SOLUTIONS TO WORKSHEET #5

Problem 1. — *In what follows, let* $L = \mathrm{SF}_K(f)$ *for some* $f \in K[x]$. *Determine* $\mathrm{Gal}(L/K)$ *and find all intermediate subfields of* L/K.

(i) $K = \mathbf{Q}$ *and* $f(x) = x^4 - 7$

(ii) $K = \mathbf{F}_5$ *and* $f(x) = x^4 - 7$

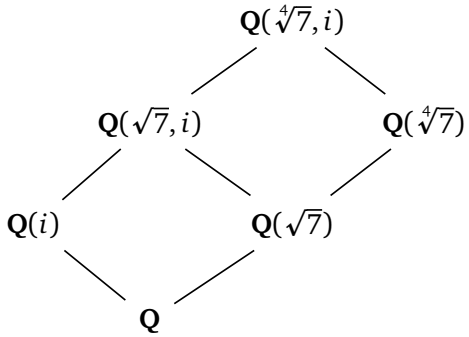
(iii) $K = \mathbf{F}_2$ *and* $f(x) = x^6 + 1$

(iv) $K = \mathbf{Q}$ *and* $f(x) = x^8 - 1$

Solution. For (i), observe that $f(x) = x^4 - 7$ factors over $\mathbf{C}$ as

$$f(x) = x^4 - 7 = (x^2 + \sqrt{7})(x^2 - \sqrt{7}) = (x + i\sqrt[4]{7})(x - i\sqrt[4]{7})(x + \sqrt[4]{7})(x - \sqrt[4]{7})$$

where $i := \sqrt{-1}$, and so $L \subseteq \mathbf{Q}(\sqrt[4]{7}, i)$. But L also properly contains each of $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{7})$, and $\mathbf{Q}(\sqrt[4]{7})$, so considering the diagram of field extensions



and noting that each line indicates an extension of degree 2, it follows that $L = \mathbf{Q}(\sqrt[4]{7}, i)$. To determine its Galois group over $\mathbf{Q}$, note first that $\mathbf{Q}(\sqrt[4]{7}, i)$ might also be viewed as the splitting field of $f(x) = x^4 - 7$ viewed as a polynomial in $\mathbf{Q}(i)$. This is an extension of degree 4, so

$$\#\,\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{7}, i)/\mathbf{Q}(i)) = 4.$$

One $\mathbf{Q}(i)$-automorphism $\sigma : \mathbf{Q}(\sqrt[4]{7}, i) \to \mathbf{Q}(\sqrt[4]{7}, i)$ is that determined by $\sqrt[4]{7} \mapsto i\sqrt[4]{7}$; precisely,

$$\sigma(a + b \cdot 7^{1/4} + c \cdot 7^{1/2} + d \cdot 7^{3/4}) := a + bi \cdot 7^{1/4} - c \cdot 7^{1/2} - di \cdot 7^{3/4}$$

where $a, b, c, d \in \mathbf{Q}(i)$. Since i is a primitive 4-th root of unity, this automorphism has order 4, which implies that this Galois group is generated by σ and is isomorphic to the cyclic group of order 4:

$$\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{7}, i)/\mathbf{Q}(i)) = \langle \sigma \rangle \cong C_4.$$

Viewed as a $\mathbf{Q}$-automorphism, the Galois correspondence shows that σ generates a subgroup in $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{7}, i)/\mathbf{Q})$ isomorphic to $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{7}, i)/\mathbf{Q}(i)) \cong C_4$ and that its quotient is

$$\frac{\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{7}, i)/\mathbf{Q})}{\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{7}, i)/\mathbf{Q}(i))} \cong \mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q}).$$

As is familiar, $\mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q}) \cong C_2$ and is generated by the $\mathbf{Q}$-involution $\tau : \mathbf{Q}(i) \to \mathbf{Q}(i)$ determined by $i \mapsto -i$. Thus the Galois group of interest is a group of order 8 which is an extension of the form

$$1 \to C_4 \to \mathrm{Gal}(\mathbf{Q}(\sqrt[4]{7}, i)/\mathbf{Q}) \to C_2 \to 1.$$

Date: October 9, 2025.

