MA 3419: Galois theory
Selected answers/solutions to the assignment due November 14, 2017

1. The multiplicative group $(\mathbb{Z}/13\mathbb{Z})^\times$ is cyclic generated by 2; the powers of 2 modulo 13 are, in the order of the exponent, $1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7$. Thus, denoting by ξ the primitive root $e^{2\pi/13}$ of unity of degree 13, we may consider the quantities

$$A = \xi + \xi^4 + \xi^3 + \xi^{12} + \xi^9 + \xi^{10},$$
$$A' = \xi^2 + \xi^8 + \xi^6 + \xi^{11} + \xi^5 + \xi^7.$$

Clearly, $A + A' = -1$, and $AA' = -3$, so A and A' are roots of the quadratic equation $x^2 + x - 3 = 0$. Next, we consider the quantities

$$B = \xi + \xi^{12},$$
$$B' = \xi^4 + \xi^9,$$
$$B'' = \xi^3 + \xi^{10}.$$

We have $B+B'+B'' = A$, $BB'+BB''+B'B'' = -1$, $BB'B'' = 2+A'$, so B, B', and B'' are roots of a cubic equation with coefficients of $\mathbb{Q}(A, A')$. Clearly, $\xi + \xi^{12} = \xi + \xi^{-1} = 2\cos(2\pi/13)$.

2. Roots of $x^3 - 5$ are $\sqrt[3]{5}$, $\omega\sqrt[3]{5}$, $\omega^2\sqrt[3]{5}$, where ω is a primitive cube root of 1. Thus, the splitting field of $x^3 - 5$ over $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Q}(\sqrt[3]{5}, \omega, \sqrt{2})$. Note that $\omega \notin \mathbb{Q}(\sqrt{2})$ since ω is not real, so $[\mathbb{Q}(\omega, \sqrt{2})\colon \mathbb{Q}] = 4$ by Tower Law. Also, $\mathbb{Q}(\sqrt[3]{5}, \omega, \sqrt{2})$ contains a subfield $\mathbb{Q}(\sqrt[3]{5})$ of degree 3 (since $x^3 - 5$ is irreducible by Eisenstein), so $[\mathbb{Q}(\sqrt[3]{5}, \omega, \sqrt{2})\colon \mathbb{Q}]$ is divisible by 3. Since $[\mathbb{Q}(\sqrt[3]{5}, \omega, \sqrt{2})\colon \mathbb{Q}] \leqslant 12$, these observations show that $[\mathbb{Q}(\sqrt[3]{5}, \omega, \sqrt{2})\colon \mathbb{Q}] = 12$, and that the elements $\sqrt{2}^i\omega^j\sqrt[3]{5}^k$ with $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant 1$, and $0 \leqslant k \leqslant 2$ form a basis over $\mathbb{Q}$. Consequently, the elements $\omega^j\sqrt[3]{5}^k$ with $0 \leqslant j \leqslant 1$, and $0 \leqslant k \leqslant 2$ form a basis over $\mathbb{Q}(\sqrt{2})$. Any automorphism sends ω to ω or ω^2, and $\sqrt[3]{5}$ to $\omega^k\sqrt[3]{5}$, where $0 \leqslant k \leqslant 2$, so there are six automorphisms, as expected (it is the degree of the extension). The group generated by these is S_3, as one can note from their action on the elements $x_i = \omega^{i+1}\sqrt[3]{5}$, $i = 1, 2, 3$.

3. We have $x^4 - 2x^2 - 5 = x^4 - 2x^2 + 1 - 6 = (x^2 - 1)^2 - 6 = (x^2 - 1 - \sqrt{6})(x^2 - 1 + \sqrt{6})$. This means that the roots of this polynomial are $\pm\sqrt{1 + \sqrt{6}}$ and $\pm\sqrt{1 - \sqrt{6}} = \pm\frac{\sqrt{-5}}{\sqrt{1+\sqrt{6}}}$, so the splitting field is $\mathbb{Q}(\sqrt{1 + \sqrt{6}}, \sqrt{-5})$.

Let us show that $1 + \sqrt{6}$ is not a square in $\mathbb{Q}(\sqrt{6})$. If it were, we would have $(a + b\sqrt{6})^2 = 1 + \sqrt{6}$ for some rational a, b, or $a^2 + 6b^2 = 1, 2ab = 1$. This means that $\frac{1}{4b^2} + 6b^2 = 1$. Clearing the denominator, $24b^4 - 4b^2 + 1 = 0$, and this does not have real roots, let alone rational ones.

Therefore, $[\mathbb{Q}(\sqrt{1 + \sqrt{6}})\colon \mathbb{Q}] = 4$. Finally, $\sqrt{-5} \notin \mathbb{Q}(\sqrt{1 + \sqrt{6}})$ since it is not a real number, so $[\mathbb{Q}(\sqrt{1 + \sqrt{6}}, \sqrt{-5})\colon \mathbb{Q}(\sqrt{1 + \sqrt{6}})] = 2$. By Tower Law, $[\mathbb{Q}(\sqrt{1 + \sqrt{6}}, \sqrt{-5})\colon \mathbb{Q}] = 8$.

