Commutative Algebra Chapter 1 Problems

Zih-Yu Hsieh

June 30, 2025

1 D

Question 1.1: Exercise 1.13 (unsolved);

1. $\sqrt{I} = R \iff I = R$.
2. If ideal P is prime, then $\sqrt{P^n} = P$ for all $n \in \mathbb{N}$.

Pf:

1. $\Longrightarrow$: If $\sqrt{I} = R$, then since $R = \sqrt{I} = \varphi^{-1}(\text{Nil}(R/I))$ (where φ is the projection onto R/I), then we have $\text{Nil}(R/I) = R/I$. However, if ring $S \neq (0)$, then $\text{Nil}(S) \subsetneq S$, so since $\text{Nil}(R/I) = R/I$, we must have $R/I = (0)$, showing that $I = R$. $\Longleftarrow$: If $I = R$, it follows that $\sqrt{I} = R$.

2. Given P is a prime ideal, then for any $n \in \mathbb{N}$, any $x \in \sqrt{P^n}$ satisfies $x^k \in P^n \subseteq P$, hence by induction one can prove that $x \in P$. So, $\sqrt{P^n} \subseteq P$. Also, for all $x \in P$, $x^n \in P^n$, hence $P \subseteq \sqrt{P^n}$, eventually proving that $\sqrt{P^n} = P$.

2 D

Question 2.1: Let x be a nilpotent element of a ring R. Show that $1 + x$ is a unit is R. Deduce that the sum of a nilpotent element and a unit is a unit.

Pf:

Given that $x \in R$ is nilpotent, then $x^k = 0$ for some $k \in \mathbb{N}$ (also, this implies that $y = -x$ is also nilpotent with the same constant).

Then, $1 + x = 1 - (-x) = 1 - y$, which consider the following equation:

$$1 = 1 - 0 = 1 - y^k = (1 - y)\left(\sum_{i=0}^{k-1} y^i\right) \tag{2.1}$$

In other words, the above term is the inverse of $1 - y = 1 + x$, which implies it is invertible.

Now, for any unit $u \in R$ and nilpotent $x \in R$, since $u + x = u(1 + u^{-1}x)$, where $u^{-1}x$ is nilpotent, then $u + x$ is product of two units, hence is a unit.

3 ND

Question 3.1: Let R be a ring. Let $f = a_0 + a_1x + ... + a_nx^n \in R[x]$. Prove that:

1. f is a unit $\iff a_0$ is a unit in R and $a_1, ..., a_n$ are nilpotent.
2. f is nilpotent $\iff a_0, ..., a_n$ are nilpotent.
3. f is a zero-divisor $\iff$ there exists $a \neq 0$ in R such that $af = 0$.
4. f is primitive if $(a_0, ..., a_n) = R$ (as an ideal). Prove that $f, g \in R[x]$, then fg is primitive $\iff f$ and g are primitive.

Pf:

1. $\Longrightarrow$: Given $f = a_0 + a_1x + ... + a_nx^n$ is a unit, there exists $g = b_0 + b_1x + ... + b_mx^m$, where $fg = 1$. Which, the constant coefficient is given by $a_0b_0 = 1$, so a_0, b_0 are both units.

   Now, we'll use induction to prove that $a_n^{r+1}b_{m-r}$ is nilpotent, given $0 \leq r \leq m$: First consider the base case $r = 0$, the coefficient for degree $(n + m - r) = n + m$ is given by $a_nb_m = 0$. Then, for $r = 1$, the coefficient for $n + m - r$ is given by $a_{n-1}b_m + a_nb_{m-1} = 0$, multiply by a_n on both sides, we get:

   $$a_{n-1}b_ma_n + a_n^2b_{m-1} = 0 \Longrightarrow a_n^2b_{m-1} = 0 \tag{3.1}$$

   Now, suppose for given $0 \leq r < m$, the equation is true, then for $r + 1$, we get the coefficient of degree $(n + m - (r + 1))$ be as follow:

   $$\sum_{\max\{0, n-(r+1)\} \leq i \leq n} a_ib_{n+m-(r+1)-i} = 0 \tag{3.2}$$

   Which, multiply by a_n^{r+1}, since $n - (r + 1) \leq i \leq n$, then $n \leq r + 1 + i \leq n + r + 1$, hence the coefficient $b_{m-(r+1+i-n)}$ has $0 \leq r + 1 + i - n \leq r + 1$, which for ever index i with this expression being at most r, by induction hypothesis, $a_n^{r+1}b_{m-(r+1+i-n)} = 0$, hence every term (besides when the expression is $r + 1$) gets annihilated. So, eventually we get:

   $$r + 1 + i - n = r + 1 \Longrightarrow i = n \Rightarrow a_n \cdot a_n^{r+1}b_{n+m-(r+1-n)} = 0 \Longrightarrow a_n^{r+2}b_{m-(r+1)} = 0 \tag{3.3}$$

   This completes the induction.

   Hence, for $r = m$, we get $a_n^{m+1}b_0 = 0$, because b_0 is a unit, then a_n is in fact nilpotent, which $-a_nx^n$ is also nilpotent.

   By Question 2.1, $f - a_nx^n$ is still a unit, and with degree $n - 1$. Then, the other non-constnat coefficients can be proven to be nilpotent by induction.

2. $\Longrightarrow$: If f is nilpotent, then $f^k = (a_0 + a_1x + ... + a_nx^n)^k = 0$ for some $k \in \mathbb{N}$. Which, the leading term is $a_n^k(x^n)^k = 0$, hence $a_n^k = 0$, or a_n is nilpotent. Since a_nx^n is also nilpotent, then $f - a_nx^n$ is nilpotent (with $\deg(f - a_nx^n) = n - 1$). So, since the base case $f = a_0$ is nilpotent implies a_0 is nilpotent, by induction we can show that each a_i is nilpotent.

   $\Longleftarrow$: If each coefficient is nilpotent, it's obvious that each degree's component is nilpotent (based on the proof above), hence f is the sum of nilpotent elements, which is nilpotent.