There are two possibilities: either the Galois group is $C_4 \times C_2$ or else it is the dihedral group D_8 of order 8. To see that it is *not* the direct product, extend τ to a $\mathbf{Q}$-automorphism $\tilde{\tau}\colon \mathbf{Q}(\sqrt[4]{7}, i) \to \mathbf{Q}(\sqrt[4]{7}, i)$. Its fixed field is $\mathbf{Q}(\sqrt[4]{7})$. However, as we have essentially seen before on a previous set, the extension $\mathbf{Q} \subset \mathbf{Q}(\sqrt[4]{7})$ is *not* Galois. This means that the subgroup

$$C_2 \cong \langle \tilde{\tau} \rangle \subset \mathrm{Gal}(\mathbf{Q}(\sqrt[4]{7}, i)/\mathbf{Q})$$

generated by $\tilde{\tau}$ is *not* normal, thereby ruling out the direct product $C_4 \times C_2$. This shows that

$$\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{7}, i)/\mathbf{Q}) \cong D_8.$$

It is now straightforward to match the intermediate extensions in the diagram above with the subgroups of D_8, showing that the diagram is complete.

For (ii), write $f(x) = x^4 - 7 = x^4 - 2 \in \mathbf{F}_5[x]$. Since

$$1^4 \equiv 2^4 \equiv 3^4 \equiv 4^4 \equiv 1 \pmod 5$$

this polynomial has no roots in $\mathbf{F}_5$. So consider the field extension $\mathbf{F}_5(\alpha) := \mathbf{F}_5[x]/(x^4 - 2)$ obtained by adjoining a root of f; in other words, α is a 4-th root of 2. With this in mind, α^2 must be a square root of 2, so over $\mathbf{F}_5(\alpha)$, the polynomial $f(x)$ factors as

$$f(x) = x^4 - 2 = (x^2 + \alpha^2)(x^2 - \alpha^2).$$

Note that $2^2 = 4 \equiv -1 \pmod 5$, which is to say that 2 is a square root of 1 in $\mathbf{F}_5$. Thus $f(x)$, in fact, splits over $\mathbf{F}_5(\alpha)$:

$$f(x) = x^4 - 2 = (x + 2\alpha)(x - 2\alpha)(x + \alpha)(x - \alpha).$$

Since the extension $\mathbf{F}_5 \subset \mathbf{F}_5(\alpha)$ is obtained by adjoining a single root of the irreducible quartic polynomial $f(x)$, it is of degree 4 and also must be the splitting field of $f(x)$. We have seen on the previous set that the Galois group

$$\mathrm{Gal}(\mathbf{F}_5(\alpha)/\mathbf{F}_5) = \mathrm{Gal}(\mathbf{F}_{625}/\mathbf{F}_5) \cong C_4$$

is the cyclic group of order $4 = [\mathbf{F}_5(\alpha) : \mathbf{F}_5]$, and it may be generated by the Frobenius automorphism $\mathrm{Fr}\colon \mathbf{F}_5(\alpha) \to \mathbf{F}_5(\alpha)$ which raises everything to the 5-th power. In terms of the primitive element α, this acts as:

$$\begin{aligned}\mathrm{Fr}(a + b\cdot\alpha + c\cdot\alpha^2 + d\cdot\alpha^3 + e\cdot\alpha^4) &= a + b\cdot\alpha^5 + c\cdot\alpha^{10} + d\cdot\alpha^{15} + e\cdot\alpha^{20} \\ &= a + 2b\cdot\alpha + 4c\cdot\alpha^2 + 8d\cdot\alpha^3 + 16e\cdot\alpha^4 \\ &= a + 2b\cdot\alpha + 4c\cdot\alpha^2 + 3d\cdot\alpha^3 + e\cdot\alpha^4\end{aligned}$$

where $a, b, c, d, e \in \mathbf{F}_5$. Thus Fr may also be described as the $\mathbf{F}_5$-automorphism determined by $\alpha \mapsto 2\alpha$, which when viewing $2 = \sqrt{-1}$ in $\mathbf{F}_5$, is similar to the situation (i). Finally, the cyclic group C_4 has only a single nontrivial subgroup $C_2 = \langle \mathrm{Fr}^2 \rangle$, and its fixed field is given by $\mathbf{F}_5(\alpha^2) \cong \mathbf{F}_{25}$. Thus the complete diagram of intermediate extensions is

$$\mathbf{F}_5 \subset \mathbf{F}_5(\alpha^2) \subset \mathbf{F}_5(\alpha) = \mathrm{SF}_{\mathbf{F}_5}(f(x)).$$

