ALGEBRA

RIPAN DAS

Contents

1. Relation

1.1. **Introduction.**

Definition 1.1. *Let A, B be two set, we define Cartesian product of two set as*

$$A \times B := \{(a, b) : a \in A, b \in B\}.$$

Let S be an non-empty set, a binary relation R is a subset of $S \times S$. Let $\rho \subseteq S \times S$. ρ is said to be $reflexive$ if $(a, a) \in \rho \ \forall a \in S$. ρ is said to be *symmetric* if $(a, b) \in \rho \Rightarrow (b, a) \in \rho$ and ρ is said to be *transitive* if $(a, b), (b, c) \in \rho \Rightarrow (a, c) \in \rho$. A relation ρ is said to be equivalence relation if ρ is $reflexive$, *symmetric* and *transitive*. ρ is said to be *antisymmetric* if $(a, b), (b, a) \in \rho \Rightarrow a = b$. A relation ρ is said to be partial ordered relation if ρ is $reflexive$, *antisymmetric* and *transitive*.

Definition 1.2. *Let S be an non-empty set. Let $\{P_\alpha\}_{\alpha\in\Lambda}$ be a collection of subsets of S, i.e. $P_\alpha \subseteq S \ \forall \alpha \in \Lambda$ such that*
(a) $P_\alpha \cap P_\beta = \emptyset \ \forall \alpha \neq \beta$ in Λ,
(b) $\cup_{\alpha\in\Lambda} P_\alpha = S$.
Then the collection $\{P_\alpha\}_{\alpha\in\Lambda}$ is called the partition of S.

Let S be an non-empty set, and $\{P_\alpha\}_{\alpha\in\Lambda}$ be a partition of S. $a, b \in S$ define a relation $\sim$ on S, $a \sim b$ iff $\exists\ \alpha \in \Lambda$ such that $a, b \in P_\alpha$ (check $\sim$ is an equivalence relation).
Suppose S be an non-empty set and " $\sim$ " $\subseteq S \times S$ be an equivalence relation on S. For $x \in S$ $cl(x) = \{y \in S | x \sim y\}$ is a subset of S. If $x \sim x'$ then $cl(x) = cl(x')$. Let $y \in cl(x) \Rightarrow x \sim y$. Now $x \sim x'$ is given $\Rightarrow x' \sim x$ (as $\sim$ is symmetric). $x' \sim x$ and $x \sim y \Rightarrow x' \sim y \Rightarrow y \in cl(x')$. Therefore $cl(x) \subseteq cl(x')$. Now $y \in cl(x)$ then $x' \sim y$, $x \sim x'$ is given $\Rightarrow x \sim y$ (as $\sim$ is transitive), $\Rightarrow y \in cl(x)$ $\Rightarrow cl(x') \subseteq cl(x) \Rightarrow cl(x) = cl(x')$. Note that $cl(x) = cl(x')$, now $x \sim x' \Rightarrow x \in cl(x) = cl(x')$ $\Rightarrow x \in cl(x') \Rightarrow x \sim x'$.
Observation: $cl(x) \cap cl(x') = \emptyset$ iff $x \nsim x'$ suppose $x \nsim x'$; if $y \in cl(x) \cap cl(x')$ then $x \sim y$ and $x' \sim y \Rightarrow x \sim x'$, contradiction.
Next we want to show $cl(x) \cap cl(x')$ then $x \nsim x'$. If $x \sim x'$ then we have proved $cl(x) = cl(x')$. Now $x \in cl(x) \cap cl(x')$ so $cl(x) \cap cl(x') \neq \emptyset$. Therefore $\mathfrak{F} = \{cl(x) | x \in S$ and distinct class$\}$ forms a partition of S. E.g. Take the set $S = \mathbb{Z}$, fix $n \in \mathbb{Z}$, define $\sim \subseteq \mathbb{Z} \times \mathbb{Z}$ as $a \sim b$ iff $n | b - a$. Check that $\sim$ is an equivalence relation.

2. Mappings

Definition 2.1. *Let A, B be two non empty sets. $f : A \to B$ is said to be mapping if $f \subseteq A \times B$ and for each $x \in A$ $\exists!\ y \in B$ such that $(a, b) \in f$.*

Example 2.2. *$A = \{1, 2, 3\}$ and $B = \{x, y, z, w\}$, consider $\rho = \{(1, x), (2, y), (3, w)\}$, $\sigma = \{(1, x), (2, x), (3, w)\}$, $\tau = \{(1, x), (1, y)(2, x), (3, z)\} \subseteq A \times B$ then ρ, σ is a mapping where τ is not.*

Notation: Let $f : A \to B$ be a mapping and $(x, y) \in f \subseteq A \times B$ then we write $y = f(x)$ called the image of x. A is called the domain and B is codomain. Let $f : A \to B$ be a mapping, $X \subseteq A$ then $g := f|_X : X \to B$ be also a mapping. $f|_X$ is called the restriction of f on X.

Definition 2.3. *Let $f : A \to B$ be a mapping, f is said to be injective if $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$, contra-positively stated if $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.*

Definition 2.4. *A mapping $f : A \to B$ is said to be surjective if for each $y \in B$ $\exists$ $x \in A$ such that $f(x) = y$. f is said to be bijective iff f is injective and surjective.*

Observation: Let A, B be two sets and $\mathcal{F} = \{f : A \to B\}$ be the collection of all mapping from A to B, then $|\mathcal{F}| = |B|^{|A|}$, i.e., B^A denote the functions from A to B. If, $|A| = n$, $|B| = m$ and $n \leq m$, number of injective map from A to B is $m(m-1)\cdots(m-(n-1)) = \dfrac{m!}{(m-n)!}$

Composition of two mapping: Let $f : A \to B$ and $g : B \to C$ be two mapping, define $g \circ f : A \to C$ as $(g \circ f)(x) = g(f(x))$.

Theorem 2.5. *Let $f : A \to B$ and $g : B \to C$ be two mapping. If f, g are injective then $g \circ f$ is also injective. Conversely, if $g \circ f : A \to C$ is injective then f is injective.*

Proof. Suppose f, g are injective map, then $x_1, x_2 \in A$, now $g(f(x_1)) = g(f(x_2))$ since f is injective, $g(x_1) = g(x_2)$, now injectivity of g implies $x_1 = x_2$ hence $g \circ f$ is injective. Now, $g \circ f$ is injective, pick $x_1, x_2 \in A$, $f(x_1) = f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2))$ since $g \circ f$ is injective $\Rightarrow x_1 = x_2$. □

Theorem 2.6. *Let, $f : A \to B$ and $g : B \to C$ be two mapping. If f, g are surjective then $g \circ f$ is also surjective. Conversely, if $g \circ f : A \to C$ is surjective then g is surjective.*

Proof. Suppose f, g are surjective. Let $z \in C$, $\exists$ $y \in B$ such that $g(y) = z$, for this $y \in B$ $\exists$ $x \in A$ such that $f(x) = y \Rightarrow (g \circ f)(x) = g(f(x)) = g(y) = z \Rightarrow x$ is a preimage of z, hence $g \circ f$ is surjective. Suppose $g \circ f$ is surjective. Let $z \in C$ $\exists$ $x \in A$ such that $(g \circ f)(x) = z$. Let $y = f(x)$ $\Rightarrow g(y) = z$, hence g is surjective. □

Theorem 2.7. *Let, $f : A \to B$ and $g : B \to C$ be two mapping. If f, g are bijective then $g \circ f$ is also bijective. Conversely, if $g \circ f : A \to C$ is bijective then we can only say that f is injective and g is surjective.*

Proof. Suppose f, g are bijective then $g \circ f$ is injective and surjective so $g \circ f$ is bijective. Again, $g \circ f$ is bijective, then $g \circ f$ is injective so f is injective, $g \circ f$ is surjective so g is surjective. □

Definition 2.8. *Let $f : A \to B$ be a mapping. If there exists $g : B \to A$ such that $g \circ f : A \to A$, $g \circ f = id_A$ and $f \circ g : B \to B$, $f \circ g = id_B$, then we say that f is invertible and g is an inverse of f.*

Notation: $g = f^{-1}$

Theorem 2.9. *Suppose $f : A \to B$ be an invertible map. Then f has unique inverse.*

Proof. Suppose $g_1 : B \to A$ and $g_2 : B \to A$ be two inverses of f. We have $g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2$ $\Rightarrow (g_1 \circ id_B) = (id_A \circ g_2) \Rightarrow g_1 = g_2$. □

Observation: Let $f : A \to B, g : B \to C$ and $h : C \to D$ be three mappings, then $(h \circ g) \circ f : A \to D$ and $h \circ (g \circ f) : A \to D$ are the same mapping. Pick $x \in A$. $(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x)))$. On the other hand, $(h \circ (g \circ f))(x) = h(g \circ f(x)) = h(g(f(x)))$. $\therefore$ $(h \circ g) \circ f = h \circ (g \circ f)$, i.e., mapping composition is associative.

Theorem 2.10. *Let $f : A \to B$ be a mapping. f is invertible iff f is a bijection. In this case f^{-1} is also a bijection.*

Proof. $f : A \to B$ be a mapping. If there exists $g : B \to A$ such that $g \circ f = id_A$ and $f \circ g = id_B$ then we say that f has an inverse. Because identity mapping is a bijective mapping, so in case of $g \circ f$, f is an injective mapping and in case of $f \circ g$, f is surjective. Hence f is bijective. Similar argument shows that g is also bijective.

Definition 2.11. *A set A is said to be finite if it is empty or there exists a bijection from A to the set $J_n = \{1, \cdots, n\}$ for some natural number n.*

Observation: Suppose $S = \{x_1, \cdots, x_n\}$ be a finite set, if $f : S \to S$ is injective then f is surjective. $f(S) = \{f(x_1), \cdots, f(x_n)\}$. Suppose f is injective then $f(x_i) = f(x_j) \Rightarrow x_i = x_j$. Therefore, $| f(S) | = n$. Now $f(S) \subseteq S$ and $| S | = n \Rightarrow f(S) = S$ (as S is finite) $\Rightarrow f$ is surjective. If f is surjective then for each $y \in S$, $f^{-1}(y) \neq \emptyset$. If $|f^{-1}(y)| > 1$ (for some y) we arrive a contradiction that $|S| > |S|$ (since S is finite). $\therefore |f^{-1}(y)| = 1 \ \forall \ y \in S$ and $f^{-1}(y_1) \cap f^{-1}(y_2) = \emptyset \ \forall \ y_1, y_2 \in S$ otherwise $|S| < |S| \Rightarrow f$ is injective.

Remark 2.12. *A map f on a finite set S is injective iff it is surjective.*

Lemma 2.13. *Let $a_0 \in A$. Then there exists a bijection $f : A \to J_{n+1}$ iff there exists a bijection $g : A \setminus \{a_0\} \to J_n$.*

Proof. Suppose there exists a bijection $g : A \setminus \{a_0\} \to J_n$. We define $f : A \to J_{n+1}$ by

$$f(x) = \begin{cases} g(x), & \text{if } x \in A \setminus \{a_0\} \\ n+1, & \text{if } x = a_0 \end{cases}$$

Then clearly f is a bijection. Conversely, Suppose there exists a bijection $f : A \to J_{n+1}$. If $f(a_0) = n + 1$ then the required function g is $f\Big|_{A\setminus\{a_0\}}$. If $f(a_0) \neq n + 1$, let $f(a_o) = m$ where $1 \leq m \leq n$. As f is surjective so there exists $a_1 \in A \setminus \{a_0\}$ such that $f(a_1) = n + 1$. Define, $h : A \to J_{n+1}$ by

$$\begin{aligned} h(a_0) &= n+1 \\ h(a_1) &= m \\ h(x) &= f(x) \quad \text{if } x \in A \setminus \{a_0, a_1\} \end{aligned}$$

Then clearly h is a bijection and so the required g is $h\Big|_{A\setminus\{a_0\}}$. □

Lemma 2.14. *Let $f : A \to J_n$ be a bijection. Let $B \subsetneq A$. Then there doesn't exists any bijection $g : B \to J_n$ but there exists a bijection $g : B \to J_m$ for some $m < n$ provided $B \neq \emptyset$.*

Proof. If $B = \emptyset$ then there is nothing to prove. So we assume $B \neq \emptyset$ and we prove it by induction. If $n = 1$ then A is singleton and so $B = \emptyset$. Thus there exists no bijection $g : B \to J_1$. Next we assume that this statement holds for $n = k$ and prove it for $n = k + 1$. Suppose, $f : A \to J_{k+1}$ be a bijection and B is a non-empty proper subset of A. Let $b_0 \in B$ and $a_0 \in A \setminus B$. Then by previous

lemma there exists a bijection $g : A \setminus \{b_0\} \to J_k$. Now, $B \setminus \{b_0\}$ is a proper subset of $A \setminus \{b_0\}$ and so by induction hypothesis,

(1) there exists no bijection $h : B \setminus \{b_0\} \to J_k$,
(2) either $B \setminus \{b_0\} = \emptyset$ or there is a bijection $h' : B \setminus \{b_0\} \to J_m$ for some $m < k$.

By previous lemma and (1) there is no bijection from B to J_{k+1}. If $B \setminus \{b_0\} = \emptyset$ then there exists a bijection from B to J_1. If $B \setminus \{b_0\} \neq \emptyset$ then by lemma 2.13 and (2) there is a bijection from B to J_{m+1}. Thus there is a bijection from B to J_p with $p < k + 1$. Hence, by principle of induction the result follows. □

Corollary 2.15. *If A is a finite then there is no bijection of A with a proper subset of itself.*

Proof. If possible there is a bijection $f : A \to B$ where $B \subsetneq A$. By definition, there is a bijection $g : A \to J_n$ for some $n \in \mathbb{N}$. Then the map $g \circ f^{-1} : B \to J_n$ is a bijection. This contradicts the previous lemma. □

Corollary 2.16. *The numbers of elements in a finite set A is uniquely determined by A.*

Proof. If possible let there are two different bijection $f : A \to J_n$ and $g : A \to J_m$ where $m < n$ then $J_m \subsetneq J_n$ and $f \circ g^{-1} : J_m \to J_n$ is a bijection. This contradicts lemma 2.14. □
Thus we conclude that a subset of a finite set is finite.

Theorem 2.17. *Let $A \neq \emptyset$ and $n \in \mathbb{N}$. Then the following are equivalent:*

(1) *There is a surjective function $f : J_n \to A$,*
(2) *There is a injective function $g : A \to J_n$,*
(3) *A is finite and has at most elements.*

Proof. (1) $\Rightarrow$ (2) Given $f : J_n \to A$ which is surjective. We define $g : A \to J_n$ as follows: For $a \in A, \exists m \in J_n$ such that $f(m) = a$. Out of all such m's choose the smallest one sat m_a. We write $g(a) = m_a$. So g is well defined by Well ordering principle of $\mathbb{N}$. Let $a, b \in A$ and $a \neq b$ then $g(a) \neq g(b)$ otherwise $m_a = m_b$ but $f(m_a) \neq f(m_b)$ which contradicts the fact that f is mapping. Therefore, g is surjective.
(2) $\Rightarrow$ (3) Give $g : A \to J_n$ which is injective. Then $g : A \to g(A) \subsetneq J_n$ is a bijection. Now, there exists a bijection $h : g(A) \to J_m$ for some $m \leq n$. So, $h \circ g : A \to J_m$ is a bijection. Thus A is finite and has at most m elements.
(3) $\Rightarrow$ (1) Let A has m elements where $1 \leq m \leq m$. Then there is a bijection $g : A \to J_m$. If $m = n$ then $g^{-1} : J_m \to A$ is a surjection. If $m < n$ then define $f : J_n \to A$ by

$$f(k) = \begin{cases} g^{-1}(k), & \text{if } 1 \leq k \leq m \\ g^{-1}(1), & \text{if } m < k \leq n \end{cases}$$

Then f is a surjection. □

Definition 2.18. *A set A is said to be infinite if it is not finite. A is said to be countably infinite if there is a bijection between A and $\mathbb{N}$.*

Definition 2.19. *A set A is said to be countable if it is either finite or countably infinite. A set that is not countable is said to be uncountable.*

Theorem 2.20. *There is a bijection from J_m onto J_n iff $m = n$.*

Proof. Suppose, $f : J_m \to J_n$ is a bijection. Then $m \leq n$. Again, $f^{-1} : J_n \to J_m$ is a bijection, then $n \leq m$. So, $m = n$. Converse part is trivial. □

Theorem 2.21. *Every subset of $\mathbb{N}$ is countable.*

Proof. Let $A \subseteq \mathbb{N}$. If $A = \emptyset$ or contains finite number of elements then A is finite and so countable. Suppose, A be not finite then we want to show that there is a bijection between A and $\mathbb{N}$. We define f by induction as follows:

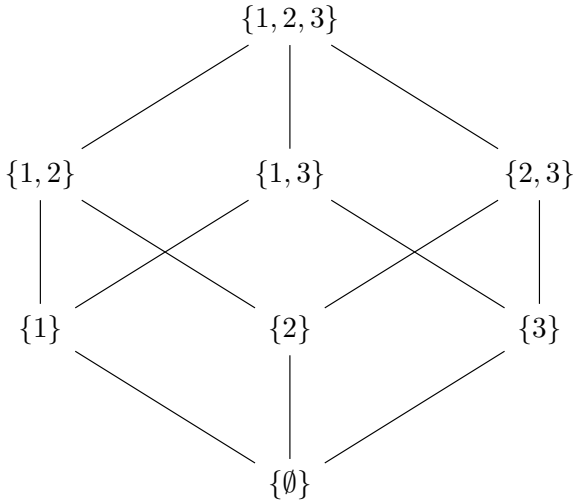
$$f(1) = \text{smallest element of } A$$

This choice is possible for well ordering principle of $\mathbb{N}$. Suppose, $f(1), f(2), \cdots f(k)$ are all defined then define $f(k+1) =$ smallest element of $A \setminus \{f(1), \cdots, f(k)\}$. Note that $A \setminus \{f(1), \cdots, f(k)\} \neq \emptyset$ otherwise A is finite as $f : \{1, \cdots, k\} \to A$ is bijective. Thus $f(n)$ is defined for all $n \in \mathbb{N}$. By definition $f : \mathbb{N} \to A$ is injective. We next show that f is surjective. Let $a \in A$ be any element. By the injectivity of f, we have $f(\mathbb{N}) \nsubseteq \{1, \cdots, a\}$ then $\exists\ m_0 \in \mathbb{N}$ such that $f(m_0) > a$. Let $S = \{n \in \mathbb{N} : f(n) \geq a\}$ then $m_0 \in S$ and so $S \neq \emptyset$. Hence S has a least element say $m_a, f(m_a) \geq a$ then $\forall\ n < m_a$ we have $f(n) < a \Rightarrow a \notin \{f(1), \cdots, f(m_a - 1)\}$. By definition $f(m_a)$ is the smallest element of $A \setminus \{f(1), \cdots, f(m_a - 1)\} \Rightarrow f(m_a) \leq a$, so $f(m_a) = a$ and f is surjective. Thus f is bijective so A is countably infinite. □

Theorem 2.22. *Let $A \neq \emptyset$. Then the followings are equivalent:*

(1) *There exists a surjection $f : \mathbb{N} \to A$,*
(2) *There exists an injection $g : A \to \mathbb{N}$,*
(3) *A is countable.*

Proof.



3. Cardinal and Ordinal

4. Group theory

Definition 4.1. *Let G be a non-empty set. $\circ : G \times G \to G$ be a binary operation on G such that*
(i) $a \circ b \in G \ \forall a, b \in G$
(ii) $a \circ (b \circ c) = (a \circ b) \circ c \ \forall a, b, c \in G$ *i.e., $\circ$ is associative*
(iii) $\exists\ e_G \in G$ *such that* $a \circ e_G = e_G \circ a = a \ \forall\ a \in G$, e_G *called identity element of* G
(iv) for each $a \in G \ \exists\ a^{-1} \in G$ *such that* $a \circ a^{-1} = a^{-1} \circ a = e_G$ a^{-1}*) is called inverse element of* a
Then $(G, \circ)$ is called a group.

Example 4.2. (1) *Show that $(\mathbb{Z}, +)$ is a group where $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $(a, b) \mapsto a + b$*
(2) *Show that $(\mathbb{Z}, .)$ is not a group where $. : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $(a, b) \mapsto ab$*
(3) *Show that $(\mathbb{N} \cup \{0\}, +)$ is not a group where $+ : \mathbb{N} \cup \{0\} \times \mathbb{N} \cup \{0\} \to \mathbb{N} \cup \{0\}$ defined by $(a, b) \mapsto a + b$. Example $2, 3$ are called semi-group.*
(4) *A group is said to be finite group if the underlying set G is finite. Consider the set $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \cdots, \overline{n-1}\}$, set of all reduced residue class of n i.e., set of remainders upon dividing by n. Then $\mathbb{Z}/n\mathbb{Z}$ form a group under addition defined as $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $(\overline{a}, \overline{b}) \mapsto \overline{a+b}$. Check that $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group. Try to find more finite group.*
Define, $M_n(\mathbb{R}) = \{A_{n\times n} |\ A = (a_{ij})_{n\times n},\ (a_{ij}) \in \mathbb{R}\}$
$GL_n(\mathbb{R}) = \{A_{n\times n} \in M_n(\mathbb{R} |\ det(A) \neq 0\}$
Check that whether the followings are group or not:
(5) $(M_n(\mathbb{R}), +)$, (6) $(M_n(\mathbb{R}), .)$, (7) $(GL_n(\mathbb{R}), +)$, (8) $(GL_n(\mathbb{R}), .)$

Theorem 4.3. *Let, $(G, \circ)$ be a group, then identity element is unique.*

Proof. Let e_G and e'_G be two identity element. $e'_G \circ e_G = e'_G$ (by property of e_G) and $e'_G \circ e_G = e_G$ (by property of e'_G). Therefore, $e_G = e'_G$. □

Theorem 4.4. *Let, $(G, \circ)$ be a group, then inverse of an element is unique.*

Proof. Let a' and a'' be two inverses of a. $a' \circ (a \circ a'') = (a' \circ a) \circ a'' \Rightarrow a' \circ e_G = e_G \circ a'' \Rightarrow a' = a''$ □

4.1. Sub-Group.

Definition 4.5. *Let G be a group with respect to $\circ$, Let $H \subseteq G$ such that $(H, \circ|_{H\times H} : H \times H \to H)$ is a group, then H is called the subgroup of G.*

Notation: $H < G$

Example 4.6. *Consider the group $(\mathbb{Q}, +)$. Now $\mathbb{Z} \subseteq \mathbb{Q}$. Consider $+|_{\mathbb{Z}\times\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. $(\mathbb{Z}, +|_{\mathbb{Z}\times\mathbb{Z}})$ forms a group then $\mathbb{Z} < \mathbb{Q}$.*

Theorem 4.7. *Let $(G, \circ)$ be a group and $H < G$ iff $x, y \in H \Rightarrow y^{-1}x \in H$.*

Proof. $y, y \in H \Rightarrow y^{-1}y \in H \Rightarrow e \in H$. Pick $y \in H$ and $e \in H \Rightarrow y^{-1}e \in H \Rightarrow y^{-1} \in H$. $y, x \in H$ $\Rightarrow y, x^{-1} \in H \Rightarrow (x^{-1})^{-1}y \in H \Rightarrow xy \in H$. H is closed under multiplication. $\circ$ is associative on G then $\circ$ is associative on H. So, H is a subgroup of G. Conversely, If $H < G$ then $x, y \in H$ $\Rightarrow x, y^{-1} \in H \Rightarrow y^{-1}x \in H$. □

Theorem 4.8. *Let $(G, \circ)$ be a group. $H \subseteq G$, H is a subgroup of G iff (a) $x, y \in H \Rightarrow xy \in H$ and (b) $x \in H \Rightarrow x^{-1} \in H$.*

Proof. To show that H is a subgroup of G, it is enough to show that $e \in H$. Given, $x \in H \Rightarrow x^{-1} \in H$ so that $x \cdot x^{-1} \in H \Rightarrow e \in H$. Conversely, H is a subgroup of G then $x, y \in H \Rightarrow xy \in H$, H is closed under multiplication. Since H is a subgroup of G an element $x \in H \Rightarrow x^{-1} \in H$. □

4.2. **Symmetric Group.** Let S be a set and $S \neq \emptyset$, define

$$A(S) = \{f : S \to S : f \text{ is bijection}\}$$

Now,

$$\begin{aligned} \circ : A(S) \times A(S) &\to A(S) \\ (f, g) &\mapsto f \circ g \end{aligned}$$

Then it is easy to check that $A(S)$ is a group under mapping composition. Let $S = \{1, \cdots, n\}$ then we denote $A(S)$ by S_n. Therefore,

$$S_n = \{f : \{1, \cdots, n\} \to \{1, \cdots, n\} : f \text{ is bijection}\}$$

If $f \in S_n$ then we denote f as follow

$$f := \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$$

Let

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

Then

$$\begin{aligned} f \circ g &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \end{aligned}$$

And

$$\begin{aligned} g \circ f &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \end{aligned}$$

Let $1 < r \leq n$ and pick $x_1, \cdots, x_r \in \{1, \cdots, n\}$ then an r cycle $(x_1 \cdots x_n) = x_1 \mapsto x_2 \mapsto x_3 \mapsto \cdots \mapsto x_{r-1} \mapsto x_r \mapsto x_1$ and $y \mapsto y$ where $y \in \{1, \cdots, n\} \setminus \{x_1, \cdots, x_n\}$. An 3 cycle $(2, 3, 5) \in S_5$ is look like $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}$. Let $a \in S_n$ be a permutation then a^i

4.3. **Group Homomorphism.**

Definition 4.9. *Let G, G' be two groups. A map $\phi : G \to G'$ is said to be a group morphism if $\phi(xy) = \phi(x)\phi(y), \forall\ x, y \in G$.*

Definition 4.10. *Let $\phi : G \to G'$ be a group morphsim if there exists another group morphism $\psi : G' \to G$ such that $\phi \circ \psi = id_{G'}$ and $\psi \circ \phi = id_G$ then ϕ is said to be an isomorphism (or invertible group homomorphism) and ψ is called inverse of ϕ.*

Theorem 4.11. *A group homomorphism $\phi : G \to G'$ is an isomorphsim iff it is bijective.*

Proof. If $|phi : G \to G'$ is an isomorphism then $\exists\ \psi : G' \to G$ such that $\phi \circ \psi = id_{G'}$ and $\psi \circ \phi = id_G \Rightarrow \phi \circ \psi$ and $\psi \circ \phi$ are bijective map hence ϕ is bijective. Conversely, if ϕ is a bijective group homomorphism then as a set map there exists a mapping $\psi : G' \to G$. Our claim is that ψ is a morphism. Let $x', y' \in G'$ then $\psi(x'y') = t$ (say) then $\phi \circ \psi(x'y') = \phi(t)$. Let $\phi(x) = x', \phi(y) = y' \Rightarrow \psi(x') = x, \psi(y') = y$ then $\phi(x)\phi(y) = x'y' = \phi(t) \Rightarrow \phi(xy) = \phi(t) \Rightarrow xy = t \Rightarrow \psi(x')\psi(y') = t = \psi(x'y')$. Therefore, ψ is a group morphism. □

Definition 4.12. *Let $\phi : G \to G'$ be a group morphism. We define kernel of ϕ is*

$$\ker \phi := \{x \in G : \phi(x) = e_{G'}\}.$$

Definition 4.13. *Let G be a group and $N < G$. N is said to be normal subgroup of G is it satisfies following equivalent conditions:*

(1) $xyx^{-1} \in N, \forall\ y \in N, \forall\ x \in G$,
(2) $xNx^{-1} = N, \forall\ x \in G$,
(3) $xN = Nx, \forall\ x \in G$.

Notation. If N is a normal subgroup of G then we write $N \trianglelefteq G$.

Observation 4.14. *Let $N < G$, N is normal iff N is kernel of some group homomorphism.*

Proof. At first we show that if $\phi : G \to G'$ is a group morphism then $\ker \phi$ is a normal subgroup of G. Let $a, b \in \ker \phi$ then $\phi(a^{-1}b) = \phi(a)^{-1}\phi(b) = e_{G'} \Rightarrow a^{-1}b \in \ker \phi$. Thus $\ker \phi$ is a subgroup of G. Let $x \in \ker \phi$ and $g \in G$ then $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e_{G'} \Rightarrow gxg^{-1} \in \ker \phi \Rightarrow \ker \phi \trianglelefteq G$. Conversely, if $N \trianglelefteq G$ then we consider the following group morphism

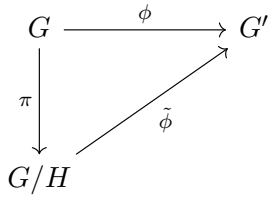
$$\phi : G \to G/N$$
$$x \mapsto xN$$

Then $\ker \phi = \{x \in G : \pi(x) = eN\} = \{x \in G : xN = eN\} = \{x \in G : x \in N\} = N \cap G = N$. □

Observation 4.15. *Let $\phi : G \to G'$ is a injective group homomrophism iff $\ker \phi = \{e_G\}$.*

Proof. Suppose, ϕ is injective. Note that $\phi(e_G) = e_{G'}$ ($\phi(e_G \cdot e_G) = \phi(e_G) \Rightarrow \phi(e_G)\phi(e_G) = \phi(e_G) \Rightarrow \phi(e_G) = e_{G'}$) then $\ker \phi = \{e_G\}$ (as ϕ is injective). Conversely, let $\ker \phi = \{e_G\}$ and $\phi(x) = \phi(y) \Rightarrow \phi(x)\phi(y)^{-1} = e_{G'} \Rightarrow \phi(xy^{-1}) = e_{G'} \Rightarrow xy^{-1} \in \ker \phi = \{e_G\} \Rightarrow xy^{-1} = e_G \Rightarrow x = y \Rightarrow \phi$ is injective. □

Theorem 4.16 (First isomorphism theorem)**.** *Let $\phi : G \to G'$ be a group homomorphism and $H \trianglelefteq G$. If $H \leq \ker\phi$ then there exists an unique group homomorphism $\tilde{\phi} : G/H \to G'$ such that the diagram is commutative i.e, $\phi = \tilde{\phi} \circ \pi$.*



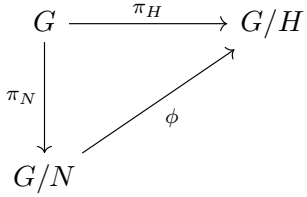
Moreover,

(1) *ϕ is surjective iff $\tilde{\phi} : G/H \to G'$ is surjective,*
(2) *If $H = \ker\phi$ then $\tilde{\phi} : G/\ker\phi \to G'$ is injective,*
(3) *If ϕ is surjective and $H = \ker\phi$ then $G/\ker\phi \cong G'$.*

Proof. Given $H \trianglelefteq G$ and $H \leq \ker\phi$ then we define $\tilde{\phi} : G/H \to G'$ by $\tilde{\phi}(xH) = \phi(x)$. We claim that $\tilde{\phi}$ is well defined. Let $xH = yH \Rightarrow y^{-1}x \in H \subseteq \ker\phi \Rightarrow \phi(y^{-1}x) = e_{G'} \Rightarrow \phi y = \phi(x) \Rightarrow \tilde{\phi}(xH) = \tilde{\phi}(yH) \Rightarrow \tilde{\phi}$ is well defined. If $\theta : G/H \to G'$ be another morphism such that $\theta \circ \pi = \phi$ then $\theta \circ \pi(x) = \phi(x) \Rightarrow \theta(xH) = \tilde{\phi}(xH), \forall\ x \in G \Rightarrow \theta = \tilde{\phi}$. Therefore, $\tilde{\phi}$ is unique.
(1) We note that $\operatorname{Im}\phi = \operatorname{Im}\tilde{\phi}$. If $x' \in \operatorname{Im}\phi$ then $\exists\ x \in G$ such that $\phi(x) = x' \Rightarrow \tilde{\phi}(xH) = x' \Rightarrow x' \in \operatorname{Im}\tilde{\phi} \Rightarrow \operatorname{Im}\phi \subseteq \operatorname{Im}\tilde{\phi}$. Pick $y' \in \operatorname{Im}\tilde{\phi}$ then $\exists\ yH \in G/H$ such that $\tilde{\phi}(yH) = y' \Rightarrow \tilde{\phi} \circ \pi(y) = y' \Rightarrow \phi(y) = y' \Rightarrow y \in \operatorname{Im}\phi \Rightarrow \operatorname{Im}\tilde{\phi} \subseteq \operatorname{Im}\phi$. Hence, $\operatorname{Im}\phi = \operatorname{Im}\tilde{\phi}$. Therefore ϕ is surjective if and only if $\tilde{\phi}$ is surjective.
(2) Let $H = \ker\phi$ and $\tilde{\phi}(x\ker\phi) = \tilde{\phi}(y\ker\phi) \Rightarrow \phi(x) = \phi(y) \Rightarrow \phi(y^{-1}x) = e_{G'} \Rightarrow y^{-1}x \in \ker\phi \Rightarrow y\ker\phi = x\ker\phi \Rightarrow \tilde{\phi}$ is injective. Therefore, $G/\ker\phi \cong \operatorname{Im}\phi$.
(3) If ϕ is surjective then $\operatorname{Im}\phi = G' \Rightarrow G/\ker\phi \cong G'$. □

Theorem 4.17 (Third isomorphism theorem)**.** *If $N \trianglelefteq G$, $H \trianglelefteq G$ and $N \leq H$ then $H/N \trianglelefteq G/N$ and $\dfrac{G/N}{H/N} \cong G/H$.*

Proof. Let us consider the following commutative diagram.



From above diagram $\ker\pi_H = H$ and $\ker\pi_N = N$. By first isomorphism theorem $\phi : G/N \to G/H$ is well defined group homomorphism. Since π_H is surjective, ϕ is surjective. $\ker\phi = \{xN \in G/N : \phi(xN) = eH\} = \{xN \in G/H : x \in H\} = H/N \Rightarrow H/N \trianglelefteq G/N$ (as H/N is kernel of ϕ) and by first isomorphism theorem $\dfrac{G/N}{H/N} \cong G/H$. □

Question 4.18. *Classify all the subgroups of G/N where $N \trianglelefteq G$.*

Ans. Let $Q \leq G/N$ and we consider the natural projection map $\pi : G \to G/N$ defined by $\pi(x) = xN$. Clearly π is surjective. We claim that $\pi^{-1}(Q)$ is a subgroup of G. Let $x, y \in \pi^{-1}(Q) \Rightarrow xN, yN \in Q$. Since, $Q \leq G/N \Rightarrow (y^{-1}N)(xN) \in Q \Rightarrow (y^{-1}x)N \in Q \Rightarrow y^{-1}x \in \pi^{-1}(Q) \Rightarrow \pi^{-1}(Q) \leq G$. Let $H = \pi^{-1}(Q)$. Note that $e_G N \in Q$ (as $Q \leq G/N$) then $\pi^{-1}(\{e_G N\}) \subseteq \pi^{-1}(Q) \Rightarrow N \subseteq H \Rightarrow N \leq H$. Now we will show that $H/N = Q$. We have $\pi(H) = H/N \Rightarrow \pi(\pi^{-1}(Q)) = H/N$. Since π is surjective $H/N = \pi(\pi^{-1}(Q)) = Q$. Conversely, if $N \leq H$ then $H/N \leq G/N$ so all the subgroups of G/N are of the form H/N where $N \leq H \leq G$.

Question 4.19. *What are the normal subgroups of G/N where $N \trianglelefteq G$?*

Ans. From previous problem we see that every subgroups of G/N is of the form H/N where $N \leq H \leq G$. Suppose, $H/N \trianglelefteq G/N$ then $\dfrac{G/N}{H/N} \cong G/H$. If $H \ntrianglelefteq G$ then G/H will not form a group but $\dfrac{G/N}{H/N}$ is a group which is a contradiction. Therefore, H must be a normal subgroup of G. Conversely, if $N \trianglelefteq H \trianglelefteq G$ then we will show that $H/N \trianglelefteq G/N$. Let $xN \in H/N$ and $gN \in G/N \Rightarrow (gN)(xN)(gN)^{-1} = (gxg^{-1})N \in H/N$ (as $H \trianglelefteq G$ and $x \in H, g \in G \Rightarrow gxg^{-1} \in H$) hence $H/N \trianglelefteq G/N$.

4.3.1. *Correspondence theorem.* Let $\phi : G \to G'$ be a group morphism and $H \leq G$. Define $\phi_H := \phi\big|_H : H \to G'$ be a group morphism then $\ker \phi_H = \ker \phi \cap H$.

Proposition 4.20. *Let $\phi : G \to G'$ be a group homomprhism and $H' \leq G$. Define $\phi^{-1}(H') = H := \{g \in G : \phi(g) \in H'\}$ then $H \leq G$ containing $\ker \phi$. If $H' \trianglelefteq G'$ then $H \trianglelefteq G$. If ϕ is surjective then $H \trianglelefteq G \Rightarrow H' \trianglelefteq G'$.*

Proof. We know that $\ker \phi \leq G$. Let $g \in \ker \phi \Rightarrow \phi(g) = e_{G'} \in H' \Rightarrow g \in \phi^{-1}(H') = H \Rightarrow \ker \phi \subseteq H$. Let $x, y \in H \Rightarrow \phi(x), \phi(y) \in H'$. Since $H' \leq G' \Rightarrow \phi(x)^{-1}\phi(y) = \phi(x^{-1}y) \in H' \Rightarrow x^{-1}y \in H \Rightarrow H \leq G$. Suppose, $H' \trianglelefteq G'$. Let $x \in H$ and $g \in G$ then $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1} \in H'$ (as $\phi(x) \in H'$ and $\phi(g) \in G'$ and $H' \trianglelefteq G'$) therefore, $gxg^{-1} \in H$ hence $H \trianglelefteq G$. Let ϕ be a surjective map and H is normal subgroup of G. Let $x' \in H'$ and $g' \in G'$. Since ϕ is surjective there exists $x \in H$ and $g \in G$ such that $\phi(x) = x'$ and $\phi(g) = g'$. Now, $g'x'g'^{-1} = \phi(g)\phi(x)\phi(g)^{-1} = \phi(gxg^{-1})$.

Theorem 4.21 (Correspondence theorem)**.** *Let $\phi : G \to G'$ be a surjective group morphism with kernel K. Then there exists a bijective correspondence between subgroups of G' and subgroups of G that contain K. Moreover, If H and H' are corresponding subgroups then $H \trianglelefteq G$ iff $H' \trianglelefteq G'$ and $|H| = |H'||K|$.*

Proof. Let $K \leq H \leq G$ and $H' \leq G$. We need to show

(1) $\phi(H) \leq G'$,
(2) $K \leq \phi^{-1}H \leq G$,
(3) $H' \trianglelefteq G'$ iff $H \trianglelefteq G$,
(4) $\phi(\phi^{-1}(H')) = H'$ and $\phi^{-1}(\phi(H)) = H$,
(5) $|\phi^{-1}(H')| = |H'||K|$.

(1) Pick $x, y \in H$, as $H \leq G \Rightarrow x^{-1}y \in H$. Now $\phi(x^{-1}y) = \phi(x)^{-1}\phi(y) \in \phi(H) \Rightarrow \phi(H) \leq G'$.
(2) and (3) follows from previous proposition.

(4) $\phi^{-1}(H') = \{x \in G : \phi(x) \in H'\} = H \leq G$. Clearly, $x \in H \Rightarrow \phi(x) \in H' \Rightarrow \phi(H) = H'$ (as ϕ is surjective, every $y \in H'$ has preimage in G) then $\phi(\phi^{-1}(H')) = H'$. For any map $\phi : G \to G'$ with $H \subseteq G \Rightarrow H \subseteq \phi^{-1}(\phi(H))$. We only need to prove the reverse inclusion. Let $x \in \phi^{-1}(\phi(H)) \Rightarrow \phi(x) \in \phi(H) = H'$. Since ϕ is surjective and $\phi(x) \in H' \Rightarrow x \in H \Rightarrow \phi^{-1}(\phi(H)) \subseteq H \Rightarrow H = \phi^{-1}(\phi(H))$.
(5) Since ϕ is surjective, by first isomorphism theorem $G/K \cong G'$. Pick $H' \leq G'$ then H' is of the form H/K for some $K \leq H \leq G$ where $H = \phi^{-1}(H') = \{x \in G : \phi(x) \in H'\} \Rightarrow |H'| = \dfrac{|H|}{|K|} \Rightarrow |H| = |H'||K| \Rightarrow |\phi^{-1}(H')| = |H'||K|$. □

4.3.2. *Chinese Remainder theorem.*

Theorem 4.22. *If* $\gcd(p, q) = 1$ *then*

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}.$$

Proof. Since $\gcd(p, q) = 1$ there exists $u, v \in \mathbb{Z}$ such that $pu + qv = 1$. Define,

$$\mathbb{Z} \xrightarrow{\theta} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$
$$x \mapsto (x + p\mathbb{Z}, x + q\mathbb{Z})$$

Then clearly θ is a group morphism. Now, $\ker\theta = \{x \in \mathbb{Z} : (x + p\mathbb{Z}, x + q\mathbb{Z}) = (0 + p\mathbb{Z}, 0 + q\mathbb{Z})\}$. Since $x + p\mathbb{Z} = 0 + p\mathbb{Z} \Rightarrow x \in p\mathbb{Z} \Rightarrow p\big|x$. Similarly, $q\big|x$ therefore, $\mathrm{lcm}(p, q)\big|x \Rightarrow pq\big|x \Rightarrow x \in pq\mathbb{Z}$. Conversely, if $x \in pq\mathbb{Z} \Rightarrow pq\big|x \Rightarrow p|x$ and $q|x \Rightarrow x + p\mathbb{Z} = 0 + p\mathbb{Z}$ and $x + q\mathbb{Z} = 0 + q\mathbb{Z} \Rightarrow x \in \ker\theta$. Therefore, $\ker\theta = pq\mathbb{Z}$. Now we will show that θ is surjective. Let $(a + p\mathbb{Z}, b + q\mathbb{Z}) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Now consider $y = aqv + bpu$ then $y - a = aqv + bpu - a = a(qv - 1) + bpu = -apu + bpu \in p\mathbb{Z} \Rightarrow y + p\mathbb{Z} = a + p\mathbb{Z}$. Similarly, $y - b = aqv + bpu - b = aqv + b(pu - 1) = aqv - bqv \in q\mathbb{Z} \Rightarrow y + q\mathbb{Z} = b + q\mathbb{Z}$. Therefore, $\theta(y) = (y + p\mathbb{Z}, y + q\mathbb{Z}) = (a + p\mathbb{Z}, b + q\mathbb{Z}) \Rightarrow \theta$ is surjective. By first isomorphsim theorem $\mathbb{Z}/\ker\theta \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \Rightarrow \mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. □

4.3.3. *Product group.*

Proposition 4.23. *Let* $H, K \leq G$ *and* $f : H \times K \to G$ *be the multiplication map defined by* $(h, k) \mapsto hk$. *Image set* $\mathrm{Im}\, f (= HK) = \{hk : h \in H, k \in K\}$.

(1) f *is injective iff* $H \cap K = \{e\}$,
(2) f *is homomorphism iff* $HK = KH$,
(3) H *is normal subgroup of* G *then* $HK < G$,
(4) f *is an isomorphism iff* $H \cap K = \{e\}; HK = G; H, K \trianglelefteq G$.

Proof. (1) Let f is injective and $x \in H \cap K \Rightarrow x^{-1} \in H$ and $f(x^{-1}, x) = e = f(e, e)$ which is a contradiction therefore, $H \cap K = \{e\}$. Conversely, let $H \cap K = \{e\}$. Let $f(h_1, k_1) = f(h_2, k_2) \Rightarrow h_1k_1 = h_2k_2 \Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} \Rightarrow h_2^{-1}h_1 = e = k_2k_1{-}1 \Rightarrow h_1 = h_2$ and $k_1 = k_2$ which implies f is injective.
(2) Let $A = (h_1, k_1), B = (h_2, k_2) \Rightarrow AB = (h_1h_2, k_1k_2)$ then $f(AB) = h_1h_2k_1k_2 = f(A)f(B) = h_1k_1h_2k_2$ thus f is a group morphism iff $HK = KH$.
(3) Let $H \trianglelefteq G$ then for all $g \in G, gH = Hg$. In particularly $kH = Hk, \forall\, k \in K$. Now, $(h_1k_1)^{-1}h_2k_2 = k_1^{-1}h_1^{-1}h_2k_2 = h_1^{-1}k_1^{-1}h_2k_2 = h_1^{-1}h_2k_1^{-1}k_2 \in HK \Rightarrow HK \leq G$.

(4) Suppose all the given condition holds then f is both injective and surjective so f is bijective. From (2) we have f is a morphsim hence f is an isomorphism. Converse is also holds. $\square$

4.4. **Group Action.**

Definition 4.24. *An action of a group G on a set $S(\neq \emptyset)$ is a function*

$$\begin{aligned} \cdot : G \times S &\to S \\ (g, s) &\mapsto gs \end{aligned}$$

such that

(1) $e \cdot x = x, \forall\ x \in S$,
(2) $g_1(g_2 s) = (g_1 g_2)x, \forall\ g_1, g_2 \in G$ *and* $\forall\ x \in S$.

Example 4.25. (1) *Let G be a group and $H \leq G$ then*

$$\begin{aligned} \cdot : H \times G &\to G \\ (h, g) &\mapsto hg \end{aligned}$$

Clearly this is a group action.

(2) *Let G and H are same as (1) and cosider*

$$\begin{aligned} \cdot : H \times G &\to G \\ (h, g) &\mapsto hgh^{-1} \end{aligned}$$

Check that this is a group action.

(3) *Let $I_n = \{1, \cdots, n\}$ and let us consider the map*

$$\begin{aligned} \cdot : S_n \times I_n &\to I_n \\ (\sigma, n) &\mapsto \sigma(n) \end{aligned}$$

Then '$\cdot$' is a group action.

(4) *Let H and K be a subgroup of G and let $\sum$ be the set of all left coset of K in G then*

$$\begin{aligned} \cdot : H \times \sum &\to \sum \\ (h, xK) &\mapsto hxK \end{aligned}$$

Then check that '$\cdot$' is a group action.

(5) *Let H and G are same as (1) and S be the set of all subgroups of G. Consider the mapping*

$$\begin{aligned} \cdot : H \times S &\to S \\ (h, K) &\mapsto hKh^{-1} \end{aligned}$$

'$\cdot$' is a group action on S.

Theorem 4.26. *Let G be a group that acts on a set S*

(1) *The relation on S defined by $x \sim x'$ iff there exists $g \in G$ such that $x' = gx$. Then '$\sim$' is an equivalence relation.*
(2) *For each $x \in S$, $G_x = \{g \in G : gx = g\}$ is a subgroup of G.*

Proof. (1) $x \sim x$ as $x = ex, \forall\ x \in S$. If $x \sim x'$ then by definition we have $x' = gx \Rightarrow g^{-1}x' = x \Rightarrow x' \sim x$ and if $x \sim x'$ and $x' \sim x''$ then we have $x' = g_1x, x'' = g_2x'$ for some $g_1, g_2 \in G$ then $x'' = (g_2g_1)x$ hence $x \sim x''$. Therefore, '$\sim$' is an equivalence relation on S.
(2) Clearly G_x is non empty as $e \in G_x$ for all $x \in S$. Let $g_1, g_2 \in G_x$ then by definition $g_1x = x$ and $g_2x = x \Rightarrow x = g_2^{-1}x$. So, $(g_2^{-1}g_1)x = g_2^{-1}(g_1x) = g_2^{-1}x = x \Rightarrow g_2^{-1}g_1 \in G_x$ hence G_x is subgroup of G. □

Notation:

(1) For each $x \in S$ we denote $\mathrm{cl}(x)$ by $\mathcal{O}_x$ is called orbit of x, thus

$$\mathcal{O}_x = \{gx : g \in G\}$$

(2) G_x is called stabilizer or isotropy group of x.

Proposition 4.27. *Let G be a group act on a set S then $|\mathcal{O}_x| = [G : G_x]$.*

Proof. Let, $\sum = \{gG_x : g \in G\}$ and define the map

$$\phi : \sum \to \mathcal{O}_x$$
$$gG_x \mapsto gx$$

We claim that ϕ is well defined. Let $g_1G_x = g_2G_x \Rightarrow g_2^{-1}g_1 \in G_x \Rightarrow (g_2^{-1}g_1)x = x \Rightarrow g_1x = g_2x$. Hence ϕ is well defined and injective map. Let $gx \in \mathcal{O}_x \Rightarrow gx = \phi(gG_x)$ which imply ϕ is surjective. Therefore, ϕ is bijective and $|\mathcal{O}_x| = |\sum| = [G : G_x]$. □

Corollary 4.28. *Let G be a finite group. Then number of elements in conjugacy class of $x \in G$ is $[G : C_G(x)]$ which divides $|G|$ where $C_G(x)$ is centralizer of x.*

Proof. Recall $C_G(x) = \{g \in G : gx = xg\}$. Now we consider the conjugacy group action

$$\cdot : G \times G \to G$$
$$(g, h) \mapsto ghg^{-1}$$

Then $\mathcal{O}_x = \{gxg^{-1} : g \in G\}$ and $G_x = \{g \in G : gxg^{-1} = x\} = C_G(x)$. By the previous proposition $|\mathcal{O}_x| = [G : C_G(x)]$. Since $[G : C_G(x)] \big| |G| \Rightarrow |\mathcal{O}_x| \big| |G|$. □

Corollary 4.29. *Let G be a finite group and $K \leq G$. Then the number of subgroups conjugates to K is $[G : N_G(K)]$, which divides $|G|$ where $N_G(K) = \{g \in G : gK = Kg\}$.*

Proof. Let, S be the set of all subgroup of G and we define an action on S as

$$\cdot : G \times S \to S$$
$$(g, K) \mapsto gKg^{-1}$$

Then $G_K = \{g \in G : gKg^{-1} = K\} = N_G(K)$ and $\mathcal{O}_K = \{gKg^{-1} : g \in G\}$ then $|\mathcal{O}_K|$ is the number of conjugates of K. So, $|\mathcal{O}_K| = [G : N_G(K)]$ therefore, number of conjugates of K is $[N : N_G(K)]$ which divides $|G|$. □

Proposition 4.30. *Let G be a finite group then*

$$|G| = |Z(G)| + \sum_{[G:C_G(x_i)]\neq 1} [G : C_G(x_i)]$$

This equation is called the class equation of G.

Proof. Consider the conjugacy group action

$$\cdot : G \times G \to G$$
$$(g, h) \mapsto ghg^{-1}$$

Let $\mathcal{O}_{x_1}, \mathcal{O}_{x_2}, \cdots, \mathcal{O}_{x_n}$ be distinct classes of G then $\mathcal{O}_{x_1}, \mathcal{O}_{x_2}, \cdots, \mathcal{O}_{x_n}$ create a partition on G hence

$$|G| = \sum_{i=1}^{n} |\mathcal{O}_{x_i}|$$

Now, $\mathcal{O}_{x_i} = [G : C_G(x_i)]$ so $|G| = \sum_{i=1}^{n} [G : C_G(x_i)]$. Next we observe that $|\mathcal{O}_{x_i}| = 1 \Leftrightarrow gxg^{-1} = x_i, \forall\ g \in G \Leftrightarrow x_i g = g x_i, \forall\ g \in G \Leftrightarrow x_i \in Z(G)$ then we can write

$$\begin{aligned} |G| &= \sum_{i=1}^{n} |\mathcal{O}_{x_i}| \\ &= \sum_{|\mathcal{O}_{x_i}|=1} |\mathcal{O}_{x_i}| + \sum_{|\mathcal{O}_{x_i}|\neq 1} |\mathcal{O}_{x_i}| \\ &= |Z(G)| + \sum_{|\mathcal{O}_{x_i}|\neq 1} |\mathcal{O}_{x_i}| \\ &= |Z(G)| + \sum_{[G:C_G(x_i)]\neq 1} [G : C_G(x_i)] \end{aligned}$$

This completes the proof. □

4.4.1. *Cayley's theorem.* Let S be a set and $S \neq \emptyset$, define

$$A(S) = \{f : S \to S : f \text{ is bijection}\}$$

Now,

$$\circ : A(S) \times A(S) \to A(S)$$
$$(f, g) \mapsto f \circ g$$

Then it is easy to check that $A(S)$ is a group under mapping composition.

Theorem 4.31. *If a group G acts on a set S then this action induce a group homomorphism from G to $A(S)$.*

Proof. Let

$$\cdot : G \times S \to S$$
$$(g, s) \to gs$$

be the group action. Define

$$\theta : G \to A(S)$$
$$g \mapsto \tau_g$$

where

$$\tau_g : S \to S$$
$$s \mapsto gs$$

We will show that τ_g is a bijection. Let $\tau_g(s_1) = \tau_g(s_2) \Rightarrow gs_1 = gs_2 \Rightarrow s_1 = s_2$. Let $s \in S$ then $s = \tau_g(g^{-1}s)$. Therefore, τ_g is a bijection and $\tau_g \in A(S)$. Next we will show that $\tau_{g_1} \circ \tau_{g_2} = \tau_{g_1g_2}$. Let $\tau_{g_1} \circ \tau_{g_2}(s) = \tau_{g_1}(g_2s) = (g_1g_2)(s) = \tau_{g_1g_2}(s), \forall\ s \in S$. Hence, $\tau_{g_1} \circ \tau_{g_2} = \tau_{g_1g_2}$. Now $\theta(g_1g_2) = \tau_{g_1g_2} = \tau_{g_1} \circ \tau_{g_2} = \theta(g_1)\theta(g_2)$. Therefore, θ is a group homomorphism. □

Corollary 4.32. *If we take $S = G$ and the action is usual group action then $\theta : G \to A(G)$ is injection hence $G \leq A(G)$. In particular if $|G| = n$ then $G \hookrightarrow S_n$. This is known as Cayley's theorem.*

Proof. $\ker\theta = \{g \in G : \tau_g = id\}$. Now, $\tau_g = id \Leftrightarrow \tau_g(x) = id(x), \forall\ x \in G$. In particularly, if $x = e$ then $\tau_g(e) = e \Rightarrow ge = e \Rightarrow g = e \Rightarrow \ker\theta = \{id\}$. Hence θ is injective and $G \leq A(G)$. In particularly if $|G| = n$ then $A(G) = S_n$ and $G \hookrightarrow S_n$. □

Corollary 4.33. *Let G be a group,*

(1) *For each $g \in G$, conjugaction by g induces a automorphism of G,*
(2) *There is a homomorphism whose kernel is $Z(G)$.*

Proof. (1) Consider,

$$\tau_g : G \to G$$
$$x \mapsto gxg^{-1}$$

Clearly τ_g is a homomorphism. We will show that τ_g is an automorphism. Let $\ker\tau_g = \{x \in G : gxg^{-1} = e\} = \{e\}$ and let $x \in G$ then $x = \tau_g(g^{-1}xg)$ then τ_g is a bijection so it is an automorphism. (2) Consider the map

$$\theta : G \to Aut(G)$$
$$g \to \tau_g$$

where $\tau_g : G \to G$ is defined by $\tau_g(x) = gxg^{-1}$. Then θ is a group morphism and $\ker\theta = \{x \in G : \tau_g = id_G\} = \{x \in G : gxg^{-1} = x, \forall\ x \in G\} = \{x \in G : xg = gx, \forall\ x \in G\} = Z(G)$. □

Observation 4.34. *By first isomorphism theorem $G/Z(G) \hookrightarrow Aut(G)$. Now, $Im\theta = \{\tau_g : g \in G$ where τ_g is defined above. τ_g is called inner automorphism and $Im\theta$ will be denoted by $Inn(G)$. So, $G/Z(G) \cong Inn(G) \leq Aut(G)$.*

Proposition 4.35. *Let H be a subgroup of G and G acts on the set of all left coset of H by left translation i.e,*

$$\cdot : G \times S \to S$$
$$(g, xH) \mapsto gxH$$

This action will induce a group homomorphism and $\ker\theta < H$.

