SPRING 2024: MATH 791 EXAM 3 SOLUTIONS

You will work in teams on this exam. You may use your notes, the Daily Summary, and any homework you have done (providing full details), but you may not consult any other sources, including, any algebra textbook, the internet, any graduate students not on your team, or any professor except your Math 791 instructor. You may not cite without proof any facts not covered in class or the homework. All members of each team should contribute to the team's effort. The solutions should be typeset in LaTex. Each team member should also participate in the typesetting effort. Each team should upload a pdf file of its solution to Canvas no later than 5pm, Friday May 10. Note: Please do not upload solutions in any other format.

Each problem is worth 10 points. To receive full credit, all proofs must be complete and contain the appropriate amount of detail. Good luck on the exam!

1. Show that the identity map is the only automorphism of $\mathbb{R}$.[1] Hint: Use the automorphism properties to prove that an automorphism of $\mathbb{R}$ must be a continuous function from $\mathbb{R}$ to $\mathbb{R}$.

Solution. Let $\sigma : \mathbb{R} \to \mathbb{R}$ be an automorphism. There are many ways to solve this problem. We begin by noting that if $a \in \mathbb{R} \geq 0$, then $\sigma(a) = \sigma(\sqrt{a} \cdot \sqrt{a}) = \sigma(\sqrt{a})^2 \geq 0$. Thus, if $a \geq b$, then $a - b \geq 0$, so that $0 \leq \sigma(a-b) = \sigma(a) - \sigma(b)$, and thus $\sigma(a) \geq \sigma(b)$. In other words, σ preserves order. Now suppose $\{x_n\}$ is a sequence converging to 0. Then $\{x_n^2\}$ also converges to 0. For each n there exists a rational number such that $0 \leq x_n^2 \leq r_n$, with $\{r_n\}$ converging to 0. Thus, $0 \leq \sigma(x_n^2) = \sigma(x_n)^2 \leq \sigma(r_n) = r_n$, from which it follows that $\{\sigma(x_n)^2\}$ and hence $\{\sigma(x_n)\}$ converges to 0. Therefore σ is continuous at 0. Now let $a \in \mathbb{R}$ be any real number and suppose $\{x_n\}$ converges to a. Then $\{x_n - a\}$ converges to 0, and hence $\{\sigma(x_n - a)\}$ converges to 0, from which it follows $\{\sigma(x_n)\}$ converges to $\sigma(a)$. Therefore σ is continuous at a, and hence a continuous function. Since σ fixes every rational number and every real number is a limit of rational numbers, it follows that σ fixes every real number, i.e., σ is the identity. □

2. Let F be a field of characteristic zero, $a \in F$ and $n \geq 1$. Suppose F contains a primitive nth root of unity, ϵ, and set $f(x) = x^n - a$. Let $\alpha \in \overline{F}$ be a root of $f(x)$. Show that $F(\alpha)$ is Galois over F and that $\text{Gal}(F(\alpha)/F)$ is abelian.

Solution. The roots of $f(x)$ are $\alpha, \alpha\epsilon, \ldots, \alpha\epsilon^{n-1}$, which are distinct. Thus $\mathbb{Q}(\alpha)$ is the splitting field of $f(x)$ over $\mathbb{Q}$, and is therefore Galois over $\mathbb{Q}$, by the lecture of April 19. Let $\sigma, \tau \in \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$. Then $\sigma(\alpha) = \alpha\epsilon^i$ and $\tau(\alpha) = \alpha\epsilon^j$, for some $1 \leq i, j \leq n-1$. Thus,

$$\sigma\tau(\alpha) = \sigma(\alpha\epsilon^j) = \epsilon^j\sigma(\alpha) = \epsilon^j\epsilon^i\alpha = \epsilon^i\epsilon^j\alpha = \epsilon^i\tau(\alpha) = \tau(\alpha\epsilon^i) = \tau\sigma(\alpha).$$

Since σ, τ are determined by their effect on α, we have $\sigma\tau = \tau\sigma$, as elements of $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$. Since σ, τ are arbitrary, this gives what we want. □

3. The famous Kronecker-Weber Theorem states that an abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension of $\mathbb{Q}$. In other words, if $\mathbb{Q} \subseteq K$ is a finite, Galois extension and $\text{Gal}(K/\mathbb{Q})$ is abelian, then there exists $n \geq 1$ and a primitive nth root of unity ϵ such that $K \subseteq \mathbb{Q}(\epsilon)$. For arbitrary extensions, this theorem fails. Let $\sqrt[3]{2}$ denote the real cube root of 2. Prove that $\mathbb{Q}(\sqrt[3]{2})$ is not contained in $\mathbb{Q}(\epsilon)$, for any nth root of unity ϵ.

