Solutions to Math 418 Final Exam — May 7, 2024

1. (25 points) Let $f(x) = x^3 + px + q \in \mathbb{Z}[x]$, where $p \equiv 2 \mod 6$ and $q \equiv 1 \mod 6$.

   (a) (10 points) Prove that $f(x)$ is irreducible.

   The reduction modulo 3 of f is $\overline{f} = x^3 + 2x + 1 \in \mathbb{F}_3[x]$. Since this is a cubic, it either has a root or is irreducible. But we can plug in 0, 1, and 2 to see that $\overline{f}(0) = \overline{f}(1) = \overline{f}(2) = 1 \neq 0$, so $\overline{f}$ and f are irreducible.

   (b) (15 points) Prove that the Galois group for f over $\mathbb{Q}$ is S_3. [Hint: consider the discriminant $D = -4p^3 - 27q^2$ of f taken modulo 8.]

   Since f is irreducible, its Galois group $\mathrm{Gal}(f)$ is a transitive subgroup of S_3, so $\mathrm{Gal}(f) = A_3$ or S_3. It equals the former if $\sqrt{D} \in \mathbb{Q}$, and the latter otherwise. By Gauss' Lemma, $\sqrt{D} \in \mathbb{Q}$ if and only if $\sqrt{D} \in \mathbb{Z}$.

   Consider the residue of D modulo 8. Since p is even, so is p^3, so $-4p^3$ is a multiple of 8. Since q is odd, we must have $q^2 \equiv 1 \mod 8$ (check the four cases), so $-27q^2 \equiv -3 \equiv 5 \mod 8$. However, 5 is not a square modulo 8, so $\sqrt{D} \notin \mathbb{Z}$, and therefore $\mathrm{Gal}(f) = S_3$.

2. (20 points) Let $I = (x^2, y^2 - x) \subseteq \mathbb{C}[x, y]$

   (a) (10 points) Use the affine Nullstellensatz to determine $I(V(I))$, where $V(I)$ denotes the affine variety corresponding to I.

   Clearly, $I \subsetneq \mathbb{C}[x, y]$ since I contains no nonzero constants. By the affine Nullstellensatz, $I(V(I)) = \sqrt{I}$, so we only need to compute $\sqrt{I}$. We have $x^2 \in I$, so $x \in \sqrt{I}$. Since we also have $y^2 - x \in \sqrt{I}$, $y^2 = y^2 - x + x \in \sqrt{I}$, and since $\sqrt{I}$ is a radical ideal, $y \in \sqrt{I}$ (or just notice directly that $y^4 = x^2 + (x + y^2)(y^2 - x) \in I$).

   Now we have $(x, y) \subseteq \sqrt{I}$, and since (x, y) is a maximal ideal, it is radical, so $I(V(I)) = \sqrt{I} = (x, y)$.

   (b) (10 points) Prove (rigorously) that I is not a homogeneous ideal, but that $I(V(I))$ is a homogeneous ideal.

   By part a, $I(V(I)) = (x, y)$, and since the generators are homogeneous, so is the ideal.

   On the other hand, we show that I is not homogeneous by showing that $x \in I$, since homogeneous ideals contain the homogeneous components of their generators. Suppose we have a linear combination $h = fx^2 + g(y^2 - x)$, $f, g \in \mathbb{C}[x, y]$. Every term in fx^2 is a multiple of x^2, so the coefficient of y^2 in h is the constant term c of g and the coefficient of x in h is $-c$. If $h = x$, then we would have both $c = 0$ and $c = -1$, which is a contradiction. Therefore, $x \notin I$ and so I is not a homogeneous ideal.

3. (40 points) Let $K = \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$ be the splitting field of $x^5 - 2$ over $\mathbb{Q}$, and let $G = \mathrm{Gal}(K/\mathbb{Q})$.

   (a) (5 points) Determine the degree $[K : \mathbb{Q}]$.

   We have $K = \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$, and because the degrees $[\mathbb{Q}(\sqrt[5]{2} : \mathbb{Q}] = 5$ and $[\mathbb{Q}(\zeta_5 : \mathbb{Q}] = 4$ are coprime, we have $5 | [K : \mathbb{Q}]$, $4 | [K : \mathbb{Q}]$, and $[K : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[5]{2} : \mathbb{Q}][\mathbb{Q}(\zeta_5 : \mathbb{Q}] = 20$, so $[K : \mathbb{Q}] = 20$.