Proof. Let $g \in \ker\theta$ then $\theta(g) = \tau_g = id \Rightarrow gxH = xH, \forall\ g \in G$ [where $\tau_g : S \to S$ defined by $\tau_g(xH) = gxH$]. In particular, if we take $x = e$ then $gH = H \Rightarrow g \in H \Rightarrow \ker\theta < H$. □

Corollary 4.36. *Let G be a finite group and $H < G$ with $[G : H] = n$, and no non-trivial normal subgroup of G is contained in H, then G is isomorphic to a subgroup of S_n.*

Proof. Let S be the set of all left coset of H then $|H| = [G : H] = n$. We consider

$$\cdot : G \times S \to S$$
$$(g, xH) \mapsto gxH$$

then this action will induce a group homomrphism $\theta : G \to A(S)$. By previous corollary, $\ker\theta < H$ but $\ker\theta$ is a normal subgroup of G so by our hypothesis $\ker\theta = \{e\}$. Therefore, $\theta : G \to A(S) = S_n$ is injective and $G < S_n$. □

Corollary 4.37. *Let G is a finite group and $H < G$ with $[G : H] = p$, where p is the least prime dividing $|G|$, then H is normal in G.*

Proof. Let S be the set of all left coset of H in G and G acts on S by left translation then this action will induce a group morphism

$$\theta : G \to A(S) = S_p$$

and $\ker\theta < H < G$. Therefore,

$$[G : \ker\theta] = [G : H][H : \ker\theta].$$

By first isomorphism theorem $G/\ker\theta \hookrightarrow S_p$ and

$$|G/\ker\theta|\big||S_p| = p! \Rightarrow [G : \ker\theta]\big|p! \Rightarrow [G : H][H : \ker\theta]\big|p! \Rightarrow [H : \ker\theta]\big|(p-1)!.$$

If q is another prime such that $q|(p-1)!$ then $q < p$. Now, $[H : \ker\theta]\big|[G : \ker\theta]$ and $[G : \ker\theta]\big||G| \Rightarrow [H : \ker\theta]\big||G|$. If $[H : \ker\theta] \neq 1$ then there exists a prime q such that $q\big|[H : \ker\theta] \Rightarrow q\big||G|$. But $q\big|[H : \ker\theta] \Rightarrow q < p$ and p is the least prime dividing group's order which is a contradiction. Therefore, $[H : \ker\theta] = 1 \Rightarrow H = \ker\theta$ and H is a normal subgroup of G. □

Definition 4.38. *Let G be a group acting on a set X. The action is said to be faithful or effective if $gx = x \Rightarrow g = e, \forall\ x \in X$. Equivalently the homomorphism from G to $A(X)$ is injective.*

The action is called free (or semi-regular or fixed point free) if the statement $gx = x$ for some $x \in X \Rightarrow g = e$. In other words no non-trivial element of G fixes a point of X (A much stronger property than faithfulness). The action of any group on itself by left multiplication is free. A finite set may act faithfully on a set of size much smaller than its cardinality. For example the abelian 2-group $(\mathbb{Z}/2ZZ)^n$ acts faithfully on a set of size $2n$.

Definition 4.39. *Let G be a group acting on a set S. The action is said to be transitive if for any two elements $x, y \in S$ and there exists $g \in G$ such that $gx = y$.*

The action is simply transitive if it is both transitive and free. This means that given any $x, y \in S$ the element g in definition is unique.

Definition 4.40. *The action of G on a set S is called primitive if there is no partition of S preserved by all the elements of G apart from the trivial partition.*

Proposition 4.41.
(1) *The group action is transitive iff it has exactly one orbit i.e., $\exists\ x \in S$ such that $\mathcal{O}_x = S$.*
(2) *The action of G on S is free iff all stabilizers are trivial.*
(3) *Let G be a group acting on a set S then this action induce a group morphism $\theta : G \to A(S)$ and $\ker f = \bigcap_{x \in S} G_x$. If $\ker f = \{e\}$ then the action is faithful.*
(4) *Let $x, y \in S$ and there exists $g \in G$ such that $y = gx$ then, $gG_xg^{-1} = G_y$.*

Proof. (4) Let $h \in G_y \Rightarrow hy = y \Rightarrow h(gx) = gx \Rightarrow (g^{-1}hg)x = x \Rightarrow g^{-1}hg \in G_x \Rightarrow h \in gG_xg^{-1} \Rightarrow G_y \subseteq gG_xg^{-1}$. Let $p \in G_x \Rightarrow px = x \Rightarrow p(g^{-1}y) = g^{-1}y \Rightarrow (gpg^{-1})y = y \Rightarrow gpg^{-1} \in G_y \Rightarrow gG_xg^{-1} \subseteq G_y$ Therefore $G_y = gG_xg^{-1}$. □

4.4.2. *Sylow's theorem.*

Lemma 4.42 (Key lemma)**.** *If a group H of order p^n (p is prime) acts on a finite set S and*

$$S_0 := \{s \in S : hs = s, \forall\ h \in H\},$$

then

$$|S| \equiv |S_0| \ (mod\ p).$$

Proof. If H acts on S then $|S| = \sum_{\text{distinct}} |\mathcal{O}_x|$. Now, $|\mathcal{O}_x| = 1 \Rightarrow \mathcal{O}_x = \{x\} \Rightarrow hx = x, \forall\ h \in H \Rightarrow x \in S_0$. Therefore we can write

$$\begin{aligned} |S| &= \sum_{|\mathcal{O}_x|=1} |\mathcal{O}_x| + \sum_{|\mathcal{O}_x|>1} |\mathcal{O}_x| \\ &= |S_0| + \sum_{[H:H_x]>1} [H : H_x] \qquad\qquad [\text{as } [H : H_x] = |\mathcal{O}_x|] \end{aligned}$$

Now, $1 \neq [H : H_x] \big| |H| = p^n \Rightarrow p \big| [H : H_x]$. Therefore, $|S| = |S_0| + pl$ [where $p| \sum_{[H:H_x]>1} [H : H_x]] \Rightarrow |S| \equiv |S_0| \ (mod\ p)$. □

Theorem 4.43 (Cauchy)**.** *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Proof. (Mckay) Let

$$S := \{(a_1, \cdots, a_p) : a_i \in G, 1 \leq i \leq p, a_1 \cdots a_p = e\}.$$

Then $|S| = |G|^{p-1}$ and $p\big||G|$. Now let us consider the following action

$$\mathbb{Z}/p\mathbb{Z} \times S \to S$$
$$(i, (a_1, \cdots, a_p)) \mapsto (a_{i+1}, \cdots, a_p, a_1, \cdots, a_i)$$

Note that $a_1 \cdots a_p = e \Rightarrow a_2 \cdots a_p = a_1^{-1} \Rightarrow a_2 \cdots a_p a_1 = e$ therefore, $a_{i+1} \cdots a_p a_1 \cdots a_i = e$ hence $a_{i+1} \cdots a_p a_1 \cdots a_i \in S$. Clearly the above action defines a group action.

$$S_0 = \{(a_1, \cdots, a_p) \in S : (a_{i+1}, \cdots, a_p, a_1, \cdots, a_i) = (a_1, \cdots, a_p), 1 \leq i \leq p\}$$

Therefore, $(a_1, \cdots, a_p) \in S_0 \Leftrightarrow a_1 = a_2 = \cdots = a_p$ and $a_1 \cdots a_p = e$. Since, $(e, \cdots, e) \in S_0, S_0 \neq \emptyset$. Therefore, by Key lemma $|S| \equiv |S_0| \ (mod\ p)$ and $p\big||S| \Rightarrow |S_0| \equiv 0 \ (mod\ p)$. Again, $|S_0| \neq 0 \Rightarrow |S_0| > 1$ then there exists $a \neq e$ such that $(a, \cdots, a) \in S_0 \Rightarrow a^p = e$. □

Definition 4.44. *A group in which every element has order p^n (for some $n \geq 0$, for fixed prime p) is called a $p-$group. If G is a group and $H < G$, such that H is a $p-$group, then we call H is a $p-$subgroup of G.*

Corollary 4.45. *A finite group G is a $p-$group iff $|G|$ is a power of p.*

Proof. Suppose, G is a finite $p-$group, if $|G| = p^l m$, where $m > 1$ and $p \nmid m$, then there exists a prime $q \neq p$ such that $q|m \Rightarrow q\big||G|$. By Cauchy's theorem there is an element $a \in G$ such that $a^q = e$ which is a contradiction. Therefore, $|G| = p^n$ for some $n > 0$. Conversely, if $|G| = p^m$ for some $m > 0$ then for any $a \in G$ $o(a)\big||G|$ i.e., $a^k = e$ for some $0 \leq k \leq m$. □

Lemma 4.46. *Let H be a $p-$subgroup of G then*

$$[N_G(H) : H] \equiv [G : H] \ (mod\ p).$$

Proof. Let S be the set of all left coset of H in G and we consider the action

$$\cdot : H \times S \to S$$
$$(h, xH) \mapsto hxH$$

Thus,

$$\begin{aligned} S_0 &= \{xH \in S : hxH = xH, \forall\ h \in H\} \\ &= \{xH \in S : x^{-1}hx \in H, \forall\ h \in H\} \\ &= \{xH \in S : x^{-1}Hx = H\} \qquad [x^{-1}Hx = H \Leftrightarrow x \in N_G(H) \Rightarrow xH \in N_G(H)/H] \\ &= N_G(H)/H \end{aligned}$$

By Key lemma, $|S| \equiv |S_0| \ (mod\ p) \Rightarrow [G : H] \equiv [N_G(H) : H] \ (mod\ p)$. □

Corollary 4.47. *If H is a $p-$subgroup of a finite group G such that $p\big|[G : H]$ then $N_G(H) \neq H$.*

Proof. If $N_G(H) = H \Leftrightarrow [N_G(H) : H] = 1$. But $[G : H] \equiv [N_G(H) : H] \ (mod\ p)$. If $p\big|[G : H]$ then $0 \equiv [N_G(H) : H] \ (mod\ p) \Rightarrow N_G(H) \neq H$. □

Theorem 4.48 (First Sylow theorem)**.** *Let G be a group of $p^n m$ with $n \geq 1$, p is prime and $\gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of G of order p^i $(i < n)$ is normal in p^{i+1} order subgroup.*

Proof. Since $p\big||G|$ by Cauchy's theorem there is an element $a \in G$ such that $a^p = e$. We take $H_1 = \langle a \rangle$ then $|H_1| = p$. Let us assume by induction that there exists a group H_i of order p^i where $i < n$. Since, $i < n$, $p\big|[G : H_i] = p^n m/p^i = p^{n-i}m$ therefore by previous corollary $N_G(H_i) \neq H_i$. As $p\big||N_G(H_i)/H_i|$ by Cauchy's theorem $\exists\ xH_i \in N_G(H_i)/H_i$ such that $o(xH_i) = p$. Take, $H_i < H_{i+1} < N_G(H_i)$ such that $H_{i+1}/H_i = \langle xH_i \rangle$ [Note that $H_{i+1} < N_G(H_i) \Rightarrow H_i \trianglelefteq H_{i+1}$]. Therefore, $|H_{i+1}| = |H_i||H_{i+1}/H_i| = p^i \cdot p = p^{i+1}$ and $H_i \trianglelefteq H_{i+1}$. □

Corollary 4.49. *The center $Z(G)$ of a non-trivial finite $p-$group G contains more than one element.*

Proof. We know that

$$|G| = |Z(G)| + \sum [G : C_G(x_i)].$$

Since each $[G : C_G(x_i)] > 1$ and divides $|G| = p^n$ $(n \geq 1)$, p divides each $[G : C_G(x_i)]$ and $|G|$ and therefore $p\big||Z(G)|$. By Cauchy's theorem $\exists\ a \neq e$ such that $a^p = e$ and $a \in Z(G)$. □

Definition 4.50. *A subgroup P of a group G said to be Sylow $p-$subgroup if P is maximal $p-$subgroup of G.*

By Sylow's first theorem Sylow $p-$subgroup exists and order is p^n where $|G| = p^n m$, with $\gcd(p, m) = 1$.

Note 4.51. *Converse of Lagrange's theorem is partially true by Sylow's theorem. Converse of Lagrange theorem is not true in general. For example there is no group of order 6 in A_4.*

Corollary 4.52. *Let G be a group of order $p^n m, \gcd(p, m) = 1$ where $p \geq 1$ and p is prime. Let H be a $p-$subgroup of G.*

1. *H is a Sylow $p-$subgroup of G iff $|H| = p^n$.*
2. *Every conjugate of a Sylow $p-$subgroup is a Sylow $p-$subgroup.*
3. *If there is only one Sylow $p-$subgroup P, then $P \trianglelefteq G$.*

Proof. (1) Follows form Sylow's first theorem.
(2) $|P| = |x^{-1}Px| = p^n, x \in G$. Then $x^{-1}Px$ is also a Sylow $p-$subgroup by (1).
(3) If there exists only one Sylow $p-$subgroup P, then $x^{-1}Px = P, \forall\ x \in G \Rightarrow P \trianglelefteq G$. □

Theorem 4.53 (Second Sylow theorem)**.** *If H is a $p-$subgroup of a finite group G and P is any Sylow $p-$subgroup, then there exists $x \in G$ such that $H < xPx^{-1}$. In particular any two Sylow $p-$subgroups are conjugate.*

Proof. Let S be the set of all left coset of P in G and we consider the following group action

$$H \times S \to S$$
$$(h, xP) \mapsto hxP$$

Then $S_0 = \{xP \in S : hxP = xP, \forall\ h \in H\}$ and by Key lemma $|S| \equiv |S_0|\ (mod\ p)$ but $|S| = [G : H] = m$ and $p \nmid m \Rightarrow |S_0| \not\equiv 0\ (mod\ p) \Rightarrow |S_0| \neq 0$. Now,

$$xP \in S_0 \Leftrightarrow hxP = xP, \forall\ h \in H \Leftrightarrow x^{-1}hx \in P, \forall\ h \in H \Leftrightarrow x^{-1}Hx \in P \Leftrightarrow x^{-1}Hx < P.$$

Since, $|S_0| \neq 0 \Rightarrow \exists\ xP \in S_0$ such that $H < xPx^{-1}$. If H is a Sylow $p-$subgroup then $|H| = |P| = |xPx^{-1}|$ hence $H = xPx^{-1}$. □

Theorem 4.54 (Third Sylow theorem)**.** *If G is a finite group and p is a prime, then number of Sylow $p-$subgroup of G divides $|G|$ and is of the form $kp+1$ for some $k \geq 0$.*

Proof. By second Sylow theorem any two Sylow $p-$subgroups are conjugate. So we need to find number of conjugate subgroups of P (where P is a Sylow subgroup) and that is $[G : N_G(P)]$. We know that $[G; N_G(P)] \big| |G|$ by Corollary 4.14. Let S be the set of all Sylow $p-$ subgroups of G and consider the following group action

$$P \times S \to S$$
$$(x, K) \mapsto xKx^{-1}$$

Therefore, $S_0 = \{K \in S : xKx^{-1} = K, \forall\ x \in P\}$ and by Key lemma $|S| \equiv |S_0|\ (mod\ p)$. Let $Q \in S_0 \Leftrightarrow xQx^{-1} = Q, \forall\ x \in P \Leftrightarrow P < N_G(Q)$ but both P and Q are Sylow $p-$subgroups of G and hence of $N_G(Q)$ and they are conjugate in $N_G(Q)$. Since, $Q \trianglelefteq N_G(Q) \Rightarrow P = Q$ therefore, $S_0 = \{P\}$ and $|S_0| = 1 \Rightarrow |S| = 1 + kp$. □

Theorem 4.55. *If P is a Sylow $p-$subgroup of a group G, then $N_G(N_G(P)) = N_G(P)$.*

Proof. Every conjugate of P is a Sylow $p-$subgroup of G and of any subgroup of G that contains it. Since P is normal in $N_G(P)$, P is the only Sylow $p-$subgroup of $N_G(P)$. Therefore, $x \in N_G(N_G(P)) \Rightarrow xN_G(P)x^{-1} = N_G(P) \Rightarrow xPx^{-1} < N_G(P) \Rightarrow xPx^{-1} = P \Rightarrow x \in N_G(P)$. Hence, $N_G(N_G(P)) < N_G(P)$. The other inclusion is obvious. □

Question 4.56. *Let $H, K < G$. We define $HK := \{hk : h \in H, k \in K\}$. If either $H \trianglelefteq G$ or $K \trianglelefteq G$ then HK is a subgroup of G. Also show that*

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)}.$$

If $H, K \trianglelefteq G$ then $HK \cong H \times K$ provided $H \cap K = \{e\}$.

Ans. Given $H, K < G$ and $K \trianglelefteq G$ then $gK = Kg$ for all $g \in G$, in particularly $hK = Kh, \forall\ h \in H$. Now, $(h_1k_1)^{-1}h_2k_2 = k_1^{-1}h_1^{-1}h_2k_2 = h_1^{-1}k_1^{-1}h_2k_2 = h_1^{-1}h_2k_1^{-1}k_2 \in HK$ (as $k_1^{-1}k_2 \in K$, and $h_1^{-1}h_2 \in H$). Therefore HK is a subgroup of G. Define a map

$$\theta : H \times K \to HK$$
$$(h, k) \mapsto hk$$

where $H, K \trianglelefteq G$ and $H \cap K = \{e\}$. Consider the commutator $(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$. Since $K \trianglelefteq G$ left hand side is in K, similarly $H \trianglelefteq G$, right hand side is in H. As $H \cap K = \{e\} \Rightarrow hkh^{-1}k^{-1} = e \Rightarrow hk = kh$ therefore, $HK = KH$. We will show that θ is a homomorphism. $\theta((h_1, k_1)(h_2, k_2)) = \theta((h_1h_2, k_1k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \theta((h_1, k_1))\theta((h_2, k_2))$. Our next job is to show that θ is injective. Let $\theta(h_1, k_1) = \theta(h_2, k_2) \Rightarrow h_1k_1 = h_2k_2 \Rightarrow h_2^{-1}h_1 = k_2k_1^{-1}$. Since $H \cap K = \{e\}$ we have $h_2^{-1}h_1 = e$ and $k_2k_1^{-1} = e$ which give $h_1 = h_2$ and $k_1 = k_2$ thus θ is injective. For any $hk \in HK$ we have $(h, k) \in H \times K$ such that $\theta((h, k)) = hk \Rightarrow \theta$ is surjective hence bijective. Therefore, $H \times K \cong HK$.

Question 4.57. *Every group of order p^2 is abelian where p is prime.*

Ans. Let G be a group of order p^2 and $Z(G)$ be its center. Then $|Z(G)| = p$ or p^2. If $|Z(G) = p^2$ then $G = Z(G)$ hence G is abelian. If $|Z(G)| = p$ then $|G/Z(G)| = p$ which imply $G/Z(G)$ is cyclic hence G is abelian. Therefore, any group of order p^2 is abelian.

Question 4.58. *Classify all the groups of order* $2p$*, where* p *is prime.*

Ans. **Case 1.** If $p \neq 2$. Let $|G| = 2p$, by Cauchy's theorem there exists an element $e \neq a \in G$ such that $o(a) = p$. Let $H = \langle a \rangle$ then $[G : H] = 2$ hence $H \trianglelefteq G$. Again by Cauchy's theorem there exists an element $b \in G$ such that $o(b) = 2$. Let $K = \langle b \rangle$. As $H \trianglelefteq G$ and $H = \langle a \rangle \Rightarrow bab^{-1} \in H$. Let $bab^{-1} = a^i$ (say), where $1 \leq i \leq p-1$. Now, $a = b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^ib^{-1} = (bab^{-1})^i = a^{i^2} \Rightarrow a^{i^2-1} = e$. Since, $o(a) = p$ we have $p \big| i^2 - 1 \Rightarrow p \big| (i+1)(i-1) \Rightarrow p \big| i+1$ or $p \big| i-1$ (as p is prime). If $p \big| i-1 \Rightarrow i = 1$ if $p \big| i+1 \Rightarrow i = p-1$. For $i = 1$ we have $bab^{-1} = a \Rightarrow ba = ab \Rightarrow o(a)o(b) = o(ab) = 2p$ (as $\gcd(o(a), o(b)) = 1$). Now, $H \trianglelefteq G \Rightarrow HK < G$ and $|HK| = \dfrac{|H||K|}{|H \cap K|}$. Now we will show that $H \cap K = \{e\}$. If not let $x \in H \cap K \Rightarrow o(x) \big| |H|$ as well as $o(x) \big| |K|$ which is impossible unless $o(x) = 1$. Hence H and K intersect trivially. Therefore, $|HK| = 2p$ and $HK = G$.

$$G = HK = \langle a, b : a^p = b^2 = e, ba = ab \rangle \tag{1}$$

$$G = HK = \langle a, b : a^p = b^2 = e, bab^{-1} = a^i \rangle \tag{2}$$

From (1) we get G is abelian and $o(ab) = 2p$ therefore, G is cyclic, hence $G \cong \mathbb{Z}/2p\mathbb{Z}$. Form (2) $bab^{-1} = a^i = a^{p-1} = a^{-1} \Rightarrow ba = a^{-1}b$. Hence, $G \cong D_{2p}$.
Case 2. When $p = 2$, $|G| = 2 \cdot 2 = 2^2$. Therefore, any group of order p^2 is abelian. If there exists an element $a \in G$ such that $o(a) = 4$ then $G \cong \mathbb{Z}/4\mathbb{Z}$. If there does not exists $a \in G$ such that $o(a) = 4$ then $o(a) = 2, \forall\ a \in G \setminus \{e\}$ (by Lagrange theorem). Therefore, $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Question 4.59. *Classify all the groups of order* pq *where* p, q *are primes and* $p < q$.

Ans. By Cauchy's theorem $\exists\ a, b \in G$ such that $o(a) = p$ and $o(b) = q$. Let $H = \langle a \rangle$ and $K = \langle b \rangle$. Since, $[G : K] = p$, least prime dividing the group's order, we have $K \trianglelefteq G$. Thus $HK < G$ and $|HK| = \dfrac{|H||K|}{|H \cap K|}$. By similar reason $H \cap K = \{e\}$ hence $|HK| = pq$ and therefore, $HK = G$. Since, $K \trianglelefteq G$, $aba^{-1} \in K \Rightarrow aba^{-1} = b^i$ (say) where $1 \leq i \leq q-1$. Now, $b = a^pba^{-p} = a^{p-1}(aba^{-1})a^{-(p-1)} = a^{p-1}b^ia^{-(p-1)} = \cdots = b^{i^p} \Rightarrow b^{i^p-1} = e \Rightarrow q \big| i^p - 1 \Rightarrow i^p \equiv 1\ (mod\ q)$.
Case 1. If $p \nmid q-1$. Then number of Sylow $p-$subgroup is $1 + kp$ with $k \geq 0$ and $1 + kp \big| q$. Since q is prime, $1 + kp = 1$ or $1 + kp = q$. If $1 + kp = 1$ then number of Sylow $p-$subgroup is 1 and $H \trianglelefteq G$. Therefore, $G \cong H \times K = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Since, $\gcd(p, q) = 1 \Rightarrow G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$. If $1 + kp = q \Rightarrow kp = q - 1 \Rightarrow p \big| q - 1$ which contradicts our assumption.

Question 4.60. *Find a normal subgroup of a group of order* 12.

Question 4.61. *Show that there exists a normal subgroup in a group of order* pqr *where* $p < q < r$ *and* p, q, r *are distinct primes.*

Question 4.62. *Every group of even order has an element of order* 2.

Ans. Let G be a group such that $|G| = 2n$. We construct a set $A = \{x \in G : x = x^{-1}\}$. Then $A \neq \emptyset$ as $e \in A$. Suppose $|A| = 1$ then $|G \setminus A| = 2n - 1$ and every element of $G \setminus A$ has inverse

different from itself thus $G \setminus A$ has even number of element which is impossible therefore A must have $e \neq x \in G$ such that $x = x^{-1} \Rightarrow x^2 = e$.

Question 4.63. *Show that in any group of order p^2 there exists a normal subgroup of order p and also show that normal subgroup of order p lies at the center of the group.*

Ans. Since any group of order p^2 is abelian we have $G = Z(G)$ abd by Cauchy's theorem $\exists\ a(\neq e) \in G$ such that $a^p = e$. Consider $H = \langle a \rangle$ then $H \trianglelefteq G$ since G is abelian and H lies at the center of G.

Question 4.64. *Show that in any group of order $2p$ there exists a normal subgroup of order p.*

Ans. By Cauchy's theorem there exists $a \in G$ such that $a^p = e$ and we consider $H = \langle a \rangle$ then $[G : H] = 2$ which imply $H \trianglelefteq G$.

Question 4.65. *Let G be a finite abelian group of order n and $m|n$, then G has a subgroup of order m.*

Ans. Given $|G| = n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ where p_i's are distinct primes. By Sylow's first theorem we get Sylow p_i-subgroup and we denote it by H_i then $|H_i| = p_i^{\alpha_i}$. Since G is abelian and $H_i \cap H_j = \{e\}$ with $H_i H_j = H_j H_i, \forall\ i \neq j$. Therefore, $G \cong H_1 \times \cdots \times H_r = H_1 \cdots H_r$. Since $m|n$ let us assume that $m = p_1^{\beta_1} \cdots p_r^{\beta_r}$ where $0 \leq \beta_i \leq \alpha_i$ with $1 \leq i \leq r$. Again by Sylow's first theorem we have subgroups of order

G is a finite abelian group of order $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ then $G \cong \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$.

Question 4.66.

Question 4.67.

Question 4.68.

5. Ring Theory

Definition 5.1. *Let R be an non empty set equipped with two binary operation $+$ and $\cdot$ then $(R,+,\cdot)$ is said to be ring if*
(i) $(R,+)$ is a commutative group
(ii) $(R,\cdot)$ is a semi-group and
(iii) $a\cdot(b+c)=a\cdot b+a\cdot c\ \forall a,b,c\in R$
R is said to be commutative ring with identity if $a\cdot b=b\cdot a\ \forall a,b\in R$ and $1\in R$.

For rest of this discussion our assumption is R is a commutative ring with identity unless and otherwise stated.

Remark 5.2. *If G is an arbitrary abelian group then G can be made into a ring by defining $ab=0$ for all $a,b\in G$. This ring has no multiplicative identity.*

5.1. **Sub-ring.**

Definition 5.3. *Let $S\subseteq R$, S is a subring of $(R,+,\cdot)$ if $(S,+|_{S\times S}:S\times S\to S,\cdot|_{S\times S}:S\times S\to S)$ is a ring.*

5.2. **Ideals.**

Definition 5.4. *Let I be an non-empty subset of R. I is said to be ideal of R if $a,b\in I\Rightarrow a+b\in I$ and $r\in R$, $a\in I\Rightarrow ra\in I$.*

Observation 5.5. *Every ideal is a subring of R but not every subring is ideal. For example $\mathbb{Z}$ is a subring of $\mathbb{Q}$ but not ideal. Consider the subring $R[x^2]$ of $R[x]$ which is not an ideal.*

Note that, if $1_R\in I$ then $I=R$. Let $A\subseteq R$ be a subset of R. Ideal generated by A means intersection of all ideals containing A say I. Then $A\subseteq I$. As, $a\in A\Rightarrow a\in I$ and $r\in R, a\in A\Rightarrow ra\in I$ then we have $\{r_1a_1+\cdots+r_na_n|r_i\in R,a_i\in A\}\subseteq I$. We claim $I=\{r_1a_1+\cdots+r_na_n|r_i\in R,a_i\in A\}$.

Proof. Suppose, $x=a_1r_1+\cdots+a_nr_n$ and $y=b_1r_1'+\cdots+b_nr_n'$ then $x+y\in\{r_1a_1+\cdots+r_na_n|r_i\in R,a_i\in A\}$. Pick, $r\in R$ and $x=a_1r_1+\cdots+a_nr_n\in\{r_1a_1+\cdots+r_na_n|r_i\in R,a_i\in A\}$ then $rx\in\{r_1a_1+\cdots+r_na_n|r_i\in R,a_i\in A\}$. Therefore, $\{r_1a_1+\cdots+r_na_n|r_i\in R,a_i\in A\}$ is an ideal. Clearly, $A\in\{r_1a_1+\cdots+r_na_n|r_i\in R,a_i\in A\}$.

Definition 5.6. *Let R be a ring. An ideal I is said to be finitely generated if it is generated by finite number of elements of R i.e, if $a_1,\cdots,a_n\in R$ then finitely generated ideal generated by $a_1,\cdots,a_n$ is*

$$I=\langle a_1,\cdots,a_n\rangle=\left\{\sum_{i=1}^{n}a_ir_i|\ r_i\in R\right\}$$

Definition 5.7. *Let R be a ring. An ideal is said to be principal ideal if it is generated by a single element i.e, if $a\in R$ principal ideal generated by $\langle a\rangle=\{ar|\ r\in R\}$.*

Definition 5.8. *Let R be a ring. An ideal $I\subseteq R$ is said to be prime ideal of R if $ab\in I\Rightarrow a\in I$ or $b\in I$. Equivalently I is a prime ideal if $a\notin I, b\notin I$ but $ab\in I$.*
Define, $specR=\{P\subseteq R|\ P$ is a prime ideal of $R\}$

Definition 5.9. *Let R be a ring. An ideal $M \subseteq R$ is said to be maximal ideal of R if $M \subseteq I$ where I is an ideal implies either $M = I$ or $I = R$.*
Define, $maxspecR = \{M \subseteq R |\ M$ is a maximal ideal of $R\}$

Theorem 5.10. *Let R be a commutative ring with identity then $maxspecR \neq \emptyset$.*

Proof. Let $\Sigma = \{I \subseteq R |\ I$ is an ideal of R and $I \neq R\ \}$, then $\Sigma \neq \emptyset$ as $(0) \in \Sigma$. Let use consider the partial order relation, set inclusion $\subseteq$ on Σ. Let $\{I_\lambda\}_{\lambda\in\Lambda}$ be a chain in Σ. We claim $\bigcup_{\lambda\in\Lambda} I_\lambda$ is an ideal in Σ. Let $x, y \in \bigcup_{\lambda\in\Lambda} I_\lambda$ then $x \in I_\alpha$ and $y \in I_\beta$, for some $\alpha, \beta \in \Lambda$. Since $\{I_\lambda\}_{\lambda\in\Lambda}$ is a chain, either $I_\alpha \subseteq I_\beta \Rightarrow x, y \in I_\beta$ or $I_\beta \subseteq I_\alpha \Rightarrow x, y \in I_\alpha$. Then $x + y \in I_\alpha$ or $I_\beta \Rightarrow x + y \in \bigcup_{\lambda\in\Lambda} I_\lambda$. Choose $r \in R$ and $x \in I_i$ then $rx \in I_i \Rightarrow rx \in \bigcup_{\lambda\in\Lambda} I_\lambda$. Hence $\bigcup_{\lambda\in\Lambda} I_\lambda$ is an ideal in R. Now, $\bigcup_{\lambda\in\Lambda} I_\lambda \neq R$ because if $\bigcup_{\lambda\in\Lambda} I_\lambda = R$ then $I_i = R$ for some $i \in \Lambda$ (contradiction). Therefore $\bigcup_{\lambda\in\Lambda} I_\lambda$ is an upper bound for a chain in Σ. By Zorn's Lemma Σ has an maximal element say m and $m \neq R$ since $m \in \Sigma$. If $m \in I$ I is an ideal then either $I = m$ or $I = R$. Then $m \in maxspecR \Rightarrow maxspecR \neq \emptyset$. □

Definition 5.11. *A non-zero element $r \in R$ is said to be zero divisor if $\exists\ s(\neq 0) \in R$ such that $rs = 0$.*

Example 5.12. *In the ring $\mathbb{Z}/6\mathbb{Z}$, $\bar{2}$ has zero divisor. More generally $\mathbb{Z}/n\mathbb{Z}$ has zero divisor where n is not a prime number.*

Definition 5.13. *A ring R is said to be integral domain if R does not contain any zero divisor i.e., if $ab = 0$ $(a, b \in R) \Rightarrow$ either $a = o$ or $b = 0$.*
Alternatively, A ring R is said to be integral domain if $\langle 0\rangle$ is the prime ideal of R.

Example 5.14. *The ring of integers $\mathbb{Z}$ is an integral domain. For any prime p, $\mathbb{Z}/p\mathbb{Z}$ is an integral domain.*

Remark. *An integral domain is also called entire ring(S Lang).*

Definition 5.15. *A ring is said to be field if $\langle 0\rangle$ is the only maximal ideal of R. In other word, R has no non trivial proper maximal ideal.*

Example 5.16. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Lemma 5.17. *A finite integral domain is a field.*

Proof. Let $0 \neq a_1 \in R$, if $a_1 = 1$ then it has inverse. Otherwise let $R = \{1, 0, a_1, \cdots, a_n\}$ (i.e., $a_1 \neq 1$). Consider,

$$\{a_1, 0, a_1^2, \cdots a_1 a_n\} \subseteq R \tag{3}$$

then $a_1 a_i \neq 0, 1 \leq i \leq n$ (R is integral domain). Let $a_i \neq a_j$ and $a_1 a_i = a_1 a_j$ gives $a_i = a_j$ therefore, $a_i \neq a_j \Rightarrow a_1 a_i \neq a_1 = a_i$. Form (1)

$$\{a_1, 0, a_1^2, \cdots, a_1 a_n\} = R = \{1, 0, \cdots, a_n\}$$

$1 \in R$ and $1 \neq 0, 1 \neq a_1$ then $\exists\ 1 \leq i \leq n$ such that $a_1 a_i = 1 \Rightarrow a_1$ has multiplicative inverse, hence R is a field. $\square$

Exercise 5.18. *Show that $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is an integral domain hence a field for any prime p.*

Exercise 5.19. *Show that above definition of field implies that every elements of field is unit.*

Definition 5.20. *Let R be a ring then R is said to be simple if R has no proper non trivial ideal i.e., only ideals of R is only zero ideal and R itself. In particular a commutative ring is simple iff it is a field.*

Observation 5.21. *Center of a simple ring is necessarily a field.*

Definition 5.22. *Let R, S be rings. $f : R \to S$ is said to be ring homomorphism if*
(i) $f(a+b) = f(a) + f(b)$
(ii) $f(ab) = f(a)f(b)$
(iii) $f(1_R) = 1_S$

Definition 5.23. *Let $f : R \to S$ be a ring homomorphism we define $Kerf = \{r \in R | f(r) = 0\}$ and $Imf = \{s \in S | f(r) = S\}$*

Check that $Kerf, Imf$ is subring of R and S respectively. $Kerf$ is an ideal of R. Pick $x, y \in Kerf \subseteq R$ then $f(x) = 0 = f(y)$. Now $f(x+y) = f(x) + f(y) = 0 \Rightarrow x + y \in Kerf$. Pick $s, s' \in Imf \subseteq S$ then $f(a) = s, f(b) = s'$ for some $a, b \in R$. Now $f(a+b) = f(a) + f(b) = s + s'$ $\Rightarrow s+s' \in Imf$. $x, y \in Kerf$ then $f(x) = 0 = f(y)$. Now $f(x+y) = f(x)+f(y) = 0 \Rightarrow x+y \in Kerf$. Pick $r \in R, x \in Kerf$, $f(rx) = f(r)f(x) = 0 \Rightarrow rx \in Kerf$.
Check that: Let $f : R \to S$ be a ring homomorphism $J \subseteq S$ is an ideal of S, then $f^{-1}(J) = \{x \in R | f(x) \in J\}$ is an ideal of R. Pick $a, b \in f^{-1}(J)$ then $f(a) = s, f(b) = s'$ for some $p, q \in S$ $\Rightarrow f(a+b = f(a)+f(b) = s+s' \Rightarrow f^{-1}(s+s') = a+b \in f^{-1}(J)$. Take $r \in R, a \in f^{-1}(J) \Rightarrow f(r) = r'$ for some r' and $f(a) = p \Rightarrow f(ra) = f(r)f(a) = r'p \in J$ since J is an ideal $\Rightarrow ra \in f^{-1}(J)$. Hence $f^{-1}(J)$ is an ideal of R.
Notation: $J^c = f^{-1}(J)$ is called the contraction of J.
Let $f : R \to S$ be a ring homomorphism, $I \subseteq R$ is an ideal of R, then $f(I)$ is need not be an ideal of S. $\phi : \mathbb{Z} \hookrightarrow \mathbb{Q}$ by $x \mapsto x$. $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$ but not of $\mathbb{Q}$ as $2 \in 2\mathbb{Z}$ and $\frac{1}{2} \in \mathbb{Q} \Rightarrow 2 \cdot \frac{1}{2} = 1 \notin 2\mathbb{Z}$.
Observation: If $\phi : R \to S$ is a surjective ring homomorphism, then $\phi(I)$ is an ideal of S where $I \subseteq R$ is an ideal. Let $a, b \in I$. $\phi(a) = p, \phi(b) = q$ Now, $\phi(a+b) = \phi(a) + \phi(b) = p + q$. Let $r' \in R$ and $\phi(a) \in \phi(I)$(then $a \in I$), $\exists\ r \in R$ such that $\phi(r) = r' \Rightarrow r'\phi(a) = \phi(r)\phi(a) = \phi(ra) \in \phi(I)$. Therefore, $\phi(I)$ is an ideal of S.
Observation *(i)* I, J be two ideals of R. $I + J = \{x + y | x \in I, y \in J\}$. $I + J$ is an ideal of R.
(ii) I, J be two ideals of R. $IJ = \left\{ \sum_{\substack{\text{finite} \\ \text{sum}}} xy : x \in I, y \in J \right\}$. IJ is an ideal of R.
(iii) $I \cap J$ is an ideal of R.
(iv) $(I : J) = \{x \in R |\ xJ \subseteq I\}$ is an ideal of R.
Let $f : R \to S$ be a ring homomorphism. $I \subseteq R$, $J \subseteq S$ be ideals.

(v) $f(I)$ is need not be an ideal of S but $I^e := f(I)S = \left\{ \sum_{\substack{\text{finite}\\ \text{sum}}} f(r)s : \ r \in I, s \in S \right\}$

(vi) If f is surjective then $f(I) = I^e$ hence $f(I)$ is an ideal of S.

Notation: $f(I) = I^e$ is called the expansion of I

(vii) If $P \in specS$ then $f^{-1}(P) \in specR$ hence $f : R \to S$ induces a map $f_* : specS \to specR$ by $P \mapsto f^{-1}(P) = P^c$.

$(viii)$ $I \subseteq I^{ec}$

(ix) $J^{ce} \subseteq J$

(x) $J_1 \subseteq J_2$ in S then $J_1^c \subseteq J_2^c$

(xi) $I_1 \subseteq I_2$ in R then $I_1^e \subseteq I_2^e$

(xii) $I^{ece} = I^e$

$(xiii)$ $J^{cec} = J^c$

Proof. (i) Pick $a, b \in I + J$ then $a = x_1 + y_1$ and $b = x_2 + y_2 \Rightarrow a + b = x_1 + y_1 + x_2 + y_2$ $\Rightarrow a + b \in I + J$. Take $r \in R$, $r(x + y) = rx + ry \in I + J$ (as I,J are ideals $rx \in I$, $ry \in J$). Hence $I + J$ is an ideal.

(ii) Let $a = \sum_{\substack{\text{finite}\\ \text{sum}}} x_1y_1$, $b = \sum_{\substack{\text{finite}\\ \text{sum}}} x_2y_2$. $a + b = \sum_{\substack{\text{finite}\\ \text{sum}}} x_1y_1 + \sum_{\substack{\text{finite}\\ \text{sum}}} x_2y_2 = \sum_{\substack{\text{finite}\\ \text{sum}}} xy \in IJ$. Let $r \in R$ and $a = \sum_{\substack{\text{finite}\\ \text{sum}}} xy$ then $ra = r\sum_{\substack{\text{finite}\\ \text{sum}}} xy = \sum_{\substack{\text{finite}\\ \text{sum}}} (rx)y \in IJ$.

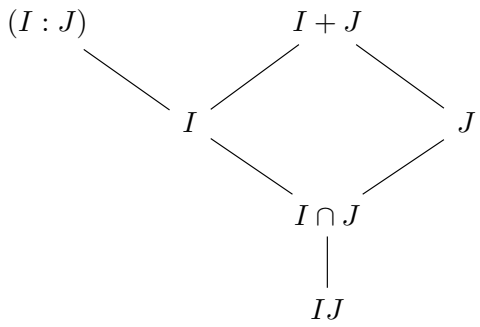
(iii) Let $x, y \in I \cap J \Rightarrow x, y \in I$ and $x, y \in J \Rightarrow x + y \in I$ and $x + y \in J$ then $x + y \in I \cap J$. Now, $r \in R$, $x \in I \cap J$ then $x \in I$, $x \in J \Rightarrow rx \in I$, $rx \in J \Rightarrow rx \in I \cap J$.

(iv) Take $x, y \in (I : J)$ then $xJ, yJ \subseteq I \Rightarrow (x+y)J \subseteq I \Rightarrow x+y \in (I : J)$. Let $r \in R$ and $x \in (I : J)$ then $xj \subseteq I \Rightarrow (rx)J \subseteq I \Rightarrow rx \in (I : J)$.

(v) Let $x = \sum_{\substack{\text{finite}\\ \text{sum}}} f(r)s$ and $y = \sum_{\substack{\text{finite}\\ \text{sum}}} f(r')s'$ then $x+y = \sum_{\substack{\text{finite}\\ \text{sum}}} f(r)s + \sum_{\substack{\text{finite}\\ \text{sum}}} f(r')s' \Rightarrow x+y \in f(I) = I^e$. Let $p \in S \Rightarrow p\sum_{\substack{\text{finite}\\ \text{sum}}} f(r)s = \sum_{\substack{\text{finite}\\ \text{sum}}} f(r)(ps) \in I^e$, so I_e is an ideal.

(vi) □

Lattice diagram of ideal of R :



Question 5.24. *Let $I = \langle a, b\rangle$ then what will be the generators of I^2.*

Ans. As $I = \langle a, b\rangle$, $I = \{ra + sb : r, s \in R\}$. We know that

$$\begin{aligned} I^2 &= \left\{ \sum_{\substack{\text{finite}\\ \text{sum}}} xy : x, y \in I \right\} \\ &= \left\{ \sum_{\substack{\text{finite}\\ \text{sum}}} (r_1a + s_1b)(r_2a + s_2b) : r_i, s_i \in R \right\} \\ &= \left\{ \sum_{\substack{\text{finite}\\ \text{sum}}} r_1r_2a^2 + s_1s_2b^2 + (r_1s_2 + s_1r_2)ab : r_i, s_i \in R \right\} \\ &= \langle a^2, ab, b^2\rangle \end{aligned}$$

We have examples of ideals such that $I \neq I^2$.

Theorem 5.25 (Multinomial theorem)**.** $(f_1+f_2+\cdots+f_k)^n = \displaystyle\sum_{i_1+i_2+\cdots+i_k=n} \frac{n!}{i_1!i_2!\cdots i_k!} f_1^{i_1} f_2^{i_2} \cdots f_k^{i_k}$ *where* $0 \leq i_l \leq n$, $1 \leq l \leq k$

Definition 5.26 (Radical Ideal)**.** *Let $I \subseteq R$ be an ideal of R. Define $\sqrt{I} = \{x \in R : x^n \in I$ for some $n \in \mathbb{N}$ $\}$*

Claim: $\sqrt{I}$ is an ideal of R called radical of I.

Proof. Let $x, y \in \sqrt{I} \Rightarrow x^{n_1}, y^{n_2} \in I$ for some $n_1, n_2 > 0$. Now, $(x+y)^{n_1+n_2} = \displaystyle\sum_{r=0}^{n_1+n_2} \binom{n_1+n_2}{r} x^r y^{n_1+n_2-r}$. If $r < n_1$, then $n_1 + n_2 - r > n_2 \Rightarrow y^{n_1+n_2-r} \in I \Rightarrow x^r y^{n_1+n_2-r} \in I$. If $r \geq n_1$, then $x^r \in I$ $\Rightarrow x^r y^{n_1+n_2-r} \in I$ therefore $(x + y)^{n_1+n_2} \in I \Rightarrow x + y \in \sqrt{I}$. Let $r \in R$ then $(rx)^{n_1} = r^{n_1}x^{n_1} \in I$ $\Rightarrow rx \in \sqrt{I}$. So, $\sqrt{I}$ is an ideal. □

Definition 5.27 (Nil Radical)**.** *Let R be a commutative ring with identity. $nil(R) = \{x \in R|$ $x^n = 0$ for some $n > 0\}$ then $nil(R)$ is an ideal of R called nil radical.*

Notation: $\sqrt{0} = nil(R)$

$x, y \in nil(R)$ then $x^n = 0$, $y^m = 0$. $(x+y)^{n+m} = \displaystyle\sum_{r=0}^{m+n} \binom{k}{r} x^r y^{n+m-r}$ if $k \geq m$ then $x^k = 0$ if $k < m$ then $n + m - r \geq n \Rightarrow y^{n+m-r} = 0$. Therefore $(x + y)^{m+n} = 0 \Rightarrow x + y \in nil(R)$. Take $a \in R$, $x \in nil(R)$ then $(ax)^n = a^n x^n = 0$, so $nil(R)$ is an ideal.

Lemma 5.28. *Let R be a commutative ring with identity and S be a subset of R which is disjoint from an $\mathfrak{a}$ then*

$$\sum = \{I \subseteq R : I \text{ is an ideal of } R \text{ and } \mathfrak{a} \subseteq I, I \cap S = \emptyset\}$$

has a maximal element. Moreover, if S is multiplicative then the maximal element is a prime ideal.

Proof. Clearly $\sum$ is non empty as $\mathfrak{a} \in \sum$. Now we cosider a chain of ideal $\{I_\lambda\}_{\lambda\in\Lambda}$ in $\sum$ then $\bigcup_{\lambda\in\Lambda} I_\lambda$ is an ideal. If $\bigcup_{\lambda\in\Lambda} I_\lambda \cap S \neq \emptyset$ then $I_\lambda \cap S \neq \emptyset$ for some $\lambda \in \Lambda$ which is a contradiction therefore, $\bigcup_{\lambda\in\Lambda} I_\lambda \in \sum$. So, every chain in $\sum$ has a upper bound in $\sum$ by Zorn's lemma $\sum$ has a maximal element say P.

Let S be a multiplicative set, we show that P is a prime ideal. If not assume $a \notin P, b \notin P$ but $ab \in P$ clearly, $P \subsetneq P + \langle a\rangle$ and $P \subsetneq P + \langle b\rangle$. Since, P is maximal in $\sum$, $P + \langle a\rangle$ and $P + \langle b\rangle \notin \sum$ and therefore, $S \cap P + \langle a\rangle \neq \emptyset$. Let $f_1 = p_1 + at_1$ and $f_2 = p_2 + bt_2 \Rightarrow f_1 f_2 = (p_1 + at_2)(p_2 + bt_2) = p_1p_2 + bp_1t_2 + p_2at_1 + abt_1t_2 \in P$ ($\because ab \in P$) which is a contradiction. Therefore, P is a prime ideal. □

Theorem 5.29. *Let R be a commutative ring with identity then* $\sqrt{0} = \bigcap_{P\in specR} P$

Proof. Let $x \in nil(R)$, then $x^n = 0 \in P$ then $x^n \in P$ for all $P \in specR \Rightarrow x \in P$ for all $P \in specR \Rightarrow x \in \bigcap_{P\in specR} P \Rightarrow nil(R) \subseteq \bigcap_{P\in specR} P$. For the other inclusion, we show that if $x \notin \sqrt{0} \Rightarrow x \notin \bigcap_{P\in \operatorname{spec} R} P$. Let $x \notin nil(R)$ then $x^n \neq 0$ for all $n \in \mathbb{N}$. Let us consider the set

$$\sum = \{I \subseteq R : I \text{ is an ideal of } R \text{ and } x^n \notin I, \forall\ n \in \mathbb{N}\}$$

then $\sum \neq \emptyset$ as $(0) \in \sum$. Let $\{I_\lambda\}_{\lambda\in\Lambda}$ be a chain in $\sum$. Claim: $\bigcup_{\lambda\in\Lambda} I_\lambda \in \sum$. If $x^n \in \bigcup_{\lambda\in\Lambda} I_\lambda \in \sum$ for some $n \in \mathbb{N}$ then $x^n \in I_\lambda$ for some $\lambda \in \Lambda$ a contradiction. Therefore each chain in $\sum$ has an upper bound $\bigcup_{\lambda\in\Lambda} I_\lambda \in \sum$. By Zorn's lemma $\sum$ has a maximal element say P. Claim: P is a prime ideal. If not let $a, b \notin P$ but $ab \in P$. Then $P \subsetneq P + (a)$ and $P \subsetneq P + (b)$ but P is a maximal element in $\sum \Rightarrow P + (a) \notin \sum$ and $P + (b) \notin \sum$ then $\exists\ m, n \in \mathbb{N}$ such that $x^m \in P + (a)$ and $x^n \in P + (b) \Rightarrow x^m = r_1 + at_1$ and $x^n = r_2 + bt_2$ where $r_1, r_2 \in P$ and $t_1, t_2 \in R \Rightarrow x^m \cdot x^n = (r_1 + at_1)(r_2 + bt_2) = r_1r_2 + r_1bt_2 + r_2at_1 + abt_1t_2 \in P$ (as $ab \in P$) $\Rightarrow x^{n+m} \in P$ a contradiction as $P \in \sum$. Therefore P is a prime ideal and $x^n \notin P\ \forall n \in \mathbb{N}$. In particular $x^1 \notin P \Rightarrow x \notin \bigcap_{P\in specR} P$. Therefore $\bigcap_{P\in specR} P \subseteq nil(R)$. Therefore $\bigcap_{P\in specR} P = nil(R)$. □

Corollary 5.30. $\sqrt{I} = \bigcap_{P\in specR} P$ *where* $I \subseteq P$.

Proof. Let $x \in \sqrt{I} \Rightarrow x^n \in I \subseteq P$ for some $n \in \mathbb{N}$ then $x \in P \Rightarrow \sqrt{I} \subseteq P \Rightarrow \sqrt{I} \subseteq \bigcap_{P\in \operatorname{spec} R} P$. Now, assume that $x \notin \sqrt{I} \Rightarrow x^n \notin I, \forall\ n \in \mathbb{N}$. Therefore, $\{1, x, x^2, \cdots\}$ is a multiplicative set disjoint from I and by Lemma 5.28 there is a prime ideal P containing I and not containing x. Thus $\sqrt{I} = \bigcap_{P\in specR} P$ where $I \subseteq P$. □

Observation: (*i*) $I \subseteq \sqrt{I}$.
(*ii*) $I \subseteq J \Rightarrow \sqrt{I} \subseteq \sqrt{J}$.

(iii) If $P \in \operatorname{spec} R$ then $\sqrt{P^n} = P \ \forall \ n \in \mathbb{N}$.
(iv) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
(v) $\sqrt{\sqrt{I}} = \sqrt{I}$
(vi) If I is an ideal then $\sqrt{I^n} = \sqrt{I}$
(vii) Suppose, I, J are ideals of R. If $\sqrt{I}, \sqrt{J}$ are comaximal then I, J are also comaximal.
$(viii)$ If $x \in \sqrt{0}$ then $1 + x$ is a unit.
(ix) Units of $R = R - \bigcup_{m \in \operatorname{maxspec} R} m$.
Ans. (i) $x \in I \Rightarrow x^1 \in I \Rightarrow x \in \sqrt{I}$, hence $I \subseteq \sqrt{I}$.
(ii) Pick $x \in \sqrt{I} \Rightarrow x^n \in I \subseteq J \Rightarrow x \in \sqrt{J} \Rightarrow \sqrt{I} \subseteq \sqrt{J}$.
(iii) $P^n \subseteq P$ for all $n \in \mathbb{N}$ then $\sqrt{P^n} \subseteq \sqrt{P}$. Claim $\sqrt{P} = P$. We have $P \subseteq \sqrt{P}$. Let $x \in \sqrt{P}$ $\Rightarrow x^n \in P$ for some $n \Rightarrow x \in P$ (since P is prime ideal) $\Rightarrow \sqrt{P} \subseteq P$ therefore $\sqrt{P} = P$. Then we have $\sqrt{p^n} \subseteq \sqrt{P} = P$. Let $x \in P \Rightarrow x^n \in P^n \subseteq \sqrt{P^n}$. Hence $P \subseteq \sqrt{P^n} \Rightarrow P = \sqrt{P^n}$
(iv) Pick $x \in \sqrt{I \cap J} \Rightarrow x^n \in I \cap J \Rightarrow x^n \in I$ and $x^n \in J \Rightarrow x \in \sqrt{I} \cap \sqrt{J}$ hence, $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$. Again, let $y \in \sqrt{I} \cap \sqrt{J} \Rightarrow y \in \sqrt{I}$ and $y \in \sqrt{J} \Rightarrow y^n \in I, J \Rightarrow y \in \sqrt{I \cap J} \Rightarrow \sqrt{I} \cap \sqrt{J} \subseteq \sqrt{I \cap J}$ therefore, $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
$(viii)$ If $x \in \sqrt{0}$ then $x^n = 0$ for some natural number n but this gives $(1 + x)(1 - x + x^2 + \cdots + (-1)^{n-1}x^{n-1}) = 1 - x^n = 1$ therefore, $1 + x$ is a unit.
(ix) As every ideal is contained in some maximal ideal so if we pick any $x \in \bigcup_{m \in maxspecR} m$ then x must be in some ideal of R so x cannot be a unit.

Definition 5.31. *A ring R is said to be reduced if $nil(R) = 0$.*

Observation 5.32. *For any ring R, $R/nil(R)$ is reduced.*

Definition 5.33. *Let R be any ring. We define the ideal $Jac(R) = \bigcap_{m \in maxspecR} m$.*

$Jac(R)$ is called the Jacobson ideal of R.