Solution. Suppose by way of contradiction that $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\epsilon)$, where ϵ is an nth root of unity. By enlarging the extension, we may, without loss of generality, assume that ϵ is a primitive nth root of unity. Thus, the extension is a Galois extension (its the splitting field of $x^n - 1$ over $\mathbb{Q}$) with abelian Galois group (by Problem 10). Since $x^3 - 2$ has a root in $\mathbb{Q}(\epsilon)$, it has all of its roots in $\mathbb{Q}(\epsilon)$, by the property of splitting field shown in the lecture of April 17. If we write K for the splitting field of $x^3 - 2$ over $\mathbb{Q}$, then we have $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\epsilon)$. Since K is Galois over $\mathbb{Q}$, by the Galois Correspondence Theorem $\text{Gal}(K/F)$ is a homomorphic image of $\text{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$. However the latter is abelian, while the former is isomorphic to S_3, which gives the required contradiction. □

[1] By contrast, there are *uncountably many* automorphisms of $\mathbb{C}$!

4. For $f(x) = x^3 + x + 1$ and $g(x) = x^4 + 3x^2 + x + 7$ in $\mathbb{Q}[x]$:

(i) Find rational polynomials $a(x), b(x) \in \mathbb{Q}[x]$ such that $1 = a(x)f(x) + b(x)g(x)$.

(ii) Prove that $g(x)$ is irreducible over $\mathbb{Q}$. Then, let $\alpha \in \mathbb{C}$ be a root of $g(x)$ and find $f(\alpha)^{-1}$ as an element of $\mathbb{Q}(\alpha)$, written in terms of the basis $1, \alpha, \alpha^2, \alpha^3$.

(iii) Similarly, for $h(x) = x^3 + 4x^2 + x$, find $f(\alpha)h(\alpha)$ as an element of $\mathbb{Q}(\alpha)$, written in terms of the basis.

Solution. For (i), the first step is to use the Euclidean algorithm to find, the GCD, i.e., the last non-zero remainder upon repeated applications of the division algorithm. This leads to:

$$\begin{aligned} g(x) &= xf(x) + (2x^2 + 7) \\ f(x) &= \frac{x}{2}(2x^2 + 7) + (-\frac{5}{2}x + 1) \\ 2x^2 + 7 &= -(\frac{4}{5}x + \frac{8}{25})(-\frac{5}{2}x + 1) + \frac{183}{25}. \end{aligned}$$

Recalling that GCDS are unique up to units, we see that 1 is the GCD of $f(x)$ and $g(x)$. We use backwards substitution with the equations above to solve for $\frac{183}{25}$ in terms of $f(x)$ and $g(x)$.

$$\begin{aligned} \frac{183}{25} &= 1 \cdot (2x^2 + 7) + (\frac{4}{5}x + \frac{8}{25})(-\frac{5}{2}x + 1) \\ \frac{183}{25} &= 1 \cdot (2x^2 + 7) + (\frac{4}{5}x + \frac{8}{25})(f(x) - \frac{x}{2}(2x^2 + 7)) \\ \frac{183}{25} &= (\frac{4}{5}x + \frac{8}{25})f(x) + (1 - \frac{2}{5}x^2 - \frac{4}{25}x)(2x^2 + 7) \\ \frac{183}{25} &= (\frac{4}{5}x + \frac{8}{25})f(x) + (1 - \frac{2}{5}x^2 - \frac{4}{25}x)(g(x) - xf(x)) \\ \frac{183}{25} &= (\frac{8}{25} - \frac{1}{5}x + \frac{4}{25}x^2 + \frac{2}{5}x^3)f(x) + (1 - \frac{2}{5}x^2 - \frac{4}{25}x)g(x). \end{aligned}$$

Multiplying the last equation by $\frac{25}{183}$, we obtain

$$a(x) = \frac{8}{183} - \frac{5}{183}x + \frac{4}{183}x^2 + \frac{10}{183}x^3 \quad \text{and} \quad b(x) = \frac{25}{183} - \frac{10}{183}x^2 - \frac{4}{183}x.$$

For (ii), note that $g(x)$ is a primitive polynomial, thus, by Gauss's Lemma, to see that $g(x)$ is irreducible over $\mathbb{Q}$, it suffices to see that $g(x)$ is irreducible over $\mathbb{Z}$. By the Rational Root Test, $g(x)$ does not have a root in $\mathbb{Q}$, so $g(x)$ does not factor as a product of a linear polynomial and a cubic polynomial with coefficients in $\mathbb{Z}$. Suppose $g(x) = (x^2 + a_1x + a_0)(x^2 + b_1x + b_0)$, with each $a_i, b_i \in \mathbb{Z}$. This single equation in $\mathbb{Z}[x]$ gives rise to the system of equations over $\mathbb{Z}$

$$\begin{aligned} a_1 + b_1 &= 0 \\ a_1b_1 + a_0 + b_0 &= 3 \\ a_0b_1 + a_1b_0 &= 1 \\ a_0b_0 &= 7. \end{aligned}$$

I will leave it to you to verify that this system of equations has no solutions over $\mathbb{Z}$, which implies that $g(x)$ is irreducible over $\mathbb{Z}$.

To find $f(\alpha)^{-1}$, upon substituting α in the the last displayed equation above in problem 3 involving $\frac{183}{25}$, we see that

$$f(\alpha)^{-1} = a(\alpha) = \frac{8}{183} - \frac{5}{183}\alpha + \frac{4}{183}\alpha^2 + \frac{10}{183}\alpha^3.$$

For (iii), one calculates $f(x)h(x) = (x^2 + 4x - 1)g(x) + (-8x^3 - 3x^2 - 26x + 7)$, so writing $f(\alpha)g(\alpha)$ in terms of the basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ we get $f(\alpha)h(\alpha) = -8\alpha^3 - 3\alpha^2 - 26\alpha + 7$.

