Zhengdong Zhang
Email: zhengz@uoregon.edu
Course: MATH 649 - Abstract Algebra
Instructor: Professor Sasha Polishchuk

Final Exam - Week 11
ID: 952091294
Term: Spring 2025
Due Date: 10^{th} June, 2025

Problem 1
Prove that the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2+\sqrt{2}})$ is Galois and compute its Galois group.

Solution: Let $a = \sqrt{2+\sqrt{2}}$ and $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$. Consider the polynomial

$$f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x].$$

Use the prime number 2 and by Eisenstein's Criterion, f is irreducible in $\mathbb{Q}[x]$. By direct computation, we have $f(a) = 0$. This means f is the minimal polynomial of a over $\mathbb{Q}$. Factoring f in $\mathbb{C}[x]$, and we obtain

$$\begin{aligned} f(x) &= x^4 - 4x^2 + 2 \\ &= (x^2-2)^2 - 2 \\ &= (x^2 - a^2)(x^2 - \frac{2}{a^2}) \\ &= (x-a)(x+a)(x - \frac{\sqrt{2}}{a})(x + \frac{\sqrt{2}}{a}) \end{aligned}$$

Note that $\sqrt{2} = a^2 - 2 \in K$. All four roots of f are in K. This implies K is the splitting field of f and we know that every finite extension over a characteristic 0 field is sepaprable, so $\mathbb{Q} \subset K$ is a Galois extension. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ be the Galois group. We have

$$|G| = [K : \mathbb{Q}] = \deg f = 4.$$

Since $K/\mathbb{Q}$ is a finite normal extension and f is irreducible over $\mathbb{Q}$, there exists $\sigma \in G$ such that $\sigma(a) = \frac{\sqrt{2}}{a}$ by transitivity of Galois action. Then

$$2 - \sqrt{2} = \frac{2}{a^2} = (\sigma(a))^2 = \sigma(a^2) = \sigma(2+\sqrt{2}) = 2 + \sigma(\sqrt{2}).$$

because σ fix elements in $\mathbb{Q}$. So

$$\sigma(\frac{\sqrt{2}}{a}) = \frac{\sigma(\sqrt{2})}{\sigma(a)} = \frac{-\sqrt{2}}{\frac{\sqrt{2}}{a}} = -a.$$

This implies $\sigma^2(a) \neq a$. So σ does not have order 2 in G, then σ must have order 4 because $|G| = 4$. Thus, σ generates G and we can see that $G \cong C_4$.

Problem 2

Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial. Assume f has both real and non-real roots. Prove that the Galois group of f is non-ableian.

Solution: Let K be the splitting field of f. Q has characteristic 0, so $K/\mathbb{Q}$ is a Galois extension. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ be the Galois group. Let $z \in \mathbb{C}$ be a complex root of f and $a \in \mathbb{R}$ be a real root of f. Note that $\bar{z}$ is also a root of f because

$$0 = \overline{f(z)} = \bar{f}(\bar{z}) = f(\bar{z})$$

and $f \in \mathbb{Q}[x]$ implies that $f = \bar{f}$. Consider a field automorphism $\sigma \in G$ by sending all roots of f to its complex conjugate. We know f has complex roots, so σ is not the identity element. We have

$$\sigma(z) = \bar{z}, \quad \sigma(a) = a, \quad \sigma(\bar{z}) = z.$$

Since f is irreducible over $\mathbb{Q}$, there exists $g \in G$ such that $g(a) = z$ by transitivity of Galois action. Then we have

$$g\sigma(a) = g(a) = z,$$
$$\sigma g(a) = \sigma(z) = \bar{z}.$$

This implies $\sigma g \neq g\sigma$. So G is not an abelian group.

Problem 3

Let R be a commutative Noetherian local ring with maximal ideal M which satisfies $M^2 = M$. Prove that R is a field. Show that this is false if R is not required to be Noetherian.

Solution: R is a Noetherian local ring, so the unique maximal ideal M is a finitely generated R-module, and $M = J(R)$ the Jacobson ideal of R. $M^2 = M$ is equivalent to $J(R)M = M$, by Nakayama's lemma, $M = 0$. This implies $R \cong R/(0)$ is a field.