5.3. **Prime avoidance lemma.**

Theorem 5.34. *Let $P_1, \cdots, P_n \in \operatorname{spec} R$ then*

$$I \subseteq \bigcup_{i=1}^{n} P_i \Rightarrow I \subseteq P_i \text{ for some } i.$$

Proof. We have to prove that if $I \nsubseteq P_i, \ \forall \ 1 \leq i \leq n$ then $I \nsubseteq \bigcup_{i=1}^{n} P_i$. We proceed by induction on n. If $n = 1$ then we are done. Suppose, the statement is true for $n - 1$ ideals. We consider $P_2, \cdots, P_n$ and we have $I \nsubseteq P_i, \ 2 \leq i \leq n$ then by induction hypothesis $I \nsubseteq \bigcup_{i=2}^{n} P_i$ then $\exists x_i \in I$ such that $x \notin \bigcup_{i=2}^{n} P_i$ i.e., $x \notin P_i, \ 2 \leq i \leq n$. If $x_1 \notin P_1$ then $x_1 \notin \bigcup_{i=1}^{n} P_i$ and hence $I \nsubseteq \bigcup_{i=1}^{n} P_i$ and we are done. So we may assume $x_1 \in P_1$ and $x_1 \notin P_i, \ 2 \leq i \leq n$. Now we consider $\{P_1, P_2, \cdots, P_n\} \setminus \{P_2\}$ and

by similar approach we get $x_2 \in I$ with $x_2 \in P_2$ and $x_2 \notin P_i,\ \{1,\ldots,n\} \setminus \{2\}$ and lastly we get $x_n \in I$ with $x_n \in P_n$ and $x_n \notin P_1,\ 1 \leq i \leq n-1$. We consider

$$x = x_2 \cdots x_n + x_1 x_3 \cdots x_n + x_1 x_2 x_4 \cdots x_n + \cdots + x_1 \cdots x_{n-1}$$

then $x \in I$. We claim that $x \notin \bigcup_{i=1}^{n} P_i$ i.e., $x \notin P_1,\ 1 \leq i \leq n$. If $x \in P_i$ for some i. Let

$$y_i = x_1 \cdots \widehat{x_i} \cdots x_n$$

then $x_i | y_j$ for $i \neq j \Rightarrow y_j \in P_i\ [x_i \in P_i] \Rightarrow \sum_{\substack{j=1 \\ j \neq i}}^{n} y_j \in P_i \Rightarrow x - \sum_{\substack{j=1 \\ j \neq i}}^{n} y_j \in P_i\ [\because x \in P_i] \Rightarrow y_i \in P_i \Rightarrow$ $x_1 \cdots \widehat{x_i} \cdots x_n \in P_i$ but $x_j \notin P_i,\ j \neq i$ [since P_i is a prime ideal] $\Rightarrow x \notin \bigcup_{i=1}^{n} P_i$. Hence, $I \nsubseteq$. □

Remark 5.35. *Prime avoidance lemma is not true for infinite number of prime ideals.*

Example 5.36. *Let $R = K[x_1, \cdots, x_n, \cdots]$ (infinitely many variables). Let $I = (x_1, \cdots, x_n, \cdots), P_i = (x_1, \cdots, x_i), i \in \mathbb{N}$ then $R/P_i \cong K[x_{i+1}, x_{i+2}, \cdots,]$ (integral domain) then $P_i \in$ spec R. But $I \subseteq \bigcup_{i \in \mathbb{N}} P_i$ and $I \subseteq P_i\ \forall i \in \mathbb{N}$.*

Theorem 5.37 (Prime avoidance lemma)**.** *Let R be a commutative ring with 1, I be an ideal of R and $f \in R$. Suppose $P_1, \cdots, P_r \in$ spec R such that $f + I = \bigcup_{i=1}^{r} P_k$ then $\langle f, I \rangle \subseteq P_i$ for some $i \in \{1, \cdots, r\}$.*

Proof. Let $\sum$ be the collection of all $s \in \mathbb{N}$ such that there exist $t \in R$ and an ideal J of R such that $t + J \subseteq \bigcup_{i=1}^{s} P_i$ but $\langle t, J \rangle \nsubseteq P_i, 1 \leq i \leq s$. If $\sum \neq \emptyset$ then by well ordering principle of Natural numbers, $\sum$ has a least element say $l \in \sum$. So there exist $g \in R$ and $\mathfrak{A} \subseteq R$ such that $g + \mathfrak{A} \subseteq \bigcup_{i=1}^{l} P_i$ but $\langle g, \mathfrak{A} \rangle \nsubseteq P_i, 1 \leq i \leq l$. We note that $l \geq 2$ and $P_i \nsubseteq P_j$. We claim that $g \in \bigcap_{i=1}^{l} P_i$. If not, $g \notin P_{i_0}$ for some $i_0 \in \{1, \cdots, l\}$, then $(g + P_{i_0}\mathfrak{A}) \cap P_{i_0} = \emptyset$ hence $g + P_{i_0}\mathfrak{A} \subseteq \bigcup_{\substack{j=1 \\ j \neq i_0}}^{l} P_j$. Since l is the minimal element of $\sum$, we have $\langle g, P_{i_0}\mathfrak{A} \rangle \subseteq P_{j_0}$ for some $j_0 \in \{1, \cdots, l\}$ but $j_0 \neq i_0$. Then $P_{i_0}\mathfrak{A} \subseteq P_{j_0} \Rightarrow P_{i_0} \subseteq P_{j_0}$ which is a contradiction (since if $\mathfrak{A} \subseteq P_{j_0}$ then $\langle g, P_{j_0}\mathfrak{A} \rangle \subseteq P_{j_0}$ implies $g \in P_{j_0} \Rightarrow \langle g, \mathfrak{A} \rangle \subseteq P_{j_0}$ but $\langle g, \mathfrak{A} \rangle \nsubseteq P_i$ for all $1 \leq i \leq l$ so, $\mathfrak{A} \nsubseteq P_{j_0}$). Therefore, $g \in \bigcap_{i=1}^{l} P_i \Rightarrow \mathfrak{A} \subseteq \bigcup_{i=1}^{l} P_i \Rightarrow \mathfrak{A} \subseteq P_s$ for some $1 \leq s \leq l$. Then by our assumption $\langle g, \mathfrak{A} \rangle \subseteq P_s$ but $\sum \neq \emptyset$ which is a contradiction. Hence our assumption is not true that is $\sum = \emptyset$. □

Proposition 5.38. *Let $I_1, \cdots, I_r$ be ideals of R and $P \in$ spec R. If $\bigcap_{k=1}^{r} I_k \subseteq P$ then $I_k \subseteq P$ for some $k \in \{1, \cdots, r\}$.*

Proof. Since $\prod_{k=1}^{r} I_k \subseteq \bigcap_{k=1}^{r} I_k \subseteq P$, by definition of prime ideal $I_k \subseteq P$ for some $1 \leq k \leq r$. □

Theorem 5.39 (Module theoretic version)**.** *Let R be a commutative ring with 1 and $P_1, \cdots, P_m \in spec\, R$, M be an $R-$module and $x_1, \cdots, x_n \in M$. Consider the submodule $N = \langle x_1, \cdots, x_n \rangle$ of M. If $N_{P_j} \nsubseteq P_j M_{P_j}, j = 1, \cdots, m$ then there exist $a_2, \cdots, a_n \in R$ such that $x_1 + \sum_{i=1}^{n} a_i x_i \notin P_j M_{P_j}$.*

5.4. **Quotient Ring.**

Definition 5.40. *Let R be a ring and $I \subseteq R$ be a ideal of R. We consider the set $R/I := \{x + I | x \in R\}$ the set of all left coset of I in the additive group $(R, +)$.*

Note that $x + I = y + I \Leftrightarrow x - y \in I$.
Define $+ : R/I \times R/I \to R/I$ by $(x + I, y + I) \mapsto (x + y) + I$ and $\cdot : R/I \times R/I \to R/I$ by $(x + I, y + I) \mapsto (xy) + I$.
Claim: '+,' and '$\cdot$' are well-defined. Let $x_1 + I = y_1 + I$ and $x_2 + I = y_2 + I \Rightarrow x_i - y_i \in I$, $i \in \{1, 2\}$. Suppose, $x_i = y_i + t_i$ where $t_i \in I$, $i \in \{1, 2\}$. So, $(x_1 + x_2) - (y_1 + y_2) = t_1 + t_2 \in I$ $\Rightarrow (x_1 + x_2) - (y_1 + y_2) \in I \Rightarrow (x_1 + x_2) + I = (y_1 + y_2) + I$. Therefore, $+$ is well-defined. Now $x_1x_2 = t_1y_2 + t_1y_2 + t_2y_1 + t_1t_2 \Rightarrow x_1x_2 - y_1y_2 \in I \Rightarrow x_1x_2 + I = y_1y_2 + I$. Hence, $\cdot$ is well-defined. Check $(R/I, +, \cdot)$ is a commutative ring with identity $0 + I$. Note that $x + I = 0 + I \Leftrightarrow x \in I$.

6. Homomorphism of rings

Definition 6.1. *Let R, S be rings. $f : R \to S$ is said to be ring homomorphism if*
(i) $f(a + b) = f(a) + f(b)$ $\forall a, b \in R$
(ii) $f(ab) = f(a)f(b)$ $\forall a, b \in R$
(iii) $f(1_R) = 1_S$
Here S is said to be R-algebra if there exists a ring homomorphism from R to S.

Note that for any ring R, there is a canonical ring homomorphism $f : \mathbb{Z} \to R$ defined by $n \mapsto \underbrace{1_R + \cdots + 1_R}_{n \text{ times}}$, $-n \mapsto \underbrace{(-1_R) + \cdots + (-1_R)}_{n \text{ times}}$

Definition 6.2. *Let $f : R \to S$ be a ring homomorphism we define $Ker f = \{r \in R | f(r) = 0\}$ and $Im f = \{s \in S | f(r) = S\}$*

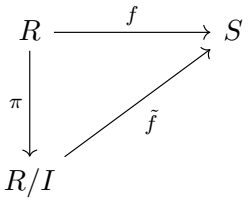
Check that $Ker f$ is an ideal of R and $Im f$ is a subring of S.

Definition 6.3. *Let $f : R \to S$ be a ring homomorphism. f is said to be an isomorphism if $\exists$ another ring homomorphism $g : S \to R$ such that $g \circ f = id_R$ and $f \circ g = id_S$.*

Theorem 6.4. *$f : R \to S$ is an isomorphism iff f is bijective.*

Proof. $(\Rightarrow)$ Obvious.
$(\Leftarrow)$ Suppose, f is bijective then $\exists\, g : S \to R$ such that $f \circ g = id_S$ and $g \circ f = id_R$. We need to check that g is a ring homomorphism. Let $s_1, s_2 \in S$. $(f \circ g)(s_1 + s_2) = s_1 + s_2 = (f \circ g)(s_1) + (f \circ g)(s_2)$ $\Rightarrow f[g(s_1+s_2)-g(s_1)-g(s_2)] = 0$ (since f is a homomorphism). As f is bijective f is injective also so $g(s_1+s_2) = g(s_1)+g(s_2)$. Again $f(g(s_1s_2)) = s_1s_2 = f(g(s_1))f(g(s_2)) \Rightarrow f[g(s_1s_2)-g(s_1)g(s_2)] = 0$ $\Rightarrow g(s_1s_2) = g(s_1)g(s_2)$. Hence g is a ring homomorphism. □

Theorem 6.5 (First Isomorphism Theorem)**.** *Let $f : R \to S$ be a ring homomorphism. $I \subseteq \operatorname{Ker} f$ be an ideal of R then there exists a unique ring homomorphism $\tilde{f} : R/I \to S$ such that the diagram commutes i.e., $\tilde{f} \circ \pi = f$.*



Moreover, if $I = \operatorname{Ker} f$ then $\tilde{f}$ is injective. Therefore, $R/\operatorname{Ker} f \simeq \operatorname{Im} f$
By definition $\operatorname{Im} \tilde{f} = \operatorname{Im} f$ so that if $\tilde{f}$ is surjective then f is also surjective then $R/\operatorname{Ker} f \simeq S$.

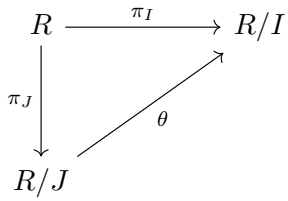
Proof. Define, $\tilde{f} : R/I \to S$ by $(x + I) \mapsto f(x)$. Claim: $\tilde{f}$ is well defined. Let, $x + I = y + I \Rightarrow x - y \in I \subseteq \operatorname{Ker} f \Rightarrow f(x - y) = 0 \Rightarrow f(x) = f(y) \Rightarrow \tilde{f}(x + I) = \tilde{f}(y + I)$. Therefore $\tilde{f}$ is well-defined. $[\tilde{f}(x + y + I) = f(x + y) \Rightarrow f(x) + f(y)$ (as f is a ring homomorphism) $\Rightarrow \tilde{f}(x + y + I) = \tilde{f}(x + I) + \tilde{f}(y + I)$ and $\tilde{f}(xy + I) = f(xy) = f(x)f(y) = \tilde{f}(x + I)\tilde{f}(y + I)$ so, $\tilde{f}$ is a ring homomorphism.] Uniqueness: Suppose g is another ring homomorphism such that $g : R/I \to S$ such that $g \circ \pi = f$. Then $f(x) = g \circ \pi(x) \Rightarrow \tilde{f}(x + I) = f(x) = g(x + I)$ so we have $g = \tilde{f}$. Therefore $\tilde{f}$ is unique. Now suppose $I = \operatorname{Ker} f$ then $\tilde{f}(x + \operatorname{Ker} f) = \tilde{f}(y + \operatorname{Ker} f) \Rightarrow f(x) = f(y) \Rightarrow f(x - y) = 0 \Rightarrow x - y \in \operatorname{Ker} f \Rightarrow x + \operatorname{Ker} f = y + \operatorname{Ker} f$ hence $\tilde{f}$ is injective. Therefore, $R/\operatorname{Ker} f \cong \operatorname{Im} \tilde{f} = \operatorname{Im} f$ (by definition $\operatorname{Im} \tilde{f} = \operatorname{Im} f$). If $\tilde{f}$ is surjective then so f hence $S = \operatorname{Im} \tilde{f} = \operatorname{Im} f$. Therefore, $R/\operatorname{Ker} f \cong S$. □

Question 6.6. *What are the ideals of R/I?*

Ans. Ideals of R/I are exactly the set $\Sigma = \{J/I : I \subseteq J \subseteq R$ and J is an ideal of $R\}$. We consider the surjective ring homomorphism $\pi : R \to R/I$. Let Q be an ideal of R/I then $\pi^{-1}(Q) = Q^c$ is an ideal of R now $0 + I \subseteq Q \Rightarrow \pi^{-1}(0 + I) \subseteq Q^c \Rightarrow I \subseteq Q^c$. Claim: $Q^c/I = Q$, since π is surjective $\pi(\pi^{-1}(Q)) = Q = \pi(Q^c) = Q^c/I$. Conversely, if we take $J/I \subseteq R/I$ with $I \subseteq J \subseteq R$ then $(x + I), (y + I) \in J/I$ where $x, y \in J$ as $x + y \in J \Rightarrow (x + I) + (y + I) = (x + y) + I \in J/I$. Let $r + I \in R/I$ and $x + I \in J/I$ as J is an ideal $r \in R$ and $x \in J$ we have $rx \in J$ so that $rx/I \in J/I$. Therefore, J/I is an ideal of R/I.

Theorem 6.7 (Third isomorphism theorem)**.** *We have seen that if $I \subseteq J \subseteq R$ then J/I is an ideal of R/I hence prove that $\dfrac{R/I}{J/I} \cong \dfrac{R}{J}$.*

Proof. Define $\pi_J : R \to R/J$ by $x \mapsto x + J$ now, $I \subseteq J = \operatorname{Ker} \pi_J$ by first isomorphism theorem there exists an unique ring homomorphism $\theta : R/I \to R/J$ such that the diagram is commutative i.e., $\pi_J = \theta \circ \pi_I$.



Claim: $\operatorname{Ker}\theta = J/I$. Let $x+I \in \operatorname{Ker}\theta \Leftrightarrow \theta(x+I) = 0+J \Leftrightarrow x+J = 0+J \Leftrightarrow x+J$ hence, $\operatorname{Ker}\theta = J/I$ as π_J is surjective by first isomorphism theorem $\dfrac{R/I}{J/I} \cong \dfrac{R}{J}$. □

Theorem 6.8. *Let P be an prime ideal of an ring R then R/P is an integral domain.*

Proof. As R is commutative ring with 1_R and $P \in \operatorname{spec} R$, we get R/P is also commutative ring. Let $(a+P)(b+P) = 0+P \Rightarrow ab+P = 0+P \Rightarrow ab \in P$ as P is an prime ideal and $ab \in P$ we have either $a \in P$ or $b \in P$ then $a+P = 0+P$ or $b+P = 0+P$ therefore, R/P is an integral domain. Conversely, suppose, R/P is an integral domain and let $x, y \in R$ such that $xy \in P$ then $xy+P = 0+P$ in R/P this implies $(x+P)(y+P) = 0+P$. As R/P is integral domain we have either $x+P = 0+P$ or $y+P = 0+P$ hence, $x \in P$ or $y \in P$ this gives $P \in \operatorname{spec} R$. □

Theorem 6.9. *Let $m \in \operatorname{maxspec} R$ then R/m is a field.*

Proof. As R is commutative ring with 1_R and $m \in \operatorname{maxspec} R$, we get R/m is also commutative ring. Let $x+m \in R/m$ with $x+m \neq 0+m \Rightarrow x \notin m \Rightarrow m \subsetneq m+(x)$ since m is a maximal ideal $m+(x) = R \Rightarrow 1 \in m+(x) \Rightarrow 1 = t+xy$ where $t \in m$ and $y \in R$ then $xy-1 \in m \Rightarrow xy+m = 1 = m \Rightarrow (x+m)(y+m) = 1+m$ hence R/m is a field.
Conversely, R/m is a field suppose, $m \subseteq I$ if $m \neq I$ $\exists x \in I$ such that $x \in m$ this gives $x+m \neq 0+m$ then $\exists y \neq 0$ such that $(x+m)(y+m) = 1+m$ [as R/m is a field] then we have $xy-1 \in m \subseteq I$ since $x \in I \Rightarrow xy \in I \Rightarrow xy-(xy-1) \in I \Rightarrow 1 \in I \Rightarrow I = R$ hence $m \in \operatorname{maxspec} R$.

Alternative proof: Let $m \subseteq I \subseteq R$ then $I/m \subseteq R/m$ is an ideal. If m is an maximal ideal then either $I = m$ and $m = R$ then ideals of R/m is $0+m$ or R/m hence R/m is a field. Conversely, if R/m is a field, ideals of R/m is zero ideal and R/m itself then $m \subseteq I \subseteq R$ implies either $m = I$ and $I = R$ hence m is a maximal ideal. □

Question 6.10. *Find* $\operatorname{spec}(R/I)$.

Ans. Let us take an ideal P/I where $I \subseteq P$ and $P \in \operatorname{spec} R$ then $\dfrac{R/I}{P/I} \cong R/P$. As $P \in \operatorname{spec} R$ and R is a commutative ring R/P is a integral domain then $P/I \in \operatorname{spec}(R/I)$. Conversely, if $P/I \in \operatorname{spec}(R/I)$ then $\dfrac{R/I}{P/I} = R/P$ is an integral domain hence $P \in \operatorname{spec} R$.

Question 6.11. *Find* $\operatorname{maxspec}(R/I)$.

Ans. Let us take an ideal m/I where $I \subseteq m$ and $m \in \operatorname{maxspec} R$ then $\dfrac{R/I}{m/I} \cong R/m$. As $m \in \operatorname{maxspec} R$ and R is a commutative ring R/m is a field then $m/I \in \operatorname{maxspec}(R/I)$. Conversely, if $m/I \in \operatorname{maxspec}(R/I)$ then $\dfrac{R/I}{m/I} = R/m$ is a field hence $m \in \operatorname{maxspec} R$.

Corollary 6.12. $\operatorname{maxspec} R \subseteq \operatorname{spec} R$

Proof. Let $m \in \operatorname{maxspec} R \Rightarrow R/m$ is a field $\Rightarrow R/m$ is an integral domain $\Rightarrow m \in \operatorname{spec} R$ therefore, $\operatorname{maxspec} R \subseteq \operatorname{spec} R$. □

Corollary 6.13. $\sqrt{0} \subseteq \operatorname{Jac} R$

Proof. Let $x \in \sqrt{0}$ and $m \in \operatorname{maxspec} R \subseteq \operatorname{spec} R \Rightarrow x^n = 0 \in m \Rightarrow x \in m \Rightarrow m \in \bigcap_{m \in maxspec\ R} m \Rightarrow x \in \operatorname{Jac} R$. □

Definition 6.14. *A ring is said to be local if it has unique maximal ideal.*

Construction of local ring: Let R be a commutative ring with 1 and $m \in \operatorname{maxspec} R$ then for any $k \in \mathbb{N}^+$ the ring R/m^k is local. Moreover, $\operatorname{spec} R/m^k = \{m/m^k\}$. Every prime ideal of R/m^k is of the form P/m^k where $m^k \subseteq P$ and P is a prime ideal of R. Taking radical on both side we get, $\sqrt{m^k} \subseteq \sqrt{P} \Rightarrow m \subseteq P$ since m is an maximal ideal, $m = P$ hence $spec(R/m^k) = \{m/m^k\}$.

Example 6.15. *$\mathbb{Z}/p^n\mathbb{Z}$ is a local ring with maximal ideal $\langle \bar{p} \rangle$.*

Remark 6.16. *Let (R, m, K) be a local ring. $x \in R - m \Leftrightarrow x$ is a unit in R.*

Definition 6.17. *A ring is said to be semi local if it has finite number of maximal ideals.*

6.1. **Characteristic of a Ring.** Let R be a commutative ring with identity. We consider the ring homomorphism

$$\begin{aligned} \theta : \mathbb{Z} &\to R \\ n &\mapsto \underbrace{1_R + \cdots + 1_R}_{\text{n times}} \\ -n &\mapsto \underbrace{(-1_R) + \cdots + (-1_R)}_{\text{n times}} \\ 0 &\mapsto 0 \end{aligned}$$

Check that θ is a ring homomorphism. Then $\operatorname{Ker}\theta = 0$ or $m\mathbb{Z}$ for some $m \in \mathbb{Z}, m > 0$. If $\operatorname{Ker}\theta = 0$ we call $\operatorname{Char} R = 0$, if $\operatorname{Ker}\theta = m\mathbb{Z}$ we call $\operatorname{Char} R = m$.

Remark 6.18. *If $\operatorname{Ker}\theta = 0$ then $\mathbb{Z} \hookrightarrow R$ i.e., $\mathbb{Z}$ is a subring of R, if $\operatorname{Ker}\theta = m\mathbb{Z}$ then $\mathbb{Z}/m\mathbb{Z} \hookrightarrow R$.*

Remark 6.19. *If R is an integral domain then $\operatorname{Ker}\theta = 0$ or $\operatorname{Ker}\theta = p\mathbb{Z}$ for some prime p since $\mathbb{Z}/m\mathbb{Z}$ is an integral domain iff m is prime. In this case $\mathbb{Z}/p\mathbb{Z} \hookrightarrow R$ [Note that $\mathbb{Z}/p\mathbb{Z}$ is a field].*

Remark 6.20. *If R is a field then $\operatorname{Ker}\theta = 0$ or $p\mathbb{Z}$. If $\operatorname{Char} R = 0$ we say that $\mathbb{Q} \hookrightarrow R$. Let $p/q \in \mathbb{Q}, q \in \mathbb{Z} \hookrightarrow R \Rightarrow q^{-1}$ exists in R (since R is a field) therefore, $p, q^{-1} \in R \Rightarrow p/r \in R \Rightarrow \mathbb{Q} \hookrightarrow R$. If $\operatorname{Char} R = p$ then $\mathbb{Z}/p\mathbb{Z} \hookrightarrow R$ these type of field is called prime sub field.*

Problem 6.21. *Find all dense subfield of $\mathbb{C}$.*

Ans. We know that $\mathbb{C}$ is a vector space over $\mathbb{R}$ with $\dim_{\mathbb{R}} \mathbb{C} = 2$. If $\alpha = a + ib, b \neq 0$ then $\{1, \alpha\}$ is a basis of $\mathbb{C}$ over $\mathbb{R}$. Let F be a dense subfield of $\mathbb{C}$ then $\operatorname{Char}\mathbb{C} = 0 \Rightarrow \operatorname{Char} R = 0 \Rightarrow \mathbb{Q} \hookrightarrow F$. If $F \subseteq \mathbb{R} \Rightarrow \overline{F} \subseteq \overline{\mathbb{R}}$ [Closure of $\mathbb{R}$ in $\mathbb{C}$ is $\mathbb{R}$]. Then we have a contradiction hence $F \nsubseteq \mathbb{R}$ then there exists $\alpha \in F$ such that $\alpha \notin \mathbb{R}$. If $\alpha = a + ib$ then $b \neq 0$ therefore, $\mathbb{Q}(\alpha) \hookrightarrow F$ [as $\alpha \in F$].
Claim: $\mathbb{Q}(\alpha)$ is dense in $\mathbb{C}$. Let $z \in \mathbb{C}$ since $\{1, \alpha\}$ is a basis of $\mathbb{C}$ over $\mathbb{R}$ then $z = x + y\alpha$. Now, $\mathbb{Q}$ is dense in $\mathbb{R}$ implies there exists $\{x_n\}, \{y_n\} \subseteq \mathbb{Q}$ such that $\lim x_n = x, \lim y_n = y$ therefore, $x_n + y_n\alpha \in \mathbb{Q}(\alpha)$ and $\lim(x_n + y_n\alpha) = x + y\alpha$ hence, $\mathbb{Q}(\alpha)$ is dense in $\mathbb{C}$.

7. Product ring

Let $\{R_i\}_{i\in\Lambda}$ be a collection of rings then the cartesian product ring is defined on base set $\prod_{i\in\Lambda} R_i$ (cartesian product). We define,

$$+ : \left(\prod_{i\in\Lambda} R_i \times \prod_{i\in\Lambda} R_i\right) \to \prod_{i\in\Lambda} R_i$$

by $(a_i, b_i) \mapsto a_i + b_i$ and,

$$\cdot : \left(\prod_{i\in\Lambda} R_i \times \prod_{i\in\Lambda} R_i\right) \to \prod_{i\in\Lambda} R_i$$

by $(a_i, b_i) \mapsto (a_i)(b_i)$. Check that $\left(\prod_{i\in\Lambda} R_i, +, \cdot\right)$ is a ring. Let $R_1, \cdots, R_n$ be rings and $I_i \subseteq R_i$ be ideals of R_i. We consider the ring homomorphism,

$$\begin{aligned} R_1 \times \cdots \times R_n &\xrightarrow{\theta} R_1/I_1 \times \cdots \times R_n/I_n \\ (x_1, \cdots, x_n) &\mapsto (x_1 + I, \cdots, x_n + I) \end{aligned}$$

Clearly θ is a surjective ring homomorphism and kernel of this map is

$$\begin{aligned} \operatorname{Ker}\theta &= \{(x_1, \cdots, x_n) \in R_1 \times \cdots \times R_n : x_i \in I_i, 1 \le i \le n\} \\ &= I_1 \times \cdots \times I_n \end{aligned}$$

By first isomorphism theorem

$$\frac{R_1 \times \cdots \times R_n}{I_1 \times \cdots \times I_n} \cong R_1/I_1 \times \cdots \times R_n/I_n.$$

Question 7.1. *Let $R = R_1 \times \cdots \times R_n$ where $R_i's$ are rings. What are the ideals of R?*

Ans. Ideals of R is of the form $I_1 \times \cdots \times I_n$ where $I_i \subseteq R_i$ are ideals. Let $J \subseteq R$ be an ideals. Consider the map

$$\begin{aligned} R_1 \times \cdots \times R_n &\xrightarrow{\pi_i} R_i \\ (x_1, \cdots, x_n) &\mapsto x_i \end{aligned}$$

π_i is a surjective ring homomorphism. Let $I_i = \pi_i(J) \subseteq R_i$ is an ideal [since π_i is surjective].
Claim: $I_1 \times \cdots \times I_n = J$. Let $(x_1, \cdots, x_n) \in I_1 \times \cdots \times I_n \Rightarrow \pi_i((x_1, \cdots, x_n) = x_i \in \pi_i(J) = I_i$ therefore, $x_i \in \pi_i(J)$ then there exists $a_i \in J$ such that $\pi_i(a_i) = x_i$. Now, $a_i \in J \Rightarrow (0, \cdots, 1_{R_i}, \cdots, 0)a_i \in J \Rightarrow (0, \cdots, a_i, \cdots, 0)$ [as $\pi_i(a_i) = x_i$] then $\sum_{i=1}^{n}(0, \cdots, x_i, \cdots, 0) \in J \Rightarrow (x_1, \cdots, x_n) \in J \Rightarrow I_1 \times \cdots \times I_n \subseteq J$. Let $(x_1, \cdots, x_n) \in J \Rightarrow \pi_i((x_1, \cdots, x_n)) \in \pi_i(J) = I_i \Rightarrow (x_1, \cdots, x_n) \in I_1 \times \cdots \times I_n \Rightarrow J \subseteq I_1 \times \cdots \times I_n$. Hence, $J = I_1 \times \cdots \times I_n$.
Conversely, if we take $I_1 \subseteq R_i$ then $I_1 \times \cdots \times I_n$ is an ideal of $R_1 \times \cdots \times R_n$.

Observation 7.2. *Product ring is never an integral domain.*

Question 7.3. *What is the* $\operatorname{spec}(R_1 \times \cdots \times R_n)$?

Ans.

$$\begin{aligned}\operatorname{spec}(R_1 \times \cdots \times R_n) &= \{P_1 \times \cdots \times R_n : P_1 \in \operatorname{spec} R_1\} \\ &\quad \cup \{R_1 \times P_2 \times \cdots \times R_n : P_2 \in \operatorname{spec} R_2\} \\ &\quad \cup \cdots \cup \{R_1 \times \cdots \times P_n : P_n \in \operatorname{spec} R_n\} \\ &= \bigcup_{i=n}^{n} \operatorname{spec} R_i\end{aligned}$$

Let $Q \subseteq R = R_1 \times \cdots \times R_n$ be a prime ideal then $Q = I_1 \times \cdots \times I_n$ where I_i is an ideal of R_i then

$$R/Q = \frac{R_1 \times \cdots \times R_n}{I_1 \times \cdots \times I_n} \cong R_1/I_1 \times \cdots \times R_n/I_n$$

As R/Q is an integral domain $\exists\ i$ such that $R_j/I_j = 0,\ \forall j \neq i, 1 \leq i \leq n$ this gives $I_j = R_j,\ \forall j \neq i, 1 \leq i \leq n$ and $R/Q = R_i/I_i$ (integral domain) then $I_i \in \operatorname{spec} R_i$. Let $I_i = P_i \in \operatorname{spec} R_i$ so that

$$\begin{gathered}Q = R_1 \times \cdots \times R_{i-1} \times I_i \times R_{i+1} \times \cdots \times R_n \\ R_1 \times \cdots \times R_{i-1} \times P_i \times R_{i+1} \times \cdots \times R_n\end{gathered}$$

Conversely, if we take $Q = R_1 \times \cdots \times R_{j-1} \times P_j \times R_{j+1} \times \cdots \times R_n$ where $P_j \in \operatorname{spec} R_j$ then

$$\frac{R_1 \times \cdots \times R_n}{R_1 \times \cdots \times P_j \times \cdots \times R_n} \cong R_j/P_j \quad \text{(integral domain)}$$

Hence we get

$$R_1 \times \cdots \times P_j \times \cdots \times R_n \in \operatorname{spec}(R_1 \times \cdots \times R_n)$$

we identify $R_1 \times \cdots \times P_j \times \cdots \times R_n$ to P_j then $\operatorname{spec}(R_1 \times \cdots \times R_n) = \bigcup_{i=n}^{n} \operatorname{spec} R_i$.

Question 7.4. *What is the* $\operatorname{maxspec}(R_1 \times \cdots \times R_n)$?

Ans.

$$\begin{aligned}\operatorname{maxspec}(R_1 \times \cdots \times R_n) &= \{m_1 \times \cdots \times R_n : m_1 \in \operatorname{maxspec} R_1\} \\ &\quad \cup \{R_1 \times m_2 \times \cdots \times R_n : m_2 \in \operatorname{maxspec} R_2\} \\ &\quad \cup \cdots \cup \{R_1 \times \cdots \times m_n : m_n \in \operatorname{maxspec} R_n\} \\ &= \bigcup_{i=n}^{n} \operatorname{maxspec} R_i\end{aligned}$$

Let $Q \subseteq R = R_1 \times \cdots \times R_n$ be a maximal ideal then $Q = I_1 \times \cdots \times I_n$ where I_i is an ideal of R_i then

$$R/Q = \frac{R_1 \times \cdots \times R_n}{I_1 \times \cdots \times I_n} \cong R_1/I_1 \times \cdots \times R_n/I_n$$

As R/Q is an field $\exists\ i$ such that $R_j/I_j = 0,\ \forall j \neq i, 1 \leq i \leq n$ this gives $I_j = R_j,\ \forall j \neq i, 1 \leq i \leq n$ and $R/Q = R_i/I_i$ (field) then $I_i \in \operatorname{maxspec} R_i$. Let $I_i = m_i \in \operatorname{maxspec} R_i$ so that

$$\begin{gathered}Q = R_1 \times \cdots \times R_{i-1} \times I_i \times R_{i+1} \times \cdots \times R_n \\ R_1 \times \cdots \times R_{i-1} \times m_i \times R_{i+1} \times \cdots \times R_n\end{gathered}$$

Conversely, if we take $Q = R_1 \times \cdots \times R_{j-1} \times m_j \times R_{j+1} \times \cdots \times R_n$ where $m_j \in \operatorname{maxspec} R_j$ then

$$\frac{R_1 \times \cdots \times R_n}{R_1 \times \cdots \times m_j \times \cdots \times R_n} \cong R_j/m_j \quad \text{(field)}$$

Hence we get

$$R_1 \times \cdots \times m_j \times \cdots \times R_n \in \operatorname{maxspec}(R_1 \times \cdots \times R_n)$$

we identify $R_1 \times \cdots \times m_j \times \cdots \times R_n$ to m_j then $\operatorname{maxspec}(R_1 \times \cdots \times R_n) = \bigcup_{i=n}^{n} \operatorname{maxspec} R_i$.

Question 7.5. *What will happen in case of arbitrary product* $\prod_{i \in I} R_i$?

Ans.

Observation 7.6. *Product ring is never a local ring.*

Question 7.7. *Give an example of a ring which has five maximal ideals.*

Ans. Take direct product of five local ring.

7.1. **Chinese Remainder Theorem.** Let I, J be two ideals of R and we consider the map

$$\theta : R \to R/I \times R/J$$
$$x \mapsto (x + I, x + J)$$

then $\operatorname{Ker} \theta = I \cap J$. Let $x \in \operatorname{Ker} \theta \Leftrightarrow x + I = 0 + I$ and $x + J = 0 + J \Leftrightarrow x \in I, J \Leftrightarrow x \in I \cap J$. By first isomorphism theorem

$$\frac{R}{I \cap J} \overset{\tilde{\theta}}{\hookrightarrow} R/I \times R/J$$

If we consider the comaxilaity condition on I and J i.e., $1 \in I + J$ then
(i) $IJ = I \cap J$
(ii) θ is surjective hence,
(iii) $\dfrac{R}{I \cap J} \cong R/I \times R/J$ (Chinese Remainder theorem)

Proof. (i) Let $a \in I \cap J$ and $1 \in I \cap J \Rightarrow 1 = s + t$ for some $s \in I$ and $t \in J$. Then $a = a \cdot 1 = a(s+t) = as + at \quad [a \in J, s \in I \text{ and } a \in I, t \in J] \Rightarrow a \in IJ$ then $I \cap J \subseteq IJ$. Therefore, $IJ = I \cap J$.
(ii) Let $(x + I, y + J) \in R/I \times R/J$ and we consider $t = sx + ry$ $[1 = r + s, r \in I, s \in J]$ then $t - x = x(s-1) + ry = -rx + ry \in I$ so that $t + I = x + I$ again $t - y = sx + (r-1)y = sx - sy \in J$ then $t + J = y + J$. This gives $\theta(t) = (t + I, t + J) = (x + I, y + J)$ hence θ is surjective therefore, $\dfrac{R}{I \cap J} \cong R/I \times R/J$.
Let $I_1, \cdots, In$ be ideals of R such that $1 \in I_i + I_j, i \neq j, 1 \leq i, j \leq n$ then

$$\frac{R}{I_1 \cdots I_n} \cong R/I_1 \times \cdots \times R/I_n$$

Proof. $n = 2$ we are done. Let $I = I_n$ and $J = I_1 \cdots I_{n-1}$ by Chinese remainder theorem $\dfrac{R}{I_1 \cdots I_n} \cong R/I_n \times R/I_1 \cdots I_{n-1}$ by induction $R/I_1 \cdots I_{n-1} \cong R/I_1 \times \cdots \times R/I_{n-1}$, hence

$$\frac{R}{I_1 \cdots I_n} \cong R/I_1 \times \cdots \times R/I_n.$$

□

Definition 7.8. *Let R be any ring and $e \in R$ is said to be idempotent element if $e^2 = e$.*

Definition 7.9. *A ring is said to be Boolean ring if every non-identity element is idempotent element.*

Observation 7.10. *R is direct product of two rings iff exists a non trivial idempotent $e \in R$.*

Proof. Suppose, $e \in R$ and $e \neq 0, 1$ be a non trivial idempotent such that $e^2 = e \Rightarrow e(1-e) = 0$. $R \cong R/(0) = R/\langle e(1-e)\rangle$ as $1 \in \langle e\rangle + \langle 1-e\rangle$. By Chinese remainder theorem

$$R \cong R/eR \oplus R/(1-e)R$$

Now $R \xrightarrow{\theta} R(1-e)$ by $x \mapsto x(1-e)$ since θ is surjective homomorphism $\operatorname{Ker}\theta = \{x(1-e) : x(1-e) = 0\}$. Now, $x = x \cdot 1 = x(e + (1-e)) = xe$ $[x(1-e) = 0]$ and $x \in eR$ and $eR \subseteq \operatorname{Ker}\theta$ then $\operatorname{Ker}\theta = eR$

$$R/eR \cong R(1-e)$$

Similarly, $R/(1-e)R \cong Re$ therefore, $R \cong Re \oplus R(1-e)$.
Conversely, if $R \cong R_1 \oplus R_2$ take $e = (1, 0)$ and $e \neq (0, 0), (1, 1)$ then $e^2 = e$, e is non trivial idempotent. □

8. Field of fraction and Localization

8.1. **Field of fraction.**

Definition 8.1. *Let R be a ring and $S \subseteq R$ is said to be multiplicatively closed set if*

(i) $1 \in S$

(ii) $a, b \in S \Rightarrow ab \in S$.

Example 8.2. (1) *Let $a \in R$ then the set $\{1, a, a^2, \cdots\}$ is a multiplicatively closed set.*

(2) *If $P \in spec\ R$ then $R - P$ is a multiplicatively closed set.*

Construction of fraction ring.

Let S be a multiplicatively closed set of R. We define a relation $\sim$ on $\Sigma = \{a/b|\ a \in R, b \in S\}$ in the following way.

$$\frac{a}{b} \sim \frac{c}{d} \text{ if and only if } \exists\ s \in S \text{ such that } s(ad - bc) = 0$$

Check that '$\sim$' is an equivalence relation.

$$\frac{a}{b} \sim \frac{a}{b} \text{ as } s(ab - ab) = 0,\ \forall a \in R, b \in S$$

Therefore $\sim$ is reflexive. Now suppose,

$$\frac{a}{b} \sim \frac{c}{d} \text{ then } \exists s \in S \text{ such that } s(ad - bc) = 0 \Rightarrow (-s)(bc - da) = 0 \Rightarrow \frac{c}{d} \sim \frac{a}{b}$$

Hence $\sim$ is symmetric. Let $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \Sigma$ where $a, c, e \in R$ and $b, d, f \in S$ then there exists $s_1, s_2 \in S$ such that

$$s_1(ad - bc) = 0 \text{ and } s_2(cf - ed) = 0$$

but this gives

$$\begin{aligned} 0 &= s_2 s_1(adf - bcf) + s_1 s_2(bcf - bed) \\ &= s_1 s_2(adf - bed) \\ &= s'(af - be) \quad \text{as } s_1, s_2, d \in S \Rightarrow s' = s_1 s_2 d \in S \text{ (say)} \end{aligned}$$

then we have

$$\frac{a}{b} \sim \frac{c}{d}, \frac{c}{d} \sim \frac{e}{f} \Rightarrow \frac{a}{b} \sim \frac{e}{f}$$

therefore, $\sim$ is symmetric also. Hence $\sim$ is an equivalence relation. We define,

$$S^{-1}R := \{cl(a/b) : a/b \in \Sigma\}$$

By abuse of notation we only write $\frac{a}{b}$ instead of $cl(a/b)$. Now,

$$\begin{aligned} + : S^{-1}R \times S^{-1}R &\to S^{-1}R \\ \left(\frac{a}{b}, \frac{c}{d}\right) &\mapsto \frac{ad + bc}{bd} \\ \cdot : S^{-1}R \times S^{-1}R &\to S^{-1}R \\ \left(\frac{a}{b}, \frac{c}{d}\right) &\mapsto \frac{ad}{bc} \end{aligned}$$

Show that '+' and '$\cdot$' is well defined. Let $\frac{a}{b} = \frac{a_1}{b_1}$ and $\frac{c}{d} = \frac{c_1}{d_1}$ then $\exists s_1, s_2 \in S$ such that

$$s_1(ab_1 - a_1b) = 0 \text{ and } s_2(cd_1 - c_1d) = 0$$

Now,

$$s_1s_2dd_1(b_1a - ba_1) + s_1s_2bb_1(cd_1 - c_1d) = 0$$
$$\frac{ad + bc}{bd} = \frac{a_1d_1 + b_1c_1}{b_1d_1}$$

Therefore, '+' is well defined. Similarly,

$$s_1s_2cd_1(ab_1 - a_1b) + s_1s_2a_1b(cd_1 - c_d) = 0$$
$$\frac{ac}{bd} = \frac{a_1c_1}{b_1d_1}$$

Hence '$\cdot$' is well defined also. Therefore, $\left(S^{-1}R, +, \cdot\right)$ is a ring with identity where $0/1$ is additive identity and $1/1$ is multiplicative identity. Net we consider the ring homomorphism

$$\theta : R \to S^{-1}R \tag{4}$$
$$a \mapsto a/1$$

It is called canonical ring homomorphism.

Remark 8.3. *If $0 \in S$ then for each element a/b of $S^{-1}R$ have $0(a \cdot 1 - b \cdot 0) = 0 \Rightarrow a/b = 0/1$ therefore, $S^{-1}R$ is a trivial ring.*

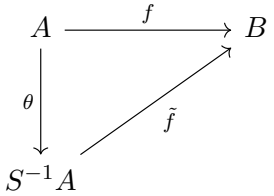
Remark 8.4. *$\theta(S) \subseteq S^{-1}R$ is a set of units. Let $s/1 \in \theta(S) \Rightarrow s/1 \cdot 1/s = 1/s \cdot s/1 = 1/1$ [as $s \in S \Rightarrow 1/s \in S^{-1}R$]. Therefore, $\theta(S) \subseteq$ units of $S^{-1}R$.*

Remark 8.5. *If S contain no zero divisor then θ is injective. As $\operatorname{Ker}\theta = \{r \in R : r/1 = 0/1\}$. Let $r \in \operatorname{Ker}\theta \Leftrightarrow \exists s \in S$ such that $s(r \cdot 1 - 1 \cdot 0) = 0 \Leftrightarrow rs = 0 \Leftrightarrow r = 0$.*

Corollary 8.6. *If R is integral domain then θ is injective.*

Universal property of localised ring.

Theorem 8.7. *Let $f : A \to B$ be a ring homomorphism and $S \subseteq A$ be a multiplicatively closed set such that $f(S) \subseteq$ units in B then there is a unique ring homomorphism $\tilde{f} : S^{-1}A \to B$ such that the diagram is commutative.*



Proof. Define $\tilde{f} : S^{-1}A \to B$ by $\tilde{f}(a/b) = \frac{f(a)}{f(b)}$. We claim that $\tilde{f}$ is well defined. Let $a/b \sim c/d$ then there exists $s \in S$ such that $s(ad - bc) = 0 \Rightarrow f(s)(f(a)f(d) - f(b)f(c)) = 0$. Since $f(s)$ is

unit in S, $f(a)f(d) = f(b)f(c)$ therefore we have $f(a)/f(b) = f(c)/f(d)$ [since $f(b), f(d)$ is units in B].

$$\begin{aligned}\tilde{f}(a_1/b_1 + a_2/b_2) &= \tilde{f}\left(\frac{a_1b_2 + b_2a_1}{b_1b_2}\right) = \frac{f(a_1b_2 + b_1a_2)}{f(b_1b_2)} \\ &= \frac{f(a_1)f(b_2) + f(a_2)f(b_1)}{f(b_1)f(b_2)} \\ &= \frac{f(a_1)}{f(b_2)} + \frac{f(a_2)}{f(b_2)} \\ &= \tilde{f}(a_1/b_1) + \tilde{f}(a_2/b_2)\end{aligned}$$

Similarly,

$$\tilde{f}\left(\frac{a_1}{b_1} \cdot \frac{a_2}{b_2}\right) = \tilde{f}\left(\frac{a_1a_2}{b_1b_2}\right) = \frac{f(a_1)f(a_2)}{f(b_1)f(b_2)} = \tilde{f}(a_1/b_1)\tilde{f}(a_2/b_2)$$

and $\tilde{f}(1/1) = 1_B$. Therefore, $\tilde{f} \circ \theta(a) = \tilde{f}(a/1) = f(a)/f(1) = f(a)$ for all $a \in A \Rightarrow \tilde{f} \circ \theta = f$ (i.e., the diagram is commutative).

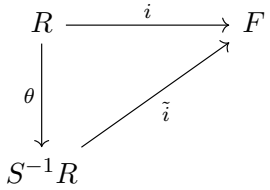
Uniqueness. Suppose, there is another ring homomorphism $g : S^{-1}A \to B$ such that $g \circ \theta = f$. Let $a/b \in S^{-1}A, a \in A, b \in S \Rightarrow g \circ \theta(b) = f(b) \Rightarrow g(b/1) = f(b)$. Now,

$$g(1/s) = g((\theta(s))^{-1}) = (g(\theta(s)))^{-1} = 1/f(s).$$

Therefore, $g(a/b) = g(a/1 \cdot 1/b) = g(a/1)g(1/b) = f(a)/f(b) = \tilde{f}(a/b)\ \forall a/b \in S^{-1}B \Rightarrow g = \tilde{f}$. □

Observation 8.8. *Let R be an integral domain then there is a smallest field $Q(R)$ containing R.*

Proof. Let $S = R \setminus \{0\}$ then S is a multiplicatively closed set in R. Now, R is an integral domain implies $\theta : R \to S^{-1}R$ is injective hence R is a subring of $S^{-1}R$. We note that $S^{-1}R$ is a field. If $a/b \in S^{-1}R$ with $a/b \neq 0/1$ i.e., $sa \neq 0$ for all $s \in R \setminus \{0\} \Rightarrow a \neq 0$ then $b/a \in S^{-1}R$ therefore, $a/b \cdot b/a = 1/1 \Rightarrow b/a$ is a inverse of a/b is $S^{-1}R$.
Let $R \subseteq F$ and F is a field then $S = R \setminus \{0\} \subseteq F$ is units in F. By Universal property there exists a ring homomorphism $\tilde{i} : S^{-1}R \to F$ such that the diagram is commutative.



But,

$$\tilde{i}(a/b) = \frac{i(a)}{i(b)} = \frac{a}{b}$$

is not a zero map $\Rightarrow \tilde{i}$ is injective hence $S^{-1}R \subseteq F$. Therefore, $S^{-1}R$ is the smallest field containing R. □

Notation. $S^{-1}R := Q(R)$ is the field of fraction of R (where R is an integral domain).

Observation 8.9. *If R is an integral domain, then $S^{-1}R$ is also an integral domain where S is a multiplicatively closed set of R and $0 \notin S$.*

Proof. Let $a/b, a'/b' \in S^{-1}R$. If $\dfrac{aa'}{bb'} = \dfrac{0}{1} \Rightarrow \exists t \in S$ such that

$$\begin{aligned} 0 &= t(aa' \cdot 1 - bb' \cdot 0) \\ &= t(ab) \\ &= ab \quad \text{as } t \in S \end{aligned}$$

Therefore, $a = 0$ or $b = 0$ this implies $a/b = 0/1$ or $a'/b' = 0/1$. □

Problem 8.10. *Ideals of $S^{-1}R$ is of the form $S^{-1}I$ where $I \subseteq R$ is an ideals of R and $S \cap I = \emptyset$.*

Proof. Let $a/b, c/d \in S^{-1}I$ where $a, c \in I$ and $b, d \in S$ then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \in S^{-1}I \text{ as } a \in I, b \in S \Rightarrow ad \in I, \text{ and } b, d \in S \Rightarrow bd \in S$$

Let $s/t \in S^{-1}R$ and $a/b \in S^{-1}I \Rightarrow \dfrac{s}{t} \cdot \dfrac{a}{b} = \dfrac{sa}{tb} \in S^{-1}I$. Therefore, $S^{-1}I$ is an ideal of $S^{-1}R$. Now, if $S \cap I \neq \emptyset$ then $x \in S$ and under canonical map $\theta(x)$ is an unit of $S^{-1}R$ similarly $x \in I$ is a unit in R hence $I = R$. Therefore, $S \cap I = \emptyset$.
Conversely, let $Q \subseteq S^{-1}R$ is an ideal let $J = \theta^{-1}(Q)$. Show that $S^{-1}J = Q, S \cap J = \emptyset$. So every ideal of $S^{-1}R$ is of the form $S^{-1}J$ where $S \cap J = \emptyset$. □

Problem 8.11. *Let $P \in \operatorname{spec} R$ and $S = R - P$ we define $R_P := S^{-1}R$. Show that R_P is a local ring with maximal ideal $S^{-1}P$.*

Proof. Let $S = R - P$ and $m = S^{-1}P$. Let $a/s, a'/s \in S^{-1}P \Rightarrow \dfrac{a's + as'}{ss'} \in S^{-1}P, ss' \in S$ ($a's, s'a \in P$ as $a, a' \in P$). Now if $b/r \in S^{-1}R$ and $a/s \in S^{-1}P$ then $\dfrac{b}{r} \cdot \dfrac{a}{s} = \dfrac{ab}{rs} \in S^{-1}P$ (as $rs \in S$ and $ab \in P$) so $S^{-1}P$ is an ideal. We need to show that $S^{-1}R \setminus S^{-1}P$ has only units. Let $a/s \in S^{-1}R \setminus S^{-1}P$ then $a \in S, s \in S \Rightarrow \dfrac{s}{a} \in S^{-1}R \setminus S^{-1}P$.

Problem 8.12. *$\mathbb{Z}$ is an integral domain. Consider $S = \mathbb{Z} \setminus p\mathbb{Z}$, p prime. Let $\mathbb{Z}_p = S^{-1}\mathbb{Z}$ is an integral domain. What is the field of fraction of $\mathbb{Z}_p$?*

Ans.

9. Polynomial ring

Let R be a ring and $R[X]$ is the set of all sequences of elements of R $(a_0, a_1, a_2, \cdots)$ such that $a_i = 0$ for all but finitely many indices i.

(1) $R[X]$ is a ring with addition and multiplication defined as

$$(a_0, a_1, a_2, \cdots) + (b_0, b_1, b_2, \cdots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \cdots)$$

and

$$(a_0, a_1, a_2, \cdots)(b_0, b_1, b_2, \cdots) = (c_0, c_1, c_2, \cdots)$$

where $c_i = \sum_{k=0}^{i} a_k b_{i-k}$

(2) If R is a integral domain then $R[X]$ is integral domain.

(3) The map

$$R \xrightarrow{\phi} R[X]$$
$$r \mapsto (r, 0, 0, \cdots)$$

is an injective ring homomorphism.

Theorem 9.1. *Let R be a commutative ring with 1_R, denote $X = (0, 1_R, 0\cdots)$ in $R[X]$. Then show that*

(1) $X^n = (0, 0, \cdots, 1_R, 0, \cdots)$ *(n+1 position)*

(2) $r \in R, rX^n = (0, 0, \cdots, r, 0, \cdots)$ *(n+1 position)*

(3) *For each $f \in R[X]$ there is a $n \in \mathbb{N}$ such that $f = a_0 + a_1X + \cdots + a_nX^n$. The integer n and the elements $a_i, 0 \leq i \leq n$ are unique in the sense that $f = b_0 + b_1X + \cdots b_mX^m$ then $m \geq n$ and $a_i = b_i$, $i = 0, \cdots, n$ and $b_k = 0, n < k \leq m$.*

a_0 is constant of f and n is called degree of f.

Proof. (1) True for $n = 1$ as $X^1 = (0, 1_R, \cdots)$ by definition. Let $X^{n-1} = (0, \cdots, 1_R, \cdots)$ (n^{th} position) then $X^n = X^{n-1}X = (0, \cdots, 1_R, \cdots)(0, 1_R, \cdots) = (c_0, c_1, \cdots)$. If $0 \leq s \leq n$ then $c_s = \sum_{i=0}^{s} a_i b_{s-i}$ where $(a_0, a_1, \cdots) = (0, \cdots, 1_R, \cdots)$ and $(b_0, b_1, \cdots) = (0, 1_R, \cdots)$. If $i \leq s < n$ then $a_i = o \Rightarrow c_s = 0$ for $s < n$ and $c_n = a_n b_{n-n} = a_n b_0 = 0$ and $c_{n+1} = a_n b_{(n+1)-n)} = a_n b_1 = 1_R$. If $s > n + 1, c_s = a_n b_{s-n}$. Now, $s > n + 1 \Rightarrow s - n > 1 \Rightarrow b_{s-n} = 0 \Rightarrow c_s = 0$. Therefore, $X^n = (0, \cdots, 1_R, 0\cdots)$ $(n + 1^{th}$ position).

(2) $rX^n = (r, 0, \cdots)(0, \cdots, 1_R, \cdots) = (0, \cdots, r, \cdots)$.

(3) Let $f = (a_0, a_1, \cdots) \in R[X]$ where a_i's all but finitely many are non zeroes. Then $f = (a_0, \cdots, 0) + (0, a_1, \cdots, 0) + \cdots + (0, \cdots, a_n, 0, \cdots) = \sum_{i=1}^{n} a_i X^i$.

Uniqueness: Let $f = b_0 + b_1X + \cdots + b_mX^m = (b_0, b_1, \cdots, b_m, 0, \cdots)) = (a_0, a_1, \cdots a_n, \cdots)$ which imply $b_0 = a_0, b_1 = a_1, \cdots$. Now, n is the largest integer such that $a_n \neq 0$ if $m < n$ then $b_n = 0$ and $a_n = b_n \Rightarrow a_0 = 0$ which is a contradiction. Therefore, $m \geq n$ and $b_i = 0$ for all $n < i \leq m$. $\square$

9.1. **Substitution or Evaluation.** Let R be a subring of S and U be a subset of S then $R[U]$ is the usbring of S generated by R and U or the smallest subring of S containing both R and U.

Question 9.2. *Ler R be a subring of S and U, V be subset of S then show that $R[U][V] = R[U \cup V] = R[V][U]$.*

If U is finite i.e., $U = \{u_1, \cdots, u_n\}$ then $R[U] = R[u_1][u_1, \cdots, u_n]$. So it suffices to study $R[u]$ i.e., R is a subring of S and $u \in S$ then by definition we know that $R[u]$ is a subring of S. As $u \in R[u], u, u^2, \cdots, u^n \in R[u]$ for some $n \in \mathbb{N}$ and $R \in R[u]$ as well so $a_0 + a_1u + \cdots + a_nu^n \in R[u], a_i \in R; 1 \leq i \leq n$. Let

$$R' = \{a_0 + a_1u + \cdots + a_nu^n : a_i \in R; 0 \leq i \leq n, n \in \mathbb{N}\}$$

i.e., R' is the collection of all polynomial "expression" in u with coefficient from R. Then it is easy to see that R' is closed under addition. Let $a_0 + \cdots + a_nu^n, b_0 + \cdots + b_mu^m \in R[u]$ then $(a_0 + \cdots + a_nu^n)(b_0 + \cdots + b_mu^m) = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_ib_{k-i} \right) u^k \in S$ but $u^k \in R'$ and $\sum_{i=0}^{k} a_ib_{k-i} \in R'$ hence the product is also in R' therefore, R' is a subring of S. Also R is a subring of R' and $u \in R'$ so $R[u] \subseteq R' \subseteq R[u]$ hence $R' = R[u]$.

Remark 9.3. *Representation of an element of $R[u]$ as polynomial expression may not be unique as in $\mathbb{Z}[i]$ we write $i^2 = -1$ which is two different representation.*

Clearly we have a ring homomorphism

$$\phi : R[x] \to R[u]$$
$$a_0 + \cdots + a_nx^n \mapsto a_0 + \cdots + a_nu^n$$

then it is easy to see that ϕ is onto and $R[x]/\ker\phi \cong R[u]$.

