ABSTRACT ALGEBRA — FINAL EXAM

ARDEN RASMUSSEN

1. Problem

Basic Concepts: For each of the following concepts of abstract algebra provide a definition and and example. When instructed provide a counterexample.

(a). **Group.** A group is a set of elements G and an operation $\star$, expressed as $(G, \star)$, where

- $\star$ is associative.
- $\star$ has an identity in G, that is to say there is some $1 \in G$ such that $1 \star a = a \star 1 = a \forall a \in G$.
- Every element in G has an inverse with respect to $\star$, we can write this as $\forall a \in G \exists a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = 1$.
- Optionally $\star$ may be commutative.

$(\{0\}, +)$ is a group.

(b). **Ring.** A ring is a set of elements R, and a $+$ and $\cdot$ operators, expressed as $(R, +, \cdot)$, and

- $(R, +)$ is a commutative group.
- $\cdot$ is associative.
- $\cdot$ distributes over $+$.
- $\cdot$ may or may not be commutative.
- $\cdot$ may or may not have an identity.
- Elements of R may or may not have an inverse with respect to $\cdot$.

$\mathbb{C}$ is a ring.

(c). **Integral domain.** An integral domain, is a ring $(R, +, \cdot)$ where there are no zero divisors, where $a \neq 0 \in R$ is called a zero divisor if there is some $b \neq 0 \in R$ such that $a \cdot b = 0$.

$\mathbb{Q}$ is an integral domain, $\mathbb{C}'$ is not an integral domain

(d). **Euclidean domain.** A commutative ring with identity $(R, +, \cdot)$ that is an Integral domain, is called an Euclidean Domain if there exists a function

$$N : R \to \mathbb{N} \cup \{0\}$$

with respect to which R has division algorithm.

$\mathbb{R}[X]$ is a euclidean domain, $\mathbb{R}[X, Y]$ is not a euclidean domain.

(e). **PID.** Integral Domains in which every ideal is principal are called principal ideal domains (PID)

$\mathbb{Z}$ is a PID, $\mathbb{R}[X, Y]$ is not a PID.

(f). **UFD.** If $(R, +, \cdot)$ is a commutative integral domain with identity, in which every non-zero, non-unit

- has a factorization in terms of irreducible
- that factorization is unique up to permutations and associates

then $(R, +, \cdot)$ is a Unique Factorization Domain (UFD)

$\mathbb{R}[X]$ is a UFD, $\mathbb{Z}[i\sqrt{5}]$ is not a UFD.

(g). **Homomorphism.** A function $F : R \to S$ between two rings with identity is said to be a homomorphism if

- $F(r_1 + r_2) = F(r_1) + F(r_2)$.
- $F(r_1 \cdot r_2) = F(r_1) \cdot F(r_2)$.
- $F(1) = 1$.

$F : \mathbb{R}[X] \to \mathbb{R}$ given by $F : P(X) \to P(1)$ is a homomorphism. The function $F : \mathbb{Z}[i] \to \mathbb{Z}[2i]$ given by $F(a + bi) = a + 2bi$ is not a homomorphism.

(h). **Kernel and Image.** Given a homomorphism $F : R \to S$ then kernel and image are defined as the below.

$$\begin{aligned} \mathrm{Ker}\,(F) &= \{r \in R | F(r) = 0\} \subseteq R \\ \mathrm{Im}\,(F) &= \{s \in S | \exists r \in R, F(r) = s\} \subseteq S \end{aligned}$$

The kernel an image of the homomorphism $F : \mathbb{R}[X] \to \mathbb{R}$ given by $F : P(X) \to P(1)$ are

$$\mathrm{Ker}\,(F) = (1 - X) \quad \mathrm{Im}\,(F) = \mathbb{R}.$$

(i). **Isomorphism.** A homomorphism $F : R \to S$ is called an isomorphism if F is a bijection.

$F : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ given by $F(a + b\sqrt{2}) = a - b\sqrt{2}$ is an isomorphism.

