SOLUTIONS TO WORKSHEET #11

Problem 1. — *Let K be a field and $L = K(\alpha)$ a field extension of K. Supposing that the minimal polynomial f of α over K has degree n, show that*

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} \mathrm{Nm}_{L/K}(f'(\alpha)),$$

where f' denotes the formal derivative of f.

Solution. Assume first that the extension $L \mid K$ is Galois, so that L is in fact the splitting field of f. Write $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$, where $\alpha = \alpha_1$, say. Computing using the chain rule gives

$$f'(\alpha) = f'(\alpha_1) = (\alpha_1 - \alpha_2)\cdots(\alpha_1 - \alpha_n) = \prod_{j=2}^{n} (\alpha_1 - \alpha_j).$$

Towards computing the norm, observe that since f is the minimal polynomial of $\alpha = \alpha_1$ over K, it is irreducible, and so the Galois group $\mathrm{Gal}(L \mid K)$ acts transitively on the α_i; write $\sigma_i \in \mathrm{Gal}(L \mid K)$ for the automorphism that satisfies $\sigma_i(\alpha_1) = \alpha_i$. Then

$$\mathrm{Nm}_{L/K}(f'(\alpha)) = \prod_{i=1}^{n} \sigma_i(f'(\alpha)) = \prod_{i=1}^{n} f'(\sigma_i(\alpha_1)) = \prod_{i=1}^{n} f'(\alpha_i) = \prod_{1 \le i \ne j \le n} (\alpha_i - \alpha_j).$$

To obtain the discriminant, it remains to order the differences $\alpha_i - \alpha_j$: exactly half of the $n(n-1)$ factors are in the wrong order, so flipping that many signs gives

$$(-1)^{\frac{n(n-1)}{2}} \mathrm{Nm}_{L/K}(f'(\alpha)) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = \Delta(f).$$

In the general case where $L \mid K$ is not necessarily Galois, one may show that the norm may be computed in a similar fashion, but instead of automorphisms over K, one takes $\sigma_i \colon L \to \overline{K}$ the n distinct K-homomorphisms into the algebraic closure which satisfy $\sigma_i(\alpha_1) = \alpha_i$. With this, the proof proceeds as above. ∎

Problem 2. — *For each of the following polynomials $f(x) \in \mathbf{Q}[X]$, compute the Galois group of the extension $\mathrm{SF}_{\mathbf{Q}}(f)/\mathbf{Q}$.*

(i) $f(x) = x^4 + x^3 + x^2 + 1$.

(ii) $f(x) = x^4 - 4x^3 + 4x^2 + 6$.

Proof. Recall that the *resolvent* of a quartic polynomial $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$ is the cubic polynomial $r(x) := (x-\beta_1)(x-\beta_2)(x-\beta_3)$ where

$$\beta_1 := \alpha_1\alpha_2 + \alpha_3\alpha_4, \qquad \beta_2 := \alpha_1\alpha_3 + \alpha_2\alpha_4, \qquad \beta_3 := \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

The resolvent has two key properties: First, $f(x)$ and $r(x)$ have the same discriminant. For this, it suffices to identify the two half-discriminants:

$$\begin{aligned}
\Delta(r)^{1/2} &= (\beta_1 - \beta_2)(\beta_1 - \beta_3)(\beta_2 - \beta_3) \\
&= (\alpha_1\alpha_2 + \alpha_3\alpha_4 - \alpha_1\alpha_3 - \alpha_2\alpha_4)(\alpha_1\alpha_2 + \alpha_3\alpha_4 - \alpha_1\alpha_4 - \alpha_2\alpha_3)(\alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_4 - \alpha_2\alpha_3) \\
&= (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4) \\
&= \Delta(f)^{1/2}.
\end{aligned}$$

Date: December 4, 2025.

Second, if $f(x) = x^4 + ax^3 + bx^2 + cx + d$, then

$$r(x) = x^3 - bx^2 + (ac - 4d)x + 4bd - a^2d - c^2.$$

Expanding the factored expression for f and comparing coefficients shows that

$$\begin{aligned} -a &= \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4, \\ b &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4, \\ -c &= \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4, \text{ and} \\ d &= \alpha_1\alpha_2\alpha_3\alpha_4. \end{aligned}$$