Theorem 9.4 (Fundamental morphism property of polynomials)**.** *Let R_1, R_2 be two rings and $u \in R_2$. Let $\phi : R_1 \to R_2$ be a ring homomorphism then ϕ has a unique extension to a ring homomorphism*

$$\phi_u : R_1[x] \to R_2$$

such that $\phi_u(x) = u$.

Proof. We define the map as follows

$$\phi_u : R_1[x] \to R_2$$
$$a_0 + \cdots + a_nx^n \mapsto \phi(a_0) + \phi(a_1)u + \cdots + \phi(a_n)u^n$$

Then its is easy to see that ϕ_u is an ring homomorphism and $\phi_u(x) = \phi(1)u = u$. Let $a \in R_1, \phi_u(a) = a = \phi(a)$ therefore, $\phi_u\big|_{R_1} = \phi$. If $\psi : R_1[x] \to R_2$ is another ring homomorphism such that $\psi_u\big|_{R_1} = \phi$ and $\phi(x) = u$ then $\psi = \phi_u$(check).

Now let R be a subring of S and $u \in S$. Take $\phi : R \to S$ be the inclusion map. Then by previous theorem there exists am unique extension $\psi : R[x] \to S$ such that $\psi\big|_R = id$ and $\psi(x) = u$. This is commonly called "substitution" or "evaluation". Let $I = \ker\psi$ then $R[x]/I \cong R[u]$. Let

$a \in I \cap R$ then $\psi(a) = 0$ but $a \in R$ then $a = 0 \Rightarrow I \cap R = \{0\}$. Therefore, we got $R[u] \cong R[x]/I$ and $I \cap R = \{0\}$. Conversely, let I be an ideal of $R[x]$ such that $I \cap R = \{0\}$ then consider the natural projection map $\pi : R[x] \to R[x]/I$ then $\pi\big|_R$ is injective. Let $\pi\big|_R(a) = 0 \Rightarrow a + I = 0 + I \Rightarrow a \in I$ and $a \in R \Rightarrow a \in I \cap R = \{0\} \Rightarrow a = 0$. So we may think $R \hookrightarrow R[x]/I$ and R can be regarded as a subring of $R[x]/I$. As $R[x]$ is generated by R and x, $R[x]/I$ is generated by R and $x + I$ if we write $u = x + I$ then $R[x]/I \cong R[u]$. $\square$

10. Euclidean domain, Principal ideal domain, Unique factorization domain

Factorization in commutative ring.

Definition 10.1. *A non-zero element of a commutative ring R is said to be divide an element $b \in R$ (notation $a|b$) if $\exists\ x \in R$ such that $ax = b$. Elements a, b of R are said to be associates $(a \sim b)$ if $a|b$ and $b|a$.*

Theorem 10.2. *Let a, b & $u \in R$ be elements of a commutative ring R with identity.*
(1) *$a|b$ iff $(b) \subseteq (a)$*
(2) *a, b are associates iff $(a) = (b)$*
(3) *u is unit iff $u|r$ for all $r \in R$*
(4) *u is unit iff $(u) = R$*
(5) *The relation a is a associates of b is an equivalence relation on R*
(6) *If $a = br$ with $r \in R$, a unit, then a and b are associates. If R is integral domain, converse is also true.*

Proof. (1) Suppose, $a|b$ then $b = ac$ for some $r \in R$ this implies, $b \in (a) \Rightarrow (b) \subseteq (a)$. Conversely, Suppose, $(b) \subseteq (a)$. Now,$b \in (b) \subseteq (a) \Rightarrow b \in (a) \Rightarrow b = ac \Rightarrow a|b$.
(2) Let a, b are associates then $a|b$ and $b|a$. From previous one we have $(b) \subseteq (a)$ and from later part we have $(a) \subseteq (b)$, hence $(a) = (b)$. Conversely, if $(a) = (b)$ then we have $(b) \subseteq (a)$ and $(a) \subseteq (b)$. Therefore, we have a, b are associates.
(3) Suppose, u is unit in R then there exists $v \in R$ such that $uv = 1 \Rightarrow u(vr) = r \Rightarrow u|r\ \forall r \in R$. Conversely, if $u|r$, for all $r \in R$ then $u|1 \Rightarrow \exists v \in R$ such that $uv = 1$ hence u is a unit.
(4) If u is a unit then $uv = 1$ for some $v \in R$. Therefore, $1 \in (u) \Leftrightarrow (u) = R$.
(5) Left as exercise.
(6) Left as exercise.

Definition 10.3. *Let R be a commutative ring with id. An element $c \in R$ is irreducible provided that*
(i) c is non-zero, non-unit element
(ii) $c = ab$ implies a or b is unit.

Definition 10.4. *An element p of R is prime provided*
(i) p is non-zero, non-unit
(ii) $p|ab \Rightarrow p|a$ or $p|b$.

Definition 10.5. *An integral domain R is said to be PID or principal ideal domain if every ideal of R is principally generated.*

Theorem 10.6. *Let p and c be non-zero elements in an integral domain R.*
(i) p is prime iff (p) is a non-zero prime ideal.
(ii) c is irreducible iff (c) is maximal in set of all proper principal ideals of R.
(iii) Every prime element of R is irreducible.
(iv) If R is a PID, then p is prime iff p is irreducible.
(v) Every associates of an irreducible (prime) element of R is irreducible(prime).
(vi) The only divisor of an irreducible elements of R are its associates and units of R.

Proof. (i) Let p is prime. Now, if $ab \in (p) \Rightarrow ab = pk \Rightarrow p|ab$ then either $p|a$ or $p|b$ therefore, $(a) \subseteq (p)$ or $(b) \subseteq (p)$ hence (p) is an prime ideal. Conversely, Let (p) is a prime ideal and let $p|ab \Rightarrow ab \in (p) \Rightarrow a \in (p)$ or $b \in (p) \Rightarrow p|a$ or $p|b$. Therefore, p is a prime element.
(ii) Suppose, c is irreducible and Σ = set of all principal ideals in R. suppose, $(c) \subseteq (r) \Rightarrow c \in (r) \Rightarrow c = rs$ where s is unit in R therefore, $(c) = (r)$ hence (c) is maximal ideal in Σ. Conversely, Let (c) is maximal element in Σ. If $c = rs \Rightarrow c \in (r) \Rightarrow (c) \subseteq (r) \Rightarrow c = r \Rightarrow r|c$ then $r = ck$ for some $k \in R$ then we have

$$c = rs = cks \Rightarrow c(1 - ks) = 0$$

Since R is an integral domain $1 - ks = 0 \Rightarrow s$ is unit therefore, c is irreducible.
(iii) Let p be a prime element in R and $p = rs \Rightarrow rs \in (p) \Rightarrow r \in (p)$ or $s \in (p)$ then $r = pl_1$ or $s = pl_2$. If $r = pl_1$ then $p = pl_1 s \Rightarrow p(1 - l_1 s) = 0 \Rightarrow 1 - l_1 s = 0 \Rightarrow s$ is unit therefore, p is irreducible. If $s = pl_2$ by similar way we get p is irreducible.
(iv) If R is integral domain then prime element implies irreducible element. If R is PID we need to show that irreducible implies prime. Let c be an irreducible element then (c) is maximal in Σ then (c) is maximal ideal then (c) is prime ideal therefore, c is prime element.
(v) Suppose, a is irreducible and b is associates of a then $(b) = (a)$. but (a) is maximal in Σ therefore, (b) is also maximal hence b is irreducible.
(vi) Let a be an irreducible and $b|a$. Suppose, b is not an unit then $(b) \in \Sigma$. Now, $b|a$ implies $(a) \subseteq (b)$ since (a) is maximal, $(b) = (a)$. Therefore, b and a are associates. □

Exercise 10.7. *Show that $\mathbb{Z}$ is a PID.*

Proof. Let $I \subseteq R$ be an ideal. If $I = \langle 0 \rangle$ then we are done. Let say $I \neq \{0\}$ and n be the least positive integer in I. Clearly, $\langle n \rangle \subseteq I$. Suppose, $x \in I$ then by division algorithm $\exists\ q, r \in I$ such that $x = nq + r$ where $r = 0$ or $r < n$. As, $r = x - nr \in I$ then r must be zero otherwise it contradict the definition of n. Therefore, $x = nq$ and $I = \langle n \rangle = n\mathbb{Z}$. □

10.1. **Division in $\mathbb{Z}[i]$.** Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$ then there exists $\gamma, \delta \in \mathbb{Z}[i]$ such that $\alpha = \gamma \cdot \beta + \delta$ where $\delta = 0$ or $|\delta| < |\beta|$. We want to find $\gamma \in \mathbb{Z}[i]$ such that $\left|\frac{\alpha}{\beta} - \gamma\right| < 1$ i.e., $\left|\frac{\gamma}{\beta}\right| < 1$. Consider the complex number $\frac{\alpha}{\beta} \in \mathbb{C}$. Maximum distance of $\frac{\alpha}{\beta}$ from a point in $\mathbb{Z}[i]$ is $\leq \frac{1}{2}$(diagonal) $= 1/2 \cdot \sqrt{2} = \sqrt{2} < 1$. Hence, $\gamma \in \mathbb{Z}[i]$ and $\left|\frac{\alpha}{\beta} - \gamma\right| < 1$ therefore, $\delta = \alpha - \beta\gamma$.

Definition 10.8. *Let R be a ring. A norm is a function $N : R \to \mathbb{N}$ such that $N(0) = 0$.*

Definition 10.9. *Let R be a commutative ring with 1. R is Euclidean ring if there exists a norm function $N : R \setminus \{0\} \to \mathbb{N}$ such that*

1. *If $a, b \in R$ and $ab \neq 0$ then $N(a) \leq N(ab)$,*
2. *If $a, b \in R$ and $b \neq 0$ then there exists q, r such that $a = qb + r$ with $r = 0$ or $N(r) < N(b)$.*

Definition 10.10. *An Euclidean ring which is integral domain is Euclidean domain.*

Example 10.11. *Let F be a field then F is a ED. Let $a, b(\neq 0) \in F$ then $a = (ab^{-1})b + 0$ hence $N : F \to \mathbb{N}$ sends everyone to zero.*

Exercise 10.12. *Show that $\mathbb{Z}[i]$ is an Euclidean domain.*

Proposition 10.13. *Every Euclidean ring is principal ideal ring.*

Proof. If $0 \neq I \subseteq R$ be an ideal. Choose $a \in I$ such that $N(a)$ is the least integer in the set $\{N(a) : a \neq 0, a \in I\}$. If $b \in I$ then $b = aq + r$ with $r = 0$ or $N(r) < N(a)$. If $r \neq 0$ then $r = b - aq \in I$ is a contradiction. Therefore, $r = 0$ then $b = aq \Rightarrow b \in \langle a \rangle \Rightarrow I \subseteq \langle a \rangle$. Again, $a \in I \Rightarrow \langle a \rangle \subseteq I$. Therefore, $I = \langle a \rangle$. □

Proposition 10.14. *If K is a field then $K[x]$ is a Euclidean domain.*

Proof. Let $N : K[x] \setminus \{0\} \to \mathbb{N}$ by $N(f(x)) = \deg f$. Suppose, $f, g \in K[x] \setminus \{0\}, K$ is integral domain then $K[x]$ is also integral domain hence $fg \neq 0$. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $g(x) = b_m x^m + \cdots + b_1 x + b_0$ so that $fg = a_0 b_0 + \cdots a_n b_m x^{n+m}$ where $a_n b_m \neq 0$. Clearly, $\deg(fg) \geq \deg f$. $g(x) \neq 0$. If $\deg f < \deg g$ then $f = 0 \cdot g + f$ so we assume that $\deg f > \deg g$. If $m \leq n$ then

$$f = \frac{a_n}{b_m} x^{n-m}(b_m x^m + \cdots + b_0) + r_1(x)$$

where

$$r_1(x) = f - \frac{a_n}{b_m} x^{n-m} g(x)$$

and $\deg r_1(x) < \deg f$. If $\deg r_1(x) < \deg g(x)$ the we are done. Otherwise, let $r_1(x) = \dfrac{r_s}{b_m} x^{s-m} g(x) + r_2(x)$ where $\deg r_2(x) < \deg r_1(x)$. Continuing this process we get $f(x) = p(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg f(x)$. □

Remark. (1) *The same proof works for any commutative ring R and in $R[x]$ provided that $g(x)$ has leading term unit i.e., in particular if g is monic otherwise division is not possible for example $\mathbb{Z}[x]$ is not an Euclidean domain.*

(2) *The quotient and remainder is unique.*

Definition 10.15. *Let R be a commutative ring and a, b be non zero elements in R then greatest common divisor (gcd) of a, b is a non zero element d such that*

(1) *$d|a$ and $d|b$*
(2) *If $c|a$ and $c|b$ then $c|d$.*

Notation: $d = \gcd(a, b)$.
Check that,

(1) If $d = \gcd(a, b)$ and u is a unit then du is also a gcd.
(2) Let R be a domain and d, d' are both gcd of a, b then there exist a unit $u \in R$ such that $d = ud'$.

10.2. **Algorithm for finding gcd of two elements in a Euclidean domain.** Let R be an Euclidean domain and $a, b \in R$ be two non zero elements then,

$$\begin{aligned} a &= q_0 b + r_0, & N(r_0) &< N(b) \\ b &= q_1 r_0 + r_1, & N(r_1) &< N(r_0) \\ r_0 &= q_2 r_1 + r_2, & N(r_2) &< N(r_1) \\ &\vdots & &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, & N(r_n) &< N(r_{n-1}) \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

where r_n be the last non zero remainder. Note that the process must stop after finite stage as

$$N(b) > N(r_0) > N(r_1) > \cdots$$

is a strictly decreasing chain of positive integers.
Claim: $r_n = \gcd(a, b)$

(1) $r_n | a$ and $r_n | b$ (start from the bottom and go up)
(2) If $e | a$ and $e | b$ then $e | r_n$ (start from top and go down)

Show that $\langle a, b \rangle = \langle r_n \rangle$.
Conclusion: In an Euclidean domain, gcd exists. Further if $d = \gcd(a, b)$ then $\exists\ x, y \in R$ such that $ax + by = d$.

Theorem 10.16. *Every Euclidean domain is Principal ideal domain.*

Proof. Let R be an Euclidean domain and N be the standard Euclidean norm. Suppose, I is an ideal of R. If $I = \langle 0 \rangle$ then we are done so let us assume that $I \neq \langle 0 \rangle$.

$$\Sigma = \{N(a) : a \in I\}$$

By well ordering principal of natural number, I has a element that has minimum norm say a then $\langle a \rangle \subseteq I$. Now, pick $b \in I$ then by division algorithm, there exists $q, r \in R$ such that $b = aq + r$ with $r = 0$ or $N(r) < N(a)$. If $r \neq 0$ then $r = b - aq \in I$ with norm less than a which contradicts the choice of a. Hence, $r = 0$ and $I \subseteq \langle a \rangle$. Therefore, $I = \langle a \rangle$. □

Lemma 10.17. *Any two non zero element $a, b \in R$ where R is Euclidean domain having gcd d then $d = ax + by$ for some $x, y \in R$.*

Proof. Let, $I = \{as + bt : s, t \in R\}$. Suppose, $d \in I$ has minimum norm and $d = ax + by$ for some $x, y \in R$. As, $d \in I$, by division algorithm, $a = dq_1 + r_1$ with $r_1 = 0$ or $N(r_1) < N(d)$. Now, $r_1 = a - dq_1 \in I$ and $N(r_1) < N(d)$ which is contradiction, therefore, $r_1 = 0$ and $d | a_1$. Similarly we can show $d | b$. Hence, d is a common divisor of a, b. Moreover, $d = ax + by$ so every common divisor of a, b is also divide d hence $d = \gcd(a, b)$. □

Example 10.18. $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. $\mathbb{Z}[\sqrt{-5}]$ *is not an PID, hence not an ED.*

Note that $\mathbb{Z}[\sqrt{-5}]$ has a norm

$$\begin{aligned} N : \mathbb{Z}[\sqrt{-5}] &\to \mathbb{N} \\ z &\mapsto |z|^2 \end{aligned}$$

and N is multiplicative i.e., $N(z_1 z_2) = N(z_1)N(z_2)$.

Units of $\mathbb{Z}[\sqrt{-5}]$. Let $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ and $N(a + b\sqrt{-5}) = 1 \Rightarrow a^2 + 5b^2 = 1$ this gives, $a = \pm 1$ and $b = 0$. Therefore, $1, -1$ are the only norm one element. Now, let αbe a unit in $\mathbb{Z}[\sqrt{-5}]$ then there exists β such that

$$\begin{aligned} \alpha\beta &= 1 \\ N(\alpha\beta) &= N(1) \\ N(\alpha)N(\beta) &= 1 \end{aligned}$$

Hence, $N(\alpha) = 1$ gives only units of $\mathbb{Z}[\sqrt{-5}]$ are 1 and -1.

Question. *Show that $\mathbb{Z}[\sqrt{-5}]$ is not a PID.*

Ans. Consider the ideal $I = \langle 2, 1 + \sqrt{-5}\rangle$ we claim that I is not principal ideal. First we show that $I \neq \mathbb{Z}[\sqrt{-5}]$. Let

$$\begin{aligned} 1 &= 2\alpha + \beta(1 + \sqrt{-5}) \\ &= 2(a + b\sqrt{-5}) + (c + d\sqrt{-5})(1 + \sqrt{-5}) \\ &= (2a + c - 5d) + (2b + d + c)\sqrt{-5} \end{aligned}$$

Comparing the coefficient of real and imaginary part, we get $2a + c - 5d = 1$ and $2b + d + c = 0$. From this two equation we get $2a = 1$ which is a contradiction.
Suppose, $\langle 2, 1 + \sqrt{-5}\rangle = \langle \alpha\rangle$ for some $\alpha \in \mathbb{Z}[\sqrt{-5}]$. As, $2 \in \langle \alpha\rangle$ there exists $\beta \in \mathbb{Z}[\sqrt{-5}]$ such that $2 = \alpha\beta$ similarly, $1 + \sqrt{-5} = \gamma\alpha$ for some $\gamma \in \mathbb{Z}[\sqrt{-5}]$. Applying norm, we get $4 = N(2) = N(\alpha)N(\beta)$ then $N(\alpha) = 1, 2$ and 4. $N(\alpha) = 1$ will imply α is a unit and $I = \mathbb{Z}[\sqrt{-5}]$. Again, from second equation we get $6 = N(\alpha)N(\gamma)$. From these two equation we get $N(\alpha) = 2$. Let, $\alpha = a + b\sqrt{-5}$ so that $2 = N(\alpha) = a^2 + 5b^2$ but no integer solution can be found for this equation. Hence I is not principally generated, therefore, $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

Question 10.19. *Give an example of an element which is irreducible but not prime.*

Ans. In $\mathbb{Z}[\sqrt{-5}]$, 2 is irreducible but not prime. Let, $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. Applying norm, we have $4 = (a^2 + 5b^2)(c^2 + 5d^2)$ then either $a^2 + 5b^2 = 1$ or $c^2 + 5d^2 = 1$ (as we saw there is no element of norm 2 in $\mathbb{Z}[\sqrt{-5}]$). Therefore, either $a + b\sqrt{-5}$ is unit or $c + d\sqrt{-5}$ is unit. Hence, 2 is irreducible.
We show that 2 is not a prime as $2|6 = 2|(1 + \sqrt{-5})(1 - \sqrt{-5})$ but $2 \nmid (1 + \sqrt{-5})$ and $2 \nmid (1 - \sqrt{-5})$. Therefore, 2 is not a prime element.

Definition 10.20. *An integral domain is said to be a Factorization domain if every non zero, non unit element can be factored as product of irreducible elements.*

Definition 10.21. *A factorization domain is said to be Unique Factorization Domain (UFD) if every non zero, non unit element a can be factored as $a = p_1 \cdots p_n$ where p_i's are irreducible. If $a = q_1 \cdots q_m$ where q_i's are irreducible then $m = n$ and p_i is associated with $q_{\sigma(i)}$ for some $\sigma \in S_n$.*

Note: $\mathbb{Z}[\sqrt{-5}]$ is not an UFD since, $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ are two different factorization of 6. We claim that

(1) 2,3,$1+\sqrt{-5}$ and $1-\sqrt{-5}$ are irreducible,
(2) $2 \nsim 1+\sqrt{-5}$ or $1-\sqrt{-5}$ and $3 \nsim 1+\sqrt{-5}$ or $1-\sqrt{-5}$.

Suppose, 2 is reducible then $2 = (a+b\sqrt{-5})(c+d\sqrt{-5}) \Rightarrow 4 = (a^2+5b^2)(c^2+5d^2)$ then one of them must be a unit. Similarly if $3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$ then $9 = (a^2+5b^2)(c^2+5d^2)$ implies one of them must be unit. Suppose, $1+\sqrt{-5} = (a+b\sqrt{-5})(c+d\sqrt{-5})$ then $6 = (a^2+5b^2)(c^2+5d^2)$ which gives either $a^2+5b^2 = 1, 2, 3$ or 6. As we know there is no element of norm 2,3 in $\mathbb{Z}[\sqrt{-5}]$ either $a^2+5b^2 = 1$ or 6 which give $a+b\sqrt{-5}$ is unit or $c+d\sqrt{-5}$ is unit. Suppose, $2 \sim 1+\sqrt{-5}$ which imply $2 = u(1+\sqrt{-5})$ for some unit u. After applying norm, we have $4 = 6$ which is impossible.

Proposition 10.22. *In a Principal ideal domain, every non-zero prime ideal is maximal.*

Proof. Let $P = \langle p\rangle$ be a non-zero proper prime ideal. Assume that $P \subseteq M$, where M is a maximal ideal. As R is a PID, $M = \langle m\rangle$. Since, $p \in \langle m\rangle \Rightarrow p = \lambda m$. We know that in an integral domain, prime element implies irreducible element therefore, λ is unit or m is unit. m is not unit as $\langle m\rangle = R$, so λ is unit then $\langle p\rangle = \langle m\rangle$. □

Remark. *$\langle m\rangle = \langle \lambda m\rangle$ if λ is a unit. Clearly, $\langle \lambda m\rangle \subseteq \langle m\rangle$. λ is unit implies $m = \lambda^{-1}(\lambda m) \Rightarrow \langle m\rangle \subseteq \langle \lambda m\rangle$. Therefore, $\langle m\rangle = \langle \lambda m\rangle$.*

Proposition 10.23. *In a Principal ideal domain, gcd of two elements exists.*

Proof. Consider the ideal generated by $\langle a, b\rangle$. As, R is PID, $\langle a, b\rangle = \langle d\rangle$ for some $d \in R \setminus \{0\}$. $a, b \in \langle d\rangle$ therefore, $d|a$ and $d|b$. Let $e \in R \setminus \{0\}$ such that $e|a, e|b$ then $a, b \in \langle e\rangle \Rightarrow \langle a, b\rangle \subseteq \langle e\rangle \Rightarrow \langle d\rangle \subseteq \langle e\rangle \Rightarrow e|d$. So, d is gcd of a, b. Moreover, if $d = \gcd(a, b)$ then there exists $x, y \in R \setminus \{0\}$ such that $d = ax + by$. □

Question. *Show that in an integral domain gcd may not exist.*

Ans. In $\mathbb{Z}[\sqrt{-5}]$, $\gcd(6, 2(1+\sqrt{-5}))$ doesn't exists. Let $\alpha = 6 = 2\cdot 3$ and $\beta = 2(1+\sqrt{-5})$. If possible, let $\gamma = \gcd(\alpha, \beta)$ then $\gamma|6 \Rightarrow N(\gamma)|36 \Rightarrow N(\gamma) = 1, 2, 3, 4, 6, 9, 12, 18, 36$ and $\gamma|2(1+\sqrt{-5}) \Rightarrow N(\gamma)|24 \Rightarrow N(\gamma) = 1, 2, 3, 4, 6, 8, 12, 24$. Clearly $2|\alpha$ and $2|\beta$ as γ is gcd of α and β, $2|\gamma \Rightarrow 4|N(\gamma)$. Similarly, $(1+\sqrt{-5})|\gamma \Rightarrow N(1+\sqrt{-5})|N(\gamma) \Rightarrow 6|N(\gamma)$. From above relation only possible value for $N(\gamma)$ is 12. Let $\gamma = a+b\sqrt{-5} \Rightarrow 12 = N(\gamma) = a^2+5b^2$ but there is no integer solution exists. Therefore, γ doesn't exist.

Observation 10.24. *Let $X = \{a_1, \cdots, a_n\}$ and $d = \gcd(X)$ then*

(1) *If R is a principal ideal domain, then $d = a_1r_1 + \cdots + a_nr_n$,*
(2) *If R is Unique factorization domain, then $\gcd(X)$ exists.*

Question. *Are irreducibles prime in UFD?*

Ans. Yes. Let p be an irreducible and assume that $p|ab \Rightarrow ab = \lambda p$. Factorizations of the elements of the above equation gives

$$(ua_1 \cdots a_n)(vb_1 \cdots b_m) = (w\lambda_1 \cdots \lambda_k)p$$

Then p must be either a_i or b_i which imply either $p|a$ or $p|b$. Thus p is prime.

Proposition 10.25. *In a UFD, gcd of two element exist.*

Proof. Let R be a UFD and $a, b \in R \setminus \{0\}$ then unique factorizations of a and b into irreducible element gives

$$a = up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$
$$b = vp_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$$

where u, v are units and $\alpha_i, \beta_i \geq 0$ for all $i \in \{1, \cdots, n\}$. Let $d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$ where $\gamma_i = \min\{\alpha_i, \beta_i\}$ for all $1 \leq i \leq n$. Then $d = \gcd(a, b)$. □

Note that gcd of $2, x$ exists and is equal to 1 but 1 can't be written as $1 = 2f(x) + xg(x)$.

Theorem 10.26. *Let R be a UFD and P be any non zero prime ideal then there exists a non zero prime ideal P_1 such that $P_1 \subsetneq P$ and P_1 is principal.*

Proof. Since P is a non zero prime ideal, we pick $r \in P$. Then $r = \pi_1^{s_1} \cdots \pi_k^{s_k} \in P \Rightarrow \pi_i^{s_i} \in P$ for some i which imply $\pi_i \in P \Rightarrow (\pi_i) \subsetneq P$. This proof follows from the fact that irreducibles are prime in UFD. □

Corollary 10.27. *In a UFD R, $P \subsetneq R$ is a prime ideal. Then P is principal iff $P = 0$ or $P \supsetneq P_1$, P_1 is prime implies $P_1 = 0$.*

Proof. If $P = 0$ then $P = \langle \emptyset \rangle$. Let P is a non zero prime ideal which is also principally generated then by previous theorem there exists a prime ideal $P_1 = \langle \pi \rangle \subsetneq P$. Both P, P_1 are maximal in the set of all principally generated ideals of R (as p, π are irreducible in R) we have $P_1 = 0$. Conversely, let $P \neq 0$ is a prime ideal and $P_1 \subsetneq P$ such that P_1 is prime and P_1 is zero ideal.

Question 10.28. *Is $\mathbb{Z}[x]$ PID?*

Ans. No. Since the ideal $\langle p, x \rangle$ is not principal where $p \in \mathbb{Z}$ is prime. We know that $\langle p, x \rangle$ is prime in $\mathbb{Z}[x]$ and $(p) \subsetneq \langle p, x \rangle$ is a non zero prime ideal. By previous corollary $\langle p, x \rangle$ is not principal.

Lemma 10.29. *Let R be a PID and $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be a chain of ideals then there exist $n \in \mathbb{N}$ such that $I_n = I_k$ for all $n \geq k$.*

Proof. Let $I = \bigcup_{n \in \mathbb{N}} I_n$ then I is an ideal and $I = \langle a \rangle$ for some $a \in R$ as R is PID. Therefore, $a \in I = \bigcup_{n \in \mathbb{N}} I_n \Rightarrow a \in I_n$ for some $n \in \mathbb{N} \Rightarrow \langle a \rangle \subseteq I_n \Rightarrow I \subseteq I_n$. Clearly, $I_n \subseteq I$ hence $I = I_n \Rightarrow I_n = I_{n+1} = I_{n+2} \cdots$. □

Theorem 10.30. *Every Principal ideal domain is Unique factorization domain.*

Proof. There are two different proof of this theorem and we present it one by one. Let R be a PID and $r \in R$ be a non zero, non unit element. If r is irreducible then we stop. If not $r = r_1 r_2$ where $r_, r_2$ is not unit. If r_1, r_2 are irreducible then we stop. If not, say r_1 is reducible then $r_1 = r_{11} r_{12}$ where neither r_{11} nor r_{12} is unit then $\langle r \rangle \subsetneq \langle r_1 \rangle$(as r_2 is not unit) and $\langle r_1 \rangle \subsetneq \langle r_{11} \rangle$ (since r_{12} is not an unit). Also note that they all are proper ideal and

$$\langle r \rangle \subsetneq \langle r_1 \rangle \subsetneq \langle r_{11} \rangle \subsetneq \cdots$$

This is an increasing chain of ideal and as R is PID, it stabilize after some finite step. Thus we conclude that r is a product of finitely many irreducible. We claim that such factorization is unique. Let $r = p_1 \cdots p_n = q_1 \cdots q_m$ be two factorization of r into irreducibles. p_1 is irreducible and R is PID then p_1 is prime thus $p_1 | q_1 \cdots q_m \Rightarrow p_1 | q_i$ for some i. Renaming if necessary, let $p_1 | q_1 \Rightarrow q_1 = \lambda_1 p_1$. As, q_1 is irreducible, λ_1 is unit and $r = p_1 \cdots p_n = (\lambda_1 p_1) \cdots q_m \Rightarrow p_2 \cdots p_n = \lambda_1 q_2 \cdots q_m$ then $p_2 | q_i$ for some $2 \leq i \leq m$. Renaming if necessary, let say $p_2 | q_2 \Rightarrow p_2 = \lambda_2 q_2$ where λ_2 is an unit. Therefore, $n = m$ and $p_i \sim q_i$ for all i.

Another proof. We consider

$$\sum = \{x \in R : x \text{ is non-zero, non-unit and can't be written as finite product of irreducibles}\}$$

If $\sum \neq \emptyset$, let $a \in \sum$, since a is non-zero,non-unit $\langle a \rangle \subseteq R$ is proper so there is an irreducible $c_a \in R$ such that $\langle a \rangle \subseteq \langle c_a \rangle$. Therefore, $c_a | a \Rightarrow a = c_a x_a$. If x_a is a unit then c_a and a is associates so a is irreducible. Hence, x_a can't be a unit. If x_a is finite product of irreducible then also this is a contradiction. Again $x_a = 0 \Rightarrow a = 0$, so $x_a \in \sum$. Note that, $\langle a \rangle \subsetneq \langle x_a \rangle$. Now we define a map

$$\begin{aligned} f : \sum &\to \sum \\ a &\mapsto x_a \end{aligned}$$

f is well defined. [Suppose, $a = c_a x_a = c_a y_a \Rightarrow x_a = y_a$] Now, define

$$\begin{aligned} \phi : \mathbb{N} &\to \sum \\ n &\mapsto f^n(a) := x_{\phi(n)} \end{aligned}$$

Then

$$\langle a \rangle \subsetneq \langle x_{\phi(1)} \rangle \subsetneq \langle x_{\phi(2)} \rangle \subsetneq \cdots \tag{5}$$

Since R is PID, the chain must be stationary i.e., $\exists\ n \in \mathbb{N}$ such that $\langle x_{\phi(n)} \rangle = \langle x_{\phi(i)} \rangle, \forall\ i \geq n$. Therefore, $\sum$ is empty.
Let $a = c_1 \cdots c_n = d_1 \cdots d_m$ where c_i, d_i are irreducible and $c_i | d_{i_j}$ for some $i_j \in \{1, \cdots, m\}$. Since, both are ireeducible c_i and d_{i_j} are associates. Lrt $c_i = u_i d_{i_j}$ and $d_{i_j} = v_i c_i$. If $n > m$ then we get $c_{m+1} \cdots c_n = u_1 \cdots u_m$ which is a contradiction. If $m > n$, $v_1 \cdots v_n =$ product of some d_i's, again a contradiction. Therefore, $n = m$. □

Lemma 10.31. *Let I be an ideal of R and $f \in R$ be an element of R. Suppose, $J = I + \langle f \rangle$ and J and $(I : J)$ both are principal then I is principal and $I = J \cdot (I : J)$.*

Proof. Let $x \in I \subseteq J = \langle a + ft \rangle$ (say) where $a \in I, t \in R$ then $x = s(a + ft)$. Let $y \in J$ then $y = r(a + ft)$ where $r \in R$. $sy = sr(a + ft) = xr \in I \Rightarrow sJ \subseteq I$ as $y \in J$ is chosen arbitrarily then $s \in (I : J)$ thus $x \in J \cdot (I : J)$. Therefore, $I \subseteq J(I : J)$. Let $\sum a_i s_i \in J(I : J)$ where

$a_i \in J, s_i \in (I : J)$ then $a_i s_i \in I \Rightarrow \sum a_i s_i \in I \Rightarrow J(I : J) \subseteq I$. Hence, $I = J(I : J)$. Let $(I : J) = \langle \beta \rangle$ then $I = \langle (a + ft)\beta \rangle$, hence I is principal. □

Theorem 10.32. *Let R be an integral domain. R is principal ideal domain iff every prime ideal is principal.*

Proof. ($\Rightarrow$) Trivial.

($\Leftarrow$) Suppose, R is an integral domain in which every prime ideals are principal. Let $\sum = \{I \subseteq R : I$ is an ideal of R and I is not principal$\}$. If $\sum \neq \emptyset$ then consider $\{I_\lambda\}_{\lambda \in \Lambda}$ be a chain in $\sum$. If $\bigcup_{\lambda \in \Lambda} I_\lambda = \langle a \rangle$ then $a \in I_\lambda$ for some $\lambda \in \Lambda \Rightarrow I_\lambda = \langle a \rangle$ is a contradiction as $I_\lambda \in \sum$. Therefore, $\bigcup_{\lambda \in \Lambda} I_\lambda$ is not a principal ideal, hence $\bigcup_{\lambda \in \Lambda} I_\lambda \in \sum$. Every chain in $\sum$ has an upper bound. Therefore, by Zorn's lemma $\sum$ has a maximal element say P. We will show that P is a prime ideal. If not suppose $a \notin P, b \notin P$ and $ab \in P$. Let $J = P + \langle a \rangle$ then $P \subsetneq J$ and $b \in (P : J)$ [$\because ab \in P$] imply $P \subsetneq (P : J)$ [as $b \in (P : J)$ but $b \notin P$]. Since P is maximal element of $\sum$, J and $(P : J)$ both are principal ideal and by previous lemma $P = J(P : J)$ is principal. This gives a contradiction that $P \in \sum$. Therefore, P is a prime then P is principal again contradiction as $P \in \sum$. Hence, $\sum = \emptyset$ and R is PID. □

Question. *Which odd primes of $\mathbb{Z}$ can be expressed as sum of two squares?*

Ans. All odd primes of the form $4k + 1$.

Question. *Suppose, p be a prime of the form $4k + 1$. Can p be written as sum of two squares?*

Ans. Suppose p is not irreducible in $\mathbb{Z}[i]$ i.e., $p = (a+bi)(c+di) \Rightarrow N(p) = N(a+bi)N(c+di) \Rightarrow p^2 = (a^2 + b^2)(c^2 + d^2)$. If one of the factor becomes 1 then p is irreducible. If p is not irreducible then $a^2+b^2 = c^2+d^2 = p$. So its enough to show that p is not irreducible in $\mathbb{Z}[i]$. As $\mathbb{Z}[i]$ is UFD, we will show that p is not prime in $\mathbb{Z}[i]$. So we wish to show that if $p = 4k+1$ then $X^2+1 \equiv 0 \ (mod\ p)$ has a solution.

11. Noetherian and Artinian ring

Definition 11.1. *Let R be a ring and Σ be the set of all ideals of R. We say Σ satisfy a.c.c (ascending chain condition) if for any increasing chain $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ in Σ there exists $n \in \mathbb{N}$ such that $I_n = I_{n+1} = \cdots$ and we say R satisfies d.c.c (descending chain condition) if for any decreasing chain $I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$ in Σ, there exists $n \in \mathbb{N}$ such that $I_n = I_{n+1} = \cdots$.*

Observation 11.2. *R satisfies acc iff every ideal in R is finitely generated.*

Proof. Suppose, R satisfies acc. If $\exists\ I \in \Sigma$ such that I is not finitely generated. Let $a_0 \in I, a_1 \in I - a_0R, a_2 \in I - (a_0R + a_1R)$ and so on. Note that I is not finitely generated this implies,

$$I - \left(\sum_{i=1}^{n} a_iR\right) \neq \emptyset$$

If $I - \left(\sum_{i=1}^{n} a_iR\right) = \emptyset \Rightarrow I \subseteq \sum_{i=1}^{n} a_iR \subseteq I$ as $a_i \in I$ for all i then $I = \sum_{i=1}^{n} a_iR$, we arrive at a contradiction. So we get a sequence of increasing ideal $J_0 = a_0R, \cdots, J_n = \sum_{i=1}^{n} a_iR$ and

$$J_0 \subseteq J_1 \subseteq \cdots \subseteq J_n \subseteq \cdots$$

and $J_{n-1} \subsetneq J_n$, contradiction. Hence I is finitely generated.
Conversely, If every ideal of R is finitely generated and we have a chain

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

then $\bigcup_{i=1}^{\infty} I_i$ is finitely generated ideal. Let $\bigcup_{i=1}^{\infty} I_i = \langle a_1, \cdots, a_r\rangle, a_i \in R$ then there exists j_k such that $a_k \in I_{j_k}, k \in \{1, \cdots, r\}$. Let $n = \max\{j_k|\ 1 \leq k \leq r\}$ then $\bigcup_{i=1}^{\infty} I_i = \langle a_1, \cdots, a_r\rangle = I_n$ this implies $I_n = I_{n+1} = \cdots$ hence R satisfies acc.

Example 11.3. *$\mathbb{Z}$ satisfies acc since every ideal of $\mathbb{Z}$ is principal.*

Definition 11.4. *A commutative ring with identity which satisfies acc is called Noetherian ring, and if it satisfies dcc we call it Artinian ring.*

Exercise 11.5. *$\mathbb{Z}$ is not an Artinian ring. $\mathbb{Z}/n\mathbb{Z}$, any field is Artinian ring. Let K be a field then $K[t]/t^n$ is Artinian for every integer $n > 1$.*

Let $R = K[x]/(x^2)$ then ideals are is of the form $I/(x^2)$ where $(x^2) \subseteq I$ i.e., $x^2 \in I$. Let $I = \langle f(x)\rangle$ then $f(x)|x^2 \Rightarrow f(x) = x$ or x^2 therefore, ideals are $0, x/(x^2)$ this implies R is Artinian. R is Noetherian ring and $K[x]/x^2$ is infinite ring as R is a vector space over K of dimension 2. Therefore, R is infinite.

Problem 11.6. *Is $C[0,1]$ Noetherian?*

Ans. Let $\Sigma_x = \{f \in C[0,1] : f(t) = 0,\ \forall t \in [0,x],\ 0 \le x \le 1\}$. If $x > y$ then $\Sigma_x \supsetneq \Sigma_y$ so if we choose $r_1 \le r_2 \le \cdots$ where $r_i's$ are rationale then we have

$$\Sigma_0 \subsetneq \Sigma_{r_1} \subsetneq \Sigma_{r_2} \subsetneq \cdots$$

therefore, $C[0,1]$ is not Noetherian then $C[0,1]$ is not Artinian also.
Note: A ring is Artinian implies it is also Noetherian (with dim 0). Artinian ring but not Noetherian is not possible.

Problem 11.7. *Show that if K be a field then $K[x]$ is PID.*

Ans. Let $I \subseteq K[x]$ be an ideal. If $I = 0$ then it is principal. If $I \neq 0$ then we consider the set

$$\Gamma = \{n : n = \deg f,\ f \in I\}$$

By well ordering principle of natural number Γ has an least element say m_0 then there exists $g \in I$ such that $\deg g = m_0$. If $f \in I$ by division algorithm $f = gq + r$ where $r = 0$ or $\deg r < \deg g$. As $f, g \in I \Rightarrow r \in I$ if $r \neq 0$ then we get a contradiction as $\deg r < \deg g$. Therefore, $\deg g = m_0$ is the least element in $\Gamma \Rightarrow f = gq \Rightarrow I \subseteq \langle g \rangle$ but $g \in I \Rightarrow I = \langle g \rangle$. □

Problem 11.8. *Is $K[x_1, \cdots, x_n]$ Noetherian?*

Ans. Yes (Hilbert basis theorem)

Observation 11.9. *If R is an Artin integral domain, then R is a field.*

Proof. Let $x \neq 0$ the we consider the chain of ideals

$$(x) \supseteq (x^2) \supseteq (x^3) \supseteq \cdots$$

then there exists $n \in \mathbb{N}$ such that $(x^n) = (x^{n+1}) = \cdots \Rightarrow x^n \in (x^{n+1}) \Rightarrow x^n = yx^{n+1} \Rightarrow x^n(xy-1) = 0$ since R is integral domain $xy - 1 = 0 \Rightarrow xy = 1 \Rightarrow x$ is a unit hence R is a field. □

Lemma 11.10. *If R is an Artin ring then maxspec R is finite.*

Proof. Suppose, $\{m_1, m_2, \cdots\} \subseteq \operatorname{maxspec} R$ (an infinite set) and consider the chain

$$m_1 \supseteq m_1 \cap m_2 \supseteq m_1 \cap m_2 \cap m_3 \supseteq \cdots$$

then for some k we get $m_1 \cap \cdots \cap m_k = m_1 \cap \cdots \cap m_k \cap m_{k+1} \Rightarrow m_{k+1} \supseteq m_1 \cap \cdots \cap m_k$ by prime avoidance lemma $m_{k+1} \supseteq m_i$ for some $i \in \{i, \cdots, k\}$ but m_{k+1}, m_i both maximal this implies maxspec R is finite. □

Remark 11.11. *Any Artin ring is semi local.*

Observation 11.12. *If (R, m) is a Artin local ring then $m^k = 0$ for some $k \in \mathbb{N}$.*

12. Zariski topology

Let R be a commutative ring with 1 and $I \subseteq R$ is an ideal of R. Define

$$V(I) = \{P \in \operatorname{spec} R : I \subseteq P\}$$

Then the followings hold:

(1) $V(0) = \operatorname{spec} R$
(2) $V(1) = \emptyset$
(3) If $I \subseteq J$ then $V(J) \subseteq V(I)$
(4) $V(I) \cup V(J) = V(IJ) = V(I \cap J)$
(5) $\bigcup_{i=1}^{n} V(I_i) = V\left(\prod_{i=1}^{n} I_i\right) = V\left(\bigcap_{i=1}^{n} I_i\right)$
(6) $V(I) = V(\sqrt{I})$
(7) Let $\{I_\alpha\}_{\alpha\in\Lambda}$ be a collection of ideals in R then $\bigcap_{\alpha\in\Lambda} V(I_\alpha) = V\left(\sum_{\alpha\in\Lambda} I_\alpha\right)$

Proof. (3) Let $I \subseteq J$. Pick $P \in V(J) \Rightarrow J \subseteq P \Rightarrow I \subseteq P \Rightarrow P \in V(I) \Rightarrow V(J) \subseteq V(I)$.
(4) Let $P \in V(I) \cup V(J) \Rightarrow P \in V(I)$ or $P \in V(J)$ then $I \subseteq P$ or $J \subseteq P \Rightarrow IJ \subseteq P \Rightarrow P \in V(IJ) \Rightarrow V(I) \cup V(J) \subseteq V(IJ)$. For reverse inclusion, let $P \in V(IJ) \Rightarrow IJ \subseteq P \Rightarrow I \subseteq P$ or $J \subseteq P$ then $P \in V(I)$ or $P \in V(J) \Rightarrow P \in V(I) \cup V(J) \Rightarrow V(IJ) \subseteq V(I) \cup V(J)$. Therefore, $V(I) \cup V(J) = V(IJ)$. We have $IJ \subseteq I \cap J \Rightarrow V(I \cap J) \subseteq V(IJ)$. For other case let $I \cap J \subseteq I$ and $I \cap J \subseteq J$ then $V(I) \subseteq V(I \cap J)$ and $V(J) \subseteq V(I \cap J) \Rightarrow V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(IJ) = V(I) \cup V(J)$. Hence,

$$V(I) \cup V(J) = V(IJ) = V(I \cap J)$$

(5) Inductively from (4).
(6) We know $I \subseteq \sqrt{I} \Rightarrow V(\sqrt{I}) \subseteq V(I)$. Let $P \in V(I) \Rightarrow I \subseteq P \Rightarrow \sqrt{I} \subseteq \sqrt{P} = P \Rightarrow P \in V(\sqrt{I}) \Rightarrow V(I) \subseteq V(\sqrt{I})$.
(7) $I_\alpha \subseteq \sum_{\alpha\in\Lambda} I_\alpha \Rightarrow V\left(\sum_{\alpha\in\Lambda} I_\alpha\right) \subseteq V(I_\alpha) \Rightarrow V\left(\sum_{\alpha\in\Lambda} I_\alpha\right) \subseteq \bigcap_{\alpha\in\Lambda} V(I_\alpha)$. Let $P \in \bigcap_{\alpha\in\Lambda} V(I_\alpha) \Rightarrow P \in V(I_\alpha), \forall\, \alpha \in \Lambda \Rightarrow I_\alpha \subseteq P, \forall\, \alpha \in \Lambda \Rightarrow \sum_{\alpha\in\Lambda} I_\alpha \subseteq P \Rightarrow P \in V\left(\sum_{\alpha\in\Lambda} I_\alpha\right) \Rightarrow \bigcap_{\alpha\in\Lambda} V(I_\alpha) \subseteq V\left(\sum_{\alpha\in\Lambda} I_\alpha\right)$.
Hence $\bigcap_{\alpha\in\Lambda} V(I_\alpha) = V\left(\sum_{\alpha\in\Lambda} I_\alpha\right)$. □

Let $X = \operatorname{spec} R$ and $\tau = \{\operatorname{spec} R \setminus V(I) : I \text{ is an ideal of } R\}$ then check that (X, τ) is a topological space. If $I = \emptyset$ then $V(I) = \operatorname{spec} R$ so $\emptyset \in \tau$, if $I = R$ then $V(I) = \emptyset$ so $X \in \tau$. Let

$\{U_\alpha\}_{\alpha\in\Lambda} \in \tau$ then $U_\alpha = V(I_\alpha)^c$ as we have

$$\bigcap_{\alpha\in\Lambda} V(I_\alpha) = V\left(\sum_{\alpha\in\Lambda} I_\alpha\right)$$
$$\left[\bigcap_{\alpha\in\Lambda} V(I_\alpha)\right]^c = \left[V\left(\sum_{\alpha\in\Lambda} I_\alpha\right)\right]^c$$
$$\bigcup_{\alpha\in\Lambda} U_\alpha = V\left(\sum_{\alpha\in\Lambda} I_\alpha\right)^c$$

Thus $\bigcup_{\alpha\in\Lambda} U_\alpha \in \tau$. Let $\{U_I\}_{i=1}^n \in \tau \Rightarrow U_i = V(I_i)^c, 1 \le i \le n$ then

$$\begin{aligned} U_1 \cap U_2 \cap \cdots \cap U_n &= V(I_1)^c \cap \cdots \cap V(I_n)^c \\ &= [V(I_1) \cup \cdots \cup V(I_n)]^c \\ &= \left[V\left(\sum_{i=1}^n I_i\right)\right]^c \in \tau \end{aligned}$$

Therefore, τ is a topology on spec R this topology is called as Zariski topology on *specR*.

Lemma 12.1. *Show that $V(I) = V(J)$ if and only if $\sqrt{I} = \sqrt{J}$.*

Proof. ($\Rightarrow$) Suppose, $V(I) = V(J)$. Now we know that

$$\sqrt{I} = \bigcap_{P\in V(I)} P \quad \text{and} \quad \sqrt{J} = \bigcap_{P\in V(J)} P$$

Since $V(I) = V(J)$ we get $\sqrt{I} = \sqrt{J}$.
($\Leftarrow$) Suppose, $\sqrt{I} = \sqrt{J}$ and $P \in V(I) \Leftrightarrow I \subseteq P \Leftrightarrow \sqrt{I} \subseteq \sqrt{P} = P \Leftrightarrow \sqrt{J} \subseteq P \Leftrightarrow P \in V(J)$. Thus $V(I) = V(J)$. □

Let $m \in$ maxspec R then $V(m) = \{m\}$. Similarly,

$$V(m^r) = \{P \in specR : m^r \subseteq P\} = \{P \in specR : \sqrt{m^r} \subseteq \sqrt{P}\} = \{P \in specR : m \subseteq P\} = \{m\}$$

Observation 12.2. *In a commutative ring any two maximal ideals are comaximal. Moreover, any power of two comaximal ideals are comaximal. Let $m_1, m_2 \in$ maxspec R then $V(m_1 + m_2) = \emptyset$ as $m_1 + m_2 = 1$ i.e., they are comaximal ideals in R. Similarly $m_1^{r_1}$ and $m_2^{r_2}$ are also comaximal because*

$$V(m_1^{r_1} + m_2^{r_2}) = V(m_1^{r_1}) \cap V(m_2^{r_2}) = \{m_1\} \cap \{m_2\} = \phi = V(1)$$

therefore, $1 \in m_1^{r_1} + m_2^{r_2}$. It follows from the previous lemma as $1 = \sqrt{1} = \sqrt{m_1^{r_1} + m_2^{r_2}} = \sqrt{\sqrt{m_1^{r_1}} + \sqrt{m_2^{r_2}}} = \sqrt{m_1 + m_2}$.

Let R be a commutative ring with 1 such that maxspec $R = \{m_1, \cdots, m_r\}$ and

$$m_1^{\alpha_1} \cdots m_r^{\alpha_r} = 0$$

Then

$$R = R/(0) = R/m_1^{\alpha_1} \cdots m_r^{\alpha_r} \cong R/m_1^{\alpha_1} \times \cdots \times R/m_r^{\alpha_r}$$

i.e., R can be written as finite product of local rings.

Exercise 12.3. *Try to find an example of a ring in which product of maximal ideals is 0.*

Example 12.4. *Give an example of a ring R such that R is not integral domain but $nil(R) = \{0\}$.*

Ans. Product of any two integral domain.

13. Exercise

Exercise 13.1. $\dfrac{R[x]}{(x-a)} \cong R$ *where* $a \in R$.

Proof.

$$R[x] \xrightarrow{\theta} R$$
$$f(x) \mapsto f(a)$$

Then θ is a ring homomorphism. Let $c \in R$ then $\theta(x-a+c) = c$ therefore, θ is surjective. $\ker\theta = \{f(x) \in F[x] : f(a) = 0\}$ then clearly, $\langle x-a\rangle \subseteq \ker\theta$. Let $f(x) \in \ker\theta \Rightarrow f(x) = q(x)(x-a) + r(a) \Rightarrow \theta(f(x)) = \theta(q(x))\theta(x-a) + \theta(r(a)) \Rightarrow (r(a)) = 0 \Rightarrow \ker\theta \subseteq \langle x-a\rangle$. Thud, $\ker\theta = \langle x-a\rangle$. By first isomorphism theorem $R[x]/\langle x-a\rangle \cong R$. □

Exercise 13.2. *Let* $C[0,1] = \{f : [0,1] \to \mathbb{R} : f$ *is continuous*$\}$ *be a ring and* $c \in [0,1]$. *Define a map*

$$\phi : C[0,1] \to \mathbb{R}$$
$$f \quad \mapsto f(c)$$

Show that ϕ *is a surjective ring homomorphism. Let* $m_c = \{f \in C[0,1] : f(c) = 0\}$. *Also show that* $C[0,1]/m_c \cong \mathbb{R}$.

Proof.

$$\phi : C[0,1] \to \mathbb{R}$$
$$f \quad \mapsto f(c)$$

Clearly, ϕ is a ring homomorphism. Pick any $a \in R$ then the constant map $f(x) = a \in C[0,1]$ which imply $\phi(f(x)) = a$ therefore, ϕ is surjective. $\ker\phi = \{f(x) \in C[0,1] : f(c) = 0\} = m_c$ by first isomorphism theorem, $C[0,1]/m_c \cong \mathbb{R}$. □

Exercise 13.3. $\dfrac{\mathbb{R}[x]}{\langle x^2+1\rangle} \cong \mathbb{C}$.

Proof.

$$\mathbb{R}[x] \xrightarrow{\theta} \mathbb{C}$$
$$f(x) \mapsto f(i)$$

Then θ is a ring homomorphism. Let $a + ib \in \mathbb{C}$ then $\theta(a+bx) = a + ib$ therefore, θ is surjective. $\ker\theta = \{f(x) \in \mathbb{R}[x] : f(i) = 0\}$ then clearly, $\langle x^2+1\rangle \subseteq \ker\theta$. Let $f(x) \in \ker\theta \Rightarrow f(x) = q(x)(x^2+1) + ax + b \Rightarrow \theta(f(x)) = \theta(q(x))\theta(x^2+1) + \theta(ax+b) \Rightarrow b + ia = 0 \Rightarrow \ker\theta \subseteq \langle x^2+1\rangle$. Thud, $\ker\theta = \langle x^2+1\rangle$. By first isomorphism theorem $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$. □

Exercise 13.4. $\dfrac{\mathbb{C}[x]}{\langle x^2+1\rangle} \cong \mathbb{C} \times \mathbb{C}$.

Proof. As, $x^2+1 = (x+i)(x-i)$ and $1 = \dfrac{1}{2i}[(x+i)-(x-i)]$ which imply $\langle x-i\rangle$ and $\langle x+i\rangle$ are co-maximal. By Chinese remainder theorem $\mathbb{C}[x]/\langle x^2+1\rangle = \mathbb{C}[x]/\langle x+i\rangle\langle x-i\rangle = \mathbb{C}/\langle x+i\rangle \times \mathbb{C}[x]/\langle x_i\rangle = \mathbb{C} \times \mathbb{C}$.

Exercise 13.5. $\dfrac{\mathbb{Z}[x]}{\langle 2x-1\rangle} \cong \mathbb{Z}\left[1/2\right].$

Proof.

$$\mathbb{Z}[x] \xrightarrow{\theta} \mathbb{Z}[1/2]$$
$$f(x) \mapsto f(1/2)$$

As, $\mathbb{Z} \subseteq \mathbb{Q} \Rightarrow \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ and $f(x) \in \ker\theta \Leftrightarrow f(1/2) = 0$.

Exercise 13.6. $\dfrac{\mathbb{R}[x]}{\langle 2x-1\rangle} \cong \mathbb{R}.$

Proof. By problem 12.1

Exercise 13.7. $\dfrac{\mathbb{R}[x]}{\langle x^3-x\rangle} \cong \mathbb{R}\times\mathbb{R}\times\mathbb{R}$

Proof. $(x^3-x) = x(x-1)(x+1)$ thus $1 = \dfrac{1}{2}[(x+1)-(x-1)] = [x-(x-1)] = [(x+1)-x]$ therefore, $\langle x\rangle, \langle x-1\rangle, \langle x+1\rangle$ are mutually co-maximal ideal hence by chiense remainder theorem, $\mathbb{R}[x]/\langle x^3-x\rangle \cong \mathbb{R}[x]/\langle x\rangle \times \mathbb{R}[x]/\langle x-1\rangle \times \mathbb{R}[x]/\langle x+1\rangle \cong \mathbb{R}\times\mathbb{R}\times\mathbb{R}$.
Find the pre-image of (1,2,3). Let $f(x) \in \mathbb{R}[x]$ such that $f(x) + \langle x^3+1\rangle = (1,2,3)$ then $f(x) = a+bx+cx^2$ where $a,b,c \in \mathbb{R}$ then $f(0) = a = 1, f(1) = a+b+c = 3$ and $f(-1) = a-b+c = 2$. Solving the equations we have $f(x) = 1 + \dfrac{x}{2} + \dfrac{3x^2}{2}$. □

Exercise 13.8. *Parabola*

$$\theta : K[x,y] \to K[t]$$
$$x \mapsto t$$
$$y \mapsto t^2$$

Find $\operatorname{Ker}\theta$.