5. Let $F \subseteq K$ be an extension of fields with $[K : F] < \infty$. Prove that $|\text{Gal}(K/F)| \leq [K : F]$. Hint: Write $K = F(\alpha_1, \ldots, \alpha_n)$ and use induction together with the Crucial Proposition from April 12. Start by getting a good understanding of the case $n = 2$. For this, find the number of field homomorphisms $F(\alpha_1) \to F(\alpha_1, \alpha_2)$

fixing F. (Note any homomorphism between fields is one-to-one, and thus an isomorphism on to its image.) Now work out how to use the Crucial Proposition to count the number of automorphisms of $F(\alpha_1, \alpha_2)$ that fix F. Once you have done this, you should be able to do the general case.

Solution. Since K is finite over F, we can assume $K = F(\alpha_1, \ldots, \alpha_n)$. We may further assume that no α_{i+1} belongs to $F(\alpha_1, \ldots, \alpha_i)$. We induct on i to show that the number of field homomorphisms from $F(\alpha_1, \ldots, \alpha_i)$ to K fixing F is less than or equal to $[F(\alpha_1, \ldots, \alpha_i) : F]$. The case $i = 1$ is clear, for if $f(x)$ denotes the minimal polynomial of α_1 over F, and $\phi : F(\alpha_1) \to K$ is a homomorphism fixing F, then $\phi(\alpha_1)$ must be a root of $f(x)$. Since there are at most $\deg(f(x)) = [F(\alpha_1) : F]$ roots of $f(x)$ in K, this gives what we want.

Now suppose $i > 1$ and there are s field homomorphisms from $E := F(\alpha_1, \ldots, \alpha_i)$ to K fixing F with $s \leq [F(\alpha_1, \ldots, \alpha_i) : F]$. Let $g(x)$ denote the minimal polynomial of α_{i+1} over E. Let $\phi : E \to K$ be a field homomorphism fixing F. Set $E' := \phi(E)$, so that ϕ is field isomorphism from E to E'. As in the Crucial Proposition, we let $g^{\phi}(x)$ denote the polynomial in $E'[x]$ obtained by applying ϕ to the coefficients of $g(x)$. Suppose $d := \deg(g(x))$ and $\sigma : E(\alpha_{i+1}) \to K$ is a field homomorphism extending ϕ. Then $\sigma(\alpha_{i+1})$ must be a root of $g^{\phi}(x)$ in K. Since there are at most d such roots, the number of field homomorphisms $\sigma : E(\alpha_{i+1}) \to K$ extending ϕ is less than or equal to $d = [E(\alpha_{i+1}) : E]$. Now, suppose $\tau : E(\alpha_{i+1}) \to K$ is a field homomorphism fixing F. Then $\tau_{|_E} : E \to K$ is a field homomorphism from E to K fixing F. In other words, any field homomorphism from $E(\alpha_{i+1}) \to K$ fixing F is the extension of a field homomorphism from E to K fixing F. Now, there are s field homomorphisms $\phi : E \to K$ and at most d extensions of each ϕ to $E(\alpha_{i+1})$, therefore there are at most

$$sd \leq [E : F] \cdot [E(\alpha_{i+1}) : E] = [F(\alpha_1, \ldots, \alpha_{i+1}) : F],$$

homomorphisms from $F(\alpha_1, \ldots, \alpha_{i+1})$ to K fixing F. Thus, by induction on i, when $i = n$, we have that the number of field homomorphisms from $K \to K$ fixing F is less than or equal to $[K : F]$, which completes the proof. □

6. Let $\gamma \in \mathbb{C}$ be a primitive 8th root of unity (e.g., $e^{\frac{2\pi i}{8}}$) and set $K := \mathbb{Q}(\gamma)$.
   (i) Find (with proof) the minimal polynomial of γ.
   (ii) Find $\mathrm{Gal}(K/\mathbb{Q})$.
   (iii) Write out a group table in terms of automorphisms for the Galois group you found in (ii).
   (iv) For $\alpha := \gamma + \gamma^2$, find the minimal polynomial $p(x)$ for α over $\mathbb{Q}$ and all of the roots of $p(x)$.

Solution. Since γ satisfies $x^8 - 1 = (x^4 - 1)(x^4 + 1)$, and does not satisfy $x^4 - 1$, γ satisfies $x^4 + 1$. To see that $x^4 + 1$ is irreducible over $\mathbb{Q}$, since it is a primitive polynomial, it suffices to show that $x^4 + 1$ is irreducible over $\mathbb{Z}$. $x^4 + 1$ clearly has no roots in $\mathbb{Z}$, so one has to show that there is not an equation of the form $x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d)$, with $a, b, c, d \in \mathbb{Z}$. This polynomial equation yields a system of four equations in the unknowns a, b, c, d:

$$\begin{aligned} a + c &= 0 \\ ac + b + d &= 0 \\ ad + bc &= 0 \\ bd &= 1 \end{aligned}$$

The last equation implies $b = d = 1$ or $b = d = -1$. Suppose $b = d = 1$. Then the first two equations give $a + c = 0$ and $ac = -2$. Since $a = -c$, the second equation becomes $c^2 = 2$, which has no solution over $\mathbb{Z}$. Similarly, if $b = d = -1$, the system has not solution, so that $x^4 + 1$ is irreducible over $\mathbb{Q}$. Thus, $x^4 + 1$ is the minimal polynomial of γ over $\mathbb{Q}$. It follows that $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$ and $1, \gamma, \gamma^2, \gamma^3$ is a basis for $\mathbb{Q}(\gamma)$ over $\mathbb{Q}$. This gives part(i).

