Abstract Algebra

- A Journey from Concretization to Abstraction -

Ji, Yong-Hyeon

A document presented for
the Abstract Algebra

Department of Information Security, Cryptology, and Mathematics
College of Science and Technology
Kookmin University

August 12, 2024

Contents

Chapter 1

Visual Group Theory

Mathematical Definitions and Examples

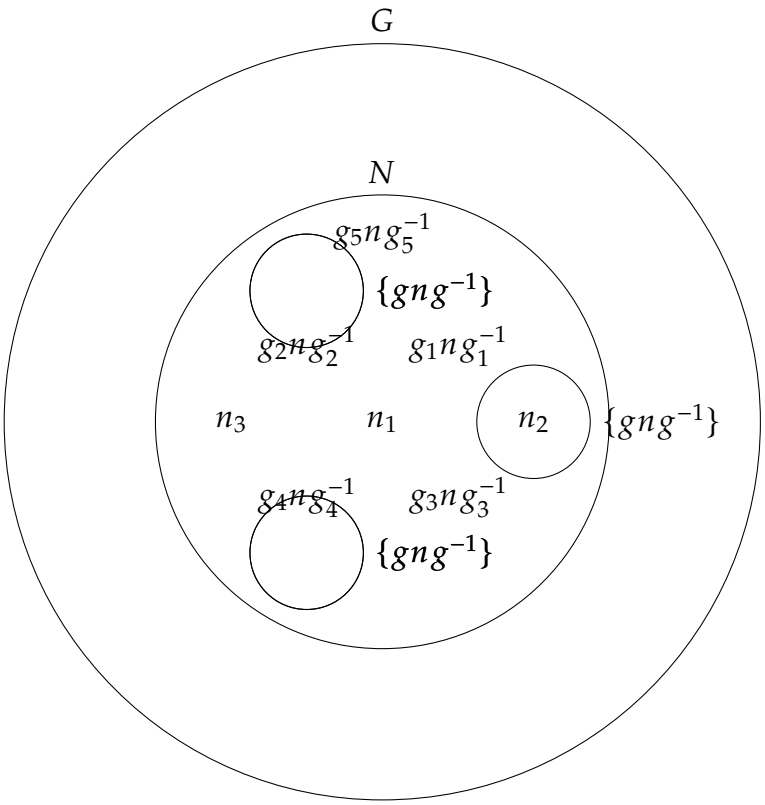
1. Normal Subgroup

Definition:

A subgroup N of a group G is called a *normal subgroup* if it is invariant under conjugation, that is, for every element $g \in G$ and $n \in N$, the element $gng^{-1} \in N$.

Symbolically:

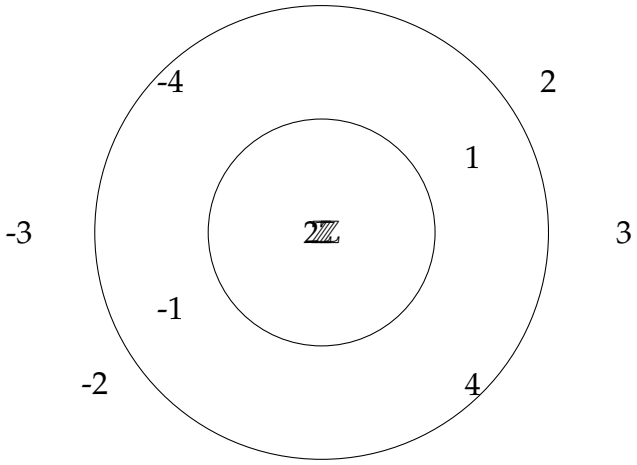
$$N \triangleleft G \iff \forall g \in G, \forall n \in N,\ gng^{-1} \in N.$$



Examples:

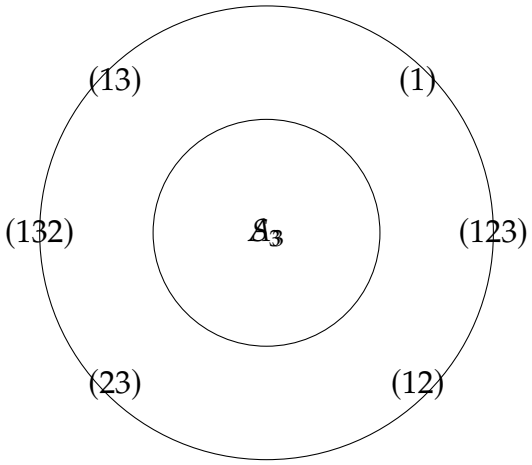
1. In the group of integers $(\mathbb{Z}, +)$, the subgroup $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ is a normal subgroup since $\mathbb{Z}$ is abelian.

$$2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\} \triangleleft \mathbb{Z}$$



2. In the symmetric group S_3, the subgroup $A_3 = \{(1), (123), (132)\}$ (the alternating group) is a normal subgroup.

$$A_3 = \{(1), (123), (132)\} \triangleleft S_3$$



2. Quotient Group (Factor Group)

Definition:

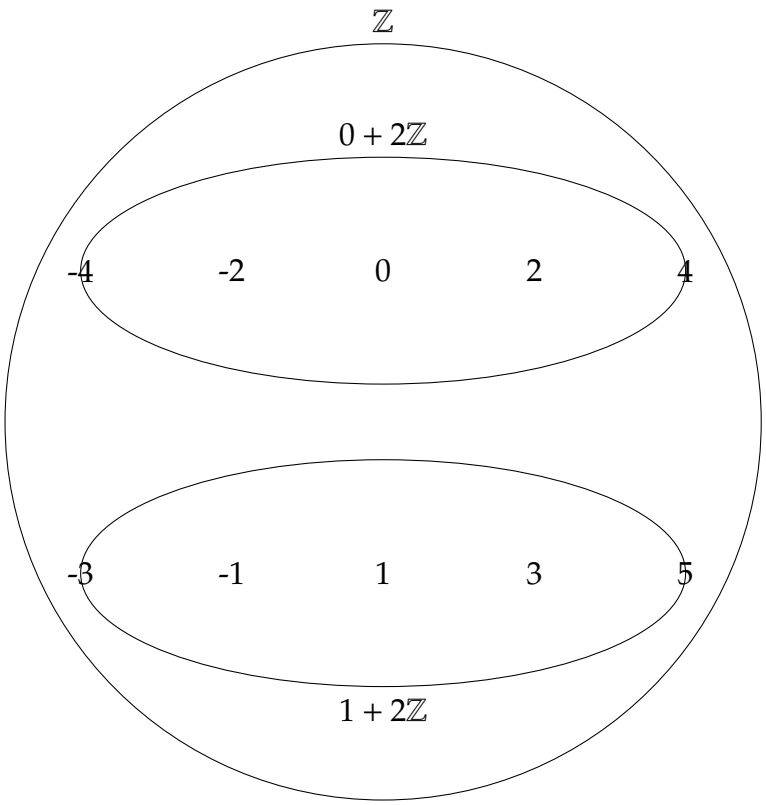
Given a group G and a normal subgroup N of G, the *quotient group* (or *factor group*) G/N is the set of left cosets of N in G with the group operation defined by:

$$(gN) \cdot (hN) = (gh)N$$

Examples:

