V. Fields and Galois Theory

V.4. **Galois Group of a Polynomial.**

2. Suppose K is a subfield of $\mathbb{R}$ and that f is irreducible of degree 3. Let $D(f)$ be the discriminant of f. Then

   a) $D > 0 \iff f$ has three real roots.

   b) $D < 0 \iff f$ has precisely one real root.

   First, note by basic calculus or complex analysis, that the roots of a polynomial with real coefficients always occur in conjugate pairs. This implies that f must have either 1 or 3 real roots. Since the discriminant is defined only in terms of the distinct roots, $D(f) \neq 0$. In sum, (a) and (b) are essentially equivalent statements, and it suffices to prove only (b).

   $\boxed{\Rightarrow}$ f has odd degree, so f has at least one real root u_1, by exercise III.6.16, or by the statement above. Let u_2, u_3 be the other two roots of f. Then

$$\begin{aligned} u_2, u_3 \in \mathbb{R} &\implies (u_1 - u_2), (u_1 - u_3), (u_2 - u_3) \in \mathbb{R} \\ &\implies (u_1 - u_2)(u_1 - u_3)(u_2 - u_3) = \Delta \in \mathbb{R} \\ &\implies D = \Delta^2 > 0. \end{aligned}$$

   So it must be the case that $u_2, u_3 \in \mathbb{C}\backslash\mathbb{R}$

   $\boxed{\Leftarrow}$ Let $f = (x - u_1)(x - u_2)(x - u_3)$ with $u_1 \in \mathbb{R}$ and $u_2, u_3 \in \mathbb{C}\backslash\mathbb{R}$. Note that $u_3 = \overline{u_2}$, so we get

$$\begin{aligned} \Delta &= (u_1 - u_2)(u_1 - u_3)(u_2 - u_3) \\ &= (u_1 - (a + bi))(u_1 - (a - bi))(2bi) \\ &= 2bi(u_1 - a - bi)(u_1 - a + bi) \\ &= 2bi((u_1 - a) - bi)((u_1 - a) + bi) \\ &= 2bi\left((u_1 - a)^2 + b^2\right), \end{aligned}$$

   which is clearly purely imaginary. Hence, $D = \Delta^2 < 0$. ■

3. f is a separable cubic with Galois group S_3 and roots $u_1, u_2, u_3 \in F$. Then the distinct intermediate fields of $F : K$ are $F, K(\Delta), K(u_1), K(u_2), K(u_3), K$, and the corresponding subgroups of the Galois group are $1, A_3, T_1, T_2, T_3, S_3$, where $T_i = \{(1), (jk)\}$ for $j, k \neq i$.

Note that if F is the splitting field of f over K, then $1, A_3, T_1, T_2, T_3, S_3$ are *all* the distinct subgroups of $\mathrm{Aut}_K F$. By the Fundamental Theorem of Galois Theory, there is a bijective correspondence between these subgroups and the intermediate fields of the extension $F : K$. We know by Corollary 4.7 that $\mathrm{Aut}_{K(\Delta)} F = \mathrm{Aut}_K F \cup A_3 = A_3$, so it only remains to check that $\mathrm{Aut}_{K(u_i)} F = T_i$. But we have by the definition of T_1 that $T_1 = \{\tau_1, \tau_2\}$, where

$$\tau_1 = \begin{pmatrix} u_1 & u_2 & u_3 \\ u_1 & u_2 & u_3 \end{pmatrix} \quad \text{and} \quad \tau_2 = \begin{pmatrix} u_1 & u_2 & u_3 \\ u_1 & u_3 & u_2 \end{pmatrix},$$

and similarly for T_2, T_3. So clearly, the elements of T_i are precisely those automorphisms which fix u_i and thus $K(u_i)$. ■

6. Over any base field K, $f(x) = x^3 - 3x + 1$ is either irreducible or splits over K.

First note that $f' = (x^3 - 3x + 1)' = 3x^2 - 3$, so

$$f \text{ has multiple roots} \iff 3x^2 - 3 = 0 \iff \mathrm{char}\, K = 3.$$

case i) $\mathrm{char}\, K \neq 3$.

Suppose f has roots u_1, u_2, u_3. Suppose f neither is irreducible nor splits in K. Then f is reducible $\implies$ $u_1 \in K$. Then $f(x) = (x - u_1)g(x)$, where $g(x) \in K[x]$ is irreducible. Note: $\deg g = 2$, so $[F : K] = 2$.

Let F be the splitting field of g over K (so F is also the splitting field of f). Since we are considering the case that $u_2 \neq u_3$, g is a separable polynomial. Hence, F is the splitting field of a separable polynomial, and thus Galois over K.

Now we consider $\sigma \in \mathrm{Aut}_K F$. $\sigma(u_1) = u_1$ because σ fixes K and $u_1 \in K$. Since σ permutes the roots of f, $\sigma(u_2) = u_2$ or u_3. Consider the case $\sigma(u_2) = u_3$. We compute

$$\begin{aligned} \sigma(\Delta) &= \sigma\left((u_1 - u_2)(u_1 - u_3)(u_2 - u_3)\right) \\ &= \left(\sigma(u_1) - \sigma(u_2)\right)\left(\sigma(u_1) - \sigma(u_3)\right)\left(\sigma(u_2) - \sigma(u_3)\right) \\ &= (u_1 - u_3)(u_1 - u_2)(u_3 - u_2) \\ &= -\Delta \end{aligned}$$

But we can also compute Δ directly; application of 4.8 shows that the discriminant of f is

$$D(f) = -4(-3)^3 - 27(1)^2 = 81$$

This implies that $\Delta = \pm 9$. Since $\pm 9 \in K, \forall K$, $\Delta \in K$. However, $\sigma \in \mathrm{Aut}_K F \implies \sigma(\Delta) = \Delta$. But then $9 = -9 \implies 9 \equiv 0 \implies \mathrm{char}\, K = 3$, $\not\subset \mathrm{char}\, K \neq 3$ was our hypothesis for case (i).

case ii) $\mathrm{char}\, K = 3$.