3. Suppose f is a zero-divisor, then there exists $g = b_0 + b_1x + ... + b_mx^m$, where $fg = 0$, and here can assume m is the smallest nonnegative integer that achieves this.

   This shows that $a_nb_m = 0$ (the leading coefficient). Hence, if consider $f(a_ng) = a_{n(fg)} = 0$, since if a_ng is nonzero, then it has degree at most $m - 1 < m = \deg(g)$, hence it reaches a contradiction (since g is assumed to be the smallest). Then, $a_ng = 0$.

Therefore, $(f - a_n x^n)g = fg - (a_n g)x^n = 0$, where $f - a_n x^n$ has degree at most $n-1$. Hence, applying induction, we can deduce that for every a_k, there exists nonzero polynomials g_k, such that $a_k g_k = 0$. If multiply the leading coefficients of all g_k together, since each leading coefficient of g_k multiplied with a_k provides 0, this product annihilates all coefficients of f, hence its product with f provides 0.

4. First, recall that all the coefficients of fg are finite sum of productst of the coefficients of f and g, hence let $I = (a_0, a_1, ..., a_n)$, $J = (b_0, b_1, ..., b_m)$ represents the ideals of f and g's coefficients respectively, we get that K (the ideal corresponds to fg) satisfies $K \subseteq IJ$ (since the generators of K, the coefficients of fg are inside IJ).

   $\Longrightarrow$: To prove the contrapositive, assume either f or g is not primitive, then since either I or J are proper ideals of R, we have $K \subseteq IJ \subsetneq R$, hence since K is proper, fg is not primitive.

   $\Longleftarrow$: IF f and g are primite, here using f as an example, since there exists $k_0, k_1, ..., k_n \in R$, such that $k_0 a_0 + k_1 a_1 + ... + k_n a_n = 1$,

4 D

Question 4.1: Generalize the results in Question 3.1 to polynomial rings with several variables.

Pf:

All the setup can be done through induction. For base case $n = 1$ it is verified in Question 3.1. Now, if all the statements are true for $n - 1$ (where $n \in \mathbb{N}$), then since $R[x_1, ..., x_n] = K[x_n]$, where $K = R[x_1, ..., x_{n-1}]$. Then:

1. $f \in K[x_n]$ is a unit $\Longleftrightarrow$ constant coefficient $f_0 \in K = R[x_1, ..., x_{n-1}]$ is unit, and the other coefficients $f_1, ..., f_k \in K$ are nilpotent. Which, since the constant of $f \in R[x_1, ..., x_n]$ is provided in f_0, while other non-constant terms' coefficients scattered in $f_1, ..., f_k$ (and also the non-constant coefficients in f_1 as a member of polynomial ring $R[x_1, ..., x_{n-1}]$), by induction hypothesis, this happens iff the constant coefficient of f (also the constant coefficient of f_0) is unit, while the other terms are nilpotent.

2. $f \in K[x_n]$ is nilpotent $\Longleftrightarrow$ all coefficients $f_0, ..., f_k \in R[x_1, ..., x_{n-1}]$ is nilpotent. Again, by induction hypothesis, all the coefficients of $f_0, ..., f_k$ in R (also the coefficients of f) must be nilpotent.

3. $f \in K[x_n]$ is a zero divisor $\Longleftrightarrow$ all its coefficients $f_0, ..., f_k \in R[x_1, ..., x_{n-1}]$ all have some $a_0, ..., a_k \in R$, such that for each index i, $a_i f_i = 0$; which, f multiplied by $a_0 ... a_k$ would make all coefficients $f_i \in R[x_1, ..., x_{n-1}]$ go to 0, hence $a = a_0 ... a_k$ is the desired element with $af = 0$.

4. $fg \in K[x_n]$ is primitive $\Longleftrightarrow$ f and g are primitive in $K[x_n]$. Which, their coefficients in $R[x_1, ..., x_{n-1}]$ must have gcd being 1. However, the gcd of all its coefficients in R also divides all their coefficients in $R[x_1, ..., x_{n-1}]$, hence the gcd in R is limited to be 1.

5 D

Question 5.1: In the ring $R[x]$, the Jacobson radical is equal to the nilradical.

Pf: Let N be the nilradical, and J be the Jacobson radical of $R[x]$. Since J is the intersection of all maximal ideals, N is the intersection of all prime ideals, while maximal ideals are prime, then $N \subseteq J$ (N could be the intersection of more ideals, since prime is not necessarily maximal).

Now, if $f \in J$, by definition $1 - f$ is a unit. This happens $\iff$ every non-constant coefficients of $1 - f$ is nilpotent (they are given by $-a_1, ..., -a_n$, the negaitve non-constant coefficients of f), while the constant coefficient of f, say a_0 satisfies $1 - a_0$ being a unit (since $1 - a_0$ is the constant coefficient of $1 - f$). So, all the non-constant coefficients of f are nilpotent.

Then, since $1 - yf$ is also a unit for all $y \in R[x]$, consider $y = 1 + x$: The polynomial $(1 + x)f$ is given as follow:

$$(1 + x)f = a_0 + \sum_{i=1}^{n}(a_{i-1} + a_i)x^i + a_n x^{n+1} \tag{5.1}$$

Then, $1 - (1 + x)f$ has $-(a_0 + a_1)$ as the degree 1 coefficient. Since, $1 - (1 + x)f$ is a unit, this enforces $-(a_0 + a_1)$ to be nilpotent; and since a_1 is nilpotent, a_0 must also be nilpotent (since $\mathrm{Nil}(R)$ is an ideal, which forms a group under addition).

So, because every coefficients are nilpotent, f is nilpotent, hence $f \in N$, showing the other inclusion $J \subseteq N$.

6 D

Question 6.1: Let R be a ring, and consider $R[[x]]$ (formal power series ring). Show that:

1. f is a unit in $R[[x]] \iff a_0$ is a unit in R.
2. If f is nilpotent, then a_n is nilpotent for all $n \geq 0$. Is the converse true?
3. f belongs to the Jacobson radical of $R[[x]] \iff a_0$ belongs to the Jacobson radical of R.
4. The contraction of a maximal ideal M of $R[[x]]$ is a maximal ideal of R, and M is generated by M^c and x.
5. Every prime ideal of R is the contraction of a prime ideal of $R[[x]]$.

