Question 1

Show that every left ideal of the product $R \times S$ of two rings is a product $I \times J$ of left ideals I and J of R and S, respectively.

Solution: Let H be a left ideal of the product $R \times S$. Then, $H = A \times B$ for some set A and B. Consider $(1_R, 0) \in R \times S$, so, $(1_R, 0)(a, b) \in H$ for $(a, b \in H)$. But $(1_R, 0)(a, b) = (a, 0) \in A \times B$, implying that $a \in A$. And similarly, it is possible, by considering the product with $(0, 1_S) \in R \times S$ to concludes that $(a, b) \in H$ implies $b \in B$.

Now, considering that for any $r \in R$, $(r, s)(a, b) = (ra, sb) \in A \times B$. Therefore, $ra \in A$ and $sb \in B$. Thus, A and B are left ideals. This proves that the ideal is a product $I \times J$ of left ideals I of R and J of S

Question 2

Find all prime and maximal ideals in $\mathbb{Z}/n\mathbb{Z}$

Solution: Notice that $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring. Let $p_1^{a_1}, \dots, p_k^{a_k}$ be the prime decomposistion of n.

Firstly, notice that $p_i\mathbb{Z}/n\mathbb{Z} = \{ p_i k \mid \forall k \in \mathbb{Z}/n\mathbb{Z} \}$ is an ideal. This is because for any $a \in \mathbb{Z}/n\mathbb{Z}$, it follows that $akp_i = (ak)p_i \in p_i\mathbb{Z}/n\mathbb{Z}$. Moreover, they are prime ideal, as if $ab \in p_i\mathbb{Z}/n\mathbb{Z}$, then $p_i | ab$, which means either $p_i | a$ or $p_i | b$ because p_i is a prime number. This means that either $a \in p_i\mathbb{Z}/n\mathbb{Z}$ or $b \in p_i\mathbb{Z}/n\mathbb{Z}$

Then for any other non-zero I such that $I \neq \mathbb{Z}/n\mathbb{Z}$ and $(I, +) < (G, +)$. If there is $p_i\mathbb{Z}/n\mathbb{Z} \subset I$ and $p_j\mathbb{Z}/n\mathbb{Z} \subset I$ for $i \neq j$, then $p_i \in I$ and $p_j \in I$, so $1 = ap_i + bp_j \in I$ since $\gcd(p_i, p_j) = 1$. Thus, $I = R$. In this case, for $ap_i \in p_i\mathbb{Z}/n\mathbb{Z}$ and $bp_j \in p_j$ gives $(ap_i) \cdot (bp_j) = abp_ip_j \in (p_ip_j)\mathbb{Z}/n\mathbb{Z}$. Therefore, I cannot be prime.

And also, if for the ideal of the form, $I = p_i^r\mathbb{Z}/n\mathbb{Z}$, with $r > 1$, it would follow that p_i^{r-1} or $p_i \in I$ but neither p_i nor $p_i^{r-1} \in I$. Therefore, I is not prime.

So, the only possible prime ideal of $\mathbb{Z}/n\mathbb{Z}$ are $p_i\mathbb{Z}/n\mathbb{Z}$ for each prime divisor of n.

Note that no other I is possible as I must be an additive subgroup of R.

Now, consider any bigger ideal I that contain $p_i\mathbb{Z}/n\mathbb{Z}$, if it contains any other number not divisible by p_i, then that number must be divisible by p_j with some $j \neq i$, then $I = \mathbb{Z}/n\mathbb{Z}$ was shown. Therefore, $p_i\mathbb{Z}/n\mathbb{Z}$ are all maximal.

Lastly, since a maximal ideal must be prime, then $p_i\mathbb{Z}/n\mathbb{Z}$ are all prime ideal implies that they are all of the maximal ideals of $\mathbb{Z}/n\mathbb{Z}$.

Question 3

Let I be a proper ideal of a commutative ring R. Show that there is a maximal ideal of R containing I.

Solution: Let S be a set of all proper ideal of R that contains I, and define $\preccurlyeq$ operator as an ordering of S by set inclusion. Then, $(S, \preccurlyeq)$ is a poset.

If I is maximal, then the statment holds trivially, so assume that I is non-maximal. Given an ideal I, $I \in S$, there exists a chain $I \preccurlyeq I_1 \preccurlyeq \cdots \preccurlyeq I_k \preccurlyeq \cdots$. This is true because if there is no ideal (not neccessary maximal) that contains I, then I must be maximal by definition.