For (iii), notice first that $f(x) = x^6 + 1$ factors over $\mathbf{F}_2$ as

$$f(x) = x^6 + 1 = (x^3 + 1)^2 = (x + 1)^2(x^2 + x + 1)^2$$

and so the splitting field of $f(x)$ is also the splitting field of $g(x) := x^2 + x + 1$, which is now irreducible over $\mathbf{F}_2$. As usual, let $\mathbf{F}_2(\alpha) := \mathbf{F}_2[x]/(x^2 + x + 1)$ be the field extension obtained by adjoining a root α of $g(x)$. Over $\mathbf{F}_2(\alpha)$, this factors as

$$g(x) = x^2 + x + 1 = (x + \alpha)(x + \alpha^2) = (x + \alpha)(x + \alpha + 1)$$

from which it follows that $\mathrm{SF}_{\mathbf{F}_2}(f) = \mathrm{SF}_{\mathbf{F}_2}(g) = \mathbf{F}_2(\alpha) \cong \mathbf{F}_4$ and $\mathrm{Gal}(\mathbf{F}_4/\mathbf{F}_2) = C_2$, generated by the Frobenius $\mathrm{Fr}\colon \mathbf{F}_4 \to \mathbf{F}_4$ which squares everything. There are no nontrivial intermediate extensions here by degree reasons.

For (iv), factor $f(x) = x^8 - 1$ over $\mathbf{Q}$ by successively recognizing differences of squares:

$$f(x) = x^8 - 1 = (x^4+1)(x^4-1) = (x^4+1)(x^2+1)(x+1)(x-1).$$

Thus the splitting field L of $f(x)$ is also the splitting field of the two polynomials x^2+1 and x^4+1. In particular, $\mathbf{Q}(i) \subset L$, at which point

$$L = \mathrm{SF}_{\mathbf{Q}}(f) = \mathrm{SF}_{\mathbf{Q}}(x^2+1, x^4+1) = \mathrm{SF}_{\mathbf{Q}(i)}(x^4+1) = \mathrm{SF}_{\mathbf{Q}(i)}(x^2+i, x^2-i).$$

Writing $e^{i\pi/4}$ for a primitive 4-th root of $-1 = e^{i\pi}$, it follows that $L \subseteq \mathbf{Q}(e^{i\pi/4})$ since

$$f(x) = (x + e^{i3\pi/4})(x - e^{i3\pi/4})(x + e^{i\pi/4})(x - e^{i\pi/4})(x+i)(x-i)(x+1)(x-1)$$

or more uniformly:

$$f(x) = x^8 - 1 = \prod_{k=1}^{8} (x - e^{ik\pi/4}).$$

In fact, $\mathbf{Q}(e^{i\pi/4})$ may also be identified as the splitting field over $\mathbf{Q}$ of just the polynomial x^4+1, which implies that

$$\mathrm{Gal}(\mathbf{Q}(e^{i\pi/4})/\mathbf{Q}) \cong C_4$$

and the cyclic generator $\sigma\colon \mathbf{Q}(e^{i\pi/4}) \to \mathbf{Q}(e^{i\pi/4})$ is determined by $e^{i\pi/4} \mapsto e^{i\pi/2} = i$. This again only has a single subgroup, generated by $\sigma^2\colon e^{i\pi/4} \mapsto e^{i\pi} = -1$, and its fixed field is $\mathbf{Q}(i)$. Thus the complete set of intermediate field extensions between $\mathbf{Q}$ and $\mathbf{Q}(e^{i\pi/4})$ is

$$\mathbf{Q} \subset \mathbf{Q}(i) \subset \mathbf{Q}(e^{i\pi/4}).$$

Since $L \neq \mathbf{Q}(i)$, this implies that $L = \mathbf{Q}(e^{i\pi/4})$. ■

Problem 2. — *Let L/K be a (finite) Galois extension such that $\mathrm{Gal}(L/K) = A_4$. Prove that there is no intermediate field $K \subset F \subset L$ satisfying that $[F : K] = 2$.*

Solution. By the Galois correspondence, such an intermediate field extension F is the fixed field of some subgroup $H \subset \mathrm{Gal}(L/K) = A_4$. Since any field extension of degree 2 is Galois, in fact, H must be normal subgroup of index 2 in A_4. Since $\#A_4 = 12$, we seek a subgroup H of order 6. There are two groups of order 6, namely, the cyclic group C_6, and the symmetric group S_3 on 3 elements. But

$$A_4 = \ker(\mathrm{sgn}\colon S_4 \to \{+1, -1\})$$

and so contains no elements of even order. In particular, no elements of order 6, excluding C_6, nor any element of order 2, excluding S_3 which contains transpositions. Thus such an $H \subset A_4$ cannot exist and so no intermediate field F as above exists. ■