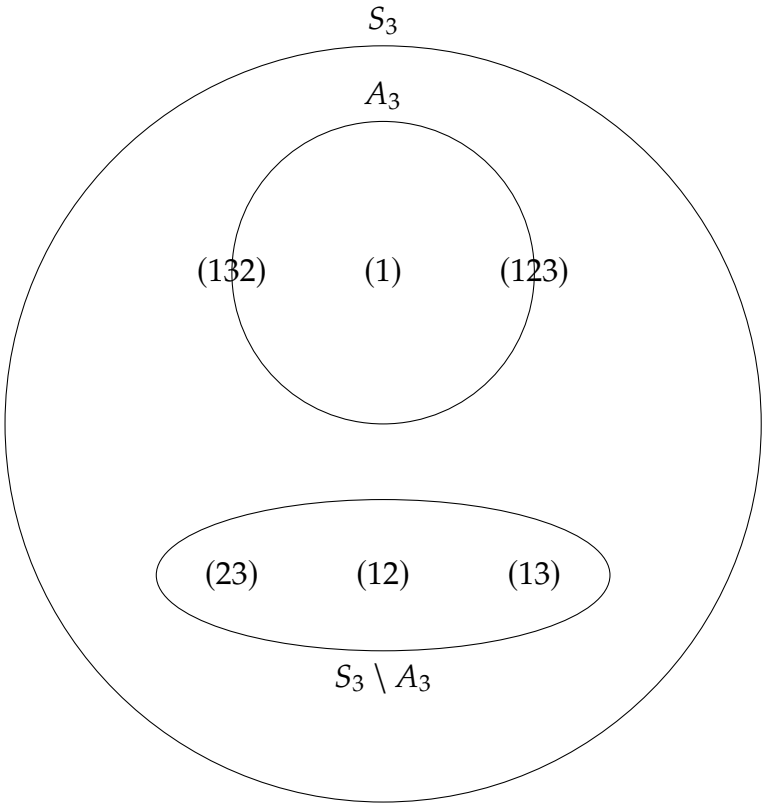
1. For $(\mathbb{Z}, +)$ and $N = 2\mathbb{Z}$, the quotient group $\mathbb{Z}/2\mathbb{Z}$ consists of two cosets: $0 + 2\mathbb{Z}$ and $1 + 2\mathbb{Z}$.

$$\mathbb{Z}/2\mathbb{Z} = \{0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}\}$$



2. In S_3, the quotient group S_3/A_3 is isomorphic to $\mathbb{Z}_2$.

$$S_3/A_3 \cong \mathbb{Z}_2$$



3. Ring

Definition:

A *ring* is a set R equipped with two binary operations $+$ and $\cdot$ (addition and multiplication) such that:

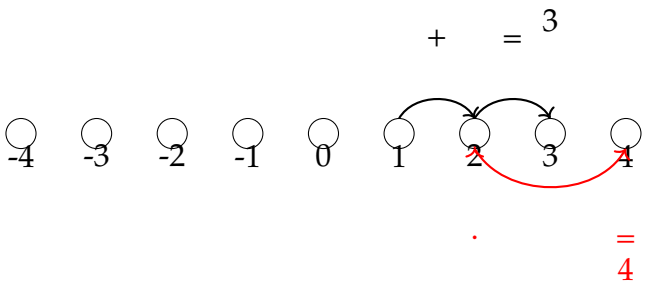
1. $(R, +)$ is an abelian group.

2. $(R, \cdot)$ is a monoid.

3. Multiplication is distributive over addition: for all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

Examples:
1. The set of integers $\mathbb{Z}$ with usual addition and multiplication.

$\mathbb{Z}$ is a ring



2. The set of 2×2 matrices over $\mathbb{R}$, $M_2(\mathbb{R})$, with matrix addition and multiplication.

$M_2(\mathbb{R})$ is a ring

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 6 & 8 \\ 10 & 12 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix}$$

4. Ideal

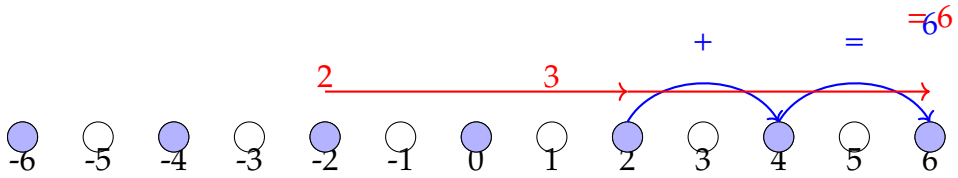
Definition:
An *ideal* I of a ring R is a subset of R such that:

1. I is an additive subgroup of R.

2. For every $r \in R$ and $i \in I$, both ri and ir are in I.

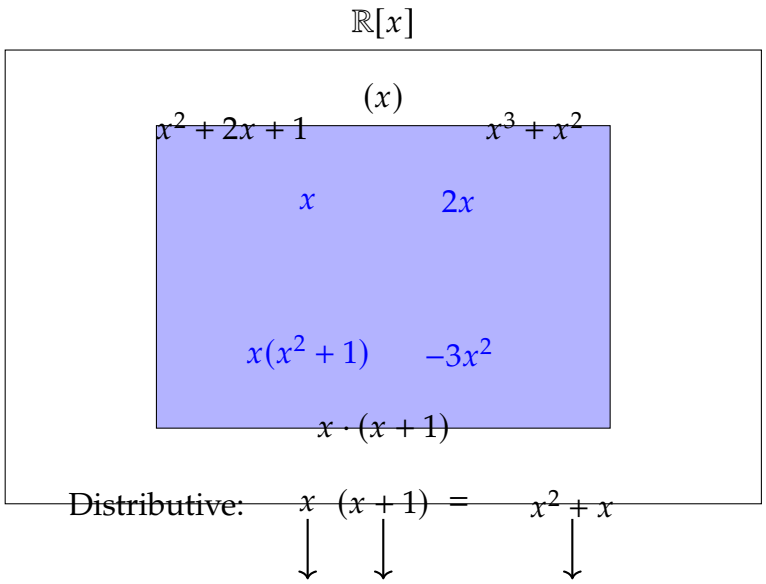
Examples:
1. In $\mathbb{Z}$, the set $2\mathbb{Z}$ (all even integers) is an ideal.

$$2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\} \text{ is an ideal of } \mathbb{Z}$$



2. In the ring $\mathbb{R}[x]$, the set of polynomials divisible by x, denoted by (x), is an ideal.

$$(x) = \{x \cdot f(x) \mid f(x) \in \mathbb{R}[x]\} \text{ is an ideal of } \mathbb{R}[x]$$



5. Prime Ideal

Definition:

An ideal P in a ring R is a *prime ideal* if $P \neq R$ and whenever $a \cdot b \in P$ for $a, b \in R$, then $a \in P$ or $b \in P$.

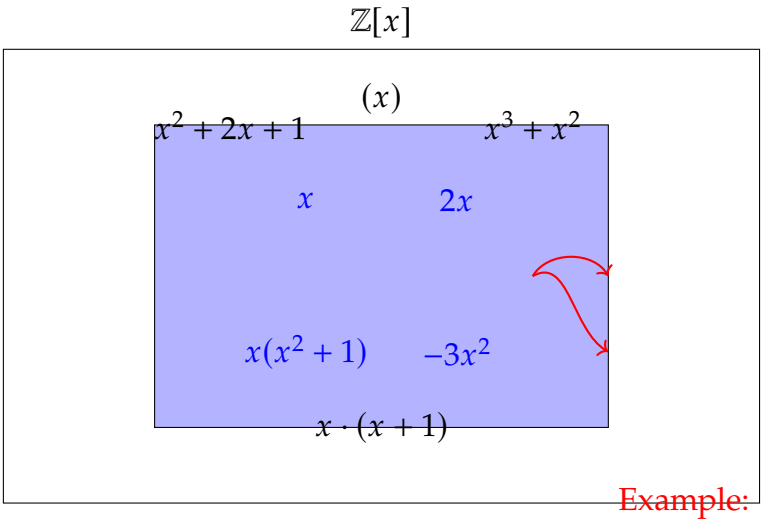
Examples:

