

**Exercise 6.1.** Find Galois groups for the following polynomials  $f$  over  $\mathbb{Q}$ :

1.  $(t^2 - 3)(t^2 + 1)$

*Solution.* We first note that  $t^2 - 3$  is irreducible by Eisenstein's Criterion with  $p = 3$ , and  $t^2 + 1$  is irreducible since  $-1$  is not a square in  $\mathbb{Q}$ . Then,  $f$  has 4 roots:  $\alpha_{1,2} = \pm i$ ,  $\alpha_{3,4} = \pm\sqrt{3}$ . Since  $\deg(\mu_i^{\mathbb{Q}}) = 2$  and  $\deg(\mu_{\sqrt{3}}^{\mathbb{Q}}) = 2$ , we have that  $[\mathbb{Q}(i) : \mathbb{Q}] = 2$  and  $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$  respectively by the tower law. Hence, for  $L = \mathbb{Q}(i, \sqrt{3})$ , we have that  $[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}][\mathbb{Q}(i) : \mathbb{Q}] = 4$ . Suppose we have some non-constant polynomial  $P \in L[t]$  such that  $P(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = 0$ . Let  $\sigma \in S_4$  such that  $(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \alpha_{\sigma(3)}, \alpha_{\sigma(4)}) = 0$ . We know that  $\sigma$  can only permute algebraic conjugates, so  $\pm i \mapsto \mp i$  and  $\pm\sqrt{3} \mapsto \mp\sqrt{3}$ . Thus, the only options for  $\sigma$  are  $e, (12), (34)$ , and  $(12)(34)$ . Hence  $\text{Gal}_{\mathbb{Q}}(f) = \{e, (12), (34), (12)(34)\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$   $\square$

2.  $t^4 - t^2 + 1$

*Solution.* Note that  $t^4 - t^2 + 1 = \Phi_{12}$ . From lecture, we saw that  $\text{Gal}_{\mathbb{Q}}(\Phi_n) \cong \mathbb{Z}_n^*$ , the multiplicative group of units mod  $n$ . Noting that  $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ , we can see that the order of each element is 2. Thus  $\text{Gal}_{\mathbb{Q}}(\Phi_n) \cong \mathbb{Z}_{12}^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ .  $\square$

3.  $t^4 - 2$

*Solution.* By Eisenstein's criterion with  $p = 2$ , this polynomial is irreducible and the four roots are  $\alpha_{1,2} = \pm\sqrt[4]{2}, \alpha_{3,4} = \pm i\sqrt[4]{2}$ . The splitting field extension for this polynomial is  $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ , so let  $L = \mathbb{Q}(\sqrt[4]{2}, i)$ . Since  $[L : \mathbb{Q}(i)] = 4$  and  $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ , we have that  $[L : \mathbb{Q}] = 8$  by the tower law. We know any permutation of roots can only permute algebraic conjugates of the same minimum polynomial over  $\mathbb{Q}$ . Since  $\mu_{\sqrt[4]{2}}^{\mathbb{Q}} = t^4 - 2$ , it has conjugates  $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$ . Also  $\mu_i^{\mathbb{Q}} = t^2 + 1$ , so it has conjugates  $i, -i$ . Define a permutation  $\sigma$  such that  $\sigma(\sqrt[4]{2}) = i\alpha$  and  $\sigma(i) = i$ , and let  $\tau$  be complex conjugation. This gives us that  $\sigma^k(\sqrt[4]{2}) = i^k\sqrt[4]{2}$ ,  $\sigma^4 = e$ , and  $\tau^2 = e$ . Next, we have

$$\tau \circ \sigma \circ \tau(\sqrt[4]{2}) = \tau \circ \sigma(\tau(\sqrt[4]{2})) = \tau \circ \sigma(-\sqrt[4]{2}) = \tau(i\sqrt[4]{2}) = \tau(i)\tau(\sqrt[4]{2}) = (-i)\sqrt[4]{2}$$

and

$$\sigma^{-1}(\sqrt[4]{2}) = \sigma^3(\sqrt[4]{2}) = i^3\sqrt[4]{2} = (-i)\sqrt[4]{2}.$$

Hence,  $\tau\sigma\tau = \sigma^{-1}$ . The identities  $\sigma^4 = e, \tau^2 = e$ , and  $\tau\sigma\tau = \sigma^{-1}$  indicate that the Galois group of this polynomial is isomorphic to  $D_4$ , the dihedral group of 4 points. Hence  $\text{Gal}_{\mathbb{Q}}(f) \cong D_4$ .  $\square$