For part (ii), $\gamma, \gamma^3, \gamma^5, \gamma^7$ are the four primitive 8th roots of unity. Since they satisfy $x^8 - 1$ and do not satisfy $x^4 - 1$, they must be the roots of $x^4 + 1$. Thus, by the Crucial Proposition, it follows that the non-trivial automorphisms of $\mathrm{Gal}(K/\mathbb{Q})$ take γ to the elements $\gamma^3, \gamma^5, \gamma^7$, respectively. If we call these automorphisms, σ, τ, δ, we have $\mathrm{Gal}(K/\mathbb{Q}) = \{id, \sigma, \tau, \delta\}$. $\sigma^2(\gamma) = \sigma(\gamma^3) = \gamma^9 = \gamma$, so $\sigma^2 = id$. Similarly, $\tau^2 = id = \delta^2$, so that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

For part (iii), $\sigma\tau(\gamma) = \sigma(\gamma^5) = \gamma^{51} = \gamma^7 = \delta(\gamma)$, so $\sigma\tau = \gamma$. Similarly, $\tau\delta = \sigma$ and $\sigma\delta = \tau$, and this together with the fact that $\mathrm{Gal}(K/\mathbb{Q})$ is abelian yields the following group table

$\cdot$	id	σ	τ	δ
id	id	σ	τ	δ
σ	σ	id	δ	τ
τ	τ	δ	id	σ
δ	δ	τ	σ	id

For part (iv), multiplying each basis element by α yields the following system of equations

$$\begin{aligned} \alpha \cdot 1 &= 0 \cdot 1 + 1 \cdot \gamma + 1 \cdot \gamma^2 + 0 \cdot \gamma^3 \\ \alpha \cdot \gamma &= 0 \cdot 1 + 0 \cdot \gamma + 1 \cdot \gamma^2 + 1 \cdot \gamma^3 \\ \alpha \cdot \gamma^2 &= -1 \cdot 1 + 0 \cdot \gamma + 0 \cdot \gamma^2 + 1 \cdot \gamma^3 \\ \alpha \cdot \gamma^3 &= -1 \cdot 1 + -1 \cdot \gamma + 0 \cdot \gamma^2 + 0 \cdot \gamma^3. \end{aligned}$$

We may rewrite this system of equation as a matrix equation

$$\begin{pmatrix} \alpha & -1 & -1 & 0 \\ 0 & \alpha & -1 & -1 \\ 1 & 0 & \alpha & -1 \\ 1 & 1 & 0 & \alpha \end{pmatrix} \cdot \begin{pmatrix} 1 \\ \gamma \\ \gamma^2 \\ \gamma^3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Since the corresponding system of equations has a non-trivial solution, the determinant of the coefficient matrix equals zero. This shows that α is a root of the polynomial $p(x) = x^4 + 2x^2 + 4x + 2$. By Eisenstein's criterion, $p(x)$ is irreducible over $\mathbb{Q}$, so that $p(x)$ is the minimal polynomial for α over $\mathbb{Q}$.

There are several ways to find the other roots of $p(x)$. Here is one way. If we apply the automorphisms in $\mathrm{Gal}(K/\mathbb{Q})$ to α, we will obtain the other roots of $p(x)$.

(i) $\sigma(\alpha) = \sigma(\gamma) + \sigma(\gamma)^2 = \gamma^3 + \gamma^6$.
(ii) $\tau(\alpha) = \tau(\gamma) + \tau(\gamma)^2 = \gamma^5 + \gamma^{10} = \gamma^2 + \gamma^5$.
(iii) $\delta(\alpha) = \delta(\gamma) + \delta(\gamma)^2 = \gamma^7 + \gamma^{14} = \gamma^6 + \gamma^7$.

Thus, the roots of $p(x)$ are $\gamma, \gamma^3 + \gamma^6, \gamma^2 + \gamma^5, \gamma^6 + \gamma^7$.

7. Construct a field K with 125 elements and exhibit explicitly the automorphism group of K.

Solution. Here are two solutions to this problem. The first solution answers this question directly, while the second solution can easily be generalized to show that for any prime p and $n \geq 1$, there exists a field with p^n elements whose automorphism group is isomorphic to $\mathbb{Z}_n$.

