mathbb{R}$ is a Galois extension.

(b) Suppose that $E/\mathbb{R}$ is an extension of odd order. Prove that $E = \mathbb{R}$. [Hint: you may use that every odd degree polynomial in $\mathbb{R}[x]$ has a root in $\mathbb{R}$ - this follows from the intermediate value theorem.]

(c) Show that $|G| = 2^m$ for some $m \geq 1$. [Hint: if not, then use Sylow's theorem and the Galois correspondence to find an odd order extension of $\mathbb{R}$.]

(d) Let $H = \text{Gal}(F(i)/\mathbb{C})$. Prove that $|H| = 2^{m-1}$.

(e) Suppose that $m \geq 2$. Prove that H has a subgroup of size 2^{m-2} . [Hint: use that any p -group has a non-trivial center - we proved this last semester using the class equation.]

(f) Prove that $F = \mathbb{C}$. [Hint: it suffices to show that $m = 1$, so suppose that $m \geq 2$ and use the previous step to get a contradiction.]

(a) $\mathbb{R}$ is perfect, and since $F(i)/\mathbb{R}$ is algebraic, $F/\mathbb{R}$ is separable (from proposition in class). Then $f(x)(x^2 + 1)$ is separable, so $F(i)$ is the splitting field of a separable polynomial and thus $F(i)/\mathbb{R}$ is Galois.

(b) $E/\mathbb{R}$ is an extension of odd order, then E is the splitting field of some odd degree polynomial $f(x) \in \mathbb{R}[x]$, then $f(x)$ has a root in $\mathbb{R}$, but then there are an even amount of roots in $E \setminus \mathbb{R}$ so $E = \mathbb{R}(c_1, \dots, c_{2n})$ but then $[E : \mathbb{R}]$ is even.

(c) Suppose $|G| \neq 2^m$, then there is an odd prime p in the prime factorization of $|G|$ such that $p^n \parallel |G|$ for some (maximal) n , then by Sylow's first theorem, there exists a subgroup $H \leq G$ such that $|H| = p^n$, then let L be the corresponding subfield such that $\text{Gal}(F(i)/L) = H$, then since $F(i)/\mathbb{R}$ is Galois, $F(i)/L$ is Galois, so $p^n = |H| = |\text{Gal}(F(i)/L)| = [F(i) : L]$, but this is an extension of L not $\mathbb{R}$?

(d) Since $\mathbb{C} = \mathbb{R}(i)$ with minimal polynomial $x^2 + 1$, $[\mathbb{R}(i) : \mathbb{R}] = 2$ and then by tower theorem we get that $[F(i) : \mathbb{R}] = [F(i) : \mathbb{C}][\mathbb{C} : \mathbb{R}] \implies 2^m = |H| \cdot 2$ so $|H| = 2^{m-1}$.

(e) Since H has a non-trivial center, so H has a subgroup of order 2^i , $i \in \{1, \dots, m-2\}$, then there must be a subgroup of order 2 contained in the center, because for the center Z

to be of size 2^i , there must be inverse pairs, leaving one element a and the identity not paired, so $a^{-1} = a$ and $N = \{e, a\}$ is a normal subgroup, and thus H/N is isomorphic to a subgroup $J \leq H$ with order 2^{m-2} by first isomorphism theorem (this is sketchy).

- (f) Suppose $m \geq 2$, then $\text{Gal}(F(i)/\mathbb{C})$ has a subgroup J of size 2^{m-2} corresponding to intermediate field L