Now, consider that the union $\bigcup I_i$ is an ideal such that it contains $I, I_1, \cdots, I_k \cdots$. This is due to the fact that if $t \in \bigcup I_i$, it follows that $t \in I_i$ for some i, then for all $r \in R$, $rt, tr \in I_i$, thus $t \in \bigcup I_i$. And for $s, t \in \bigcup I_i$, it holds that $s \in I_i$ and $t \in I_j$ for some i and j. Let, without loss of generality, $i \geq j$, then $s, t \in I_i$ as $I_j \preccurlyeq I_i$, so $s \pm t \in I_i \subset \bigcup I_i$

Therefore, by zorn's lemma, there exists a maximal element M of S. That maximal element M is a proper ideal that contains I, and is not contained in any other proper ideal of R that contains I. However, any ideal that might contains M will always contains I, thus, there is no such proper ideal containing M. Therefore, M is the maximal ideal containing I by definition.

Question 4

Let I and J be ideals of a commutative ring R such that $I + J = R$. Show that $I^n + J^m = R$ for any positive integers n, m.

Solution: Consider that $I + J$ is the ideal $\{ i + j \mid i \in I, j \in J \}$. Since $I + J = R$, it follows that $1 = i + j$ for some $i \in I, j \in J$.

$$\begin{aligned}1 = 1^{n+m} = (i+j)^{n+m} &= (i^{n+m} + (n+m)i^{n+(m-1)}j + \cdots + j^{n+m}) \\ &= i^n(i^m + (n+m)i^{m-1}j + \cdots + \frac{(n+m)!}{n!m!}j^m) + j^m(j^n + \cdots + \frac{(n+m)!}{n!m!}i^n)\end{aligned}$$

Moreover, I^n and J^m are ideals as it was proven that for any ideal S, T, ST is an ideal. Then an induction can be made to argue that I^n is ideal as $I^n = I^{n-1}I$.

But $i^n \in I^n$ and $j^m \in J^m$. Therefore, $1 \in I^n + J^m$, and since $I^n + J^m$ is also an ideal, it follows that $I^n + J^m = R$

Question 5

Let S and T be multiplicative subsets of a commutative ring R. Let $\phi : R \to S^{-1}R$ be the ring homomorphism given by $r \mapsto r/1$. Show that two localizations $(ST)^{-1}R$ and $\phi(T)^{-1}(S^{-1}R)$ are isomorphic.

Solution: If $0 \in T$ or $0 \in S$, then $(ST)^{-1}R$ is a zero ring, and $\phi(T)^{-1}(S^{-1}R)$ is also a zero ring, thus they are isomorphic. Now, assume $0 \notin T$ and $0 \notin S$

Firstly, notice that as S, T are multiplicative subset, then $ST = \{ st \mid s \in S, t \in T \}$ is a multiplicative subset, as $(st)(s't') = ss'tt' \in ST$ for $st, s't' \in ST$, and $1 \in S$, $1 \in T$, so $1 \in ST$.

Notice that $S^{-1}R$ is a domain.

Consider a homomorphism $\psi : (ST)^{-1}R \to \phi(T)^{-1}(S^{-1}R)$ defined by $r/st \mapsto \frac{r/s}{t/1}$). Then, ψ is well-define since for $r'/s't' = r/st$, it follows that $u(r'st - rs't') = 0$ for some $u \in S$. But then, $\frac{r/s}{t/1} = \frac{r'/s'}{t'/1}$ because $(r/s)(t'/1) = (r/s')(t/1)$ as $rt'/s = rt/s'$ due to the fact that $u(rt's' - r'ts) = 0$ from above statment.

Next, ψ is an homomorphism because

$$\begin{aligned}\psi(r/st + r'/s't') = \psi(\frac{rs't' + r'st}{sts't'}) &= \frac{(rs't' + r'st)/ss'}{tt'/1} \\ &= \frac{rt'/s + r't/s'}{tt'/1} \\ &= \frac{r/s}{t/1} + \frac{r'/s'}{t'/1} \\ &= \psi(r/st) + \psi(r'/s't')\end{aligned}$$

shows the that addition is preserved and

$$\begin{aligned}\psi((r/st)(r'/s't')) = \psi(\frac{rr'}{ss'tt'}) &= \frac{rr'/ss'}{tt'/1} \\ &= \frac{(r/s)(r'/s')}{(t/1)(t'/1)} \\ &= \frac{r/s}{t/1}\frac{r'/s'}{t'/1} \\ &= \psi(r/st)\psi(r'/s't')\end{aligned}$$

shows that the multiplication is preserved.