1. In $\mathbb{Z}$, the ideal (p) where p is a prime number (e.g., (5)) is a prime ideal.

$$(5) = \{5k \mid k \in \mathbb{Z}\} \text{ is a prime ideal of } \mathbb{Z}$$

2. In $\mathbb{Z}[x]$, the ideal (x) is a prime ideal.

$$(x) = \{x \cdot f(x) \mid f(x) \in \mathbb{Z}[x]\} \text{ is a prime ideal of } \mathbb{Z}[x]$$



~~Example:~~
$(x + 1) \cdot x = x^2 + x$
$(x^2 + x) \in (x)$ implies
$(x + 1) \in \mathbb{Z}[x]$ or $x \in (x)$

6. Maximal Ideal

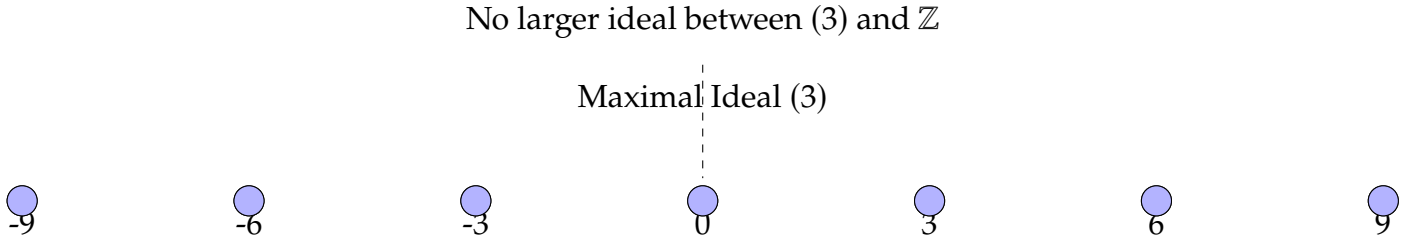
Definition:

An ideal M in a ring R is a *maximal ideal* if $M \neq R$ and there are no other ideals I such that $M \subset I \subset R$.

Examples:

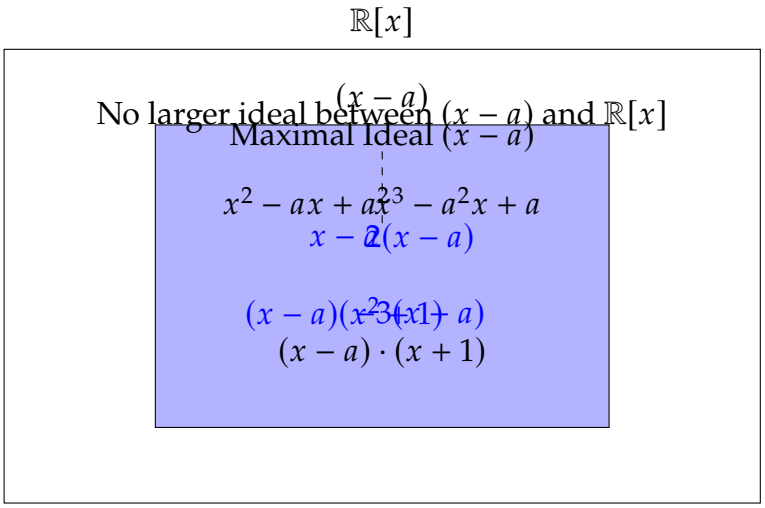
1. In $\mathbb{Z}$, the ideal (p) where p is a prime number (e.g., (3)) is a maximal ideal.

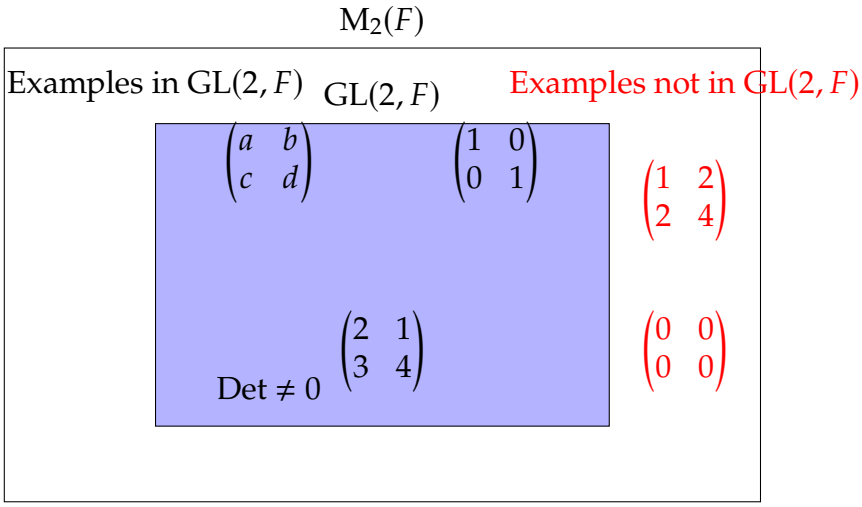
$$(3) = \{3k \mid k \in \mathbb{Z}\} \text{ is a maximal ideal of } \mathbb{Z}$$

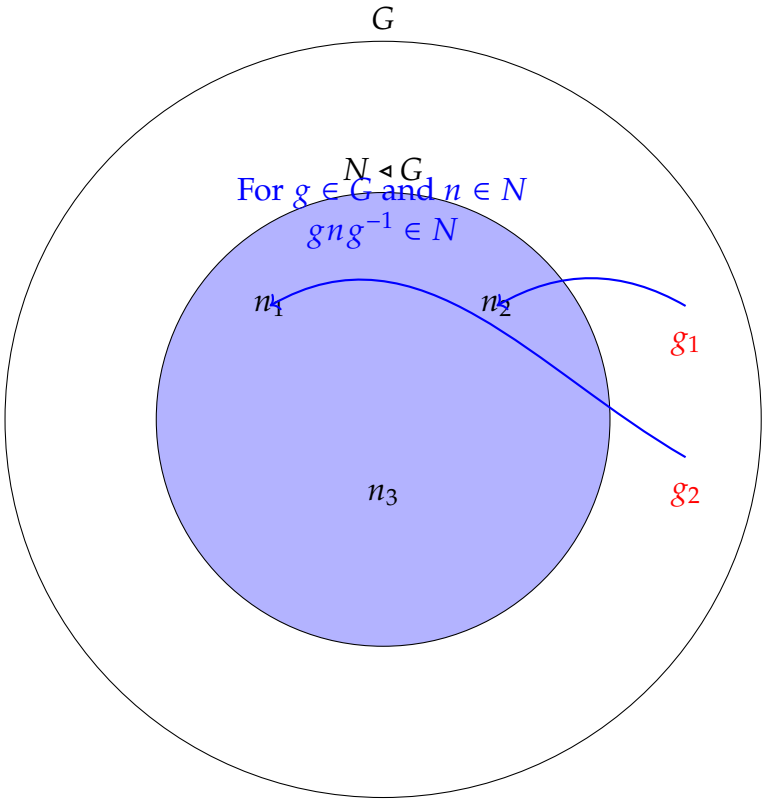


2. In $\mathbb{R}[x]$, the ideal $(x - a)$ where $a \in \mathbb{R}$ is a maximal ideal.

$$(x - a) = \{(x - a) \cdot f(x) \mid f(x) \in \mathbb{R}[x]\} \text{ is a maximal ideal of } \mathbb{R}[x]$$


$\mathbb{R}[x]$
No larger ideal between $(x-a)$ and $\mathbb{R}[x]$
$(x-a)$
Maximal Ideal $(x-a)$
$x^2 - ax + ax^{23} - a^2x + a$
$x - a(x-a)$
$(x-a)(x^{23}(x1) + a)$
$(x-a)\cdot(x+1)$