Exercise 13.9. *Twisted cubic curve*

$$\theta : K[x,y,z] \to K[t]$$
$$x \mapsto t$$
$$y \mapsto t^2$$
$$z \mapsto t^3$$

Find $\operatorname{Ker}\theta$.

Ans. $\ker\theta = \langle y-x^2, z-x^3\rangle$. Let $f(x,y,z) \in \ker\theta$, by division algorithm

$$f(x,y,z) = (z-x^3)g(x,y,z) + r(x,y)$$
$$r(x,y) = (y-x^2)h(x,y) + r_1(x)$$

Therefore,

$$f(x,y,z) = (z-x^3)g(x,y,z) + (y-x^2)h(x,y) + r_1(x)$$

Applying θ on both side, we get,

$$0 = 0 + r_1(t) \Rightarrow r_1(x) = 0$$

Thus, $f(x,y,z) = (z-x^3)g(x,y,z) + (y-x^2)h(x,y) \Rightarrow f(x,y,z) \in \langle z-x^3, y-x^2\rangle$. Conversely, $z-x^3 \in \ker\theta, y-x^2 \in \ker\theta \Rightarrow \langle z-x^3, y-x^2\rangle \subseteq \ker\theta \Rightarrow \ker\theta = \langle z-x^3, y-x^2\rangle$. □

Exercise 13.10.

$$\begin{aligned}\theta : K[x,y,z] &\to K[t]\\ x &\mapsto t^2\\ y &\mapsto t^3\\ z &\mapsto t^5\end{aligned}$$

Find $\operatorname{Ker}\theta$.

Exercise 13.11.

$$\begin{aligned}\theta : K[x,y] &\to K[t]\\ x &\mapsto t^a\\ y &\mapsto t^b\end{aligned}$$

Where K is any field and $\gcd(a,b) = 1$. *Show that* $\operatorname{Ker}\theta = \langle y^a - x^b\rangle$.

Proof. Let $f(x,y) \in \ker\theta$. Since, $y^a - x^b$ is monic in y

$$f(x,y) = (y^a - x^b)g(x,y) + (r_0(x) + r_1(x)y + \cdots + r_{a-1}(x)y^{a-1}))$$

Applying θ both side,

$$0 = 0 + r_0(t^a) + r_1(t^a)t^b + \cdots + r_{a-1}(t^a)t^{b(a-1)}$$

Let $r_i(x) = a_{0,i} + a_{1,i}x + \cdots + a_{k_i,i}x^{k_i}, 0 \le i \le a-1, a_{ij} \in K$ then

$$\begin{aligned}r_i(t^a) &= a_{0,i} + a_{1,i}t^a + \cdots + a_{k_i,i}t^{ak_i}\\ r_i(t^a)t^{ib} &= a_{0,i}t^{ib} + a_{1,i}t^{a+ib} + \cdots + a_{k_i,i}t^{ak_i+b}\end{aligned}$$

therefore,

$$\begin{aligned}0 = \sum_{i=0}^{a-1} r_i(t^a)t^{ib} &= \sum_{i=0}^{a-1}(a_{0,i}t^i b + a_{1,i}t^{a+ib} + \cdots + a_{k_i,i}t^{ak_i+ib})\\ &= (a_{0,0} + a_{0,1}t^b + \cdots + a_{0,a-1}t^{a-1}b) + (a_{1,0}t^a + a_{1,1}t^{a+b} + \cdots + a_{1,a-1}t^{a+(a-1)b})\\ &\quad + \cdots + (a_{k_0,0}t^{ak_0} + a_{k_1,1}t^{ak_1+b} + \cdots + a_{k_{a-1},a-1}t^{ak_{a-1}+(a-1)b}) \qquad (6)\end{aligned}$$

Let $k_1a + j_1b = k_2a + j_2b$ with $k_1 > k_2 \Rightarrow (k_1-k_2)a = (j_2-j_1)b$. As, $\gcd(a,b) = 1$, $a|j_2 - j_1$ but $0 \le j_2 \le a-1, 0 \le j_1 \le a-1$ and $j_2 > j_1 \Rightarrow j_2 = j_1 \Rightarrow k_2 = k_1$. Therefore, no two powers of t are same in the expression (3) which implies, $a_{ij} = 0, \forall\ ij \Rightarrow r_i(x) = 0, 0 \le i \le a-1 \Rightarrow f(x,y) = (y^a - x^b)g(x,y) \Rightarrow f(x,y) \in \langle y^b - x^a\rangle$. Again, $\theta(y^b - x^a) = t^{ab} - t^{ab} = 0 \Rightarrow y^b - x^a \in \ker\theta \Rightarrow \ker\theta = \langle y^b - x^a\rangle$. □

Exercise 13.12.

$$\begin{aligned} K[x_1, x_2, \cdots, x_n] &\xrightarrow{\theta} K[t] \\ x_1 &\mapsto t \\ x_2 &\mapsto t^{a_2} \\ &\vdots \\ x_n &\mapsto t^{a_n} \end{aligned}$$

Find $\operatorname{Ker}\theta$.

Exercise 13.13. *Let X be a compact Hausdroff space. Maximal ideals of $C(X) := \{f : X \to \mathbb{R} : f \text{ is continuous}\}$ is the set $\Sigma = \{m_c : c \in X\}$ where $m_c = \{f \in C(X) : f(c) = 0\}$.*

Proof. At first we show that m_c is a maximal ideal for each $c \in X$. We fix $c \in X$ and consider the map

$$\begin{aligned} C(X) &\xrightarrow{\theta_c} \mathbb{R} \\ f &\mapsto f(c) \end{aligned}$$

Clearly, θ_c is surjective as for any $a \in \mathbb{R}$ take constant map $f(x) = a, \forall\ x \in X$ then $\theta_c(f) = a$ and $\ker\theta_c = m_c$ (by definition of θ_c) therefore, $C(X)/m_c \cong \mathbb{R}$ which imply m_c is a maximal ideal. Let $m \in \operatorname{maxspec} C(X)$ and suppose, $m \neq m_c, \forall\ c \in X$. the for each $c \in X, \exists\ f_c \in m$ such that $f_c(x) \neq 0$. Since, f_c is continuous there exists an open set $U_c \subseteq X$ such that $f_c(U_c) \neq 0$ and $X \subseteq \bigcup_{c\in X} U_c$, since X is compact, $\exists\ c_1, \cdots c_n \in X$ such that $X \subseteq \bigcup_{i=1}^{n} U_{c_i}$. Now, consider the function $f = f_{c_i}^2 + \cdots f_{c_n}^2$ and ley $y \in X \subseteq \bigcup_{i=1}^{n} U_{c_i}$ then $y \in U_{c_i}$ for some i which imply $f_{c_i}(y) \neq 0 \Rightarrow f(y) \neq 0$. Since $y \in X$ is arbitrary, $f(y) \neq 0, \forall\ y \in X$ and $1/f$ is unit and $f \in m$ as $f_{c_i} \in m$ which is a contradiction. Therefore, $m = m_x$ for some $c \in X$.

Observation.

$$\begin{aligned} X &\xrightarrow{\phi} \operatorname{maxspec} C(X) \\ c &\mapsto m_c \end{aligned}$$

We show that ϕ is a bijection. We already showed ϕ is surjective. Suppose, $x \neq y$, X is compact, Hausdorff therefore, X is normal. By Uryshon lemma $\exists\ f, g \in C(X)$ such that $f(x) = 0, f(y) = 1$ and $g(x) = 1, g(y) = 0 \Rightarrow m_x \neq m_y$.

□

Exercise 13.14. *Let $a = (a_1, \cdots, a_n) \in \mathbb{C}^n$ and $m_a = \langle x_1 - a_1, \cdots, x_n - a_n\rangle$. Show that m_a is a maximal ideal of $\mathbb{C}[x_1, \cdots, x_n]$.*

Proof.

$$\begin{aligned} \mathbb{C}[x_1, \cdots, x_n] &\xrightarrow{\theta} \mathbb{C} \\ f(x_1, \cdots, x_n) &\mapsto f(a_1, \cdots, a_n) \end{aligned}$$

By Taylor's theorem

$$f(x_1,\cdots,x_n)=f(a_1,\cdots,a_n)+\frac{1}{1!}\left[\sum_{i=1}^{n}(x_i-a_i)\frac{\partial f}{\partial x_i}(a_1,\cdots,a_n)\right]$$
$$+\frac{1}{2!}\left[\sum_{1\le i,j\le n}(x_i-a_i)(x_j-a_j)\frac{\partial^2 f}{\partial x_i\partial x_j}(a_1,\cdots,a_n)\right]+\cdots$$

Now, if $f\in\ker\theta\Rightarrow f(a_1,\cdots,a_n)=0$, therefore,

$$f(x_1,\cdots,x_n)=0+\frac{1}{1!}\left[\sum_{i=1}^{n}(x_i-a_i)\frac{\partial f}{\partial x_i}(a_1,\cdots,a_n)\right]$$
$$+\frac{1}{2!}\left[\sum_{1\le i,j\le n}(x_i-a_i)(x_j-a_j)\frac{\partial^2 f}{\partial x_i\partial x_j}(a_1,\cdots,a_n)\right]+\cdots\in\langle x_1-a_1,\cdots,x_n-a_n\rangle$$

Hence, $\ker\theta\subseteq m_a$. Since, $x_i-a_i\in\ker\theta\Rightarrow m_a\in\ker\theta\Rightarrow m_a=\ker\theta$.
Let $p\in\mathbb{C}$ then $\theta(x_1-a_1+p)=p\Rightarrow\theta$ is surjective thus

$$\mathbb{C}[x_1,\cdots,x_n]/m_a\cong\mathbb{C}$$

so, m_a is a maximal ideal. □

Remark. *Converse of the theorem (for $\mathbb{C}$) is also true i.e., any maximal ideal of $\mathbb{C}[x_1,\cdots,x_n]$ is of the form m_a for some $a\in\mathbb{C}^n$.*

Remark. *Converse of the theorem is not true for $\mathbb{R}$ (a non algebraically closed field).*

Example. *$\langle x^2+1\rangle\subseteq\mathbb{R}[x]$ is maximal ideal but not of the form $\langle x-c\rangle$ for some $c\in\mathbb{R}$.*

Exercise 13.15. *Let R be an integral domain then so $R[x]$.*

Proof. Let $f(x)=a_0+\cdots+a_nx^n; a_i\in R, 0\le i\le n$ where $a_n\neq 0$. Suppose, $g(x)=b_0+\cdots+b_mx^m$ be the least degree polynomial such that $f(x)g(x)=0$ (where $f(x),g(x)\neq 0$) then we have

$$a_0b_0+a_nb_mx^{m+n}=0$$

comparing the coefficient from both side of the equation, $a_nb_m=0$ but $a_n,b_m\neq 0$ then we get a contradiction as R is assumed to be an integral domain. □

Exercise 13.16. *Suppose, R is a commutative ring with identity and $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$ then f is an unit of $R[x]$ iff a_0 is unit and $a_1,\cdots,a_n$ are nilpotent. f is nilpotent iff all of $a_i's$ are nilpotent.*

Proof. Let us consider the homomorphism

$$R[x]\xrightarrow{\theta}R/P[x]$$
$$a_0+\cdots+a_nx^n\mapsto(a_0+P)+\cdots+(a_n+P)x^n$$

Suppose, $f\in R[x]$ is a unit then $\theta(f)$ is unit in $R/P[x]$ and as R/P is integral domain, $R/P[x]$ is also integral domain hence, $\theta(f)\in R/P$ [units of $R[x]$ = units of R if R is an integral domain]. Thus, $(a_0+P)+\cdots+(a_n+P)x^n\in R/P\Rightarrow a_i+P=0+P; 1\le i\le n\Rightarrow a_i\in P$. Since, P is

chosen arbitrarily, $a_i \in \bigcap_{P \in \operatorname{spec} R} P = \sqrt{0}; 1 \leq i \leq n$. Therefore, $a_1, \cdots, a_n$ are nilpotent. As f is unit there exists $g \in R[x]$ such that $fg = 1$. Comparing the coefficient we have $a_0 b_0 = 1 \Rightarrow a_0$ is unit. Conversely, if a_0 is a unit and $a_1, \cdots, a_n$ are nilpotent then $a_0 + a_1 x + \cdots + a_n x^n$ is an unit.

Now, suppose, $f(x)$ is nilpotent. As R/P is integral domain, $a_i + P = 0 + P; 0 \leq i \leq n$ then $a_i \in \sqrt{0}$ for all i so that all a_i's are nilpotent. Conversely, if $a_0, \cdots, a_n$ is nilpotent then $a_0 + a_1 x + \cdots + a_n x^n$ is nilpotent i.e., $f(x)$ is nilpotent. □

Proposition 13.17. *If R is an integral domain and $f(x) \in R[x]$ is an unit then $f \in R$.*

Proof. Let $f(x) = a_0 + \cdots + a_n x^n; n \geq 1$ and $g(x) = b_0 + \cdots + b_m x^m$ (least degree) and $fg = 1$. Thus, $(a_0 + \cdots + a_n x^n)(b_0 + \cdots + b_m x^m) = 1 \Rightarrow a_n b_m = 0$. Since $n \geq 1, a_n \neq a_0$. Therefore, $a_n b_m = 0 \Rightarrow a_n = 0$ or $b_m = 0$ which is a contradiction. So, $n = 0$ i.e., $f \in R$. □

Exercise 13.18. $K[[x]] = \left\{ \sum_{i=0}^{\infty} a_i x^i : a \in K \right\}$ *is ring of formal power series, where*

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

and

$$\left(\sum_{i=0}^{\infty} a_i x^i \right) \left(\sum_{i=0}^{\infty} b_i x^i \right) = \left(\sum_{i=0}^{\infty} c_i x^i \right) \quad \text{where } c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

Show that $K[[x]]$ is a ring, $K[x] \subseteq K[[x]]$. Find $\operatorname{maxspec} K[[x]]$.

$$K[[x, x^{-1}]] = \left\{ \sum_{i=-\infty}^{\infty} a_i x^i : a_i \in K \right\}$$

is ring of Laurent series where addition and multiplication are similar as formal power series ring.

Exercise 13.19. *Let K be a field, $\phi : K[x \to K[x]$ is an automorphism then $\phi(x) = \lambda x + \mu, \lambda \in K^*, \mu \in K$.*

Observation 13.20. *If $\operatorname{char} R = p > 0$ (p is prime) then the map $\phi : R \to R$ defined by $\phi(x) = x^p$ is a homomorphism. Also note that $p | \binom{p^n}{i}, 1 \leq i \leq p^n - 1, n \in \mathbb{N}$.*

Proof. Let $a, b \in R$ then $\phi(a + b) = (a + b)^p = \sum_{i=1}^{p} \binom{p}{i} a^{p-i} b^i$ where $p | \binom{p}{i}, 1 \leq i \leq p - 1$ then $\phi(a + b) = a^p + b^p = \phi(a) + \phi(b)$. Clearly $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b), \phi(1) = 1$ and $\phi(0) = 0$ thus ϕ is an ring homomorphism.

Exercise 13.21. *Is ϕ injective?*

Ans. No in general as consider the ring $R = \mathbb{Z}/p\mathbb{Z}[x]/\langle x \rangle^p$ then $\phi(\bar{x}) = 0$ so kernel is not trivial.

Exercise 13.22. *Let* $\operatorname{Char} K = p > 0$ *and* K *is a field. Choose* $r \geq 2$ *such that* $p \nmid r$. *Define,*

$$\begin{aligned} \phi : K[x,y] &\to K[t] \\ x &\mapsto -t - t^{rp} \\ y &\mapsto t^{p^2} \end{aligned}$$

Find $\operatorname{Ker}\phi$ *and show that* ϕ *is surjective.*

Proof. The map

$$\begin{aligned} \phi : K[x,y] &\to K[t] \\ x &\mapsto -t - t^{rp} \\ y &\mapsto t^{p^2} \end{aligned}$$

Then $\phi(x^p) = (-1)(t + r^{rp})^p = -(t^p + t^{rp^2})$ and $\phi(y^r) = t^{rp^2} \Rightarrow \phi(y^r + x^p) = -t^p \Rightarrow \phi(y^r + x^p)^r = -t^{pr}$. Now, $\phi(-x + (y^r + x^p)^r) = -\phi(x) + \phi(y^r + x^p)^r = t - t^{rp} - t^{pr} = t$. So, ϕ is surjective. And $\phi(x^r + y^p)^p = -t^{p^2} = -\phi(y) \Rightarrow \phi(y + (x^r + y^p)^p) = 0$.

Exercise 13.23. *Let* F *be a field of characteristic* $p > 0$. *Is* $\phi : F \to F$ *defined by* $x \mapsto x^p$ *surjective?*

Exercise 13.24. *Give an example of countably infinite field with finite characteristic.*

Ans. We know that $K = \mathbb{Z}/p\mathbb{Z}(x)$ is a field with $\operatorname{char} R = p$. Note that if a ring is countable then its fraction ring is also countable. So its enough to show that $\mathbb{Z}/p\mathbb{Z}[x]$ is countably infinite. Clearly, $\mathbb{Z}/p\mathbb{Z}[x]$ is a vector space over $\mathbb{Z}/p\mathbb{Z}$ and basis is $\{1, x, \cdots, x^n : n \in \mathbb{N}\}$ so cardinality of $\mathbb{Z}/p\mathbb{Z}[x]$ is $p \times \aleph = \aleph$.

Exercise 13.25. $(15\mathbb{Z} : 6\mathbb{Z}) = ?$

Ans Recall that $(I : J) = \{x \in R : xJ \subseteq I\}$ then by definition of colon ideal $(15\mathbb{Z} : 6\mathbb{Z}) = \{x \in \mathbb{Z} : (6x) \subseteq (15)\} = \{x \in \mathbb{Z} : 6x = 15y\} = \{x \in \mathbb{Z} : 2x = 5y\} = \{x \in \mathbb{Z} : x = 5\lambda\} = 5\mathbb{Z}$.

Exercise 13.26. *Are* $\mathbb{R}$ *and* $\mathbb{C}$ *isomorphic as ring?*

Exercise 13.27. *Are* $\mathbb{Q}$ *and* $\mathbb{Z}$ *isomorphic as ring?*

Exercise 13.28. *Is* $(\mathbb{R}^2, +) \cong (\mathbb{R}, +)$?

Exercise 13.29. *Show that* $\langle 2, x\rangle$ *is a maximal ideal in* $\mathbb{Z}[x]$.

Exercise 13.30. $\dfrac{\mathbb{Z}[x]}{\langle n, x\rangle} \cong \mathbb{Z}/n\mathbb{Z}$

Exercise 13.31. R *is a ring. Assume that every prime ideal is finitely generated then every ideal is finitely generated.*

Exercise 13.32.

See **Appendix I** for more exercise on ring theory.

14. Module Theory

14.1. **Introduction. Motivation for Module theory:** Why should we study module theory? One can say that while defining vector space, we take a non-empty abelian group V and a field K and define something called scalar multiplication $\cdot : K \times V \to V$ by $(\alpha, v) \mapsto \alpha \cdot v$ which follow some properties which we are not listed here. So one can think we can replace field and instead of field what happened if we take a ring not necessarily commutative and not necessarily having multiplicative identity. The result turns out to be a motivation for the study of module theory but we do something apart form this. So we first prove this theorem analogous to Cayley's theorem in group theory. Before this we construct a ring from an abelian group which is pretty much obvious and easy to do.

Let $(M, +)$ be an abelian group and $End\ (M) := \{\phi : M \to M : \phi \text{ is a group homomorphism}\}$. Now we define addition and multiplication in this that $(End\ (M), +, \cdot)$ is a ring. Define addition on $End\ (M)$ as

$$+ : End\ (M) \times End\ (M) \to End\ (M)$$
$$(\phi, \psi) \mapsto (\phi + \psi)$$

now, $(\phi + \psi)(m) = \phi(m) + \phi(m), \forall\ m \in M$ then check that $(End\ (M), +)$ is a group. Now, define multiplication as mapping composition i.e., $\phi, \psi \in End\ (M)$ and $(\phi) \cdot (\psi) = \phi \circ \psi$, check that $(End\ (M), +, \cdot)$ is ring with unity as identity function.

Theorem 14.1. *Let R be a ring then R is isomorphic to a subring of an endomorphism ring of an abelian group.*

Proof. As R is a ring, $(R, +)$ is an abelian group then $(End\ (R), +, \cdot)$ is a ring. Now define

$$R \xrightarrow{\phi} End\ (R)$$
$$a \mapsto \tau_a$$

where $\tau_a : R \to R$ defined by $\tau_a(x) = ax$. As, τ_a is a group homomorphism, $\tau_1 \in End\ (R)$. Now, $\tau_{a+b}(x) = (a + b)x = ax + bx = \tau_a(x) + \tau_b(x) = (\tau_a + \tau_b)(x), \forall\ x \in R$ then $\tau_{a+b} = \tau_a + \tau_b$ and $\tau_{ab}(x) = abx = a\tau_b(x) = (\tau_a)(\tau_b)(x), \forall\ x \in R$ hence, $\tau_{ab} = \tau_a \circ \tau_b$. Now, we show that ϕ is an injective ring homomorphism. let $a, b \in R$ then $\phi(a + b) = \tau_{a+b} = \tau_a + \tau_b = \phi(a) + \phi(b)$ and $\phi(ab) = \tau_{ab} = \tau_a\tau_b = \phi(a)\phi(b)$ and $\phi(1) = \tau_1 = id_R$. Therefore, ϕ is a ring homomorhism. Let $\phi(a) = \phi(b) \Rightarrow \tau_a = \tau_b \Rightarrow ax = bx$, in particularly if $x = 1$ then $a = b$ so ϕ is injective. □

Let R be a ring and $(M, +)$ is an abelian group. Suppose that there is a ring morphism $\phi : R \to End\ (M)$ such that

(1) $\phi(a)(m+n) = \phi(a)(m)+\phi(a)(n), \forall\ a \in R$ and $\forall\ m, n \in M$ as $\phi(a) : M \to M$ is a morphism,
(2) $\phi(a + b) = \phi(a) + \phi(b) \Rightarrow \phi(a + b)(m) = \phi(a)m + \phi(b)m, \forall\ a, b \in R$ and $\forall\ m \in M$,
(3) $\phi(ab) = \phi(a)\phi(b) \Rightarrow \phi(ab)(m) = \phi(a)[\phi(b) \cdot (m)], \forall\ m \in M$,
(4) If R has unity then $\phi(1) = 1$ which is identity map and $\phi(1)m = m, \forall\ m \in M$.

Definition 14.2. *Let $(M, +)$ be an abelian group and R be an ring. Define, $\cdot : R \times M \to M$ by $(r, m) \mapsto rm$ be a map called scalar multiplication. M is said to be an left $R-$module if it satisfies*

the following properties:
1) $(r+s)m = rm + sm \ \forall r, s \in R$ *and* $\forall m \in M$
2) $r(m+n) = rm + rn \ \forall r \in R$ *and* $\forall m, n \in M$
3) $(rs)m = r(sm) \ \forall r, s \in R$ *and* $\forall m \in M$
If R *has identity element then* $1_R m = m \ \forall m \in M$*, then* M *is said to be unitary module. If* M *is defined over an division ring then* M *is said to be a vector space over* R*.*

Definition 14.3. *Let* M *be an* $R-$*module.* $N \subseteq M$ *be a subgroup of* M *and* $\cdot|_{R\times N} : R \times N \to N$ *with* $(N, \cdot|_{R\times N})$ *satisfies the module property.*

Theorem 14.4. *Let* M *be an* $R-$*module and* $N \subseteq M$*.* N *is submodule iff,*
1) $n_1, n_2 \in N \Rightarrow n_1 + n_2 \in N$
2) $r \cdot n \in N \ \forall r \in R$ *and* $\forall n \in N$*.*

Proof. Obvious. □

Note 14.5. *Note that if* R *is module over itself, then submodules of* R *are precisely the ideals of* R*. Now, suppose* S *is an* $R-$*algebra. If* $f : R \to S$ *is surjective then the submodules of* S *are the precisely the ideals of* S*. To see this, let* N *be an submodule of* S*. Then for any* $n \in N$ *and for any* $r \in R$*,* $r \cdot n := f(r)n \in N$*. Then* N *is an ideal of* S *as for any* $s \in S$ *there exists* $r \in R$ *such that* $f(r) = s$ *then* $r \cdot n = f(r)n = sn \in N$*.*

Example 14.6. *Take* $R = \mathbb{Z}$ *and* $S = \mathbb{Q}$ *and* $i : \mathbb{Z} \to \mathbb{Q}$ *be the inclusion map.* $2\mathbb{Z}$ *is an submodule of* $\mathbb{Q}$ *but not an ideal of* $\mathbb{Q}$*.*

Let M be an $R-$module and $A \subseteq M$, the intersection of all submodule containing A is the smallest submodule containing A. We say that the submodule generated by A and denotes by $\langle A\rangle$. Let

$$LC(A) := \{r_1a_1 + \cdots + r_na_n : r_i \in R, a_i \in A\}$$

then show that

(1) $LC(A)$ is a submodule of M,
(2) $A \subseteq LC(A)$,
(3) $\langle a\rangle = LC(A)$.

Special case If $|A| < \infty$ then we say $\langle A\rangle$ is finitely generated i.e., if $A = \{a_1, \cdots, a_n\}$ then $\langle A\rangle := \{r_1a_1 + \cdots + r_na_n : r_i \in R, a_i \in A\}$
Notation. $\langle A\rangle = Ra_1 + \cdots + Ra_n$.

Definition 14.7. *Let* R *be an commutative ring with identity and* M *be an* $R-$*module,* $I \subseteq R$ *be ann ideal of* R*.*

$$IM := \left\{ \sum_{\substack{finite \\ sum}} a_i m_i : a_i \in I, m_i \in M \right\}$$

then IM *is an* $R-$*module and* $IM \subseteq M$*.*

Let $\sum_{\substack{\text{finite}\\\text{sum}}} a_i m_i, \sum_{\substack{\text{finite}\\\text{sum}}} b_j m'_j \in IM$ where $a_i, b_j \in I$ and $m_i, m'_j \in M$ then $\sum_{\substack{\text{finite}\\\text{sum}}} a_i m_i + \sum_{\substack{\text{finite}\\\text{sum}}} b_j m'_j = \sum_{\substack{\text{finite}\\\text{sum}}} c_j m''_j \in IM$ and $r \in R$ and $\sum_{\substack{\text{finite}\\\text{sum}}} a_i m_i \in IM \Rightarrow \sum_{\substack{\text{finite}\\\text{sum}}} (ra_i) m_i \in IM$ as $ra_i \in I$ as I is an ideal, therefore, IM is an $R-$module.

Definition 14.8. *Let M, N be $R-$modules. $f : M \to N$ is said to be module homomorphism if*
1) $f(m_1 + m_2) = f(m_1) + f(m_2)\ \forall m_1, m_2 \in M$
2) $f(rm) = rf(m)\ \forall r \in R$ and $\forall m \in M$.

We define $\operatorname{Ker} f = \{m \in M |\ f(m) = 0\}$. Note that f is injective iff $\operatorname{Ker} f = \{0\}$. Suppose f is injective. We know that $f(0) = 0$ so $\operatorname{Ker} f = \{0\}$. Conversely, $\operatorname{Ker} f = \{0\}$. Now, $f(x) = f(y) \Rightarrow f(x - y) = 0 \Rightarrow x - y \in \operatorname{Ker} f = \{0\} \Rightarrow x = y$ hence f is injective. If $f : M \to N$ be an $R-$module homomorphism then $\ker f$ is submodule of M and $\operatorname{Im} f$ is submodule of N.

We define

$$\operatorname{Hom}_R(M, N) := \{f : M \to N : f \text{ is a } R-\text{module homomorphism}\}$$

Note that,

$$\cdot : R \times \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(M, N)$$

defined by $(r, f) \mapsto rf$ where $(rf)(m) = r \cdot (f(m))\ \forall m \in M$. Then it is easy to check that $\operatorname{Hom}_R(M, N)$ is a left $R-$*module.*

Remark. *Let $N \subseteq M$ be a submodule then N is kernel of some $R-$module homomorphism for some suitable $R-$module.*

Definition 14.9. *A module homomorphism $f : M \to N$ is said to be an isomorphism if $\exists\ g : N \to M$ module homomorphism such that $f \circ g = id_N$ and $g \circ f = id_M$*

Note that $f : M \to N$ be a module homomorphism is isomorphism iff f is bijective.

Proof. ($\Rightarrow$) Obvious.
($\Leftarrow$) Suppose, f is bijective then $\exists\ g : N \to M$ such that $f \circ g = id_N$ and $g \circ f = id_M$. We need to check that g is a module homomorphism. Let $n_1, n_2 \in N$. $(f \circ g)(n_1 + n_2) = n_1 + n_2 = (f \circ g)(n_1) + (f \circ g)(n_2) \Rightarrow f[g(n_1 + n_2) - g(n_1) - g(n_2)] = 0$ (since f is a homomorphism). As f is bijective f is injective also so $g(n_1 + n_2) = g(n_1) + g(n_2)$. Again let $r \in R$ and $n \in N$. $f(g(rn)) = rn = rf(g(n)) = f(rg(n)) \Rightarrow f[g(rn) - rg(n)] = 0$ this implies $g(rn) = rg(n)$. Hence g is a module homomorphism. □

Notation: If M, N be $R-$*modules*. If M and N are isomorphic then $M \simeq N$

Theorem 14.10. *Show that* $\operatorname{Hom}_R(R, M) \simeq M$

Proof. Define, $\theta : \operatorname{Hom}_R(R, M) \to M$ by $\theta(f) = f(1)$. $\theta(f_1 + f_2) = (f_1 + f_2)(1) = f_1(1) + f_2(1) = \theta(f_1) + \theta(f_2)$. Now, $\operatorname{Ker} f = \{f \mid \theta(f) = 0\} \Rightarrow \operatorname{Ker} f = \{f \mid f(1) = 0\}$. Let $r \in R \Rightarrow f(r) = rf(1) = 0$ $\Rightarrow f \equiv 0 \Rightarrow \theta$ is injective. Let $m \in M$. We consider the map $f \in \operatorname{Hom}_R(R, M)$ such that $f(r) = rm$

(check that f is a module homomorphism) $\Rightarrow f(1) = m = \theta(f)$ hence, θ is surjective. Then θ is an isomorphism. Therefore, $\mathrm{Hom}_R(R, M) \simeq M$. □

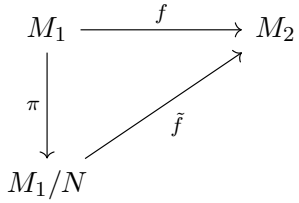
14.2. **Quotient Module.** Let $N \subseteq M$ be a submodule. Consider the quotient group $(M/N, +)$ and the scalar multiplication map

$$\cdot : R \times M/N \to M/N$$
$$(r, x + N) \mapsto (rx + N)$$

Claim: '$\cdot$' is well defined. Let $x+N = y+N \Rightarrow x-y \in N \Rightarrow r(x-y) \in N \Rightarrow rx+N = ry+N$, hence '$\cdot$' is well defined. Check that M/N is an $R-$module. Let $\pi : M \to M/N$ defined by $\pi(x) = x + N$ is a surjective homomorphism whose kernel is N.

14.2.1. *Isomorphism theorems for module.*

Theorem 14.11 (First isomorphism theorem)**.** *Let M_1, M_2 be two $R-$modules and $f : M_1 \to M_2$ be $R-$module homomorphism. Suppose, $N \subseteq \mathrm{Ker}\, f$ be a submodule of M_1 then there exists an unique $R-$module homomorphism $\tilde{f} : M_1/N \to M_2$ such that the diagram commutes i.e., $f = \tilde{f} \circ \pi$.*



Moreover, if $I = \mathrm{Ker}\, f$ then $\tilde{f}$ is injective hence $M_1/\mathrm{Ker}\, f \cong \mathrm{Im}\, f$. If $\tilde{f}$ is surjective then f is also surjective then $M_1/\mathrm{Ker}\, f \cong M_2$.

Proof. Define, $\tilde{f} : M_1/N \to M_2$ by $(x + N) \mapsto f(x)$. Claim: $\tilde{f}$ is well defined. Let, $x + N = y + N$ $\Rightarrow x - y \in N \subseteq \mathrm{Ker}\, f \Rightarrow f(x - y) = 0 \Rightarrow f(x) = f(y) \Rightarrow \tilde{f}(x + N) = \tilde{f}(y + N)$. Therefore $\tilde{f}$ is well-defined. $[\tilde{f}(x + y + N) = f(x + y) \Rightarrow f(x) + f(y)$ (as f is a ring homomorphism) $\Rightarrow \tilde{f}(x + y + N) = \tilde{f}(x + N) + \tilde{f}(y + N)$ and $\tilde{f}(xy + N) = f(xy) = f(x)f(y) = \tilde{f}(x + N)\tilde{f}(y + N)$ so, $\tilde{f}$ is a ring homomorphism.] Uniqueness: Suppose g is another ring homomorphism such that $g : M_1/N \to M_2$ such that $g \circ \pi = f$. Then $f(x) = g \circ \pi(x) \Rightarrow \tilde{f}(x + N) = f(x) = g(x + N)$ so we have $g = \tilde{f}$. Therefore $\tilde{f}$ is unique. Now suppose $N = \mathrm{Ker}\, f$ and let $x + N \in \mathrm{Ker}\, \tilde{f} \Rightarrow$ $\tilde{f}(x + N) = 0 = f(x) \Rightarrow x \in \mathrm{Ker}\, f \Rightarrow x + N = x + \mathrm{Ker}\, f = 0$ [as $N = \mathrm{Ker}\, f$] so $\tilde{f}$ is injective. Therefore, $M_1/\mathrm{Ker}\, f \cong \mathrm{Im}\, \tilde{f} = \mathrm{Im}\, f$ (by definition $\mathrm{Im}\, \tilde{f} = \mathrm{Im}\, f$). If $\tilde{f}$ is surjective then so f hence $M_2 = \mathrm{Im}\, \tilde{f} = \mathrm{Im}\, f$. Therefore, $M_1/\mathrm{Ker}\, f \cong M_2$. □

Observation. $\dfrac{M + N}{N} \cong \dfrac{M}{N \cap M}$

Proof.

$$M \overset{i}{\hookrightarrow} M + N \overset{\pi}{\to} \frac{M + N}{N}$$
$$x \mapsto x + 0 \mapsto x + N$$

therefore $f = \pi \circ i$, let $x \in \operatorname{Ker} f \subseteq M \Leftrightarrow x + N = 0 \Leftrightarrow x \in N \Leftrightarrow x \in M \cap N$ hence $\dfrac{M}{M \cap N} \hookrightarrow \dfrac{M+N}{N}$. Let $m+n \in M+N$ then $(m+n)+N = m+N \Rightarrow f(m) = m+N = (m+n)+N$ gives the surjectivity of f hence we get our desire result.

Observation. Suppose $P \subseteq N \subseteq M$ then $N/P = \{x+P : x \in N\}$ is a submodule of M/P. Show that $\dfrac{M/P}{N/P} \cong \dfrac{M}{N}$. Define $f : M/P \to M/N$ by $(x+P) \mapsto (x+N)$ therefore, f is well defined by first isomorphism theorem. $\operatorname{Ker} f = \{x+P : f(x+P) = 0+N\} = \{x+P : x+N = 0+N\} = N/P$ as f is surjective we have $\dfrac{M/P}{N/P} \cong \dfrac{M}{N}$.

14.3. **Chinese remainder theorem.** Let M be an $R-$ module and I, J be two ideals of R. Recall that IM is a submodule of M. Now we consider the map

$$\begin{aligned}\theta : M &\to M/IM \times M/JM \\ m &\mapsto (m + IM, m + JM)\end{aligned}$$

then it is easy to show that θ is a $R-$module morphism.

$$\ker\theta = \{m \in M : \theta(m) = (0 + IM, 0 + JM)\} = IM \cap JM.$$

In general, $(I \cap J)M \subseteq IM \cap JM$ as $I \cap J \subseteq I \Rightarrow (I \cap J)M \subseteq IM$ similarly, $(I \cap J)M \subseteq JM$ hence $(I \cap J)M \subseteq IM \cap JM$.

Question 14.12. *Find an example where* $(I \cap J)M \neq IM \cap JM$.

Now back to our discussion, we assume that I, J are comaximal, i.e, $I + J = 1$. Then what we can show that the θ described above is surjective as well as $(I \cap J)M = IM \cap JM$ and we show this one by one. Since $I + J = 1 \Rightarrow x + y = 1, x \in I, y \in J$. Let $(m_1 + IM, m_2 + JM) \in M/IM \times M/JM$

$$\begin{aligned}m_2x + m_1y - m_1 &= m_2x + m_1(y - 1) \\ &= m_2x - m_1x \in IM \\ (m_2x + m_1y) + IM &= m_1 + IM\end{aligned}$$

Similarly,

$$\begin{aligned}m_2x + m_1y - m_2 &= m_2(x - 1) + m_1y \\ &= m_1 - m_2y \in JM \\ (m_2x + m_1y) + JM &= m_2 + JM\end{aligned}$$

Therefore, $\theta(m_2x + m_1y) = (m_1 + IM, m_2 + JM)$ which proves that θ is surjective. By first isomorphism theorem

$$M/(IM \cap JM) \cong M/IM \times M/JM.$$

As we assume I, J are comaximal, let $m \in IM \cap JM$ then

$$m = 1 \cdot m = (x + y)m, \qquad x + y = 1, x \in I, y \in J.$$

Thereofore, $m \in JM, x \in I \Rightarrow xm \in (IJ)M$. Similarly, $m \in IM, y \in J \Rightarrow ym \in (IJ)M \Rightarrow m \in (IJ)M$. Now

$$(IJ)M \subseteq (I \cap J)M \subseteq IM \cap JM \subseteq (IJ)M.$$

Thus if I and J are comaximal we have $(IJ)M = (I \cap J)M = IM \cap JM$.

Let V be a vector space over a field F and $T : V \to V$ be a linear operator. Let $p = p_1^{r_1} \cdots p_k^{r_k}$ be the minimal polynomial of T. Now V is an $F[x]$ module via T. Clearly, (p) is an ideal of $F[x]$ and $(p)V$ is a subspace of V. Then

$$V/(p)V = V/(p_1^{r_1} \cdots p_k^{r_k})V = V/(p_1^{r_1})V \cdots (p_k^{r_k})V \cong V/(p_1^{r_1})V \times \cdots \times V/(p_k^{r_k})V.$$

14.4. **Module Structure.**

(1) Let R, S be two rings and $f : R \to S$ be a ring homomorphism (i.e., S is a R algebra). If M is an $S-$module then M is an $R-$module (via f) as,

$$\cdot : R \times M \to M$$

where $(r, m) \mapsto f(r)m$ be the scalar multiplication map.

(2) If S is a $R-$algebra then scalar multiplication map defined by $\cdot : R \times S \to S$, $\cdot(r, s) = f(r)s$ which makes S is an $R-$module.

(3) Let $T : V \to V$ be a linear operator on a vector space V over a field K then V is a $K[x]$ module via

$$K[x] \times V \to V$$
$$(f(x), v) \mapsto f(T)v$$

(4) Let R be a commutative ring and M be a left $R-$module. Define,

$$\cdot : M \times R \to M$$
$$(m, r) \mapsto m \cdot r := rm$$

where rm is usual left scalar multiplication. Check that M is a right $R-$module.

Definition 14.13. *Let M be an $R-$module we define,*

$$\operatorname{Ann}_R M = \{r \in R : rm = 0 \text{ for all } m \in M\}$$

is an ideal of R. An $R-$module M is said to be faithful $R-$module if $\operatorname{Ann} M = 0$.

Let $r_1, r_2 \in \operatorname{Ann} M \Rightarrow r_1 m = 0 = r_2 m$ for all $m \in M \Rightarrow (r_1 + r_2)m = 0$ for all $= m \in M \Rightarrow r_1 + r_2 \in \operatorname{Ann} M$. Similarly let $r \in R$ and $r_1 \in \operatorname{Ann} M$ then $r(r_1 m) = r \cdot m = 0$ for all $m \in M$ then $rr_1 \in \operatorname{Ann} M$. Therefore, $\operatorname{Ann} M$ is an ideal of R.

Problem 14.14. *Let V be a vector space over a field K and let $T : V \to V$ be a linear operator, then V is a $K[x]$ module via T. Show that V is not faithful $K[x]$ module i.e.,* $\operatorname{Ann} V \neq 0$

Ans. By Cayley-Hamilton theorem.

Exercise 14.15. *Let,*

$$\pi : R \to R/Ann\ M$$

be the projection map. Show that M is a faithful $R/Ann\ M$ module.

Ans. Define the scalar multiplication map

$$\cdot : R/Ann\ M \times M \to M$$

by $(r + Ann\ M, m) \mapsto rm$. Claim: '$\cdot$' is well defined, Let $r_1 + Ann\ M = r_2 + Ann\ M \Rightarrow r_1 - r_2 \in Ann\ M \Rightarrow (r_1 - r_2)m = 0$ for all $m \in M$ then $r_1 m = r_2 m$ hence $\cdot$ is well defined. Now,

$$Ann_{(R/Ann\ M)} M = \{r + Ann\ M : (r + Ann\ M)m = 0 \text{ for all } m \in M\}$$

Let $r + Ann\ M \in Ann_{R/Ann\ M} M \Rightarrow rm = 0$ for all $m \in M \Rightarrow r \in Ann\ M \Rightarrow r + Ann\ M = 0 + Ann\ M$ in $R/Ann\ M$ this implies M is a faithful $R/Ann\ M$ module.

Question 14.16. *Let R, S be two rings and S is an $R-$algebra. Let M be an $R-$module then under what condition M is a $S-$module ?*

Observation 14.17. *Let $f : R \to S$ be a surjective ring homomorphism and* $\text{Ker} \subseteq Ann_R M$ *then if M is a $R-$module then M is an $S-$module.*

Proof. Define

$$\cdot : S \times M \to M$$
$$(s, m) \mapsto f(r)m$$

and suppose, s has two pre image i.e., $s = f(r_1) = f(r_2) \Rightarrow f(r_1 - r_2) = 0 \Rightarrow r_1 - r_2 \in \text{Ker}\, f \subseteq Ann_R M \Rightarrow (r_1 - r_2)m = 0$ for all $m \in M \Rightarrow r_1 m = r_2 m$ i.e., the map is well defined. □

14.5. **Nakayama Lemma.**

Definition 14.18. *Let M be an $R-$module. S be a subset of M. We say that S is a generating set for M if any $m \in M$ can be written as finite R linear combination of elements in S that is there exist $\{s_1, \cdots, s_r\} \subseteq S$ such that for any $m \in M$ can be written as $m = \sum_{i=1}^{r} r_i s_i$ where $r_i \in R, 1 \leq i \leq r$.*

Notation. $M = \langle S \rangle$.

Remark 14.19. *Suppose M and N be $R-$Modules and $f : M \to N$ be an epimorphism. If S is a generating set of M then $f(S)$ is also generating set of N.*

Definition 14.20. *Let $S \subseteq M$ be a generating set of M. S is said to be minimal generating set if any proper subset of S doesn't generate M.*

Note that $S_1 = \langle 1 \rangle = \mathbb{Z}$ and $S_2 = \langle 3, 5 \rangle = \mathbb{Z}$ but $|S_1| \neq |S_2|$ i.e, cardinality of minimal generating set may not be equal.

Exercise 14.21. *Let R be a commutative ring with identity. $m \in maxspecR$. Show that $spec(R/m^k) = \{m/m^k\}$ where $k \in \mathbb{N}$, hence R/m^k is a local ring.*

Proof. Every prime ideal of R/m^k is of the form P/m^k where $m^k \subseteq P$ and P is a prime ideal of R. Taking radical on both side we get, $\sqrt{m^k} \subseteq \sqrt{P} \Rightarrow m \subseteq P$ since m is an maximal ideal, $m = P$ hence $spec(R/m^k) = \{m/m^k\}$. □

Definition 14.22. *A Module M is said to be finitely generated if there exists $\{m_1, \cdots, m_k\} \subseteq M$ such that $M = \langle m_1, \cdots, m_k \rangle$.*

Note 14.23. *A module M is finitely generated if and only if there exists a surjection from $R^k \to M$ for some $k \in \mathbb{N}$.*

14.5.1. *NAK (version 1).*

Lemma 14.24. *Let M be an finitely generated $R-$module and $I \subseteq R$ is an ideal of R if $IM = M$ then there exists $x \in I$ such that $(1 + x)M = 0$.*

Recall that $IM = \left\{ \sum_{\substack{\text{finite} \\ \text{sum}}} rm : r \in I, m \in M \right\}$ and $IM \subseteq M$ is a submodule.

Proof. Suppose $M = \langle m_1, \ldots, m_k \rangle$ and $IM = M$ then for $m_i \in IM, 1 \leq i \leq k$

$$\begin{aligned} m_1 &= r_{11}m_1 + r_{12}m_2 + \cdots + r_{1k}m_k \\ m_2 &= r_{21}m_1 + r_{22}m_2 + \cdots + r_{2k}m_k \\ &\vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ m_k &= r_{k1}m_1 + r_{k2}m_2 + \cdots + r_{kk}m_k \end{aligned}$$

Then we can write it

$$\underbrace{\begin{pmatrix} r_{11}-1 & r_{12} & \cdots & r_{1k} \\ r_{21} & r_{22}-1 & \cdots & r_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ r_{k1} & r_{k2} & \cdots & r_{kk}-1 \end{pmatrix}}_{A} \begin{pmatrix} m_1 \\ \vdots \\ m_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Multiplying by $\operatorname{adj} A$ we get

$$(\operatorname{adj} A)A \begin{pmatrix} m_1 \\ \vdots \\ m_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

This gives

$$\det A \begin{pmatrix} m_1 \\ \vdots \\ m_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Hence, $(\det A) \cdot m_i = 0$ for all $i \Rightarrow (\det A) \cdot M = 0$. We note that $\det A$ is of the form $1 + x$ where $x \in I$, therefore $(1 + x)M = 0$.

We prove that $\det A$ is of the form $1 + x$ where $x \in I$. We proceed by induction on k. It is true for $k = 1$. Now,

$$\det \begin{pmatrix} r_{11}-1 & \cdots & r_{1k} \\ \vdots & \ddots & \vdots \\ r_{k1} & \cdots & r_{kk}-1 \end{pmatrix} = (r_{11}-1)\det A_{11} - r_{12}\det A_{12} + \cdots + (-1)^k r_{1k} \det A_{1k}$$

By induction $\det A_{11} = 1 + x_1, x_1 \in I$ then $(r_{11} - 1)(1 + x_1) + y = 1 + x$ where $y \in I$ (as $r_{1i} \in I, 2 \leq i \leq k$) $\square$

14.5.2. *NAK (version 2).*

Lemma 14.25. *Let (R, m) be a local ring and M is finitely generated $R-$module such that $mM = M$ then $M = 0$.*

Proof. $\exists\ x \in m$ such that $(1+x)M = 0$ (by version 1). Now, (R, m) is a local ring and $x \in m$ then $1 + x$ is a unit, let $y(1 + x) = 1$. Therefore, $y(1 + x)M = y \cdot 0 \Rightarrow M = 0$. □

14.5.3. *NAK (version 3).*

Lemma 14.26. *Let (R, m) be a local ring and $N \subseteq M$, M is finitely generated. Suppose, $N+mM = M$ then $N = M$*

Proof. $N + mM = M \Rightarrow \dfrac{N + mM}{N} \cong \dfrac{M}{N} \Rightarrow m(M/N) \cong (M/N) \Rightarrow M/N = 0$. Therefore, $N = M$ [Note that M is finitely generated implies M/N is also finitely generated] □

14.6. **Finitely generated $R-$module.** Let (R, m, K) be a local ring and M is an $R-$module then M/mM is a K vector space under the scalar multiplication map

$$\begin{aligned} \cdot : & R/m \times M/mM \to M/mM \\ & (r + m, m_1 + mM) \mapsto rm_1 + mM \end{aligned}$$

Then check that the map is well defined. Let $r_1 + m = r_2 + m \Rightarrow r_1 - r_2 = \alpha \in m$ then $r_1 = r_2 + \alpha$. On the other hand let $m_1 + mM = m_2 + mM \Rightarrow m_1 - m_2 \in mM \Rightarrow m_1 - m_2 = \sum_{i=1}^{l} r_i'\beta_i \Rightarrow m_1 = m_2 + \sum_{i=1}^{l} r_i'\beta_i$. Then

$$r_1m_1 = (r_2 + \alpha)(m_2 + \sum_{i=1}^{l} r_i'\beta_i) = r_2m_2 + \left(\sum_{i=1}^{l}(r_2r_i)\beta_i + \alpha m_2 + \sum_{i=1}^{l}(r_i'\alpha)\beta_i\right)$$

Everything within the parentheses in above expression lies in mM hence $r_1m_1 - r_2m_2 \in mM \Rightarrow r_1m_1 + mM = r_2m_2 + mM$.
Next we consider the map

$$\begin{aligned} \pi : & M \to M/mM \\ & m_1 \to m_1 + mM \end{aligned}$$

Suppose, M is a finitely generated $R-$module and $S \subseteq M$ be a minimal generating set of M. Show that $\pi(S)$ is a basis of the K vector space M/mM. Let $S = \{m_1, \cdots, m_l\}$ and let $\alpha \in M \Rightarrow \alpha = \sum_{i=1}^{l} r_im_i$ then

$$\begin{aligned} \alpha + mM &= \left(\sum_{i=1}^{l} r_im_i\right) + mM \\ &= \sum_{i=1}^{l}(r_i + m)(m_i + mM) \end{aligned}$$

Therefore, we get span $\pi(S) = M/mM$. Next we show that $\pi(S)$ is linearly independent. Suppose,

$$\sum_{i=1}^{l}(r_i+m)(m_i+mM)=0$$

If $r_j+m \neq 0+m$ for some $j \in \{1,\cdots,l\}$ then $r_j \notin m$. Since R is local, r_j is a unit then $\exists u_j \in R$ such that $u_j r_j = 1$ then

$$\begin{aligned}(r_j+m)(m_j+mM) &= -\sum_{\substack{i=1\\ i\neq j}}^{k}(r_i+m)(m_i+mM)\\ m_j+mM &= -\sum_{\substack{i=1\\ i\neq j}}^{k}(u_j+m)(r_i+m)(m_i+mM)\\ &= \left(-\sum_{\substack{i=1\\ i\neq j}}^{k}(u_j r_i m_i)\right)+mM\end{aligned}$$

Therefore, $m_j + \sum_{\substack{i=1\\ i\neq j}}^{k}(u_j r_i m_i) \in mM$ then

$$m_j+\sum_{\substack{i=1\\ i\neq j}}^{k}(u_j r_i m_i)=\sum_{i=1}^{l}a_i m_i,\ a_i \in m, 1\leq i\leq l \tag{7}$$

We claim that $S \setminus \{m_j\}$ is also a generating set of M, hence we get a contradiction. From (1), $(1-a_j)m_j = \sum_{\substack{i=1\\ i\neq j}}^{l}(a_i - u_j r_i)m_i$ as $a_j \in m \Rightarrow 1-a_j$ is unit then $\exists b_j \in R$ such that $(1-a_j)b_j = 1$ therefore, $m_j = \sum_{\substack{i=1\\ i\neq j}}^{l}(a_i - u_j r_i)b_j m_i$. Let $s_i = (a_i - u_j r_i)b_j, 1 \leq i \leq l, i \neq j$. Let $s \in M$ and

$$\begin{aligned}s &= \sum_{i=1}^{l}t_i m_i = \sum_{\substack{i=1\\ i\neq j}}^{l}t_i m_i + t_j m_j\\ &= \sum_{\substack{i=1\\ i\neq j}}^{l}t_i m_i + t_j\left(\sum_{\substack{i=1\\ i\neq j}}^{l}s_i m_i\right)\\ &= \sum_{\substack{i=1\\ i\neq j}}^{l}(t_i + t_j s_i)m_i, \quad \text{contradiction}\end{aligned}$$

Therefore, $\pi(S)$ is linearly independent hence $\pi(S)$ is a basis.

Corollary 14.27. *Let $S_1, S_2 \subseteq M$ be two minimal generating set of M. Then $\pi(S_1)$ and $\pi(S_2)$ are two bases of M/mM this implies, $|\pi(S_1)| = |\pi(S_2)| \Rightarrow |S_1| = |S_2|$.*

Note that, $|S| = |\pi(S)|$ as $\pi(S)$ is linearly independent in M/mM.

14.6.1. *Construction of minimal generating set of M, where M is finitely generated R-module and R is a local ring.* M is finitely generated module a over a local ring (R, m, K) then M/mM is finite dimensional K vector space. Let $\{m_1 + mM, \cdots, m_r + mM\}$ be the basis of M/mM over K where $m_i \in M, 1 \leq i \leq r$. Consider the set $S = \{m_1, \cdots, m_r\} \subseteq M$ then $\langle S \rangle \subseteq M$ is a sub module, let $N = \langle S \rangle$.
Claim: $M = N$. Suppose, $\alpha \in M \Rightarrow \alpha + mM \in M/mM$ so we can write

$$\begin{aligned} \alpha + mM &= \sum_{i=1}^{r} (r_i + m)(m_i + mM) \\ &= \sum_{i=1}^{r} r_i m_i + mM \end{aligned}$$

Therefore, $\alpha - \sum_{i=1}^{r} r_i m_i \in mM \Rightarrow \alpha \in N + mM \Rightarrow M \subseteq N + mM$, again N and mM is a sub modules of M so that $N + mM \subseteq M$. Therefore, $M = N + mM$. By NAK $M = N$.

Definition 14.28. *Let M be finitely generated $R-$module over a local ring R then $\mu(M) = |S|$ where $S \subseteq M$ is a minimal generating set for M.*

By previous discussion $\mu(M)$ is well defined.

14.7. **Product module and Free module.**

Definition 14.29. *Let $\{M_i\}_{i \in I}$ be a set of $R-$modules then, $\prod_{i \in I} M_i$ is a module with component wise scalar multiplication i.e., if $a = (a_i) \in \prod_{i \in I} M_i$, $b = (b_i) \in \prod_{i \in I} M_i$ then $a + b = (a_i + b_i)$ and if $r \in R \Rightarrow ra = (ra_i)$. $\prod_{i \in I} M_i$ is called direct product of $\{M_i\}_{i \in I}$.*

Definition 14.30. *We define direct sum of module $\bigoplus_{i \in I} M_i$ is a sub module of $\prod_{i \in I} M_i$ where elements are $a = (a_i)$, all but finitely many components are zero.*

Note that if I is finite then $\prod_{i \in I} M_i = \bigoplus_{i \in I} M_i$.

