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

July 13, 2024

Contents

Chapter 1

Visual Group Theory

Mathematical Definitions and Examples

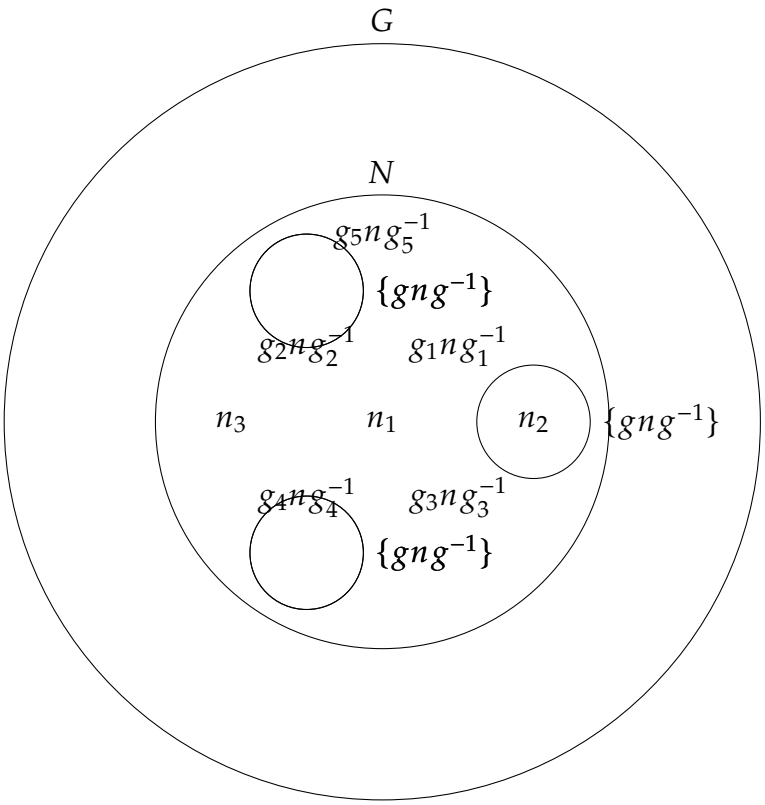
1. Normal Subgroup

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:

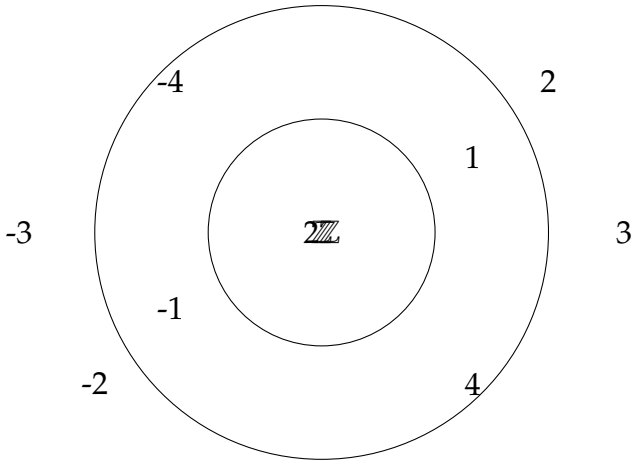
$$N \triangleleft G \iff \forall g \in G, \forall n \in N,\ gng^{-1} \in N.$$



Examples:

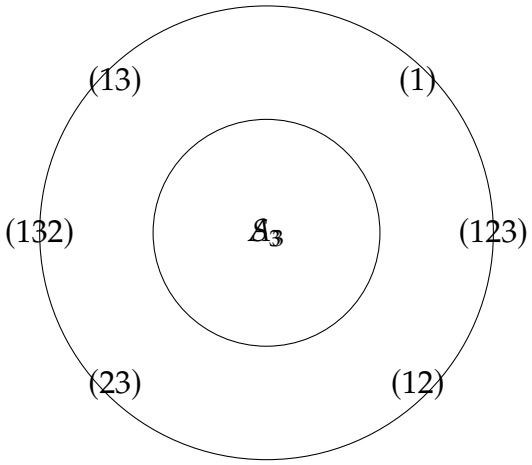
1. In the group of integers $(\mathbb{Z}, +)$, the subgroup $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ is a normal subgroup since $\mathbb{Z}$ is abelian.