Next, consider the following ring

$$R = \mathbb{Q}[x, x^{\frac{1}{2}}, x^{\frac{1}{3}}, \ldots, x^{\frac{1}{n}}, \ldots].$$

Here R is the rational field $\mathbb{Q}$ adjoining all the nth root of x for $n \geq 1$. Then R is not noetherian since it has an ascending chain of ideals

$$(x) \subsetneq (x, x^{\frac{1}{2}}) \subsetneq \cdots$$

Let m be the maximal ideal

$$(x, x^{\frac{1}{2}}, x^{\frac{1}{3}}, \ldots, x^{\frac{1}{n}}, \ldots).$$

Note that $m^2 = m$ because for any $k \geq 1$, we have

$$x^{\frac{1}{k}} = x^{\frac{1}{2k}} \cdot x^{\frac{1}{2k}}.$$

Consider the local ring R_m, it has a unique maximal ideal $M = mR_m$ satisfying

$$M^2 = (mR_m)^2 = m^2 R_m = mR_m = M.$$

Note that here R_m is not a field because $x \in R_m$ is not invertible.

Problem 4

(a) Let R be a unique factorization domain with 2 invertible, and let K be its field of fractions. For a non-unit $f \in R$ such that there are no repeated primes in the factorization of f, find the integral closure of R in $K(\sqrt{f})$.

(b) Prove that the ring $\mathbb{C}[x, y, z]/(x^2 + y^2 + z^2)$ is integrally closed.

Solution:

(a) Consider the polynomial $x^2 - f \in R[x]$. $x^2 - f$ is irreducible because f has no repeated primes. It can be easily seen that $x^2 - f$ is the minimal polynomial of $\sqrt{f}$, so the field $K(\sqrt{f})$ is isomorphic to $K[x]/(x^2 - f)$ and every element $a \in K(\sqrt{f})$ can be written as $a = m + n\sqrt{f}$ for some $m, n \in K$. Note that

$$(a - m)^2 = n^2 f.$$

So a is the root of the polynomial

$$p(x) = x^2 - 2mx + m^2 - n^2 f \in K[x].$$

If $n = 0$, then $a = m$ is integral over R if and only if $a = m \in R$.

Assume $n \neq 0$. In this case, $p(x)$ is irreducible over K because the two roots: $m + n\sqrt{f}$ and $m - n\sqrt{f}$ are not in K. Suppose a is integral over R, then there exists an irreducible monic polynomial $q(x) \in R[x] \subseteq K[x]$ such that $q(a) = 0$. This means $p(x)$ divides $q(x)$ in $K[x]$. Suppose $q(x) = h(x)p(x)$ in $K[x]$, by Gauss's lemma, $q(x)$ also has a factorization in $R[x]$ and because $q(x)$ is irreducible in $R[x]$, $h(x) = 1$. So the coefficients of $p(x)$ lies in R if a is integral over R. This implies $m \in R$ because 2 is invertible. So $n^2 f \in R$. Since $n \in K$, n can be written as $n = \frac{n_1}{n_2}$ where $n_1, n_2 \in R$ are non-units and have no common primes in the factorization. There exists $b \in R$ such that

$$bn_2^2 = fn_1^2.$$

Here f has no repeated primes, so n_2^2 must have some common primes with n_1^2. This contradicts our assumption n_1, n_2 have no common primes, so n_2 is a unit and $n \in R$. Thus, the integral closure of R in $K(\sqrt{f})$ is

$$R[\sqrt{f}] \cong R[x]/(x^2 - f).$$

(b) Let $R = \mathbb{C}[y, z]$ be a unique factorization domain. The field of fractions is $K = \mathbb{C}(y, z)$. Consider the non-unit $f = -(y^2 + z^2) \in R$. We have proved in (a) that the integral closure of R in $K(\sqrt{-(y^2+z^2)})$ is $R[x]/(x^2+y^2+z^2)$. This implies that

$$R[x]/(x^2+y^2+z^2) \cong \mathbb{C}[x,y,z]/(x^2+y^2+z^2)$$

is integrally closed.

Problem 5
Consider a quadratic extension $\mathbb{Z} \subset A := \mathbb{Z}[x]/(x^2+\alpha x+\beta)$, where $x^2+\alpha x+\beta$ is an irreducible polynomial in $\mathbb{Z}[x]$. Let $p \in \mathbb{Z}$ be a prime number. Assume $a \in A$ is such that $\mathrm{Nm}(a) = \pm p$, where $\mathrm{Nm}(a) = a \cdot \sigma(a)$ is the norm in the corresponding quadratic extension of $\mathbb{Q}$ (here σ is a nontrivial element of the Galois group). Let $(a) \subset A$ be the corresponding principal ideal.

(a) Prove that $(a) \cap \mathbb{Z} = (p)$.

(b) Prove that the ideal (a) is prime.