$M_2(F)$
Examples in GL(2, F)
GL(2, F)
Examples not in GL(2, F)
$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$
$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$
Det ≠ 0
$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$


G
$N \triangleleft G$
For $g \in G$ and $n \in N$
$gng^{-1} \in N$
n_1
n_2
n_3
g_1
g_2

Chapter 2

A Mapping $\mathbb{C}[x] \longrightarrow \mathbb{C}$

2.1 Observation

Mapping	$\psi_p : \mathbb{Z} \longrightarrow \mathbb{Z}_p$ $n \longmapsto n \bmod p = \psi_p(n)$	$\phi_a : \mathbb{C}[x] \longrightarrow \mathbb{C}$ $f(x) \longmapsto f(a) = \phi_a(f(x))$
Additive Homo.	$\psi_p(a+b) := (a+b) \bmod p$	$\phi_a(f+g) := f(a) + g(a)$
Multiplicative Homo.	$\psi_p(ab) := (ab) \bmod p$	$\phi_a(fg) := f(a)g(a)$
Kernel	$\ker(\psi_p) = p\mathbb{Z}$	$\ker(\phi_a) = (x-a)\mathbb{C}[x]$
Image	$\mathbb{Z}_p$	$\mathbb{C}$
Ideal	$p\mathbb{Z} = \langle p \rangle$	$(x-a)\mathbb{C}[x] = \langle x-a \rangle$
Prime Ideal	$\langle p \rangle$ is prime	$\langle x-a \rangle$ is prime
Maximal Ideal	$\langle p \rangle$ is maximal	$\langle x-a \rangle$ is maximal
Isomorphism	$\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$	$\mathbb{C} \simeq \mathbb{C}[x]/\langle x-a \rangle$

Theorem 2.1.1 *Every ideal I of ring R is the kernel of some ring homomorphism.*

Proof. Let I is an ideal in a ring R, that is, I is a subset of R that satisfies:

-

□

Non-Commutative Rings Without Unity and Prime Ideals

Example 1: The Ring of 2x2 Upper Triangular Matrices Over a Field $\mathbb{F}$

Consider the ring R of 2x2 upper triangular matrices over a field $\mathbb{F}$:

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{F} \right\}$$

This ring is non-commutative and does not have a unity element.

Prime Ideal

An ideal P in R can be the set of matrices where the (1,2)-entry is zero:

$$P = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{F} \right\}$$

To see why P is a prime ideal, consider matrices A and B in R. If the product $AB \in P$, then the (1,2)-entry of AB must be zero. This means either the (1,2)-entry of A is zero or the (1,2)-entry of B is zero, implying $A \in P$ or $B \in P$. Thus, P is a prime ideal.

Example 2: The Ring of Polynomials in Two Non-commuting Variables Over a Field $\mathbb{F}$

Consider the ring $R = \mathbb{F}\langle x, y \rangle$, the ring of polynomials in two non-commuting variables x and y over a field $\mathbb{F}$.

Prime Ideal

An ideal P in R can be generated by the commutator $[x, y] = xy - yx$:

$$P = (xy - yx)$$

To see why P is a prime ideal, consider two polynomials f and g in R. If $fg \in P$, then fg can be written as a multiple of $xy - yx$. If $xy - yx$ divides fg, then either $xy - yx$ divides f or $xy - yx$ divides g, meaning $f \in P$ or $g \in P$. Thus, P is a prime ideal.

Proof: Existence of a Basis for Any Vector Space using Zorn's Lemma

Theorem: Every vector space V over a field F has a basis.

Proof: To prove this, we will use Zorn's Lemma, which states:

> If every chain (totally ordered subset) of a partially ordered set S has an upper bound in S, then S contains at least one maximal element.

1. **Set Construction:** Define the set C to be the collection of all linearly independent subsets of V:
$$C = \{S \subseteq V \mid S \text{ is linearly independent}\}$$

2. **Partial Order:** Partially order C by inclusion: $S \leq T$ if $S \subseteq T$.

3. **Chain:** Let $\mathcal{A}$ be a chain in C. This means that every pair of elements in $\mathcal{A}$ is comparable under $\subseteq$. For each pair $S, T \in \mathcal{A}$, either $S \subseteq T$ or $T \subseteq S$.

4. **Upper Bound for Chain:** Define $U = \bigcup_{S \in \mathcal{A}} S$. We claim that $U \in C$, i.e., U is a linearly independent subset of V.

   - Suppose for contradiction that U is not linearly independent. Then there exists a finite subset $\{u_1, u_2, \ldots, u_n\} \subseteq U$ and scalars $a_1, a_2, \ldots, a_n \in F$, not all zero, such that:
   $$a_1 u_1 + a_2 u_2 + \cdots + a_n u_n = 0$$
   - Each u_i belongs to some $S_i \in \mathcal{A}$, and since $\mathcal{A}$ is a chain, there exists an $S \in \mathcal{A}$ such that $u_1, u_2, \ldots, u_n \in S$.
   - But S is linearly independent, so the only solution to this linear combination is $a_1 = a_2 = \cdots = a_n = 0$, a contradiction.

   Thus, U must be linearly independent, and $U \in C$ is an upper bound for the chain $\mathcal{A}$.

5. **Application of Zorn's Lemma:** By Zorn's Lemma, C contains a maximal element B.

6. **Maximal Linearly Independent Set:** Let B be a maximal element in C. We claim that B is a basis for V.

   - B is linearly independent by construction.
   - Suppose B is not a basis for V. Then there exists some vector $v \in V \setminus \text{span}(B)$. The set $B \cup \{v\}$ would then be linearly independent (otherwise v would be in the span of B), contradicting the maximality of B.

7. **Conclusion:** Therefore, B must span V, making B a basis for V.

Proof: Co-Finite Topology is a Topology

Definition: The co-finite topology on a set X is defined as follows: a subset $U \subseteq X$ is open if and only if $U = \emptyset$ or $X \setminus U$ is finite.

Proof: We need to show that the co-finite topology on X satisfies the three properties of a topology:

1. X and $\emptyset$ are in the topology.
2. The topology is closed under arbitrary unions.
3. The topology is closed under finite intersections.

1. X and $\emptyset$ are in the topology

- X is open because $X \setminus X = \emptyset$, which is finite.
- $\emptyset$ is open by definition.

2. Closed under Arbitrary Unions

Let $\{U_i\}_{i \in I}$ be an arbitrary collection of open sets in the co-finite topology. We need to show that $U = \bigcup_{i \in I} U_i$ is open.

- If any $U_i = X$, then $U = X$, which is open.
- If all $U_i \neq X$, then $X \setminus U_i$ is finite for each i.

Consider $U = \bigcup_{i \in I} U_i$. Then:

$$X \setminus U = X \setminus \left(\bigcup_{i \in I} U_i \right) = \bigcap_{i \in I} (X \setminus U_i).$$

Since each $X \setminus U_i$ is finite, the intersection of any collection of finite sets is finite (or empty). Therefore, $X \setminus U$ is finite, which implies U is open in the co-finite topology.

3. Closed under Finite Intersections

Let $U_1, U_2, \ldots, U_n$ be a finite collection of open sets in the co-finite topology. We need to show that $U = \bigcap_{i=1}^{n} U_i$ is open.

- If any $U_i = X$, then $U = \bigcap_{i=1}^{n} U_i = \bigcap_{j \neq i} U_j$, reducing the problem to fewer sets.
- If all $U_i \neq X$, then each $X \setminus U_i$ is finite.