Then, consider $\ker(\psi) = \left\{ r/st \mid \frac{r/s}{t/1} = 0 \right\} = \{ 0 \}$. This is due to the equivalence:

$$\begin{aligned}\frac{r/s}{t/1} = 0 &\iff \frac{r/s}{t/1} = \frac{0}{1} \\ &\iff \exists u \mid u(\frac{r}{s}) = 0 \\ &\iff 0 \in \phi(T) \vee \frac{r}{s} = 0 \quad \text{ as } S^{-1}T \text{ is a domain} \\ &\iff \exists u' \in S \mid u'r = 0 \text{ since } 0 \notin \phi(T) \\ &\iff \exists u' \mid u'r = 0 \iff \frac{r}{st} = 0\end{aligned}$$

And consider that ψ is surjective as for any element $\frac{r/s}{t/1} = \psi(r/st)$ and $r/st \in (ST)^{-1}R$, there is a corresponding element in the domain that maps to that desired element. Thus, by the first ring isomorphism theorem,

$$(ST)^{-1}R \simeq \phi(T)^{-1}(S^{-1}R)$$

Question 6

Let I be an ideal of a commutative ring R. Prove that

$$\operatorname{rad} I := \left\{ r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}^+ \right\}$$

is an ideal containing I. Prove also that $(\operatorname{rad} I)/I$ is an ideal of nilpotent elements of the factor ring R/I.

Solution: If $i \in \operatorname{rad} I$, and let $i^n \in I$, it follows that $(ri)^n = r^n i^n \in r^n I = I$, therefore, $ri \in \operatorname{rad} I$. Moreover, for $i, j \in \operatorname{rad} I$, with $i^n \in I$ and $j^m \in J$, it follows that

$$(i-j)^{n+m} = i^{n+m} + (n+m)i^{n+m-1}j + \cdots + j^{n+m} = i^n(i^m + \cdots + \frac{(m+n)!}{n!m!}j^m) + (\pm\frac{(m+n)!}{n!m!}i^n \cdots \pm j^n)j^m \in I$$

So, $i - j \in \operatorname{rad} I$. Hence, $\operatorname{rad} I$ is an ideal.

Now, consider if $i \in I$, then $i^n = i(i^{n-1}) \in I$, so $i \in \operatorname{rad} I$. Thus $\operatorname{rad} I$ is and ideal that contains I.

Since I is an ideal of R then it must be an ideal of $\operatorname{rad} I$. Then $\operatorname{rad} I/I \subset R/I$ as subgroup because $\operatorname{rad} I \subset R$. Consider $d + I \in \operatorname{rad} I/I$, for some $d \in \operatorname{rad} I$ and $r + I \in R/I$ for some $r \in R$. Now, notice that $(d+I)(r+I) = (rd+I)$ as I is an ideal. And since $\operatorname{rad} I$ is an ideal, it follows that $rd \in \operatorname{rad} I$, which is that $(rd + I) \in \operatorname{rad} /I$. Therefore, $\operatorname{rad} I/I$ is an ideal of R/I.

Question 7

Let M be a maximal ideal of a commutative ring R. Prove that the quotient ring R/M^n is local for any $n \geq 1$.

Solution: Assume that there is a maximal ideal N of R such that $N \neq M$ and N contains M^n. Then, as N is a prime ideal and $m^n \in N$ for all $m \in M$, it must follow that $m^{n-1}m \in N$, which is $m^{n-1} \in N$. Since n is finite and $n - 1 < n$, it is possible to conclude that $m \in N$. Therefore, $M \subset N$. But this yield a contradiction, therefore, there must be no such $N \neq M$ that contains M^n.

Consider a map $\phi : R \to R/M^n$ given by $\phi : x \mapsto x + M^n$ which is a homomorphism. The kernel of the map is $\ker \phi = M^n$. Then if I is an ideal of R, then for $i \in I$ and $r \in R$, it follows that $\phi(ir) = \phi(i)\phi(r)$. So, $\phi(I)$ is an ideal. And conversely, if I is an ideal of R/M^n, then the preimage $\phi^{-1}(I) = \{ i + m \mid i \in I, m \in M^n \}$ is an ideal as $r(i+m) = ri + rm = \phi^{-1}(ri) \in \phi^{-1}(I)$.