Solution:

(a) Obviously $(p) \subseteq \mathbb{Z}$ since p is a prime number. To show that $p \in (a)$, it is enough to prove that $\sigma(a) \in A$. Indeed, a can be written as $m + nT$ where $m, n \in \mathbb{Z}$ and T is a root of the plynomial $x^2+\alpha x+\beta$. We know that $T + \sigma(T) = -\alpha$, so

$$\sigma(m+nT) = m + n\sigma(T) = m + n(-\alpha - T) = m - n\alpha - nT \in A.$$

This implies that

$$\mathrm{Nm}(a) = a \cdot \sigma(a) = \pm p \in (a).$$

So we have $(p) \subseteq (a) \cap \mathbb{Z}$. Conversely, we know that $(a) \cap \mathbb{Z}$ is a proper ideal in $\mathbb{Z}$. Since $\mathbb{Z}$ is a PID, suppose $(a) \cap \mathbb{Z} = (b)$ for some $b \in \mathbb{Z}$. We have already proved $p \in (a)$. So $b|p$ and because p is prime, $b = p$. This proves that $(a) \cap \mathbb{Z} = (p)$.

(b) Let I be the principal ideal generated by the prime number p in A. Then

$$A/I \cong (\mathbb{Z}/p\mathbb{Z})[x]/(x^2+\alpha x+\beta).$$

Let T be one root of $x^2+\alpha x+\beta = 0$. Then every element in A/I can be written as $m + nT$ where $m, n \in \mathbb{Z}/p\mathbb{Z}$. This implies that

$$|A/I| = p^2$$

because $\mathbb{Z}/p\mathbb{Z}$ is a finite field with p elements. Note that we have proved in (a) that $p \in (a)$, thus $I \subsetneq (a)$. This is strict inclusion because if $I = (a)$. Then $\mathrm{Nm}(p) = p \cdot p = p^2$. A contradiction. So we know that

$$|A/(a)| < |A/I| = p^2.$$

Here the quotient ring $A/(a)$ has a additive group structure and can be viewed as an abelian subgroup of A/I, so $|A/(a)| = 1$ or $|A/(a)| = p$. We know that (a) is a proper ideal of A

(otherwise $(a) \cap \mathbb{Z} = \mathbb{Z}$), so $|A/(a)| = p$. The only possible ring with p elements is $\mathbb{Z}/p\mathbb{Z}$. In this case, $A/(a)$ is a domian, so (a) is a prime ideal.

Problem 6

Let $k = \mathbb{C}$. Describe the irreducible components of the following algebraic sets in $\mathbb{A}^3$.

(a) $V(y^2 - xz, x^4 - yz, z^2 - x^3y)$.

(b) $V(xz - y^2, z^3 - x^5)$.

Solution:

(a) Consider the following ring homomorphism

$$\begin{aligned} \phi : k[x, y, z] &\to k[t], \\ x &\mapsto t^3, \\ y &\mapsto t^5, \\ z &\mapsto t^7. \end{aligned}$$

Let $I \subseteq k[x, y, z]$ be the ideal

$$I = (y^2 - xz, x^4 - yz, z^2 - x^3y).$$

It is easy to check that three polynomials satisfy the relationship, so $I \subseteq \ker \phi$. Conversely, suppose $f \in \ker \phi$. f can be written as

$$f = f_1(y^2 - xz) + f_2(x^4 - yz) + f_3(z^2 - x^3y) + f_4$$

where $f_1, f_2, f_3, f_4 \in k[x, y, z]$. $f(t^3, t^5, t^7) = 0$ implies that $f_4(t^3, t^5, t^7) = 0$. Note that f_4 can be written as

$$f_4(x, y, z) = a_1(y, z)x + a_2(y, z)x^2 + a_3(y, z)x^3.$$

Here $a_i(y, z)$ has degree at most 2 and the only possible degree 2 term is cyz for some $c \in k$. Write

$$a_1(y, z)x = c_1yx + c_2zx + c_3yzx + c_4x.$$

Then $f_4(t^3, t^5, t^7) = 0$ implies that

$$c_1t^8 + c_2t^{12} + c_3t^{15} + c_4t^3 = 0.$$

So $c_1 = c_2 = c_3 = c_4 = 0$. A similar argument can show that $a_2 = a_3 = 0$. So $f_4 = 0$. This implies that $f \in I$. We can conclude that $I = \ker \phi$. Therefore, the coordinate ring $k[x, y, z]/I$ is isomorphic to a subring of $k[t]$, which is a domain. So I is prime and $V(I)$ is an irreducible algebraic set.