Consider $U = \bigcap_{i=1}^{n} U_i$. Then:

$$X \setminus U = X \setminus \left(\bigcap_{i=1}^{n} U_i \right) = \bigcup_{i=1}^{n} (X \setminus U_i).$$

Since each $X \setminus U_i$ is finite, the union of a finite number of finite sets is finite. Therefore, $X \setminus U$ is finite, which implies U is open in the co-finite topology.

Conclusion: Since the co-finite topology on X satisfies the three properties required for a topology, it is indeed a topology.

Proof: Zero Sets of Polynomials Form a Co-Finite Topology

Definition: The zero set of a polynomial $p \in \mathbb{C}[x]$ is $Z(p) = \{z \in \mathbb{C} \mid p(z) = 0\}$.

Proof: We need to show that the collection of zero sets of polynomials in $\mathbb{C}$ forms the closed sets of the co-finite topology on $\mathbb{C}$.

1. Zero Sets are Closed in the Co-Finite Topology

Let $p(x) \in \mathbb{C}[x]$ be a non-constant polynomial of degree n. By the Fundamental Theorem of Algebra, $p(x)$ has at most n roots in $\mathbb{C}$. Therefore, $Z(p)$ is finite.

The zero set of the constant polynomial $p(x) = 0$ is $\mathbb{C}$, which is the entire set.

2. Co-Finite Topology Closed Sets

The closed sets in the co-finite topology are those whose complements are finite. That is, a set $C \subseteq \mathbb{C}$ is closed if $\mathbb{C} \setminus C$ is finite or $C = \mathbb{C}$.

3. Correspondence of Zero Sets and Closed Sets

- The zero set of a non-constant polynomial is finite, corresponding to finite closed sets in the co-finite topology.
- The zero set of the constant polynomial $p(x) = 0$ is $\mathbb{C}$, corresponding to $\mathbb{C}$ itself being a closed set in the co-finite topology.

4. Characterization of Closed Sets

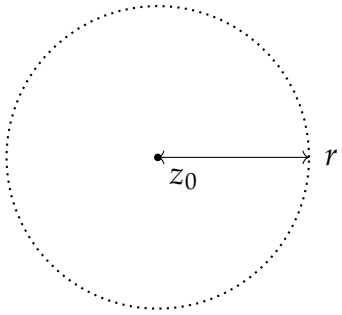
To show that the closed sets in the co-finite topology are precisely the zero sets of polynomials, consider:

- A finite set $\{z_1, z_2, \ldots, z_n\}$. This can be written as the zero set of the polynomial

$$p(x) = (x - z_1)(x - z_2) \cdots (x - z_n).$$

- The whole set $\mathbb{C}$ is the zero set of the polynomial $p(x) = 0$.

Conclusion: The closed sets in the co-finite topology on $\mathbb{C}$ are exactly the zero sets of polynomials in $\mathbb{C}[x]$. Therefore, the collection of zero sets of polynomials forms the closed sets of the co-finite topology, showing that the zero sets of polynomials generate the co-finite topology on $\mathbb{C}$.



Open Ball $B(z_0, r)$

Hence, every vector space V over a field F has a basis, as guaranteed by Zorn's Lemma.

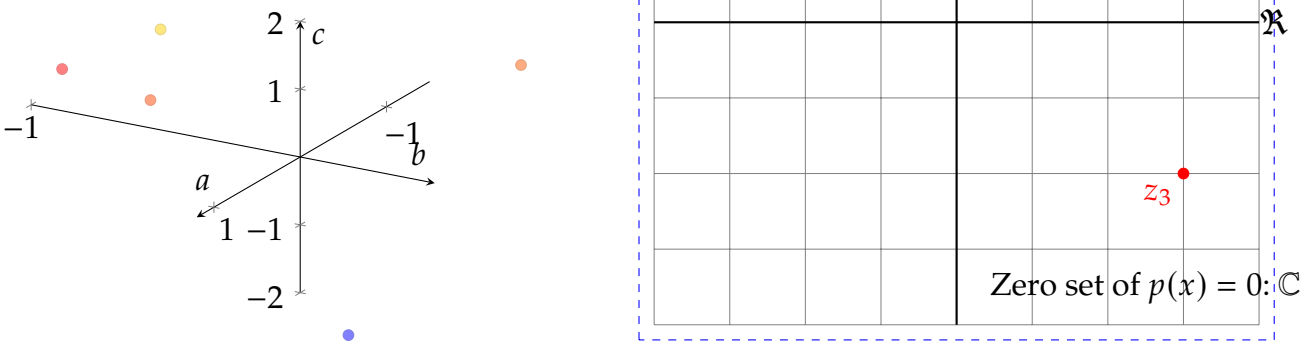
$$\mathbb{C}[x]/\langle x-\alpha\rangle = \mathbb{C}[x]/(x-\alpha)\mathbb{C}[x] \simeq \mathbb{C}.$$

Let $f, g \in I = \mathbb{C}[x]/(x-\alpha)\mathbb{C}[x]$. Then

$$f(x) = (x-\alpha)q_1(x) + r(x), q(x) = (x-\alpha)q_2(x) + r(x)$$

Then

$$f(x) \equiv g(x) \pmod{(x-\alpha)\mathbb{C}[x]} \iff f(x) - g(x) \in (x-\alpha)\mathbb{C}[x]$$



Commutative Ring: $\mathbb{Q}[x]$

↓

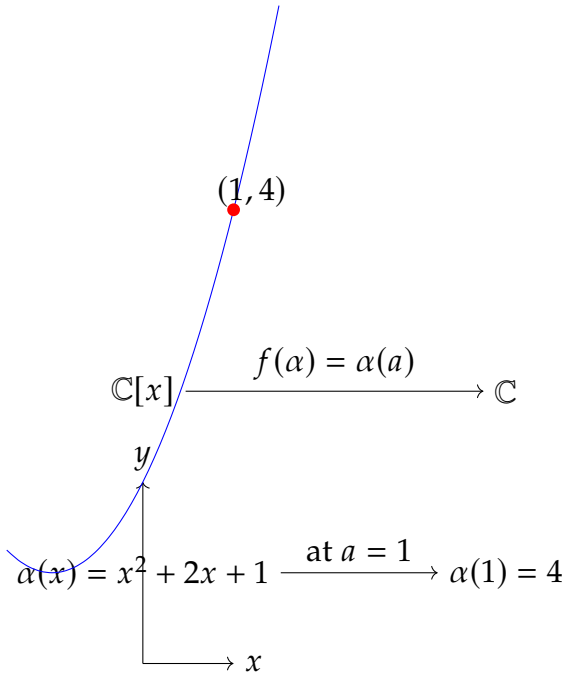
Prime Ideal: $(x^2 - 2)$

↓

Localization: $\mathbb{Q}[x]_{(x^2-2)}$

↓

Field of Fractions: $\mathbb{Q}(x)$ → Extension Field: $\mathbb{Q}(\sqrt{2})$ → Meromorphic Function: $f(z) = \frac{1}{z}$
where $\sqrt{2}$ satisfies $x^2 - 2 = 0$ on $\mathbb{C} \setminus \{0\}$



$$\mathbb{C}[x] \xrightarrow{f(\alpha) = \text{leading coefficient}} \mathbb{C}$$