Write $r(x) = x^3 + sx^2 + tx + u$. Expanding and comparing expressions easily gives the quadratic coefficient as $-s = \beta_1 + \beta_2 + \beta_3 = b$. For the linear coefficient,

$$\begin{aligned} t = \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 = (\alpha_1^2\alpha_2\alpha_3 + \alpha_1\alpha_2^2\alpha_4 + \alpha_1\alpha_3^2\alpha_4 + \alpha_2\alpha_3\alpha_4^2) + (\alpha_1^2\alpha_2\alpha_4 + \alpha_1\alpha_2^2\alpha_3 \\ + \alpha_1\alpha_3\alpha_4^2 + \alpha_2\alpha_3^2\alpha_4) + (\alpha_1^2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3^2 + \alpha_1\alpha_2\alpha_4^2 + \alpha_2^2\alpha_3\alpha_4) \end{aligned}$$

Factoring out one copy of α_i whenever a square appears gives

$$\begin{aligned} t = \alpha_1(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4) + \alpha_2(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_2\alpha_3\alpha_4) \\ + \alpha_3(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4) + \alpha_4(\alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4). \end{aligned}$$

Each parenthesized term almost looks like $-c$, but the term following α_i is missing the product $\alpha_1\alpha_2\alpha_3\alpha_4/\alpha_i$. Adding and subtracting that in each term produces

$$t = -(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)c - 4\alpha_1\alpha_2\alpha_3\alpha_4 = ac - 4d.$$

Finally, to identify the constant coefficient $-u = \beta_1\beta_2\beta_3$, compute:

$$\begin{aligned} -u &= \alpha_1^3\alpha_2\alpha_3\alpha_4 + \alpha_1^2\alpha_2^2\alpha_4^2 + \alpha_1^2\alpha_3^2\alpha_4^2 + \alpha_1\alpha_2\alpha_3\alpha_4^3 + \alpha_1^2\alpha_2^2\alpha_3^2 + \alpha_1\alpha_2^3\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3^3\alpha_4 + \alpha_2^2\alpha_3^2\alpha_4^2 \\ &= (\alpha_1^2\alpha_2^2\alpha_3^2 + \alpha_1^2\alpha_2^2\alpha_4^2 + \alpha_1^2\alpha_3^2\alpha_4^2 + \alpha_2^2\alpha_3^2\alpha_4^2) + (\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2)\alpha_1\alpha_2\alpha_3\alpha_4. \end{aligned}$$

The first parenthesized term looks like c^2 whereas the second parenthesized term looks like a^2. Both, however, are missing the cross-terms. Adding and subtracting them gives

$$\begin{aligned} -u = c^2 - 2(\alpha_1^2\alpha_2^2\alpha_3\alpha_4 + \alpha_1^2\alpha_2\alpha_3^2\alpha_4 + \alpha_1\alpha_2^2\alpha_3^2\alpha_4 + \alpha_1^2\alpha_2\alpha_3\alpha_4 + \alpha_1\alpha_2^2\alpha_3\alpha_4^2 + \alpha_1\alpha_2\alpha_3^2\alpha_4^2) \\ + a^2d - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4)d \end{aligned}$$

Factoring out $\alpha_1\alpha_2\alpha_3\alpha_4 = d$ from the first parenthesized term produces $-2bd$; similarly, the second parenthesized term may be recognized as b. Putting everything together thus gives

$$-u = c^2 + a^2d - 4bd.$$

On to the problem at hand: The resolvent for the quartic $f(x) = x^4 + x^3 + x^2 + 1$ in (i) is $r(x) = x^3 - x^2 - 4x + 3$. Notice that $r(x) \equiv x^3 + x^2 + 1 \pmod 2$, which is irreducible over $\mathbf{F}_2$, and so $r(x)$ itself is irreducible in $\mathbf{Q}[x]$. Next, making the change of variables $x = y + 1/3$ simplifies the resolvent to

$$r(y) = y^3 - \frac{13}{3}y + \frac{43}{27} \text{ and so } \Delta(f) = \Delta(r) = 4\left(\frac{13}{3}\right)^3 - 27\left(\frac{43}{27}\right)^2 = 257,$$

which is not a square in $\mathbf{Q}$. Therefore $\mathrm{Gal}(\mathrm{SF}_{\mathbf{Q}}(f) \mid \mathbf{Q}) \cong S_3$.

