PMATH 347 — Spring 2025: Class Notes

Jiucheng Zang

May 5th 2025

Contents

I. Introduction to Groups **3**

- i. Basic Axioms . . . 3
- ii. Group . . . 10
- iii. Notation . . . 10
- iv. Dihedral Group . . . 13
- v. Subgroups . . . 17
- vi. Circular Groups . . . 22
- vii. Homomorphism . . . 27
- viii. Isomorphism . . . 33
- ix. Cosets and Lagrange's Theorem . . . 37
- x. Quotient Groups . . . 50
- xi. Isomorphism Theorem . . . 54
- xii. Group Actions . . . 66
- xiii. Classification of groups . . . 80

xiv. Sylow's Theorems 81

II. Ring Theory **87**

i. Rings 87

1. Basic properties of rings 89

2. Polynomial rings 90

ii. Ideals 99

iii. Quotient Rings 104

iv. Isomorphism Theorems for Rings 107

v. Commutative Rings 114

vi. Integral Domains 118

vii. Chinese Remainder Theorem (In video) 125

viii. Principal Ideal Domain (PID) 125

III. Final Notes **131**

Notes:

- William Slofodran
- HW1 Dur May 14th

Abstracted Algebra specifically, group + ring

Pre-university algebra:

$$ax = b \to x = \frac{b}{a}$$

We have a lot of different types of numbers:

Number Set	Expressions
$\mathbb{N}$	$+, \cdot$
$\mathbb{Z}$	$+, \cdot, -$
$\mathbb{Q}$	$+, \cdot, -, /$
$\mathbb{R}$	$\ldots, \sqrt{x}$
$\mathbb{C}$	$\ldots, i$
Vector Space	$+, \cdot$
Matrix Space	$+, \cdot$, Matrix Multiplication
Polynomial Space	$+, \cdot$, Polynomial Multiplication
$\mathbb{Z}/n\mathbb{Z}$	$+, \cdot, -$

In abstract algebra, we're interested in what notion of "numbers" exist.

The different "types" of numbers are really distinguished by the operations defined on them. In this course, we are going to study operations on sets.

I. Introduction to Groups

i. Basic Axioms

Definition

A binary operation on a set x is a function $b : X \times X \to X$. Notation, We often write binary operations inline: $a + b, a \cdot b, ab$.

Symbols we can use:

$$\cdot, *, \star, \circ, \bullet, +, -, \oplus, \otimes, \diamond, \times, \boxplus, \boxdot, \vee, \wedge$$

Example

binary operation on $+, -$ on $\mathbb{N}$ are binary operations. $-$ is not a binary operation on $\mathbb{N}$.

Definition

A k-ary operation on a set x is a function $f : \underbrace{X \times \cdots \times X}_{\text{k times}} \to X$.

A unary operation is a k-ary operation with $k = 1$.

Example

- Conj on $\mathbb{C}$,
- Negation on $x \longmapsto -x$ on $\mathbb{Z}$.
- $x \longmapsto \frac{1}{x}$ on $\mathbb{Q}$ not an operation (1/0 is not defined).

This is an operation on:

$$\mathbb{Q}^x = \{x \in \mathbb{Q}, x \neq 0\}$$

Definition

A binary operation $\boxtimes$ on a set X is associative if $x \boxtimes (y \boxtimes z) = (x \boxtimes y) \boxtimes z$ for all $x, y, z \in X$.

Example

For all $x, y, z \in X$:

- $+$ on $\mathbb{N}, \mathbb{Z}$ are associative because $(a + b) + c = a + (b + c)$ for all a, b, c.
- $-$ on $\mathbb{Z}$ is not associative:

$$(3 - 4) - 5 = -1 - 5 = -6 \neq 3 - (4 - 5) = 3 - (-1) = 4.$$

- $\div$ on $\mathbb{Q}$ is not associative:

$$(8 \div 4) \div 2 = 2 \div 2 = 1 \neq 8 \div (4 \div 2) = 8 \div 2 = 4.$$

Function composition is associative

Definition

Informed defined: Let $\boxtimes$ be a binary operation on a set X. A bracketing of a sequence $a_1, a_2, \ldots, a_n$ is a way of inserting brackets into $a_1 \boxtimes a_2 \boxtimes \cdots \boxtimes a_n$ so that the expression can be evaluated.

Example

n = 4, Bracketing of a_1, a_2, a_3, a_4:

- $(((a_1 \boxtimes a_2) \boxtimes a_3) \boxtimes a_4)$
- $((a_1 \boxtimes (a_2 \boxtimes a_3)) \boxtimes a_4)$
- $(a_1 \boxtimes ((a_2 \boxtimes a_3) \boxtimes a_4))$
- $(a_1 \boxtimes (a_2 \boxtimes (a_3 \boxtimes a_4)))$
- $((a_1 \boxtimes a_2) \boxtimes (a_3 \boxtimes a_4))$

Definition

Formally, a bracketing of $a_1, a_2, \ldots, a_n$ is

- $n = 1$ the word a_1.
- $n > 1$ $(w_1 \boxtimes w_2)$ where w_1 is a bracketing of $a_1, a_2, \ldots, a_k$ and w_2 is a bracketing of $a_{k+1}, \ldots, a_n$ for some k with $1 \leq k < n$.

Proposition

A binary operation $\boxtimes$ on a set X is associative iff for every sequence $a_1, a_2, \dots, a_n, n \geq 1$, every bracketing of $a_1, a_2, \dots, a_n$ evaluated to same element of X.

Proof

$\Leftarrow$: Take $n = 3$, Then $(a \boxtimes b) \boxtimes c = a \boxtimes (b \boxtimes c)$ for all $a, b, c \in X$.
$\Rightarrow$: Proof by induction on n.
When $n = 1$, there is only one bracketing, of every sequence, so every sequence evaluates to the same element.
Assume prop is true for $n < k$, where $k > 1$, and let $a_1, a_2, \dots, a_k \in X$ if w is a bracketing of $a_1, a_2, \dots, a_k$., then $w := (w_1 \boxtimes w_2)$ where w_1 is a bracketing of $a_1, a_2, \dots, a_l, l < k \neq w_2$ is a bracketing of $a_{l+1}, \dots, a_k$.
By induction hypothesis, $w_1 = (\dots(a_1 \boxtimes a_2) \boxtimes \dots) \boxtimes a_l$ and $w_2 = (a_{l+1} \boxtimes (a_{l+2} \boxtimes (\dots (a_k - 1 \boxtimes a_k) \dots)$ in X.
Then

$$\begin{aligned} w &= w_1 \boxtimes w_2 \\ &= (A \boxtimes a_l) \boxtimes (B) \\ &= (A \boxtimes (a_l \boxtimes B)) \\ &\text{(by associativity)} \\ &= a_1 \boxtimes (a_2 \boxtimes \dots (a_l \boxtimes B) \dots) \end{aligned}$$

Hence, any bracketing of $a_1, a_2, \dots, a_k$ evaluates to $a_1 \boxtimes (a_2 \boxtimes \dots (a_{k-1} \boxtimes a_k) \dots)$.
By induction, the prop is hold.

$\square$

Note

Consequences: If $\boxtimes$ is associative, can write $a_1 \boxtimes a_2 \boxtimes \cdots \boxtimes a_n$ without brackets.

Definition

A binary operation $\boxtimes$ on a set X is commutative or abelian if $a \boxtimes b = b \boxtimes a$, for all $a, b \in X$.

Example

$+, \times$ on $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ are commutative.

Example

$+$ on matrices $\underbrace{M_n(\mathbb{R})}_{\text{nxn matrices of coefficient in } \mathbb{R}}$ is abelian, $\cdot$ is not.

Focus on associative but not abelian operations.

(i) **Group Theory**: a single associative operation with some additional properties.

(ii) **Ring theory**: two associative operations that become like $+$, $\cdot$.

Definition

An identity for a binary operations $\boxtimes$ on a set X is an element $e \in X$ such that $e \boxtimes x = x \boxtimes e = x$ for all $x \in X$.

Example

0 is an identity for $+$ on $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ . . . .
1 is an identity for $\cdot$ on $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ . . . .
I_n is an identity for $\cdot$ on $M_n(\mathbb{R})$.

Lemma

If e is an identity for $\boxtimes$ on X, then e is unique.

Proof

$$\begin{aligned} e &= e \boxtimes e' \\ &= e' \end{aligned}$$

□

Definition

Let $\boxtimes$ be a binary opetration on a set X with an identity. Let $x \in X$,
An element $y \in X$ is a left inverse of x if $y \boxtimes x = e$.
A right inverse of x if $x \boxtimes y = e$.
An inverse of x if y is both a left and right inverse of x.

Note

The element x is invertible if it has an inverse.

Lemma

Suppose $\boxtimes$ is associative. If y_L and y_R are left and right inverse of $x \in X$ respectively, then $y_L = y_R$.

Proof

$y_L = y_L \boxtimes e = y_L \boxtimes x \boxtimes y_R = e \boxtimes y_R = y_R$. (Also associativity)

$\square$

Consequence x is invertible $\iff$ x has a left and right inverse.

Note

It is possible to be left invertible but not right invertible, or vice versa. (homework)

Example

- $\mathbb{N} = \{1, 2, \dots\}$, $+$ not invertible elements.
- $\mathbb{Z}, +$ every element is invertible.
- $\mathbb{Z}, \cdot$ only 1 and -1 are invertible elements.
- $\mathbb{Q}, \cdot$ invertible elements are $\mathbb{Q}^\times$ (nonzero rationals).

Note

If x is invertible and has a unique iverse, we denote it by $x^{-1} \cdot$ (or $- x$).

Lemma Properties of inverses

Let $\boxtimes$ be an associative binary operation on a set X with an identity e. Then

1. If e is invertible, then $e^{-1} = e$.

   Proof

   $e \boxtimes e = e$.

   □

2. If a is invertible, then so is a^{-1}, and $(a^{-1})^{-1} = a$.

   Proof

   $a \boxtimes a^{-1} = e \implies a^{-1} \boxtimes a = e$.

   □

3. If a, b are invertible, then $(a \boxtimes b)^{-1} = b^{-1} \boxtimes a^{-1}$.

   Proof

   $(a \boxtimes b) \boxtimes (b^{-1} \boxtimes a^{-1}) = a \boxtimes e \boxtimes a^{-1} = a \boxtimes a^{-1} = e$.
   Similarly, $(b^{-1} \boxtimes a^{-1}) \boxtimes (a \boxtimes b) = e$.

   □

4. a is invertible $\iff$ the equation $a \boxtimes x = b, y \boxtimes a = b$ both have unique solution for element $b \in X$. (x, y are the variables)

   Proof

   $(\Rightarrow)$
   If a is invertible, then $x = a^{-1} \boxtimes b$ is a solution since $a \boxtimes (a^{-1} \boxtimes b) = e \boxtimes b = b$.
   $y = b \boxtimes a^{-1}$ is a solution to $y \boxtimes a = b$.
   exercise: Show unique properties $\Leftarrow$.
   $(\Leftarrow)$ (Uniqueness)
   Let $b = e$, the equation $a \boxtimes x = e$ must have a unique solution x. We mark it as $a_r, a \boxtimes a_r = e$. Verse-versa we get $a_l \boxtimes a = e$
   We can compute $a_l = a_l \boxtimes (a \boxtimes a_r) = (a_l \boxtimes a) \boxtimes a_r = e \boxtimes a_r = a_r$
   Thus, $a_r = a_l \Rightarrow a \boxtimes a_r = e, a_r \boxtimes a = e$
   Therefore, a is invertible with inverse a^{-1}

   □

Lemma Cancellation property

Let $\boxtimes$ be an associative binary operation on X with identity e.
If a has a left inverse, and $a \boxtimes u = a \boxtimes v$ then $u = v$.
If a has a right inverse, and $u \boxtimes a = v \boxtimes a$ then $u = v$.