This shows that there is a bijection between the set of ideal of R/M^n and ideal of R containing M^n.

Moreover, consider if $\phi(I)$ is a maximal ideal of R/M^n and there is a proper ideal $J > I$ of R. Then let $j \in J - I$. So, $\phi(j)$ must be in ideal $\phi(J)$ of R/M^n but not in $\phi(I)$. Since $\phi(I)$ is maximal, then $\phi(J)$ must be the whole ring R/M^n. However, J is a proper ideal of R, so there is $r \in R - J$. And $\phi(r) \notin \phi(J)$, which contradicts that $\phi(J)$ is the whole ring. Therefore, I must be maximal.

The contraposition yields that if I is not maximal, then $\phi(I)$ cannot be maximal.

However, there is a unique maximal ideal of R containing M^n, therefore, there cannot be two maximal ideals in the ring R/M^n. As there is a unique maximal element of R/M^n, it is local.

Question 8

Let F be a field. Define the ring $F((x))$ of formal Laurant series by

$$F((x)) = \left\{ \sum_{n \geq N}^{\infty} a_n x^n \mid a_n \in F \text{ and } N - 1 \in \mathbb{Z} \right\}$$

Prove that the field of fractions of $F[[x]]$ is $F((x))$. Prove also that the field of fractions of the power series ring $\mathbb{Z}[[x]]$ is properly contained in the field of formal Laurant series $\mathbb{Q}((x))$.

Solution: Firstly, notice that a unit in $F[[x]]$ is any element such that the constant term is non-zero. As if that is the case, then

$$(a_0 + a_1 x + \cdots)(a_0^{-1} + a_0^{-2} a_1 x + \cdots) = 1$$

But if the constant term is zero, then the element can be written as $x^k(a_k + a_{k+1}x + \cdots)$ Which means that the product

$$x^k(a_k + a_{k+1}x + \cdots)b(x) = x^k c(x) \neq 1$$

for some $b, c \in F[[x]]$

As there is a natural embedding (injective) of $F[[x]] \to F((x))$ defined by $f \mapsto f$. Consider an element $p'(x) = \sum_{i=0}^{\infty} p_i x^i$ and $q'(x) = \sum_{i=0}^{\infty} q_i x^i \neq 0$ are elements of $F[[x]]$, and their corresponding elements $p(x), q(x) \in F((x))$. Now, rewrite $q(x)$ in the form of $x^k(a_k + a_{k+1}x + \cdots)$ where a_k is non-zero, as $q(x)$ is non-zero. Then, as $(a_k + a_{k+1}x + \cdots)$ is invertible, and $(x^k)^{-1} = x^{-k}$, it follows that

$$\frac{p(x)}{q(x)} = p(x) \cdot x^{-k}(a_k + a_{k+1}x + \cdots)^{-1} = x^{-k} f(x)$$

for some $f(x)$ being an embedding of $f'(x) \in F[[x]]$. By rewriting,

$$\frac{p(x)}{q(x)} = \sum_{i=-k}^{\infty} f_{i+k} x^i$$

Thus, a fraction of any element in $F[[x]]$ can be written as an element in the ring $F((x))$.

As $F((x))$ is a ring of Laurant series, it has closure of addition and multiplication, thus, the fraction of $F[[x]]$ is the ring $F((x))$.

Next, since there is a natural homomorphism $\mathbb{Z}[[x]] \to \mathbb{Q}[[x]]$ given by $x \mapsto \frac{x}{1}$ that is injective. Then the fraction of $\mathbb{Z}[[x]]$ must be contained in the fraction of $\mathbb{Q}[[x]]$, which is $\mathbb{Q}((x))$.

Question 9

Find all idempotents in $\mathbb{Z}/p^n\mathbb{Z}$, where p is a prime integer and $n \geq 1$. Find also the number of idempotents of $\mathbb{Z}/n\mathbb{Z}$.