Definition 14.31. *Let M be an $R-$module. $S \subseteq M$ is said to be linearly independent if $\{s_1, \cdots, s_r\} \subseteq S$ (any finite subset) and $\sum_{i=1}^{r} t_i s_i = 0, t_i \in R, 1 \leq i \leq r \Rightarrow t_i = 0, \ \forall \ i$. S is said to be basis of M if S is linearly independent and $\langle S \rangle = M$.*

Definition 14.32. *An $R-$module M is said to be free if it has a basis.*

Problem 14.33. *$\bigoplus_{i \in I} R_i$ where $R_i = R$, for all $i \in I$ is a free $R-$module with a basis $\{e_i\}_{i \in I}$ where $e_i = (0, \cdots, 0, 1, 0, \cdots)$ (ith position).*

Ans. If $m \in \bigoplus_{i\in I} R_i \Rightarrow m = \sum_{i=1}^{k} c_i e_{l_i}$ for some $k \in \mathbb{Z}^+$. Suppose,

$$\sum_{i=1}^{k} t_{l_i} e_{l_i} = 0 \Rightarrow (0, \cdots, t_{l_1}, \cdots, t_{l_2}, \cdots, t_{l_k}, \cdots) = (0, 0, \cdots, 0, \cdots) \Rightarrow t_{l_i} = 0, \text{ for all } i \in I.$$

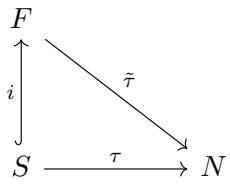
Observation 14.34. *Note that for any $m_0 \in M$ if we can write $m_0 = \sum_{i=1}^{r} t_i s_i = \sum_{i=1}^{r} t_i' s_i, 1 \leq i \leq r$ this implies, $\sum_{i=1}^{r} (t_i - t_i') s_i = 0 \Rightarrow t_i = t_i', 1 \leq i \leq r$. So each element $m_0 \in M$ has unique representation.*

Problem 14.35. *Show that $\prod_{i\in\mathbb{N}} M_i$, $M_i = \mathbb{Z}$ for all $i \in \mathbb{N}$ is not a free $\mathbb{Z}$ module.*

We discuss product module and free module further in **Appendix A** section.

14.7.1. *Universal property.*

Theorem 14.36 (Universal property)**.** *Let F be a free module with a basis S and N be any $R-$module with a set map $\tau : S \to N$ then, there exists unique module homomorphism $\tilde{\tau} : F \to N$ such that the diagram commutes.*



Proof. Let $m \in F$ then $m = \sum_{i=1}^{n} r_i s_i$ (unique representation). Define,

$$\tilde{\tau} : F \to N$$
$$m \mapsto \sum_{i=1}^{n} r_i \tau(s_i)$$

Note that $\tilde{\tau}$ is well defined as m has unique representation. Then $\tilde{\tau}(s) = \tau(s)\ \forall s \in S \Rightarrow \tilde{\tau} \circ i = \tau$. Let $g : F \to N$ be another module homomorphism such that $g \circ i = \tau \Rightarrow g(s) = \tau(s)\ \forall s \in S$. Now,

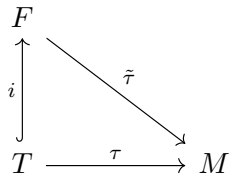
$$g(m) = g\left(\sum_{i=1}^{n} r_i s_i\right) = \sum_{i=1}^{n} r_i g(s_i) = \sum_{i=1}^{n} r_i \tau(s_i) = \tilde{\tau}(m)$$

Therefore, $g = \tilde{\tau}$. □

Theorem 14.37. *Let M be an $R-$module then there exists a free $R-$module F and a surjective module homomorphism between F and M.*

Proof. Let $S \subseteq M$ be a generating set. By Zermelo's theorem "every set can be well ordered", we may think S as a index set. Consider $F = \bigoplus_{i\in S} R_i$ where $R_i = R$ then F is a free module with basis

$\{e_i\}_{i\in S} = T$(say). Then we have a set map $\tau : T \to S(\subseteq M)$ defined by $\tau(e_s) = s$. By Universal property of free module there exists a unique module homomorphism $\tilde{\tau} : F \to M$ such that the diagram commutes.



Claim: $\tilde{\tau}$ is surjective. Let $m \in M$ then $\exists\ \{s_1, \ldots, s_r\} \subseteq S$ such that

$$\begin{aligned} m &= \sum_{i=1}^{r} r_i s_i = \sum_{i=1}^{r} r_i \tau(e_{s_i}) \\ &= \tilde{\tau}\left(\sum_{i=1}^{r} r_i e_{s_i}\right) \end{aligned}$$

Therefore, $\tilde{\tau}$ is surjective. □

14.8. **Exact Sequence.**

Definition 14.38 (Chain Complex)**.** *Let $\{M_i, \phi_i\}_{i\in\mathbb{N}}$ be a collection where M_i's are $R-$modules and $\phi_i : M_i \to M_{i-1}$ be $R-$linear map, then the sequence,*

$$\mathbb{M}_\bullet \equiv \cdots \to M_i \xrightarrow{\phi_i} M_{i-1} \xrightarrow{\phi_{i-1}} M_{i-2} \longrightarrow \cdots$$

is called chain complex if

$$\operatorname{Im}\phi_i \subseteq \ker\phi_{i-1} \text{ for all } i \in \mathbb{N}$$

The chain complex is said to be exact if

$$\operatorname{Im}\phi_i = \ker\phi_{i-1} \text{ for all } i \in \mathbb{N}.$$

Definition 14.39. *Let, $H_i(\mathbb{M}_\bullet) = \dfrac{\ker\phi_i}{\operatorname{Im}\phi_{i+1}}$ where $\mathbb{M}_\bullet$ is a chain complex, is called i^{th} homology group of $H_i(\mathbb{M}_\bullet)$. Therefore, $\mathbb{M}_\bullet$ is exact if and only if $H_i(\mathbb{M}_\bullet) = 0$ for all $i \in \mathbb{N}$.*

Definition 14.40 (Short exact sequence)**.** *Let M_1, M_2, M_3 be $R-$modules then the sequence*

$$0 \longrightarrow M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} M_3 \longrightarrow 0$$

is called short exact sequence if it is an exact sequence i.e.,
(i) ϕ_1 is injective,
(ii) $\operatorname{Im}\phi_1 = \ker\phi_2$,
(iii) ϕ_2 is surjective.

Example 14.41. *Let $f : M \to N$ be a module homomorphism then*

$$0 \longrightarrow \ker f \xrightarrow{i} M \xrightarrow{f} \operatorname{Im} f \longrightarrow 0, \quad \operatorname{Im} f \subseteq N$$

the above sequence is exact.

Example 14.42. *Let M be an $R-$module then there exists a free module F such that*

$$F \xrightarrow{\pi} M \longrightarrow 0$$

is a surjection. Therefore,

$$0 \longrightarrow \ker \pi \xrightarrow{i} F \xrightarrow{\pi} M \longrightarrow 0$$

is exact sequence and $F/\ker \pi \cong M$.

Definition 14.43. *Let $\mathbb{L}_\bullet \equiv \{M_i, \phi_i\}$ and $\mathbb{T}_\bullet \equiv \{N_i, \psi_i\}$ be two chain complexes. $\{\tau_i : M_i \to N_i\}$ is called a chain map if*

$$\begin{array}{ccccccccc}
\mathbb{L}_\bullet \equiv \cdots & \longrightarrow & M_{i+1} & \xrightarrow{\phi_{i+1}} & M_i & \xrightarrow{\phi_i} & M_{i-1} & \xrightarrow{\phi_{i-1}} & \cdots \\
 & & \downarrow{\scriptstyle \tau_{i+1}} & \circlearrowright & \downarrow{\scriptstyle \tau_i} & \circlearrowright & \downarrow{\scriptstyle \tau_{i-1}} & & \\
\mathbb{T}_\bullet \equiv \cdots & \longrightarrow & N_{i+1} & \xrightarrow{\psi_{i+1}} & N_i & \xrightarrow{\psi_i} & N_{i-1} & \xrightarrow{\psi_{i-1}} & \cdots
\end{array}$$

each diagram is commutative i.e., $\tau_i \circ \phi_{i+1} = \psi_{i+1} \circ \tau_{i+1}$ for all $i \in \mathbb{N}$.

Definition 14.44. *Let, $f : M \to N$ be a $R-$linear map then* $\operatorname{Coker} f = N/\operatorname{Im} f$ *and*

$$0 \longrightarrow \ker f \xrightarrow{i} M \xrightarrow{f} N \xrightarrow{\pi} \operatorname{coker} f \longrightarrow 0$$

is an exact sequence.

Definition 14.45. *Let $\{M^i, \phi^i\}_{i\in\mathbb{N}}$ be a collection where M^i's are $R-$modules and $\phi^i : M^i \to M^{i+1}$ be $R-$linear map, then the sequence,*

$$\mathbb{M}^\bullet \equiv \cdots \to M^i \xrightarrow{\phi^i} M^{i+1} \xrightarrow{\phi^{i+1}} M^{i+2} \longrightarrow \cdots$$

is called co-chain complex if

$$\operatorname{Im} \phi^i \subseteq \ker \phi^{i+1}, \text{ for all } i \in \mathbb{N}$$

The co-chain complex is said to be exact if

$$\operatorname{Im} \phi^i = \ker \phi^{i+1}, \text{ for all } i \in \mathbb{N}.$$

Definition 14.46. *Let, $H^i(\mathbb{M}^\bullet) = \dfrac{\ker \phi^i}{\operatorname{Im} \phi^{i-1}}$ where $\mathbb{M}^\bullet$ is a co-chain complex, is called i^{th} co-homology group of $H^i(\mathbb{M}^\bullet)$. Therefore, $\mathbb{M}^\bullet$ is exact if and only if $H^i(\mathbb{M}^\bullet) = 0$ for all $i \in \mathbb{N}$.*

Definition 14.47. *Let $\mathbb{L}^\bullet \equiv \{M^i, \phi^i\}$ and $\mathbb{T}^\bullet \equiv \{N^i, \psi^i\}$ be two co-chain complexes. $\{\tau^i : M^i \to N^i\}$ is called a co-chain map if*

$$\begin{array}{ccccccccc}
\mathbb{L}^\bullet \equiv \cdots & \longrightarrow & M^i & \xrightarrow{\phi^i} & M^{i+1} & \xrightarrow{\phi^{i+1}} & M^{i+2} & \xrightarrow{\phi^{i+2}} & \cdots \\
 & & \downarrow{\scriptstyle \tau^i} & \circlearrowright & \downarrow{\scriptstyle \tau^{i+1}} & \circlearrowright & \downarrow{\scriptstyle \tau^{i+2}} & & \\
\mathbb{T}^\bullet \equiv \cdots & \longrightarrow & N^i & \xrightarrow{\psi^i} & N^{i+1} & \xrightarrow{\psi^{i+1}} & N^{i+2} & \xrightarrow{\psi^{i+2}} & \cdots
\end{array}$$

each diagram is commutative i.e., $\psi^i \circ \tau^i = \tau^{i+1} \circ \phi^{i+1}$ for all $i \in \mathbb{N}$.

Definition 14.48. *Let $\mathcal{C}$ and $\mathcal{D}$ be two chain complexes and $f : \mathcal{C} \to \mathcal{D}$ be a chain map.*

$$\begin{array}{ccccccccccccc}
\mathcal{C} \equiv \cdots & \longrightarrow & M_{i+1} & \xrightarrow{g_{i+1}} & M_i & \xrightarrow{g_i} & M_{i-1} & \xrightarrow{g_{i-1}} & \cdots & \longrightarrow & M_0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_{i+1}} & \swarrow{\scriptstyle s_i} & \downarrow{\scriptstyle f_i} & \swarrow{\scriptstyle s_{i-1}} & \downarrow{\scriptstyle f_{i-1}} & & & & \downarrow{\scriptstyle f_0} & & \\
\mathcal{D} \equiv \cdots & \longrightarrow & N_{i+1} & \xrightarrow[h_{i+1}]{} & N_i & \xrightarrow[h_i]{} & N_{i-1} & \xrightarrow[h_{i-1}]{} & \cdots & \longrightarrow & M_0 & \longrightarrow & 0
\end{array}$$

f is said to be null homotopic if there exists a map $s_i : M_i \to N_{i+1}$ such that

$$f_i = h_{i+1} \circ s_i + s_{i-1} \circ g_i$$

for all $i \in \mathbb{N}$. If p and q be two chain maps. Then p and q are said to be homotopic if $p - q$ is null homotopic.

Proposition 14.49. *Let $p, q : \mathcal{C} \to \mathcal{D}$ be two homotopic chain maps. Then $H_i(\mathcal{C}) \xrightarrow[q_{*i}]{p_{*i}} H_i(\mathcal{D})$ are the same maps.*

Proof. Consider the diagram

$$\begin{array}{ccccccccc}
 & & \cdots & \longrightarrow & \operatorname{Ker}\alpha_{i+1} & \xrightarrow{\alpha_{i+1}} & \operatorname{Ker}\alpha_i & \xrightarrow{\alpha_i} & \operatorname{Ker}\alpha_{i-1} & \longrightarrow & \cdots \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
\mathcal{C} \equiv & \cdots & \longrightarrow & M_{i+1} & \xrightarrow{\alpha_{i+1}} & M_i & \xrightarrow{\alpha_i} & M_{i-1} & \longrightarrow & \cdots & \\
 & & & \downarrow{\scriptstyle p_{i+1}} & & \downarrow{\scriptstyle p_i} & & \downarrow{\scriptstyle p_{i-1}} & & & \\
\mathcal{D} \equiv & \cdots & \longrightarrow & N_{i+1} & \xrightarrow{\beta_{i+1}} & N_i & \xrightarrow{\beta_i} & N_{i-1} & \longrightarrow & \cdots &
\end{array}$$

Let $x \in \operatorname{Ker}\alpha_i \Rightarrow \alpha_i(x) = 0 \Rightarrow p_{i-1} \circ \alpha_i(x) = 0 \Rightarrow \beta_i \circ p_i(x) = 0 \Rightarrow p_i(x) \in \operatorname{Ker}\beta_i$. Therefore p_i maps an element of $\operatorname{Ker}\alpha_i$ into $\operatorname{Ker}\beta_i$. Now,

$$\begin{array}{ccccc}
\operatorname{Ker}\alpha_i & \xrightarrow{p_i} & \operatorname{Ker}\beta_i & \xrightarrow{\pi_i} & \dfrac{\operatorname{Ker}\beta_i}{\operatorname{Im}\beta_{i+1}} \\
\downarrow{\scriptstyle \tilde{\pi}_i} & & & \nearrow{\scriptstyle p_{*i}} & \\
\dfrac{\operatorname{Ker}\alpha_i}{\operatorname{Im}\alpha_{i+1}} & & & &
\end{array}$$

We want to show that $\operatorname{Im}\alpha_{i+1} \subseteq \operatorname{Ker}(\pi_i \circ p_i)$. Let $y \in \operatorname{Im}\alpha_{i+1}$, then there exists $y' \in M_{i+1}$ such that $\alpha_{i+1}(y') = y \Rightarrow p_i \circ \alpha_{i+1}(y') = p_i(y) \Rightarrow \beta_{i+1} \circ p_{i+1}(y') = p_i(y) \Rightarrow (\pi_i \circ \beta_{i+1}) \circ p_{i+1}(y') = (\pi_i \circ p_i)(y) \Rightarrow 0 = (\pi_i \circ p_i)(y) \Rightarrow y \in \operatorname{Ker}(\pi_i \circ p_i)$. Therefore there exists a well defined group morphism $p_{*i} : \dfrac{\operatorname{Ker}\alpha_i}{\operatorname{Im}\alpha_{i+1}} \to \dfrac{\operatorname{Ker}\beta_i}{\operatorname{Im}\beta_{i+1}}$. Similar computation for q_i leads to another map namely q_{*i}, hence we have two following maps

$$p_{*i} : \frac{\operatorname{Ker}\alpha_i}{\operatorname{Im}\alpha_{i+1}} \longrightarrow \frac{\operatorname{Ker}\beta_i}{\operatorname{Im}\beta_{i+1}} \qquad \text{and} \qquad p_{*i} : \frac{\operatorname{Ker}\alpha_i}{\operatorname{Im}\alpha_{i+1}} \longrightarrow \frac{\operatorname{Ker}\beta_i}{\operatorname{Im}\beta_{i+1}}$$

$$m_i + \operatorname{Im}\alpha_{i+1} \longmapsto p_i(m_i) + \operatorname{Im}\beta_{i+1} \qquad m_i + \operatorname{Im}\alpha_{i+1} \longmapsto q_i(m_i) + \operatorname{Im}\beta_{i+1}$$

We need to show $p_{*i} = q_{*i}$. Pick $m_i \in \operatorname{Ker}\alpha_i$ then $(p_i - q_i)(m_i) = \beta_{i+1} \circ s_i(m_i) + s_{i-1} \circ \alpha_i(m_i) = \beta_{i+1} \circ s_i(m_i) \in \operatorname{Im}\beta_{i+1} \Rightarrow p_{*i} = q_{*i}$. □

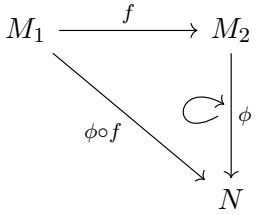
14.9. **Hom functor.** Recall, suppose M, N be two $R-$modules,

$$\mathrm{Hom}_R(M,N) := \{f : M \to N |\ f \text{ is a R-linear map}\}$$

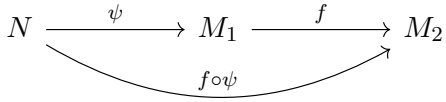
is also a $R-$module. Let $f : M_1 \to M_2$ be module homomorphism and $\phi \in \mathrm{Hom}_R(M_2, N)$ then $\phi \circ f \in \mathrm{Hom}_R(M,N)$. Thus f induces a module homomorphism

$$f^* : \mathrm{Hom}_R(M_2,N) \to \mathrm{Hom}_R(M,N)$$
$$\phi \mapsto \phi \circ f$$

i.e., $f^*(\phi) = \phi \circ f$,



and if $\psi \in \mathrm{Hom}_R(N, M_1)$ then



Thus f induces a module homomorphism

$$f_* : \mathrm{Hom}_R(N,M_1) \to \mathrm{Hom}_R(N,M_2)$$
$$\psi \mapsto f \circ \psi$$

i.e., $f_*(\psi) = f \circ \psi$.

Proposition 14.50. *For any $R-$module N, $Hom_R(-,N)$ is contra variant left exact functor and $Hom_R(N,-)$ is covariant left exact functor i.e., for any exact sequence*

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0 \tag{8}$$

of $R-$module, the induce sequence

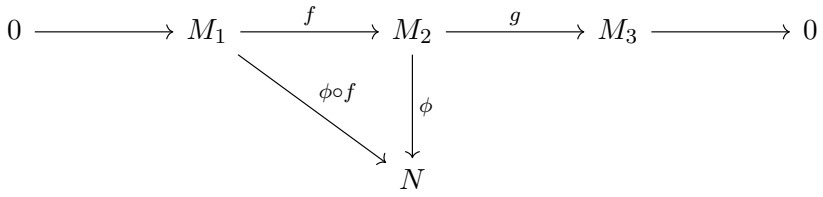
$$0 \longrightarrow Hom_R(M_3,N) \xrightarrow{g^*} Hom_R(M_2,N) \xrightarrow{f^*} Hom_R(M_1,N) \tag{9}$$

is exact and

$$0 \longrightarrow Hom_R(N,M_1) \xrightarrow{f_*} Hom_R(N,M_2) \xrightarrow{g_*} Hom_R(N,M_3) \tag{10}$$

is exact.

Proof. We show that g^* is injective. Let $g^*(\phi) = 0 \Rightarrow \phi \circ g = 0 \Rightarrow \phi \circ g(m_2) = 0$ for all $m_2 \in M_2$. Let $m_3 \in M_3$ since g is surjective $\exists m_2' \in M_2$ such that $g(m_2') = m_3 \Rightarrow \phi(g(m_2')) = \phi(m_3) \Rightarrow \phi(m_3) = 0 \Rightarrow \phi = 0$ [since m_3 is chosen arbitrarily] therefore, $\mathrm{Ker}\, g^* = \{0\}$ implies g^* is injective. Now we show that $\mathrm{Im}\, g^* = \mathrm{Ker}\, f^*$. Let $f^* \circ g^*(\phi) = f^*(\phi \circ g) = \phi \circ (g \circ f) = 0$ [$g \circ f = 0$ as the sequence (3) is exact] therefore, $\mathrm{Im}\, g^* \subseteq \mathrm{Ker}\, f^*$. Let $\phi \,\mathrm{Ker}\, f^*$ where $\phi \in \mathrm{Hom}_R(M_2,N)$ i.e., $\phi \circ f = 0$.



Let $m_3 \in M_3$, since g is surjective $\exists m_2 \in M_2$ such that $g(m_2) = m_3$. Let us define a function

$$\psi : M_3 \to N$$
$$m_3 \mapsto \phi(m_2)$$

Let $m_3 = g(m_2) = g(m_2') \Rightarrow g(m_2 - m_2') = 0 \Rightarrow m_2 - m_2' \in \operatorname{Ker} g = \operatorname{Im} f$ then $\exists m_1 \in M_1$ such that $m_2 - m_2' = f(m_1) \Rightarrow m_2 = m_2' + f(m_1) \Rightarrow \phi(m_2) = \phi(m_2') + \phi \circ f(m_1) \Rightarrow \phi(m_2) = \phi(m_2')$ [as $\phi \circ f = 0$] therefore, ψ is well defined $R-$linear map.
Claim: $g^*(\psi) = \phi$. Let $\psi \circ g(m_2) = \psi(m_3) = \phi(m_2)$, $\forall m_2 \in M_2$ therefore $g^*(\psi) = \phi$ hence $\operatorname{Im} g^* = \operatorname{Ker} f^*$.
Now we will show that f_* is injective. Let $f_*(\tau) = 0 \Rightarrow f \circ \tau = 0 \Rightarrow f(\tau(n)) = 0$ for all $n \in N$. Since f is injective, we have $\tau(n) = 0$ for all $n \in N$ then $\tau = 0$, hence f_* is injective. Next we need to show that $\operatorname{Im} f_* = \operatorname{Ker} g_*$. Let $\tau' \in \operatorname{Im} f_*$ where $\tau' \in \operatorname{Hom}_R(N, M_2)$ then $\tau' = f_*(\tau) \Rightarrow \tau'(n) = f(\tau(n))$ for all $n \in N$. Now, $\operatorname{Im} f = \operatorname{Ker} g$ and $\tau'(n) \in \operatorname{Im} f = \operatorname{Ker} g \Rightarrow g(\tau'(n)) = 0$, $\forall n \in N \Rightarrow g_*(\tau') = 0 \Rightarrow \tau' \in \operatorname{Ker} g_* \Rightarrow \operatorname{Im} f_* \subseteq \operatorname{Ker} g_*$. Suppose, $\tau' \in \operatorname{Ker} g_* \Rightarrow g_*(\tau') = 0 \Rightarrow g \circ \tau' = 0 \Rightarrow g(\tau'(n)) = 0$, $\forall n \in N$. Clearly $\tau'(n) \in \operatorname{Ker} g = \operatorname{Im} f$.

Theorem 14.51. *Let $\{M_i\}_{i\in\Lambda}$ be a collection of $R-$module and N is also be an $R-$module then*

(1) $Hom_R\left(\bigoplus_{i\in\Lambda} M_i, N\right) \cong \prod_{i\in\Lambda} Hom_R(M_i, N)$.

14.10. **Tensor Product.**

Definition 14.52. *Let $M_1, \cdots, M_k, N$ be $R-$modules. A map $f : M_1 \times \cdots \times M_k \to N$ is said to be linear in ith variable if, given fixed $m_j, j \neq i$, the map*

$$T : M_i \to N$$

defined by $T(m) = f(m_1, \cdots, m_{i-1}, m, m_{i+1}, m_k)$ is linear. The map f is said to be multilinear if it is linear in each variable.

Let M, N be two $R-$modules. Consider the free module F generated by the $M \times N$ over R, then the elements of F are of the form $\sum_{\text{finite sum}} r_i x_i$ where $r_i \in R$ and $x_i \in M \times N$. Let D be the submodule of F generated by the elements of the form

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n)$$
$$(m, n_1 + n_2) - (m, n_1) - (m, n_2)$$
$$(rm, n) - r(m, n)$$
$$(m, rn) - r(m, n)$$

where $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ and $r \in R$. Let $T = F/D$. We denote $T = M \otimes_R N$ and T is said to be Tensor product of M and N. We denote $(m, n) + D \in F/D$ by $m \otimes n$ and we have a map

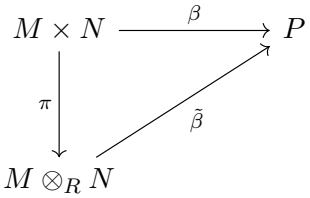
$$M \times N \xrightarrow{\pi} T$$
$$(m, n) \mapsto m \otimes n$$

We will show that π is bilinear map. $\pi((m_1 + m_2, n)) = (m_1 + m_2, n) + D$. Since

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n) \in D$$

$\pi((m_1 + m_2, n)) = (m_1 + m_2, n) + D = (m_1, n) + D + (m_2, n) + D = \pi(m_1, n) + \pi(m_2, n)$ for all $m_1, m_2 \in M$ and for all $n \in N$. Similarly we can show that θ satisfies the property of bilinear map.

Theorem 14.53 (Universal Property)**.** *For every bilinear map $\beta : M \times N \to P$ where P is an $R-$module, there exists an unique $R-$linear map $\tilde{\beta} : M \otimes_R N \to P$ such that the diagram commutes.*

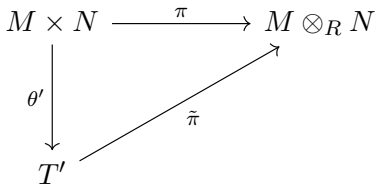


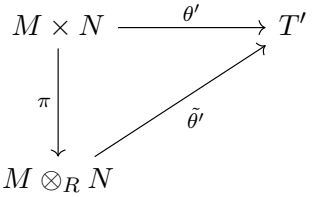
More over, if (T', θ') be another pair with such property then there exists a module isomorphism $M \otimes_R N \to T'$.

Proof. Define $\tilde{\beta} : M \otimes_R N \to P$ by $\tilde{\beta}(m \otimes n) = \beta(m, n)$ and extend it linearly. Let $m_1 \otimes n_1 = m_2 \otimes n_2 \Rightarrow (m_1, n_1) - (m_2, n_2) \in D$. Since

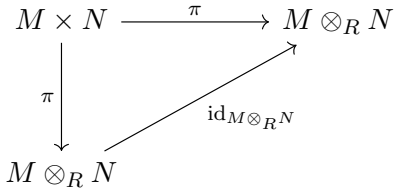
By our construction $\tilde{\beta}$ is bilinear. Suppose $\gamma : M \otimes_R N \to P$ be another $R-$linear map such that the diagram commutes. Then $\gamma(m \otimes n) = \beta(m, n) = \tilde{\beta}\pi(m, n) = \tilde{\beta}(m \otimes n)$. Hence $\gamma = \tilde{\beta}$.

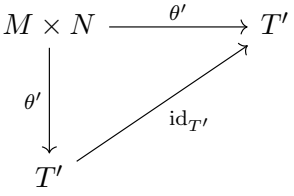
Now we assume that there exists another pair (T', θ') with same property, then





where $\tilde{\pi}$ and $\tilde{\theta'}$ are $R-$ linear map. Since the diagrams commutes, we have $\tilde{\pi} \circ \theta' = \pi$ (from first diagram) and $\tilde{\theta'} \circ \pi = \theta'$ (from second diagram). Hence $(\tilde{\theta'} \circ \tilde{\pi}) \circ \theta' = \theta'$ and $(\tilde{\pi} \circ \tilde{\theta'}) \circ \pi = \pi$. Again we consider the following diagrams





By Universal property, we have $\tilde{\theta'} \circ \tilde{\pi} = id_{T'}$ and $\tilde{\pi} \circ \tilde{\theta'} = \mathrm{id}_{M \otimes_R N}$. □

Tensor product of algebras. Let A and B be $R-$algebra, We consider the module $C = A \otimes_R B$. Let us define a mapping $\beta : A \times B \times A \times B \to C$ by $\beta(a, b, a', b') = aa' \otimes bb'$. Since β is multilinear, β induce a mapping $\tilde{\beta} : C \otimes_R C \to C$. This $\tilde{\beta}$ corresponds a bilinear mapping $\gamma : C \times C \to C$ given by $\gamma(a \otimes b, a' \otimes b') = aa' \otimes bb'$. Since γ is well define, it defines a multiplication on C and therefore C becomes a commutative ring with unity, $1 \otimes 1$ being the multiplicative identity. Since A and B are $R-$algebra, there exists $f : R \to A$ and $g : R \to B$ two ring morphisms. Now we define $\psi : R \to A \otimes_R B$ by $\psi(r) = f(r) \otimes g(r)$. Let $r_1, r_2 \in R$ then $\psi(r_1 + r_2) = f(r_1 + r_2) \otimes g(r_1 + r_2) = f(r_1) \otimes g(r_1 + r_2) + f(r_2) \otimes g(r_1 + r_2)$.

We note that C is both A and B algebra as $\mu_A : A \to A \otimes_R B$ is defined by $\mu_A(a) = a \otimes 1_B$ and $\mu_B : B \to A \otimes_R B$ is defined by $\mu_B(b) = 1_A \otimes b$. It is easy to check that both μ_A and μ_B is a ring homomorphism.

Theorem 14.54 (Properties of Tensor product)**.** *Let M, N, P and $\{M_i\}_{i \in \Lambda}$ be $R-$modules, $I \subseteq R$ be a ideal of R, S be a multiplicatively closed set in R then we have*

(1) $M \otimes_R N \cong N \otimes_R M$.
(2) $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R) P$.
(3) $M \otimes_R R \cong M$.
(4) $M \otimes_R R/I \cong M/IM$.
(5) $M \otimes_R S^{-1}R \cong S^{-1}M$.
(6) $\left(\bigoplus_{i \in \Lambda} M_i\right) \otimes_R N \cong \bigoplus_{i \in \Lambda} (M_i \otimes_R N)$.

Proof. (1) Consider the diagram

$$\begin{array}{ccc} M \times N & \underset{\beta}{\overset{\alpha}{\rightleftarrows}} & N \times M \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \tilde{\pi}} \\ M \otimes_R N & \underset{\beta'}{\overset{\alpha'}{\rightleftarrows}} & N \otimes_R M \end{array}$$

where $\alpha((m,n)) = (n,m)$ and $\beta((n,m)) = (m,n)$. We claim that $\tilde{\pi} \circ \alpha$ is bilinear. Let $(m_1 + m_2, n) \in M \times N$, $\tilde{\pi}\alpha((m_1 + m_2, n)) = \tilde{\pi}(n, m_1 + m_2) = n \otimes (m_1 + m_2) = n \otimes m_1 + n \otimes m_2 = \tilde{\pi}\alpha((m_1, n)) + \tilde{\pi}\alpha((m_2, n))$ for all $m_1, m_2 \in M$ and for all $n \in N$. Similarly other properties can be shown. By Universal property, we have a module morphism $\alpha' : M \otimes_R N \to N \otimes_R M$. Similarly the map $\beta \circ \pi$ is also bilinear so we have a $R-$ linear map $\beta' : N \otimes_R M \to M \otimes_R M$. We just need to show that $\alpha' \circ \beta = \mathrm{id}_{N \otimes_R M}$ and $\beta' \circ \alpha' = \mathrm{id}_{M \otimes_R N}$ which is easy, $\alpha' \circ \beta'(n \otimes m) = \alpha'(m \otimes n) = n \otimes n$ and $\beta' \circ \alpha'(m \otimes n) = \beta'(n \otimes m) = m \otimes n$.

(2)

(3) Let $f : M \times R \to M$ be the map where $f(m,r) = rm$. Since M is an $R-$module, f is bilinear, hence f induce a map $\tilde{f} : M \otimes_R R \to R$ such that the diagram commutes

$$\begin{array}{ccc} M \times R & \xrightarrow{\quad f \quad} & M \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \tilde{f}} & \\ M \otimes_R R & & \end{array}$$

where $\tilde{f} \circ \pi = f \Rightarrow f(m,r) = \tilde{f}\pi(m,r) \Rightarrow rm = \tilde{f}(m \otimes r)$ and $\tilde{f}$ is $R-$linear. Let $g : M \to M \otimes_R R$ defined as $g(m) = m \otimes 1$. It is easy to show that g is $R-$linear and $\tilde{f} \circ g = \mathrm{id}_M$ and $g \circ \tilde{f} = \mathrm{id}_{M \otimes_R R}$.

(4) Let $f : M \times R/I \to M/IM$ be the bilinear map defined by $f(m, r + I) = rm + IM$. By Universal property there exists a well define module morphism $\tilde{f} : M \otimes_R R/I \to M/IM$ such that the diagram commutes,

$$\begin{array}{ccc} M \times R/I & \xrightarrow{\quad f \quad} & M/IM \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \tilde{f}} & \\ M \otimes_R R/I & & \end{array}$$

where $\tilde{f}(m \otimes (r+I)) = rm + IM$. Let $g : M/IM \to M \otimes_R R/I$ be the map $g(m + IM) = m \otimes (1 + I)$. Then g is an $R-$linear map and $g \circ \tilde{f} = \mathrm{id}_{M \otimes_R R/I}$ and $\tilde{f} \circ g = \mathrm{id}_{M/IM}$.

(5) Consider

$$\begin{array}{ccc} M \times S^{-1}R & \xrightarrow{\quad f \quad} & S^{-1}M \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \tilde{f}} & \\ M \otimes_R S^{-1}R & & \end{array}$$

where $f\left(m, \frac{r}{s}\right) = rm/s$. First we need to check $f$is well defined. Let $\frac{r_1}{s_1} = \frac{r_2}{s_2}$ then there exists some $s \in S$ such that $s(r_1s_2 - s_1r_2) = 0 \Rightarrow s(r_1s_2 - s_1r_2)m = 0 \Rightarrow s(r_1s_2m - s_1r_2m) = 0 \Rightarrow \frac{r_1m}{s_1} = \frac{r_2m}{s_2}$. It is obvious that f is bilinear. Then there exits a unique module morphism $\tilde{f} : M \otimes_R S^{-1}R \to S^{-1}M$ where $\tilde{f}\left(m \otimes \frac{r}{s}\right) = \frac{rm}{s}$. Define $g : S^{-1}M \to M \times S^{-1}R$ by $g\left(\frac{m}{s}\right) = m \times \frac{1}{s}$. g is well defined module morphism and $g = \tilde{f}^{-1}$.

(6) Let $\theta_i : M_i \to \bigoplus_{i\in\Lambda} M_i$ be the inclusion map. Define

$$f : \left(\bigoplus_{i\in\Lambda} M_i\right) \times N \to \bigoplus_{i\in\Lambda}(M_i \otimes_R N)$$
$$((m_i)_{i\in\Lambda}, n) \mapsto (m_i \otimes n)_{i\in\Lambda}.$$

We will show that f is bilinear. $f((m_i)_{i\in\Lambda} + (m_i')_{i\in\Lambda}, n) = f((m_i + m_i')_{i\in\Lambda}, n) = ((m_i + m_i') \otimes n)_{i\in\Lambda} = (m_i \otimes n)_{i\in\Lambda} + (m_i' \otimes n)_{i\times\Lambda} = f((m_i)_{i\in\Lambda}, n) + f((m_i')_{i\in\Lambda}, n)$. Similarly other properties can be shown. Hence we have a map $\tilde{f} : \left(\bigoplus_{i\in\Lambda} M_i\right) \otimes_R N \to \bigoplus_{i\in\Lambda}(M_i \otimes_R N)$ defined by $\tilde{f}((m_i)_{i\in\Lambda} \otimes n) = (m_i \otimes n)_{i\in\Lambda}$. Define $g : \bigoplus_{i\in\Lambda}(M_i \otimes_R N) \to \left(\bigoplus_{i\in\Lambda} M_i\right) \otimes_R N$ by $g((m_i \otimes n_i)_{i\in\Lambda}) = \sum_{i\in\Lambda}(\theta_i(m_i) \otimes n_i)$. Note that g is $R-$linear. Now, $g \circ \tilde{f}((m_i)_{i\in\Lambda} \otimes n) = g((m_i \otimes n)_{i\in\Lambda}) = \sum_{i\in\Lambda}(\theta_i(m_i) \otimes n) = \left(\sum_{i\in\Lambda} \theta_i(m_i)\right) \otimes n = (m_i)_{i\in\Lambda} \otimes n \Rightarrow g \circ \tilde{f} = \mathrm{id}_{\left(\bigoplus_{i\in\Lambda} M_i\right) \otimes_R N}$.

Let $(m_i \otimes n_i)_{i\in\Lambda} \in \bigoplus_{i\in\Lambda}(M_i \otimes_R N)$, then $\tilde{f} \circ g((m_i \otimes n_i)_{i\in\Lambda}) = \tilde{f}\left(\sum_{i\in\Lambda}(\theta_i(m_i) \otimes n_i)\right) = \sum_{i\in\Lambda} \tilde{f}(\theta_i(m_i) \otimes n_i) = \sum_{i\in\Lambda} = \theta_i(m_i) \otimes n_i = (m_i \otimes n_i)_{i\in\Lambda} \Rightarrow \tilde{f} \circ g = \mathrm{id}_{\bigoplus_{i\in\Lambda}(M_i \otimes_R N)}$.

□

Remark 14.55. *Let $f : A \to B$ be a ring homomorphism. Suppose M is an $A-$module and N is an $B-$module. Then $M \otimes_A N$ has both A and B module structure,*

$$B \times M \otimes_A N \to M \otimes_A N$$
$$(n, m \otimes n) \mapsto m \otimes bm$$

Theorem 14.56. *Let B be an A algebra, M be an $A-$module and N, P be $B-$modules. Then*

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P).$$

Proof. It is suffices to establish the isomorphism as $B-$module.

□

Theorem 14.57 (Hom-Tensor adjunction)**.** *Let M, N, P be $R-$modules. Then*

$$Hom_R(M \otimes_R N, P) \cong Hom_R(M, Hom_R(N, P)).$$

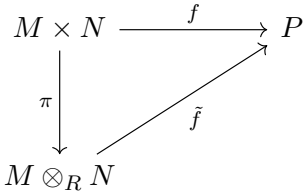
Proof. Define

$$\psi : \mathrm{Hom}_R(M \otimes_R N, P) \to \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$$
$$f \mapsto \psi(f)$$

where $\psi(f)(m)(n) = f(m \otimes n)$ and

$$\phi : \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) \to \mathrm{Hom}_R(M \otimes_R N, P)$$
$$g \mapsto \phi(g)$$

where $\phi(g)(m \otimes n) = g(m)(n)$. We shall now show that $\phi(g)$ is well defined. Consider the diagram



where $f(m,n) = g(m)(n)$. We claim that f is bilinear. $f(m_1 + m_2, n) = g(m_1 + m_2)(n) = g(m_1)(n) + g(m_2)(n) = f(m_1, n) + f(m_2, n)$ for all $m_1, m_2 \in M$ and for all $n \in N$. Now $f(m, n_1 + n_2) = g(m)(n_1 + n_2) = g(m)(n_1) + g(m)(n_2) = f(m, n_1) + f(m, n_2)$ for all $m \in M$ and for all $n_1, n_2 \in N$. Pick $r \in R, m \in M$ and $n \in N$, $f(rm, n) = g(rm)(n) = rg(m)(n) = rf(m, n)$ and $f(m, rn) = g(m)(rn) = rg(m)(n) = rf(m, n)$. By Universal property $\tilde{f}$ is well defined map such that $\tilde{f} \circ \pi = f$ and $\tilde{f} = \phi(g)$. Now it is easy to show that $\phi \circ \psi = \mathrm{id}_{\mathrm{Hom}_R(M \otimes_R N, P)}$ and $\psi \circ \phi = \mathrm{id}_{\mathrm{Hom}_R(M, \mathrm{Hom}_R(N,P))}$. □

Theorem 14.58. *Let B be an A algebra, M be an $A-$module and N, P be B modules. Then*

$$Hom_B(M \otimes_A N, P) \cong Hom_A(M, Hom_B(N, P)).$$

Proof. Note that $\mathrm{Hom}_A(M, \mathrm{Hom}_B(N, P))$ is an $B-$module,

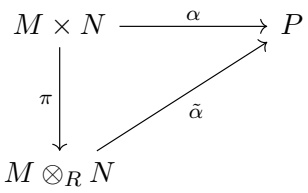
$$B \times \mathrm{Hom}_A(M, \mathrm{Hom}_B(N, P)) \to \mathrm{Hom}_A(M, \mathrm{Hom}_B(N, P))$$
$$(b, f) \mapsto (bf)$$

where $(bf) : M \to \mathrm{Hom}_B(N, P)$ is defined by $(bf)(m) := b \cdot (f(m))$.

Now, we define

$$\theta : \mathrm{Hom}_A(M, \mathrm{Hom}_B(N, P)) \to \mathrm{Hom}_B(M \otimes_A N, P)$$

where $\theta(f)(m \otimes n) = f(m)(n)$. We will show that $\theta(f)$ is well defined.



Where $\alpha(m,n) = f(m)(n)$. We claim that α is $A-$linear in first component and $B-$linear in second component. Let $m_1, m_2 \in M$ and $m \in N$, $\alpha(m_1 + m_2, n) = f(m_1 + m_2)(n) = f(m_1)(n) + f(m_2)(n) = \alpha(m_1, n) + \alpha(m_2, n)$. Let $m \in M, n_1, n_2 \in N$ then $\alpha(m, n_1 + n_2) = f(m)(n_1 + n_2) = f(m)(n_1) + f(m)(n_2) = \alpha(m, n_1) + \alpha(m, n_2)$. Now, for all $a \in A, m \in M, n \in N$, $\alpha(am, n) =$

$f(am,n) = af(m)(n) = a\alpha(m,n)$ and for all $b \in B, m \in M, n \in N$, $\alpha(m,bn) = f(m)(bn) = bf(m)(n) = b\alpha(m,n)$. Hence α is $A-$linear in first component and $B-$linear in second component. Hence $\theta(f)$ is a well defined $B-$linear map. Let

$$\psi : \mathrm{Hom}_B\left(M \otimes_A N, P\right) \to \mathrm{Hom}_A\left(M, \mathrm{Hom}_B\left(N,P\right)\right)$$
$$g \mapsto \psi(g)$$

where $\psi(g) : M \to \mathrm{Hom}_B\left(N,P\right)$ is the map $\psi(g)(m)(n) = g(m \otimes n)$. It is easy to show that ψ is a $B-$linear map and $\psi \circ \theta = \mathrm{id}_{\mathrm{Hom}_A(M,\mathrm{Hom}_B(N,P))}$ and $\theta \circ \psi = \mathrm{id}_{\mathrm{Hom}_B(M\otimes_A N,P)}$. □

Corollary 14.59. *Let*

$$0 \to M' \to M \to M'' \to 0 \tag{11}$$

be an exact sequence of $R-$modules. Let N be another $R-$module then the sequence

$$M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0 \tag{12}$$

is exact.

Proof. Let P be any $R-$module. Since (11) is exact, the sequence

$$\mathrm{Hom}_R\left(M'', \mathrm{Hom}_R\left(N,P\right)\right) \to \mathrm{Hom}_R\left(M, \mathrm{Hom}_R\left(N,P\right)\right) \to \mathrm{Hom}_R\left(M', \mathrm{Hom}_R\left(N,P\right)\right) \to 0 \tag{13}$$

is exact and by Theorem 14.53 we have

$$\mathrm{Hom}_R\left(M'' \otimes_R N, P\right) \to \mathrm{Hom}_R\left(M \otimes_R N, P\right) \to \mathrm{Hom}_R\left(M' \otimes_R N, P\right) \to 0$$

is exact. Hence we have (12). □

14.10.1. *Flat module.*

Definition 14.60. *A module N is said to be flat $R-$module if for every short exact sequence of $R-$modules*

$$0 \to M' \to M \to M'' \to 0$$

we have the following short exact sequence

$$0 \to M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0.$$

Remark 14.61.

(1) *An R-mdoule N is said to be flat if and only if for every short exact sequence*

$$0 \to M' \to M \to M'' \to 0$$

of $R-$modules, we have the following exact sequence

$$0 \to M' \otimes_R N \to M \otimes_R N.$$

(2) *An $R-$module N is said to be flat if for every exact sequence*

$$\sum \equiv \cdots \to M_i \to M_{i+1} \to M_{i+2} \to \cdots$$

of $R-$modules, we have the following exact sequence

$$\sum \otimes_R N \equiv \cdots \to M_i \otimes_R N \to M_{i+1} \otimes_R N \to M_{i+2} \otimes_R N \to \cdots .$$

Definition 14.62. *An $R-$module N is said to be faithfully flat module if it is a flat module and any sequence of*

$$\sum \equiv \cdots \to M_i \to M_{i+1} \to M_{i+2} \to \cdots$$

of $R-$modules, $\sum \otimes_R N$ is exact implies $\sum$ is an exact sequence.

Definition 14.63. *Let S be an $R-$algebra. S is said to be flat over R if S is a flat $R-$module.*

Example 14.64. *Let S be a multiplicatively closed set of a ring R then $S^{-1}R$ is a flat $R-$module.*

Question 14.65. *Let I be an ideal of R. Is R/I flat?*

Lemma 14.66. *Let M, N be flat $R-$modules then $M \otimes_R N$ and $M \oplus N$ is also flat.*

Proof. (1) Let

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

be an exact sequence of $R-$modules, since M is flat, the following sequence

$$0 \to M_1 \otimes_R M \to M_2 \otimes_R M \to M_3 \otimes_R M \to 0$$

is exact and so the sequence

$$0 \to (M_1 \otimes_R M) \otimes_R N \to (M_2 \otimes_R M) \otimes_R N \to (M_3 \otimes_R M) \otimes_R N \to 0.$$

Hence

$$0 \to M_1 \otimes_R (M \otimes_R N) \to M_2 \otimes_R (M \otimes_R N) \to M_3 \otimes_R (M \otimes_R N) \to 0$$

is exact. Therefore, $M \otimes_R N$ is flat.

(2) Since M and N are flat the sequences

$$0 \to M_1 \otimes_R M \xrightarrow{\alpha_M} M_2 \otimes_R M \xrightarrow{\beta_M} M_3 \otimes_R M \to 0$$

and

$$0 \to M_1 \otimes_R N \xrightarrow{\alpha_N} M_2 \otimes_R N \xrightarrow{\beta_N} M_3 \otimes_R N \to 0$$

are exact. Therefore the sequence

$$0 \to M_1 \otimes_R M \oplus M_1 \otimes N \xrightarrow{(\alpha_M, \alpha_N)} M_2 \otimes_R M \oplus M_2 \otimes N \xrightarrow{(\beta_M, \beta_N)} M_3 \otimes_R M \oplus M_3 \otimes N \to 0$$

is exact. So we have the following exact sequence,

$$0 \to M_1 \otimes_R (M \oplus N) \to M_2 \otimes_R (M \oplus N) \to M_3 \otimes_R (M \oplus N) \to 0.$$

Hence $M \oplus N$ is a flat $R-$module.

□

Remark 14.67. *Let S be a flat $R-$ algebra and N be a flat $S-$module. Then N is a flat $R-$module.*

Proof. Let

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

be an exact sequence of $R-$modules. Since S is flat $R-$module,

$$0 \to M_1 \otimes_R S \to M_2 \otimes_R S \to M_3 \otimes_R S \to 0$$

is an exact sequence of $R-$module. Since S is an $R-$algebra, each $M_i \otimes_R S, 1 \leq i \leq 3$ also has $S-$module structure. So the above sequence is an exact sequence of $S-$module. Since N is flat $S-$module,

$$0 \to (M_1 \otimes_R S) \otimes_S N \to (M_2 \otimes_R S) \otimes_S N \to (M_3 \otimes_R S) \otimes_S N \to 0$$

is exact and so the sequences are

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 \otimes_R (S \otimes_S N) & \longrightarrow & M_2 \otimes_R (S \otimes_S N) & \longrightarrow & M_3 \otimes_R (S \otimes_S N) & \longrightarrow & 0 \\ & & \wr\!\!\downarrow & & \wr\!\!\downarrow & & \wr\!\!\downarrow & & \\ 0 & \longrightarrow & M_1 \otimes_R N & \longrightarrow & M_2 \otimes_R N & \longrightarrow & M_3 \otimes_R N & \longrightarrow & 0 \end{array}$$

therefore, N is a flat $R-$module. □

Theorem 14.68. *Let M and N be two $S^{-1}R$ modules, then M, N are also $R-$modules via $\psi : R \to S^{-1}R$. Then $M \otimes_{S^{-1}R} N \cong M \otimes_R N$.*

Proof. We note that $M \otimes_R N$ is an $S^{-1}R-$module. We will show that $M \otimes_R N$ and $M \otimes_{S^{-1}R} N$ is same as $S^{-1}R-$module, hence they are same as $R-$module also. In $M \otimes_R N$,

$$\frac{a}{s}(m \otimes n) = \frac{am}{s} \otimes n = \frac{am}{s} \otimes \frac{ns}{s} = \frac{sm}{s} \otimes \frac{an}{s} = m \otimes \frac{an}{s}.$$

Thus $\frac{a}{s}m \otimes n = m \otimes \frac{an}{s}$ in $M \otimes_R N$. So they are same as $S^{-1}R-$module. □

Theorem 14.69. *Let S be an $R-$algebra and M be an $S-$module. A necessary and sufficient condition for M to be flat over R is that for every $p \in spec\, S$, M_p is flat R_q-module where $q = p \cap R$.*

Proof. First we note that M_p is an R_q module. As S is an $R-$algebra, there exists $f : R \to S$ and $f(p) \subseteq q$ then by Universal property of localization there exists an unique morphism $f_p : R_q \to S_p$ to make S_p an R_q-algebra. Now $S_p \otimes_S M \cong M_p$. Thus M_p is an S_p-module hence M_p is an A_q-module. Suppose M is flat. Consider the exact sequence of R_q-modules (also as $R-$modules)

$$0 \to M_1 \to M_2 \to M_3 \to 0 \tag{14}$$

By previous theorem,

$$M_p \otimes_{R_q} M_i \cong M_p \otimes_R M_i, 1 \leq i \leq 3. \tag{15}$$

Now From (14)

$$0 \to M_1 \otimes_R M \to M_2 \otimes_R M \to M_3 \otimes_R M \to 0$$

is an exact sequence of $S-$mdoule (since M is an $S-$module). As S_p is flat over S we have the following exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (M_1 \otimes_R M) \otimes_S S_p & \longrightarrow & (M_2 \otimes_R M) \otimes_S S_p & \longrightarrow & (M_3 \otimes_R M) \otimes_S S_p & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \\
0 & \longrightarrow & M_1 \otimes_R (M \otimes_S S_p) & \longrightarrow & M_2 \otimes_R (M \otimes_S S_p) & \longrightarrow & M_3 \otimes_R (M \otimes_S S_p) & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \\
0 & \longrightarrow & M_1 \otimes_R M_p & \longrightarrow & M_2 \otimes_R M_p & \longrightarrow & M_3 \otimes_R M_p & \longrightarrow & 0
\end{array}$$

From (15) we have the following exact sequence

$$0 \to M_1 \otimes_{R_q} M_p \to M_2 \otimes_{R_q} M_p \to M_3 \otimes_{R_q} M_p \to 0.$$

Thus M_p is a flat R_q module.

Conversely, let M_p be flat over R_q for all $p \in \operatorname{spec} S$ and $q = p \cap R$. Consider the exact sequence of $R-$modules $0 \to N' \xrightarrow{\phi} N$ then

$$0 \to \operatorname{Ker}(\phi \otimes 1) \xrightarrow{i} N' \otimes_R M \xrightarrow{\phi \otimes 1} N \otimes_R M$$

where $\operatorname{Ker}(\phi \otimes 1), N' \otimes_R M$ and $N \otimes_R M$ are $S-$modules and S_p is flat over S. Thus we have the exact sequence

$$\begin{array}{ccccccc}
0 & \longrightarrow & (\operatorname{Ker}(\phi \otimes 1)) \otimes_S S_p & \longrightarrow & (N' \otimes_R M) \otimes_S S_p & \longrightarrow & (N \otimes_R M) \otimes_S S_p \text{ is exact} \\
 & & \| & & \| & & \| \\
0 & \longrightarrow & (\operatorname{Ker}(\phi \otimes 1))_p & \longrightarrow & N' \otimes_R (M \otimes_S S_p) & \longrightarrow & N \otimes_R (M \otimes_S S_p) \text{ is exact} \\
 & & \| & & \| & & \| \\
0 & \longrightarrow & (\operatorname{Ker}(\phi \otimes 1))_p & \longrightarrow & N' \otimes_R M_p & \longrightarrow & N \otimes_R M_p \text{ is exact} \\
 & & \| & & \| & & \| \\
0 & \longrightarrow & (\operatorname{Ker}(\phi \otimes 1))_p & \longrightarrow & N' \otimes_R (R_q \otimes_{R_q} M_p) & \longrightarrow & N \otimes_R (R_q \otimes_{R_q} M_p) \text{ is exact} \\
 & & \| & & \| & & \| \\
0 & \longrightarrow & (\operatorname{Ker}(\phi \otimes 1))_p & \longrightarrow & (N' \otimes_R R_q) \otimes_{R_q} M_p & \longrightarrow & (N \otimes_R R_q) \otimes_{R_q} M_p \text{ is exact} \\
 & & \| & & \| & & \| \\
0 & \longrightarrow & (\operatorname{Ker}(\phi \otimes 1))_p & \longrightarrow & N'_q \otimes_{R_q} M_p & \longrightarrow & N_q \otimes_{R_q} M_p \text{ is exact}
\end{array}$$

Again we have the exact sequence $0 \to N_q \to N_q$, since R_q is flat over R. As M_p is flat over R_q, the following sequence

$$0 \to N'_q \otimes_{R_q} M_p \to N_q \otimes_{R_q} M_p$$

is exact. Therefore, $(\operatorname{Ker}(\phi \otimes 1))_p = 0$ for all $p \in \operatorname{spec} S$. By Local-global property, $\operatorname{Ker}(\phi \otimes 1) = 0$. So the sequence $0 \to N' \otimes_R M \to N \otimes_R M$ is exact. □

Lemma 14.70. *Let M be an $R-$module. For $p \in \operatorname{maxspec} R$, we have the map $\theta_p : M \to M_p$ given by $m \mapsto \frac{m}{1}$. Let $x \in M$ such that $\theta_p(x) = 0$ for all $p \in \operatorname{maxspec} R$ then $x = 0$.*

Proof. Let $x \neq 0$ then $\mathrm{Ann}_R(x) \neq R$ so there exists $m \in \mathrm{maxspec}\, R$ such that $\mathrm{Ann}_R(x) \subseteq m$. Consider the map $\theta_m : M \to M_m$. Since $\theta_m(x) = 0 \Rightarrow \dfrac{x}{1} = \dfrac{0}{1} \Rightarrow u(x \cdot 1 - 0 \cdot 1) = 0 \Rightarrow ux = 0 \Rightarrow u \in \mathrm{Ann}_R(x)$ which is a contradiction. Hence $x = 0$. □

Theorem 14.71 (Local-global property)**.** *Let M be an $R-$module. Then the followings are equivalent:*

(1) $M = 0$.
(2) $M_p = 0$ *for all* $p \in \mathrm{spec}\, R$.
(3) $M_m = 0$ *for all* $m \in \mathrm{maxspec}\, R$.

Proof. (3) $\Rightarrow$ (1) □

Lemma 14.72. *Let $N \subseteq M$ be an $R-$module and P be a flat $R-$module. Then* $\dfrac{M \otimes_R P}{N \otimes_R P} \cong M/N \otimes_R P$.

Proof. Consider the exact sequence $0 \to N \to M \to M/N \to 0$. Since P is flat, the resulting sequence

$$0 \to N \otimes_R P \to M \otimes_R P \to M/N \otimes_R P \to 0$$

is exact. □

Corollary 14.73. *Let M, N be $R-$modules and $f \in \mathrm{Hom}_R(M, N)$. Then the followings are equivalent.*

(1) *f is injective (surjective).*
(2) *f_p is injective (surjective) for all $p \in \mathrm{spec}\, R$.*
(3) *f_m is injective (surjective) for all $m \in \mathrm{maxspec}\, R$.*

Proof. □

14.11. **Projective module.**

Theorem 14.74. *Let P be an $R-$module. Then the followings are equivalent:*

(1) *$\mathrm{Hom}_R(P, -)$ is an exact functor that is given any exact sequence of $R-$modules,*

$$0 \to M' \to M \to M'' \to 0$$

the sequence

$$0 \to \mathrm{Hom}_R\left(P, M'\right) \to \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R\left(P, M''\right) \to 0 \tag{16}$$

is exact.