(j). **Ideal.** In $(R, +, \cdot)$ commutative integral domain with identity, $I \subseteq R$ is an ideal if

- $i_1, i_2 \in I \to i_1 + i_2 \in I$
- $r \in R, i \in I \to ri \in I$

(5) over $\mathbb{Z}$ is an ideal.

(k). **Prime ideal.** P ideal is called prime if $ab \to a \in P$ or $b \in P$.

(3) over $\mathbb{Z}$, is a prime ideal. (6) over $\mathbb{Z}$, is not a prime ideal, as $3 \cdot 2 \in (6)$ but $3 \notin (6)$ and $2 \notin (6)$.

(l). **Maximal ideal.** An ideal is called maximal if it is not contained in any proper ideal.

$$I \subseteq \xcancel{J} \subseteq R \tag{1}$$

(X, Y) is maximal over $\mathbb{R}[X, Y]$. (X) is not maximal over $\mathbb{R}[X, Y]$ as $(X) \subseteq (X, Y)$.

(m). **Quotient ring.** Let R be a commutative ring with identity and an integral domain. Let I be an ideal of R. We define

- the relation $\equiv \pmod I$ by $a \equiv b \pmod I$ if and only if $a - b \in I$.
- the set $R/I = \{[a] | a \in R\}$.
- the operations $+, \cdot$ on R/I

$$[a] + [b] = [a + b] \text{ and } [a] \cdot [b] = [a \cdot b].$$

Then R/I is a quotient ring.

$\mathbb{Z}/(3)$ is a quotient ring.

(n). **Field.** A field, is a ring $(R, +, \cdot)$ where every element of R has a multiplicative inverse.

$\mathbb{Q}$ is a field, but $\mathbb{Z}$ is not.

(o). **Algebra over a field.** An algebra is a ring which also happens to be a vector space over some field of scalars.

$\mathbb{R}_{m\times n}$ is an algebra, over the field of $\mathbb{R}$ which act as the scalars.

(p). **Field extension.** Field extensions are given two fields $A \subseteq B$, B is an extension of A if they share the same operations?

$\mathbb{Q}(\sqrt{2})$ is an extension of $\mathbb{Q}$.

2. Problem

Classic constructions of Abstract Algebra — Universal Properties: Recall the construction of the field of quotients of a commutative integral domain R, Let $\equiv$ denote the equivalence relation on $R \times (R \setminus \{0\})$ given by

$$(a, b) \equiv (c, d) \longleftrightarrow \exists x, y \in R \setminus \{0\}, (ax, bx) = (cy, dy).$$

By the field of quotients of R we mean the set $\mathcal{Q}(R)$a of equivalence classes

$$\mathcal{Q}(X) = \{[(a, b)] | a, b \in R, b \neq 0\}$$

of $\equiv$ together with operations

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)] \text{ and } [(a, b)] \cdot [(c, d)] = [(ac, bd)].$$

On homework you proved that $\mathcal{Q}(R)$ indeed is a field. In this problem I as you to prove the following theorem about the field of quotients.

(a). Show that there is an injective homomorphism $i : R \to \mathcal{Q}(R)$.
Claim: $i : R \to \mathcal{Q}(R)$ defined by $i(r) = [(r, 1)]$ is an injective homomorphism.

Proof. To show that i is a homomorphism, we first show that it presevers addition, and multiplication. Consider some $a, b \in R$, then

$$i(a + b) = [(a + b, 1)] = [(a, 1)] + [(b, 1)] = i(a) + i(b).$$

Thus i preserves addition. Now we consider

$$i(a \cdot b) = [(a \cdot b, 1)] = [(a, 1)] \cdot [(b, 1)] = i(a) \cdot i(b)$$

Thus i preserves multiplication. Now we verify that $i(1) = 1$.

$$i(1) = [(1, 1)] = 1_{\mathcal{Q}(R)}.$$

Thus i also preserves identity, and so we can conclude that it is indeed a homomorphism.