(b) Consider the ring homomorphism

$$\begin{aligned}\phi : k[x,y,z] &\to k[t],\\ x &\mapsto t^3,\\ y &\mapsto t^4,\\ z &\mapsto t^5.\end{aligned}$$

Let I be the ideal

$$I = (z^3 - x^5, xz - y^2).$$

It is easy to check that $I \subseteq \ker\phi$. Conversely, suppose $f \in \ker\phi$. f can be written as

$$f(x,y,z) = f_1(x^5 - z^3) + f_2(y^2 - xz) + f_3$$

where $f_1, f_2, f_3 \in k[x,y,z]$. $f \in \ker\phi$ implies that $f_3(t^3, t^4, t^5) = 0$. Note that f_3 can be written as

$$f_3(x,y,z) = g_1(x,z) + g_2(x,z)y.$$

This implies that $g_1(t^3, t^5) = g_2(t^3, t^5) = 0$. Note that here g_1, g_2 can only have finite degrees since $x^5 - z^3 = 0$. A similar argument as (a) implies that $g_1 = g_2 = 0$. So $f \in I$ and the coordinate ring $k[x,y,z]/I$ is isomorphic to a subring of $k[t]$, which is a domain. Thus, I is a prime ideal and $V(I)$ is an irreducible algebraic set.

Problem 7

Let $X \subset \mathbb{A}^n$ be a non-empty algebraic set (we work over an alegbraically closed field k).

(a) Prove that X is not connected in Zariski topology if and only if there exists two proper ideals I and J in $k[x_1, \ldots, x_n]$ such that $I + J = (1)$ and $I \cap J = I(X)$.

(b) Prove that X is connected if and only if for any $f \in k[X]$ such that $f^2 = f$, one has either $f = 0$ or $f = 1$.

Solution:

(a) Assume X is not connected in Zariski topology. Then there exists two non-empty closed subset $X_1, X_2 \subset X$ such that $X_1 \sqcup X_2 = X$. Take $I = I(X_1)$ and $J = I(X_2)$. They are proper ideals since both of them are non-empty. Then we have

$$V(I(X_1) + I(X_2)) = V(I(X_1)) \cap V(I(X_2)) = X_1 \cap X_2 = \varnothing = V(1)$$

because their disjoint union is equal to X. Similarly,

$$V(I(X_1) \cap I(X_2)) = V(I(X_1)) \cup V(I(X_2)) = X = V(I(X)).$$

By Nullstellensatz, this implies that $I + J = (1)$ and $I \cap J = I(X)$.

Conversely, assume there exists proper ideals $I, J \subset k[x_1, \ldots, x_n]$ such that $I + J = (1)$ and $I \cap J = I(X)$. Consider two closed subset of X: $X_1 = V(\sqrt{I})$ and $X_2 = V(\sqrt{J})$. Note that

$1 \in I + J \subseteq \sqrt{I} + \sqrt{J}$. Then we have

$$X_1 \cup X_2 = V(\sqrt{I}) \cup V(\sqrt{J}) = V(\sqrt{I \cap J}) = V(\sqrt{I(X)}) = X,$$
$$X_1 \cap X_2 = V(\sqrt{I}) \cap V(\sqrt{J}) = V(\sqrt{I} + \sqrt{J}) = V(1) = \varnothing.$$

This tells us that $X = X_1 \sqcup X_2$, so X is not connected.

(b) Assume X is connected and suppose there exists non-constant polynomial $f \in k[X]$ such that $f^2 = f$. Without loss of generality, we can assume f is irreducible. Consider the ring homomorphism

$$q : k[x_1, \dots, x_n] \to k[X].$$

Consider two ideals $I = (f)$ and $J = (1 - f)$ in $k[X]$. The preimage $q^{-1}(I)$ and $q^{-1}(J)$ are proper ideals of $k[x_1, \dots, x_n]$ because $f \neq 0$ and $f \neq 1$. Since q is surjective, choose $g \in k[x_1, \dots, x_n]$ such that $q(g) = f$. Then $g \in q^{-1}(I)$ and $1 - g \in q^{-1}(J)$. We have

$$q^{-1}(I) + q^{-1}(J) = (1) = k[x_1, \dots, x_n].$$

On the other hand,

$$q^{-1}(I) \cap q^{-1}(J) = q^{-1}(I \cap J) = q^{-1}((f(1-f))) = q^{-1}((0)) = I(X)$$

because $I(X)$ is the kernel of the map q. From what we proved in (a), we know that X is not connected.

Conversely, suppose X is not connected. Then there exists two proper ideals

$$I, J \subseteq k[x_1, \dots, x_n]$$

such that $I + J = (1)$ and $I \cap J = I(X)$. Choose $g \in I$ satisfying $g \notin I \cap J$ (This can be done because they are proper ideals). Then $1 - g \in J$. So $g(1-g) \in I \cap J = I(X)$. Consider the image $q(g) = f$ in $k[X]$. $f \neq 0$ in $k[X]$ because $g \notin I(X)$. $f \neq 1$ because I is a proper ideal of $k[x_1, \dots, x_n]$. And we have $f^2 = f$ since $g(1-g) \in I(X)$.