Pf:

1. $\implies$: If f is a unit in $R[[x]]$, there exists $g \in R[[x]]$, with $fg = 1$. Then, the constant coefficient 1 is given by the multiplication ofconstant coefficients of f and g, showing that a_0 (constant coefficient of f) is a unit.

   $\impliedby$: If a_0 is a unit in R, our goal is to find $g = \sum_{n=0}^{\infty} b_n x^n$, where $fg = 1$.

   First, it's clear that $b_0 = a_0^{-1}$. Now, for b_1, since we want the degree 1 coefficient of fg to be 0, and the degree 1 coefficient is given b $a_0 b_1 + a_1 b_0$, then set $b_1 = -a_0^{-1} a_1 b_0$, we get the desired result.

   Inductively, when $b_0, ..., b_{n-1}$ all have fixed expression using the collections of a_n, since degree n coefficient of fg is given by $\sum_{i=0}^{n} a_i b_{n-i}$, then if we want the expression to be 0, we can set b_n as follow:

   $$a_0 b_n + \sum_{i=1}^{n} a_i b_{n-i} = 0, \quad b_n = -a_0^{-1} \sum_{i=1}^{n} a_i b_{n-i} \tag{6.1}$$

   So, there exists an expression of g, where $fg = 1$, showing that f is a unit.

2. Here, if f is nilpotent, then $f^n = 0$ for some $n \in \mathbb{N}$. Then, the constant coefficient becomees $a_0^n = 0$, showing that the constant term is nilpotent. THn, $f - a_0 x^0$ becomes a power series with smallest degree 1, and is also nilpotent.

   Now, by induction, if proven that the deg $\leq n - 1$ terms are nilpotent, then subtracting out these terms, we get $f_n = a_n x^n + ...$ is nilpotent. Then, there exists $k \in \mathbb{N}$, where $f_n^k = 0$. Then, the smallest degree is x^{nk}, with coefficient $a_n^k = 0$. Hence, a_n is also nilpotent. Then by induction, all coefficients are nilpotent.

3. $\Longrightarrow$: suppose f belongs to the Jacobson radical of $R[[x]]$, then for all $g \in R[[x]]$ (in particular, can choose $g \in R$), satisfies $1 - gf$ being a unit in $R[[x]]$, which is achieved only when the constant coefficient is a unit (proven in 1.). So, since its constant coefficient is given by $1 - g_0 f_0$, since for all $g_0 \in R$ this term is a unit, we have f_0 being in the Jacbson radical of R.

   $\Longleftarrow$: Suppose f_0 belongs to the Jacobson radical of R, then for all $g \in R[[x]]$, the term $1 - gf$ has constant coefficient $1 - g_0 f_0$, which is a unit, hence $1 - gf$ is a unit. THis shows that f belongs to the Jacobson Radical of $R[[x]]$.

4. Given a projection map $p : R[[x]] \twoheadrightarrow R$ that returns the constant coefficient, and $M \subset R[[x]]$ is maximal. Then, if consider its contraction $M_c := p(M)$, and the projection map $\pi : R \twoheadrightarrow R/M_c$, then the composition becomes $\pi \circ p : R[[x]] \twoheadrightarrow R/M_c$, where we claim that $\ker(\pi \circ p) = M$:

   First, all $f \in M$ satisfies $p(f) \in M_c$, so $\pi(p(f)) = 0$, which $M \subseteq \ker(\pi \circ p)$; also, if $\pi(p(f)) = 0$, it shows that $p(f) \in M_c$, which $f \in p^{-1}(M_c)$. We know by definition $M \subseteq p^{-1}(M_c)$, and $p^{-1}(M_c)$ is an ideal. Then, by maximality of M, either $m = p^{-1}(M_c)$, or $p^{-1}(M_c) = R[[x]]$. However, if the second condition happens, we have $M_c = R$, showing that 1 has a preimage in M (which turns out that preimage is a unit by 1.), so $M = R$, contradicitng the maximality. Hence, we must have $M = p^{-1}(M_c)$, which also shows that $\ker(\pi \circ p) = M$.

   Hence, by First Isomorphism Theorem, $R/M_c \cong R[[x]]/\ker(\pi \circ p) = R[[x]]/M$ (which is a field by maximality), hence $M_c \subset R$ is maximal.

   Finally, $M \subseteq (M_c, x)$ by definition; to show the other inclusion, it suffices to show that $(x) \subseteq M$; notice that all $f \in (x)$ has no constant term, hence for any $g \in R[[x]]$, gf also has no constant term, then $1 - gf$ has constant term 1, showing that it's a unit. Hence, f actually belongs to the Jacobson radical of $R[[x]]$ (the intersection of all maximal ideal of $R[[x]]$). With M being maximal, $(x) \subseteq M$, hence for any $m \in M_c$ (where $M_c \subset M$, since everything beyond constant term can be canceld by (x)) and any $g, h \in R[[x]]$, with $x \cdot h \in M$, we have $m \cdot g + x \cdot h \in M$, showing that $(M_c, x) \subseteq M$. Therefore, $M = (M_c, x)$, M is generated by all its element's constant coefficient and x.

5. Suppose $P \subset R$ is a prime ideal, using the same projection map p in part 4, consider $p^{-1}(P) \subset R[[x]]$: Again, given projection map $\pi : R \twoheadrightarrow R/P$, our goal is to prove $\ker(\pi \circ p) = p^{-1}(P)$.

   It's clear that $p^{-1}(P) \subseteq \ker(\pi \circ p)$ (all f in it has $p(f) \in P$, so $\pi(p(f)) = 0$). Then, for all f with $\pi(p(f)) = 0$, we have $p(f) \in P$, hence $f \in p^{-1}(P)$, this shows that $\ker(\pi \circ p) = p^{-1}(P)$.