Solution: Consider an element $a \in \mathbb{Z}/p^n\mathbb{Z}$ such that $a^2 = a$. Clearly, $0^2 = 0$ and $1^2 = 1$. Apart from that, $a^2 \equiv a \pmod{p^n}$, which implies $a(a-1) \equiv 0 \pmod{p^n}$. But as a and $(a-1)$ are coprime, then $p^n \mid a$ or $p^n \mid a-1$, which yields two solutions. If $p^n \mid a$, then $a = 0$, otherwise, a $= 1$ (in $\mathbb{Z}/p^n\mathbb{Z}$). Thus, only 0 and 1 are the idempotents of $\mathbb{Z}/p^n\mathbb{Z}$

For $\mathbb{Z}/n\mathbb{Z}$. Write $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ for distinct prime p_i. Then, consider the system

$$\begin{aligned} a(a-1) &\equiv 0 \pmod{p_1^{k_1}} \\ a(a-1) &\equiv 0 \pmod{p_2^{k_2}} \\ &\cdots \\ a(a-1) &\equiv 0 \pmod{p_m^{k_m}} \end{aligned}$$

Where each congruence equation yields two solutions. Thus, as $p_1^{k_1}, p_2^{k_2}, \ldots, p_m^{k_m}$ are pairwise relatively prime, then by the chineses remainder theorem, one can construct $a(a-1) \equiv 0 \pmod{n}$ in 2^m ways.

Therefore, there are 2^m idempotents in $\mathbb{Z}/n\mathbb{Z}$

Question 10

Let $f_1(x), f_2(x), \ldots f_k(x)$ be polynomials with integer coefficients of the same degree d. Let $n_1, n_2, \ldots, n_k$ be integers which are relatively prime in pairs (ie. $\gcd(n_i, n_j) = 1$ for all $i \neq j$). Use the Chinese Remainder Theorem to prove that there exists a polynomial $f(x)$ with integer coefficients of degree d with

$$f(x) \equiv f_1(x) \pmod{n_1}, \quad f(x) \equiv f_2(x) \pmod{n_2}, \quad \ldots, \quad f(x) \equiv f_k(x) \pmod{n_k}$$

ie. the coefficients of $f(x)$ agree with the coefficients of $f_i(x) \pmod{n_i}$. Show that if all the $f_i(x)$ are monic, then $f(x)$ may also be chosen monic.

Solution: For polynomials with degree $d = 0$, the statement is holds trivially as it resembles the chinese remainder theorem. Now, assume for induction that the statement holds for any polynomials of degree d.

Let $g_1(x), g_2(x), \ldots, g_k(x)$ be polynomials of degree $d+1$, then $g_i(x) = a_i x^{d+1} + f_i(x)$ for some $f_i(x)$ being a degree d polynomial. Since $f_i(x)$ are degree d, then there is a degree d polynomial $f(x)$ satisfying that

$$f(x) \equiv f_1(x) \pmod{n_1}, \quad f(x) \equiv f_2(x) \pmod{n_2}, \quad \ldots, \quad f(x) \equiv f_k(x) \pmod{n_k}$$

by the induction hypothesis.

Now, as $n_1, \ldots, n_k$ are coprime, then there exists a such that

$$a \equiv a_1 \pmod{n_1}, \quad a \equiv a_2 \pmod{n_2}, \quad \ldots, \quad a \equiv a_k \pmod{n_k}$$

by the chinese remainder theorem.

By multiplying x^{d+1} gives

$$ax^{d+1} \equiv a_1 x^{d+1} \pmod{n_1}, \quad ax^{d+1} \equiv a_2 x^{d+1} \pmod{n_2}, \quad \ldots, \quad ax^{d+1} \equiv a_k x^{d+1} \pmod{n_k}$$

Which, upon setting $g(x) = ax^{d+1} + f(x)$ gives

$$g(x) \equiv g_1(x) \pmod{n_1}, \quad g(x) \equiv g_2(x) \pmod{n_2}, \quad \ldots, \quad g(x) \equiv g_k(x) \pmod{n_k}$$

Therefore, the statement holds generally by induction.

Now, if $g_1(x), \ldots g_k(x)$ are all monic of degree d, then consider that there is $f(x)$ of degree $d-1$ that satisfies the condition for all $f_i(x) = g_i(x) - x^d$. Then $g(x) = x^d + f(x)$ satisfies the condition, and is monic. Therefore, if all the functions $g_i(x)$ are monic, the $g(x)$ can be chosen to be monic.