$$\alpha(x) = 3x^2 + 2x + 1 \xrightarrow{\text{leading coefficient}} 3$$

$3x^2$

$$\mathbb{C}[x] \xrightarrow{f(\alpha) = \text{constant term}} \mathbb{C}$$

$$\alpha(x) = x^2 + 2x + 1 \xrightarrow{\text{constant term}} 1$$

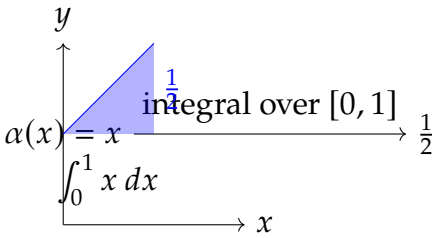
constant term

$$\mathbb{C}[x] \xrightarrow{f(\alpha) = \sum a_i} \mathbb{C}$$

$$\alpha(x) = x^2 + 2x + 1 \xrightarrow{\text{sum of coefficients}} 4$$

$1 + 2 + 1 = 4$

$$\mathbb{C}[x] \xrightarrow{f(\alpha) = \int_a^b \alpha(x)\,dx} \mathbb{C}$$



$\mathbb{C}[x]$

$\alpha(x) = x^2 + 2x + 1 \qquad \beta(x) = 3x^3 + x + 5$

$\gamma(x) = 2x^2 - ix + 1 \qquad \delta(x) = 4$

$\epsilon(x) = ix^4 - 2x + 3$

$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ General Form

$\vdots$

$1 \qquad x \qquad x^2 \qquad x^3 \qquad \cdots$

Basis of $\mathbb{C}[x]$

Vector Space $\mathbb{C}[x]$

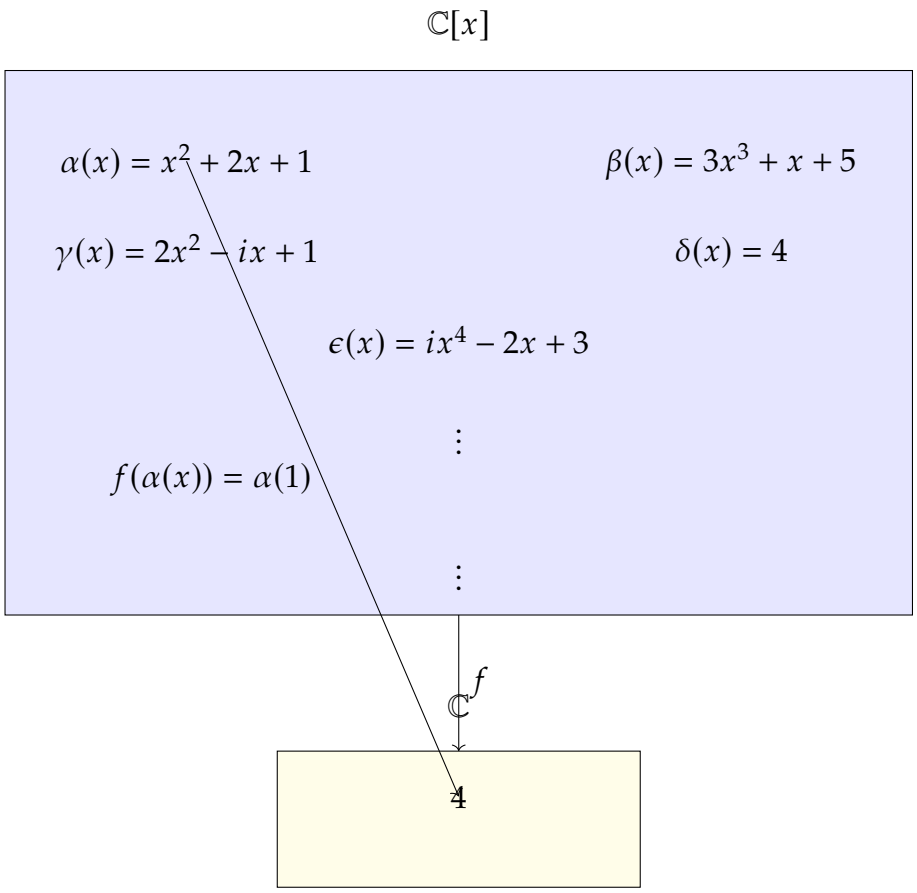
$\mathbb{C}[x]$

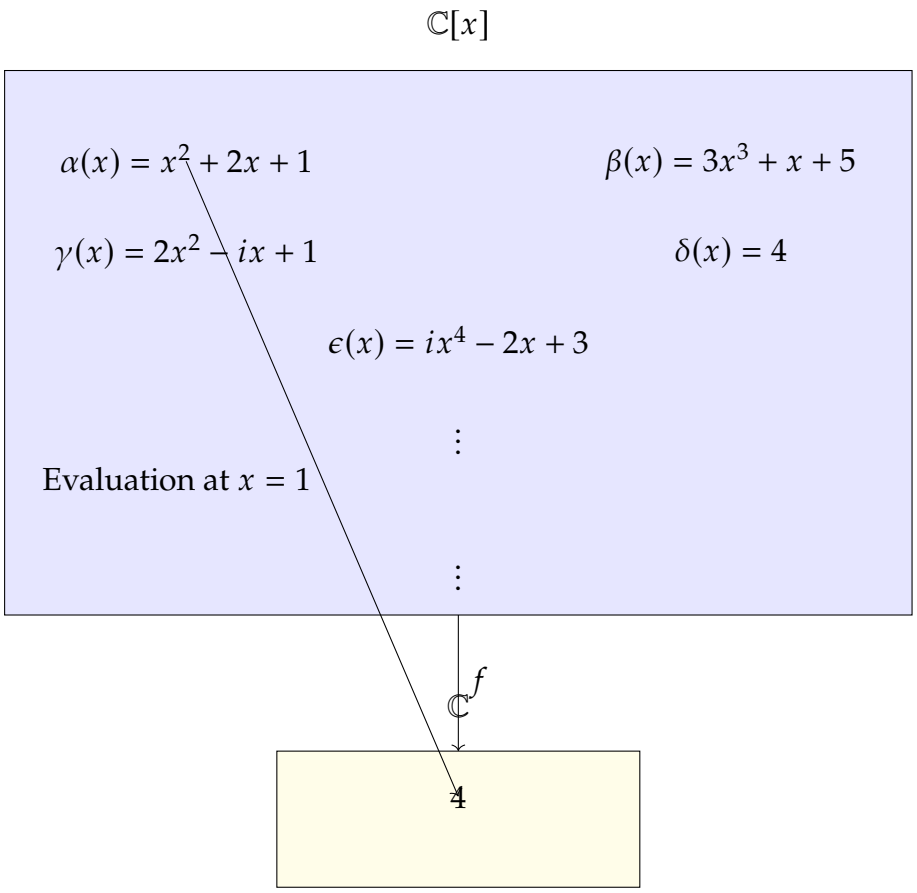
$\alpha(x) = x^2 + 2x + 1 \qquad \beta(x) = 3x^3 + x + 5$

$\gamma(x) = 2x^2 - ix + 1 \qquad \delta(x) = 4$

$\epsilon(x) = ix^4 - 2x + 3$

$\vdots \qquad \vdots \qquad \vdots$

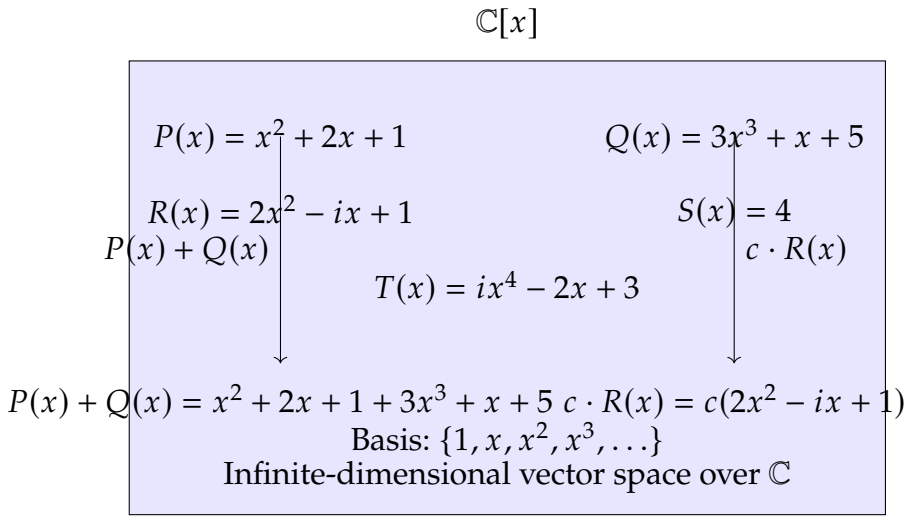

$\mathbb{C}[x]$
$\alpha(x) = x^2 + 2x + 1$
$\beta(x) = 3x^3 + x + 5$
$\gamma(x) = 2x^2 - ix + 1$
$\delta(x) = 4$
$\epsilon(x) = ix^4 - 2x + 3$
$f(\alpha(x)) = \alpha(1)$
f
$\mathbb{C}$
4