**Exercise 6.2.1.** Find  $\text{Gal}_{\mathbb{F}_3(t^2)}(\mathbb{F}_3(t))$ .

*Solution.* Let  $K = \mathbb{F}_3(t^2)$  and  $L = \mathbb{F}_3(t)$ . In  $K[t]$ , the element  $t$  is a root of the polynomial  $x^2 - t^2 = (x + t)(x - t)$ . Any field automorphism  $\sigma \in \text{Gal}_K(L)$  can only permute between algebraic conjugates, so the only two automorphisms are  $\sigma(t) = t$  and  $\sigma(t) = -t \equiv 2t \pmod{3}$ . Thus  $\text{Gal}_{\mathbb{F}_3(t^2)}(\mathbb{F}_3(t)) \cong \mathbb{Z}_2$ .  $\square$

**Exercise 6.2.2.** Find  $\text{Gal}_{\mathbb{F}_2(t^2)}(\mathbb{F}_2(t))$ .

*Solution.* Similarly to the exercise above, the element  $t$  is a root of  $x^2 - t^2 = (x + t)(x - t)$ . However, note that  $-t \equiv t \pmod{2}$ . Thus the only automorphism possible is  $\sigma(t) = t$ , whence  $\text{Gal}_{\mathbb{F}_2(t^2)}(\mathbb{F}_2(t)) = \{e\}$ , the trivial group.  $\square$

**Exercise 6.3.1.** Let  $K - M - L$  be a field extension and  $L : K$  is a normal extension. Prove that  $L : M$  is also a normal extension.

*Solution.* By theorem,  $L : K$  is normal  $\iff L$  is a splitting field for some  $f \in K[t]$ . By definition of  $K[t]$ ,  $f(t) = \sum_{i=0}^n c_i t^i$  for  $c_i \in K$ . However,  $K - M \implies K \subseteq M \implies c_i \in M \forall i \implies f \in M[t]$ . Hence all coefficients of  $f$  are contained in  $M$  and  $L$  is a splitting field for some  $f \in M[t] \iff L : M$  is a normal extension.  $\square$

**Exercise 6.3.2.** Give an example of three fields  $K, M, L$  such that  $[L : K] = 4$  and  $[M : K] = [L : M] = 2$  (hence  $K - M$  and  $M - L$  are normal extensions) but  $L : K$  is not a normal extension.

*Solution.* Consider the tower of fields  $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ . Observe that  $\mu_{\sqrt{2}}^{\mathbb{Q}}(x) = x^2 - 2$ , whence  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ . Thus  $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$  is normal. Additionally,  $\mu_{\sqrt[4]{2}}^{\mathbb{Q}(\sqrt{2})}(x) = x^2 - \sqrt{2}$ , whence  $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$ . Thus  $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})$  is normal. By definition,  $L : K$  is normal extension if every  $f \in K[t]$  that has a root in  $L$  splits over  $L$ . However upon inspecting the extension  $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$ , we notice that  $\mu_{\sqrt[4]{2}}^{\mathbb{Q}} = x^4 - 2$  has roots  $\pm\sqrt[4]{2}$  and  $\pm i\sqrt[4]{2}$ . Since  $i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$ , the extension is thus not normal.  $\square$

**Exercise 6.4.** Let  $L : K$  be a splitting field extension for a non-constant polynomial  $f \in K[t]$ . Prove that  $|\text{Gal}_K(L)|$  divides  $(\deg f)!$ .

*Solution.* Since  $L$  is the splitting field extension for  $f$  over  $K$ , we know that  $\text{Gal}_K(L) = \text{Gal}_K(f)$ . By lemma, we have that  $|\text{Gal}_K(f)| \leq S_{\deg f}$  and by Lagrange,  $|\text{Gal}_K(f)| \mid |S_{\deg f}| = (\deg f)!$ .  $\square$

**Exercise 6.5.1.** Let  $f = t^3 + t + 1 \in \mathbb{F}_2[t]$ . Prove that  $\text{Gal}_{\mathbb{F}_2}(f)$  is isomorphic to  $\mathbb{Z}_3$ .

*Solution.* We can see that  $f(1) = 1 + 1 + 1 \equiv 1 \pmod{2} \neq 0$  and  $f(0) = 1 \neq 0$ , whence  $f$  is irreducible over  $\mathbb{F}_2$ . If  $\mathbb{F}_2(\alpha)$  is some extension field of  $\mathbb{F}_2$  where  $\alpha$  is a root of  $f$ , we know  $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 3$ . Moreover, an  $\mathbb{F}_2$ -homomorphism  $\sigma : \mathbb{F}_2(\alpha) \rightarrow \mathbb{F}_2$  is unique to the destination of  $\alpha$ , and we know  $\alpha$  can only be sent to its own algebraic conjugates, of which there are 3. Hence,  $|\text{Gal}_{\mathbb{F}_2}(f)| = 3$ , and the only group of order 3 is  $\mathbb{Z}_3$ .  $\square$

**Exercise 6.5.2.** Let  $f = t^3 + t^2 + 1 \in \mathbb{F}_2[t]$ . Prove that  $\text{Gal}_{\mathbb{F}_2}(f)$  is isomorphic to  $S_3$ .

*Solution.* Typo?  $\square$