Now we will show that it is injective. Assume that it is not injective, that is to say there exists some $a, b \in R$ with $i(a) = i(b)$. We express this as

$$[(a, 1)] = [(b, 1)].$$

From the definition of $\equiv$ this means that there exists some $x, y \in R \setminus \{0\}$ such that

$$(ax, x) = (by, y).$$

From this it is clear that $x = y$, and so subsequently we find $a = b$, but this is a contradiction of our assumption. Thus we can conclude that i is injective. □

(b). Suppose $\Gamma : R \to F$ is another injective homomorphism of R into a field F. Show that

$$\gamma : \mathcal{Q}(R) \to F \text{ defined by } \gamma([a, b]) = \Gamma(a) \cdot \Gamma(b)^{-1}$$

is a (well-defined) homomorphism.
Claim: $\gamma : \mathcal{Q}(R) \to F$ defined by $\gamma([(a, b)]) = \Gamma(a) \cdot \Gamma(b)^{-1}$ is a well-defined homomorphism.

Proof. First we show that γ is a homomorphism. To show this, we demonstrate the preservation of addition, multiplication, and unit. Consider some $[(a, b)], [(c, d)] \in \mathcal{Q}(R)$.

$$\gamma([(a, b)] + [(c, d)]) = \gamma([(ad + bc, bd)]) = \Gamma(ad + bc) \cdot \Gamma(bd)^{-1}$$

Then since Γ is a homomorphism, we can rewrite this to be

$$\begin{aligned}\Gamma(ad)\Gamma(bd)^{-1} + \Gamma(bc)\Gamma(bd)^{-1} &= \Gamma(a)\Gamma(b)^{-1}\Gamma(d)\Gamma(d)^{-1} + \Gamma(b)\Gamma(b)^{-1}\Gamma(c)\Gamma(d)^{-1} \\ &= \Gamma(a)\Gamma(b)^{-1} + \Gamma(c)\Gamma(d)^{-1} \\ &= \gamma([a, b]) + \gamma([c, d])\end{aligned}$$

Then to demonstrate the preservation of multiplication, consider

$$\gamma([(a, b)] \cdot [(c, d)]) = \gamma([(ac, bd)]) = \Gamma(ac)\Gamma(bd)^{-1}$$

Again by the homomorphic nature of Γ we can rewrite this to be

$$\Gamma(a)\Gamma(b)^{-1}\Gamma(c)\Gamma(d)^{-1} = \gamma([(a, b)]) \cdot \gamma([(c, d)]).$$

Finally we show that 1 is preserved.

$$\gamma([(1, 1)]) = \Gamma(1)\Gamma(1)^{-1} = 1$$

Thus it is clear that γ is a homomorphism.

Now we prove that γ is well defined. Consider $[(a, b)] = [(c, d)]$, with some $x, y \in R \setminus \{0\}$ such that $(ax, bx) = (cy, dy)$. We notice that

$$\gamma([(a, b)]) = \gamma([(ax, bx)]) \text{ and } \gamma([(c, d)]) = \gamma([(cy, dy)]).$$

Now we compute

$$\begin{aligned}\gamma([(a, b)]) = \gamma([(ax, bx)]) &= \Gamma(ax)\Gamma(bx)^{-1} \\ &= \Gamma(cy)\Gamma(dy)^{-1} = \gamma([(cy, dy)]) = \gamma([(c, d)])\end{aligned}$$

And thus γ is well defined. □

(c). Show that $\gamma \circ i = \Gamma$.

Proof. Consider our definition of γ and i, then we consider

$$\gamma \circ i = \gamma(i(r)) = \gamma([(r, 1)]) = \Gamma(r)\Gamma(1)^{-1}$$

Since Γ is a homomorphism, then $\Gamma(1) = 1$ and $\Gamma(1)^{-1} = 1^{-1} = 1$. So we find

$$\Gamma(r)\Gamma(1)^{-1} = \Gamma(r).$$

Thus it becomes clear that $\gamma \circ i = \Gamma$. □

3. Problem

Application ot Number Theory: Let p be a prime number and consider the field $\mathbb{Z}/(p)$ of integers modulo p.

