Question 1

Let R be a domain which is not a field. Prove that $R[x]$ is not a principal ideal doamin.

Solution: Since R is not a field, there is a non-zero a such that $a \notin R^\times$. Let I be the ideal generated by a and x. If I is principal, then $I = bR[x]$ for some $b \in R[x]$. Let $b = b_x x + b_0$, then consider $x \in I$, so $x = f(b_x x + b_0)$ for some $f = \sum_{i=0}^k f_i x^i$. Since a is non-zero, b_0 is non-zero. R is a domain, f_0 must be 0. But then f_i for $1 \leq i \leq k$ must be 0 since $f_i x^i (b_x x)$ must be 0. This means that $f = 0$, but $0(b_x x + b_0) \neq x$. Thus I cannot be principal.

Question 2

Let S be a multiplicative subset of a principal ideal domain R. Show that the localization $S^{-1}R$ is also a principal domain.

Solution: Let J be an ideal $\left\{ \frac{a/s}{} \right\}$ in $S^{-1}R$. If $\frac{a}{s} \in J$, then $\frac{a}{s} \cdot \frac{s}{1} = \frac{a}{1} \in J$, because J is an ideal. Then, let $I = \left\{ a \mid \frac{a}{1} \in J \right\} \subset R$. Then, $0 \in I$. Moreover, if $a, b \in I$ and $r \in R$, then $\frac{a}{1}, \frac{b}{1} \in J$, and $\frac{r}{1} \in S^{-1}R$. Therefore, $\frac{ab}{1}, \frac{a-b}{1}, \frac{ar}{1} \in J$, which means that $ab, a-b, ar \in I$. Thus, I is an ideal of R.

Now, assume that I is principal, and $I = aR$ for some element $a \in R$. Then, for any element $\frac{b}{s} \in J$, it is true that $\frac{b}{s} = \frac{b}{1}\frac{1}{s}$ where $\frac{1}{s} \in S^{-1}R$. Thus, if $\frac{b}{1} \in J$, then $\frac{b}{s} \in J$. However, if since $b \in I$, $b = ax$ for some element $x \in R$. Which means that $\frac{b}{1} = \frac{a}{1}\frac{x}{1}$ for some $\frac{x}{1} \in S^{-1}R$. Thus, any element of J is generated by $\frac{a}{1}$. So, $S^{-1}R$ is a principal ideal domain.

Question 3

Show that $R = \left\{ a + b\theta \mid \theta = \frac{1+\sqrt{-19}}{2}, a, b \in \mathbb{Z} \right\}$ is not a Euclidean domain. (Hint: First, show that $N(x) = x\bar{x} = a^2 + 5b^2 + ab$ for $x = a + b\theta$ and $R^\times = \{ \pm 1 \}$. Assume that R is a Euclidean domain with ϕ. Choose $a \in R$ such that $\phi(a)$ is the smallest integer in $\{ \phi(x) \mid x \neq 0, x \notin R^\times \}$. Show that there exist no q and r such that $2 = aq + r$ with $r = 0$ or $\phi(r) < \phi(a)$)

Solution: Firstly, consider that

$$\theta^2 = \left(\frac{1 + \sqrt{-19}}{2} \right)^2 = \frac{1 + 2\sqrt{-19} - 19}{4} = \frac{-9 + \sqrt{-19}}{2} = \theta - 5$$

Then, for $x = a + b\theta$, let $N(x) = a^2 + 5b^2 + ab$, so that N is multiplicative. Let $y = c + d\theta$, then

$$\begin{aligned}
N(xy) &= N((a + b\theta)(c + d\theta)) \\
&= N((ac - 5bd) + (ad + cb + bd)\theta) \\
&= (ac - 5bd)^2 + 5(ad + cb + bd)^2 + (ac - 5bd)(ad + cb + bd) \\
&= a^2c^2 - 10abcd + 25b^2d^2 + 5a^2d^2 + 5c^2b^2 + 5b^2d^2 + 10abcd + 10b^2cd + 10abd^2 \\
&\quad + a^2cd + abc^2 - 5abd^2 - 5b^2cd - 5b^2d^2 \\
&= a^2c^2 + abcd + 25b^2d^2 + 5a^2d^2 + 5c^2b^2 + 5b^2cd + 5abd^2 + a^2cd + abc^2 \\
&= a^2c^2 + 5b^2c^2 + abc^2 + 5a^2d^2 + 25b^2d^2 + 5abc^2 + a^2cd + 5b^2cd + abcd \\
&= (a^2 + 5b^2 + ab)(c^2 + 5d^2 + cd) \\
&= N(x)N(y)
\end{aligned}$$

