

## Math 418, Spring 2025 – Practice Problems 3

14.2.3 Determine the Galois group of  $(x^2 - 2)(x^2 - 3)(x^2 - 5)$ . Determine all the subfields of the splitting field of this polynomial.

**Solution.** This is a degree 8 Galois extension with Galois group  $C_2 \times C_2 \times C_2$ . Since every non-identity element has order 2, we have 7 subgroups of order 2. We also have 7 subgroups of order 4 (the quotients of the 7 previous subgroups).

To find the intermediate fields, compute directly. For instance, the fixed field of  $\sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}, \sqrt{5} \mapsto -\sqrt{5}$  is  $\mathbb{Q}(\sqrt{6}, \sqrt{10})$ , and the fixed field of this element along with  $\sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3}, \sqrt{5} \mapsto -\sqrt{5}$  is  $\mathbb{Q}(\sqrt{6})$ .

14.2.10 Determine the Galois group of the splitting field over  $\mathbb{Q}$  of  $x^8 - 3$ .

**Solution.** The splitting field of  $x^8 - 3$  is  $\mathbb{Q}(\zeta_8, \sqrt[8]{3}) = \mathbb{Q}(i, \sqrt{2}, \sqrt[8]{3})$ , which has degree 32 over  $\mathbb{Q}$ . The automorphisms are the 32 possible choices of  $i \mapsto \pm i, \sqrt{2} \mapsto \pm\sqrt{2}, \sqrt[8]{3} \mapsto \zeta_8^a \sqrt[8]{3}$ . The subgroup sending  $i \mapsto i, \sqrt{2} \mapsto \sqrt{2}$  is isomorphic to  $C_8$  and the subgroup fixing  $\sqrt[8]{3}$  is  $V_4$ . The first subgroup is normal, and so the Galois group is  $C_8 \rtimes V_4$ .

14.2.13 Prove that if the Galois group of the splitting field of a cubic over  $\mathbb{Q}$  is the cyclic group of order 3 then all the roots of the cubic are real.

**Solution.** Real cubics must have at least one real root by the intermediate value theorem. If the other two roots are nonreal, complex conjugation is an element of order 2.

14.3.1 Factor  $x^8 - x$  into irreducibles in  $\mathbb{Z}[x]$  and in  $\mathbb{F}_2[x]$ .

**Solution.** Over  $\mathbb{Z}$ , we have  $x^8 - x = x(x^7 - 1) = x(x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$ , since  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ . Over  $\mathbb{F}_2$ ,  $x^8 - x$  is the product of *all* irreducible polynomials over  $\mathbb{F}_2$  of degree 1 and 3. (This is Proposition 14.18 in Dummit & Foote. Notice that the roots of every such polynomial live in  $\mathbb{F}_{2^j}$  for some  $j \leq 3$ , and those fields are contained in  $\mathbb{F}_8$ , which consists of the roots of  $x^8 - x$ ). The factorization is  $x(x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ , and we can check that the degree is right.

14.4.4 Let  $f(x) \in F[x]$  be an irreducible polynomial of degree  $n$  over the field  $F$ , let  $L$  be the splitting field of  $f(x)$  over  $F$  and let  $\alpha$  be a root of  $f(x)$  in  $L$ . If  $K$  is any Galois extension of  $F$ , show that the polynomial  $f(x)$  splits into a product of  $m$  irreducible polynomials each of degree  $d$  over  $K$ , where  $d = [K(\alpha) : K] = [(L \cap K)(\alpha) : L \cap K]$  and  $m = n/d = [F(\alpha) \cap K : F]$ .

**Solution.** The factorization of  $f$  over  $K$  is the same as over  $L \cap K$  since every linear factor of  $f$  and hence every product of those factors lies in  $L[x]$ . Thus, the two

definitions of  $d$  are the same. Let  $H$  be the subgroup of  $\text{Gal}(L/F)$  corresponding to the intermediate field  $L \cap K$ . By our construction of minimal polynomials, we have for any root  $\alpha$  of  $f$ ,

$$m_{\alpha, L \cap K}(x) = \prod_{\beta \in H\alpha} (x - \beta).$$

Thus, the degrees of the irreducible factors of  $f(x)$  over  $L \cap K$  equal the sizes of the  $H$ -orbits of the roots of  $f$ .

$H$  is normal in  $G$  by the Fundamental Theorem, property 4, since  $K/F$  is Galois. By Dummit & Foote Exercise 4.9a, since  $G$  acts transitively on the roots of  $f$  and  $H$  is normal, the  $H$ -orbits must be the same size; thus all degrees are the same. This degree must be the degree of the minimal polynomial of  $\alpha$  over  $L \cap K$ , which is  $[(L \cap K)(\alpha) : L \cap K]$ .