For the first solution, consider $p(x) = x^3 + x + 1 \in \mathbb{Z}_5[x]$. It is easy to see that $p(x)$ does not have a root in the field $\mathbb{Z}_5$, so that $p(x)$ is irreducible over $\mathbb{Z}_5$. Let α be a root of $p(x)$ and set $K := \mathbb{Z}_5(\alpha)$. Since $[K : \mathbb{Z}_5] = 3$, K has 125 elements. Now consider the Frobenius map $\sigma : K \to K$ given by $\sigma(a) = a^p$, for all $a \in K$. This is a 1-1 field homomorphism, and since K is finite, it must be onto, and hence σ is an automorphism of K. Any such automorphism fixes $\mathbb{Z}_5$, so $\sigma \in \mathrm{Gal}(K/\mathbb{Z}_5)$. Now, $\sigma^2(\alpha) = \alpha^{25}$. If $\sigma^2 = id$, then $\alpha^{25} = \alpha$ in K. Thus, in the multiplicative group K^*, $\alpha^{24} = 1$. But $|K^*| = 124$, and 24 does not divides 124, so we cannot have $\alpha^{25} = \alpha$, i.e., $\sigma^2 \neq id$. On the other hand, $\sigma^3(\alpha) = \alpha^{125}$. In K^*, $\alpha^{124} = 1$, so $\alpha^{125} = \alpha$, which shows that $\sigma^3 = id$. Thus,

$$3 = |\{id, \sigma, \sigma^2\}| \leq |\mathrm{Gal}(K/\mathbb{Z}_5)| \leq [K : \mathbb{Z}_5] = 3,$$

showing that $\langle \sigma \rangle = \mathrm{Gal}(K/\mathbb{Z}_5) \cong \mathbb{Z}_3$.

For the second solution, consider the splitting field K of $f(x) = x^{5^3} - x$ over $\mathbb{Z}_5$[2]. Since $f'(x) = -1 \not\equiv 0$ modulo 5, the GCD $f(x)$ and $f'(x)$ equals 1, so by the lecture of April 3, $f(x)$ has 125 distinct roots in K.

[2] In the general case, one takes K to be the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$. As in this special case, the Frobenius automorphism generates the automorphism group of K, which will be isomorphic to $\mathbb{Z}_n$. The proof is exactly the same as the present case.

Let $a, b \in K$ be roots of $f(x)$. Then $f(a+b) = (a+b)^{125} - (a+b) = a^{125} - b^{125} - a - b = a + b - a - b = 0$ in K. Similarly, $f(ab) = (ab)^{125} - ab = a^{125}b^{125} - ab = ab - ab = 0$. Suppose $a \neq 0$. Then,

$$0 = f(1) = f(aa^{-1}) = (aa^{-1})^{125} - aa^{-1} = a^{125}(a^{-1})^{125} - aa^{-1} = a(a^{-1})^{125} - aa^{-1} = a \cdot \{(a^{-1})^{125} - a^{-1}\}.$$

Since $a \neq 0$, $(a^{-1})^{125} - a^{-1} = 0$, and we have that $a+b, ab, a^{-1}$ are roots of $f(x)$. Note also that the elements of $\mathbb{Z}_5$ are roots of $f(x)$. Thus, the 125 roots of $f(x)$ form a subfield of K containing $\mathbb{Z}_5$, and must equal K, since K is obtained by adjoining the roots of $f(x)$ to $\mathbb{Z}_5$. In other words, the splitting field of $x^{125} - x$ over $\mathbb{Z}_5$ is a field with 125 elements.

Now, since $|K| = 125$, $[K : \mathbb{Z}_5] = 3$. Consider $\sigma : K \to K$ given by $\sigma(a) = a^5$, for all $a \in K$. Since $(a+b)^5 = a^5 + b^5$ and $(ab)^5 = ab$ in K, σ is a field homomorphism, and is clearly 1-1. Since K is finite, σ is an automorphism. Now, by the Primitive element Theorem, $K = \mathbb{Z}_5(c)$, for some $c \in K$. Suppose $\sigma^2 = id$. Then $c = \sigma^2(c) = (c^5)^5 = c^{25}$. Similarly $(c^2)^{25} = c^2$. Since every element t of $\mathbb{Z}_5$ satisfies $t^5 = t$, it follows that every element $a \in K$ satisfies $a^{25} = a$, since $a = u + vc + wc^2$, for some $u, v, w \in \mathbb{Z}_5$. But then $x^{25} - x$ has 125 roots, which is a contradiction. Thus, $\sigma^2 \neq id$. Now, suppose $a \in K$, Then $\sigma^3(a) = a^{5^3} = a^{125} = a$. Thus, $\sigma^3 = id$. Thus, id, σ, σ^2 are three distinct automorphisms of K and belong to $\text{Gal}(K/\mathbb{Z}_5)$. Since the order of the Galois group is less than or equal to the degree of the extension, we have $|\text{Gal}(K/\mathbb{Z}_5)| = 3$. Since any automorphism of K fixes $\mathbb{Z}_5$, $\langle\sigma\rangle \cong \mathbb{Z}_3$ is the automorphism group of K. □

8. Let p be a prime. Prove that for all $n \geq 1$, there exists an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$.

Solution. The same argument (though more general) given in the previous problem, shows that if K is the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$, then K is a field with p^n elements. Thus, $[K : \mathbb{Z}_p] = n$. Let $a \in K$ be a primitive element for K over $\mathbb{Z}_p$. Then the minimal polynomial for a over $\mathbb{Z}_p$ is irreducible and has degree n. □

9. Let $\alpha := \sqrt{2+\sqrt{2}}$. Show that $\mathbb{Q}(\alpha)$ is a Galois extension of $\mathbb{Q}$ and $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}_4$. Find all intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$.