Note also that for any $0 \neq x \in R$, it follows that $N(x) \geq 1$ since

$$N(x) = a^2 + 5b^2 + ab = \left(a + \frac{b}{2} \right)^2 + 19 \left(\frac{b}{2} \right)^2 \geq 1$$

Moreover, $N(1) = 1$, so if $x \in R^\times$, then $N(x) = 1$. Now, if $x = a + b\theta$, then $b > 0$ implies $N(x) > 1$, and if $b = 0$, $N(x) = a^2 = 1$ only for $a = \pm 1$. So the only solutions for $N(x) = 1$ are $x = 1$ and $x = -1$. Then, it is easy to check that $-1 \cdots -1 = 1$, thus $-1 \in R^\times$. Therefore, $R^\times = \{ \pm 1 \}$

Assume for contradiction that R is a Euclidean Domain with ϕ. Then let $0 \neq a \notin R^\times$ be the element with $\phi(a)$ being smallest in the set $\{ \phi(x) \mid x \neq 0, x \notin R^\times \}$.

Note for future usage that there is no element $x \in R$ for which $N(x) = 2$ or $N(x) = 3$. This is due to the fact that if that there is, then let that element be $a + b\theta$. Now, $(a + b/2)^2 + 19(b/2)^2 \leq 3$, so $b = 0$ otherwise $19(b/2)^2 > 3$. but then there is no $a^2 = 2$ and no $a^2 = 3$ for $a \in \mathbb{Z}$, thus a contradiction.

Now, let $2 = aq + r$. If $r = 0$, then $2 = aq$. This could happen only if $N(a) = 2$ or $N(a) = 4$ since $N(2) = 4$. However, there is no element with $N(x) = 2$, so $N(a) = 4$. Now, consider $\theta = aq' + r'$. Since $N(\theta) = 5$, then $r' \neq 0$ because $N(a) \nmid N(\theta)$. But because of the minimality of a, r must be a unit. Now, $N(\theta+1) = 7$ and $N(\theta-1) = 5$ are both prime. This means that $N(a) \nmid N(\theta+1)$ and $N(a) \nmid N(\theta-1)$, so $\theta \neq aq' + r'$ for any $q', r' \in R$.

In the other case, if $r \neq 0$, then $r \in R^\times$ is forced as otherwise $\phi(r) \geq \phi(a)$. So either $1 = aq$ or $3 = aq$. However, a is not a unit, thus $1 \neq aq$ for any $q \in R$. If $3 = aq$, then $9 = N(3) = N(a)N(q)$, which is that $N(a) = 3$ or $N(a) = 9$. However, there is no element with $N(x) = 3$. So it must be the case that $N(a) = 9$. But then, consider $\theta = aq' + r'$. Notice that as $N(\theta) = 5$, then $r' \neq 0$, which means that $r' \in R^\times$. But $N(a) \nmid N(\theta+1)$ and $N(a) \nmid N(\theta-1)$, so $\theta \neq aq' + r'$ for any $q', r' \in R$.

This contradiction showed that R is not a euclidean domain.

Question 4

Let R be a domain. Show that R is a unique factorization domain if and only if every irreducible element of R is prime and R satisfies ACC on principal ideals.

Solution:
($\Longrightarrow$):

If R is a unique factorization domain, then every irreducible element of R is prime. Consider if p is an irreducible element and $p \mid xy$ for some $x, y \in R$, then $xy = pz$ for some $z \in R$. Now, as R is a unique factorization domain, write $x = ua_1 \cdots a_n$, $y = vb_1 \cdots b_m$, and $z = wc_1 \cdots c_k$ for unit u, v, w and irreducible elements $a_1, \dots, a_n, b_1, \dots, b_m, c_1, \dots, c_k$. Then,

$$(uvw^{-1})a_1 \dots a_n b_1 \dots b_m = pc_1 \cdots c_k$$

So by uniqueness of factorization, $p \sim a_i$ or $p \sim b_i$ for some i, which means either $p \mid x$ or $p \mid y$.