Note that our extension is a Galois extension, so its Galois group contains 8 elements. Each of these elements sends $\sqrt{1 + \sqrt{6}}$ to one of the four roots of this polynomial, and $\sqrt{-5}$ to $\pm\sqrt{-5}$; this data defines an automorphism completely, and this gives at most 8 distinct automorphisms. Thus, each of these is a well defined automorphisms. If we define an automorphism σ by letting $\sigma(\sqrt{1 + \sqrt{6}}) = \frac{\sqrt{-5}}{\sqrt{1+\sqrt{6}}}$, $\sigma(\sqrt{-5}) = -\sqrt{-5}$, and $\tau(\sqrt{1 + \sqrt{6}}) = \sqrt{1 + \sqrt{6}}$,

$\tau(\sqrt{-5}) = -\sqrt{-5}$, then we have

$$\sigma^2(\sqrt{1+\sqrt{6}}) = \sigma(\frac{\sqrt{-5}}{\sqrt{1+\sqrt{6}}}) = \frac{-\sqrt{-5}}{\frac{\sqrt{-5}}{\sqrt{1+\sqrt{6}}}} = -\sqrt{1+\sqrt{6}}, \quad \sigma^2(\sqrt{-5}) = \sqrt{-5},$$

$$\sigma^3(\sqrt{1+\sqrt{6}}) = \sigma(\sigma^2(\sqrt{1+\sqrt{6}})) = -\sigma(\sqrt{1+\sqrt{6}}) = -\frac{\sqrt{-5}}{\sqrt{1+\sqrt{6}}}, \quad \sigma^3(\sqrt{-5}) = -\sqrt{-5},$$

and finally

$$\sigma^4(\sqrt{1+\sqrt{6}}) = \sigma(\sigma^3(\sqrt{1+\sqrt{6}})) = \sigma(-\frac{\sqrt{-5}}{\sqrt{1+\sqrt{6}}}) = \frac{\sqrt{-5}}{\frac{\sqrt{-5}}{\sqrt{1+\sqrt{6}}}} = \sqrt{1+\sqrt{6}}, \quad \sigma^4(\sqrt{-5}) = \sqrt{-5},$$

so $\sigma^4 = e$. Also, we have $\tau^2 = e$. Finally,

$$\tau\sigma^3(\sqrt{1+\sqrt{6}}) = \tau(-\frac{\sqrt{-5}}{\sqrt{1+\sqrt{6}}}) = \frac{\sqrt{-5}}{\sqrt{1+\sqrt{6}}} = \sigma\tau(\sqrt{1+\sqrt{6}})$$

and $\tau\sigma^3(\sqrt{-5}) = \sqrt{-5} = \sigma\tau(\sqrt{-5})$. This means that $\sigma\tau = \tau\sigma^3$, and altogether σ and τ generate the dihedral group D_4 of 8 elements, which is therefore the Galois group.

4. The splitting field of f is $\mathbb{Q}(\sqrt[4]{2}, i)$, by a standard argument it is a field of degree 8. Each Galois group element is completely determined by the action on $\sqrt[4]{2}$ and on i: $\sqrt[4]{2}$ is sent to $i^l\sqrt[4]{2}$, and i is sent to $\pm i$. If we consider in the complex plane the square formed by the roots of x^4-2, then the Galois group action on the roots is manifestly the dihedral group D_4 action by symmetries of that square: the element σ for which $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$, $\sigma(i) = i$, implements the rotation of the square, while the element τ for which $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$, $\tau(i) = -i$ implements the reflection about the diagonal.

Subgroups of D_4 are: four subgroups generated by the reflections τ, $\sigma\tau$, $\sigma^2\tau$, $\sigma^3\tau$, the subgroup of order 2 generated by σ^2, the subgroup of order 4 generated by σ, and the two Klein 4-groups generated by σ^2 and τ and by σ^2 and $\sigma\tau$. The invariant subfield of the subgroup generated by σ^2 and τ is $\mathbb{Q}(\sqrt{2})$, the invariant subfield of the subgroup generated by σ^2 and $\sigma\tau$ is $\mathbb{Q}(i\sqrt{2})$, the invariant subfield of the subgroup generated by σ is $\mathbb{Q}(i)$, the invariant subfield of the subgroup generated by σ^2 is $\mathbb{Q}(\sqrt{2}, i)$, the invariant subfield of the subgroup generated by τ is $\mathbb{Q}(\sqrt[4]{2})$, the invariant subfield of the subgroup generated by $\sigma\tau$ is $\mathbb{Q}((1+i)\sqrt[4]{2})$, the invariant subfield of the subgroup generated by $\sigma^2\tau$ is $\mathbb{Q}(i\sqrt[4]{2})$, the invariant subfield of the subgroup generated by $\sigma^3\tau$ is $\mathbb{Q}((1-i)\sqrt[4]{2})$.