Proof

Suppose a has a left inverse and $a \boxtimes u = a \boxtimes v$.
Let b be a left inverse. Then $b \boxtimes a \boxtimes u = b \boxtimes a \boxtimes v \Rightarrow e \boxtimes u = e \boxtimes v \Rightarrow u = v$.
(Right inverse vece-versa)

□

Note

We call $(\star)$ left Cancellation and $(\star\star)$ right Cancellation.

Example

$\mathbb{Z}$ with Every non-zero element has a left and right cancellation

$$ab = ac, a \neq 0 \Rightarrow b = c$$

But only ± 1 an invertible element.

ii. Group

Definition

A group is a pair $(G, \boxtimes)$ where G is a set and $\boxtimes$ is an associative binary operation on G with an identity e, s.t. every element of G is invertible.

iii. Notation

If the operation is clear we will usually just write G instead of $(G, \boxtimes)$.

We often use $\cdot$ as the default symbol for the operation on a group. We also often write gh instead of $g \cdot h$. The identity we be denoted by u or e_G or 1 or 1_G.

We use a^{-1} for the inverse of a, These conventions are called multiplication notation.

Definition

A group $(G, \boxtimes)$ is <u>abelian</u> if $\boxtimes$ is abelian.

For abelian groups, we often use <u>addition notation</u> instead of multiplication notation, default symbol is $+$. The inverse of a is denoted by $-a$, and the identity is denoted by 0, 0_G.

Example

1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ are all abelian groups, commonly denoted by

$$a + (-a) = 0, \quad a \in \mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$$

2) $(\mathbb{Z}, \cdot)$ is not a group because not every element is invertible.

Note

We use addition notion by default for these groups. (e.g. identity is 0)
But we can use multiplication notation if we want:

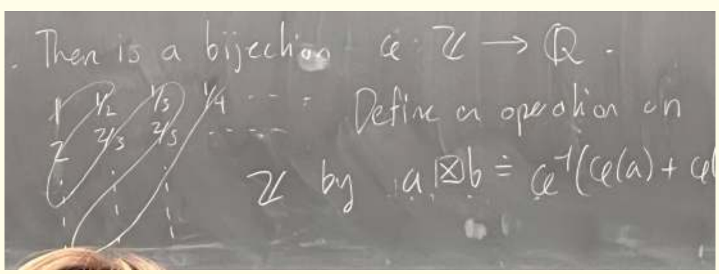
$$a \cdot b := a + b, \quad 3 \cdot 7 = 10$$

$$e = 0, \quad 3 \cdot e = 3$$

3) There is a bijection, $\phi : \mathbb{Z} \mapsto \mathbb{Q}$. Define an operation on $\mathbb{Z}$ by $a \boxtimes b = \phi^{-1}(\phi(a) + \phi(b))$
Then $(\mathbb{Z}, \boxtimes)$ is an abelian group.

Example

$$(1 \boxtimes 2 = 8)$$



Lemma

Let $\boxtimes$ be an associative binary operation with identity e on a set M.
Then $G = \{g \in M : \text{g is invertible with respect to } \boxtimes\}$
is a group with the operation $g \cdot h := g \boxtimes h$.

Note

The smallest possible group is called the trivial group it has one element.
Notation: $\{e\}, e \cdot e = e$.

Example

$$\mathbb{Q}^{\times} = \{a \in \mathbb{Q} : a \neq 0\} \text{ and } \mathbb{R}^{\times} = \{a \in \mathbb{R} : a \neq 0\}$$

a group under multiplication.
Identity: 1, Since these group are abelian groups we can also use addition notation for these groups.

$$a + b := a \cdot b, 3 + 4 = 12$$

Corollary

Let x be a set, and let

$$S_x = \{f \in Fun(x, x) : \text{f is invertible}\}$$

Then S_x is a group under function composition. (Identity $Id_X(x) = x$)

Definition

When $X := \{1, 2, \ldots, n\}$, S_X is called the permutation group of rank n, and is denoted by S_n.

Definition

The **order** of a group G is the number of elements $|G|$ in G (if G is finite), and $+\infty$ (If G is infinite). We denote the order by $|G|$ in both cases
A group is finite if G is finite, or equivalently $|G| \subset +\infty$.

Example

$|S_n| = n!$. (S_n is finite)
We can write elements of S_n in two-line notation.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

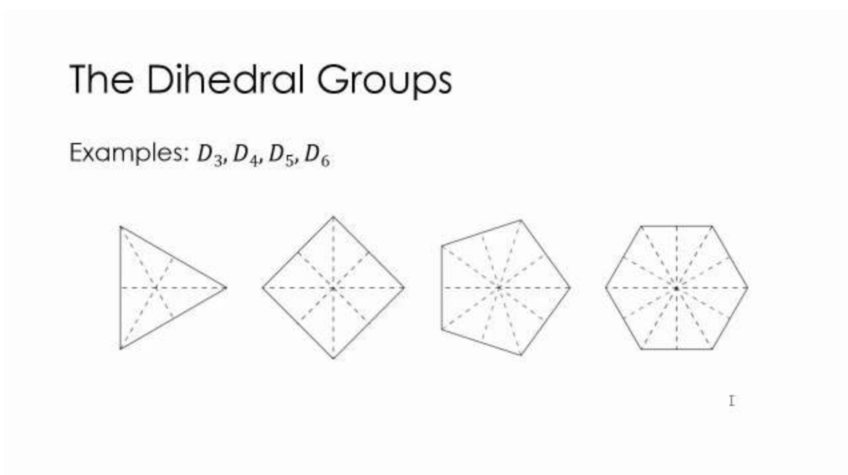
σ is invertible $\Leftrightarrow$ is $1-1$ and onto $\Leftrightarrow$
$\sigma(1), \sigma(2), \ldots, \sigma(n)$ go through $1, \ldots, n$ with the number of operation exactly once.
$\sigma(1) = n, \sigma(2) = n-1, \ldots, \sigma(n) = 1$, $n! = n \cdot (n-1) \cdots 2 \cdot 1$.

iv. Dihedral Group

Example

$M_n\mathbb{R}$ $n \times n$ matrices on $\mathbb{R}$.
Matrix mult is associative.
The identity matrix $\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ is identity.
The set of invertible matrices forms a group called the general linear group (over $\mathbb{R}$) denoted by $GL_n\mathbb{R}$.

Let $P_n, n \geq 3$ denote the regular n-gon in the plane.



H contains points: $v_k = (cos\frac{2\pi k}{n}, sin\frac{2\pi k}{n})$ for $0 \leq k \leq n, v_k = v_0$.

Along with the line segments connecting them.

Definition

A symmetry of the n-gon is an element $T \in GL_2\mathbb{R}$ such that $T(P_n) = P_n$.
The set of symmetries of P_n is called the dihedral group of rank, and denoted by D_{2n} or D_n.

Lemma

D_{2n} is a group under matrix multiplication.

Proof

In later chapter (subgroups)

□

D_{2n} contains

- $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the identity symmetry.
- Rotation s by $\frac{2\pi}{n}$ radians is an element

$$s(v_1) = v_{i+1}, \quad i = 0, \ldots, n-1$$

- Reflection r through the x-axis is an element

$$r(v_k) = v_{n-k}$$

Note

Let G be a group, $g \in G$.

$$g^n = \underbrace{g \cdot g \cdots g}_{\text{n times}}$$

$$g^{-n} = \underbrace{g^{-1} \cdots g^{-1}}_{\text{n times}}$$

$$g^0 = e$$

$$g^{-n} = (g^n)^{-1} = (g^{-1})^n$$

For any $m, n \in \mathbb{Z}$,

$$g^m g^n = g^{m+n}$$

Addition notation: We write g^n as $ng = g + g + \cdots + g$ (n times).

Warning H is not necessarily the case that

$$(gh)^n = g^n h^n \quad \text{if } \circ \text{ is non-abelian}$$

Definition

The order of $g \in G$ is

$$|g| = \min\{k \geq 1 : g^k = e\} \cup \{+\infty\}$$

Example

$|e| = 1, \quad |g| = 1 \iff g = e.$

- $\mathbb{Z}^+ = \infty, \quad k1 = 0 \iff k = 0.$
- $\mathbb{Z}/n\mathbb{Z}$ under 1, $|[1]| = n, \quad k[1] = 0 \iff n \mid k.$

Lemma (Properties of order)

(i) If $g^n = e$, then $g^{n-1} \cdot g = e \Rightarrow g^{n-1} = g^{-1}$. In particular, if $|g| = n < +\infty$, then $g^{n-1} = g^{-1}$.

(ii) $g^n = e \Rightarrow (g^n)^{-1} = e \Leftrightarrow (g^{-1})^{-1} = e$. So $|g^{-1}| = |g|$.

Example

$$-[1] = (n-1)[1] = [n-1] \in \mathbb{Z}/n\mathbb{Z}$$

In D_{2n}, we have

- $|s| = n$. (Rotate n times by $\frac{2\pi}{n}$)
- $|r| = 2$. (Reflect twice by $2\pi/n$)

So, $e, s, s^2, \cdots, s^{n-1} \in D_{2n}, \quad r, sr, s^2r, \cdots, s^{n-1}r \in D_{2n}$.

Proposition

$$D_{2n} = \{s^i : 0 \le i < n\} \cup \{s^i r : 0 \le i < n\}$$

and

$$|D_{2n}| = 2n, \quad rs = s^{-1}r = s^{n-1}r.$$

Proof

Claim 1: If $S, T \in D_{2n}$, and $S(v_0) = T(v_0)$, $S(v_1) = T(v_1)$, then $S = T$.

Proof

Two linear transformations that agree on a basis are equal.

□

Claim 2: If $T \in D_{2n}$, then

$$(T(v_0), T(v_1)) \in \{(v_i, v_{i+1}) : 0 \le i < n-1\} \cup \{(v_{i+1}, v_i) : 0 \le i < n-1\}$$

Proof

By Graphs

$$\begin{aligned}
(s^i(v_0), s^i(v_1)) &= (v_i, v_{i+1}), \quad 0 \le i \le n-1 \\
(r(v_0), r(v_1)) &= (v_0, v_{n-1}) \\
(s^i r(v_0), s^i r(v_1)) &= (v_i, v_{i-1})
\end{aligned}$$

□

Claim 3: The function $\phi : D_{2n} \to V, T \mapsto (T(v_0), T(v_1))$ is a bijection.

Proof

Injective by Claim 1.
Subjective by calculation.

□

So $|D_{2n}| = |V| = 2n$, and $\phi^{-1}((v_i, v_{i+1})) = s^i$, $u^{-1}((v_i, v_{i-1})) = s^i r$.
So $\{s^i : 0 \le i \le n-1\} \cup \{s^i r : 0 \le i \le n-1\} = D_{2n}$.

- $rs(v_0) = r(v_1) = v_{n-1}$
- $rs(v_1) = r(v_2) = v_{n-2}$

So, $rs = s^{n-1}r = s^{-1}r$.