(a). Show that for all $[k] \neq [0]$ the mapping

$$x \mapsto [k] \cdot x$$

is a bijection from the set of nonzero element of $\mathbb{Z}/(p)$ to itself. Alternativly, argue that

$$[k], [2k], [3k], \ldots, [(p-1)k]$$

is a permutation of $[1], [2], [3], \ldots, [(p-1)]$.
Claim: $[k], [2k], \ldots, [(p-1)k]$ is a permutation of $[1], [2], \ldots, [(p-1)]$.

Proof. Without loss of generality we can assume that $k < p$. Because of the unique factorization of $\mathbb{Z}$, we know that for any α in $1, 2, \ldots, (p-1)$, then we know that the factorizations of $\alpha k = q_1 q_2 \cdots q_n r_1 r_2 \cdots r_m$, and since both k and α are less than p and so $p \notin q_1, q_2, \ldots, q_n, r_1, r_2, \ldots, r_m$, thus we know that $[\alpha k] \neq [0]$, so that means that for each $[\alpha k]$ is equal to some $[1], \ldots [(p-1)]$.

Each αk must be unique. We show this by contradiction. Consider some $\alpha, \beta \in 1, 2, \ldots, (p-1)$ with $[\alpha k] = [\beta k]$, then since $\mathbb{Z}$ is an euclidean domain, we know that we can cancel, so we rewrite this expression and cancel $[k]$ from both sides, to find

$$\begin{aligned} [\alpha k] &= [\beta k] \\ [\alpha][k] &= [\beta][k] \\ [\alpha] &= [\beta]. \end{aligned}$$

Thus each of the $[\alpha k]$ must be unique and can must also be one of $[1], [2], \ldots, [(p-1)]$. Since there are p terms in $[k], [2k], \ldots, [(p-1)k]$, and each is unique and can be expressed as equal to some $[1], [2], \ldots, [(p-1)]$ of wich there are only p to chose from, then each $[1], [2], \ldots, [(p-1)]$ must be mapped to. Thus $[k], [2k], \ldots, [(p-1)k]$ is a permutation of $[1], [2], \ldots, [(p-1)]$. □

(b). Argue that for all $[k] \neq [0]$ we have $[k]^{p-1} = [1]$.
Claim: For any $[k] \neq [0]$ we know $[k]^{p-1} = [1]$.

Proof. Consider from the previous problem, the product of the sequence of elements. That is we consider $[k][2k]\cdots[(p-1)k]$. From the previous problem, we know that this is equal to

$$\begin{aligned}[k][2k]\cdots[(p-1)k] &= [1][2]\cdots[(p-1)]\\ [k]^{p-1}[1][2]\cdots[(p-1)] &= [1][2]\cdots[(p-1)]\end{aligned}$$

Then we use the ability to cancle values in fields, to find

$$[k]^{p-1} = [1]$$

□

(c). Factorize the polynomial $X^{p-1} - 1$ over $\mathbb{Z}/(p)$.
Claim: The factorization of the polynomal $X^{p-1} - 1$ over $\mathbb{Z}/(p)$ is given by $(X + 1)(X+2)\cdots(X+(p-1))$.

Proof. Consider some polynomial $X^{p-1} - 1$, We are able to verify that our proposed factorization is indeed the factorization of this polynomial, by verify that every factor in the factorization is irreducible, and the roots of the factorization and the roots of $X^{p-1} - 1$ are the same.

First we verify that all the components of the factorization are indeed irreducible, this is clear as every factor has a degree of 1, and thus we know that they are irreducible.

Now we verify that the roots of the factorization are equivalent to the roots of the polynomial. It is clear from the construction that the roots of the factorization are $[1], [2], \ldots, [(p-1)]$, and if we plug any of those into the polynomial $X^{p-1} - 1$, from the previous step, we know that the X^{p-1} for any of these potential roots will be $[1]$, so we find that the polynomial evaluates to $[1] - [1] = [0]$. Thus the roots of the polynomial and the factorization match.