   Then, by first isomorphism theorem, since $\pi \circ p : R[[x]] \twoheadrightarrow R/P$, we have:

$$R[[x]]/p^{-1}(P) = R[[x]]/\ker(\pi \circ p) \cong R/P \tag{6.2}$$

   This shows that $p^{-1}(P)$ is a prime ideal, since $R[[x]]/p^{-1}(P)$ is an integral domain.

7 ND

Question 7.1: A ring R is such that every ideal not contained in the nilradical contains a nonzero idempotent (an elemenet e with $e^2 = e \neq 0$). Prove that the nilradical and the Jacobson radical of R are equal.

Pf:

Let N, J represent the niradical and Jacobson radical respectively. It is clear that $N \subseteq J$ by definition.

To prove that $J \subseteq N$ by contradiction, suppose the contrary that $J \not\subseteq N$, by assumption there exists nonzero $e \in J$ with $e^2 = e$ (which implies e is not nilpotent, hence $e \notin N$). Which by definition of Jacobson radical, every $k \in R$ satisfies $1 - ke$ being a unit

8 ND

Question 8.1: Let R be a ring in which every element satisfies $x^n = x$ for some $n > 1$. Show that every prime ideal in R is maximal.

Pf:

First, $\text{Nil}(R) = (0)$: If $x \in \text{Nil}(R)$, then since there exist $n, k \in \mathbb{N}$, with $x^n = x$ and $x^k = 0$ (where we demand k to be the smallest, and $n > 1$ by assumption), there are two cases to consider:

1. If $k \leq n$, then $x^n = 0$, showing that $x = 0$.
2. if $k > n$, then $k = ln + r$ for some $l, r \in \mathbb{N}$, and $0 \leq r < n$. Which, the following is satisfiesd:

$$x^k = x^{ln+r} = (x^n)^l \cdot x^r = x^{l+r} = 0 \tag{8.1}$$

   Notice that $l + r < ln + r = k$ by assumption that $n > 1$, so we reach a contradiction (since there exists $l + r < k$, with $x^{l+r} = 0$).

Hence, the second case doesn't exist, where the first case shows that $\text{Nil}(R) = (0)$.

9 D

Question 9.1: Let $R \neq 0$ be a ring. Show that the set of prime ideals of R has minimal elements with respect to inclusion.

Pf:

We'll prove by Zorn's Lemma, where let A be the set of all prime ideals, and the Partial Order given by $P_1 \succeq P_2$ iff $P_1 \subseteq P_2$.

Let $C \subseteq A$ be a chain, and let $P_C = \bigcap_{P \in C} P$. It is clear that P_C is an ideal, and if $P_C \in A$, then P_C is an upper bound of C. So, it suffices to show that $P_C \in A$ (or P_C is a prime ideal).

Suppose $x, y \in R$ satisfies $xy \in P_C$, then since for any prime ideal $P \in C$, $xy \in P$, then either $x \in P$ or $y \in P$. If all $P \in C$ contains x (or y), then we're done. Now, if some contains x and some contains y, consider the subchain $C_x := \{P \in C \mid x \in P\}$:

- If C_x is comaximal in C (in a set theoretic), then for every $P \in C$, there exists $P_x \in C_x$, where $P_x \succeq P$, so $P_x \subseteq P$, hence $x \in P$, showing that $x \in P_C$.
- Else if C_x is not comaximal in C, then there exists $P \in C$, where all $P_x \in C_x$ has $P \succneq P_x$ (which $P \notin C_x$). Hence, $y \in P$, showing that all $P_x \in C_x$ has $P \subsetneq P_x$, or $y \in P_x$. So, given $P \in C$, regardless of its containment in C_x, we have $y \in P$, showing that $y \in P_C$.

The above statements show that P_C is prime, hence $P_C \in A$, every chain has an upper bound. Then, by Zorn's Lemma, this POset has a maximal element, which is the minimal elements with respect to inclusion.

10 D

Question 10.1: Let $I \subsetneq R$ be an ideal. Show that $I = \sqrt{I} \iff I$ is an intersection of prime ideals.

$\Longrightarrow$: If $\sqrt{I} = I$, since the projection map $\varphi : R \twoheadrightarrow R/I$ satisfies the following:

$$I = \sqrt{I} = \varphi^{-1}(\mathrm{Nil}(R/I)) = \bigcap_{\overline{P} \subset R/I \text{ prime}} \varphi^{-1}\left(\overline{P}\right) = \bigcap_{I \subseteq P \subset R \text{ prime}} P \tag{10.1}$$

Which is an intersection of prime ideals.

$\Longleftarrow$: Suppose $\{P_i\}_{i\in \mathrm{A}}$ is a collection of prime ideals, and define $I := \bigcap_{i\in\mathrm{A}} P_i$. Then, for all $x \in \sqrt{I}$, since there exists $n \in \mathbb{N}$, with $x^n \in I$, because $x^n \in P_i$ for all index $i \in \mathrm{A}$, then $x \in P_i$, hence $x \in I$, showing that $\sqrt{I} \subseteq I$. Since the other inclusion is trivially true, $\sqrt{I} = I$.

11 D

Question 11.1: Let R be a ring, $\mathrm{Nil}(R)$ be its nilradical. Show that the following are equivalent:
1. R has exactly one prime ideal.
2. Every element of R is either a unit or nilpotent.
3. $R/\mathrm{Nil}(R)$ is a field.

$1 \Longrightarrow 2$: Suppose R has precisely one prime ideal, then since $\mathrm{Nil}(R)$ is the intersection of all prime ideals, $\mathrm{Nil}(R) = P$ (the prime ideal). This also enforces $\mathrm{Nil}(R)$ to be maximal (since every commutative ring has a maximal ideal, and all maximal ideal is prime).