Leading Coefficient: 3

Constant Term: 1

Sum of Coefficients: 4



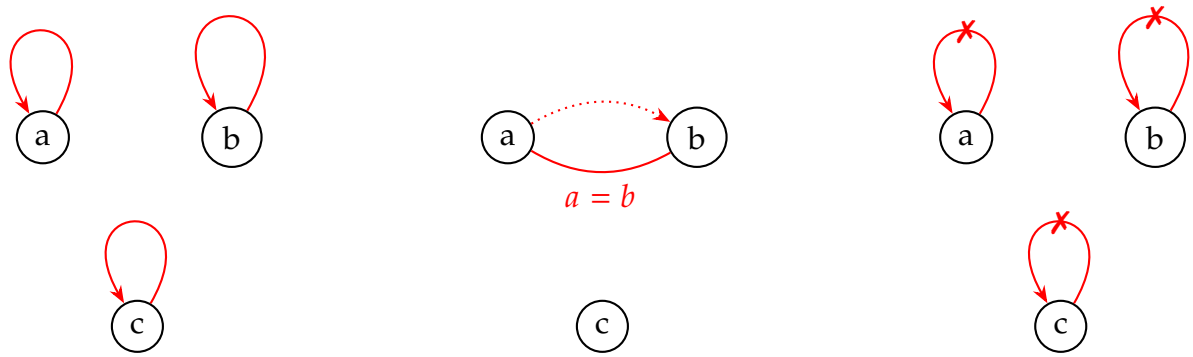
2.2 Zorn's Lemma and Basis

2.2.1 Relations

Let $\mathcal{R} \subseteq A \times A$ be a relation on a set A.

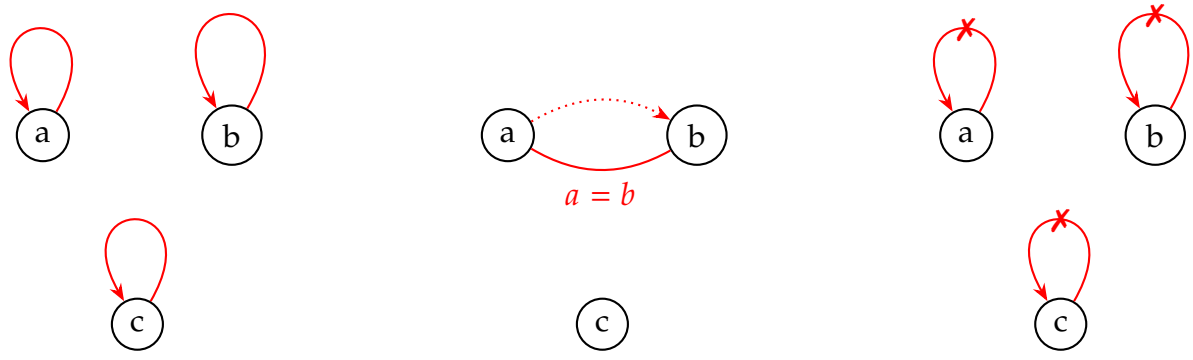
Property Type	Condition	Definition	Example
Reflexive Properties	Reflexive	$\forall a \in A,\ (a,a) \in R$	Equality relation on $\mathbb{R}$
	Coreflexive	$\forall a,b \in A,\ (a,b) \in R \Rightarrow a = b$	Identity relation $\{(a,a) : a \in A\}$
	Irreflexive (Anti-reflexive)	$\forall a \in A,\ (a,a) \notin R$	"Is less than" relation on $\mathbb{R}$
	Non-Reflexive	$\exists a \in A,\ (a,a) \notin R$	"Is a friend of" relation
Symmetric Properties	Symmetric	$\forall a,b \in A,\ (a,b) \in R \Rightarrow (b,a) \in R$	Equality relation on $\mathbb{R}$
	Asymmetric	$\forall a,b \in A,\ (a,b) \in R \Rightarrow (b,a) \notin R$	"Is parent of" relation
	Anti-Symmetric	$\forall a,b \in A,\ (a,b) \in R$ and $(b,a) \in R \Rightarrow a = b$	"Is less than or equal to" relation on $\mathbb{R}$
	Non-Symmetric	$\exists a,b \in A,\ (a,b) \in R$ and $(b,a) \notin R$ or $(a,b) \notin R$ and $(b,a) \in R$	"Is sibling of" relation
Transitive Properties	Transitive	$\forall a,b,c \in A,\ (a,b) \in R$ and $(b,c) \in R \Rightarrow (a,c) \in R$	Divisibility relation on $\mathbb{N}$
	Anti-Transitive	$\forall a,b,c \in A,\ (a,b) \in R$ and $(b,c) \in R \Rightarrow (a,c) \notin R$	Hard to find simple example
	Non-Transitive	$\exists a,b,c \in A,\ (a,b) \in R$ and $(b,c) \in R$ and $(a,c) \notin R$	"Is a friend of"

Table 2.1: Conditions and Examples for Relation Properties



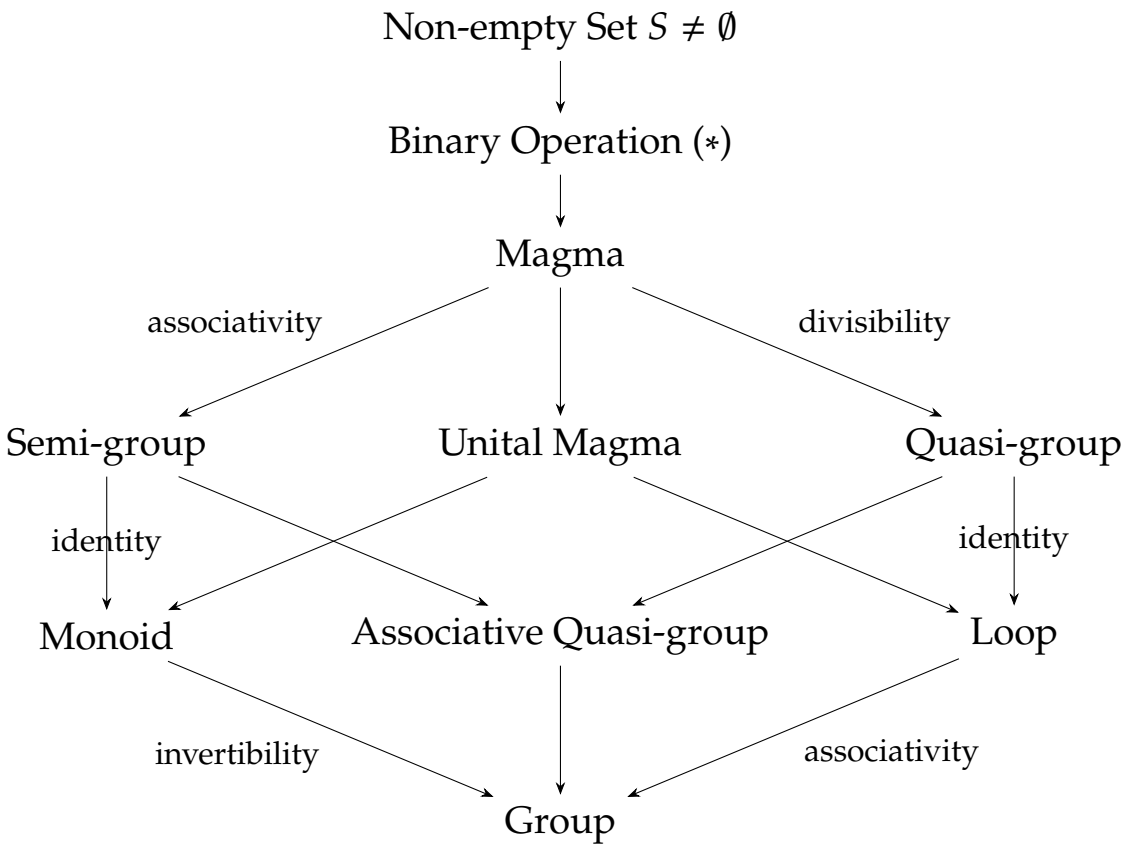
(a) Reflexive (b) Co-reflexive. (c) Irreflexive