Since the roots are the same, and the elements of the factorization are irreducible, then we knwo that this must be the unique prime factorization of the polynomial $X^{p-1} - 1$. □

(d). Based on the above prove the following two classic theorems of number theory:

$$\mathrm{GCD}\,(k,p) = 1 \to k^{p-1} \equiv 1 \pmod{p} \text{ and } (p-1)! \equiv -1 \pmod{p}.$$

Claim: If $\mathrm{GCD}\,(k,p) = 1$ then $k^{p-1} \equiv 1 \pmod{p}$.

Proof. Since p is prime and $k < p$, then the $\mathrm{GCD}\,(k,p) = 1$ as the prime factorization of k does not include p. Then as we have already shown, $k^{p-1} \equiv 1 \pmod{p}$ if p is prime. □

Claim: $(p-1)1 \equiv -1 \pmod{p}$.

Proof. First we consider the polynomial presented in problem (c), and the factorization demonstrated. We will call the factorization $Q(X)$, and the polynomial

$F(X)$. By the previous problem, we know that $F(X) = Q(X)$. Let us consider pluging in $[0]$ for X, then we find

$$\begin{aligned} F([0]) &= Q([0]) \\ [0]^{p-1} - 1 &= ([0]+1)([0]+2)\cdots([0]+(p-1)) \\ [0] + [-1] &= (1)(2)\cdots(p-1) \\ [-1] &= (p-1)! \end{aligned}$$

Thus we can see that $(p-1)! \equiv -1 \pmod{p}$. □

(e). Now let F denote any finite field and let $|F|$ denote the number of elements of F generalize the above to prove

$$\alpha^{|F|-1} = 1$$

for all non-zero $\alpha \in F$. What, if anything, can you say about the product of all non-zero elements of F?
Claim: For any finite field F, let $|F|$ denote the number of elements of the filed, then $\alpha^{|F|-1} = 1$ for all $\alpha \in F$.

Proof. We know that for any finite field it is possible to construct a polynomial such that $P(X) \neq 0$, but $P(\alpha) = 0 \forall \alpha \in F$. This polynomial is given by the form

$$\begin{aligned} X^{|F|} - X &= 0 \\ X^{|F|} &= X \\ X^{|F|-1} &= 1. \end{aligned}$$

By simple rearrangement, and use of cancellation, which we have available as $F[X]$ is itself a field, we find that $X^{|F|-1} = 1$ for all $X \in F$. □

Claim: The product of all nonzero elements of the field is equal to the additive inverse of the multiplicative identity -1.

Proof. Considering the same polynomial $P(X) = X^{|F|} - X$, we know that the factorization of this polynomial is given by

$$\begin{aligned} X^{|F|} - X &= X(X-\alpha_1)\cdots(X_{\alpha|F|-1}) \\ X^{|F|-1} - 1 &= (X-\alpha_1)\cdots(X_{\alpha|F|-1}). \end{aligned}$$

Then is we plug in 0 into this expression we find

$$\begin{aligned} 0^{|F|-1} - 1 &= (0-\alpha_1)\cdots(0-\alpha_{|F|-1}) \\ -1 &= \alpha_1\cdots\alpha_{|F|-1}. \end{aligned}$$

Thus we can conclude that the product of all nonzero elements of the field is equal to the additive inverse of the multiplicative identity of that field, which we have expressed as -1. □

4. Problem

Advanced Topic: Recall the following

- For an ideal I of the polynomail ring $\mathbb{C}[X_1, X_2, \ldots, X_n]$ we define

$$\operatorname{rad}(I) = \left\{P \in \mathbb{C}[X_1, X_2, \ldots, X_n] | \exists k \in \mathbb{N}, p^k \in I\right\}$$

  Here $\mathbb{N}$ denotes the set of positive integers. Recall that $\operatorname{rad}(I)$ was on the first midterm exam.
- An ideal I of $\mathbb{C}[X_1, X_2, \ldots, X_n]$ is said to be radical if $\operatorname{rad}(I) = I$.
- For an ideal I in the polynomial ring $\mathbb{C}[X_1, X_2, \ldots, X_n]$ we define

$$\mathscr{Z}(I) = \{\alpha \in \mathbb{C}^n | \forall P \in I, P(\alpha) = 0\}.$$