The resolvent for the quartic $f(x) = x^4 - 4x^3 + 4x^2 + 6$ is $r(x) = x^3 - 4x^2 - 24x = x(x^2 - 4x - 24)$, which is reducible. The discriminant in this case may be computed using the discriminant of the quadratic equation together with the fact that 0 is a root:

$$\Delta(f) = \Delta(r) = 24^2(4^2 + 4 \cdot 24) = 64512$$

and this is not a square, meaning that the extension $\mathbf{Q} \subset \mathrm{SF}_{\mathbf{Q}}(r)$ has degree 2. Since f is irreducible over $\mathbf{Q}$ by Eisenstein's criterion with respect to $p = 2$, this implies that $\mathrm{Gal}(\mathrm{SF}_{\mathbf{Q}}(f) \mid \mathbf{Q}) \cong C_4$. ■

Problem 3. — *For $\alpha \in \mathbf{Q}$, let $f_\alpha(x) = x^4 + x^3 + x^2 + x + \alpha$ and let G_α denote the Galois group of the extension $\mathrm{SF}_{\mathbf{Q}}(f_\alpha)/\mathbf{Q}$. Find four integers $\alpha_1, \alpha_2, \alpha_3$ and α_4 such that the corresponding groups G_{α_i} are pairwise non-isomorphic.*

Solution. The resolvent for the quartic $f_\alpha(x) = x^4 + x^3 + x^2 + x + \alpha$ is

$$r_\alpha(x) = x^3 - x^2 + (1-4\alpha)x + 3\alpha - 1 = y^3 + \frac{1}{3}(2-12\alpha)y - \frac{1}{27}(20-45\alpha)$$

where $x = y + 1/3$ as before. With the simplified form, the discriminant may be computed to be

$$\Delta(f_\alpha) = \Delta(r_\alpha) = -\frac{4}{27}(2-12\alpha)^3 - \frac{1}{27}(20-45\alpha)^2 = 256\alpha^3 - 203\alpha^2 + 88\alpha - 16.$$

Taking $\alpha = 0$ gives reducible $f_0(x)$ and $r_0(x) = (x-1)(x^2+1)$, which shows that the Galois group is C_4. Taking $\alpha = 1$ gives irreducible $f_1(x)$—as may be verified reduction modulo 2—and $r_1(x) = (x-2)(x^2+x-1)$, so the Galois group is D_4. Taking $\alpha = 2$ gives irreducible $f_2(x)$ and irreducible $r_2(x) = x^3 - x^2 - 7x + 5$—these may be verified reduction modulo 5 and 3, respectively. The discriminant is 1396, which is not a square, and so the Galois group of f_2 is S_4.

I can't seem to find a fourth integer α to obtain either A_4 or V. Another value that does seem interesting is $\alpha = 12$, in which case $r_{12}(x) = (x-7)(x^2+6x-5)$ and $f_{12}(x)$ is irreducible, so has Galois group D_4. ■

Problem 4. — *Let p be a prime and let $n \geq 4$. Prove that there does not exist a polynomial $f \in \mathbf{F}_p[x]$ of degree n such that $\mathrm{SF}_{\mathbf{F}_p}(f_\alpha)/\mathbf{F}_p$ has Galois group isomorphic to A_n or S_n. What happens if $n = 3$?*

Solution. This is just because all extensions of finite fields have cyclic Galois groups and that neither A_n nor S_n are cyclic groups when $n \geq 4$. When $n = 3$, $A_3 \cong C_3$ and so taking any polynomial giving a degree 3 extension of $\mathbf{F}_3$ will work. ■

Problem 5. — *Consider the polynomial $f(x) = x^5 + 20x + 16 \in \mathbf{Q}[x]$. It is known that the Galois group of the extension $\mathrm{SF}_{\mathbf{Q}}(f)/\mathbf{Q}$ has order at least 15. Prove that this group must be A_5.*

Solution. Reduction modulo 3 shows that the polynomial $f(x) = x^5 + 20x + 16$ is irreducible, so that the Galois group $G := \mathrm{Gal}(\mathrm{SF}_{\mathbf{Q}}(f) \mid \mathbf{Q})$ is a transitive subgroup of S_5. Next, its discriminant is

$$\Delta = 2^8 \cdot 20^5 + 5^5 \cdot 16^4 = 1\,024\,000\,000 = 2^{16} \cdot 5^6$$

which is a square, which implies that $G \subseteq A_5$. Since $\#G \geq 15$, it can either be the general affine group of $\mathbf{F}_5$ or else is A_5; to rule out the latter, use Dedekind's recipe. Reducing f modulo 7 makes it reducible with factors

$$f(x) \equiv x^5 + 6x + 2 = (x+3)(x+2)(x^3 + 2x^2 + 5x + 5) \pmod 7.$$

Dedekind's recipe implies that G contains a 3-cycle, and so $3 \mid \#G$. This rules out the general affine group since it has 20 elements, and so it follows that $G \cong A_5$. ■