Solution. Set $\beta := \sqrt{2-\sqrt{2}}$. Then it is easy to check that $p(x) = x^4 - 4x^2 + 2$ is the minimal polynomial for α over $\mathbb{Q}$ and that the roots of $p(x)$ are $\pm\alpha$ and $\pm\beta$. Moreover, $\frac{\sqrt{2}}{\alpha} = \beta$ showing that $\pm\beta \in \mathbb{Q}(\alpha)$. Thus, $\mathbb{Q}(\alpha)$ is the splitting field of $p(x)$ over $\mathbb{Q}$, and is therefore Galois over $\mathbb{Q}$.

Define $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ by $\sigma(\alpha) = \beta$, which we can do by the Crucial Proposition of April 12. Since $\alpha^2 - 1 = \sqrt{2}$, $\sigma(\sqrt{2}) = \beta^2 - 2 = -\sqrt{2}$. Thus, $\sigma(\beta) = \frac{\sigma(\sqrt{2})}{\sigma(\alpha)} = \frac{-\sqrt{2}}{\beta} = -\alpha$, and therefore $\sigma^2(\alpha) = -\alpha$. Similarly, we have $\sigma^3(\alpha) = -\beta$, and $\sigma^4(\alpha) = \alpha$, showing that $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}_4$, since we have $|\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = 4$.

Finally, since $\langle\sigma^2\rangle$ is the only proper subgroup of $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$, $\mathbb{Q}(\alpha)^{\sigma^2}$ is the only intermediate field. Since $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma^2(\sqrt{2}) = \sqrt{2}$. It follows that $\mathbb{Q}(\sqrt{2})$ is the only intermediate field. □

10. For $n \geq 1$, consider the complex number $\epsilon := e^{\frac{2\pi i}{n}}$, a primitive nth root of unity.

(i) Show that $\mathbb{Q}(\epsilon)$ is a splitting field for $x^n - 1$ over $\mathbb{Q}$.

(ii) By definition, $\gamma \in \mathbb{C}$ is a primitive nth root of unity if and only if $\gamma^n = 1$ and $\gamma^r \neq 1$ for $r < n$. Prove that: ϵ^i is a primitive nth root of unity if and only if i and n are relatively prime if and only if $\langle\epsilon^i\rangle = \langle\epsilon\rangle$ and that this accounts for all primitive nth roots of unity. Conclude that there are $\phi(n)$ primitive nth roots of unity.

(iii) Let $\{\epsilon, \epsilon^{i_2}, \dots, \epsilon^{i_{\phi(n)}}\}$ be the primitive nth roots of unity and set $\Phi_n(x) := (x-\epsilon)(x-\epsilon^{i_1})\cdots(x-\epsilon^{i_{\phi(n}})$, the nth *cyclotomic polynomial.* Prove that $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

(iv) Use induction on n to show that $\Phi_n(x) \in \mathbb{Z}[x]$.

(v) Calculate $\Phi_{12}(x)$.

(vi) A standard fact is $\Phi_n(x)$ is irreducible over $\mathbb{Z}$, equivalently, over $\mathbb{Q}$. Use this fact to prove that $\text{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q}) \cong (\mathbb{Z}_n)^*$, the multiplicative group of units in the ring $\mathbb{Z}_n$.

Solution. For (i), $1, \epsilon, \dots, \epsilon^{n-1}$ are n distinct complex numbers and they all are roots of unity, i.e., roots of $x^n - 1$. If we adjoin these to $\mathbb{Q}$, we simply get $\mathbb{Q}(\epsilon)$, so that $\mathbb{Q}(\epsilon)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$.

For (ii), note that $C := \{1, \epsilon, \dots, \epsilon^{n-1}\}$ is a cyclic group of order n generated by ϵ, thus, $o(\epsilon^i) = n$ if and only if $\langle \epsilon^i \rangle = C$ if and only if i is less than n and relatively prime to n. This accounts for all primitive nth roots of unity, since such a complex number is a root of $x^n - 1$, and hence ϵ^j, for some $0 \leq j \leq n-1$.

For (iii), we note that if C is a cyclic group of order n, then $n = \Sigma_{d|n}\phi(d)$, since every element in C has order d for $d \mid n$, and there are $\phi(d)$ elements of order d - since a cyclic group of order n has a unique subgroup of order d for each $d \mid n$. Thus, taking C as above, we can write C as a disjoint union of sets C_d, with $d \mid n$, where C_d are the elements of C having order d. But then, C_d is just the set of primitive dth roots of unity. It follows that $\Phi_d(x) = \prod_{\alpha \in C_d}(X - \alpha)$and hence $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