□

Corollary

$rs' = s^{-1}r = s^{n-1}r$ for all $i \in \mathbb{Z}$.

v. Subgroups

Definition

Let G be a group A subset $H \subseteq G$ is a subgroup if

1. for all $g, h \in H$, $g \cdot h \in H$ (closed under group operation)
2. if $g \in H$, then $g^{-1} \in H$ (closed under inverses)
3. $e_G \in H$ (contains identity)

Notation $H \leq G$

Proposition

If $H \leq G$, then H is a group with operation $\circ H : H \times H \to H, \quad (g, h) \mapsto g \cdot h$.

Proof

First $\circ H$ is well-defined because h is closed under $\circ G$.
Next, $e_G \in H$, so e_G is an identity for $\circ H$.
$\circ H$ is associative because $\circ G$ is associative.
Finally, every element of H has an inverse wrt $\circ H$, it has an inverse H wrt $\circ G$.

□

Example

- $\mathbb{Z}^+ \leq \mathbb{Q}^+ \leq \mathbb{R}^+ \leq \mathbb{C}^+$ $\mathbb{N}^+ \neq\leq \mathbb{Z}^+$
- $D_{2n} \leq GL_2\mathbb{R}$ (exercise)
- $\mathbb{Q}_{>0} \leq \mathbb{Q}^\times \leftarrow$ group of invertible elements of $\mathbb{Q}$ under multiplication
- $\{e^i : 0 \leq i < n\} \leq D_{2n}$

Example

Why is $s^i \cdot s^j = s^k$ for $0 \le k < n$? If $0 \le i, j < n$?

$$\begin{aligned} s^i \cdot s^j &= s^{i+j} = s^{an+k} \quad \text{for some } a \in \mathbb{Z} \\ &= (s^n)^a \cdot s^k = e^a \cdot s^k = s^k \end{aligned}$$

Inverses:

$$\begin{aligned} (s^i)^{-1} &= s^{-i} = s^{n-i} \\ &= (s^0)^{-1} s^0 = e \end{aligned}$$

Example

$m\mathbb{Z} = \{mk : k \in \mathbb{Z}\} \le \mathbb{Z}^+$

$$mk_1 + mk_2 = m(k_1 + k_2) \in m\mathbb{Z}$$
$$-mk = m(-k) \in m\mathbb{Z}$$
$$0 = m \cdot 0 \in m\mathbb{Z}$$

Example

If G is any group then $G \le G$, and $\{e_G\} \le G$, the trivial subgroup.

Definition

Say $H \le G$ is a proper subgroup if $H \ne G$, and write $H < G$.

Proposition

We don't need to check all the properties in the definition of a subgroup,
Let $H \subseteq G$ be a subset of a group G. Then $H \leq G$ if and only if

1. H is non-empty,
2. if $g, h \in H$, then $g \cdot h^{-1} \in H$ (closed under group operation and inverses)

Proof

($\Rightarrow$) Trivial
($\Leftarrow$) Suppose (1) and (2) hold.
By (a), H contains an element $g_0 \in H$.
By (b), $e = g \cdot g^{-1} \in H$.
If $h \in H$, then $e \cdot h^{-1} = h^{-1} \in H$ by (b).
If $g, h \in H$, then $h^{-1} \in h$, so $g \cdot (h^{-1})^{-1} \in H$, but $g \cdot (h^{-1})^{-1} = g \cdot h$.
So props (1) - (3) hold of definition of subgroup.

□

Example

If W is a subspace of a vector space V, then $W \leq V^+$, V^+ is V under addition.
$0 \in W$ is non-empty and if $v, w \in W$, then $v - w \in W$, so w is a subgroup.

Proposition

Suppose G is a group, and $H \leq G$ is finite. Then $H \leq G \iff$

(a) $H \neq \emptyset$

(b) $g, h \in H$ then $g \cdot h \in H$

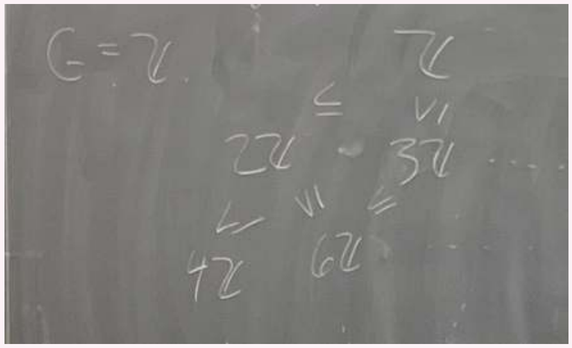
Proof

($\Rightarrow$) Trivial
($\Leftarrow$) Suppose $g \in H$. By induction, $g^n \in H$ for all $n \geq 1$.
Because H is finite, $g^1, g^2, \ldots, g^n$ must repeat. $g^i = g^j$ for some $1 \leq i < j \leq n$.
Then $g^{j-i} = e_H \in H$, because $j - i \geq 1$.
Since $g^{j-i} = e_H$, $g^{j-i-1} \cdot g = e_H \Rightarrow g^{j-i-1} = g^{-1}$.
Since $g^{j-i-1} \in H$, $g^{-1} \in H$.
So if $g, h \in H$, then $h^{-1} \in H$, so $g \cdot h^{-1} \in H$.
Hence, $H \leq G$.

□

Definition

Set of subgroups of G form a lattice.



Proposition

Suppose $\hat{f}$ is a non-empty set of subgroup of G, then

$$k = \cap_{H \in \hat{f}} H$$

is a subgroup of G.

Proposition

Recap:
Suppose F is a non-empty set of subgroup of a group G. Then set of subgroup of a group G. Then

$$K := \bigcap_{h \in F} h \text{ is a subgroup of } G$$

Proof

$e \in H$ iff $h \in F \implies e \in K$.
If $g, h \in K \Rightarrow g, h \in H$ for all $H \in F$.
$\Rightarrow gh^{-1} \in H$ for all $H \in F$.
$\Rightarrow gh^{-1} \in K$ for all $H \in F$.
So $K \leq G$.

□

Definition

Let S be a subset of a group G. Then $\langle S \rangle := \bigcap_{S \leq H \leq G} H$ is called the subgroup of G generated by S.

Proposition

If $S \leq K \leq G$, then $\langle S \rangle \leq K$.
So $\langle S \rangle$ is the smallest possible subgroup of G containing S.
(By Prop, $\langle S \rangle$ is a subgroup)

Example

$\langle \emptyset \rangle = \bigcap_{H \leq G} H = \{e\} = \langle \{e\} \rangle$,
$\langle G \rangle = G$.

Note

$\langle \{s_1, \ldots, s_k, \ldots\} \rangle = \langle s_1, \ldots, s_k \rangle$

Example

In D_{2n}, $\langle s \rangle \supseteq \{s\} \Rightarrow s^i e \langle s \rangle$ for all i
We previously saw that $\{s^i : 0 \leq i < n\} \leq D_{2n}$.
So $\langle s \rangle = \{s^i : 0 \leq i < n\}$.

Note

If $S \subseteq G$, $s^{-1} = \{s^{-1} : s \in S\}$.

Proposition

Suppose $S \subseteq G$, G is a group.
Let K be the set of all finite products of elements from $S \cup S^{-1}$ (including the empty product e), i.e.,

$$K = \left\{ s_1 s_2 \cdots s_k : k \geq 0,\ s_i \in S \cup S^{-1} \right\}$$

Then $K = \langle S \rangle$.

Proof

Claim 1 $S \subseteq K \subseteq \langle S \rangle$.

Proof

$S \subseteq K$ is clear.
Use induction to show $K \subseteq \langle S \rangle$.

□

Claim 2 $K \subseteq G$.

Proof

$e \in K$. Suppose $g = s_1 s_2 \cdots s_k \in K, h = t_1 t_2 \cdots t_l \in K$.
When $k, l \geq 0$, $s_1, \ldots, s_k, t_1, \ldots, t_l \in S \cup S^{-1}$.
($k = 0$ means $g = e$, same for $l = 0$)
Then $gh^{-1} = s_1 s_2 \cdots s_k t_l^{-1} t_{l-1}^{-1} \cdots t_1^{-1} \in K$, because $s_1, \ldots, s_k, t_l^{-1}, t_{l-1}^{-1}, \ldots, t_1^{-1} \in S \cup S^{-1}$.
So $K \leq G$.

□

By Claim 1 and Claim 2, $K \subseteq \langle S \rangle \subset K \Rightarrow K = \langle S \rangle$.

□

vi. Circular Groups

Definition

Say $S \subseteq G$ generates G if $\langle S \rangle = G$.
A group is cyclic if $G = \langle S \rangle$ for some $a \in G$. A cyclic subgroup of a group G is a subgroup of the form $\langle S \rangle$ for some $a \in G$.

Lemma

If G is a group then

(a) If $a \in G$, then $\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$.

(b) If $a \in G$, and $|a| = n < +\infty$, then $\langle a \rangle = \{a^i : 0 \leq i < n\}$.

Proof

(a) Is a corollary of preceding proposition.

(b) If $i = kn + r$ for some $k \in \mathbb{Z}$, $0 \leq r < n$. Then $a^i = a^r$, so

$$\{a^i : i \in \mathbb{Z}\} = \{a^r : 0 \leq r < n\}$$

$\square$

Example

1. $\langle e \rangle = \{e\}$,
2. $\mathbb{Z}^+ = \langle 1 \rangle = \{n \cdot 1 : n \in \mathbb{Z}\}$, If $n \in \mathbb{Z}$, then $\langle n \rangle = \{kn : k \in \mathbb{Z}\} = n\mathbb{Z}$.

Homework: All subgroups of $\mathbb{Z}$ are cyclic and infinite.

Proposition

$|\langle a\rangle| = |a|$.

Proof

By lemma, we know $|\langle a\rangle| \leq |a|$.
If $|\langle a\rangle| = +\infty$, then $|a| = \infty$. Then $\langle a\rangle = \{a^i : i \in \mathbb{Z}\}$, so in must have $a^i = a^j$ for some $0 \leq i < k \leq n$.
Then $a^{i-j} = e$ so $|a| \leq j - i \leq n$.
So $|a| \leq |\langle a\rangle|$. We conclude $|a| = |\langle a\rangle|$.

□

Example

(a)

$$\begin{aligned}\mathbb{Z}|a| &= |\langle a\rangle| = \{|a\mathbb{Z}|\} \\ &= \begin{cases}\infty & a \neq 0 \\ 1 & a = 0\end{cases}\end{aligned}$$

(b) $\mathbb{Z}/n\mathbb{Z}\ |\pm 1| = |\langle \pm 1\rangle| = |\mathbb{Z}/n\mathbb{Z}| = n$.

Lemma

If $G = \langle s\rangle$, and $T \subseteq G$, then $G = \langle T\rangle \Leftrightarrow S \subseteq \langle T\rangle$.

Proof

($\Rightarrow$): Obvious.
($\Leftarrow$): $S \subseteq \langle T\rangle \Rightarrow G = \langle S\rangle \subseteq \langle T\rangle$.

□

When does $[a] \in \mathbb{Z}/n\mathbb{Z}$ generic $\mathbb{Z}/n\mathbb{Z}$?