Now, suppose $u \in R \setminus \mathrm{Nil}(R)$ (i.e. not nilpotent), then since $\mathrm{Nil}(R) \subsetneq \mathrm{Nil}(R) + (u)$, then $\mathrm{Nil}(R) + (u) = R$, showing that $1 = ku + x$ for some $k \in R$ and $x \in \mathrm{Nil}(R)$. Notice that $-x$ is nilpotent, which $1 - x$ is a unit, hence $1 - x = ku$, showing that ku is a unit, which u is a unit.

Hence, every element of R is either a unit or nilpotent.

$2 \Longrightarrow 3$: Suppose every element is either a unit or nilpotent, then for all $\overline{u} \in R/\mathrm{Nil}(R)$ (with $\overline{u} := u \bmod \mathrm{Nil}(R)$) that is nonzero, since u is a unit, then inherantly, $\overline{u}$ is also a unit in $R/\mathrm{Nil}(R)$, showing that it is a field.

$3 \Longrightarrow 1$: Suppose $R/\mathrm{Nil}(R)$ is a field, then $\mathrm{Nil}(R)$ is maximal. Now, suppose P is a prime ideal, then because $\mathrm{Nil}(R) \subseteq P \subsetneq R$, then this enforces $\mathrm{Nil}(R) = P$. Hence, there is only one prime ideal, namely $\mathrm{Nil}(R)$.

12 D

Question 12.1: A ring R is a *Boolean Ring* if $x^2 = x$ for all $x \in R$. In a boolean ring R, show that:
1. $2x := x + x = 0$ for all $x \in R$.
2. Every prime ideal P is maximal, and R/P is a field with two elements.
3. Every finitely generated ideal in R is principal.

Pf:
1. For all $x \in R$, since $x^2 = x$, we have $x + 1 = (x + 1)^2 = x^2 + 2x + 1 = x + 2x + 1$, hence after cancellation, $2x = 0$.
2. Based on Question 8.1, since all element $x \in R$ has some $n > 1$, with $x^n = x$ (in this case, $n = 2$), then all prime ideal P is maximal, showing that R/P is a field.

   Now, suppose $x \in R$ satisfies $\overline{x} \in R/P$ is nonzero, then since $(\overline{x})^2 = \overline{x}$, then it is a root of the polynomial $y^2 - y \in R/P[y]$. Since this is a UFD, then there exists only two solution, namely 0 and 1. because $\overline{x} \neq 0$ by assumption, then $\overline{x} = 1$. Hence, $R/P \cong \mathbb{Z}_2$.

3. We'll approach by induction. Given $I = (x, y)$, consider $z = x + y + xy \in I$: We have $xz = x^2 + xy + x^2y = x + xy + xy = x$, and $yz = xy + y^2 + xy^2 = xy + y + xy = y$. So, $I = (x, y) \subseteq (z)$ (while $(z) \subseteq I$ by definition). Hence, $(z) = I$, showing that I is principal.

   Now, if this is true for $n - 1$ generators, for $I = (a_1, ..., a_n)$, since $I = (a_1, ..., a_{n-1}) + (a_n) = (z) + (a_n) = (z, a_n)$ for some $z \in (a_1, ..., a_{n-1})$, then $I = (z, a_n) = (z')$ for some $z' \in I$, showing that I is principal. This completes the induction.

13 ND

Question 13.1: A local ring contains no idempotent other than $0, 1$.

Pf:

Recall that a local ring R has exactly one maximal ideal, say M. Now, suppose $e \in R$ is idempotent, then in the residue field R/M, since it is also a root of the polynomial $x^2 - x \in (R/M)[x]$, then $e \equiv 0 \bmod M$, or $e \equiv 1 \bmod M$.

For the first case, we have $(1 + e)^2 = 1 + 2e + e^2 = 1 + 3e$

For the second case, we have $e = 1 + m$ for some $m \in M$, hence $m = e - 1$. Which, $m^2 = e^2 - 2e + 1 = -e + 1 = -(e - 1) = -m$, showing that $\left(m^2\right)^2 = m^2$

14 ND

Question 14.1: About construction of algebraic closure, read it

15 D

Question 15.1: In a ring R, let Σ be the set of all ideals in which every element is a zero-divisor. Show that the set Σ has maximal elements, and that every maximal element of Σ is a prime ideal. Hence the set of zero-divisors in R is a union of prime ideals.

Pf:

Again, we'll proceed with Zorn's Lemma with the partial order being inclusion. Given a chain $C \subseteq \Sigma$, consider the following construction of „ideal“:

$$I_C = \bigcup_{I \in C} I \tag{15.1}$$

If the above is an ideal containing only zero divisors, it's clear that it is an upper bound of C. It only contains zero divisors, because all $I \in C$ only contains zero divisors„ and it's an ideal, because the union of a chain of ideals is an ideal.

Hence, $I_C \in \Sigma$, showing that every chain in Σ has an upper bound. Then, by Zorn's Lemma, Σ has a maximal element.

Now, given that $P \in \Sigma$ is a maximal element, why is it prime? For all $x, y \in R$, suppose $xy \in P$, i.e. xy is a zero divisor. Which as a result, either x or y must be a zero divisor.

Which, WLOG, suppose x is a zero-divisor, then $x \in P$: If $x \notin P$, then notice that the ideal $(x) + P$ also contains only zero divisors (for all $k \in R$ and $p \in P$, the element $kx + p$ is a zero-divisor, since there exists $a, b \in R$, with $ax = bp = 0$, then multiply by ab provides 0), so $(x) + P \in \Sigma$; and $P \subsetneq (x) + P$, but this violates the assumption that P is a maximal element in Σ.

Hence, the assumption is false, $x \in P$. This demonstrates that P is prime.

16 D

Question 16.1: Let R be a ring and let X be the set of all prime ideals of R. For each subset E or R, let $V(E)$ denote the set of all prime ideals of R which contain E. Prove that:

1. If I is the ideal generated by E, then $V(E) = V(I) = V\left(\sqrt{I}\right)$.
2. $V(0) = X, V(1) = \emptyset$.
3. If $(E_i)_{i\in I}$ is any family of subsets of R, then:

$$V\left(\bigcup_{i\in I} E_i\right) = \bigcap_{i\in I} V(E_i) \tag{16.1}$$

4. $V(I \cap J) = V(IJ) = V(I) \cup V(J)$ for any ideals I, J of R.