Some remarks on finding invariant subfields: If $k \subset F \subset K$ is a tower where $k \subset K$ is a Galois extension, then we know that $F \subset K$ is a Galois extension too. Thus, $\#\,\mathrm{Gal}(K\colon k) = [K\colon k]$, $\#\,\mathrm{Gal}(K\colon F) = [K\colon F]$, so by Tower Law $[F\colon k]$ is the index of the subgroup $\mathrm{Gal}(K\colon F)$ of the group $\mathrm{Gal}(K\colon k)$. Therefore, two-element subgroups correspond to degree four extensions, and the four-element subgroups correspond to quadratic extensions. Now, some of the extensions above are fixed by the corresponding subgroups by direct inspection of definitions of σ and τ. Some, like $\mathbb{Q}((1+i)\sqrt[4]{2})$, are obtained as follows: the element $\lambda = \sigma\tau$ is of order 2, so for each a, the element $a + \lambda(a)$ is λ-invariant, since $\lambda(a + \lambda(a)) = \lambda(a) + \lambda^2(a) = \lambda(a) + a$. Taking $a = \sqrt[4]{2}$, we get the element $u = (1+i)\sqrt[4]{2}$. It generates a degree 4 extension, since $u^4 = -8$, and the polynomial $x^4 + 8$ is irreducible: its roots are u, iu, $-u$, $-iu$, and no product of fewer than four of those can give a rational number.

The normal extensions of $\mathbb{Q}$ are, by Galois correspondence, those corresponding to normal subgroups. Any subgroup of index 2 is normal; these correspond to quadratic extensions which are also always normal. The only subgroup of order 2 which is normal is the subgroup generated by σ^2; that subgroup is the centre of D_4. The corresponding subfield is $\mathbb{Q}(\sqrt{2}, i)$ which is the splitting field of $(x^2-2)(x^2+1)$, so a normal extension indeed.

5. In $\mathbb{F}_5$, we have $3^2 \neq 1$, $3^4 = 1$. This means that the element $x = \sqrt[4]{3}$ in the splitting field of $x^4 - 3$ is of order 16 in the multiplicative group of that field. That splitting field is of characteristic 5, so its multiplicative group has $5^k - 1$ elements, where k is the degree of the extension. By Lagrange's theorem, 16 divides $5^k - 1$, so $k \neq 1, 2, 3$, thus $k \geqslant 4$. Also, $\mathbb{F}_5$ has four distinct fourth roots of 1, so adjoining one root of $x^4 - 3$ gives the splitting field. This implies that $x^4 - 3$ is irreducible, and that the Galois group is the cyclic group of order 4 of fourth roots of 1 in $\mathbb{F}_5$.

In $\mathbb{F}_7$, we have $3^6 = 1$, $3^k \neq 1$ for $0 < k < 6$. This means that the element $x = \sqrt[4]{3}$ in the splitting field of $x^4 - 3$ is of order 24 in the multiplicative group of that field. That splitting field is of characteristic 7, so its multiplicative group has $7^k - 1$ elements, where k is the degree of the extension. Thus, it is possible that $k = 2$ would work. Let us consider the quadratic extension $\mathbb{F}_7(\sqrt{3})$. In this extension, $\sqrt{3}$ is in fact a square, since $(a + b\sqrt{3})^2 = \sqrt{3}$ has a solution $a = 1$, $b = 4$. Also, in that extension, $(3\sqrt{3})^2 = 27 = -1$, so that extension has four distinct fourth roots of -1: ± 1 and $\pm 3\sqrt{3}$. We conclude that the splitting field is $\mathbb{F}_{49}$ and the Galois group is the cyclic group of order 2.

In $\mathbb{F}_{11}$, we have $3^5 = 1$, $3^k \neq 1$ for $0 < k < 5$. This means that the element $x = \sqrt[4]{3}$ in the splitting field of $x^4 - 3$ is of order 20 in the multiplicative group of that field. That splitting field is of characteristic 11, so its multiplicative group has $11^k - 1$ elements, where k is the degree of the extension. Thus, it is possible that $k = 2$ would work. Note that $5^2 = 25 = 3$ in $\mathbb{F}_{11}$, so $\mathbb{F}_{11}(\sqrt[4]{3})$ is a quadratic extension. All fields of 121 elements are isomorphic, so that extension also contains $i = \sqrt{-1}$, and hence the four distinct fourth roots of 1. We conclude that the splitting field is $\mathbb{F}_{121}$ and the Galois group is the cyclic group of order 2.

Over $\mathbb{F}_{13}$, our polynomial splits: $x^4 - 3 = (x-2)(x+2)(x-3)(x+3)$, so the splitting field is $\mathbb{F}_{13}$, and the Galois group is trivial.

6. $K = k(a)$ if and only if $k(a)$ is not a proper subfield of K, which happens if and only if it is not a fixed field of a nontrivial subgroup of G, which happens if and only if the only element which fixes a is e, which happens if and only if $g_1(a), \ldots, g_n(a)$ are distinct elements of K.