   (b) (15 points) Determine G up to isomorphism using generators and relations. (i.e. find a set of generators for G, determine their orders and any other relations needed to determine the group)

   Let σ, τ be the automorphisms $\sigma(\sqrt[5]{2}) = \zeta_5 \sqrt[5]{2}, \sigma(\zeta_5) = \zeta_5, \tau(\sqrt[5]{2}) = \sqrt[5]{2}, \tau(\zeta_5) = \zeta_5^2$. Notice that τ has order 4, since $\tau^2(\zeta_5) = \zeta_5^4 \neq \zeta_5$, and additionally, σ has order 5. Therefore, $G = \langle \sigma, \tau \rangle$. We have the orders of both generators, and so we just need their commutation relation since then every element of G will have a unique expression $\sigma^a \tau^b, 0 \leq a < 5, 0 \leq b < 4$. We have $\tau\sigma(\sqrt[5]{2}) =$

$\tau(\zeta_5 \sqrt[5]{2}) = \zeta_5^2 \sqrt[5]{2}$, and $\tau\sigma(\zeta_5) = \tau(\zeta_5) = \zeta_5^2$. On the other hand, $\sigma^a\tau(\sqrt[5]{2}) = \sigma^a(\sqrt[5]{2}) = \zeta_5^a \sqrt[5]{2}$, and $\sigma^a\tau(\zeta_5) = \sigma^a(\zeta_5^2) = \zeta_5^2$. Matching these outputs, $\tau\sigma = \sigma^2\tau$, so

$$G = \langle \sigma, \tau | \sigma^5 = \tau^4 = 1, \tau\sigma = \sigma^2\tau \rangle.$$

(c) (10 points) Determine the subgroup of G fixing the intermediate field $E = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$, and **use this subgroup** to determine whether E is Galois over $\mathbb{Q}$. (You *must* use the Fundamental Theorem of Galois Theory for this problem).

$[E : \mathbb{Q}] = 2$ since $\zeta_5 + \zeta_5^{-1}$ is a root of the polynomial $x^2 + x + 1 \in \mathbb{Q}[x]$, so $[E : \mathbb{Q}] = 2$. By the Tower Law, $[K : E] = 10$, so $H := \text{Gal}(K/E)$ must have order 10 / index 2 in G. Now, $\sigma(\zeta_5 + \zeta_5^{-1}) = \zeta_5 + \zeta_5^{-1}$, and $\tau(\zeta_5 + \zeta_5^{-1}) = \zeta_5^2 + \zeta_5$, $\tau^2(\zeta_5 + \zeta_5^{-1}) = \zeta_5^{-1} + \zeta_5$. Therefore, $H = \langle \sigma, \tau^2 \rangle$. We claim that H is normal in G, and, consequently, that E is Galois over H. This is apparent since H is index 2 in G and all index-2 subgroups are normal. Alternatively, we can show it directly. Using the relation $\tau\sigma = \sigma^2\tau$, we have $\tau\sigma\tau^{-1} = \sigma^2 \in H$, $\sigma\sigma\sigma^{-1} = \sigma \in H$, $\tau\tau^2\tau^{-1} = \tau \in H$, and $\sigma\tau^2\sigma^{-1} = \tau^2\sigma^3 \in H$. (The last equality follows since $\sigma\tau^2 = \sigma^6\tau^2 = \tau\sigma^3\tau = \tau\sigma^8\tau = \tau^2\sigma^4$).

(d) (10 points) Determine the subgroup of G fixing the intermediate field $F = \mathbb{Q}(\sqrt[5]{2}, \zeta_5 + \zeta_5^{-1})$, and **use this subgroup** to determine whether F is Galois over $\mathbb{Q}$. (You *must* use the Fundamental Theorem of Galois Theory for this problem).