Figure 2.1: Reflexivity



(a) Reflexive (b) Co-reflexive. (c) Irreflexive

Figure 2.2: Reflexivity


Non-empty Set $S \neq \emptyset$
Binary Operation $(*)$
Magma
associativity
divisibility
Semi-group
Unital Magma
Quasi-group
identity
identity
Monoid
Associative Quasi-group
Loop
invertibility
associativity
Group

Chapter 3

Localization

Observation. Consider the ring of integers $(\mathbb{Z}, +, \times)$. For $n \neq 1$, consider the set of integer multiplies $n\mathbb{Z}$. Then $1 \notin n\mathbb{Z}$, but $(n\mathbb{Z}, \times)$ is closed under $\times$. That is, $n\mathbb{Z}$ is closed under $\times$ but not actually multiplicatively closed.

Multiplicatively Closed Subset of Ring

Definition 3.1. Let $(R, +, \times)$ be a ring with unity 1_S and zero 0_S. Then $S \subseteq R$ is **multiplicatively closed** iff

- $1_R \in S$.
- $x, y \in S \implies x * y \in S$.

Note (From $\mathbb{Z}$ to $\mathbb{Q}$)**.**

- (Numerator) $R = \mathbb{Z}$ is a ring
- (Denominators) $S = \mathbb{Z} \setminus \{0\}$ is multiplicatively closed and $1 \in S$
- ($\mathbb{Q} \simeq S^{-1}R$) Every $q \in \mathbb{Q}$ is of the form $s^{-1}r$ for $r \in R$ and $s \in S$.
- (Equivalence Relation)

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc \iff t(ab - bc) = 0 \text{ for } t \in S.$$

- $\mathbb{Q}$ is ring:
  - Q has an addition $a/b + c/d = (da + bc)/bd$
  - Q has a multiplication $a/b \cdot c/d = ac/bd$
  - Q has a zero $0/1$ and a one $1/1$.
- $\mathbb{Z}$ is a subring of $\mathbb{Q}$ by $r \mapsto r/1$.

Note (Functions close to 0 - "local functions")**.**

- (Numerator) $R = \mathbb{R}[x] \in \mathbb{R}^{\mathbb{R}}$ is a ring
- (Denominators) $S = \{s \in R : s(0) \neq 0\}$ is multiplicatively closed and $1 \in S$
- ($L \simeq S^{-1}R$) Every local function L is of the form $s^{-1}r$ for $r \in R$ and $s \in S$.

- (Equivalence Relation)
$$\frac{a}{b} = \frac{c}{d} \iff ad = bc \iff t(ab - bc) = 0 \text{ for } t \in S.$$
- Local function is ring:
  - L has an addition $a/b + c/d = (da + bc)/bd$
  - L has a multiplication $a/b \cdot c/d = ac/bd$
  - L has a zero $0/1$ and a one $1/1$.
- R has a map to L by $r \mapsto r/1$.

3.1 For completeness: The formal definition/statement

Let R be a commutative ring and S be a multiplicatively closed set with $1 \in S$.

(a) Equivalence Relation on $R \times S$
$$(a, b) \sim (c, d) \iff \exists t \in S : t(ad - bc) = 0.$$

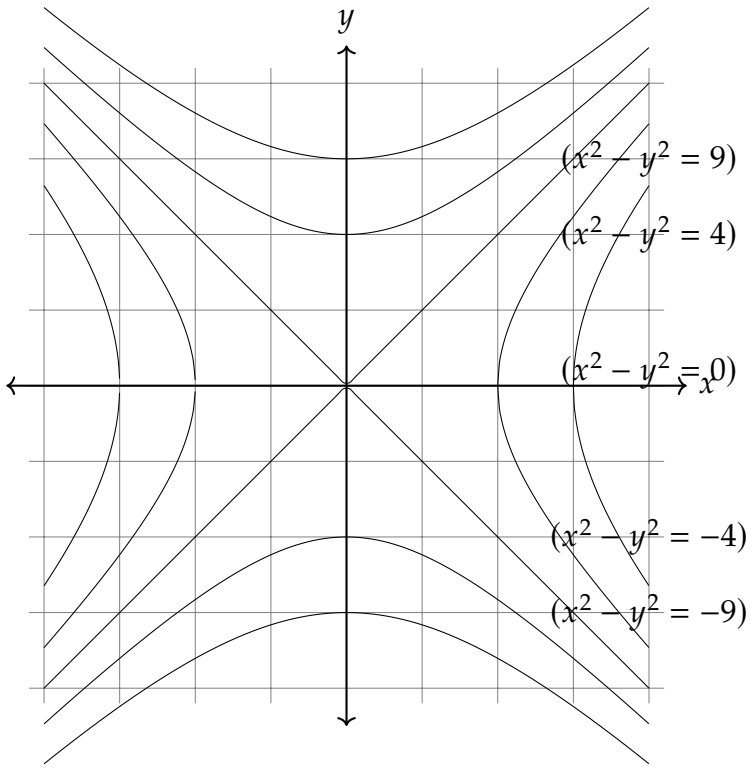
(b) [Localization (localize at S)] The set of equivalence classes $S^{-1}R$.

(c) Addition on $S^{-1}R$
$$(a, b) + (c, d) = (ad + bc, bd)$$

(d) Multiplication on $S^{-1}R$
$$(a, b) \cdot (c, d) = (ab, cd)$$

(e) (Slogan. Invert elements of S)

- $S^{-1}R$ is a ring with zero $(0, 1)$ and one $(1, 1)$
- There is a ring homomorphism $\phi : R \to S^{-1}R$ given by $r \mapsto (r, 1)$, i.$e.$, $r \mapsto r/1$
- ϕ is injective (R is a subring of $S^{-1}R$) iff S contains no zero divisor



- $X \subset\neq \mathbb{R}^2$ is the vanishing set of $(x-y)(x+y)$
- Model: the ring $R = \mathbb{R}[x,y]/\langle (x-y)(x+y)\rangle$
- $\langle x-y\rangle : X \to \mathbb{R}$ is locally at a indistinguishable from 0
- $\langle x-y\rangle - 0 \neq 0$ but $(x+y)\langle x-y-0\rangle = 0$ in R
- So $\langle x-y\rangle = 0$ in R localized at $S = \left\{s \in R : s(a) = 0\right\}$.