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} = \langle [a]\rangle &\iff [1] \in \langle [a]\rangle \\ &\iff [1] = x[a] \text{ for some } x \in \mathbb{Z}/n\mathbb{Z} \\ &\iff 1 = xa(modn) \text{ for some } x \in \mathbb{Z}/n\mathbb{Z} \\ &\iff xa - 1 = yn \text{ for some } y \in \mathbb{Z}/n\mathbb{Z}, x, y \in \mathbb{Z} \\ &\iff xa + yn = 1 \text{ for some } y \in \mathbb{Z}/n\mathbb{Z}, x, y \in \mathbb{Z} \\ &\iff \gcd(a, n) = 1\end{aligned}$$

Lemma

If $g \in G$, G is a group, and $g^n = e$, then $|g| \mid n$.

Proof

(Homework)

$\square$

Lemma

If $a \mid n$, $(n \neq 0)$ then $|[a]| = \frac{n}{a}$ in $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Proof

$n = ka$ for some $k \in \mathbb{Z}$. So $l[a] \neq 0$ for $1 \leq l < k$, and $k[a] = 0$. So $|[a]| = k$.

$\square$

Lemma

If $a, n \in \mathbb{Z}$, $n \neq 0$, $b = \gcd(a, n)$, then $\langle [a] \rangle = \langle [b] \rangle$.

Proof

Since $b \mid a$, $a = kb$ for some $k \in \mathbb{Z}$.
$\Rightarrow [a] \in \langle [b] \rangle \Rightarrow \langle [a] \rangle \subseteq \langle [b] \rangle$.
Because $b \in \gcd(a, n)$, then exists $x, y \in \mathbb{Z}$ such that $ax + ny = b \Rightarrow x[a] + [yn] = [b]$.
$\Rightarrow [b] \in \langle [a] \rangle \Rightarrow \langle [b] \rangle \subseteq \langle [a] \rangle$.

$\square$

Proposition

If $a, n \neq \mathbb{Z}$, $n \neq 0$, then $|[a]| = \frac{n}{\gcd(a,n)}$

Proof

$$[[a]] = |\langle [a] \rangle| = |\langle [b] \rangle| \quad \text{when } b = \gcd(a,n)$$

$$= |[b]| = \frac{n}{b} = \frac{n}{\gcd(a,n)}$$

□

Note

1. By Lemma $|g| = |\langle g \rangle|$
2. $\mathbb{Z}/n\mathbb{Z} = \{[k] : k = 0, 1, \ldots, n-1\}, [k] = \{m \in \mathbb{Z} : m = k(\mod n)\}$.

Corollary

1. Order of any cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ divides n.
2. For any $d \mid n$, there is a unique cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d. It is generated by $[a]$ where $a = \frac{n}{d}$.

Proof

Suppose $d = |\langle a \rangle|$ for some $a \in \mathbb{Z}$.
Then $d = \frac{n}{\gcd(a,n)} \mid n$, and $\langle [a] \rangle = \langle [\gcd(a,n)] \rangle = \langle \left[\frac{n}{d}\right] \rangle$.
So any subgroup of order d must be equal to $\langle \left[\frac{n}{d}\right] \rangle$ (uniqueness).
Conversely, given $d \mid n$, $\left[\langle [\frac{m}{d}] \rangle\right] = |\frac{n}{d}|, = \frac{n}{\frac{n}{d}} = d$.

□

Example

$\mathbb{Z}/6\mathbb{Z}$ cyclic group

- $\langle 6 \rangle = 0$, order 1.
- $\langle 3 \rangle = \{0, 3\}$, order 2.
- $\langle 2 \rangle = \{0, 2, 4\}$, order 3.
- $\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\}$, order 6.

(Square brackets optional as long as it's clear that we are in $\mathbb{Z}/n\mathbb{Z}$)

Note

All subgroups of cyclic groups in cyclic. Every cyclic group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some n.

vii. Homomorphism

Definition

Let G, H be groups. A function $f \cdot G \to H$ is a homomorphism if $f(g \cdot_G h) = f(g) \cdot_H f(h)$ for all $g, h \in G$.

Example

1. $G = GL_n\mathbb{R}$ $n \times n$ invertible matrices, $H = R^\times$
   $\det : GL_n\mathbb{R} \to \mathbb{R}^\times$,
   $\det(AB) = \det(A)\det(B)$
   det is a homomorphism.
2. If $T : V \to W$ is a linear transformation, then $T : V^+ \to W^+$ is a homomorphism
   $T(v + w) = T(v) + T(w)$
3. $\mathbb{R}_{>0} \subseteq \mathbb{R}^\times \to \mathbb{R}_{>0} : x \mapsto \sqrt{x}$
   $\sqrt{ab} = \sqrt{a}\sqrt{b}$
   Homomorphism.
4. $\varphi : \mathbb{R}^+ \mapsto \mathbb{R}^\times, x \mapsto e^x$
   $\varphi(x + y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y)$
   Homomorphism.
5. $\varphi : \mathbb{R}^+ \mapsto \mathbb{R}^\times, x \mapsto e^x$ not a homomorphism.
6. $\mathbb{Z}^+ \to \mathbb{Z}^+, x \mapsto mx$ (some $n \in \mathbb{Z}$)

$$m(x_1 + x_2) = mx_1 + mx_2$$

   Homomorphism.

Other example from group theory:

1. If $H \leq G$, then $i : H \to G : h \mapsto h$ is a homomorphism.
2. If $\varphi : G \to H, \psi : G \to H$ then $\psi \circ \varphi$ is a homomorphism.
   Check: if $g, h \in G$, then

$$\begin{aligned} \psi \cdot \varphi(gh) &= \psi(\varphi(g) \cdot \varphi(h)) \\ &= \psi(\varphi(g))\psi(\varphi(h)) \\ &= (\psi \cdot \varphi(g))(\psi \cdot \varphi(h)) \end{aligned}$$

3. If $K \leq G$, $\varphi : G \to H$ is a homomorphism then $\varphi \mid k$ is a homomorphism.

$$k \to^i G \to H, \varphi \mid k = \varphi \cdot i$$

Lemma Properties of homomorphism

1. $\varphi(e_G) = e_H$

Proof

$$\begin{aligned} c_e(e_G) &= \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G) \\ \Rightarrow e_H &= \varphi(e_G)^{-1} \cdot \varphi(e_G) = \varphi(e_G)^{-1} \cdot \varphi(e_G)\varphi(e_G) \\ &= \varphi(e_G) \end{aligned}$$

□

2. $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$

Proof

$$\begin{aligned} \varphi(e_G) &= \varphi(gg^{-1}) = \varphi(g) \cdot \varphi(g^{-1}) \\ \Rightarrow &= e_H = \varphi(g)^{-1} \cdot \varphi(g) = \varphi(g)^{-1} \cdot \varphi(g)\varphi(g) \end{aligned}$$

□

3. $\varphi(g^n) = \varphi(g)^n$ for all $g \in G$, $n \in \mathbb{Z}$

Proof

By induction on n.

(a) Base case: $n = 0$.

$$\varphi(e_G) = e_H$$

(b) Inductive step: Assume true for k, show true for $k + 1$.

$$\varphi(g^{k+1}) = \varphi(g^k g) = \varphi(g^k) \cdot \varphi(g) = \varphi(g)^k \cdot \varphi(g) = \varphi(g)^{k+1}$$

(c) Inductive step: Assume true for k, show true for $-k$.

$$\varphi(g^{-k}) = (\varphi(g^k))^{-1} = (\varphi(g)^k)^{-1} = (\varphi(g)^{-1})^k$$

□

4. $|\varphi(g)| \mid |g|$ for all $g \in G$.

Proof

Say $|g| = n < \infty$. Then $\phi(g)^n c = \varphi(g)^n = \varphi(g^n) = \varphi(e) = e$.
$\Rightarrow |\varphi(g)| \mid n$.

□

Note

If $n = \infty$, then $|\varphi(g)| \cdot \infty = \infty$, so $|\varphi(g)| = \infty$.

Notation

$$f : X \to Y$$

is a function, $S \subseteq X$.

$$f(S = \{f(x) : s \in S\})$$

Proposition

If $\phi : G \to H$ is a homomorphism, and $K \leq G$, then $\phi(K) \leq H$.

Proof

$e_G \in K \implies e_H = \phi(e_G) \in \phi(K)$.
If $g, h \in \phi(K)$, then $g = \phi(g_0), h = \phi(h_0)$ for some $g_0, h_0 \in K$.
So $g_0 h_0^{-1} \in K$ because K is a subgroup.

$$\Rightarrow gh^{-1} = \phi(g_0)\phi(h_0)^{-1} = \phi(g_0)\phi(h_0^{-1}) = \phi(g_0 h_0^{-1}) \in \phi(K)$$

$$\Rightarrow \phi(K) \text{ is a subgroup of } H$$

□

Definition

If $\{\phi : G \to H\}$ is a homomorphism, the image. Image of ϕ is the subgroup $\phi(G)$ of H (Or img)

Example

1. $\phi : \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$
   $Img = \phi(R^+) = \mathbb{R}_{>0}$
2. $\phi : \phi : \mathbb{Z} \to \mathbb{Z} : x \mapsto mx$
   $Img = \{mx : x \in \mathbb{Z}\} = m\mathbb{Z}$

Lemma

If $\phi : G \to H$ is a homomorphism and $\operatorname{Im}\phi \leq K \leq H$, then $\widetilde{G} : G \to K : g \mapsto \phi(g)$ is a homomorphism. with $Im\widetilde{G} = Im\phi$.
Say that $\widetilde{G}$ is induced by ϕ.

Lemma

A homomorphism $\phi : G \to H$ is subjective iff $Im\phi = H$.

Proof

ϕ is surjective $\iff$ $\phi(G) = H$.

□

Corollary

If $\phi : G \to H$ is a homomorphism, then ϕ induced a surjective homomorphism $\phi : G \to ImG$.

Proposition

If $\phi : G \to H$ is a homomorphism, $S \subseteq G$, then $\phi(\langle S \rangle) = \langle \phi(S) \rangle$.

Proof

$\phi(S^{-1}) = \{\phi(x^{-1}) : x \in S\} = \{\phi(x)^{-1} : x \in S\} = \phi(S)^{-1}$

$$\begin{aligned} c_e(\langle S \rangle_G) &= c_e(\{s_1 \dots s_n : n \geq 0, s_1, \dots, s_n \in S \cup S^{-1}\}) \\ &= \{\phi(s_1, \dots, s_n) : n \geq 0, s_1, \dots, s_n \in S \cup S^{-1}\} \\ &= \{t_1, \dots, t_n : n \geq 0, t_1, \dots, t_n \in \phi(S) \cup \phi(S)^{-1}\} \\ &= \langle \phi(S) \rangle_H \end{aligned}$$

□

Note

$f(S \cup T) = f(S) \cup f(T)$
$f(S \cap T) = f(S) \cap f(T)$

Notation:

$f : X \to Y$ function, $S \subseteq Y$.

$$f^{-1}(S) = \{x \in X : f(x) \in S\}$$

Proposition

If $\phi : G \to H$ is a homomorphism, $K \leq H$, then $\phi^{-1}(K) \leq G$.

Proof

$\phi(e_G) = e_H \in K$, so $e_G \in \phi^{-1}(K)$.
If $g, h \in \phi^{-1}(K)$, then $\phi(g), \phi(h) \in K$.
$\Rightarrow \phi(gh^{-1}) = \phi(g)\phi(h)^{-1} \in K$ because K is a subgroup.
$\Rightarrow gh^{-1} \in \phi^{-1}(K)$.
So, $\phi^{-1}(K)$ is a subgroup of G.