For (iv), we clearly have $\Phi_1(x) = (x-1)$ and $\Phi_2(x) = x+1$ are in $\mathbb{Z}[x]$. For $n \geq 2$, we have, by induction on n, $\Phi_d(x) \in \mathbb{Z}[x]$, for $d \mid n$ and $d < n$. Thus, we have $x^n - 1 = f(x)\Phi_n(x)$, with $x^n - 1$ and $f(x)$ in $\mathbb{Z}[x]$. For ease of notation, set $t := \phi(n)$, the degree of $\Phi_n(x)$, and set $\Phi_n(x) = x^t + c_{t-1}x^{t-1} + \cdots c_1x + c_0$. Write $f(x) = x^{n-1} + f_{n-t-1}x^{n-t-1} + \cdots + f_1x + f_0$. We show (reverse) inductively the each $c_j \in \mathbb{Z}$, by comparing the coefficients in both sides of the equation $x^n - 1 = \Phi_n(x)f(x)$. In degree $n-1$, we have $0x^{n-1} = (c_{t-1} \cdot 1 + f_{n-t-1} \cdot 1)x^{n-1}$. Since $f_{n-t-1} \in \mathbb{Z}$, $c_{t-1} \in \mathbb{Z}$. In degree $n-2$, we have $0x^{n-2} = (c_{t-2} \cdot 1 + c_{t-1}f_{n-1} + f_{n-2} \cdot 1)x^{n-2}$. Since $c_{t-1}f_{n-1} + f_{n-2} \in \mathbb{Z}$, we have $c_{t-2} \in \mathbb{Z}$. Continuing in this way, we have that each $c_j \in \mathbb{Z}$, so $\Phi_n(x) \in \mathbb{Z}[x]$.

Alternately when we use the high school algorithm to divide $f(x)$ into $x^n - 1$, each step requires multiplying the leading term of $f(x)$, which is x^{n-1}, with a previously determined integer times an appropriate power of x. This integer then becomes a coefficient in the quotient, i.e., $\Phi_n(x)$. In other words, since the leading coefficient of $f(x)$ is 1 and the coefficients of $x^n - 1$ are in $\mathbb{Z}$, all of the arithmetic in the calculation takes place in $\mathbb{Z}$, so $\Phi_n(x)$ has coefficients in $\mathbb{Z}$.

For (v), we calculate each $\Phi_d(x)$, for $d < 12$ and $d \mid 12$. It's easy to see that $\Phi_1(x) = x - 1, \Phi_2(x) = x + 1, \Phi_3(x) = x^2 + x + 1$ and $\phi_4 = x^2 + 1$. To Calculate $\Phi_6(x)$, we note that this is an irreducible factor of $x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x^3 - 1)(x + 1)(x^2 - x + 1)$, we we have $\Phi_6(x) = x^2 - x + 1$. Thus,

$$x^{12} - 1 = (x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)\Phi_{12}(x) = (x^8 - x^6 - x^2 - 1)\Phi_{12}(x).$$

Dividing $x^{12} - 1$ by $x^8 + x^6 - x^2 - 1$ gives $\Phi_{12}(x) = x^4 - x^2 + 1$.

For (vi), since $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ and each primitive nth root of unity is a root of $\Phi_n(x)$, by the Crucial Proposition, for each primitive nth root of unity ϵ^i, there is a field isomorphism $\psi : \mathbb{Q}(\epsilon) \to \mathbb{Q}(\epsilon^i)$. Since $\mathbb{Q}(\epsilon^i) \subseteq \mathbb{Q}(\epsilon)$, and $[\mathbb{Q}(\epsilon) : \mathbb{Q}] = [\mathbb{Q}(\epsilon^i) : \mathbb{Q}]$, $\mathbb{Q}(\epsilon^i) = \mathbb{Q}(\epsilon)$, so $\psi \in \mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$. There $\phi(n)$ such automorphisms, so these automorphisms give $\mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$. We define $\phi : \mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q}) \to (\mathbb{Z}_n)^*$ as follows: Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$, and assume $\sigma(\epsilon) = \epsilon^i$, with $i < n$ and relatively prime to n. Define $\phi(\sigma) = i \in (\mathbb{Z}_n)^*$. Suppose $\tau \in \mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$ and $\tau(\epsilon) = \epsilon^j$, so that $\phi(\tau) = j$ in $(\mathbb{Z}_n)^*$. Then, $\sigma\tau(\epsilon) = \epsilon^{ij}$, so $\phi(\sigma\tau) = ij$ in $(\mathbb{Z}_n)^*$. Note ij as an integer might be greater than n, but it is relatively prime to n, so its image makes sense in $(\mathbb{Z}_n)^*$, since if $ij = nq + r$, with $0 \leq r < n$, $ij = r$ in $(\mathbb{Z}_n)^*$. On the other hand $\phi(\sigma)\phi(\tau) = ij$ in $(\mathbb{Z}_n)^*$, so ϕ is a group homomorphism. Suppose $\sigma \in \mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$ belongs to the kernel of ϕ. Then, if $\sigma(\epsilon) = e^i$, $i = 1$ in $(\mathbb{Z}_n)^*$. Since $1 \leq i < n$, this means $i = 1$, so $\sigma = id$ in $\mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$. Thus, ϕ is 1-1. Since $|\mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})| = \phi(n) = |(\mathbb{Z}_n)^*|$, ϕ is an isomorphism. □

Bonus Problems. Each bonus problem is worth 10 points. Bonus problems must be completely (or very close to completely) correct in order to receive any extra points.