Next, let C be a chain of principal ideal $I_1 \subset \cdots$, and let $I_i = a_i R$ for some element $a_i \in R$. By the property of UFD, $a_1 = u_1 c_1 \cdots c_n$ for irreducible element. Then, as $aR \subset bR$ means $b \mid a$, then $a_n | a_1$ for any $n > 1$, but then $a_n = u_n c_1 \cdots c_{k_n}$ for some $0 \leq k_n \leq n$. Note that $k_n = 0$ means $a_n = u_n$

Then, let $K = \{ k_n \mid a_n = u_n c_1 \cdots c_{k_n}, \forall n \}$. Since $K \subset 0, 1, \cdots, n$, there is a minimal element by the well ordering principal, let that element be k, and $a_m = u_m c_1 \cdots c_k$. Now, if there is some $m' > m$ such that $I_{m'} \neq I_m$, then $I_m \subsetneq I_{m'}$, which means that $m' \mid m$ and $m \nmid m'$. This means that $a_{m'} = u_{m'} c_1 \cdots c_{k'}$ for some $k' < k$. This is a contradiction. Hence, $I_m = I_{m+1} = \cdots$ terminates the chain C finitely.

($\Longleftarrow$):

Let $S = \{ aR \mid a \neq 0, a \notin R^\times, a \text{ is not a product of irreducibles} \}$. If $S \neq \emptyset$, then there is a maximal element of S because every chain $C \subset S$ terminates finitely. Let bR be a maximal element of S for some $b \in R$. Then, $bR \in S$, so b is not irreducible, so $b = xy$ for some nonunit x, y. This means that $bR \subsetneq xR$ and $bR \subsetneq yR$, as if $bR = xR$, then y is a unit, and similar logic prevents $bR = yR$.

By the maximality of bR, x and y must be a product of irreducibles. Therefore, b is a product of irreducible, which gives contradiction. Therefore, $S = \emptyset$, which means that S is a factorization domain.

Now, assume that $uc_1 \cdots c_n = vd_1 \cdots d_m$ where $c_1, \dots, c_n, d_1, \dots, d_m$ are irreducible, then, they are also prime by assumption. Now, consider that c_n divides d_i for some i as they are prime, then, assume without loss of generality that $c_n \mid d_m$. Then, $uc_1 \cdots c_n = vwd_1 \cdots d_{m-1} c_n$, which is that $uc_1 \cdots c_{n-1} = vwd_1 \cdots d_{m-1}$. By induction hypothesis, $c_1 \cdots c_{n-1}$ is a unique factorization, thus $c_1 \cdots c_n$ is a unique factorization. Notice that basic case that $uc_1 = vd_1$ is unique by definition of irreducibility. Therefore, the domain is a UFD.

Question 5

Show that if the polynomial ring $R[x]$ is Noetherian, then so is R.

Solution: Let I be any ideal, then let I be generated by $G = \{ \alpha, \dots \}$ then $I' = \langle G \cup \{ x \} \rangle$ is an ideal of $R[x]$. This is because for any $f \in R[x]$ and $i \in I'$,

$$fi = f_0 i + \sum_{j=1}^{n} f_j i x^j = f_0 i + x\left(\sum_{j=1}^{n} f_j i x^{j-1}\right) = f_0 i_0 + x\left(\sum_{j=1}^{m} i_j x^{j-1} f_0 + \sum_{j=1}^{n} f_j i x^{j-1}\right) \in I'$$

as $i = i_0 + \sum_{j=1}^{m} i_j x^j$, $x \in I'$, and $i_0 \in I$.

So I' is finitely generated, thus $\{\, \alpha, \dots, x \,\}$ is finite, which means that $\{\, \alpha, \dots \}$ is finite.

Question 6

Give an example of a Noetherian ring that is not a unique factorization domain.

Solution: Consider $R = \mathbb{Z}[\sqrt{-5}] = \left\{\, a + b\sqrt{-5} \mid a, b \in \mathbb{Z} \,\right\}$. Then R is generated by 1 and $\sqrt{-5}$. Therefore, R is Noetherian since it is finitely generated. However, $6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ with 2, 3, $(1+\sqrt{-5})$, $(1-\sqrt{-5})$ be all irreducible.