(2) *Given*

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle \psi} & & \\ M & \xrightarrow{g} & M'' & \longrightarrow & 0 \end{array}$$

we have $\phi : P \to M$ such that the diagram commutes that is $g \circ \phi = \psi$.

$$\begin{array}{ccccc} & & & & P \\ & & \overset{\phi}{\swarrow} & & \downarrow \psi \\ M & \xrightarrow{g} & M'' & \longrightarrow & 0 \end{array}$$

(3) *There exist an $R-$module Q such that $P \oplus Q$ is free.*

(4) *For any epimorphism $f : M \to P$, there exists $s : P \to M$ such that $f \circ s = id_P$.*

Proof. (1) $\Rightarrow$ (2) Since (16) is exact $g_*(\alpha) = \beta \Rightarrow g \circ \alpha = \beta$. Take $\alpha = \phi$ and $\beta = \psi$.

(2) $\Rightarrow$ (1) We just need to show that g_* is surjective. Let $\gamma \in \mathrm{Hom}_R(P, M'')$. By (2) there exists $\phi \in \mathrm{Hom}_R(P, M)$ such that $g \circ \phi = \gamma \Rightarrow g_*(\phi) = \gamma$.

(2) $\Rightarrow$ (3) Given P, there exists a free module F and a surjective map $f : F \to P$.

$$\begin{array}{ccccccccc} & & & & & & P & & \\ & & & & & \overset{g}{\swarrow} & \downarrow \mathrm{id} & & \\ 0 & \longrightarrow & \mathrm{Ker}\, f & \longrightarrow & F & \xrightarrow{f} & P & \longrightarrow & 0 \end{array}$$

Since $f \circ g = \mathrm{id}_P$ the above sequence is split exact. Hence $F = P \oplus \mathrm{Ker}\, f$. So $Q = \mathrm{Ker}\, f$ is the desired module.

(3) $\Rightarrow$ (2) Consider the diagram

$$\begin{array}{ccccc} & & F & & \\ & & \downarrow \pi & & \\ & \overset{\tilde{\alpha}}{\swarrow} & P & & \\ & & \downarrow \psi & & \\ M & \xrightarrow{g} & M'' & \longrightarrow & 0 \end{array}$$

Let $S \subseteq F$ be a basis, define $\alpha : S \to M$ given by $\alpha(x) = \tau_x$ where $\tau_x \in g^{-1}(\psi \circ (x))$ is a fixed element. Then there exists $\tilde{\alpha} : F \to M$ such that $\tilde{\alpha} \circ g = \psi \circ \pi$. Then $\tilde{\alpha}|_P : P \to M$ is the required map.

(2) $\Rightarrow$ (4) Obvious.

(4) $\Rightarrow$ (3) Given P, there exists a free module F and $f : F \to P$ is a surjection. Then there is also a map $s : P \to F$ such that $f \circ s = \mathrm{id}_P$. Since the following sequence

$$0 \to \mathrm{Ker}\, f \to F \to P \to 0$$

is split exact, $F \cong P \oplus \mathrm{Ker}\, f$. □

Definition 14.75. *Any $R-$module P which satisfies any one of the above condition is called projective module.*

Remark 14.76. *Any free module F is projective since $F = F \oplus 0$. But converse is not true. Let $R = \mathbb{Z}/6\mathbb{Z}$ and $P = \mathbb{Z}/3\mathbb{Z}$. Note that P is an $R-$module, take $Q = \mathbb{Z}/2\mathbb{Z}$. Then $P \oplus Q = R$ hence P is a projective module over R but P is not free. If P is free R module then $\mathbb{Z}/3\mathbb{Z} \cong (\mathbb{Z}/6\mathbb{Z})^{|S|}$ where S is a basis of P. Therefore $3 = |\mathbb{Z}/3\mathbb{Z}| = |S||\mathbb{Z}/6\mathbb{Z}| = 6|S|$ which is impossible.*

Note 14.77. *Therefore we have the following implication*

$$\textit{Free} \Longrightarrow \textit{Projective} \Longrightarrow \textit{Flat}$$

but the reverse implications are not true. Let F be a free module, then $F \cong \bigoplus_{i\in\Lambda} R_i$ where $R_i = R$ for all $i \in \Lambda$ and

$$0 \to M' \to M \to M'' \to 0 \tag{17}$$

be an exact sequence of $R-$modules. Then we have

$$0 \to M' \otimes_R R_i \to M \otimes_R R_i \to M'' \otimes_R R_i \to 0$$

is an exact sequence of $R-$modules for all $i \in \Lambda$. Hence

$$0 \to \bigoplus_{i\in\Lambda}(M' \otimes_R R_i) \to \bigoplus_{i\in\Lambda}(M \otimes_R R_i) \to \bigoplus_{i\in\Lambda}(M'' \otimes_R R_i) \to 0$$

is exact. Therefore

$$0 \to M' \otimes_R F \to M \otimes_R F \to M'' \otimes_R F \to 0$$

is exact that is F is a flat module. Now let P be a projective module then there exist an $R-$module Q such that $P \oplus Q$ is free. By previous result we have

$$0 \to (M' \otimes_R P) \oplus (M' \otimes_R Q) \to (M \otimes_R P) \oplus (M \otimes_R Q) \to (M'' \otimes_R P) \oplus (M'' \otimes_R Q) \to 0$$

is exact. Therefore

$$0 \to M' \otimes_R P \to M \otimes_R P \to M'' \otimes_R P \to 0$$

is exact and P is flat. Note that $\mathbb{Q}$ is flat $\mathbb{Z}$ module since $\mathbb{Q} = S^{-1}\mathbb{Z}$ where $S = \mathbb{Z} \setminus \{0\}$ but $\mathbb{Q}$ is not projective. Suppose $\mathbb{Q}$ is projective $\mathbb{Z}-$module then $\mathbb{Q}$ is a free $\mathbb{Z}-$module which is a contradiction.

Definition 14.78. *Let $R-$ be a ring.n A projective module is said to be stably free if there exists a free module Q such that $P \oplus Q$ is free.*

Example 14.79. (1) *Any free module.*

Question 14.80. *Give an example of a module M and a free module F such that $F \oplus M \cong M$.*

Ans. Let $F = R^n$, $M = \bigoplus_{i\in\mathbb{N}} R_i$ where $R_i = F^n$ for all $i \in \mathbb{N}$.

Theorem 14.81. *Let (R, m) be a local ring. Then any finitely generated projective $R-$module P is free over R.*

Proof. Let $S \subseteq P$ be a minimal generating set. Let $S = \{x_1, \cdots, x_n\}$ then $\overline{S} = \{x_1 + mP, \cdots, x_n + mP\}$ is the basis of P/mP over R/m. Since $P = \langle S\rangle$ there exists a surjective map $\phi : R^n \to P$. Consider the exact sequence

$$0 \to \operatorname{Ker}\phi \xrightarrow{i} R^n \xrightarrow{\phi} P \to 0. \tag{18}$$

Then we have

$$\begin{array}{ccccccc}
\operatorname{Ker}\phi \otimes_R R/m & \xrightarrow{\tilde{i}} & R^n \otimes_R R/m & \xrightarrow{\tilde{\phi}} & P \otimes_R R/m & \longrightarrow & 0 \\
\| & & \| & & \| & & \\
\dfrac{\operatorname{Ker}\phi}{m\operatorname{Ker}\phi} & \xrightarrow{\tilde{i}} & (R/m)^n & \xrightarrow{\tilde{\phi}} & P/mP & \longrightarrow & 0
\end{array}$$

Since $\dim(R/m)^n = n = \dim P/mP$, $\tilde{\phi}$ is an isomorphism $\dfrac{\operatorname{Ker}\phi}{m\operatorname{Ker}\phi} = 0$. Since P is projective (17) is split exact. Therefore $R^n \cong \operatorname{Ker}\phi \oplus P$ and hence $\operatorname{Ker}\phi$ is finitely generated. By NAK, $\operatorname{Ker}\phi = 0$. Hence P is free. □

Proposition 14.82. *Let R be a commutative ring with 1 and $\phi : R^k \to R^n$ be an endomorphism. Then $n \leq k$.*

Proof. Let $m \in \operatorname{maxspec} R$. Consider the exact sequence

$$0 \to \operatorname{Ker}\phi \xrightarrow{i} R^k \xrightarrow{\phi} R^n \to 0. \tag{19}$$

of $R-$ modules. We have

$$\begin{array}{ccccccc}
\operatorname{Ker}\phi \otimes_R R/m & \xrightarrow{\tilde{i}} & R^k \otimes_R R/m & \xrightarrow{\tilde{\phi}} & R^n \otimes_R R/m & \longrightarrow & 0 \\
\| & & \| & & \| & & \\
\operatorname{Ker}\phi \otimes_R R/m & \xrightarrow{\tilde{i}} & (R/m)^k & \xrightarrow{\tilde{\phi}} & (R/m)^n & \longrightarrow & 0
\end{array}$$

Since $(R/m)^k$ is vector space over R/m and the map $\tilde{\phi}$ is onto, by Rank-Nullity theorem $n \leq k$. □

Theorem 14.83. *Let R be a commutative ring with 1 such that $R^m \cong R^n$ then $m = n$.*

Proof. Let $\psi : R^m \to R^n$ be the isomorphism then there exists $\phi : R^n \to R^m$ such that $\phi \circ \psi = \mathrm{id}_{R^m}$ and $\psi \circ \phi = \mathrm{id}_{R^n}$. Since ψ is onto, $n \leq m$ and ϕ is onto implies $m \leq n$. Hence $m = n$. □

For a commutative ring R with 1, we define rank $R^n = n$. For a finitely generated free module F, there exists $n \in \mathbb{R}$ such that $F \cong R^n$. So we define rank $F = n$. Let P be a finitely generated projective module over R. Define rank : $\operatorname{spec} R \to P$ given by $p \mapsto \operatorname{rank}(P_p)$.

Note 14.84. *Let P be a projective module, then there exists Q such that $P \oplus Q \cong F$ where F is a free module. Let $p \in \operatorname{spec} R$. then $(P \oplus Q) \otimes_R R_p \cong F \otimes_R R_p \Rightarrow P_p \otimes_R Q_p \cong F_p$. Since P_p is a finitely generated over a local ring in R_p, and F_p is free R_p module, therefore P_p is projective R_p module and hence P_p is free over R_p. So rank (P_p) is well defined. Note that if R is local then the rank function is constant.*

Theorem 14.85. *Let R be a semi local ring and P be a finitely generated projective module over R of constant rank then P is free.*

Proof. Let $\operatorname{maxspec} R = \{m_1, \cdots, m_r\}$ and $J = \bigcap_{i=1}^{r} m_i$ be the Jacobson radical. By Chinese Remainder theorem $P/JP \cong P/m_1P \times \cdots \times P/m_rP$ and $R/J \cong R/m_1 \times \cdots \times R/m_r$ and P/JP is R/J module. Let $S = \{s_1, \cdots, s_k\}$ be a minimal generating set of P over R. We claim that $\overline{S} = \{s_1 + JP, \cdots, s_k + JP\}$ be the minimal generating set of P/JP over R/J. If not, we assume that P/JP is generated by $\{s_1 + JP, \cdots, s_{k-1} + JP\}$. Let $N = \langle s_1, \cdots, s_{k-1}\rangle$. Pick $x \in P$ then $x + JP = \sum_{i=1}^{k-1}(r_i + J)(s_i + JP) \Rightarrow x - \sum_{i=1}^{k-1} r_i s_i \in JP \Rightarrow x \in N + JP \Rightarrow P = N + JP$. By NAK,

$P = N$ which is a contradiction. So our claim is proved. Thus P/JP is free R/J module. Now we consider the exact sequence

$$0 \to \operatorname{Ker} f \to R^k \to P \to 0. \tag{20}$$

Since P is projective, this above sequence is split exact and therefore $\operatorname{Ker} f$ is finitely generated. From (19)

$$\begin{array}{ccccccc} \operatorname{Ker} f \otimes_R R/J & \xrightarrow{i\otimes 1} & R^k \otimes_R R/J & \xrightarrow{f\otimes 1} & P \otimes_R R/J & \longrightarrow & 0 \\ \| & & \| & & \| & & \\ \dfrac{\operatorname{Ker} f}{J \operatorname{Ker} f} & \xrightarrow{i\otimes 1} & (R/J)^k & \xrightarrow{f\otimes 1} & P/JP & \longrightarrow & 0 \end{array}$$

We claim that $\{s_1 + JP, \cdots, s_k + JP\}$ is a R/J basis of P/JP. If we prove the claim then $f \otimes 1$ is an isomorphism and $\operatorname{Ker} f / J \operatorname{Ker} f = 0 \Rightarrow \operatorname{Ker} f = 0$ by NAK and $P \cong R^k$ hence P is free.

Proof of the claim.

Note 14.86. *Let F_i be free R_i module of same rank for all $1 \le i \le k$, then $F = F_1 \times \cdots \times F_k$ is free $R_1 \times \cdots \times R_k$ module. That is $F_i \cong (R_i)^l$ for some $l \in \mathbb{N}, 1 \le i \le n$. Then $F = F_1 \times \cdots \times F_k \cong (R_1)^l \times \cdots \times (R_k)^l \cong (R_1 \times \cdots \times R_k)^l$. We will prove this by induction on k. Let $\theta : R_1^l \times R_2^l \to (R_1 \times R_2)^l$ defined by $((x_1, \cdots, x_l), (x_1', \cdots, x_l')) \mapsto ((x_1, x_1'), \cdots, (x_l, x_l'))$ be the required isomorphism.*

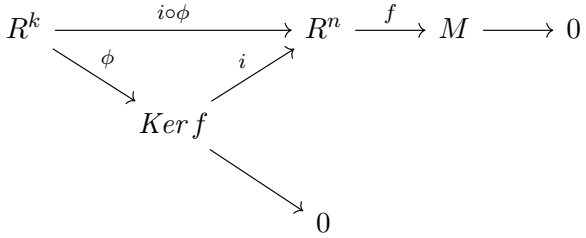
Note 14.87. *Since P is projective of constant rank, let $P_m \cong (R_m)^l$ for all $m \in mspec R$ and for some $l \in \mathbb{N}$. Let $P/mP \cong (R/m)^s$ for some $s \in \mathbb{N}$. Then $P/mP \otimes_R R_m \cong (R/m)^s \otimes_R R_m \Rightarrow \dfrac{P_m}{mP_m} \cong \left(\dfrac{R_m}{mR_m}\right)^s \cong \left(\dfrac{R_m}{mR_m}\right)^l \Rightarrow l = s$. Hence for any $m \in maxspec\, R$, $P/mP \cong (R/m)^l$. Therefore $P/JP \cong \prod_{i=1}^r P/m_i P \cong \prod_{i=1}^r (R/m_i)^l \cong \left(\prod_{i=1}^r R/m_i\right)^l \cong (R/J)^l$.*

Question 14.88. *Let R be a semi local ring and F be a finitely generated free module over R. Is any minimal generating set of F an $R-$basis of F?.*

Definition 14.89. *Let M be an $R-$module. M is said to be finitely presented if there exists finitely generated free modules F_1 and F_2 such that the following sequence is exact*

$$F_1 \to F_2 \to M \to 0.$$

Note 14.90. *Suppose M is a finitely generated module over R. If $Ker\, f$ is finitely generated then we have the following sequence*



is exact because $Ker\,\phi = Im\,\phi = Im(i \circ \phi)$. *Thus a finitely generated module may not be finitely presented. If* R *is Noetherian then it is true. Conversely any finitely presented module is finitely generated.*

Theorem 14.91. *Let* R *be a ring and* M, N *be* $R-$*modules and* S *be a flat* $R-$*algebra. Suppose* M *is of finite presentation then we have*

$$Hom_R(M,N) \otimes_R S \cong Hom_S(M \otimes_R S, N \otimes_R S).$$

Proof. Since M is of finite presentation, there exists two finitely generated free module R^p and R^q such that

$$R^p \to R^q \to M \to 0 \tag{21}$$

is exact. Then for any $R-$module N the following sequence

$$0 \to \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(R^q,N) \to \mathrm{Hom}_R(R^p,N) \tag{22}$$

is exact. As S is flat,

$$0 \to \mathrm{Hom}_R(M,N) \otimes_R S \to \mathrm{Hom}_R(R^q,N) \otimes_R S \to \mathrm{Hom}_R(R^p,N) \otimes_R S$$

is exact. Now consider the diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_R(M,N) \otimes_R S & \longrightarrow & \mathrm{Hom}_R(R^q,N) \otimes_R S & \longrightarrow & \mathrm{Hom}_R(R^p,N) \otimes_R S \\
 & & \downarrow \lambda_M & & \downarrow \lambda_{R^q} & & \downarrow \lambda_{R^p} \\
0 & \longrightarrow & \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S) & \longrightarrow & \mathrm{Hom}_S(R^q \otimes_R S, N \otimes_R S) & \longrightarrow & \mathrm{Hom}_S(R^p \otimes_R S, N \otimes_R S)
\end{array}$$

where $\lambda_M : \mathrm{Hom}_R(M,N) \otimes_R S \to \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)$ is defined by $\lambda_M(f \otimes s) = \tilde{f}$ and $\tilde{f} : M \otimes_R S \to N \otimes_R S$ is defined by $\tilde{f}(m \otimes s) = f(m) \otimes s$. By Universal property $\tilde{f}$ is well defined. Since $\mathrm{Hom}_R(R^q,N) \otimes_R S \cong (\mathrm{Hom}_R(R,N))^q \otimes S \cong N^q \otimes S = (N \otimes_R S)^q$ and $\mathrm{Hom}_S(R^q \otimes_R S, N \otimes_R S) \cong \mathrm{Hom}_S(S^q, N \otimes_R S) \cong (N \otimes_R S)^q$. Thus the mappings λ_{R^q} and λ_{R^p} are isomorphism. Since the bottom sequence of the above diagram is exact and the diagram ia commutative, λ_M is also an isomorphism. □

Corollary 14.92. *Let* M *and* N *be* $R-$*modules with* M *be of finite presentation. Then for each* $p \in spec\,R$,

$$(Hom_R(M,N))_p \cong Hom_{R^p}(M_p, N_p).$$

Proof. Take $S = R_p$. □

Theorem 14.93. *Let* R *be any ring and* M *be a finitely presented. Then the followings are equivalent:*

1. *The map* $\theta : M \otimes_R M^* \to R$ *defined by* $\theta(m,f) = f(m)$ *is an isomorphism.*
2. *There exists an* $R-$*module* N *such that* $M \otimes_R N \cong R$.
3. $M_m \cong R_m$ *for all* $m \in maxspec\,R$.
4. $M_p \cong R_p$ *for all* $p \in spec\,R$.
5. M *is projective of rank 1.*

Proof. (1) $\Rightarrow$ (2) Take $N = M^*$.
(2) $\Rightarrow$ (3) $M \otimes_R N \cong R \Rightarrow M_m \otimes_R N_m \cong R_m \Rightarrow M_m \otimes_{R_m} N_m \cong R_m \Rightarrow (M_m \otimes_{R_m} N_m) \otimes_{R_m} \frac{R_m}{mR_m} \cong \frac{R_m}{mR_m} \Rightarrow M_m \otimes_{R_m} \frac{N_m}{mN_m} \cong \frac{R_m}{mR_m} \Rightarrow \frac{M_m}{mR_m} \otimes_{R_m} \frac{N_m}{mN_m} \cong \frac{R_m}{mR_m}$[1]. Therefore, $\frac{M_m}{mM_m} \cong \frac{R_m}{mR_m}$. By NAK $M_m = \langle x \rangle, x \in M_m \Rightarrow M_m \cong \frac{R_m}{Ann_{R_m}(x)} \Rightarrow Ann_{R_m}(x)(M_m \otimes_{R_m} N_m) = 0 \Rightarrow Ann_{R_m}(x)R_m = 0 \Rightarrow Ann_{R_m}(x) = 0 \Rightarrow M_m = R_m$.

(3) $\Rightarrow$ (4) Further localization.

(4) $\Rightarrow$ (5) By definition.

(5) $\Rightarrow$ (1) Since M is of finite presentation, $(\mathrm{Hom}_R(M, R))_m \cong \mathrm{Hom}_{R_m}(M_m, R_m)$ for all $m \in \mathrm{maxspec}\, R$, that is $(M^*)_m \cong (M_m)^*$. Now M is projective of rank 1 so $M_m \cong R_m$. So we have $M_m \otimes_{R_m} (M_m)^* \cong R_m \otimes_{R_m} (R_m)^* \cong R_m$. Again from the above equation,

$$\begin{aligned} M_m \otimes_{R_m} (M_m)^* &\cong M_m \otimes_{R_m} (M^*)_m \\ &\cong M_m \otimes_R (M^*)_m \\ &\cong M_m \otimes_R (M^* \otimes_R R_m) \\ &\cong (M \otimes_R R_m) \otimes_R (M^* \otimes_R R_m) \\ &\cong (M \otimes_R M^*) \otimes_R (R_m \otimes_R R_m) \\ &\cong (M \otimes_R M^*) \otimes_R R_m \\ &\cong (M \otimes_R M^*)_m \end{aligned}$$

Hence $(M \otimes_R M^*)_m \cong R_m$ for all $m \in \mathrm{maxspec}\, R$. By Local-global property $M \otimes_R M^* \cong R$.

Note 14.94. *Let I and J be two ideals of R then $R/I \otimes_R R/J \cong \frac{R/I}{J(R/I)} \cong \frac{R/I}{(J+I)/I} \cong \frac{R}{I+J}$. (Check this isomorphism as ring.)*

Picard group. Let $\sum$ be the isomorphism classes of projective $R-$modules of rank 1. Define

$$\begin{aligned} \cdot : \sum \times \sum &\to \sum \\ ([P], [Q]) &\mapsto [P \otimes_R Q] \end{aligned}$$

We need to show that $(\sum, \cdot)$ is a group with inverse of $[P]$ is $[P^*]$. This group is called Picard group of R and it is denoted by $Pic\ R$. Let P, Q be two projective module of rank 1 then

$$(P \otimes_R Q) \otimes_R R_m \cong P_m \otimes_R Q_m \cong P_m \otimes_{R_m} Q_m \cong R_m \otimes_{R_m} R_m \cong R_m.$$

Thus $P \otimes_R Q$ is also a projective module of rank 1. By Corollary 14.88 $(M^*)_p \cong (M_p)^* \cong (R_p)^* \cong R_p$ for all $p \in \mathrm{spec}\, R$. Therefore M is projective of rank 1 implies M^* is also projective of rank 1.

Free, Projective and Flat resolution.

[1] As $K(m) := \frac{R_m}{mR_m}$ and $K(m)^l \otimes K(m)^s \cong K(m)^{ls}$.

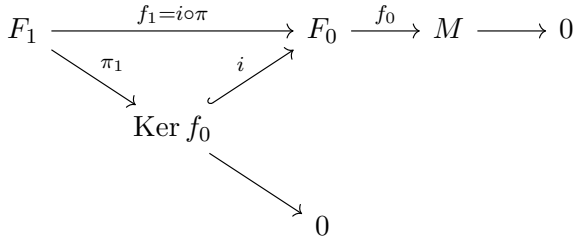
Definition 14.95. *Let M be an $R-$module. A free (or projective or flat) resolution of M over R is an exact sequence of $R-$modules*

$$\cdots \to P_2 \xrightarrow{f_2} P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} M \to 0$$

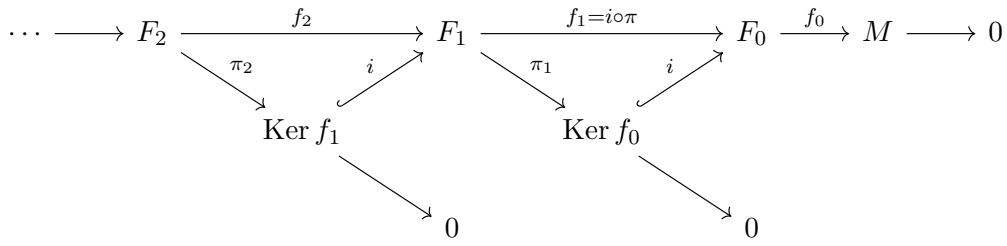
where each P_i is a free (or projective or flat respt.) $R-$module.

Lemma 14.96. *Let M be an $R-$module. Then projective resolution of M over R exists.*

Proof. For any module M, there exists a free module F and a surjective map $F_0 \xrightarrow{f_0} M \to 0$. Consider the $\operatorname{Ker} f_0$, then there exists a free module F_1 with the diagram



The above diagram is exact since $\operatorname{Ker} f_0 = \operatorname{Im} \pi_1 = \operatorname{Im} i \circ \pi_1 = \operatorname{Im} f_1$ since i is the inclusion map and π_1 is onto. Next we consider $\operatorname{Ker} f_1$, then there exists F_2 such that



Inductively we can construct a free resolution of M. Since every free module is projective and therefore flat, we have a projective (or flat) resolution. □

Tor and Ext.

Definition 14.97. *Let M be an $R-$module. We consider a projective resolution of M that is*

$$\mathcal{C} \equiv \cdots \to P_2 \xrightarrow{f_2'} P_1 \xrightarrow{f_1'} P_0 \xrightarrow{f_0'} M \to 0.$$

Let N be another $R-$module. We consider,

(1)

$$\mathcal{C} \otimes_R N \equiv \cdots \to P_2 \otimes_R N \xrightarrow{f_2} P_1 \otimes_R N \xrightarrow{f_1} P_0 \otimes_R N \xrightarrow{f_0} M \otimes_R N \to 0$$

where $f_i = f_i' \otimes 1$ for all $i \in \mathbb{N}$. Then we define $Tor_i^R(M,N) := H_i(\mathcal{C} \otimes_R N) = \dfrac{Ker\, f_i}{Im\, f_{i+1}}$.

(2)

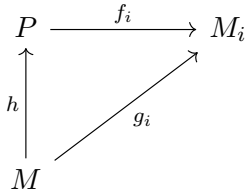
$$Hom_R(\mathcal{C}, N) \equiv \cdots \xleftarrow{f_2^*} Hom_R(P_1, N) \xleftarrow{f_1^*} Hom_R(P_0, N) \xleftarrow{f_0^*} Hom_R(M, N) \leftarrow 0.$$

we define $Ext_R^i(M,N) := H^i(Hom_R(\mathcal{C}, \mathcal{N})) = \dfrac{Ker\, f_{i+1}^*}{Im\, f_i^*}$.

Remark 14.98. *These definition doesn't depend on the choice of resolution of M.*

14.12. **Appendix A.**

Definition 14.99. *Let $\{M_i\}_{i\in I}$ be a family of $R-$module. A product of this family is a pair $(P, \{f\}_{i\in I})$ where P is an $R-$module and $f_i : P \to M_i$ is a morphism for all i such that if we have another pair $(M, \{g_i\}_{i\in I})$ where M is an $R-$module and $g_i : M \to M_i$ is a morphism for all $i \in I$ then there exists unique module homomorphism $h : M \to P$ such that the following diagram commutes i.e., $f_i \circ h = g_i, \forall\ i \in I$.*



Existence of product. We have $\{M_i\}_{i\in I}$ and $P := \prod_{i\in I} M_i = \{(m_i)_{i\in I} : m_i \in M_i\}$ and define addition and multiplication component wise i.e.,

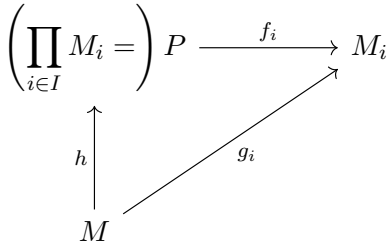
$$(m_i)_{i\in I} + (n_i)_{i\in I} = (m_i + n_i)_{i\in I} \qquad [(m_i)_{i\in I}, (n_i)_{i\in I} \in \prod_{i\in I} M_i]$$

$$r(m_i)_{i\in I} = (rm_i)_{i\in I} \qquad [(m_i)_{i\in I} \in \prod_{i\in I} M_i, r \in R]$$

then P satisfies all module axiom hence P is an $R-$module. Define,

$$P \xrightarrow{f_i} M_i$$
$$(m_i)_{i\in I} \mapsto m_i$$

then its is easy to verify that f_i is a surjective module homomorphism. Now let $(M, \{g_i\}_{i\in I})$ be a pair where M is an $R-$module and $g_i : M \to M_i$ is a morphism for all i.



Now, we need to define the map $h : M \to P$ in such a way that the above diagram commutes so commutitivity of the diagram forces us to define

$$h : M \to P$$
$$m \mapsto (g_i(m))_{i\in I}$$

i.e., $h(m)$ is an element of $\prod_{i\in I} M_i$ whose i^{th} co-ordinate is $g_i(m)$. Hence,

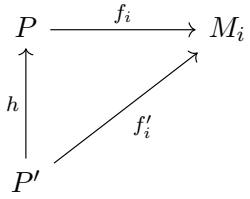
$$(f_i \circ h)(m) = f_i(h(m)) = f_i((g_i(m))_{i\in I}) = g_i(m), \forall\ i \in I$$

Therefore, $f_i \circ h = g_i, \forall\ i \in I$.
Let $h_1 : M \to P$ be another morphism such that $f_i \circ h_1 = g_i, \forall\ i \in I$. Then i^{th} component of $h(m)$

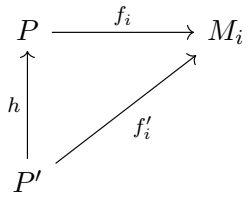
is $f_i(h(m)) = (f_i \circ h)(m) = g_i(m) = (f_1 \circ h_1)(m) = f_i(h_1(m)) = h_1(m), \forall\ m \in M$ hence h is unique.

Uniqueness of product.

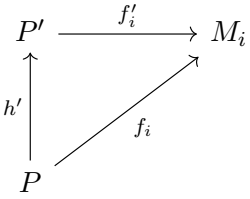
Theorem 14.100. *Let $(P', \{f_i'\}_{i\in I})$ be another product of $\{M_i\}_{i\in I}$ then there exists an unique isomorphism $h' : P' \to P$ such that the following diagram commutes for all i.*



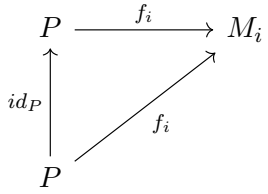
Proof. As $(P, \{f_i\}_{i\in I})$ is a product by definition $\exists!\ h : P \to P$ such that the diagram commutes,

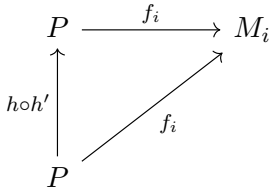


Similarly as $(P', \{f_i'\}_{i\in I})$ is a product then $\exists!\ h' : P \to P'$ such that

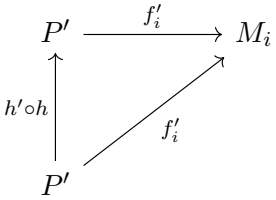


the diagram commutes. Then $f_i' = f_i \circ h$ and $f_i = f_i' \circ h, \forall\ i \in I \Rightarrow f_i = f_i \circ (h \circ h'), \forall\ i \in I$ but





these two diagram also commutes so by the definition of product $id_P = h \circ h'$. Similarly, $f_i' = f_i \circ h = f_i' \circ (h' \circ h)$ then



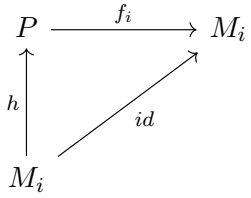
From the above diagram we have $h' \circ h = id_{P'}$. Therefore, h is an isomorphism. □

Exercise 14.101. *Show that if $(P, \{f_i\}_{i\in I})$ exists then each f_i is surjective.*

Proof. Let us take $M = M_i$ and

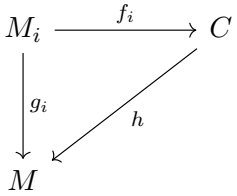
$$g_i : M_i \to M_i \text{ be the indentity map}$$
$$g_j : M_i \to M_j \text{ be the zero map}$$

then we have these tuple $(M_j, \{g_j\})$ and for each i we have



and $f_i \circ h = id \Rightarrow f_i$ is surjective. □

Definition 14.102. *Let $\{M_i\}_{i\in I}$ be a family of $R-$module. A coproduct of this family of this family is a pair $(C, \{f_i\}_{i\in I})$ where C is an $R-$module and $f_i : M_i \to C$ is a morphism for all $i \in I$ such that if there is another pair $(M, \{g_i\}_{i\in I})$ where M is an $R-$module and $g_i : M_i \to M$ is a morphism $\forall\ i \in I$ then there exists a module morphism $h : C \to M$ such that the following diagram commutes for all $i \in I$.*



Existence of coproduct. Recall that we have this $R-$module $\prod_{i\in I} M_i$ and we consider the following set

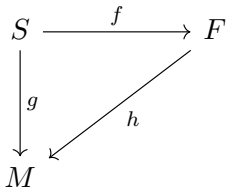
$$C = \{(m_i)_{i\in I} \in \prod_{i\in I} M_i : m_i = 0 \text{ for all but finitely many values of } i\}$$

Then C is a submodule of P. As $(m_i)_{i\in I}, (n_i)_{i\in I} \in C$ then $m_i = 0$ for all but finitely many values of i and $n_j = 0$ for all but finitely many values of i then $(m_i)_{i\in I} + (n_i)_{i\in I} \in C$ as $(m_i) + (n_i) = 0$ for all but finitely many values of i and if we pick any $r \in R$ then $r(m_i)$ also has all but finitely many terms are zero hence C is a submodule of P. Now, we define a map

$$f_i : M_i \to C$$
$$m_i \mapsto (m_j)_{j\in I} \quad \text{where } m_j = m_i \text{ if } i = j, 0 \text{ otherwise}$$

Then clearly f_i's are $R-$module homomorphism so $\ker f_i = \{m_i \in M_i : f(m_i) = 0\} \Rightarrow \{0\}$ therefore, f_i's are injective.

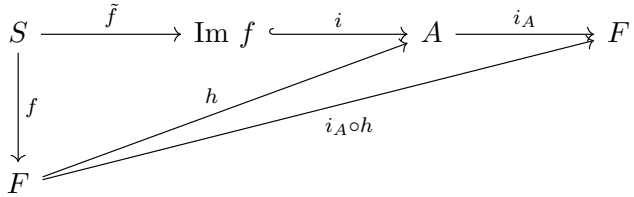
Definition 14.103. *Let R be a ring and S be a non empty set. A free $R-$module on S is an $R-$module F such that for any $R-$module M and every set map $g : S \to M$ there exists an unique $R-$module homomorphism $h : F \to M$ such that the following diagram commutes.*



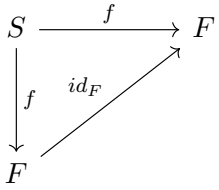
Theorem 14.104. *If (F, f) is a free module on S. Then*

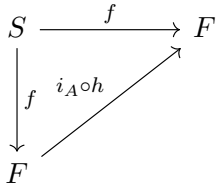
(1) *f is injective,*
(2) *Im f generates F.*

Proof. (1) Take any R module (can take $M = R$) and $x, y \in S$ with $x \neq y$. Define, $g : S \to M$ such that $g(x) \neq g(y)$. By the property of free module there exists $h : F \to M$ such that $h \circ f = g$. Then $h(f(x)) = g(x)$ and $h(f(y)) = g(y)$ thus f is injective.
(2) Let A be the submodule of F generated by $\operatorname{Im} f$. We have to show $A = F$.



We will show that i_A is surjective. We have $h \circ f = i \circ \tilde{f} \Rightarrow i_A \circ (h \circ f) = i_A \circ (i \circ \tilde{f} = f$. But

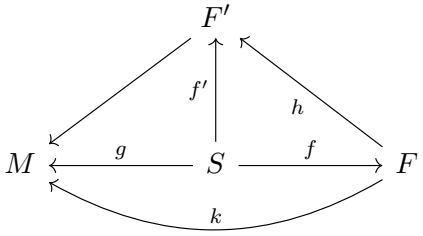




By the uniqueness of the morphism we have $id_F = i_A \circ h$ hence i_A is surjective.

Theorem 14.105 (Uniqueness of free module)**.** *Let (F, f) be a $R-$free module on a set $S(\neq \emptyset)$ then (F', f') is also free module iff there exists an unique isomorphism $j : F \to F'$ such that $h \circ f = f'$.*

Proof. Let M be an $R-$module and $g : S \to M$ is a set map then



Existence of free module. Let

$$F := \{\theta : S \to R : \theta(s) = 0 \text{ for all most all } s \in S\}$$

then F is an $R-$module. Let $\theta_1, \theta_2 \in F$ then define $\theta_1 + \theta_2$ as $(\theta_1 + \theta_2)(s) = \theta_1(s) + \theta_2(s)$ then clearly $\theta_1 + \theta_2 \in F$. Let $r \in R$ and $\theta \in F$ then $r\theta := (r\theta)(s) = r\theta(s)$ and $r\theta \in F$. Define,

$$f : S \to F$$
$$s \mapsto \chi_s$$

where $\chi_s(t) = \begin{cases} 1, & \text{if } t = s \\ 0, & \text{if } t \neq s \end{cases}$. Let M be an $R-$module and $g : S \to M$ be a set map. Define $h : F \to M$ by $h(\theta) = \sum_{s \in S} \theta(s)g(s)$ then clearly h is a module morphism. Let $t \in S$

$$\left(\sum_{s \in S} \theta(s)\chi_s \right)(t) = \theta(t)\chi_t(t) = \theta(t) \cdot 1 = \theta(t)$$

As $t \in S$ is arbitrary, $\theta = \sum_{s \in S} \theta(s)\chi_s$. Now, $(h \circ f)(s) = h(f(s)) = h(\chi_s) = \sum_{s \in S} \chi_s(t)g(t) = g(s)$. Therefore, $h \circ f = g$. Let $h' : F \to M$ is another module homomorphism such that $h' \circ f = g$. To show $h' = h$ we proceed as follows

$$\begin{aligned} h'(\theta) &= h' \left(\sum_{s \in S} \theta(s)\chi_s \right) \\ &= \sum_{s \in S} \theta(s)h'(\chi_s) \\ &= \sum_{s \in S} \theta(s)h(f(s)) \\ &= \sum_{s \in S} \theta(s)g(s) \\ &= h(\theta) \end{aligned}$$

Thus $h = h'$. □

Theorem 14.106. *Let (F, f) be a free module on S. Then $\operatorname{Im} f$ is a basis of F.*

Proof. We already showed $\operatorname{Im} f$ generates F. Let $f(x_1), \cdots, f(x_m)$ be distinct elements of $\operatorname{Im} f$. Let $\alpha_i, \beta_i \in R$ be such that

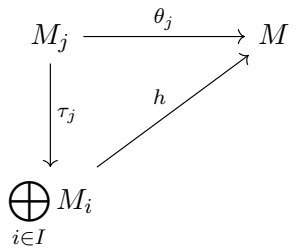
$$\alpha_1 f(x_1) + \cdots + \alpha_n f(x_n) = \beta_1 f(x_1) + \cdots + \beta_n f(x_n) \Rightarrow \sum_{i=1}^{n} (\alpha_i - \beta_i) f(x_i) = 0$$

Then $\sum_{i=1}^{n} (\alpha_i - \beta_i)\chi_{x_i} = 0 \Rightarrow \sum_{i=1}^{n} (\alpha_i - \beta_i)\chi_{x_i}(x_i) = 0 \Rightarrow \alpha_i - \beta_i = 0 \Rightarrow \alpha_i = \beta_i; 1 \leq i \leq n.$ □

Let $\{A_i\}_{i \in I}$ be a family of submodule of an $R-$module M then $\sum_{i \in I} A_i$ is a submodule of M generated by $\bigcup_{i \in I} A_i$ then check that

$$\sum_{i \in I} A_i = \left\{ \sum_{i \in I} a_i : a_i \in A_i, a_i = 0 \text{ for all most all } i \right\}$$

Let M be an $R-$module and $\{M_i\}_{i\in I}$ be a family of submodules of M then for $j \in I$ let $\theta_j : M_j \to M$ be the inclusion map then we have unique module homomorphism $h : \bigoplus_{i\in I} M_i \to M$ such that



the above diagram commutes then

$$h((x_i)_{i\in I}) = \sum_{\substack{\text{finite}\\ \text{sum}}} \theta_i(x_i) = \sum_{\substack{\text{finite}\\ \text{sum}}} x_i$$

And $\operatorname{Im} h$ is the submodule $\sum_{i\in I} M_i$ of M generated by $\bigcup_{i\in I} M_i$.

Definition 14.107. *If h is isomorphism then $\bigoplus_{i\in I} M_i \cong M$ and $\bigoplus_{i\in I} M_i$ is called internal direct sum of $\{M_i\}_{i\in I}$.*

Question 14.108. *When does it happen?*

Ans. h is an isomorphism iff each $x \in M$ can be written uniquely as $x = \sum_{\substack{\text{finite}\\ \text{sum}}} x_i, x_i \in M$.

Theorem 14.109. *Let M be an $R-$module and $\{M_i\}_{i\in I}$ be a family of submodules of M. Then the followings are equivalent:*

(1) $\sum_{i\in I} M_i$ *is the direct sum* $\bigoplus_{i\in I} M_i$,
(2) $\sum_{i\in I} x_i = 0 \Rightarrow x_i = 0, \forall\ i \in I$,
(3) *For all* $i \in I$, $M_j \cap \sum_{i\neq j} M_i = \{0\}$.

15. Field theory

Definition 15.1. *Let K, L be fields with $K \subseteq L$ then we say L is an extension field of K. Here K is called the base field.*

Notation. $L|K$.

Note that if L is an extension field of K then L is a vector space over K. Define,

$$\begin{aligned} \cdot : K \times L &\to L \\ (c, \alpha) &\mapsto c\alpha \qquad \text{[usual ring multiplication in } L\text{]} \end{aligned}$$

Definition 15.2. *L is said to be a finite extension if $\dim_K L$ is finite.*

Notation. $[L : K] := \dim_K L$.

Definition 15.3. *Let $L|K$, an element $\alpha \in L$ is said to be algebraic over K if it satisfies a polynomial $f(x) \in K[x]$ i.e., $f(\alpha) = 0$. An extension $L|K$ is said to be an algebraic extension if any $\alpha \in L$ is algebraic over K.*

Fact from ring theory.

(1) Let A be a commutative ring with 1, $m \in \operatorname{maxspec} A \Leftrightarrow A/m$ is field.
(2) If A is pid then $\operatorname{spec} A \setminus \{0\} = \operatorname{maxspec} A$.
(3) $A[X]$ is pid if and only if A is field.

Observation 15.4. *Suppose $L|K$ and $[L : K] < \infty$ then $L|K$ is algebraic.*

Proof. Let $\alpha \in L$. We consider $S = \{1, \alpha, \alpha^2, \cdots\}$. Since $\dim_K L < \infty$ and S is linearly independent there exists $n \in \mathbb{N}$ such that

$$\alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0; c_i \in K, 1 \leq i \leq n$$

that is $f(\alpha) = 0$ where $f(X) = X^n + c_1X^{n-1} + \cdots + c_n \in K[X]$. Therefore, $L|K$ is algebraic. □

Remark 15.5. *Note that converse is not true that is an algebraic extension need not be a finite extension.*

Let $L|K$ be a field extension and $\alpha \in L$. We define

$$K[\alpha] := \{f(\alpha) : f(X) \in K[X]\} \subseteq L$$

Then $K[\alpha]$ is the smallest subring containing L and α. Since $K[\alpha] \subseteq L$ and L is a field, $K[\alpha]$ is an integral domain. We define,

$$K(\alpha) := \left\{ \frac{f(\alpha)}{g(\alpha)} : f(X), g(X) \in K[X], g(\alpha) \neq 0 \right\}$$

Then $K(\alpha)$ is the quotient field of $K[\alpha]$. Let $S \subseteq L$, if $S = \{\alpha_1, \cdots, \alpha_n\}$; a finite set then

$$K[S] := \{f(\alpha_1, \cdots, \alpha_n) : f(X_1, \cdots, X_n) \in K[X_1, \cdots, X_n]\}.$$

If S is infinite then
Show that $K[S]$ is the smallest subring in L containing K and S. We define $K(S) := Q(K[S])$ (as $K[S] \subseteq L$, it is an integral domain).

Question 15.6. *Show that if $S\{\alpha_1, \cdots, \alpha_n\}$ then*

$$K(S) = \left\{ \frac{f(\alpha_1, \cdots, \alpha_n)}{g(\alpha_1, \cdots, \alpha_n)} : f, g \in K[X_1, \cdots, X_n], g(\alpha_1, \cdots, \alpha_n) \neq 0 \right\}.$$

Ans.
If S is infinite then

Example 15.7 (counterexample of the remark 15.5)**.** *We consider*

$$S = \{\sqrt{p} : p \text{ is prime}\} \subseteq \mathbb{R}$$

Then $\mathbb{Q}(S)|\mathbb{Q}$ is algebraic as each $\sqrt{p}$ satisfies $X^2 - p \in \mathbb{Q}[X]$ but $[\mathbb{Q}(S) : \mathbb{Q}]$ is not finite.

Lemma 15.8. *We consider the field extension $L \subseteq K \subseteq F$ then $[L : F] = [L : K][K : F]$.*

Proof.

Theorem 15.9. *Let $F|K$ is a field extension and $\alpha \in F$. Then $K(\alpha)|K$ is an algebraic extension iff $K[\alpha] = K(\alpha)$.*

Proof. Suppose, the extension is algebraic. Then consider the following map

$$\theta : K[X] \to K[\alpha] \subseteq F$$
$$f(X) \mapsto f(\alpha)$$

Now, $\ker\theta = \{f(X) \in K[X] : f(\alpha) = 0\} \neq 0$ (since α is algebraic over K) therefore, $K[X]/\ker\theta \hookrightarrow K[\alpha]$ and $K[X]/\ker\theta$ is an integral domain thus $\ker\theta$ is a prime ideal. Since $K[X]$ is pid, $\ker\theta = \langle p(X)\rangle, p(X)$ is monic irreducible polynomial in $K[X]$ (note that $p(X)$ is the least degree polynomial in $\ker\theta$). Let $f(\alpha) \in K[\alpha]$, we consider the polynomial $f(X) \in K[X]$ so that $\theta(f(X)) = f(\alpha)$ hence θ is surjective. Therefore, $K[X]/\langle p(X)\rangle \cong K[\alpha]$. As $K[X]/\langle p(X)\rangle$ is field, $K[\alpha]$ is also field hence $K[\alpha] = K(\alpha)$. Conversely, suppose $K[\alpha] = K(\alpha)$. Consider $\frac{1}{\alpha} \in K(\alpha)$ then $\frac{1}{\alpha} \in K[\alpha]$ thus $\frac{1}{\alpha} = f(\alpha)$ where $f(X) \in K[X]$ so α satisfies the polynomial $Xf(X) - 1 \in K[X]$. Therefore, α is algebraic over K. Hence $K(\alpha)|K$ is algebraic. □

Theorem 15.10. *Let $F|K$ be a field extension and $\alpha \in F$ is algebraic over K. Let $p(X)$ be the minimal polynomial of α Then $[K(\alpha) : K] = \deg p(X)$.*

Proof. Let $\deg p(X) = n$. We claim that $S = \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ is a basis for $K(\alpha)|K$. Let $c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = 0, c_i \in K, 0 \leq i \leq n-1$. If $c_i \neq 0$ for some i then α satisfies a polynomial over K whose degree is strictly less that n which is a contradiction since $p(X)$ is minimal polynomial of α over K. Therefore, $c_i = 0, 0 \leq i \leq n-1$. As $K(\alpha)|K$ is algebraic, $K[\alpha] = K(\alpha)$. We take $f(\alpha) \in K[\alpha], f(X) \in K[X]$ then $f(\alpha) = c_0 + c_1\alpha + \cdots + c_m\alpha^m$ for some $f(X) = c_0 + c_1X + \cdots + c_mX^m$. By division algorithm, $f(X) = q(X)p(X) + r(X)$ where $r(X) = 0$ or $\deg r(X) < \deg p(X)$ thus we have $f(\alpha) = r(\alpha)$ and $f(\alpha) = r(\alpha) \in \text{span}\ \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ (as $\deg r(X) < \deg p(X)$ or $r(X) = 0$). Therefore, S is a basis and $[K(\alpha) : K] = n = \deg p(X)$. □

Corollary 15.11. *Let $F|K$ be a field extension and $\alpha \in F$. Suppose, α is algebraic over K then $K(\alpha)|K$ is algebraic.*

Proof. $[K(\alpha) : K]$ is finite hence algebraic. □

Proposition 15.12. *Let $F|K$ be a field extension and α is transcendental (that is not algebraic) over K iff $K[X] = K[\alpha]$.*

Proof. We define

$$\theta : K[X] \to K[\alpha]$$
$$f(X) \mapsto f(\alpha)$$

Note that θ is surjective. α is transcendental iff $\ker\theta = \{0\}$. Hence $K[X] \cong K[\alpha]$. □
Note that

15.1. **Field automorphism and Galois extension.** Let F be a field,

$$\operatorname{Aut} F := \{\sigma : F \to F : \sigma \text{ is a field automorphism}\}.$$

Clearly, $\operatorname{Aut} F$ is a group under mapping composition. Let $F|K$ be a field extension, $\operatorname{Aut}_K F < \operatorname{Aut} F$ where

$$\operatorname{Aut}_K F := \{\sigma \in \operatorname{Aut} F : \sigma|_K = \mathrm{id}_K\}.$$

Any element of $\operatorname{Aut}_K F$ is called $K-$automorphism. $\operatorname{Aut}_K F$ is called the Galois group of the extension $F|K$. Let, F, E be extension field of K and $\sigma : F \to E$ be a field homomorphism such that $\sigma|_K = \mathrm{id}$ Then σ is called $K-$homomorphism.

$$\begin{array}{ccc} F & \xrightarrow{\sigma} & E \\ | & & | \\ K & \longrightarrow & K \end{array}$$

Question 15.13. *Compute the Galois group of $\mathbb{R}|\mathbb{Q}$ that is, $Aut_{\mathbb{Q}}\,\mathbb{R}$.*

Ans. Let $\sigma \in \operatorname{Aut}_{\mathbb{Q}}\mathbb{R}$. Suppose $x \in \mathbb{R}$ and $x > 0$ then $\sigma(x) = \sigma((\sqrt{x})^2 = \sigma(\sqrt{x})^2 \geq 0$. Again $\sigma(0) = 0$ and σ is an isomorphism, hence $\sigma(x) > 0$ whenever $x > 0$. Let $x, y \in \mathbb{R}$ and $x > y$ then $x - y > 0$ and it follows that $\sigma(x) > \sigma(y)$. We claim that $\operatorname{Aut}_{\mathbb{Q}}\mathbb{R} = \{\mathrm{id}_{\mathbb{R}}\}$. If not then there exists $\sigma \in \operatorname{Aut}_{\mathbb{Q}}\mathbb{R}$ such that $\sigma(x) \neq x$. Therefore, $\sigma(x) > x$ or $\sigma(x) < x$ (by Law of trichotomy). If $\sigma(x) > x$ we choose a rational $r \in \mathbb{Q}$ between $\sigma(x)$ and x that is $\sigma(x) > r > x$ (by density property of rationals) then $r - x > 0$ and $\sigma(r) > \sigma(x)$ which implies $r > \sigma(x)$ contradicting our assumption. By similar argument we can show that if $\sigma(x) < x$ then we arrived at a contradiction. Therefore, $\operatorname{Aut}_{\mathbb{Q}}\mathbb{R} = \{\mathrm{id}_{\mathbb{R}}\}$.

Question 15.14. *Compute the Galois group of $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ that is $Aut_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{2})$.*

Ans. $\mathcal{B} = \{1, \sqrt{2}\}$ is a basis of the extension $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ so any element of $\mathbb{Q}\sqrt{2}$ is of the form $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Let $\sigma \in \operatorname{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2})$ and $\sigma(\sqrt{2}) = c + d\sqrt{2}$. Now,

$$2 = \sigma(2) = \sigma((\sqrt{2}))^2 = (\sigma(\sqrt{2}))^2 = (c + d\sqrt{2})^2 = c^2 + 2d^2 + 2cd\sqrt{2}.$$

Therefore we get $2cd\sqrt{2} = 0$ which gives either $c = 0$ or $d = 0$. The case $d = 0$ is impossible since $c^2 = 2$ has no rational solution. Therefore, $c = 0$ in which case $d = 1, -1$. Thus $\sigma(\sqrt{2})$ will be

either $\sqrt{2}$ or $-\sqrt{2}$. Then $\sigma(a+b\sqrt{2}) = a \pm b\sqrt{2}$ (as $a, b \in \mathbb{Q}$). So there are only two automorphism σ_1, σ_2 with $\sigma_1 = \text{id}$ and $\sigma_2(\sqrt{2}) = -\sqrt{2}$. Therefore, $\text{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt{2}) = \{\text{id}, \sigma_2\} \cong \mathbb{Z}/2\mathbb{Z}$.

Question 15.15. *Compute the Galois group of the extensions $\mathbb{C}|\mathbb{R}$ and $\mathbb{C}|\mathbb{Q}$.*

Ans.

Theorem 15.16. *Let F be an extension field of K and $f \in K[X]$. If $u \in F$ is a root of f and $\sigma \in Aut_K\, F$, then $\sigma(u) \in F$ is also a root of f.*

Proof. If $f(X) = a_n X^n + \cdots + a_0$ with $a_n \neq 0; a_i \in K, 1 \leq i \leq n$. u is a root of f therefore, $0 = f(u) = a_n u^n + \cdots + a_0$. Applying σ both side we have

$$0 = \sigma(f(u)) = \sigma(a_n u^n + \cdots + a_0) = a_n \sigma(u)^n + \cdots + a_0.$$

Therefore, $\sigma(u)$ is also a root of $f(X)$. □

Theorem 15.17. *Let F be an extension field of K, E is an intermediate field and $H < Aut_K\, F$. We define*

(1) $H' := \{u \in F : \sigma(u) = u \text{ for all } \sigma \in H\} \subseteq F$;
(2) $E' := \{\sigma \in Aut_K\, F : \sigma(u) = u \text{ for all } u \in E\} = Aut_E\, F$.

Show that H' is a subfield of F containing K and E' is a subgroup of $Aut_K\, F$. H' is called the fixed field of H in F.

$$\begin{array}{ccc} F & \longrightarrow & F' = \{id\} \\ | & & \\ E & \longrightarrow & E' = Aut_E\, F \\ | & & \\ K & \longrightarrow & K' = Aut_K\, F \end{array} \qquad \begin{array}{ccc} \{id\}' = F & \longleftarrow & \{id\} \\ | & & \wedge \\ H' & \longleftarrow & H \\ | & & \wedge \\ K & & Aut_K\, F \end{array}$$

Note that in general $(\text{Aut}_K\, F)' \neq K$ but if $u \in K$ then $\sigma(u) = u$ for all $\sigma \in \text{Aut}_K\, F$ therefore $u \in (\text{Aut}_K\, F)' \Rightarrow K \subseteq (\text{Aut}_K\, F)'$. For example take $\mathbb{R}|\mathbb{Q}$ then $\text{Aut}_{\mathbb{Q}}\, \mathbb{R} = \{\text{id}\}$ and $(\text{Aut}_{\mathbb{Q}}\, \mathbb{R})' = \mathbb{R} \neq \mathbb{Q}$.