These results show that the sets $V(E)$ satisfies the axioms for closed sets in a topological space. The resulting topology is called the *Zariski topology*. THe topological space X is called the *prime spectrum* of R, denoted as $\mathrm{Spec}(R)$.

Pf:

1. For all $P \in V(E)$, since it contains E, it contains I, hence $P \in V(I)$, showing that $V(E) \subseteq V(I)$; on the other hand, since $E \subseteq I$, any $P' \in V(I)$ contains I, hence contains E. So, $P' \in V(E)$, showing $V(I) \subseteq V(E)$, hence the two are the same.

   Now, since for all $P \in V\left(\sqrt{I}\right)$, P containing $\sqrt{I}$ implies it contains I, hence $P \in V(I)$, or $V\left(\sqrt{I}\right) \subseteq V(I)$; then, for any $P' \in V(I)$, any $x \in \sqrt{I}$ satisfies $x^n \in I \subseteq P'$, hence $x \in P'$ can be derived through induction and the prime ideal property. So, $\sqrt{I} \subseteq P'$, showing that $P' \in V\left(\sqrt{I}\right)$. Hence, $V(I) \subseteq V\left(\sqrt{I}\right)$, the two are in fact the same.

2. For all $P \in X$, since P contains 0 by def, then $P \in V(0)$, showing that $X = V(0)$. Now, $V(1) = \emptyset$, because if there exists prime ideals are defined to be proper subgroups of R under addition, while an ideal containing 1 is R itself, so none of the prime ideals can be in $P(1)$.

3. Let $(E_i)_{i\in I}$ be a family of subests of R. For all $P \in V\left(\bigcup_{i\in I} E_i\right)$, since all $E_i \subseteq P$, then $P \in V(E_i)$, hence $P \in \bigcap_{i\in I} V(E_i)$. For the converse, if $P \in \bigcap_{i\in I} V(E_i)$, then all $E_i \subseteq P$, hence $\bigcup_{i\in I} E_i \subseteq P$, showing that $P \in V\left(\bigcup_{i\in I} E_i\right)$. This finishes both inclusion.

4. Since $IJ \subseteq (I \cap J) \subseteq I, J$, then for all $P \in V(I) \cup V(J)$, it's clear that P contains $I \cap J$, hence $P \in V(I \cap J)$; and all $P' \in V(I \cap J)$ automatically contains IJ, hence $P' \in V(IJ)$. Thos demonstrates $V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(IJ)$.

   Now, for all $P \in V(IJ)$, the goal is to prove that either $I \subseteq P$ or $J \subseteq P$: Suppose $I \subseteq P$, then we're done. Else, if $I \nsubseteq P$, there exists $x \in I \setminus P$. Then, for all $y \in J$, since $xy \in IJ \subseteq P$, then with $x \notin P$, we must have $y \in P$ due to the properties of prime ideals. Hence, $J \subseteq P$.

   As a result, we must have P containing either I or J, hence $P \in V(I) \cup V(J)$, whosing that $P(IJ) \subseteq P(I) \cup P(J)$.

   The above two casees finishes the prove that all are the same.

17 ND

Question 17.1: Draw pictures of prime spectrum of $\mathbb{Z}, \mathbb{R}, \mathbb{C}[x], \mathbb{R}[x], \mathbb{Z}[x]$.

Pf:

For $\mathbb{Z}$, all the prime ideals are $p\mathbb{Z}$, where p is prime. Then, any set $V(E)$ will be all the prime divisors of some elements in E. Because the choice of E can be arbitrary, any collection of prime ideals is closed, hence it forms a discrete topology.

For $\mathbb{R}$ and $\mathbb{C}$, since the only prime ideal is (0), it's the discrete topology.

For $\mathbb{C}[x]$, since it's an ED, and $\mathbb{C}$ is algebraically closed, all prime ideals are maximal, and must be generated by irreducible polynomials, in $\mathbb{C}$ are all the linear polynomials. This again forms a discrete topology.

For $\mathbb{R}[x]$, similar concept applies from $\mathbb{C}[x]$, but here there are irreducible polynomials not with linear order.

For $\mathbb{Z}[x]$, it is hard, because it's not a PID, so the characterization of prime ideals are more complicated.

18 D

Question 18.1: For each $f \in R$, let X_f denote the complement of $V(f)$ in $X = \text{Spec}(R)$. The sets X_f are open under Zariski Topology. Show that they form a basis of open sets for the Zariski topology, and that:

1. $X_f \cap X_g = X_{fg}$.
2. $X_f = \emptyset \iff f$ is nilpotent.
3. $X_f = X \iff f$ is a unit.
4. $X_f = X_g \iff \sqrt{(f)} = \sqrt{(g)}$.
5. X is quasi-compact (that is, every open covering of X has a finite sub-covering. The distinction from regular compactness is due to the possibility that X is not Hausdorff, such distinction happens mostly in algebraic geometry).
6. More generally, each X_f is quasi-compact.
7. An open subset of X is quasi-compact $\iff$ it is a finite union of sets X_f.

Pf:

First to prove that set of X_f forms a basis, it's because of 1. that will be proved later (for any point lying in $X_f \cap X_g$, since $X_f \cap X_g = X_{fg}$ is also a basis element), and 2. (where $X_f = X$ iff f is a unit), which the collection not only covers the whole X, it also satisfies the other basis axioms.

1. Given $f, g \in R$, then:

$$\begin{aligned} X_f \cap X_g = X \setminus (V(f) \cup V(g)) = X \setminus (V((f)) \cup V((g))) = X \setminus (V((f)(g))) = X \setminus (V((fg))) \\ = X \setminus V(fg) = X_{fg} \end{aligned} \tag{18.1}$$

2. $X_f = \emptyset \iff V(f) = X \iff$ all prime ideals P satisfies $f \in P \iff f$ is nilpotent (in the intersection of all prime ideals, the nilradicals).