$\square$

Proposition

If G is a cyclic group, then all subgroups of G are cyclic.

Proof

Suppose G is cyclic and $H \leq G$.
Since ϕ is surjective, $H = \phi(\phi^{-1}(H)) = \phi(\langle m \rangle) = \langle \phi(m) \rangle$.
So H is cyclic

$\square$

Note

(By Homework: since G is cyclic, there exists a surjective homomorphism

$$\phi : \mathbb{Z} \to G$$

Let $l = \phi^{-1}(H)$. Then $l = m\mathbb{Z}$ for some $m \in \mathbb{Z}$, i.e., l is a cyclic subgroup of $\mathbb{Z}$.)

Definition

If $\phi : G \to H$ is a homomorphism, then kernel of ϕ is the subgroup p, $\ker \phi = \phi^{-1}(e_H)$ of G.
($\ker \phi = \{g \in G : \phi(g) = e_H\}$)

Example

1. $\phi : \mathbb{R}^+ \to \mathbb{R}^\times : x \mapsto e^x$

$$\ker \phi = \{x \in \mathbb{R}^+ : e^x = 1\} = \{0\}$$

2. $\phi : \mathbb{Z} \to \mathbb{Z} : x \mapsto mx$

$$\ker \phi = \begin{cases} \{0\} & m \neq 0 \\ \mathbb{Z} & m = 0 \end{cases}$$

3. $\ker(\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times) = SL_n(\mathbb{R})$ (Special Linear Group)

Proposition

A homomorphism $\phi : G \to H$ is injective iff $\ker \phi = \{e_G\}$.

Proof

($\Rightarrow$)
If c_e is injective, $(\phi(a) = \phi(b)) \implies (a = b), \forall a, b \in G$, then $\phi(g) = e_H = \phi(e_G) \Rightarrow g = e_G$.
($\Leftarrow$)
Suppose $\ker \phi = \{e_G\}$. If $\phi(g) = \phi(h)$ for some $g, h \in G$.
$e_H = \phi(g)^{-1}\phi(h) = \phi(g^{-1}h)$.
$\Rightarrow g^{-1}h \in \ker \phi = \{e_G\}$.
$\Rightarrow g^{-1}h = e_G \implies g = h$.
So ϕ is injective.

□

viii. Isomorphism

Definition

A homomorphism $\phi : G \to H$ is an isomorphism if ϕ is bijective (i.e., injective and surjective).

Corollary

$\phi : G \to H$ is an isomorphism $\iff$ $\ker a = \{e\}$ and $Im\phi = H$.

Recall

A function $f : X \to Y$ is a bijection iff f has an inverse $f^{-1} : Y \to X$, with the property that $f \circ f^{-1} = Id_Y$ and $f^{-1} \circ f = Id_X$.

Proposition

If $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ is also an isomorphism. (and hence an isomorphism)

Proposition

If $\phi : G \to H$ is an isomorphism, then ϕ^{-1} is also a homomorphism (and hence an isomorphism).

Proof

Suppose $h_0, h_1 \in H$. Let $g_i \in G$ be the unique element with $\phi(g_i) = h_i$ for $i = 0, 1$.
Then, $\phi^{-1}(h_0 h_1) = \phi^{-1}(\phi(g_0)\phi(g_1)) = \phi^{-1}(\phi(g_0 g_1)) = g_0 g_1 = \phi^{-1}(h_0)\phi^{-1}(h_1)$.
So ϕ^{-1} is a homomorphism. Since ϕ^{-1} is invertible, ϕ^{-1} is an isomorphism.

$\square$

Corollary

A homomorphism $\phi : G \to H$ is a homomorphism $\psi : H \to G$ such that $\psi \circ \phi = \mathrm{id}_G$ and $\phi \circ \psi = \mathrm{id}_H$.

Definition

We say two groups G, H are <u>isomorphic</u> if there is an isomorphism $\phi : G \to H$.
$G \cong H$ means that G and H are isomorphic groups.

Note

Key facts

1. If $G \cong H$, then $H \cong G$.
2. If $G \cong H$ and $H \cong K$, then $G \cong K$.
3. $G \cong G$ for any group G. (Identity $G \to G : x \mapsto x$ is always an isomorphism.)

Idea: if $G \cong H$, then G and H are identical as group.
In particular, if $G \cong H$, then

1. $|G| = |H|$.
2. G is abelian if and only if H is abelian.
3. $|g| = |\phi(g)|$ for all $g \in G$. (when $\phi : G \to H$ is an isomorphism)
4. if $K \cong G$, then $K \leq G \iff c_e(K) \leq H$.

Proposition

If G and H are cyclic groups, then $G \cong H$ if and only if $|G| = |H|$.

Proof

($\Leftarrow$): Fact
($\Rightarrow$):
Let $G = \langle a \rangle$, $H = \langle b \rangle$. If $|G| = |H|$, then $n = |a| = |G| = |H| = |b|$.
Case 1: $n = \infty$. Then $G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$
When $a^i \neq a^j$ if $i \neq j$, and $H = \langle b \rangle = \{b^i : i \in \mathbb{Z}\}$, we can define $\phi : G \to H$ by $\phi(a^k) = b^k$ for all $k \in \mathbb{Z}$.
Define $\phi G \to H$, by $\phi(a^i) = b^i$. This is a bijection and

$$\phi(a^i a^j) = \phi(a^{i+j}) = b^{i+j} = b^i b^j = \phi(a^i)\phi(a^j)$$

So ϕ is a homomorphism.
Case 2: $n < \infty$. Then $G = \{a^i : 0 \leq i < n\}$ and $H = \{b^i : 0 \leq i < n\}$, where $a^i \neq a^j, b^i \neq b^j$ if $0 \leq i \neq j < n$.
Define $\phi : G \to H$ by $\phi(a^i) = b^i$ for all $0 \leq i < n$.
Clearly a bijection and

$$\begin{aligned}
\phi(a^i a^j) = \phi(a^{i+j}) &\neq b^{i+j} \quad (i + j \text{ can be larger than } n) \\
&= \phi(a^r) \quad \text{where } r = (i + j)qn + r \\
&= b^r = b^{qn+r} \qquad \text{for some } q \in \mathbb{Z} \text{ and } 0 \leq r < n \\
&= b^{i+j} = b^i b^j = \phi(a^i)\phi(a^j)
\end{aligned}$$

So ϕ is a homomorphism.

□

Corollary

If G is cyclic, then

1. If $|G| = \infty$, then $G \cong \mathbb{Z}$.
2. If $|G| = n < \infty$, then $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$.

Corollary

All cyclic groups are abelians.

Note

With multiplication notation, write $\mathbb{Z}/n\mathbb{Z}$ as $G_n = \langle a \rangle = \{a^i : 0 \leq i < n\}$, and $\mathbb{Z}^+$ as $C_\infty = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$.

ix. Cosets and Lagrange's Theorem

Definition

Let G be a group. If $g \in G$ and $S \subseteq G$, we let $gS = \{gs : s \in S\}$ and $Sg = \{sg : s \in S\}$. If $H \leq G$ then gH (resp Hg) is called the left coset (resp. right coset) of H in G.

Example

1. $m\mathbb{Z} \leq \mathbb{Z}$. Cosets are sets of the form $m\mathbb{Z} + k$ for $k \in \mathbb{Z} = \{k + mn : m \in \mathbb{Z}\}$.
2. U is a subspace of a vector space V, then $U \leq V^+$, and cosets are sets of the form $v+U, v \in V$.

Proposition

Suppose $\phi : G \to K$ is a homomorphism and $x_0 \in G$. Let $b = \phi(x_0)$. Then the set of solutions to $\phi(x) = b$ is $\phi^{-1}(\{b\}) = x_0H = Hx_0$ for $h = \ker(\phi)$.

Proof

If $h \in H$ then $\phi(x_0h) = \phi(x_0)\phi(h) = \phi(x_0) \cdot e = b$, and $\phi(hx_0)$ similarly.
So $x_0H = \phi^{-1}(\{b\})$.
If $y \in \phi^{-1}(\{b\})$, then let $h = x_0^{-1}y$. Then $y = x_0h$ and $\phi(h) = \phi(x_0)^{-1}\phi(y) = b^{-1}b = e$.
So $h \in \ker(\phi) \Rightarrow y \in x_0H$.
$\phi^{-1}(\{b\}) = Hx_0$ similarly.
Hence, $Hx_0 = \phi^{-1}(\{b\}) = x_0H$.

$\square$

Proposition

If G is a cyclic group and $H \leq G$, then $|H| \bigm| |G|$.

Proof

$H = \langle h \rangle, G = \langle g \rangle$, $n = |g|$, $h = g^k$ for some $k \in \mathbb{Z}$.
Then $h^n = e \implies |h| \bigm| n$.

$\square$

Definition

IF $H \leq G$ then
$G/H :=$ set of left cosets of H in G.
$H \backslash G :=$ set of right cosets of H in G.

Example

$n\mathbb{Z} \leq \mathbb{Z}$. Consets an $m + m\mathbb{Z}, m \in \mathbb{Z}$.

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &= \{m + n\mathbb{Z} \mid m \in \mathbb{Z}\} \\ &= \{m + n\mathbb{Z} : 0 \leq m < n - 1\} \\ &= \mathbb{Z}/n\mathbb{Z} \end{aligned}$$

Because $m + n\mathbb{Z} = m' + n\mathbb{Z}$ if and only if $m \equiv m' \pmod{n}$.
(Why G/H is a group?)

Example

$H = \langle s \rangle \leq D_{2n}$,
Then $S'H = s^i\{s^0, s^1, \ldots, s^{n-1}\} = \{s^i, s^{i+1}, \ldots, s^{i+n-1}\} = H$.

$$\begin{aligned} s^i r\langle H \rangle &= rs^{-i}H = rH = \{r, rs, rs^2, \ldots, rs^{n-1}\} \\ &= \{r, s^{-1}r, s^{-2}r, \ldots, s^{-(n-1)}r\} \\ &= \{s^i r : 0 \leq i < n - 1\} \\ &= H_r \end{aligned}$$

$G/H = \{H, rH\} = H \backslash G$

Example

$K = \langle r \rangle \leq D_{2n}$, $s^i K = \{s^i, s^i r\}$.
$s^i r K = s^i\{r, \underbrace{r^2}_{e}\} = s^i K$.
$D_{2n}/K = \{s^i K : 0 \leq i < n\}$
$K s^i = \{s^i, r s^i\} = \{s^i, s^{-i} r\} = \{s^i, s^{n-i} r\}$
$K s^i r = K r s^{-i} = K s^{-i}$.
$n = 3, i = 1, K = \{s, sr\}$

Definition

Let X be a set. A partition of X is a subset $Q \leq \underbrace{2^X}_{\text{set of subset of X}}$ such that:

1. $\cup_{S \in Q} S = X$ (the union of all sets in Q is X)
2. If $S, T \in Q$, $S \neq T$, then $S \cap T = \emptyset$ (the intersection of any two sets in Q is empty)

Proposition

Let $H \leq G$, and $g, k \in G$ then, TFAE:

1. $g^{-1}k \in H$
2. $k \in gH$ (right cosets)
3. $gH = kH$
4. $gH \cap kH \neq \emptyset$ (the intersection of two left cosets is not empty)

Proof

(1) $\implies$ (2): If $g^{-1}k \in H$, then $k = gh$ for $h = g^{-1}k \in H \implies k \in gH$.
(2) $\implies$ (3): If $k \in gH$, then $k = gh$ for some $h \in H$. If $h' \in H$, then $kh' = ghh' \in gH$. Since $hh' \in H$, because H is a subgroup, $\Rightarrow kH \subseteq gH$. Also, $gh' = ghh^{-1}h' = kh^{-1}h' \in H \in kH$ because $h^{-1}h' \in H$. So, $gH \subseteq kH$ and $gH = kH$.
(3) $\implies$ (4): Since $e \in H$, $g \in gH$. If $gH = kH$, then $gH \cap gH = gH \neq \emptyset$.
(4) $\implies$ (1): If $gH \cap kH \neq \emptyset$, then there are $h, h' \in H$ such that $gh = kh' \Rightarrow k^{-1}g = h'h^{-1} \in H$.