Problem 3. — *Give examples of finite field extensions L/K with*

(i) *L/K normal but not separable,*

(ii) *L/K separable but not normal,*

(iii) *$[L : K] = 4$ and there is no intermediate field $K \subset F \subset L$ with $[F : K] = 2$.*

Solution. For (i), let $K = \mathbf{F}_p(t)$ be a finite field of order p adjoined a single transcendental element and consider the field $L = \mathbf{F}_p(t^{1/p})$ with a p-th root of t is adjoined. Then $K \subset L$ is normal because it is the splitting field of $f(x) = x^p - t$, but it is not separable because, over L,

$$f(x) = x^p - t = (x - t^{1/p})^p.$$

For (ii), let $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt[4]{2})$. Then $K \subset L$ is separable because, as we have seen on the last set, the degree of the extension is not divisible by the characteristic. But this is not normal since $x^4 - 2$ has a root, but does not split in L.

For (iii), observe that such an extension cannot be Galois—for instance, Cauchy's theorem would imply there exists an element of order 2 in the Galois group, whence an intermediate field extension of degree 2. Also, such an extension must be separable, since a purely inseparable extension is p-power degree, but always contains degree p subextensions, and there is always a maximally separable subextension in any field extension. Thus $K \subset L$ must be a separable but not normal extension of degree 4. One way to construct such examples would be to find an irreducible polynomial $f(x) \in K[x]$ of degree 4 and take L to be a field extension in which just one root of $f(x)$ exists. In principle, a general choice of such $f(x)$ should work. Alternatively, assuming there exists a field extension with Galois group A_4 as in Problem 2—and they do exist and can be explicitly given as is done here—taking L as the fixed field of a 3-cycle will do. ■

Problem 4. — *Let $f \in \mathbf{Q}[x]$ be irreducible of prime degree p and assume that f has exactly two non-real roots. Prove that* $\mathrm{Gal}(\mathrm{SF}_{\mathbf{Q}}(f)/\mathbf{Q}) = S_p$.

Solution. Letting the Galois group $G := \mathrm{Gal}(\mathrm{SF}_{\mathbf{Q}}(f)/\mathbf{Q})$ act on the roots of f over the splitting field provides an embedding $G \hookrightarrow S_p$ of the Galois group into the symmetric group on p elements. That the rational polynomial f has exactly two non-real roots means that they must be complex conjugate, whence G contains a transposition τ. That f is irreducible implies that G acts transitively on the roots; put differently, the orbit of a single root r of f under G is size p, so by the orbit-stabilizer theorem,

$$\#G = \#\operatorname{orb}_G(r) \cdot \#\operatorname{stab}_G(r) = p \cdot \#\operatorname{stab}_G(r).$$

In particular, p divides the order of G. Since p is prime, Cauchy's theorem implies that G contains an element σ of order p which, being a subgroup of S_p, must be a p-cycle. Using primality of p once again, S_p is generated by any pair of transposition and p-cycle, so $G = S_p$. ■

Problem 5. — *Let $f(x) = x^4 + ax^2 + b$ be an irreducible quartic polynomial in $\mathbf{Q}[x]$, with roots $\pm\alpha, \pm\beta$ and let $L = \mathrm{SF}_{\mathbf{Q}}(f)$.*

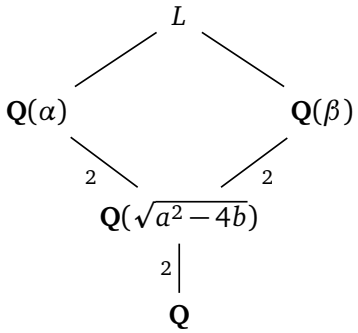
(i) *Prove that* $\mathrm{Gal}(L/\mathbf{Q})$ *is isomorphic to a subgroup of D_8.*

(ii) *Prove that this subgroup is isomorphic to C_4 if and only if $\alpha/\beta - \beta/\alpha \in \mathbf{Q}$.*

Solution. The roots of f may be explicitly determined from the quadratic formula, say:

$$\alpha := \sqrt{\frac{-a + \sqrt{a^2 - 4b}}{2}} \text{ and } \beta := \sqrt{\frac{-a - \sqrt{a^2 - 4b}}{2}}.$$