Question 7

An integral domain in which every nonzero nonunit can be factored into irreducibles is called a factorization domain. Give an example of a domain that is not a factorization domain.

Solution: Let $R = \langle \{\, \sum_{i=0} a_i b_i^{r_i} \mid a_i \in \mathbb{Z}, b_i \in \mathbb{N}, r_i \in \mathbb{Q}^+ \,\} \rangle$. In other words, R is generated by the set above.

Then R is a ring by construction, which is that the result of addition, subtraction, multiplication is a part of R.

Note that $R \subset \{\, \sum_{i=0} a_i b_i^{r_i} \mid a_i \in \mathbb{Z}, b_i \in \mathbb{N}, r_i \in \mathbb{R}^+ \,\}$.

And since for $r_i \in \mathbb{Q}^+$, $b_i^{r_i}$ is algebraic in $\mathbb{R}/\mathbb{Z}$, it follows that $R \subset \{\, a \mid a \text{ is algebraic in } \mathbb{R}/\mathbb{Z} \,\}$, which is a field, then R must contain no zero divisor, thus, R is a domain.

Notice that the unit of the ring are 1 and -1 as for any $r \in R$, the exponent r_i in $\sum_{i=0} a_i b_i^{r_i}$ is always a positive real number.

Let r be irreducible, then $r \neq 1$, then $r = \sqrt{r}\sqrt{r}$ with $\sqrt{r} \notin R^\times$. Thus, r is not irreducible. Therefore, any element is not a product of irreducible elements.

Question 8

Let R be a Noetherian ring. Show that the ring $R[[x]]$ of formal power series is Noetherian.

Solution: Assume for contradiction that $R[[x]]$ is not Noetherian, thus there is a chain $I_1 \subsetneq I_2 \subsetneq \cdots$ that does not terminate. Now, consider $\phi : R[[x]] \to R$ given by $f = 0 + 0 + \cdots + a_n x^n + \cdots \mapsto a_n$ where n is the lowest term with non-zero coefficient. Then, $\phi(I_i)$ is an ideal, since if $a \in \phi(I_i)$ and $b \in R$. Then there is $f = ax^n + \cdots, g = bx^m + \cdots$ with lowest coefficient a and b, where f and g is in I_i and $R[[x]]$ respectively. So, there is polynomial $fg \in I_i$ which has lowest coefficient ab. Thus, $ab \in \phi(I_i)$. Also, if $a, b \in \phi(I_i)$, then there is $f = ax^n + \cdots, g = bx^m + \cdots$ in I_i. Then, let $n > m$ without loss of generality. It follows that $f - gx^{n-m} = a - bx^n + \cdots$ is a polynomial in I_i. Thus, $a - b \in \phi(I_i)$.

Now, let $J_i = \phi(I_i)$. Since $I_1 \subsetneq I_2 \subsetneq \cdots$, it follows that $J_1 \subseteq J_2 \subseteq \cdots$ But if chain J_i terminates at J_n, then I_i would also have to terminate. This is because

$$\phi(I_n) = \phi(I_{n+1}) = \cdots$$

Now, let $f \in I_{k+1} - I_k$ contains the lowest non-zero term $a_n x^n$, then $fx^m \in I_n$ for some m otherwise $\phi(I_k) \neq \phi(I_{k+1})$. Thus, for each of the finite generator of J_n, the polynomial with lowest nonzero coefficient being that generator has finite degree of lowest nonzero term. Finite sum of finite is finite. Thus, there can be only finitely many $I_n = I_{n+1} = \cdots = I_{n+k}$, so the chain I must stabilize at I_{n+k}.

By contradiction, $R[[x]]$ must be Noetherian.

Question 9

Let $\phi : R \to S$ be a ring homomorphism of commutative rings. Show that if R is Noetherian, then so is $\phi(R)$

Solution: Let $\phi : R \twoheadrightarrow S$ be a surjective homomorphism induced by $\phi' : R \to S'$ with $S = \operatorname{im}\phi'$. Let I be an ideal of S, and $J = \phi^{-1}(I)$ then for $x, y \in J$ and $rinR$, it follows that $\phi(x), \phi(y) \in J$ and $\phi(r) \in S$. Thus, $\phi(xy), \phi(x-y), \phi(rx)$ are elements of I. Thus, $xy, x-y, rx$ are elements of J. Thus, a preimage of an ideal is an ideal.