1. Let p be a prime and x, y indeterminates over $\mathbb{Z}_p$. Set $F := \mathbb{Z}_p(x^p, y^p)$ and $K := \mathbb{Z}_p(x, y)$.
   (i) Show that $[K : F] = p^2$.
   (ii) Exhibit explicitly (with proof) infinitely many intermediate fields between F and K.
   (iii) Find the Galois group of K over F.

Solution. Part (i) is similar to the case for $p = 2$ that we did in class. We first note that $[F(x) : F] = p$. Clearly $x^p \in F$, so $[F(x) : F] \leq p$ and x is a root of $f(T) = T^p - x^p \in F[T]$. Over K, $f(T) = (T - x)^p$, so $f(T)$ has just one root in its splitting field. If $f(T)$ is the minimal polynomial for x over F, then $[F(x) : F] = p$. Suppose not. Then if $h(T) \in F[T]$ is the minimal polynomial for x over F, then $h(T)$ is irreducible over F and has degree $r < p$. Thus, $h'(T) \neq 0$, so the GCD of $h(T)$ and $h'(T)$ is 1. Thus, $h(T)$ has distinct roots in its splitting field. This is a contradiction, since $h(T)$ divides $f(T)$. Thus, $f(T)$ is irreducible over F, which gives what we want. Since $K = F(x)(y)$, a similar arguments shows that $g(T) = T^p - y^p$ is irreducible over $F(x)$, so $[K : F] = [F(x, y) : F] = p^2$, which is what we want.

For (ii), we first note that just as in the lecture of April 15, any $f \in K$ satisfies $f^p \in F$, so there cannot be a primitive element for the field extension $F \subseteq K$. We claim the fields $F(x + x^{p^n}y)$ are distinct, for $n \geq 1$. Suppose $E := F(x + x^{p^n}y) = F(x + x^{p^m}y)$, with $n \neq m$. Then $(x + x^{p^n}y) - (x + x^{p^m}y) = (x^{p^n} - x^{p^m})y \in E$. Since $x^{p^n} - x^{p^m} \in F$, we have $y \in E$. Thus, $x^{p^n}y \in E$, and hence $x \in E$. It follows that $K = E = F(x + x^{p^n}y)$, a contradiction. Thus, the fields $F(x + x^{p^n}y)$ are distinct, and hence there are infinitely many intermediate fields between F and K.

For (iii), if σ belongs to the Galois group, then $\sigma(x)$ must be a root of $T^p - x^p$, but this has only one root, so we must have $\sigma(x) = x$. Similarly, $\sigma(y) = y$, so the only automorphism of K fixing F is the identity automorphism. □

2. Let $F \subseteq K$ be fields with $K = F(\alpha)$. Assume $\alpha^n \in F$ and F contains a primitive nth root of unity. Prove that if $[K : F] = d$, then $\alpha^d \in F$ and $d \mid n$. Then show that $\mathrm{Gal}(K/F)$ is cyclic.

Solution. Let $\epsilon \in F$ be a primitive nth root of unity and suppose $\alpha^n = a \in F$. Let $p(x)$ denote the minimal polynomial of α over F. Then, $p(x)$ divides $x^n - a$, which equals $(x - \alpha)(x - \epsilon\alpha) \cdots (x - \epsilon^{n-1}\alpha)$. Thus, $p(x) = (x - \epsilon^{i_1}\alpha) \cdots (x - \epsilon^{i_d}\alpha)$, for some i_j. The constant term of $p(x)$ belongs to F on the one hand and equals $\epsilon^{i_1+\cdots+i_d}\alpha^d$ on the other hand. Since $\epsilon \in F$, $\alpha^d \in F$. It follows that d is the least positive integer such that $\alpha^d \in F$. To see this, write $n = qd + r$, with $0 \leq r < d$. Then $\alpha^n = (\alpha^d)^q + \alpha^r$. If $r \neq 0$, then $\alpha^r \in F$, a contradiction. Thus, $r = 0$ and $d \mid n$.

Suppose $\alpha^d = b \in F$. Then $p(x) = x^d - b$. Write $n = dc$, so that $\gamma := \epsilon^c \in F$ is a primitive dth root of unity, and the roots of $p(x)$ are $\alpha, \gamma\alpha, \gamma^2\alpha, \ldots, \gamma^{d-1}\alpha \in K$. This shows that K is the splitting field of $p(x)$ over F and the extension $F \subseteq K$ is a Galois extension. Define $\sigma : K \to K$ by $\sigma(\alpha) = \gamma\alpha$, which we can do by the Crucial Proposition. Then, $\sigma^2(\alpha) = \sigma(\gamma\alpha) = \gamma\sigma(\alpha) = \gamma^2\alpha$. Continuing, $\sigma^3(\alpha) = \gamma(\sigma^2(\alpha)) = \sigma(\gamma^2\alpha) = \gamma^2\sigma(\alpha) = \gamma^3\alpha$. Inductively, we have that $\sigma^i(\alpha) = \gamma^i\alpha$, for $1 \leq i \leq d - 1$. This gives $d - 1$ distinct non-identity elements in $\mathrm{Gal}(K/F)$, so it follows that $\langle\sigma\rangle = \mathrm{Gal}(K/F)$, since $|\mathrm{Gal}(K/F)| = d = [K : F]$. □