- Subsets $\mathbf{X} \subseteq \mathbb{C}^n$ of the form $\mathscr{Z}(I)$ are called *algebraic sets.*
- For an algebraic set $\mathbf{X}$ we define

$$\mathscr{I}(\mathbf{X}) = \{P \in \mathbb{C}[X_1, X_2, \ldots, X_n] | \forall \alpha \in \mathbf{X}, P(\alpha) = 0\}.$$

- The Strong Nullstellensatz (due to David Hilbert) states that

$$\mathscr{I}(\mathscr{Z}(I)) = \operatorname{rad}(I)$$

  for all ideals I of $\mathbb{C}[X_1, X_2, \ldots, X_n]$.

In this problem I ask you to prove the following.

(a). Prove that for all algebraic sets $\mathbf{X}$ the set $\mathscr{I}(\mathbf{X})$ is

- An ideal of $\mathbb{C}[X_1, X_2, \ldots, X_n]$.
- A radical ideal of $\mathbb{C}[X_1, X_2, \ldots, X_n]$.

Claim: All algebraic sets $\mathbf{X}$, the set $\mathscr{I}(\mathbf{X})$ are radical ideals of $\mathbb{C}[X_1, X_2, \ldots, X_n]$.

Proof. Consider some algebraic set $\mathbf{X}$. By the definition of algebraic set, then there must exist some ideal I, such that $\mathscr{Z}(I) = \mathbf{X}$. Then we consider

$$\mathscr{I}(\mathbf{X}) = \mathscr{I}(\mathscr{Z}(I))$$

Then by Strong nullstellensatz we know that $\mathscr{I}(\mathscr{Z}(I)) = \operatorname{rad}(I)$, and thus $\mathscr{I}(\mathbf{X}) = \operatorname{rad}(I)$. We conclude that for all algebraic sets $\mathbf{X}$, the set $\mathscr{I}(\mathbf{X})$ is an ideal of $\mathbb{C}[X_1, X_2, \ldots, X_n]$, since we know that $\operatorname{rad}(I)$ is an ideal.

To show that $\operatorname{rad}(I)$ is a radical ideal, we compute

$$\begin{aligned}
\operatorname{rad}(\operatorname{rad}(I)) &= \left\{P \in \mathbb{C}[X_1, X_2, \ldots, X_n] | \exists k \in \mathbb{N}, P^k \in \operatorname{rad}(I)\right\} \\
&= \left\{P \in \mathbb{C}[X_1, X_2, \ldots, X_n] | \exists k, l \in \mathbb{N}, \left(P^l\right)^k \in I\right\} \\
&= \left\{P \in \mathbb{C}[X_1, X_2, \ldots, X_n] | \exists k \in \mathbb{N}, P^k \in I\right\} \\
&= \operatorname{rad}(I).
\end{aligned}$$

Thus $\operatorname{rad}(\operatorname{rad}(I)) = \operatorname{rad}(I)$ and so we conclude that $\operatorname{rad}(I)$ is indeed a radical ideal. □

(b). Prove, through element chasing, that $\mathscr{Z}(I) = \mathscr{Z}(\text{rad}\,(I))$ for all ideals I of $\mathbb{C}[X_1, X_2, \ldots, X_n]$.
Claim: $\mathscr{Z}(I) = \mathscr{Z}(\text{rad}\,(I))$ for all ideals I of $\mathbb{C}[X_1, X_2, \ldots, X_n]$.