3. $X_f = X \Longleftrightarrow V(f) = V((f)) = \emptyset$. Which, f is a unit implies it's not contained in any prime ideals, hence $V(f) = \emptyset$. On the other hand, if $V((f)) = \emptyset$, it implies that $(f) = R$ (since all proper ideal of R is contained in some maximal ideal, hence if f is not a unit, there exists maximal ideal M, with $(f) \subseteq M$.Then, $M \in V(f)$).

    Hence, $X_f = X$ is equivalent to f being a unit.
4. Notice that $X_f = X_g$ iff $V((f)) = V(f) = V(g) = V((g))$.

    Recall that $\sqrt{I} = \bigcap_{I \subseteq P} P$ (where P runs through all the prime ideals), and such collection of ideals is precisely $V(I)$. Hence, $V(I) = V(J)$ implies $\sqrt{I} = \sqrt{J}$ (since both are the intersection of $V(I)$). The converse is also true because $V(I) = V\left(\sqrt{I}\right)$, hence $\sqrt{I} = \sqrt{J}$ implies $V(I) = V(J)$.

    So, we conclude that $X_f = X_g$ iff $V((f)) = V((g))$ iff $\sqrt{(f)} = \sqrt{(g)}$.

5. Given that the set $\left\{X_f\right\}_{f \in R}$ forms a basis of the Zariski Topology, it suffices to consider the open covering formed by subset of this basis (since every open set is union of basis elements). supopse a subset $J \subseteq R$ has $\left\{X_f\right\}_{f \in J}$ forms an open cover of X, then $X = \bigcup_{f \in J} X_f$, hence $V(J) = \bigcap_{f \in J} V(f) = X \setminus \left(\bigcup_{f \in J} X_f\right) = \emptyset$.

    Since $V(J) = V((J)) = \emptyset$ (where (J) indicates the ideal generated by J), this indicates that $(J) = R$ (since every proper ideal is contained in some maximal ideal, then if (J) is proper, $V((J)) \neq \emptyset$). So, there exists $f_1, ..., f_n \in J$, and $g_1, .., g_n \in R$, such that $\sum_{i=1}^n g_i f_i = 1$. Hence, $V((f_1, ..., f_n)) = V(\{f_1, ..., f_n\}) = \emptyset$. Then, based on the following equality, we can confirm that X_{f_i} forms an open cover of X, hence proving that a finite subcover exists:

$$V(\{f_1, ..., f_n\}) = \bigcap_{i=1}^n V(f_i) = X \setminus \left(\bigcup_{i=1}^n X_{f_i}\right) = \emptyset \Longrightarrow \bigcup_{i=1}^n X_{f_i} = X \tag{18.2}$$

6. To prove that each X_f is compact, consider a subset $J \subseteq R$ such that $X_f \subseteq \bigcup_{g \in J} X_g$: Taking the complement, we get that $V(f) \supseteq \bigcap_{g \in J} V(g) = V(J)$, so, for every prime ideal with $J \subseteq P$, since $P \in V(f)$, we have $f \in P$, hence $f \in \bigcap_{P \in V(J)} P$, which since $V(J) = V((J)) = V\left(\sqrt{(J)}\right)$, such intersection is precisely $\sqrt{(J)}$. Hence, $f \in \sqrt{(J)}$.

    So, it implies that for some $g_1, ..., g_n \in J$, $l_1, ..., l_n \in R$, and $k \in \mathbb{N}$, we have $f^k = l_1 g_1 + ... + l_n g_n$, showing that $f \in \sqrt{(g_1, ..., g_n)}$. This further implies that $V\left(\sqrt{(g_1, ..., g_n)}\right) = V(\{g_1, ..., g_n\}) = \bigcap_{i=1}^n V(g_i) \subseteq V(f)$, then taking the complement, we have $X_f \subseteq \bigcup_{i=1}^n X_{g_i}$.

    This proves the existence of finite subcover, hence showing that each X_f is compact.

7. $\Longleftarrow$: Any finite union of sets X_f is open and compact (union of open sets is open, and finite union of compact subsets is compact).

    $\Longrightarrow$: Suppose $U \subseteq X$ is open and quasi-compact, then its complement $X \setminus U = V(E)$ for some subset $E \subseteq R$. Then, consider the following equality:

$$X \setminus U = V(E) = \bigcap_{f \in E} V(f) = X \setminus \left(\bigcup_{f \in E} X_f\right) \tag{18.3}$$

(since X_f is the complement of $V(f)$).

As a result, we must have $U = \bigcup_{f \in E} X_f$, hence the collection associated to E forms an open cover of U, which by compactness, there exists $f_1, ..., f_n \in E$, such that $U = \bigcup_{i=1}^n X_{f_i}$, so it is intersection of finite X_f's.

19 D

Question 19.1: Given $X = \operatorname{Spec}(R)$, for any prime ideal $x \in X$, one would denote $P_x := x$ (even though x is essentially P_x, just for notational purpose). Show that:

1. The set $\{x\}$ is closed (x is called a „closed point“) in $\operatorname{Spec}(A) \iff P_x$ is maximal.
2. $\overline{\{x\}} = V(P_x)$.
3. $y \in \overline{\{x\}} \iff P_x \subseteq P_y$.
4. X is a T_0-space (i.e. if x, y are distinct points of X, then either there is a neighborhood of x that doesn't cotain y, or a neighborhood of y which doesn't contain x).

Pf:

1. $\Longleftarrow$: Suppose P_x is maximal, then since $V(P_x) = \{x\}$ (since x is a prime ideal containing itself, and any other prime ideal containing it must be itself due to maximality), then $\{x\}$ is closed. $\Longrightarrow$: Suppose the set $\{x\}$ is closed, then there exists subset $E \subset R$, such that $V(E) = V((E)) = V\left(\sqrt{(E)}\right) = \{x\}$.

   Which, notice that $\sqrt{(E)} = x = P_x$ in this case (properties of radicals), hence $V(P_x) = \{x\}$, showing that the only prime ideal containing itself is itself. This shows that P_x is maximal (if not, then there should be some maximal ideal containing it, and the set $V(P_x)$ would contain more than one element).