□

Corollary

The set G/H forms a partition of G.

Proof

If $gH \cap kH \neq \emptyset$, then $gH = kH$ by the previous proposition.
Also $g \in gH$ for all elements of G, so $\cup_{S \in G/H} S = G$. $\cup_{g \in G} gH$

$\square$

Definition

A relation of a set X is a subset of $X \times X$. $R \subseteq X \times X, \sim \leq X \times X$.
Notation:
aRb means $(a, b) \in R$.
$a \sim b$ means $(a, b) \in \sim$.

Example

$=, \leq, <$ on $\mathbb{N}$ $a \leq b \quad \{(1,1),(1,3)\dots\}$

Definition

A relation $\sim$ on a set X is an equivalence relation if

1. $a \sim a$ for all $a \in X$ (reflexive)
2. if $a \sim b$ then $b \sim a$ for all $a, b \in X$ (symmetric)

Example

$\equiv (\mod n)$ s a equivalence relation on $\mathbb{Z}$, and $[x] = \{y : y \equiv x \pmod n\}$

Proposition

Suppose $\sim$ is a equivalence relation on a set X, and let $x, y \in X$. Then TFAE:

1. $x \sim y$
2. $y \in [x]$ (the equivalence class of x)
3. $[x] = [y]$
4. $[x] \cap [y] \neq \emptyset$ (the intersection of two equivalence classes is not empty)

Proof

- (1) $\implies$ (2): By definition of equivalence class, $y \in [x]$.
- (2) $\implies$ (3): If $z \in [y]$, then $x \sim y \sim z \implies x \sim z$, so $z \in [x]$. Therefore, $[y] \subseteq [x]$. If $z \in [x]$, then $x \sim z$ and $x \sim y \implies y \sim x \implies y \sim x \sim z \implies y \sim z$, so $[x] \subseteq [y]$.
- (3) $\implies$ (4): $x \in [x] = [x] \cap [y]$, so $[x] \cap [y] \neq \emptyset$.
- (4) $\implies$ (1): Suppose $z \in [x] \cap [y]$, so $x \sim z, y \sim z$. So, $x \sim z \sim y \implies x \sim y$.

□

Corollary

The set of equivalence classes $\{[x]_\sim : x \in X\}$ is a partition.

Lemma

If Q is a partition of X, then the partition $\sim$ defined by $x \sim y$ if and only if there is some $S \in Q$, s.t. $x, y \in S$ is an equivalence relation and $\{[x] : x \in X\} = Q$.

Proposition

If $H \leq G$, we can define a relation $\sim_H$ on G by $g \sim_H h \iff g^{-1}h \in H$. Then $\sim_H$ is an equivalence relation, and $[g] = gH$.

Proof

$\sim_H$ is the equivalence relation defined by the partition $\{gh : g \in G\}$

□

Definition

If $H \leq G$, the <u>index</u> of H in G is

$$[G : H] := \begin{cases} |G/H| & \text{if } G/H \text{ is finite} \\ \infty & \text{if } G/H \text{ is infinite} \end{cases}$$

Lemma

The function $S \to S^{-1}$ defines a bijection $G/H \to H/G$.

Proof

If $gH \in G/H$, then $(gH)^{-1} = Hg^{-1}$.
(Check: $H^{-1} = \{h^{-1} : h \in H\}$, $\{h : h \in H\} = H \equiv \{(h^{-1})^{-1} : h \in H\}$)
So, $G/H \to H/G$. $S \mapsto S^{-1}$ is well-defined.
There's also a function $H\backslash G \to G/H$ defined by $S \mapsto S^{-1}$.
Since $(S^{-1})^{-1} = S$, this is an inverse to the first function.

□

Corollary

$$[G : H] = \begin{cases} |H\backslash G| & \text{if } H\backslash G \text{ is finite} \\ \infty & \text{if } H\backslash G \text{ is infinite} \end{cases}$$

Lemma

If $S \leq G$, and $g \in G$, then $S \to gS : h \mapsto gh$ defines a bijection $S \to gS$.
In particular, $|S| = |gS|$.

Proof

$gS \to S : s \mapsto g^{-1}s$ is an inverse.

□

Theorem Lagrange's Theorem

If $H \leq G$, then $[G] = [G : H] \cdot |H|$. (In particular, $|H|$ divides $|G|$.)
If $|G|$ is finite, then $|G : H| = \frac{|G|}{|H|}$.

Proof

If $|H| = \infty$, then $|G| = \infty$, and $|G| = [G : H] \cdot |H|$.
Since G/H is a partition of G, if $[G : H] = \infty$, then $|G| = \infty$. Theorem holds

Suppose $[G : H], |H| < +\infty$. Since G/H is again a partition

$$|G| = \sum_{gH \in G/H} |gH| = \sum_{gH \in G/H} |H| = |G : H| \cdot |H|$$

□

Example

- $[D_{2n} : \langle s \rangle] = \frac{2n}{n} = 2$. $|\langle s \rangle| =?$,
- $|D_{2n} : \langle r \rangle| = \frac{2n}{2} = n$.
- $[\mathbb{Z} : m\mathbb{Z}] = m$.

Corollary

If $x \in G$, then $|x| \mid |G|$.

Proof

$|x| = |\langle x \rangle| \mid |G|$.

□

Corollary

If $|G|$ is prime, then G is cyclic.

Proof

Let $x \in G \backslash \{e\}$. Then $|x| \mid |G|$, and since $|G|$ is prime and $|x| \neq 1$, $|x| = |G|$. So $|\langle x \rangle| = |G|$, and $G = \langle x \rangle$.

□

Order	Group
1	Trivial group $\{e\}$
2	Cyclic group C_2
3	Cyclic group C_3
4	C_4, $C_2 \times C_2$
5	C_5
6	C_6, Symmetric group $S_3(D_6$ isom), $C_2 \times C_3$
7	C_7
8	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_4, Q_8
9	C_9, $C_3 \times C_3$, $S_3 \times C_3$
10	C_{10}, D_5, $C_2 \times C_5$, D_{10}

Table 1: Groups of small order (up to order 10)

Proposition

If $\phi : G \to H$ is a group homomorphism, then there is a bijection $\phi : G/\ker(\phi) \to Im(\phi)$.
$g \ker \phi \mapsto \phi(g)$

Proof

$g \ker \phi$ is the solution set of $\phi(x) = \phi(g)$.
$\phi(g \ker \phi) = \{\phi(g)\}$ and $\phi^{-1}(\phi(g)) = g \ker \phi$.
ϕ is the function $G/\ker(\phi) \to H$
$S \mapsto \phi(S) = \{x\} \mapsto x$
We know that it maps onto $Im(\phi)$, and this function has an inverse, $x \mapsto \phi^{-1}(x)$.
$Im\phi \to G/\ker \phi$.

□

Corollary

$$[G : \ker(\phi)] = \begin{cases} |Im(\phi)| & Im\phi \text{ finite} \\ \infty & \text{otherwise} \end{cases}$$

Definition

Given G, H groups, do we have a homomorphism $G \to H$?
There's always the trivial homomorphism $G \mapsto H, g \mapsto e_H$.
Called it as the **trivial homomorphism**.

Example

If $|G|$ and $|H|$ are coprime, then there is no non-trivial homomorphism $G \to H$.
If $\phi : G \to H$ is a homomorphism, then

$$|Im(\phi)| = 1 \Rightarrow Im\phi = \{e\}$$

Recall

$(H \leq G)$
If $gH = Hh$ then $g \in Hh$ s.t. $h \in gH$, so $gH = hH = Hh = Hg$.
So gH is a right coset $\iff gH = Hg$.

Definition

$H \leq G$ is a normal subgroup if $gH = Hg$ for all $g \in G$.
Notation: $H \trianglelefteq G$.

Definition

If $g, h \in G$, the conjugate of h by g is ghg^{-1}.
Since $gS = \{gs : s \in S\}$, and $Sg = \{sg : s \in S\}$, we have

$$gSg^{-1} = \{gsg^{-1} : s \in S\}$$

Proof

$g \cdot (hS) = ghS$
$g \cdot (Sg) = Sg$
$e \cdot S = S = S \cdot e$
$S \subseteq T \Rightarrow gS \subseteq gT, S_g \subseteq T_g$
So, $gH = Hg \iff gHg^{-1} = H$.

□

Note

$S \subseteq T \iff gS \subseteq gT \iff Sg \subseteq T_g$.

Proposition

Let $N \leq G$. Then TFAE:

1. $N \trianglelefteq G (gN = Ng$ for all $g \in G)$
2. $gNg^{-1} = N$ for all $g \in G$
3. $gNg^{-1} \subseteq N$ for all $g \in G$
4. $G/N = N\backslash G$
5. $G/N \subseteq N\backslash G$
6. $N\backslash G \subseteq G/N$

Proof

1. $(1 \Rightarrow 2)$: Proved above,
2. $(2 \Rightarrow 3)$: Trivial, since $gNg^{-1} = N$ means $gNg^{-1} \subseteq N$.
3. $(3 \Rightarrow 2)$: If $gNg^{-1} \subseteq N$ for all $g \in G$. Then $N = g^{-1}gNg^{-1}g = g^{-1}Ng^{-1} \forall g \in G$.

   So, $N \leq (g^{-1})^{-1}Ng^{-1} = gNg^{-1}$ for all $g \in G$.

   So $N = gNg^{-1}$ for all $g \in G$.
4. $(1 \Rightarrow 3, 6)$, If $N \trianglelefteq G$, and $gN \in G\backslash N$, then $gN = Ng \in N\backslash G \Rightarrow G/N \subseteq N\backslash G$.
5. $(6 \Rightarrow 1)$: If $G/N \subseteq N\backslash G$, then for all $g \in G$, there is some $h \in G$ s.t. $gN = Nh \Rightarrow gN = Ng$.

So (1) holds, $(6) \Rightarrow (1)$, similar. $(1) \iff (3)$ and $(6) \iff (4)$.

□

Example

$\langle s \rangle \trianglelefteq S_n$, $\langle r \rangle \ntrianglelefteq D_{2n}$.

Example

If $a : G \to H$ is a homomorphism, then $\ker(a) \trianglelefteq G$, because $g\ker(\phi) = \phi^{-1}(\phi(g)) = \ker(\phi)g$.

Example

$Z(G) \trianglelefteq G$, the center of G.