Proof. Consider some ideal I of $\mathbb{C}[X_1, X_2, \ldots, X_n]$. Then we compute

$$\begin{aligned}\mathscr{Z}(\text{rad}\,(I)) &= \{\alpha \in \mathbb{C}^n | \forall P \in \text{rad}\,(I)\,, P(\alpha) = 0\} \\ &= \{\alpha \in \mathbb{C}^n | \exists n \in \mathbb{N}, \forall P \in \mathbb{C}[X_1, X_2, \ldots, X_n], P^n \in I, P(\alpha) = P^n(\alpha) = 0\} \\ &= \{\alpha \in \mathbb{C}^n | \forall P \in I, P(\alpha) = 0\} \\ &= \mathscr{Z}(I).\end{aligned}$$

Thus $\mathscr{Z}(I) = \mathscr{Z}(\text{rad}\,(I))$ for allideals I of $\mathbb{C}[X_1, X_2, \ldots, X_n]$. □

(c). Prove, through element chasing, that $\mathscr{Z}(\mathscr{I}(\mathbf{X})) = \mathbf{X}$ for all algebraic sets $\mathbf{X} \subseteq \mathbb{C}^n$.
Claim: For all algebraic sets $\mathbf{X} \subseteq \mathbb{C}^n$, $\mathscr{Z}(\mathscr{I}(\mathbf{X})) = \mathbf{X}$.

Proof. Consider some algebraic set $\mathbf{X}$, by the definition of algebraic set, there must exists some ideal I such that $\mathscr{Z}(I)\mathbf{X}$. Now we consider

$$\mathscr{Z}(\mathscr{I}(\mathbf{X})) = \mathscr{Z}(\mathscr{I}(\mathscr{Z}(I))).$$

Then by Strong Nullstellensatz, we know that $\mathscr{I}(\mathscr{Z}(I)) = \text{rad}\,(I)$, so we can rewrite this expression to be

$$\mathscr{Z}(\text{rad}\,(I)).$$

Then by the previous problem, we can notice that this can be expressed as

$$\mathscr{Z}(\text{rad}\,(I)) = \mathscr{Z}(I).$$

And by our assumption, we find that this must be equal to $\mathbf{X}$. Thus for any algebraic set $\mathbf{X}$, $\mathscr{Z}(\mathscr{I}(\mathbf{X})) = \mathbf{X}$. □

(d). Prove that $\mathscr{Z}$ is a bijection between the set of radical ideals of $\mathbb{C}[X_1, X_2, \ldots, X_n]$ and the set of algebraic sets in $\mathbb{C}^n$.
Claim: $\mathscr{Z}$ is a bijection between radical ideals of $\mathbb{C}[X_1, X_2, \ldots, X_n]$ and algebraic sets in $\mathbb{C}^n$.

Proof. To show that $\mathscr{Z}$ is a bijection, we must show that it is onto, and one-to-one. We will first show onto.

Consider some algebraic set $\mathbf{X}$, let us consider the ideal I given by $\mathscr{I}(\mathbf{X})$. Then we compute

$$\mathscr{Z}(I) = \mathscr{Z}(\mathscr{I}(\mathbf{X})).$$

Using the preivous problem, we see that this is equal to $\mathbf{X}$. Thus for any algebraic set $\mathbf{X}$, we can construct some radical ideal given by $\mathscr{I}(\mathbf{X})$ such that $\mathscr{Z}(I) = \mathbf{X}$. We conclude that $\mathscr{Z}$ is onto.

To prove one-to-one, consider some radical ideal $I, J \in \mathbb{C}[X_1, X_2, \ldots, X_n]$, with $\mathscr{Z}(I) = \mathbf{X} = \mathscr{Z}(J)$. Next we consider $\mathscr{I}(\mathbf{X})$, then we apply Strong Nullstellensatz

$$\begin{gathered}\mathscr{I}(\mathscr{Z}(I)) = \mathscr{I}(\mathscr{Z}(J)) \\ \text{rad}\,(I) = \text{rad}\,(J)\,.\end{gathered}$$

Then since I, J are radical ideals, we know that $\text{rad}\,(I) = I$, and $\text{rad}\,(J) = J$, so we can see that $I = J$. Thus $\mathscr{Z}$ must be one to one.

Since $\mathscr{X}$ is both onto and one-to-one, we can conclude that it is a bijection between radical ideals of $\mathbb{C}[X_1, X_2, \dots, X_n]$ and algebraic sets in $\mathbb{C}^n$. □