   Hence, $\{x\}$ is closed $\iff P_x$ is maximal.

2. For any $x \in X$,since $P_x = x$, we have $x \in V(P_x)$, then by definition, since $\overline{\{x\}}$ is the smallest closed set containing x while $V(P_x)$ is closed, $\overline{\{x\}} \subseteq V(P_x)$.

   Now, let $\{C_i := V(E_i) \subseteq X \mid i \in I\}$ denotes the collection of all closed subsets of X containing x (where each $E_i \subseteq R$), hence we have $\overline{\{x\}} = \bigcap_{i \in I} V(E_i) = V\left(\bigcup_{i \in I} E_i\right)$.

   Notice that by definition, $V(E_i)$ containing x implies that $E_i \subseteq x = P_x$, hence the union $\bigcup_{i \in I} E_i \subseteq P_x$. Which, as a result, $V(P_x) \subseteq V\left(\bigcup_{i \in I} E_i\right) = \overline{\{x\}}$.

   So, this finishes the proof that $V(P_x) = \overline{\{x\}}$.

3. Based on 2., we can conclude that $y \in \overline{\{x\}} = V(P_x) \iff P_x \subseteq y = P_y$.

4. Given x, y as two distinct points of X, there are two cases to consider:

   First (WLOG), if $x \subseteq y$ (which, since $x \neq y$, we must have $x \subsetneq y$), then as a result, we have $x \notin V(y)$ (since x doesn't contain y by definition). Which, take open subset $U = X \setminus V(y)$, we have $x \in U$; on the other hand, because y contains itself, then $y \in V(y)$, hence $y \notin U$, so U satisfies all the desired result.

   Then, if $x \not\subseteq y$, then there exist point $p \in x \setminus y$, so if consider the set $V(p)$, we have $x \in V(p)$, yet $y \notin V(p)$. Hence, take the open subset $U = X \setminus V(p)$, we have $y \in U$, yet $x \notin U$.

20 D

Question 20.1: A topological space X is said to be *irreducible* if $X \neq \emptyset$ and if every pair of nonempty open sets in X intersets, or equivalently if every nonempty open set is dense in X. Show that $X = \operatorname{Spec}(R)$ is irreducible iff the nilradical of R is a prime ideal.

Pf:

$\Longrightarrow$: We'll prove the contrapositive. If $\operatorname{Nil}(R)$ is not prime, then there exists $x, y \in R \setminus \operatorname{Nil}(R)$, where $xy \in \operatorname{Nil}(R)$. Then, if consider $V(x), V(y)$, we first have the following:

$$V(x) \cup V(y) = V((x)) \cup V((y)) = V((x)(y)) = V((xy)) = V(xy) = V(\mathrm{Nil}(R)) = X \tag{20.1}$$

Hence, let $U_x = X \setminus V(x)$ and $U_y = X \setminus V(y)$, we have $U_x \cap U_y = X \setminus (V(x) \cup V(y)) = \emptyset$. However, since both $x, y \notin \mathrm{Nil}(R)$, this indicates that $V(x), V(y) \neq X$ (if one is X, then every prime ideal contains that element, showing that it's in $\mathrm{Nil}(R)$, but this contradicts), so $U_x, U_y \neq \emptyset$.

Since there exists $U_x, U_y \neq \emptyset$, with $U_x \cap U_y = \emptyset$, then this proves that X is not irreducible.

$\Longleftarrow$: Now, suppose that $\mathrm{Nil}(R)$ is prime, notice that all prime ideal contains $\mathrm{Nil}(R)$, so $V(\mathrm{Nil}(R)) = X$. Now, given any open subsets $U_1, U_2 \subseteq X$, there exists subsets $E_1, E_2 \in R$, where $U_i = X \setminus V(E_i)$. If assume that $U_1 \cap U_2 = \emptyset$, then the complement $V(E_1) \cup V(E_2) = V((E_1)) \cup V((E_2)) = V((E_1)(E_2)) = V(\mathrm{Nil}(R)) = X$, this shows that $(E_1)(E_2)$ is contained in all prime ideals, hence $(E_1)(E_2) \subseteq \mathrm{Nil}(R)$.

If $V(E_1) = X$, then $V(E_2) = \emptyset$; which, if $V(E_1) \neq X$, then $E_1 \not\subseteq \mathrm{Nil}(R)$, there exists $e_1 \in E_1 \setminus \mathrm{Nil}(R)$. Which, since for all $e_2 \in E_2$, $e_1 e_2 \in (E_1)(E_2) \subseteq \mathrm{Nil}(R)$, we have $e_2 \in \mathrm{Nil}(R)$, showing that $E_2 \subseteq \mathrm{Nil}(R)$, or $V(E_2) = X$.

Since in either case, the union of two being X implies one of the closed set is X, then that means one of the complement is $\emptyset$, hence $U_1 \cap U_2 = \emptyset$ implies one of them is emptyset, so any two nonempty open subsets must have nontrivial intersection.

21 ND

Question 21.1: Let X be a topological space.

1. If Y is an irreducible subspace of X, then the closure $\overline{Y}$ of Y in X is irreducible.
2. Every irreducible subspace of X is contaiend in a maximal irreducible subspace.
3. The maximal irreducible subspaces of X are closed and cover X. They're called the *irreducible components* of X. What are the irreducible components of a Hausdorff space?
4. If R is a ring and $X = \mathrm{Spec}(R)$, then the irreducible components of X are the closed sets $V(P)$, where P is a minimal prime ideal of R.

Pf:

1. Suppose $Y \subseteq X$ is an irreducible subspace, then for any open subsets $U_1, U_2 \subseteq X$ such that $U_i \cap Y \neq \emptyset$, we have $(U_1 \cap Y) \cap (U_2 \cap Y) = (U_1 \cap U_2 \cap Y) \neq \emptyset$.

   Which, suppose U_1, U_2 now have nontrivial intersection with $\overline{Y}$, then it implies that U_1, U_2