14.5.2 *Determine the subfields of  $\mathbb{Q}(\zeta_8)$  generated by the periods of  $\zeta_8$  and in particular show that not every subfield has such a period as primitive element.*

**Solution.** Let  $\zeta = \zeta_8$   $G := \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times$ , which is isomorphic to the Klein-4 group  $V_4$ . The elements of  $G$  are  $\sigma_a : \zeta \mapsto \zeta^a$  for  $a = 1, 3, 5, 7$ . The subgroups and corresponding periods are:

$$\begin{array}{ccc} G & \leftrightarrow & \zeta + \zeta^3 + \zeta^5 + \zeta^7 \\ \langle \sigma_3 \rangle & \leftrightarrow & \zeta + \zeta^3 \\ \langle \sigma_5 \rangle & \leftrightarrow & \zeta + \zeta^5 \\ \langle \sigma_7 \rangle & \leftrightarrow & \zeta + \zeta^7 \\ 1 & \leftrightarrow & \zeta \end{array}$$

However, note that  $\zeta + \zeta^5 = 0$ , so the fixed field of  $\langle \sigma_5 \rangle$  is not simply  $\mathbb{Q}(\zeta + \zeta^5)$ . (Instead, it is  $\mathbb{Q}(i)$ ).

14.6.2a *Determine the Galois group of  $x^3 - x^2 - 4$*

**Solution.** This factors as  $(x - 2)(x^2 + x + 2)$ . The first factor is linear, so can be ignored. The second factor is an irreducible quadratic, so its Galois group is  $S_2 = C_2$ .

14.6.3 *Prove for any  $a, b \in \mathbb{F}_{p^n}$  that if  $f(x) = x^3 + ax + b$  is irreducible then  $-4a^3 - 27b^2$  is a square in  $\mathbb{F}_{p^n}$*

**Solution.** Note that  $-4a^3 - 27b^2$  is the discriminant; it is a square if and only if the Galois group  $G$  of  $f$  is a subgroup of  $A_3$ . If  $f(x)$  is irreducible, then  $G$  is a transitive subgroup of  $S_3$ , namely  $S_3$  or  $A_3$ . Galois group of finite field extensions are cyclic, so it must be  $A_3$ .

14.7.3 Let  $F$  be a field of characteristic  $\neq 2$ . State and prove a necessary and sufficient condition on  $\alpha, \beta \in F$  so that  $F(\sqrt{\alpha}) = F(\sqrt{\beta})$ . Use this to determine whether  $\mathbb{Q}(\sqrt{1-\sqrt{2}}) = \mathbb{Q}(i, \sqrt{2})$

**Solution.** If  $F(\sqrt{\alpha}) = F(\sqrt{\beta})$ , then  $\beta \in F(\alpha)$ , so is of the form  $\sqrt{\beta} = c_0 + c_1\sqrt{\alpha}$ . Then  $\beta = c_0^2 + c_1^2\alpha + 2c_0c_1\sqrt{\alpha}$ . Since  $\alpha, \beta \in F$ , so is  $\sqrt{\alpha}$  unless  $c_0$  or  $c_1$  is 0. The former means that  $\beta/\alpha = c_1^2$  is a square in  $F$ , and the latter means that  $\sqrt{\beta} = c_0 \in F$ . Therefore,  $F(\sqrt{\alpha}) = F(\sqrt{\beta})$  iff  $\frac{\alpha}{\beta}$  is a square in  $F$ .

Note that  $\sqrt{2}$  is in  $\mathbb{Q}(\sqrt{1-\sqrt{2}}) = \mathbb{Q}(i, \sqrt{2})$ . The latter field is  $\mathbb{Q}(\sqrt{2})(i)$ , and the former is  $\mathbb{Q}(\sqrt{2})(\sqrt{1-\sqrt{2}})$ , so they are the same field iff  $(1-\sqrt{2})/(-1)$  is a square in  $\mathbb{Q}(\sqrt{2})$ . Take the norm of  $\sqrt{2}-1$ :  $N(\sqrt{2}-1) = 3$ , which is not a square; thus  $\sqrt{2}-1$  is not a square in  $\mathbb{Q}(\sqrt{2})$  and the fields are distinct.

A-G Determine the following:

- (a) The radical of the ideal  $(18) \subseteq \mathbb{Z}$
- (b) The variety  $V(I) \subseteq \mathbb{R}^2$  for the ideal  $I = (x^2 + y^2 - 1) \subseteq \mathbb{R}[x, y]$ .

**Solution.**

- (a) Since  $18 = 2 \cdot 3^2$ ,  $(18) = (2) \cdot (3)^2$ , so  $\sqrt{(18)} = (2) \cdot (3) = (6)$ .
- (b)  $V(I)$  is the set of points  $(x, y)$  in  $\mathbb{R}^2$  such that  $x^2 + y^2 - 1 = 0$  i.e. the unit circle.