Now, let proceed by contraposition. If S is not Noetherian, there exists a chain $I_1 \subsetneq I_2 \subsetneq \cdots$ that does not terminate. As if $x \in \phi^{-1}(I_i)$, then $\phi(x) \in I_i$, which means $\phi(x) \in I_j$ for every $j > i$. So, $x \in \phi^{-1}(I_j)$. Moreover, if there is an element $y \notin I_i$ but $y \in I_{i+1}$, then there must be an element $x \in R$ such that $\phi(x) = y$. However, as $y \notin I_i$, $x \notin \phi^{-1}(I_i)$ but $x \in \phi^{-1}(I_{i+1})$. Thus, the chain is strict. Then,

$$\phi^{-1}(I_1) \subsetneq \phi^{-1}(I_2) \subsetneq \cdots$$

is a chain of ideal that does not terminate, which means that R must also be non-noetherian.

By contraposition, if R is noetherian, then S must be noetherian.

Question 10

a Show that if R is a domain, then so is $R[x]$

b Let F be a field. Show that there exist infinitely many monic, irreducible polynomial in $F[x]$.

Solution:

a Let R be a domain, then $R[x] = \left\{ \sum_{i=1}^{n} r_i x^i \mid r_i \in R \right\}$. Then for some $r = \sum_{i=1}^{n} r_i x^i$ and $s = \sum_{i=1}^{m} s_i x^i$, the product

$$\begin{aligned} rs &= \left(\sum_{i=1}^{n} r_i x^i\right)\left(\sum_{i=1}^{m} s_i x^i\right) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} r_i s_j x^{i+j} \\ &= \sum_{j=1}^{m}\sum_{i=1}^{n} s_j r_i x^{j+i} \\ &= \left(\sum_{i=1}^{m} s_i x^i\right)\left(\sum_{i=1}^{n} r_i x^i\right) \\ &= sr \end{aligned}$$

Thus, R is commutative.

Now consider that $0 = rs$, then

$$0 = \sum_{i=1}^{n}\sum_{j=1}^{m} r_i s_j x^{i+j} = \sum_{i=1}^{n+m}\sum_{j=0}^{i} r_j s_{i-j} x^i$$

Then if $r \neq 0$, there exists some $r_i \neq 0$. Then $\sum_{j=0}^{i} r_i s_{i-j} = 0$ which is that $s_0, \ldots, s_i$ are all 0. Now assume that there is $j > i$ such that $s_j \neq 0$. By the same argument, $r_0, \ldots, r_j$ must be all zero, but that means $r_i = 0$, contradicting that $r_i \neq r_0$. So, there must be no j such that $s_j \neq 0$. Thus, $s = 0$. Therefore, R has no zero divisor, and R is a domain.

b Since F is a field, then $F[x]$ is a principal ideal domain, and therefore, it is a unique factorization domain. If F is an infinite field, then the set $\{ (x+a) \mid a \in F \}$ is a set of monic irreducible elements. Thus, there are infinitely many monic irreducible polynomial. Otherwise, F is a finite field. In this case, assume for contradiction that there are finitely many irreducible polynomial $f_1, \ldots, f_n$. Then, $f = f_1 \cdots f_n + 1$ is an element of $F[x]$, which is a UFD. So, $f = f_i g$ for some $1 \leq i \leq n$ and polynomial $g \in F[x]$. But as $f_i \mid f_1 \cdots f_n$, it must follow that $f_i \mid 1$, which contradict that f_i is irreducible, thus a non-unit.

Therefore, there are infinitely many irreducible polynomial. Now, since $F[x]^\times = F^\times = F - \{0\}$. There are finite, say k, unit in the field, namely $I_1, \ldots, I_k$. If there is a finite number of monic irreducible polynomial, $m_1, \ldots, m_n$, then all irreducible are

$$I_1 m_1, \ldots, I_1 m_n, I_2 m_1, \ldots, I_2 m_n, \ldots, I_k m_n$$

Since if $I_1 f$ for any non-unit f results obviously to a reducible element. As the result contradicts with the fact that there are infinitely many irreducible, then there must be also infinitely many monic irreducible polynomial in $F[x]$.