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



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:

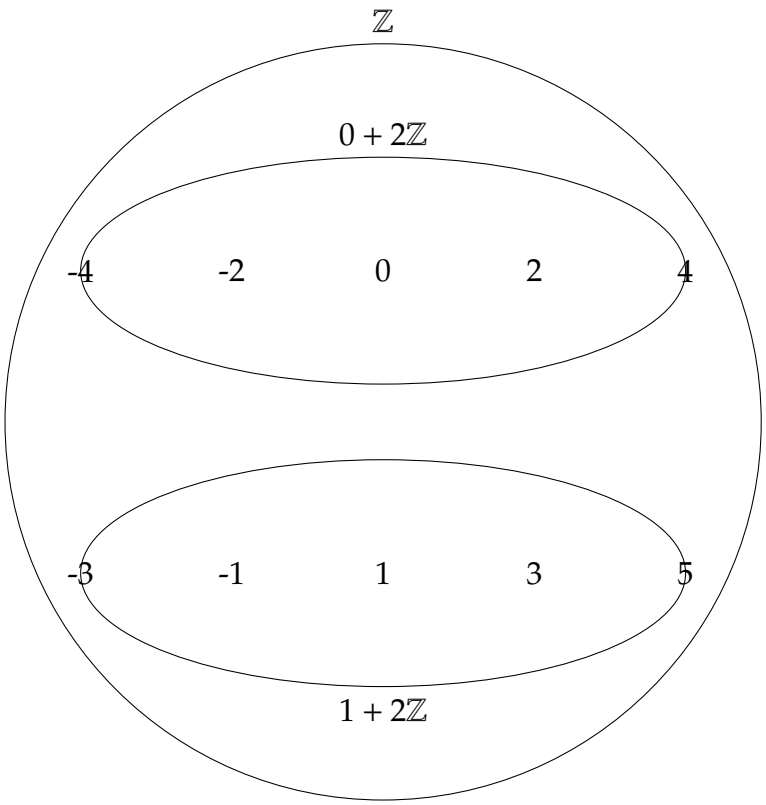
Given a group G and a normal subgroup N of G, the *quotient group* (or *factor group*) G/N is the set of left cosets of N in G with the group operation defined by:

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

Examples:

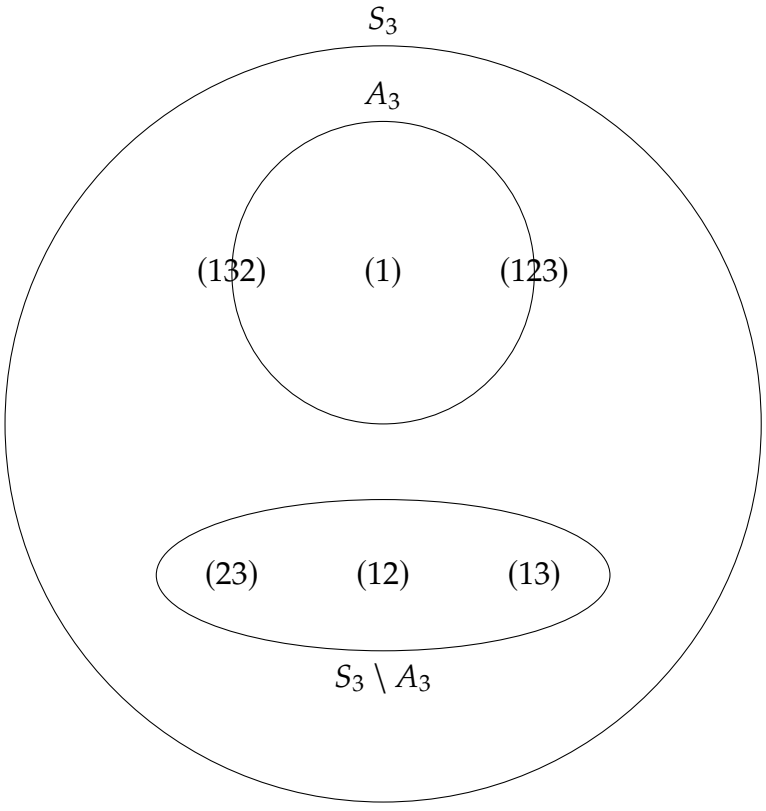
1. For $(\mathbb{Z}, +)$ and $N = 2\mathbb{Z}$, the quotient group $\mathbb{Z}/2\mathbb{Z}$ consists of two cosets: $0 + 2\mathbb{Z}$ and $1 + 2\mathbb{Z}$.