In this case,

$$f(x) = x^3 + 1 = (x-2)\left(x^2 + 2x + 1\right) = (x-2)^3,$$

so f is clearly reducible.

10. Determine the Galois groups of the following polynomials over the fields indicated.

b) $f(x) = (x^3 - 2)(x^2 - 3)(x^2 - 5)(x^2 - 7)$ over $\mathbb{Q}$.

$\deg f = 9$, so f has 9 roots $u_1, u_2, \ldots, u_9$. If u_i is a root of f, it is a root of exactly one of the irreducible factors of f. For example,

$$u^3 - 2 = 0 \implies u^2 - 3, u^2 - 5, u^2 - 7 \neq 0.$$

$(x^3 - 2)$ has Galois group $A_3 = \mathbb{Z}_3$,[1] and each of the other factors has Galois group $\mathbb{Z}_2$, so

$$\mathrm{Gal}_{\mathbb{Q}}(f) = \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

□

c) $f(x) = x^3 - x - 1$ over $\mathbb{Q}$; over $\mathbb{Q}(i\sqrt{23})$.

f is irreducible over $\mathbb{Q}$ by the rational roots test (III.6.8): the only possible roots would be ± 1, but $f(1) = -1$ and $f(-1) = -1$. Since the field is $\mathbb{Q}$, f is obviously separable, so $\mathrm{Gal}_{\mathbb{Q}}(f)$ is either S_3 or A_3, by Corollary 4.7. Then using Proposition 4.8 (with $b = 0$), we get $g(x) = f(x) = x^3 + px + q$, where $p = -1, q = -1$, so that

$$\begin{aligned} D(f) &= -4p^3 - 27q^2 \\ &= 4 - 27 \\ &= -23. \end{aligned}$$

Since $D(f) = -23$ is not the square of any rational number, $\mathrm{Gal}_{\mathbb{Q}}(f) = S_3$, by Corollary 4.7 again.

Then if we consider $\mathbb{Q}(i\sqrt{23})$, note that f is irreducible over $\mathbb{Q}(i\sqrt{23})$ because it is irreducible over $\mathbb{Q}$ and $i\sqrt{23}$ is not a root of f. Then f is separable since $\mathrm{char}\, \mathbb{Q} = 0$, and we get $\mathrm{Gal}_{\mathbb{Q}(i\sqrt{23})}(f) = A_3$, for the same reasons as above. □

h) $f(x) = (x^3 - 2)(x^2 - 5)$ over $\mathbb{Q}$.

By arguments identical to part (b), $\mathrm{Gal}_{\mathbb{Q}}(f) = \mathbb{Z}_3 \oplus \mathbb{Z}_2$. □

[1] See #11 for justification.

11. Determine all the subgroups of the Galois group and all of the intermediate fields of the splitting field of $f(x) = (x^3 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

Denote the roots of f by $u_1 = \sqrt[3]{2}e^{2\pi i/3}, u_2 = \sqrt[3]{2}e^{4\pi i/3}, u_3 = \sqrt[3]{2}, v_1 = \sqrt{3}, v_2 = -\sqrt{3}$, and note that the splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}(u_1, v_1)$. We know that $\mathrm{Gal}_{\mathbb{Q}}(f)$ will be $\mathbb{Z}_3 \oplus \mathbb{Z}_2$ or $A_3 \oplus \mathbb{Z}_2$, according as $\mathrm{Gal}_{\mathbb{Q}}(x^3 - 2)$ is $S_3 = \mathbb{Z}_3$ or A_3.

We use 4.8 to find the discriminant of $\varphi(x) = x^3 - 2$:

$$\varphi(x - \tfrac{b}{3}) = g(x) = x^3 - 2 = \varphi(x)$$

because $b = 0, c = 0$, so the discriminant of φ is

$$D(\varphi) = -27(-2)^2 = -108$$

by 4.8. Since -108 is not the square of any rational number, $\mathrm{Gal}_{\mathbb{Q}}(\varphi) = A_3$, by 4.7. Thus, $\mathrm{Gal}_{\mathbb{Q}}(f) = A_3 \oplus \mathbb{Z}_2$. Now, $A_3 = \mathbb{Z}_3$ has no nontrival proper subgroups, so the subgroup lattice of $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(u_1, v_1)$ is ...

and the intermediate field lattice is ...

So the only subgroups of $\mathrm{Gal}_{\mathbb{Q}}(f)$ are $\mathbb{Z}_3 \oplus 1$ and $1 \oplus \mathbb{Z}_2$, and the corresponding subfields of $\mathbb{Q}(u_1, v_1)$ are $\mathbb{Q}(u_1)$ and $\mathbb{Q}(v_1)$.