Example

If $\phi : G \to H$ is a group homomorphism, then $\ker(\phi) \trianglelefteq G$

Proof

If $g \in G$ and $h \in N = \ker(\phi)$, then

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)e_H\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = e_H$$

Thus $ghg^{-1} \in N$

□

Definition

If $S \subseteq G$, the normalize of S in G is $N_G(S) = \{g \in G, gSg^{-1} \subseteq S\}$.

Lemma

$N_G(S) \trianglelefteq G$

Proof

$e \in N_G(S)$, because $eSe^{-1} = S$.
If $g \in N_G(S)$, then

$$\begin{aligned} &gSg^{-1} \subseteq S \\ &\implies S = g^{-1}g \\ &\implies g^{-1} \in N_G(S) \end{aligned}$$

If $g, h \in N_G(S)$, then $ghS(gh)^{-1} = ghSh^{-1}g^{-1} = gSg^{-1} \subseteq S \implies gh \in N_G(S)$.

□

Lemma

If $H \leq G$, then $H \trianglelefteq N_G(H)$.

$$H \trianglelefteq G \iff N_G(H) = G$$

Proof

(Exercise)

$\square$

Note

Warning: Normal subgroup are not necessarily unique.
$H \trianglelefteq N_G(H) \trianglelefteq G$ does not imply $H \trianglelefteq G$.

Corollary

If $G = \langle S \rangle$, $H \leq G$
Then $H \trianglelefteq G$ if and only if $gHg^{-1} = H$ for all $g \in S$.

Proof

($\Rightarrow$) Obviously, if $H \trianglelefteq G$, then $gHg^{-1} = H$ for all $g \in G$.
($\Leftarrow$) If $gHg^{-1} = H$ for all $g \in S$, then $S \subseteq N_G(H) \implies \langle S \rangle \subseteq N_G(H)$.

$\square$

Lemma

If $|g| < \infty$, then $gSg^{-1} = S$ then $gSg^{-1} = S$ for all $g \in G$.

Proof

$$\begin{aligned} &gSg^{-1} = S \\ &g^2Sg^{-2} \subseteq gSg^{-1} \subseteq S \\ &g^nSg^{-n} \subseteq S \text{ for all } n \geq 1 \end{aligned}$$

If $k = |g|$, then $g^{k-1}Sg^{-(k-1)} = g^{-1}Sg = S$.

$$\implies S \subseteq gSg^{-1} \implies gSg^{-1} = S$$

□

Corollary

If G is finite, $H \leq G$, then $N_G(H) = \{g \in G, gHg^{-1} = H\}$.

Proof

If G is finite, then $|g| < \infty$ for all $g \in G$.
So $gHg^{-1} \subseteq H \iff gHg^{-1} = H$

□

Corollary

If G is finite and $G = \langle S \rangle$, $H \leq G$, then $H \trianglelefteq G$ if and only if $gHg^{-1} = H$ for all $g \in S$.

Note

Warning: This is not necessarily true if G is infinite.

x. Quotient Groups

Recall

$\mathbb{Z}/n\mathbb{Z}$ is a group with group operation defined by

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$$

Note: $[a] + [b] = [a + b]$
Question: Given $H \leq G$, when can we make G/H into a group using the group operation from G?

Definition

If $S, T \subseteq G$, define $S \cdot T = \{st, s \in S, t \in T\}$.

Lemma

1. If $H \leq G$, $H \cdot H = H$.

2. If $N \trianglelefteq G$, then $gN \cdot hN = ghN$ for all $g, h \in G$.

Proof

1. If $H \cdot H \subseteq H$, because $H \leq G$, then $H \cdot H \cdot e \subseteq H \cdot H$.

2. If $n \in N$, and $g, h \in G$, then $ghn = \underbrace{(g - e)}_{\in gN} - \underbrace{(hn)}_{\in hN} = gNhN$.

   If $n_1, n_2 \in N$, then $gn_1 \cdot hn_2 = ghh^{-1}n_1hn_2$, because N is normal, $h^{-1}n_1h \in N \Rightarrow h^{-1}n_1hn_2 \in N$.

   So $gn_1n_2 = ghh^{-1}n_1hn_2 \in ghN$.

   So $ghN \subseteq gN \cdot hN$, and $gN \cdot hN \subseteq ghN$.

   $\implies gN \cdot hN = ghN$.

   If $S, T \in G/N$ and $N \trianglelefteq G$, then $S \cdot T \in G/N$.

□

Theorem

If $N \trianglelefteq G$, then G/N is a group under the operation $\cdot$ on sets.
Furthermore, the function $q : G \to G/N : g \mapsto gN$ is a homomorphism with $\ker(q) = N$.
(G/N is called the quotient group, and q is called the quotient hormorphism.)

Proof

If $S, T, R \in G/N$, then

$$\begin{aligned}(S \cdot T) \cdot R &= \{st : s \in S, t \in T\} \cdot R \\ &= \{(st)r : s \in S, t \in T, r \in R\} \\ &= \{s(tr) : s \in S, t \in T, r \in R\} \\ &= S \cdot (T \cdot R)\end{aligned}$$

So $\cdot$ is associative on G/N.
If $S \in G/N$, say $S = gN = Ng$, for $g \in G$, then $N = eN = Ne \in G/N$ and $N \cdot S = N \cdot Ng = Ng$, and $S \cdot N = gN \cdot N = gN$.
So N is an identity for $\cdot$. Finally, if $S \in G/N$, then $S = gN$.

$$S \cdot g^{-1}N = gg^{-1}N = eN = N$$

and

$$gN \cdot gN = g^{-1}gN = eN = N$$

So $g^{-1}N$ is the inverse for S.

□

q is a homomorphism, suppose $g, h \in G$, then

$$q(gh) = ghN = gN \cdot hN = q(g) \cdot q(h)$$

$$g \in \ker(q) \iff q(g) = N \iff gN = N \iff g \in N, \ker q = N$$

Corollary

If $N \leq G$, then $N \trianglelefteq G$ if and only if a group H, and a homomorphism $q : G \to H$ such that $\ker(q) = N$.

Note

There's another way to think about quotient groups:

$$gN(gN \cdot hN = ghN)$$

$$gN \cdot hN = ghN \iff g^{-1}h^{-1}gh \in N$$

Example

1. $\mathbb{Z}/n\mathbb{Z}$
2. $D_{2n} \trianglerighteq \langle s \rangle$

$$D_{2n}/\langle s \rangle = \{\langle s \rangle, r\langle s \rangle\}$$
$$\langle s \rangle \cdot \langle s \rangle = \{s^{i+j} \mid i, j \in \mathbb{Z}\}$$
$$r\langle s \rangle \cdot \langle s \rangle = r\langle s \rangle \simeq \mathbb{Z}_2$$
$$\langle s \rangle \cdot r\langle s \rangle = \langle s \rangle\langle s \rangle r = r\langle s \rangle$$

$$\begin{aligned}\{rs^i \mid i \in \mathbb{Z}\} \cdot \{rs^j \mid j \in \mathbb{Z}\} &= \{rs^i \cdot rs^j \mid i, j \in \mathbb{Z}\} \\ &= \{r^2 s^{j-i} \mid i, j \in \mathbb{Z}\} \\ &= \{s^i \mid i \in \mathbb{Z}\}\end{aligned}$$

3. $GL_n\mathbb{C}/\mathbb{C}^\times = \{[T] \mid Z(GL_n\mathbb{C}) = \mathbb{C}^\times\}$
   $[T] = \{T \cdot \mathbb{C}^\times\}$. $[T] = \{\lambda T : \lambda \in \mathbb{C}^\times\}$
   $[T] \cdot [S] = [TS]$

Suppose $N \leq G$ (not necessarily normal), G/N can't be a group by declaring $[g] \cdot [h] = [gh]$.

This relation is not necessarily well-defined as a function.

Proposition

A relation on two sets X and Y is a subset $R \subseteq X \times Y$.
A relation R is a function $X \to Y$ if

1. If $x \in X$, then there is $y \in Y$ s.t. $(x, y) \in R$.
2. If $x \in X$ and $(x, y), (x, y') \in R$, then $y = y'$.

Note

A group operation is appended to be a function $G/N \times G/N \to G/N$.
There is a relation $R \subseteq (G/N \times G/N) \times (G/N)$ defined by $R = \{([g],[h],[gh]) \mid g,h \in G\}$.
Suppose $([g],[h]) \in G/N \times G/N$, then $([g],[h],[gh]) \in R$, so R satisfies the first condition.

When does R satisfy the second condition?
Suppose $x \in G/N \times G/N$ and $(x,y),(x,y') \in R$.
Since $(x,y) \in R$, we must have $(x,y) = ([g],[h],[gh])$ for some $g,h \in G$.
Since $(x,y') \in R$, we must have $(x,y') = ([g'],[h'],[g'h'])$ for some $g',h' \in G$.
We know $[g]=[g']$, $[h]=[h']$.
R defines a function $\iff$ for every $g,g',h,h' \in G$, with $[g]=[g']$ and $[h]=[h']$, we have $[gh]=[g'h']$.

Example

Take $g' = e$ and $h = h' = h_0^{-1}$,
Then

$$\begin{aligned} [gh] &= [g'h'] \\ \iff [g'h_0^{-1}] &= [h_0^{-1}] \\ \iff gh_0^{-1}N &= h_0^{-1}N \\ \iff h_0gh_0^{-1}N &= N \\ \iff h_0gh_0^{-1} &\in N \end{aligned}$$

So R defines a function $\iff h_0gh_0^{-1} \in N$ for all $g \in N$ and $h_0 \in G \iff N \trianglelefteq G$.

If $N \trianglelefteq G$ and K a group, what are the homomorphism $f: G/N \to K$?

Theorem (The universal property of quotient)

Suppose $\phi: G \to K$ is a homomorphism with $N \subseteq \ker\phi$, when $N \trianglelefteq G$.
Let q be the quotient homomorphism $G \to G/N$. Then there is a unique homomorphism $\psi: G/N \to K$ set $\phi = \psi \circ q$.

Proof

Define $\psi : G/N \to K$ by $\psi(gN) = \phi(g)$.
Show that this is well-defined. Suppose $gN = hN$. Then $g^{-1}h \leq \ker G$.
$e = \phi(g^{-1}h) = \phi(g)^{-1}\phi(h)$, so $\phi(g) = \phi(h)$.
So, ψ is well-defined. $\psi \cdot q(g) = \psi(gN) = \phi(g)$.
$\psi(gNhN) = \psi(ghN) = \phi(gh) = \phi(g)\phi(h) = \psi(gN)\psi(hN)$.
So, ψ is a homomorphism.
Finally, if $\psi' : G/N \to K$ is another homomorphism with $\psi' \cdot q = \phi$, then $\psi'(gN) = \psi'(q(g)) = \phi(g) = \psi(gN)$, for all $gN \in G/N$.
so $\psi' = \psi$.
(Or: $f \cdot g = f' \cdot g$ and g is surjective, then $f = f'$.)

□

Definition

If G, K a group, let $Hom(G, K)$ be the set of homomorphism from G to K.