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



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:

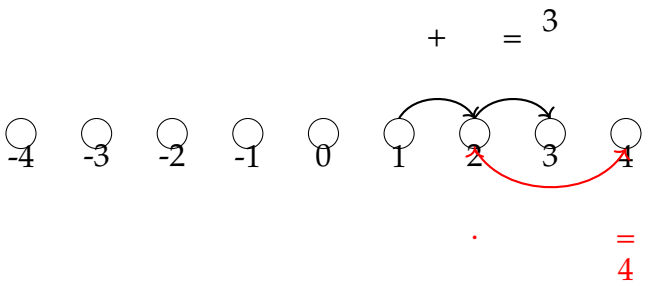
1. $(R, +)$ is an abelian group.

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

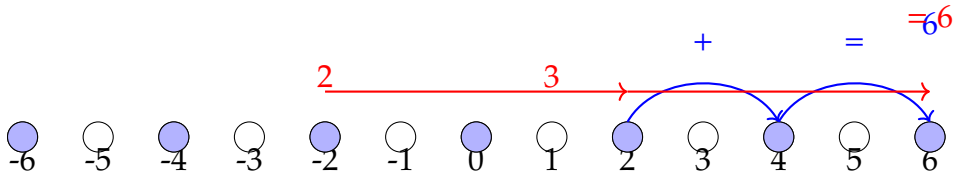
Definition:
An *ideal* I of a ring R is a subset of R such that:

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.

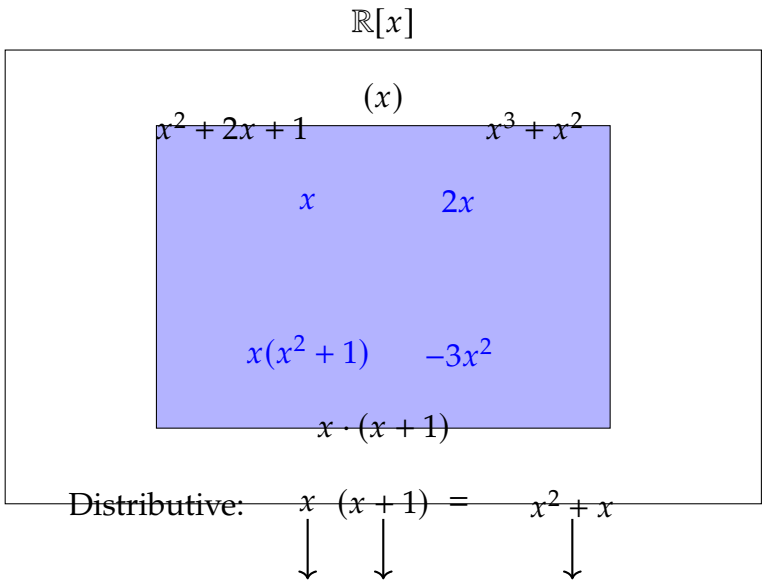
Examples:
1. In $\mathbb{Z}$, the set $2\mathbb{Z}$ (all even integers) is an ideal.