That f is irreducible implies $a^2 - 4b$ is not a square in $\mathbf{Q}$, so $\mathbf{Q} \subset \mathbf{Q}(\sqrt{a^2 - 4b})$ is a degree 2 extension. Irreducibility of f also implies that the extensions $\mathbf{Q} \subset \mathbf{Q}(\alpha)$ and $\mathbf{Q} \subset \mathbf{Q}(\beta)$ are of degree 4. Finally the expressions for α and β show that there is a diagram of field extensions of the form



showing that $[L:\mathbf{Q}] = \#\operatorname{Gal}(L/\mathbf{Q}) \in \{4,8\}$.

Since L is the splitting field of the irreducible quartic f, $\operatorname{Gal}(L/\mathbf{Q})$ is a transitive subgroup of the symmetric group S_4 on the roots of f. The restriction on the order of $\operatorname{Gal}(L/\mathbf{Q})$ means that each element is of even order. Could $\operatorname{Gal}(L/\mathbf{Q})$ only consist of elements of order 2? Well, such a subgroup of S_4 consists of transpositions (i,j) or products of disjoint transpositions $(a,b)(c,d)$. Observe, however, that the product in S_4 of disjoint transpositions with another transposition that crosses over gives a 4-cycle:

$$(a,b)(c,d)\cdot(b,c) = (a,b,d,c) \in S_4.$$

So the largest subgroup of S_4 consisting of only order 2 elements is that generated by two disjoint transpositions:

$$C_2 \times C_2 \cong \{e,(a,b),(c,d),(a,b)(c,d)\} \subset S_4.$$

But such a subgroup is not transitive! This implies that $\operatorname{Gal}(L/\mathbf{Q})$ must contain a 4-cycle, say $\sigma : L \to L$. Since σ is a $\mathbf{Q}$-automorphism and $-1 \in \mathbf{Q}$, up to replacing it by its inverse, we may assume σ acts on the roots by

$$\sigma : \alpha \mapsto \beta \mapsto -\alpha \mapsto -\beta.$$

If the cyclic group $C_4 \cong \langle\sigma\rangle \subset \operatorname{Gal}(L/\mathbf{Q})$ is a proper subgroup of the Galois group, then inspecting the diagram of field extensions shows that the Galois group additionally contains an involution $\tau : L \to L$ that is determined by, say, $\tau(\alpha) = -\alpha$ and $\tau(\beta) = \beta$. Since $\#\operatorname{Gal}(L/\mathbf{Q}) = 8$ in this case, the Galois group is generated by σ and τ, and a direct computation shows that

$$\operatorname{Gal}(L/\mathbf{Q}) \cong \langle \sigma, \tau : \sigma^4 = \tau^2 = \sigma\tau\sigma\tau = e \rangle \cong D_8.$$

These explicit descriptions of elements make it simple to characterize when $\operatorname{Gal}(L/\mathbf{Q}) \cong C_4$. If $\operatorname{Gal}(L/\mathbf{Q}) \cong C_4$, then to determine whether $x \in L$ actually lies in $\mathbf{Q}$, all we have to do is to show $\sigma(x) = x$. Consider the element $\gamma := \alpha/\beta - \beta/\alpha$. Acting by σ gives:

$$\sigma(\gamma) = \sigma\Big(\frac{\alpha}{\beta}\Big) - \sigma\Big(\frac{\beta}{\alpha}\Big) = \frac{\beta}{-\alpha} - \frac{-\alpha}{\beta} = \frac{\alpha}{\beta} - \frac{\beta}{\alpha} = \gamma$$

and so $\gamma \in \mathbf{Q}$. If $\operatorname{Gal}(L/\mathbf{Q}) \cong D_8$, however, rationality of $x \in L$ is determined not only by $\sigma(x) = x$, but also by $\tau(x) = x$. But for the element γ as above:

$$\tau(\gamma) = \tau\Big(\frac{\alpha}{\beta}\Big) - \tau\Big(\frac{\beta}{\alpha}\Big) = \frac{-\alpha}{\beta} - \frac{\beta}{-\alpha} = -\Big(\frac{\alpha}{\beta} - \frac{\beta}{\alpha}\Big) = -\gamma$$

and so $\gamma \notin \mathbf{Q}$. That was easy! Try to show that show this directly to appreciate the power of Galois theory! ■