Proof.
(1) Pick $u_1, u_2 \in H'$ then $\sigma(u_1) = u_1$ and $\sigma(u_2) = u_2$ for all $\sigma \in H$. $\sigma(u_1 - u_2) = \sigma(u_1) - \sigma(u_2) = u_1 - u_2 \in H$ for all $\sigma \in H$. And $\sigma(u_1^{-1}u_2) = \sigma(u_1)^{-1}\sigma(u_2) = u_1^{-1}u_2$ for all $\sigma \in H$. Therefore, H' is a subfield of F. Since $\text{Aut}_K\, F$ fixes K, any subgroup of $\text{Aut}_K\, F$ will also fix K, hence $K \subseteq H'$.
(2) Let $\sigma_1, \sigma_2 \in \text{Aut}_E\, F$, we have $\sigma_1(u) = u$ and $\sigma_2(u) = u$ for all $u \in E$. $(\sigma_1)^{-1}\sigma_2(u) = \sigma_1^{-1}(u) = u$ for all $u \in E$ which gives $(\sigma_1)^{-1}\sigma_2 \in E'$ therefore, $E' = \text{Aut}_E\, F < \text{Aut}_K\, F$.

□

Definition 15.18. *A field extension $F|K$ is called Galois extension if $(Aut_K\, F)' = K$.*

In our example $\mathbb{R}|\mathbb{Q}$ is not Galois. We take $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$. $\text{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt{2}) = \{\text{id}, \sigma\}; \sigma(\sqrt{2}) = -\sqrt{2}$. Let $a + b\sqrt{2} \in (\text{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt{2})'$ then $\sigma(a + b\sqrt{2}) = a + b\sqrt{2} \Rightarrow a - b\sqrt{2} = a + b\sqrt{2} \Rightarrow b = 0$. Therefore, $(\text{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\sqrt{2}))' = \mathbb{Q}$. Hence $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ is Galois.

Lemma 15.19. *Prove the followings:*

(1) $F' = \{id\}$ *and* $K' = Aut_K F$;
(2) $\{id\}' = F$;
(3) *If* $L \subseteq M$ *then* $M' < L'$;
(4) *If* $H < J$ *then* $J' \subseteq H'$;
(5) $L \subseteq L''$ *and* $H < H''$;
(6) $L' = L'''$ *and* $H' = H'''$.

Proof. (1) $F' = \{\sigma \in \mathrm{Aut}_K F : \sigma(u) = u \text{ for all } u \in F\} = \{\mathrm{id}\}$ and $K' = \mathrm{Aut}_K F$ by definition.
(2) $\{\mathrm{id}\}' = \{u \in F : \mathrm{id}(u) = u\} = F$.
(3) Let $L \subseteq M$. Let $\sigma \in \mathrm{Aut}_M F$ then $\sigma(m) = m$ for all $m \in M$ in particular, $\sigma(l) = l$ for all $l \in L$ thus $\sigma \in \mathrm{Aut}_L F$ and $M' < L'$.
(4) Let $H < J$, Take $u \in J'$ therefore, $\sigma_J(u) = u$ for all $\sigma_J \in J$, in particular, $\sigma_H(u) = u$ for all $\sigma_H \in H$ thus $u \in H'$ and $J' \subseteq H'$.
(5) $L'' = \{u \in F : \sigma(u) = u \text{ for all } \sigma \in L'\}$. Let $u \in L$ and $\sigma \in L'$ then $\sigma(u) = u$ and this is true for all $\sigma \in L'$ and for all $u \in L$ therefore, $u \in L''$ and $L \subseteq L''$.
$H'' = \{\sigma \in \mathrm{Aut}_K F : \sigma(u) = u \text{ for all } u \in H'\}$. Let $\sigma \in H$ and $u \in H'$ then $\sigma(u) = u$ for all $\sigma \in H$ and this is true for all $u \in H'$ therefore, $\sigma \in H''$ and $H < H''$.
(6) From (5), $L \subseteq L''$ and By (3), $L''' < L'$ again $L' < L'''$ by (5) hence $L' = L'''$. By (5) $H < H''$ and by (4) $H''' \subseteq H'$ and by (5) $H' \subseteq H'''$ therefore, $H' = H'''$.

□

Definition 15.20. *Let* $K \subseteq L \subseteq F$ *be the extension.* L *is said to be closed subfield of* F *with respect to the extension field* $F|K$ *if* $L'' = L$. *Let* $H < Aut_K F$, H *is said to be closed subgroup if* $H'' = H$. *In particular the extension* $F|K$ *is Galois if* $K = K''$.

Lemma 15.21. *Let* $K \subseteq L \subseteq M \subseteq F$ *be the extension and* $[M : L]$ *is finite then* $[L' : M'] \leq [M : L]$. *In particular if* $F|K$ *is finite then* $|\, Aut_K F| \leq [F : K]$.

Proof. We proceed by induction on $n = [M : L]$. If $n = 1$ then $M = L$ and consequently $L' = M'$ and we are done. Suppose $n > 1$ and this lemma is true for all $i < n$. Let $u \in M - L$, and consider the following extension $K \subseteq L \subseteq L(u) \subseteq M \subseteq F$.
Case 1. $L(u) = M$, since $[L : M]$ is finite, u is algebraic over L. Let $f(X)$ be the irreducible polynomial of u and $\sum = \{v \in F : f(v) = 0\}$ then $|\sum| < \deg f = n$ and S be the set of all left cosets of M' in L'. Define

$$\theta : S \to \sum$$
$$\tau M' \mapsto \tau(u)$$

Since u is a root of $f(X) \in L[X]$ and $\tau \in L' = \mathrm{Aut}_L F$ therefore $\tau(u)$ is also a root of f. We claim that θ is well defined and injective. Let $\tau M' = \sigma M' \Leftrightarrow \sigma^{-1}\tau \in M' = [L(u)]' \Leftrightarrow \sigma^{-1}\tau(u) = u \Leftrightarrow \tau(u) = \sigma(u)$. Therefore, $|S| \leq |\sum| \leq n$ hence $[L' : M'] \leq n$.
Case 2. If $L(u) \subsetneq M$ then consider the extension $L \subseteq L(u) \subseteq M$. Let $[L(u) : L] = r$ and $[M : L(u)] = n/r$. Since $u \notin L$, r must be bigger that 1 and $n/r < n$. By induction hypothesis

$[L(u)' : M'] \leq [M : L(u)]$ and $[L' : L(u)'] \leq [L(u) : L]$. Multiplying both of them we get $[L' : L(u)'][L(u)' : M'] \leq [M : L(u)][L(u) : L] \Rightarrow [L' : M'] \leq [M : L]$. □

Lemma 15.22. *Let F be an extension field of K and let H, J be subgroups of the Galois group $Aut_K F$ with $H < J$. If $[J : H]$ is finite, then $[H' : J'] \leq [J : H]$.*

Proof. Let $[J : H] = n$ and suppose $[H' : J'] > n$ then there exists $\{u_1, \cdots, u_{n+1}\} \in H'$ such that $\{u_1, \cdots, u_{n+1}\}$ is linearly independent over J'. Let $\{\tau_1, \cdots, \tau_n\}$ be a complete set of representatives of all left cosets of H in J that is $J = \bigcup_{i=1}^{n} \tau_i H$ and $\tau_i^{-1}\tau_j \notin H$ if $i \neq j$. We consider the linear system with n equation and $n+1$ unknowns:

$$A \equiv \begin{array}{c} \tau_1(u_1)X_1 + \cdots + \tau_1(u_{n+1})X_{n+1} = 0 \\ \vdots \qquad\qquad\qquad \vdots \\ \tau_n(u_1)X_1 + \cdots + \tau_n(u_{n+1})X_{n+1} = 0 \end{array}$$

The system has a non trivial solution. Among all such non trivial solution we choose $(a_1, \cdots, a_{n+1})$ with a minimal number of non zero's. After reindexing, if necessary we may assume $a_{r+1} = \cdots = a_{n+1} = 0$ and $a_i \neq 0, 1 \leq i \leq r$ then $r \geq 1$. Since $c(a_1, \cdots, a_{n+1}), c \in J'$ is also a solution we may further assume that $a_1 = 1_F$. Let $\tau_1 = \mathrm{id}$ (as $\{\tau_1, \cdots, \tau_n\}$ is complete list of representatives of left cosets of H in J). From the first equation we get

$$u_1 a_1 + \cdots + u_r a_r = 0.$$

$\{u_1, \cdots, u_r\}$ is linearly independent over J' and $a_i \neq 0, 1 \leq i \leq r$ there exists $i \in \{1, \cdots, r\}$ such that $a_i \notin J'$.n We have $a_1 = 1_F$ which imply $a_i \in J'$ so with out loss of generality we may assume that $a_2 \notin J'$ therefore, there exists $\sigma \in J$ such that $\sigma(a_1) \neq a_2$. Now we consider another system of linear equations:

$$B \equiv \begin{array}{c} \sigma(\tau_1(u_1))X_1 + \cdots + \sigma(\tau_1(u_{n+1}))X_{n+1} = 0 \\ \vdots \qquad\qquad\qquad\qquad \vdots \\ \sigma(\tau_n(u_1))X_1 + \cdots + \sigma(\tau_n(u_{n+1}))X_{n+1} = 0 \end{array}$$

Since $(a_1, \cdots, a_{n+1})$ is a solution of A, $(\sigma(a_1), \cdots, \sigma(a_{n+1}))$ is a solution of B. We claim that A and B has same solution. If we prove the claim then $(\sigma(a_1), \cdots, \sigma(a_{n+1}))$ is a solution of A also and therefore, $(a_1, \cdots, a_{n+1}) - (\sigma(a_1), \cdots, \sigma(a_{n+1}))$ is also a solution of A. Since $a_1 = 1_F, \sigma(a_1) = 1_F$ and $\sigma(a_2) \neq a_2$ we have a non trivial solution of A namely $(0, a_2 - \sigma(a_2), \cdots, a_r - \sigma(a_r), 0, \cdots, 0)$ which is a contradiction as $(a_1, \cdots, a_r, 0, \cdots, 0)$ is a non trivial solution with minimal number of zero's. Hence $[H' : J'] \leq [J : H]$. Now we proof the claim. At first notice that $\{\sigma\tau_1, \cdots, \sigma\tau_n\}$ is also complete list of representatives of left cosets of H in J (as $(\sigma\tau_i)^{-1}(\tau\sigma_j) = \tau_i^{-1}\tau_j \notin H$ if $i \neq j$). Therefore, $J = \bigcup_{i=1}^{n} \sigma\tau_i H$. Again if $\zeta H = \theta H \Leftrightarrow \theta^{-1}\zeta \in H \Leftrightarrow \theta^{-1}\zeta(u_i) = u_i \Leftrightarrow \theta(u_i) = \zeta(u_i), 1 \leq i \leq n+1$ (as $\{u_1, \cdots, u_{n+1}\} \subseteq H'$]). Since $\{\tau_1 H, \cdots, \tau_n H\}$ and $\{\sigma\tau_1 H, \cdots, \sigma\tau_n H\}$ are both complete list of of cosets of H, $\sigma\tau_i H = \tau_j H$ and this gives $\sigma\tau_i(u_l) = \tau_j(u_l)$ for all $l \in \{1, \cdots, n+1\}$. Let $\tau_1 = \sigma\tau_k; 1 \leq k \leq n$ so we get $\tau_1(u_1) = \sigma\tau_k(u_1), \cdots, \tau_1(u_{n+1}) = \sigma\tau_k(u_{n+1})$ therefore, the first

equation of A becomes $\sigma\tau_k(u_1)X_1 + \cdots + \sigma\tau_k(u_{n+1})X_{n+1} = 0$. This shows that A and B are the same system of linear equation therefore there solution is also same. □

Lemma 15.23. *Let $K \subseteq L \subseteq M \subseteq F$ and $\{id\} < H < J < Aut_K F$ then*

(1) *If L is closed and $[M : L]$ is finite then M is closed and $[L' : M'] = [M : L]$,*
(2) *If H is closed and $[J : H]$ is finite, then J is closed and $[H' : J'] = [J : H]$,*
(3) *IF $F|K$ is finite and Galois then all intermediate fields and all subgroups of $Aut_K F$ are closed and $|\, Aut_K F| = [F : K]$.*

Proof. (1) $[L' : M'] \leq [M : L]$ by previous lemma and $[M : L]$ is finite implies $[L' : M']$ is also finite hence $[M'' : L''] \leq [L' : M'] \leq [M : L]$. Now $M \subseteq M''$ thus $[M : L] \leq [M'' : L] \leq [L' : M'] \leq [M'' : L]$. Therefore, $[L' : M'] = [L : M]$ and $M = M''$.

(2) By previous lemma, $[H : J'] \leq [J : H]$ hence $[H' : J']$ is also finite since $[H : J]$ is finite. Therefore, $[J'' : H''] \leq [H' : J'] \leq [J : H]$. As H is closed, $H = H''$ and $[J'' : H] \leq [H' : J'] \leq [J : H]$. We have $J < J$" from previous lemma, then $[J : H] \leq [J'' : H] \leq [H' : J'] \leq [J : H]$. Thus $[H' : J'] = [J : H]$ and $J'' = J$.

(3) In particular if $F|K$ is Galois, $K = K''$ so $[K' : F'] = [F : K] \Rightarrow |\operatorname{Aut}_K F| = [F : K]$.

□

Definition 15.24. *Let $L \subseteq E \subseteq F$, E is said to be stable (relative to $F|K$) if $\sigma(E) \subseteq E$ for all $\sigma \in Aut_K F$.*

Note that $\sigma \in \operatorname{Aut}_K F$ then $\sigma^{-1} \in \operatorname{Aut}_K F$. If E is stable, $\sigma(E) \subseteq E$ and $\sigma^{-1}(E) \subseteq E \Rightarrow E \subseteq \sigma(E) \Rightarrow \sigma(E) = E$.

Lemma 15.25. *Let $F|K$ be the field extension,*

(1) *If $K \subseteq E \subseteq F$ and E is stable intermediate field, then $E' = Aut_E F \trianglelefteq Aut_K F$;*
(2) *If $H \trianglelefteq Aut_K F$ then H' is stable.*

Proof. (1) Let $\tau \in \operatorname{Aut}_K F$ and $x \in E$, $\sigma \in \operatorname{Aut}_E F = E'$. Since E is stable, $\tau^{-1}(x) \in E$ so $\sigma(\tau^{-1}(x)) = \tau^{-1}(x) \Rightarrow \tau\sigma\tau^{-1}(x)$ and this is true for any $x \in E$ therefore, $\tau\sigma\tau^{-1} \in E'$ hence $E' \trianglelefteq \operatorname{Aut}_K F$.

(2) Let $x \in H',]tau \in \operatorname{Aut}_K F$. Let $\sigma \in H$, as $H \trianglelefteq \operatorname{Aut}_K F$, $\tau^{-1}\sigma\tau \in H$ therefore, $\tau^{-1}\sigma\tau(x) = x \Rightarrow \sigma(\tau(x)) = \tau(x) \Rightarrow \tau(x) \in H'$ (since σ is chosen arbitrarily). Hence H' is stable.

□

Lemma 15.26. *Let $K \subseteq E \subseteq F$ be the extension and $F|K$ is Galois. If E is stable then $E|K$ is Galois.*

Proof. Let $u \in E \setminus K$ then $u \in F \setminus K$. Since $K = K''$, there exists $\sigma \in \operatorname{Aut}_K F$ such that $\sigma(u) \neq u$. Now $\sigma|_E : E \to E$ is the restriction map and we can do this because E is stable. Then $\sigma|_E(u) \neq u$. Therefore, $E|K$ is Galois. □

Lemma 15.27. *Let $K \subseteq E \subseteq F$ such that $E|K$ is algebraic and Galois then E is stable.*

Proof. Let $u \in E$. Since $E|K$ is algebraic, there exists an irreducible monic polynomial $f(X) \in K[X]$ such that $f(u) = 0$. Let $\deg f = n$ and $u_1, \cdots, u_r$ $(r \leq n)$ be all roots of f lies in E. We

consider the polynomial $g(X) = (X - u_1)\cdots(X - u_r) \in E[X]$. If $\sigma \in \operatorname{Aut}_K E$ then σ simply permutes the set $\{u_1, \cdots, u_r\}$. Now,

$$\begin{aligned} g(X) &= X^r - (u_1 + \cdots + u_r)X^{r-1} + \sum_{1\le i<j\le n} u_i u_j X^{r-2} + \cdots + (-1)^{r-1}\prod_{i=1}^{r} u_i \\ &= X^r + a_1 X^{r-1} + \cdots + a_r \end{aligned}$$

where $a_1 = -(u_1 + \cdots + u_r), \cdots, a_r = (-1)^{r-1}\prod_{i=1}^{r} u_i$. Since a_i's are symmetric functions of u_i's, $\sigma(a_i) = a_i, \forall\ \sigma \in \operatorname{Aut}_K E \Rightarrow a_i \in (\operatorname{Aut}_K E)'$ for all $1 \le i \le r$. Since $E|K$ is Galois, $(\operatorname{Aut}_K E)' = K \Rightarrow a_i \in K$ for all $1 \le i \le r$. Therefore, $g(X) \in K[X]$. since $u \in \{u_1, \cdots, u_r\} \Rightarrow g(u) = 0$. As f is the minimal polynomial of u in $K[X] \Rightarrow f|g$ but $\deg g \le \deg f \Rightarrow g = f$ (as both are monic). So we get that there are n distinct roots of f lies in E. Now, $\tau \in \operatorname{Aut}_K F, \tau(u)$ is also a root of $f \Rightarrow \tau(u) \in E$. Therefore, E is stable. □

Lemma 15.28. *Let $K \subseteq E \subseteq F$ be the extension and E is stable, then $Aut_K F/\ Aut_E F$ is isomorphic to the group of all $K-$automorphisms of E that are extendable to F.*

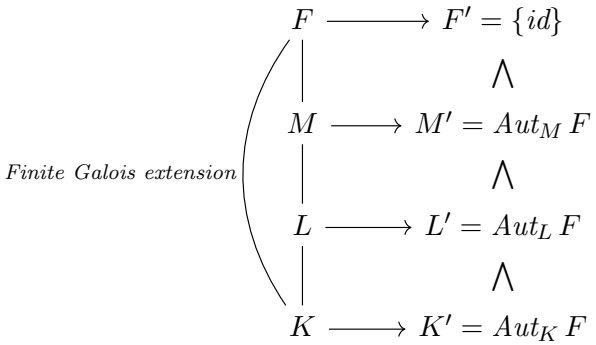
Proof. We define,

$$\begin{aligned} \theta : \operatorname{Aut}_K F &\to \operatorname{Aut}_K E \\ \sigma &\mapsto \sigma|_E \qquad\qquad (\text{since } E \text{ is stable}) \end{aligned}$$

$\ker\theta = \{\sigma \in \operatorname{Aut}_K F : \sigma|_E = \mathrm{id}\} = \operatorname{Aut}_E F$ and $\dfrac{\operatorname{Aut}_K F}{\operatorname{Aut}_E F} \cong \operatorname{Im}\theta = \{\psi \in \operatorname{Aut}_K E : \text{there exists } \tilde{\psi} \in \operatorname{Aut}_K F \text{ such that } \tilde{\psi}|_E = \psi\}$. □

Theorem 15.29 (Fundamental theorem of Galois theory)**.** *If F is a finite dimensional Galois extension of K, then there is a one to one corresponding between the set of all intermediate fields of $F|K$ and the set of all subgroups of the Galois group $Aut_K F$ (given by $E \mapsto E' = Aut_E F$) such that*

(1) *the relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups. In particular $|\ Aut_K F| = [F : K]$ that is*



(2) *$K \subseteq E \subseteq F$ is a finite Galois extension then $F|E$ is Galois but $E|K$ is Galois iff $E' \trianglelefteq Aut_K F$ and $Aut_K E \cong Aut_K F/E'$.*

Proof. (1) Since $F|K$ is Galois, every intermediate field of $F|K$ and every subgroup of $\operatorname{Aut}_K F$ is closed and by lemma 15.23, $|\operatorname{Aut}_K F| = [F : K]$.

(2) Since $F|K$ is Galois, E is closed and therefore, $F|E$ is Galois since $E = (\mathrm{Aut}_E F)' = (E')'$. Now we assume that $E|K$ is Galois, since $E|K$ is finite, it is algebraic and by lemma 15.27 E is stable which implies $E' \trianglelefteq \mathrm{Aut}_K F$. Conversely, let $E' \trianglelefteq \mathrm{Aut}_K F$ then E'' is stable and since E is closed, $E = E''$, hence $E|K$ is Galois (as $F|K$ is Galois) by lemma 15.26.

Theorem 15.30 (Artin)**.** *Let F be a field and $G < Aut F, K = \{x \in F : \sigma(x) = x \text{ for all } \sigma \in G\}$ that is fixed field of G. Then $F|K$ is Galois. If G is finite then $[F : K]$ is finite and $Aut_K F = G$.*

Proof. Let $u \in F \setminus K$ then $u \notin G'$ so there exists $\sigma \in G < \mathrm{Aut}_K F$ (Note that $\sigma \in G, x \in K \Rightarrow \sigma(x) = x \Rightarrow \sigma \in \mathrm{Aut}_K F$) such that $\sigma(u) \neq u$. Therefore, $F|K$ is Galois. Suppose, G is finite. Now, $\{\mathrm{id}\} < G < \mathrm{Aut}_K F$ and $[G : \{\mathrm{id}\}] = |G| =$ finite therefore, by Lemma 15.22 $[\{\mathrm{id}\}' : G'] \leq |G| \Rightarrow [F : K] \leq |G|$. We have proved that $F|K$ is Galois thus $[F : K] = |\mathrm{Aut}_K F|$ (by Theorem 15.29) therefore, $|\mathrm{Aut}_K F| \leq G \leq |\mathrm{Aut}_K F| \Rightarrow \mathrm{Aut}_K F = G$. □

Lemma 15.31. *Suppose $F|K$ is finite and $[F : K] = |Aut_K F|$ then $F|K$ is Galois.*

Proof. Let $G = \mathrm{Aut}_K F < \mathrm{Aut}\, F$ then $K \subseteq K'' \subseteq F$ and by Artin's theorem $F|K''$ is Galois with Galois group G. By Theorem 15.29 $[F : K''] = |G| = |\mathrm{Aut}_K F| = [F : K] = [F : K''][K'' : K] \Rightarrow [K'' : K] = 1 \Rightarrow K = K''$. Hence $F|K$ is Galois. □

Definition 15.32. *Let F be a field and $f(X) \in F[X]$ be a polynomial of positive degree. f is said to be split over F if*

$$f(X) = u_0(X - u_1) \cdots (X - u_n), u_i \in F, 0 \leq i \leq n.$$

Definition 15.33. (1) *Let K be a field and $f \in K[X]$ be a polynomial of positive degree. An extension field F of K is said to be a splitting field over K of then polynomial $f(X)$ if f splits over F and $F = K(u_1, \cdots, u_n)$ where $u_1, \cdots, u_n$ are the roots of f in F.*

(2) *Let S be a set of polynomials of positive degree in $K[X]$. An extension field F of K is said to be splitting field over K of the set S of polynomials if every polynomial in S splits over F and F is generated by the set of all roots of all polynomials in S over K.*

16. Appendix I

Exercise 16.1. *Suppose that the set R is equipped with two binary operation '$+$' and '$\cdot$' such that $(R,+)$ is a a group and $(R,\cdot)$ is a semi group with identity element 1 and $x(y+z)=xy+xz$ for all $x,y,z\in R$. Show that $(R,+,\cdot)$ is a ring i.e., show that the operation '$+$' is necessarily commutative.*

Exercise 16.2. *Let R be a ring whose additive group $(R,+)$ is cyclic. Show that R is a commutative ring.*
or, p be a prime number. Show that any ring of order p is commutative ring.

Exercise 16.3. *Give an example of a non commutative ring of order 4.*

Exercise 16.4. *Show that a ring of order 6 is commutative. Does there exists an integral domain of order 6? Justify your answer*

Exercise 16.5. *Let R be a ring with unique element $e\neq 0$ such that $ex=x$ for all x in R. Show that e is an identity element of R. Does the above result hold if e is not unique? Justify.*

Exercise 16.6. *Let R be a Boolean ring. Show that*
(i) $charR=2$,
(ii) R is a commutative ring.

Exercise 16.7. *If R is a finite non-zero Boolean ring then show that R has 2^n elements for some positive integer n. Hence conclude that there is no Boolean ring of order 6.*

Exercise 16.8. *Let R be a ring with identity. Show that R is a Boolean ring if and only if $a(a+b)b=0$ for all $a,b\in R$.*

Exercise 16.9. *Let R be a finite ring with identity and $a,b\in R$ such that $ab=1$ show that $ba=1$.*

Exercise 16.10. *Are the rings $C[0,1]$ and $D[0,1]$ integral domain? Justify your answer.*

Exercise 16.11. *Let R be a ring and $C(R)$ be the center of R. If $x^2-x\in C(R)$ then show that R is commutative.*

Exercise 16.12. *If R is division ring then show that $C(R)$ is a field.*

Exercise 16.13. *Let R be a ring with identity such that R has no divisor of zero. If every sub ring of R iss ideal of R then show that R is a commutative ring.*

Exercise 16.14. *Let R is an integral domain such that $IJ=I\cap J$ for every ideal I,J of R. Show that R is a field.*

Exercise 16.15. *Show that any integral domain with finite number of ideals is field. Hence conclude that any finite integral domain is a field.*

Exercise 16.16. *Let a,b two elements in a ring R and $m,n\in\mathbb{N}$ with $\gcd(m,n)=1$ such that $a^m=b^m$ and $a^n=b^n$. Show that $a=b$.*

Exercise 16.17. *Let R be a ring with identity and $a\in R$,*
(i) If a has left(or right) inverse but no right(left) inverse then show that a has atleast two left(right) inverse. (ii) If a has more than a left (or right) inverse then it has infinite number of such inverses.

Exercise 16.18. *Let R be a ring such that R has no non zero nilpotent element. If $e \in R$ is an idempotent element then show that $e \in C(R)$.*

Exercise 16.19. *Show that units of ring $\mathbb{Z}[i]$ forms a cyclic group.*

Exercise 16.20. *Let R be a ring with identity and $a, b \in R$. If $1 - ab$ is a unit in R then show that $1 - ba$ is also a unit in R.*

Exercise 16.21. *Let A be a left ideal and B be a right ideal of R. If $A \cap B$ is an ideal of R? Justify your answer.*

Exercise 16.22. *(i) Let R be a commutative ring with identity then show that set N of all nilpotent elements forms an ideal of R. Also show that the ring R/N has no non zero nilpotent elements. Is commutativity essential? Justify your answer.*

Exercise 16.23. *Show that a finite ring R with left and right non zero divisor has identity.*

Exercise 16.24. *If R is a finite ring with identity then show that each non zero element is either a one sided zero divisor or a unit in R.*

Exercise 16.25. *Do zero divisor of a ring form an ideal? Justify.*

Exercise 16.26. *Show that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ for any integer $n > 0$.*

Exercise 16.27. *Show that any epimorphism from the ring of integers onto itself is an isomorphism.*

Exercise 16.28. *Show that $(2\mathbb{Z}, +, \cdot)$ is not isomorphic to $(3\mathbb{Z}, +, \cdot)$.*

Exercise 16.29. *Is quotient ring of an integral domain always an integral domain?*

Exercise 16.30. *Show that there is no ring isomorphism from $(\mathbb{C}, +, \cdot)$ to $(\mathbb{R}, +, \cdot)$.*

Exercise 16.31. *Let $F = \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} : x \in \mathbb{R} \right\}$. Show that F is a field isomorphic to field of real numbers $\mathbb{R}$.*

Exercise 16.32. *Consder the ring $\mathbb{Z}$ and two ideals $I = m\mathbb{Z}$ and $J = n\mathbb{Z}$. Show that*
(i) $I + J = \gcd(m, n)\mathbb{Z}$ (ii) $I \cap J = lcm(m, n)\mathbb{Z}$
(iii) $IJ = (mn)\mathbb{Z}$ (iv) $I \subseteq J$ iff $m|n$.

Exercise 16.33. *Let $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$ and $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \middle| b \in \mathbb{R} \right\}$. Show that I is a maximal ideal of R and $R/I \cong R$.*

Exercise 16.34. *Let $f : R \to R'$ be a non-trivial homomorphism from a field onto a ring R'. Show that R' is a field.*

Exercise 16.35. *Let R be a commutative ring with identity and R' be an integral domain with identity. If $f : R \to R'$ be a non-zero homomorphism, then show that $f(1_R) = 1_{R'}$.*
In the above problem, is R' is an integral domain essential? Justify your answer.

Exercise 16.36. *(i) Are fields $\mathbb{Q}$ and $\mathbb{R}$ are isomorphic? Justify.*
(ii) Are fields $\mathbb{R}$ and $\mathbb{C}$ isomorphic? Justify.
(iii) Are the rings $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ isomorphic? Justify.

Exercise 16.37. *Let R be a ring with identity such that $(xy)^2 = x^2y^2$ for all $x, y \in R$. Show that R is commutative ring. Is the above result true , if R does not have an identity?*

Exercise 16.38. *Let R be a finite ring with m elements and $\operatorname{char} R = n$. Show that $n|m$.*

Exercise 16.39. *Let R be a commutative ring with identity such that $\operatorname{char} R = p$ ($p-$prime). Show that $(a+b)^p = a^p + b^p$ for all $a, b \in R$. Is the above result true if p is not a prime.*

Exercise 16.40. *Show that the field of rational $\mathbb{Q}$ has no proper subfields.*

Exercise 16.41. *Let R be a ring with identity and a is a nilpotent element of R then show that $1 - a$ and $1 + a$ is unit in R.*

Exercise 16.42. *Find all idempotent elements of the ring $M_2(\mathbb{R})$.*

Exercise 16.43. *Let R be a ring with identity. Show that by means of an example that A is an ideal of B and B is an ideal of R but A is not an ideal of R.*

Exercise 16.44. *Give an example to show that quotient of a ring with zero divisors may be an integral domain.*

Exercise 16.45. *Let $R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$ be a ring. Show that R has no identity element but R has infinite number of left identity element.*

Exercise 16.46. *Let R be the set of differentiable functions $f : \mathbb{R} \text{ø} \mathbb{R}$. Prove that R is commutative ring with identity when addition and multiplication are defined by $(f+g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for all $x \in \mathbb{R}$. Show that $S = \{f \in R : f(0) = 0\}$ is an ideal of R. If $T = \{f \in R : Df(0) = 0\}$, where Df is derivative of f, then show that T is subring of R which is not an ideal of R also show that $S \cap T$ is an ideal of R.*

Exercise 16.47. *Show that the rings $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$ are not isomorphic.*

Exercise 16.48. *Let F be a field. Show that $(F, +)$ and $(F \setminus \{0\}, \cdot)$ is not isomorphic.*

Exercise 16.49. *Let R be a commutative ring and let B be the set of all idempotent elements of R. Define addition '$\oplus$' and multiplication '$\odot$' on B by $x \oplus y = x + y - 2xy$ and $x \odot y = xy$. Show that $(B, \oplus, \odot)$ is a Boolean ring.*

Exercise 16.50. *Show that every Boolean ring with identity can be embedded in Boolean ring with identity.*

Exercise 16.51. *Show that any ring without identity can be embedded in any ring with identity.*

Exercise 16.52. *Show that every integral domain is embedded in a field.*

Exercise 16.53. *Let* $R = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$ *and* $R' = M_2(\mathbb{R})$ *be two rings. Then both* R *and* R' *have identity elements namely* $1_R = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ *and* $1_{R'} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *respectively. Show that the inclusion mapping* $f : R \to R'$ *does not satisfy* $f(1_R) = 1_{R'}$.

Exercise 16.54. *Ler* $R \neq 0$ *be a commutative ring with identity having no zero divisor. If every proper subring of* R *is finite then show that* R *is a field.*

Exercise 16.55. *Define two binary operation '*$\oplus$*' and '*$\odot$*' on* $\mathbb{Z}$ *by*

$$a \oplus b = a + b - 1 \text{ and } a \odot b = a + b - ab \ \forall a, b \in \mathbb{Z}$$

Show that $(\mathbb{Z}, \oplus, \odot)$ *is a ring isomorphic to* $\mathbb{Z}, +, \cdot)$.

Exercise 16.56. *Show that the rings* $\mathbb{Z}$ *and* $\mathbb{Z} \times \mathbb{Z}$ *are not isomorphic. Is the groups* $(\mathbb{Z}, +)$ *and* $(\mathbb{Z} \times \mathbb{Z}, +)$ *isomorphic?*

Exercise 16.57. *Let* $f : R \to R'$ *be a ring homomorphism where* R, R' *are commutative ring with identity. Does* f *maps* (i) *idempotent elements to idempotent elements?*
(ii) *nilpotent elements to nilpotent elements?*
(iii) *Zero divisors to zero divisors?*

Exercise 16.58. *Let* e *be a central idempotent element of* R *i.e,* $e \in C(R)$ *and* $e^2 = e$. *Show that* eR *and* $(1 - e)R$ *are ideals of* R. *Also show that* $R = eR \oplus (1 - e)R$.

Exercise 16.59. *Let* $f : R \to R'$ *be a ring epimorphism. Justify each of the followings(either prove or disprove).*

(1) *If* R *is commutative then* R' *is commutative.*
(2) *If* R *has identity* 1_R *and* R' *has identity* $1_{R'}$ *then* $f(1_R) = 1_{R'}$.
(3) *If* R *has zero divisor then* R' *has zero divisor.*
(4) *If* R *is an integral domain then* R' *is also an integral domain.*
(5) *If* R *is a field then* R' *is a field.*

Exercise 16.60. *Find the total number of ring homomorphism from* $\mathbb{Z}/4\mathbb{Z}$ *to* $\mathbb{Z}/6\mathbb{Z}$.

Exercise 16.61. *Let* $P_1, P_2 \in spec\, R$. *Is* $P_1 \cap P_2 \in spec\, R$? *Justify.*

Exercise 16.62. *Let* R *be a commutative ring with identity and* $m \in maxspec\, R$ *such that* $m^2 = 0$ *then show that* R *is local.*

Exercise 16.63. *Let* R *be a commutative ring with identity in which every ideal of* R *is prime ideal then show that* R *is a field.*

Exercise 16.64. *Let* R *be a commutative ring with identity in which* A, B *be two distinct maximal ideals of* R *then show that* $AB = A \cap B$.

Exercise 16.65. *Let* $R = C[0, 1]$ *and for* $r \in [0, 1]$, $m_r = \{f \in C[0, 1] : f(r) = 0\}$. *Show that* $m_r \in maxspec\, R$.
Note that maximal ideals of R *is of the form* m_r *for some* $r \in [0, 1]$.

Exercise 16.66. *Is the ideal* $I = \{f \in C[0,1] : f(0) = 0 = f(1)\}$ *is a maximal ideal of* $C[0,1]$?

Exercise 16.67. *Let* R *be a commutative ring with identity such that for every* $x \in R$ *satisfies* $x^n = x$ *for some* $n > 1$. *Show that very prime ideal of* R *is maximal ideal.*

Exercise 16.68. *Let* R *and* R' *be two commutative ring with identity and* $f : R \to R'$ *be an epimorphism. Show that*
(1) $\ker f$ *is a prime ideal of* R *if* R' *is an integral domain.*
(2) $\ker f$ *is a maximal ideal of* R *if* R' *is a field.*

Exercise 16.69. *Let* R *be a ring and* P *be an ideal of* R *containing an ideal* I *of* R. *Show that*
(1) $P \in spec\, R$ *iff* $P/I \in spec(R/I)$.
(2) $P \in maxspec\, R$ *iff* $P/I \in mspec(R/I)$.

Exercise 16.70. *Let* (R, m, K) *be a local ring then only idempotent elements of* R *is* $0, 1$.

Exercise 16.71. *Let* $f : R \to S$ *be a ring homomorphism. Let* $P \in spec\, S$ *then show that* $f^{-1}P \in spec\, R$. *Does the above result true if* P *is a maximal ideal.*

Exercise 16.72. *Suppose,* A, B *are comaximal ideals of* R *and* A, C *are comaximal ideals of* R. *Show that* A, BC *are comaximal.*

Exercise 16.73. *Show that* $R = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Q} \right\}$ *is a non commutative subring of* $M_2(\mathbb{Q})$. *If* $I = \{A \in R : A^2 = 0\}$ *then show that* I *is an ideal of* R *and* $R/I \cong \mathbb{Q}$.

Exercise 16.74. *Show that* $\mathbb{Z} \times \{0\}$ *is a prime ideal of* $\mathbb{Z} \times \mathbb{Z}$ *but not a maximal ideal of* $\mathbb{Z} \times \mathbb{Z}$.

Exercise 16.75. *Let* R *be a commutative ring with identity then prove that there exists an epimorphism from* R *onto some field.*

Exercise 16.76. *Let* R *be a commutative regular ring with identity then every prime ideal of* R *is a maximal ideal.*

Exercise 16.77. *Show that there does not exists*
(1) An epimorphism from $\mathbb{Z}/24\mathbb{Z}$ *onto the ring* $\mathbb{Z}/7\mathbb{Z}$.
(2) A monomorphism from $\mathbb{Z}/6\mathbb{Z}$ *to* $\mathbb{Z}/11\mathbb{Z}$.

Exercise 16.78. *Show that the ring of integer is not isomorphic to any of its proper subring.*

Exercise 16.79. *Show that any homomorphism from a field to any ring either monomorphism or zero homomorphism.*

Exercise 16.80. *Let* R *be a commutative ring with identity and* $S = R \times R$. *We define two binary operation '*$+$*' and '*$\cdot$*' on* S *by* $(a, b) + (c, d) = (a + c, b + d)$ *and* $(a, b) \cdot (c, d) = (ac + bd, bc + ad)$ *for all* $(a, b), (c, d) \in S$. *Show that* S *is a commutative ring with identity having zero divisors. Prove that if* R *is an integral domain then then the zero divisors of* S *are of the form* (a, a) *and* $(a, -a)$.

Exercise 16.81. *Let S be any arbitrary set and $\mathcal{P}(S)$ be its power set. Define '$+$' and '$\cdot$' by $X + Y = X\Delta Y = (X \setminus Y) \cup (Y \setminus X)$ and $X \cdot Y = X \cap Y$ for all $X, Y \in \mathcal{P}(S)$. Show that $(\mathcal{P}(S), \Delta, \cap)$ is a commutative ring with identity having zero divisors such that each element is idempotent.*

Exercise 16.82. *Let p be a prime number. Show that there are two non-isomorphic rings with p elements.*

Exercise 16.83. *How many non-isomorphic rings are there of order 105? Justify.*

Exercise 16.84. *Let x be an nilpotent element and y be an unit of a commutative ring with identity R. Show that $x+y$ is also a unit in R. For $y = 1$ is commutativity necessary? Justify. If the element x, y do not commute then show that the above property does not hold.*

Exercise 16.85. *Show that the ring $\mathbb{Z}/n\mathbb{Z}$ has non-zero nilpotent elements if and only if n is not square free.*

Exercise 16.86. *In a ring R with identity such that $x^6 = x$ for all $x \in R$. Show that $x^2 = x$ for all $x \in R$.*

Exercise 16.87. *Let R be a ring with identity and e be an idempotent element in R such that $e \neq 0, 1$. Show that e is a zero divisor.*

Exercise 16.88. *Let R be a ring, $a \in R$ and $b(\neq 0) \in R$ such that $aba = 0$. Show that a is a left or right zero divisor in R.*

Exercise 16.89. *Give an example of ring homomorphism $f : R \to R'$ and an ideal I of R such that $f(I)$ is not an ideal of R'.*

Exercise 16.90. *Let R be a ring with identity. If $ab + ba = 1$ and $a^3 = a$ then show that $a^2 = 1$.*

Exercise 16.91. *If $ab = a$ and $ba = b$ in a ring then show that $a^2 = a$ and $b^2 = b$.*

Exercise 16.92. *Let R be a commutative ring with identity. If I and J are comaximal ideal of R then show that I^2 and J^2 are comaximal ideal.*

Exercise 16.93. *Let R be a commutative ring with identity. Show that R is a field if and only if R has no nonzero proper ideals.*

Exercise 16.94. *Show that $\mathbb{Z}/2\mathbb{Z} \cong 5\mathbb{Z}/10\mathbb{Z}$ as ring.*

Exercise 16.95. *Let R be the set of all rationals of the form a/b (in lowest terms) such that b is not a multiple of 3. Show that R is a subring of $\mathbb{Q}$.*
Let I be a subset of R consisting of those elements whose numerators are divisible by 3. Prove that I is an ideal of R. Also show that R/I is a field.

Exercise 16.96. *Let R be a ring and I be a left ideal, J be a right ideal of R. Show that R is a regular ring if and only if $IJ = I \cap J$.*

Exercise 16.97. *Show that the center of a regular ring is regular.*

Exercise 16.98. *Let R be a regular ring. If I is an ideal of R and J is an ideal of J then show that J is an ideal of R.*

Exercise 16.99. *Let R be an integral domain and let F be a field such that $F \subset R$. If R is a finite dimensional vector space over F then show that R is a field.*

Exercise 16.100. *Let $I = \langle x^2 + x + 1 \rangle$. Is $\mathbb{Z}_3[x]/I$ an integral domain? Justify.*

Exercise 16.101. *Show that $\langle x^2 + 1 \rangle$ is not an prime ideal of $\mathbb{Z}_2[x]$.*

Exercise 16.102. *Show that any non zero ideal of a PID if a unique product of prime ideals.*

Exercise 16.103. *Find $\gcd(2, x)$ in $\mathbb{Z}[x]$ and show that it can not be put in the form $2r(x) + xs(x)$ for some $r(x), s(x) \in \mathbb{Z}[x]$.*

Exercise 16.104. *Let R be an integral domain the n prove that R and $R[x]$ have same characteristic.*

Exercise 16.105. *Let $R = \mathbb{Z} \times \mathbb{Z}$. Show that the polynomial $(1, 0)x$ has infinitely many roots in R.*

Exercise 16.106. *Let R be an integral domain then show that units of $R[x]$ is contained in R.*

Exercise 16.107. *Let $f : R \to S$ be a epimorphism of rings. If R is an PIR then show that S is also a PIR. Does the result hold for PID Justify.*

Exercise 16.108. *Prove that the ring $\mathbb{Z}/n\mathbb{Z}$ is a PIR for all n.*

Exercise 16.109. *In $\mathbb{Z}[i]$ find the $\gcd(2-7i, 2+11i)$. Also find x, y such that $\gcd(2-7i, 2+11i) = x(2-7i) + y(2+11i)$.*

Exercise 16.110. *Let I be set of all non- units of $\mathbb{Z}[i]$. Is I is an ideal? Show that for any non-trivial ideal P of $\mathbb{Z}[i]$, the quotient ring $\mathbb{Z}[i]/P$ is finite ring.*

Exercise 16.111. *In $\mathbb{Z}[i]$, show that 3 is a prime element but 5 is not a prime element.*

Exercise 16.112. *Show that the polynomial ring $\mathbb{Q}[x, y]$ is UFD but not PID.*

Exercise 16.113. *If $f(x)$ is an irreducible polynomial over $\mathbb{R}$ then show that either $f(x)$ is linear or $f(x)$ is quadratic. The irreducible polynomial in $\mathbb{C}[x]$ is exactly the linear polynomials.*

Exercise 16.114. *Show that there only three irreducible monic polynomials over $\mathbb{Z}/3\mathbb{Z}$. In general, for a prime p find the number of irreducible monic polynomial over $\mathbb{Z}/p\mathbb{Z}$.*

Exercise 16.115. *Let R be a commutative ring with identity such that $R[x]$ is PID then show that $R[x]$ is ED.*

Exercise 16.116. *Is the quotient ring $\mathbb{C}[x]/\langle x^2 + 1 \rangle$ an integral domain?*

Exercise 16.117. *Show that* (i) $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$.
(ii) $\mathbb{Z}[x]/\langle n, x \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

Exercise 16.118. *Show that x^3+mx+n is irreducible in $\mathbb{Z}[x]$ whenever m and n are odd number.*

Exercise 16.119. *Show that the polynomial $f(x) = x^{2222} + 2x^{2220} + 4x^{2218} + \cdots + 2220x^2 + 2222$ is irreducible in $\mathbb{Z}[x]$.*

Exercise 16.120. *Let F be a field. Prove that $\sum_{i\geq 0} a_i x_i \in F[x]$ is a unit iff $a_0 \neq 0$.*

Exercise 16.121. *Let $\alpha = \frac{a}{2^b}$ where a is an odd integer and $b > 0$. Verify that $\mathbb{Z}[\alpha] = \mathbb{Z}\left[\frac{1}{2}\right]$ and that any element of this ring can be uniquely written as $\frac{m}{2^n}$ where m is odd and $n \geq 0$. Find units of this rings.*

Exercise 16.122. *Let S be the set of odd prime numbers. Let $R = \mathbb{Z}\left[\left\{\frac{1}{p}\right\}_{p\in S}\right]$. Prove that every element of R can be written as $\frac{a}{b}2^n$ where a, b are odd and $n >\geq 0$. Find the units in R. Deduce that every non-zero ideal in R is of the form $2^n R$ for $n \geq 0$.*

Exercise 16.123. *Let R be a ring. Let $a_1, \cdots, a_n \in R$. Prove that the map $R[x_1, \cdots, x_n] \xrightarrow{\phi} R[x_1, \cdots, x_n]$ sending $x_i \mapsto x_i - a_i$ is an $R-$linear isomorphism. Deduce that every $f \in R[x_1, \cdots, x_n]$ admits a unique expansion $f = \sum c_{j_1 \cdots j_n}(x_1 - a_1)^{j_1} \cdots (x_n - a_n)^{j_n}$.*

Exercise 16.124. *Prove that there is a unique $R-$linear isomorphism*

$$R[x_1, \cdots, x_m, y_1, \cdots, y_n] \to R[\tilde{x_1}, \cdots, \tilde{x_m}][\tilde{y_1}, \cdots, \tilde{y_n}]$$

sending $x_i \mapsto \tilde{x_i}$ and $y_j \mapsto \tilde{y_j}$.

Exercise 16.125. *Find the $\gcd(2x^4 + 3x^3 + 6x^2 + 3x + 2, 2x^4 + 2x^3 + 5x^2 + x + 2)$ in $\mathbb{Q}[x]$. Express the gcd as a linear combination of these two polynomial.*

Exercise 16.126. *Fix $n > 0$ in $\mathbb{Z}$. Set $R := \mathbb{Z}[\frac{1}{n}]$. Prove that for any ideal $I \subseteq R, I \cap \mathbb{Z} \cdot R = I$. Deduce that R is a PID. Find all prime elements(upto associates) in R.*

Exercise 16.127. *Let $R = F[x, y]$ where F is a field. Let $m = \langle a, b\rangle$. For each $k > 1$, find a minimal generating set for m^k.*

Exercise 16.128. *Find elements that are irreducible but not primes in (1) $R = \mathbb{Q}[t^2, t^3]$, (2) $\mathbb{Z}[2i]$.*

Exercise 16.129. *Let $R = \mathbb{Z}[\sqrt{-5}]$. Let $I_1 = \langle 1 + \sqrt{-5}, 2\rangle, I_2 = \langle 1 - \sqrt{-5}, 2\rangle, J_1 = \langle 1 + \sqrt{-5}, 3\rangle, J_2 = \langle 1 - \sqrt{-5}, 3\rangle$. Verify the followings:*
(1) $I_1 = I_2$, (2) $I_1 I_2 = \langle 2\rangle$, (3) $J_1 J_2 = \langle 3\rangle$, (4) $I_1 \cdot J_1 = \langle 1 + \sqrt{-5}\rangle$, (5) $I_2 J_2 = \langle 1 - \sqrt{-5}\rangle$, (6) $R = I_1 + J_1 = I_1 + J_2 = J_1 + J_2$.

Exercise 16.130. *Let R be a ring. Let $a_1, \cdots, a_n \in R$. Consider the evaluation map $R[x_1, \cdots, x_n] \xrightarrow{\phi} R$ sending $f(x_1, \cdots, x_n)$ to $f(a_1, \cdots, a_n)$. Prove that $\ker \phi = \langle x_1 - a_1, \cdots, x_n - a_n\rangle$.*

Exercise 16.131.

Exercise 16.132.

17. Appendix II

Cartesian product, Partially ordered set and Zorn's lemma

17.1. Cartesian Product.

Definition 17.1. *Let A, B be two set, we define Cartesian product of two set as*

$$A \times B := \{(a, b) : a \in A, b \in B\}.$$

Now, we give an alternative definition of Cartesian product.

Definition 17.2. *Let I be an indexing set and let $\{A_i\}_{i\in I}$ be collection of sets. A choice function f is any function*

$$f : I \to \bigcup_{i\in I} A_i$$

such that $f(i) = A_i$ for all i.

Definition 17.3. *We define $\prod_{i\in I} A_i = \left\{ f : I \to \bigcup_{i\in I} A_i : f(i) \in A_i, \forall i \in I \right\}$ i.e., set of all choice function from I to $\bigcup_{i\in I} A_i$ and is denoted by $\prod_{i\in I} A_i$ (where if any A_i is empty or I is empty then Cartesian product is empty). The elements of Cartesian product is denoted by $\prod_{i\in I} a_i$ where this denote the choice function $f(i) = a_i$ for all $i \in I$.*

If $I = \{1, 2, \cdots, n\}$ for some $n \in \mathbb{N}$ and if f is a choice function from I to $A_1 \cup A_2 \cup \cdots \cup A_n$ where each A_i is non empty, we can associates to f a unique ordered n-tuple:

$$f \to (f(a_1), f(a_2), \cdots, f(a_n))$$

Note that by definition of a choice function $f(i) \in A_i$ for all i, so the above n-tuple has an element of A_i in the i^{th} position for each i.
Conversely, given an n-tuple $(a_1, \cdots, a_n)$ where $a_i \in A_i$ for all i, there is a unique choice function, f from I to $\bigcup_{i\in I} A_i$ associated to it, namely

$$f(i) = a_i, \quad \text{for all } i \in I.$$

Thus there is an one-to-one correspondence between ordered n-tuple and elements of $\prod_{i\in I} A_i$. Therefore, from now we can write the elements of $\prod_{i\in I} A_i$ as ordered n-tuple.

If $I = \mathbb{N}$, we shall similarly write $\prod_{i=1}^{\infty} A_i$ or $A_i \times A_2 \times \cdots$ for the Cartesian product of A_i's and we shall write the ordered n-tuple as $(a_1, a_2, \cdots)$ i.e., infinite sequences whose i^{th} term is in A_i.
Note that when $I = \{1, \ldots, n\}$ or $\mathbb{N}$ then we have used natural ordering of I to arrange the elements of our Cartesian products into n-tuple. Any other ordering gives rise to a different representation of the elements of the same Cartesian product.

Example 17.4. $\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$ *is the usual n-tuple from real entries.*
Suppose, $I = \mathbb{N}$ *then* $\prod_{i=1}^{\infty} A_i$ *where* $A_i = A$ *denote the set of infinite sequence. In particularly if* $A = \mathbb{R}$ *then* $\prod_{i=1}^{\infty} A_i$ *is the set of all real sequence.*

Proposition 17.5. *Let* I *be a non-empty countable set and for each* $i \in I$ *let* A_i *be a set. Then*

$$\left| \prod_{i \in I} A_i \right| = \prod_{i \in I} |A_i|$$

Proof.

17.2. **Partially ordered set and Zorn's lemma.**

Definition 17.6. *A partial order on a non-empty set A is a relation $\leq$ on A satisfying*
(1) *$x \leq x$ for all $x \in A$ i.e., $\leq$ is reflexive,*
(2) *if $x \leq y$ and $y \leq x$ then $x = y$ for all $x, y \in A$(anti-symmetric),*
(3) *if $x \leq y$ and $y \leq z$ then $x \leq z$ for all $x, y, z \in A$ (transitive).*

Definition 17.7. *Let $(A, \leq)$ be a non-empty partially ordered set*
(1) *A subset B of A is called chain if for all $x, y \in B$ either $x \leq y$ or $y \leq x$.*
(2) *An upper bound for a subset B of an element $u \in A$ such that $b \leq u$ for all $b \in B$.*
(3) *A maximal element of A is an element $m \in A$ such that if $m \leq x$ for any $x \in A$, then $m = x$.*

A chain is also called a tower or called a totally ordered or linearly ordered subset.

Example 17.8.

Exercise 17.9. *Show that in a partially ordered set maximal element may not be unique.*

Exercise 17.10. *When maximal element in a partially ordered set is unique?*

Definition 17.11. *Let $(X, \leq)$ be an partial ordered set. X is said to be linearly ordered if any two elements of X are comparable.*

Zorn's lemma: Let $(A, \leq)$ be a non-empty partially ordered set such that every chain has an upper bound, then A has a maximal element.
The Axiom of Choice: Cartesian product of non-empty set indexed by non-empty set is non-empty.
Hausdroff's maximality principle: Every partial ordered set has a maximal linearly ordered subset.

Definition 17.12. *Let A be a non-empty set. A well ordering on A is a total ordering on A such that every non-empty subset of A has a minimum element, i.e., for each non-empty $B \subseteq A$ there is some $s \in B$ such that $s \leq b$, for all $b \in B$.*

Well-ordering Principle: Every non-empty set can be well ordered.

Theorem 17.13. *Assuming the usual(Zermelo-Frankel)axioms of set theory, the following are equivalent:*

(1) *Well ordering principle*
(2) *Zorn's lemma*
(3) *Axiom of choice*
(4) *Hausdroff's maximality principle*

Proof. See Topology-Dugunji.

It is noted that $\mathbb{R}$ is a vector space over $\mathbb{Q}$ where $\dim_{\mathbb{Q}} \mathbb{R}$ is infinite (prove!). Now $\{1, \sqrt{2}\}$ is linearly independent set over $\mathbb{Q}$ (why)? so we can extend this set of a basis of $\mathbb{R}$. Let β be that basis. Then any $c \in \mathbb{R}$ we can write

$$c = c_1\sqrt{2} + \text{ finite sum}$$

Now we define a function $f : \mathbb{R} \to \mathbb{R}$ as follow

$$f(x) = \begin{cases} c_1, & \text{if } c_1 \neq 0 \\ 0, & \text{if } c_1 = 0 \end{cases}$$

Check that this function is well defined and prove the following: $f(x+y) = f(x) + f(y)$ and f is discontinuous at 0 not only that f is continuous no where on $\mathbb{R}$.

$\xrightarrow{vvsxk;sklsklsgvklsdklgdskldsklvdklsvdlsbsdlbdsilofbss} jhhj$

Definition 17.14. *jjj*

Question 17.15. *fgfg*

Question.

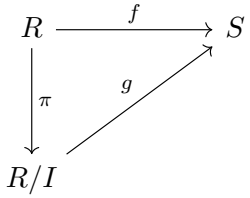
qns*

qns*

$\mathbb{ABCDEFGHIJKLMNOPQRSTUVWXYZ}$

GFGFG $\mathcal{ABCDEFGHIJKLMNOPQRSTUVWXYZ}$

Theorem 17.16 (First isomorphism theorem)**.** *Let $\phi : R \to S$ be a ring morphism and $I \subseteq \operatorname{Ker} f$ is an ideal of R. Then there is an unique ring morphism $g : R/I \to S$ such that the diagram commutes i.e.,*



Moreover,

(1) *If $I = \operatorname{Ker} f$ then g is injective, therefore, $R/\operatorname{Ker} f \cong \operatorname{Im} f$.*
(2) *$\operatorname{Im} f = \operatorname{Im} g$.*
(3) *If f is onto, then $R/\operatorname{Ker} f \cong S$.*

Proof. $\bigcup_{i=1}^{n} S_i$

$\lim_{n\to\infty} x_n = s$

$\int_a^b f(x)dx$

$\frac{a}{b}$ $\overline{\frac{a}{B}}$

$S = f = \{d\} = \{f : G \to G : f \text{ is a} \quad \text{group} \qquad \text{morphim}\}$

$\binom{a}{a}\sqrt{7}$