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



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 $b \in P$.

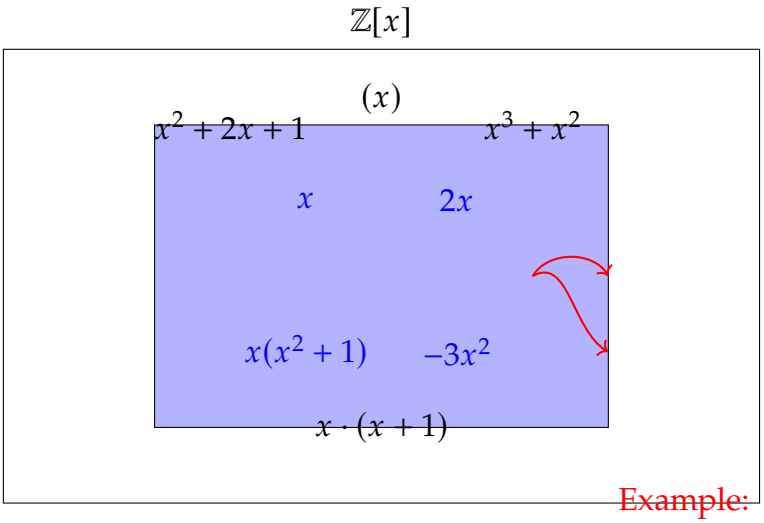
Examples:

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

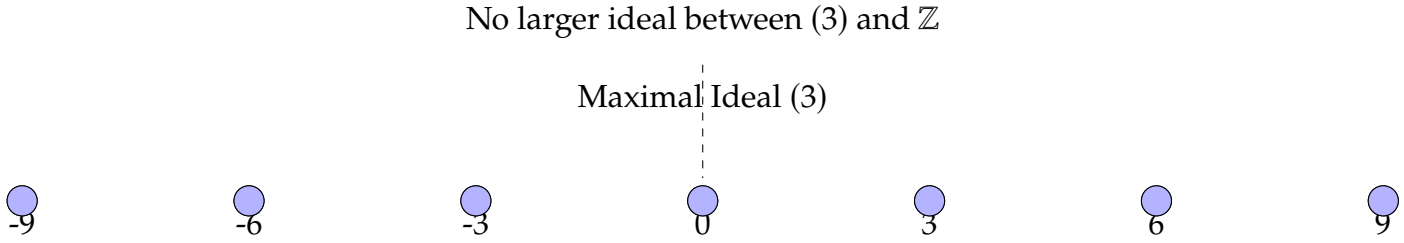
Definition:

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:

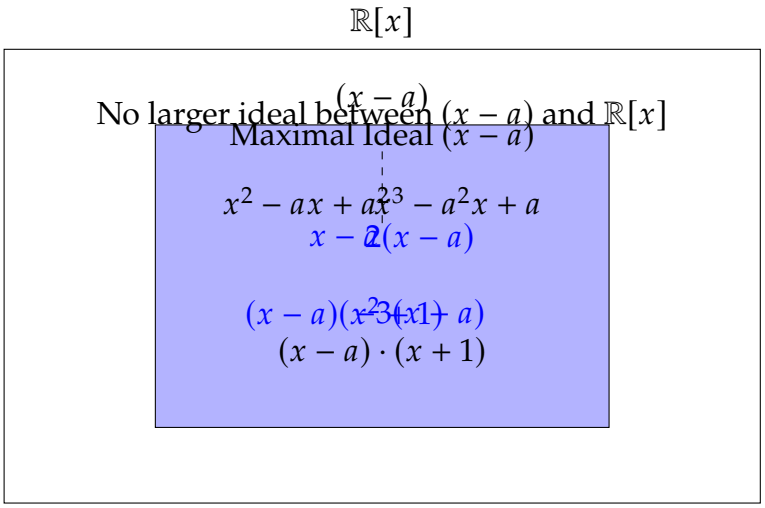
1. In $\mathbb{Z}$, the ideal (p) where p is a prime number (e.g., (3)) is a maximal ideal.