By the Tower Law, $[F : \mathbb{Q}] = [F : E][E : \mathbb{Q}] = 2 \cdot 5 = 10$ since $\zeta_5 + \zeta_5^{-1} \notin \mathbb{Q}(\sqrt[5]{2})$. (Alternatively, we can note that $[K : F] = 2$ since ζ_5 is a root of the polynomial $x^2 - (\zeta_5 + \zeta_5^{-1})x + 1$). This means that $J := \text{Gal}(K/F)$ has order 2. Since $\tau^2(\sqrt[5]{2}) = \sqrt[5]{2}$, $\tau^2(\zeta_5 + \zeta_5^{-1}) = \tau(\zeta_5^2 + \zeta_5^3) = \zeta_5^{-1} + \zeta_5$, we have $J = \langle \tau^2 \rangle$.
Now, $\sigma\tau^2\sigma^{-1} = \sigma^{16}\tau^2\sigma^{-1} = \tau^2\sigma^3 \notin \langle \tau^2 \rangle$, so $\langle \tau^2 \rangle$ is not normal in G, and therefore F is not Galois over $\mathbb{Q}$.

4. (20 points) Please complete **TWO** of the following problems, some of which are on the following page. If you have work on more than two problems, **you must CLEARLY specify which two problems you would like graded**; otherwise, the first two will be graded

I would like the following two parts of this problem graded: __________________________

(a) (10 points) Prove that every $\alpha \in \mathbb{F}_{p^n} \setminus \mathbb{F}_p$ satisfies the equation

$$\alpha^{p^n-3} + \alpha^{p^n-4} + \cdots + \alpha + 1 = -\alpha^{-1}.$$

Since $\alpha \in \mathbb{F}_{p^n}$, which is the splitting field of $x^{p^n} - x$ (see Dummit and Foote, p.549-550), α is a root of that polynomial. Since $\alpha \notin \mathbb{F}_p$, $\alpha \neq 0, 1$, so we can divide by $x(x-1)$, and thus α is a root of $x^{p^n-2} + x^{p^n-3} + \cdots + x + 1$. Plugging in α, moving the 1 to the other side, and dividing by α gives the result.

(b) (10 points) Let $f(x) = x^3 + 2x + 2 \in \mathbb{Q}[x]$ (you may take for granted that f is irreducible). Let θ be a root of $f(x)$ in some extension field. Determine $(1 + \theta)^{-1}$ in $\mathbb{Q}(\theta)$ as a polynomial in θ.

We have $\theta^3 + 2\theta + 2 = 0$, so if $(1+\theta)^{-1} = a\theta^2 + b\theta + c$, then

$$\begin{aligned} 1 &= (1+\theta)(a\theta^2 + b\theta + c) \\ &= a\theta^3 + (a+b)\theta^2 + (b+c)\theta + c \\ &= a(-2\theta - 2) + (a+b)\theta^2 + (b+c)\theta + c \\ &= (a+b)\theta^2 + (-2a+b+c)\theta + c - 2a. \end{aligned}$$

Since $1, \theta, \theta^2$ form a basis for $\mathbb{Q}(\theta)/\mathbb{Q}$, we must have $a+b=0, -2a+b+c=0, c-2a=1$, and this yields $a=1, b=-1, c=3$, so $(1+\theta)^{-1} = \theta^2 - \theta + 3$.

(c) (10 points) Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ be irreducible. Prove that the affine variety $V((f))$ is irreducible.

First note that $\mathbb{C}[x_1, \ldots, x_n]$ is a UFD since $\mathbb{C}$ is a UFD and a ring R is a UFD if and only if $R[x]$ is a UFD. An element r in a UFD is irreducible if and only if it is prime, and an element r in an integral domain is prime if and only if (r) is a prime ideal. Combining these facts, (f) is a prime ideal. Therefore, $V((f))$ is an irreducible variety by a proposition proved in lecture 37.

(d) (10 points) Let R be a Euclidean domain, with norm $N : R \to \mathbb{Z}_{\geq 0}$. Let m be the minimum integer in the set of norms of nonzero elements of R i.e.

$$m = \min\{N(a) | a \in R \setminus \{0\}\}.$$

Prove that every nonzero element of R of norm m is a unit.

Let $a \in R \setminus \{0\}$ such that $N(a) = m$. Since R is a Euclidean domain, there exist $q, r \in R$ such that $1 = qa + r$ and either $r = 0$ or $N(r) < N(a)$. Since no nonzero element of r has norm less than $N(a)$, $r = 0$, so $1 = qa$, and so a is a unit.