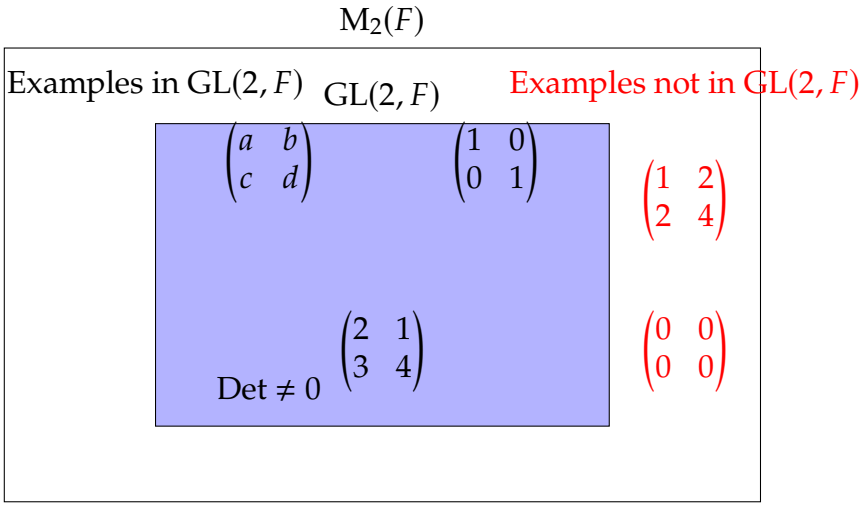
$$(3) = \{3k \mid k \in \mathbb{Z}\} \text{ is a maximal ideal of } \mathbb{Z}$$

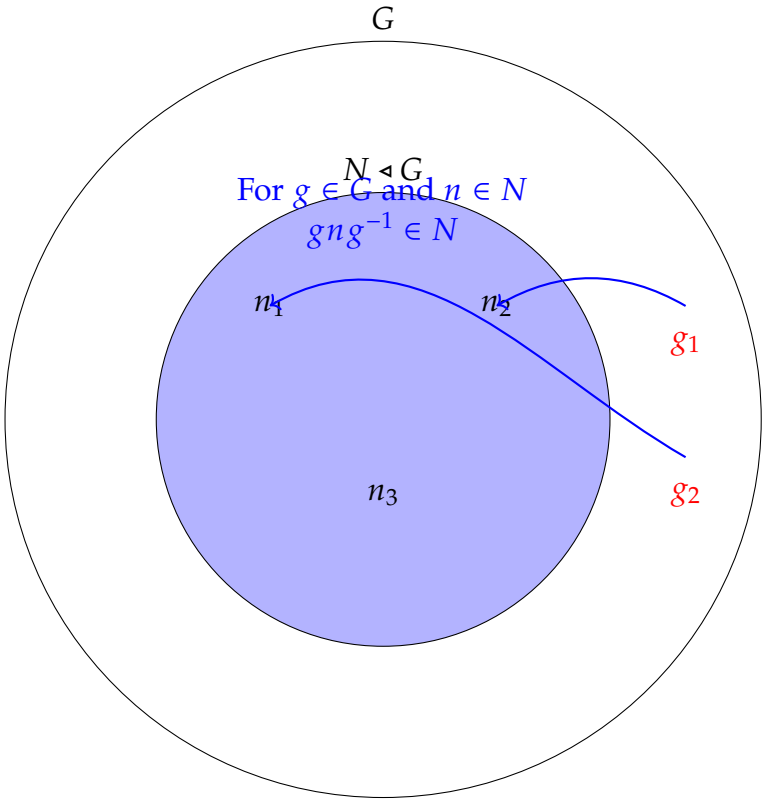


2. In $\mathbb{R}[x]$, the ideal $(x - a)$ where $a \in \mathbb{R}$ is a maximal ideal.

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


$\mathbb{R}[x]$
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