Corollary

If $N \trianglelefteq G$ and K is a group then the function

$$q^* : Hom(G/K, K) \to \{\phi \in Hom(G, K) \mid N \subseteq \ker \phi\}$$

xi. Isomorphism Theorem

Recall

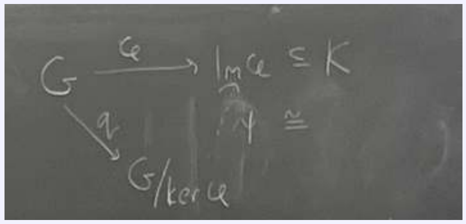
If $\phi : G \to L$ is a homomorphism, then there is a bijection

$$G/\ker(\phi) \to K : g\ker(\phi) \mapsto \phi(g)$$

Theorem 1st Isomorphism Theorem

Suppose $\phi : G \to K$ is a homomorphism, and $q \to G\ker(\phi)$ is the quotient map. Then there is an isomorphism.

$$\psi : G/\ker(\phi) \to Im(\phi) \quad \psi \cdot q = \phi(g)$$



Proof

$\ker\phi \geq \ker\psi$, so by the universal proposition of quotient groups, there is a homomorphism $\psi : G/\ker(\phi) \to Im(\phi)$ such that $\psi \cdot q = \phi$.
If $y \in G$, then $\phi(g) = \psi \circ q(g) = \psi(g\ker(\phi))$. so, $Im(\phi) = Im(\psi)$. We can regard ψ as a homomorphism $\psi : G \to Im(\phi)$.
We previously showed that the function

$$G/\ker(\phi) \to Im(\phi) : g\ker(\phi) \mapsto \phi(g)$$

is a bijection, so ψ is an isomorphism.

□

1. $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \underbrace{\cong}_{\text{1st iso thm}} Im\det = \mathbb{R}^\times$.

   Note: $\det \begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \end{pmatrix} = \lambda = Im\det = \mathbb{R}^\times$

   $SL_n(\mathbb{R}) = \ker(\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times)$, so by the 1st isomorphism theorem,

2. $\mathbb{R}^+/\mathbb{Z}^+ \cong Im(\exp)$.

   $\mathbb{R}^+ \to \mathbb{C}^\times : \theta \mapsto e^{2\pi i\theta}$

$$\ker(\exp) = \{\theta : e^{2\pi i\theta} = 1\} = \mathbb{Z}^+$$

$$Im(\exp) = \{z \in \mathbb{C}^\times : |z| = 1\} = S^1$$

   (Circle group)

Question: What are the subgroups of G/M?

Recall

If $\phi : G \to K$ is a homomorphism then

1. $H \leq G \Rightarrow \phi(H) \leq K$.
2. If $H \leq K \Rightarrow \phi^{-1}(H) \leq G$.

For any function $f : X \to Y$, if $S \subseteq T \subseteq Y \Rightarrow f^{-1}(S) \subseteq f^{-1}(T)$. and $S \leq T \leq X$ then $f(S) \leq f(T)$.

Lemma

If $\phi : G \to K$ is a homomorphism, then

1. $H \leq K$ then $\ker\phi \leq \phi^{-1}(H) \leq G$.
2. $H\ker(\phi) \leq H' \leq G$ then $\phi^{-1}(\phi(H')) = H'$.

Proof

1. $\ker\phi = \phi^{-1}(\{e_K\}) \leq \phi^{-1}(H)$.
2. $\phi^{-1}(\phi(H')) = H'$.

   Suppose $g \in \phi^{-1}(\phi(H'))$, then

$$\begin{aligned} &\phi(g) \in \phi(H') \\ \Rightarrow &\phi(g) = \phi(h) \text{ for some } h \in H' \\ \Rightarrow &h^{-1}g \in \ker(\phi) \\ \Rightarrow &g = h \cdot h^{-1}g \in H' \\ &\phi^{-1}(\phi(H')) \subseteq H' \end{aligned}$$

Note

Is it that $\phi(\phi^{-1}(H)) = H$?

If $f : X \to Y$ is surjective, then $f(f^{-1}(S)) = S$ for all $S \subseteq Y$.
Also in general, if $f : X \to Y$ is a function, then $f(S \cap T) \neq f(S) \cap f(T)$.
but $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$.

$\square$

Theorem Correspondence Theorem for subjective homomorphism

Let $\phi : G \to K$ be a surjective homomorphism.
Then there is a bijection correspondence

$\Rightarrow$: $H' \mapsto \phi(H')$
$\Leftarrow$: $\phi^{-1}(H) \leftarrow H$.

Note

Furthermore, if $\ker(\phi) \leq H, H_1, H_2 \leq G$ then

1. $H_1 \leq H_2 \iff \phi(H_1) \leq \phi(H_2)$.
2. $\phi(H_1 \cap H_2) = \phi(H_1) \cap \phi(H_2)$.
3. $H \trianglelefteq G \iff \phi(H) \trianglelefteq G$.

Proof

1. Suppose $H \leq K$, then $\phi(\phi^{-1}(H)) = H$ because ϕ is surjective.

   If $H' \geq \ker(\phi)$, then $\phi^{-1}(\phi(H')) = H'$ by lemma.

   Part 1: If $H \leq K$, then $\phi(\phi^{-1}(H)) = H$ since ϕ is surjective.

   Part 2: If $H' \geq \ker(\phi)$, then $\phi^{-1}(\phi(H')) = H'$.

   Therefore, the maps $H' \mapsto \phi(H')$ and $H \mapsto \phi^{-1}(H)$ are inverses, so the correspondence is a bijection.

2. $H_i = \phi^{-1}(K_i)$ $k_i \leq k$.

$$\begin{aligned} H_1 \cap H_2 &= \phi^{-1}(K_1) \cap \phi^{-1}(K_2) \\ &= \phi^{-1}(K_1 \cap K_2) \end{aligned}$$

   $K_i = \phi(H_i)$, so $H - 1 \cap H_2 = \phi^{-1}(\phi(H_1) \cap \phi(H_2))$.

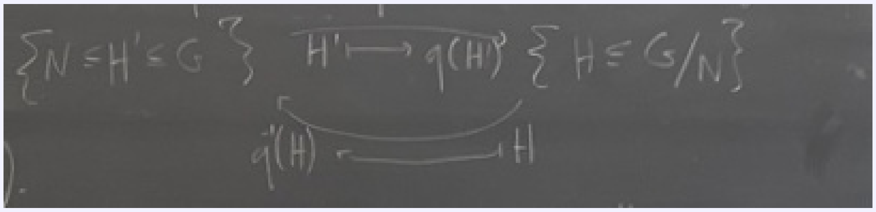
$$\phi(H_1 \cap H_2) = \phi(\phi^{-1}(\phi(H_1) \cap \phi(H_2))) = \phi(H_1) \cap \phi(H_2)$$

3. (Hmw)

□

Theorem Correspondence Theorem for quotient groups

Let $N \subseteq G$, and let $q : G \to G/N$ be the quotient group. Then there is a bijection



Note

Furthermore, if $N \leq H, H_1, H_2 \leq G$, then

1. $H_1 \leq H_2 \iff q(H_1) \leq q(H_2)$
2. $q(H_1 \cap H_2) = q(H_1) \cap q(H_2)$
3. $H \cong G \iff q(H) \cong G/N$

Proof

q is surjective, $\phi : G \to K$ is a surjective homomorphism, then by 1st isomorphism theorem, $G/\ker(\phi) \cong Im\phi = K$.
So the correspondence thm for quotients implies the correspondence for subjective homomorphism. These two are equivalent.

□

Proposition

What is $q(H)$ when $N \leq H \leq G$?
Let $N \trianglelefteq G$, $G \to G/N$ quotient homomorphism, and $N \leq K \leq G$. Then $N \trianglelefteq K$ and the funciton

$$\begin{aligned} q : & K/N \to q(K) \leq G/N \\ & kN \mapsto kN \end{aligned}$$

is a isomorphism. (Consequently, we denote $q(K)$ as K/N)

Proof

$kNk^{-1} = N$ for all $k \in K$,
$\implies kNk^{-1} = N$ for all $k \in K \Rightarrow N \trianglelefteq K$.
If $K_1N = K_2N$, $\phi : K/N \to G/N : kN \mapsto kN$ is well-defined.
Since $q(K) = \{kN : k \in K\}$, ϕ gives a surjective function $K/N \to q(K)$.

$$\begin{aligned} \phi(k_1N \cdot k_2N) &= \phi(k_1k_2N) \\ &= k_1k_2N \\ &= k_1N \cdot k_2N = \phi(k_1N) \cdot \phi(k_2N) \end{aligned}$$

ϕ is injective because

$$\begin{aligned} & \phi(k_1N) = \phi(k_2N) \\ \iff & k_1N = k_2N \in G \\ \iff & k_1^{-1}k_2 \in N \\ \iff & k_1N = k_2N \end{aligned}$$

□

$$D_{2n} = \{s^i r^j : 0 \leq i < n-1, 0 \leq j < 1\}$$

Every element can be written uniquely as hk for $h \in H = \langle s \rangle$, $k \in K = \langle r \rangle$.

In general, given $H, K \in G$, when can we write every element of G uniquely as hk fir $h \in H$, $k \in K$?

Lemma

The function $m : H \times K \to G \ (h,k) \mapsto hk$ is injective if and only if $H \cap K = \{e\}$.

Proof

If $h \in H \cap K$, then $(h, h^{-1}) \mapsto e$, $(e,e) \mapsto e$, so if $e \neq h \in H \cap K$, then m is not injective.
Suppose $H \cap K = \{e\}$, and $h_1k_1 = h_2k_2$ for $h_1, h_2 \in H$, $k_1, k_2 \in K \Rightarrow \underbrace{h_2^{-1}h_1}_{\in H} = \underbrace{k_2k_1^{-1}}_{\in K}$.

$\Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} = e \Rightarrow h_1 = h_2$ and $k_1 = k_2$.
Thus, m is injective.

□

We can write every element of G uniquely as hk for $h \in H, k \in K \iff HK = G$ and $H \cap K = \{e\}$.

$$HK = \bigcup_{h \in H} hK \text{ is a partition of } HK$$

Let $X = \{hK : h \in H\}$

Lemma

Let $h_1, h_2 \in H$, Then $h_1K = h_2K$ if and only if $h_1^{-1}h_2 \in H \cap K$, if and only if $h_1 H \cap K = h_2 H \cap K$.

Proof

From basic facts and $h_1^{-1}h_2 \in H$,

□

Corollary

$H / H \cap K \implies X : hH \cap K \mapsto hK$ is a bijection.

Proof

$h_1 H \cap K = h_2 H \cap K \implies h_1K = h_2K \implies$ function is well-defined.
Function is subjective by definition of X.
Injectivity: $h_1k = h_2k \implies h_1 H \cap K = h_2 H \cap K$.
$|X| = [H : H \cap K]$

□

Corollary

If $H, K \leq G$ then $|HK| \times |H \cap K| = |H| \times |K|$.

Proof

$|HK| = |X| \cdot |K| = [H : H \cap K] \cdot |K|$.
Multiply by $|H \cap K|$ and apply Lagrange's theorem gives corollary.

$\square$

Corollary

$$|HK| \times |H \cup K| = |H| \times |K|$$

$$[H : H \cap K] = |x|$$

$$|HK| = |X| \cdot |K| = [H : H \cap K] \cdot |K|$$

If everything finite, $[H : H \cap K] = |HK|/|K|? = \underbrace{[HK \times K]}_{\text{May not a group}}$

Proposition

Let $H, K \leq G$. Then $HK \leq G \iff HK = KH \iff KH \subseteq HK$.

Proof

Suppose $HK \leq G$. IF $h \in H, k \in K$, then $h, k \in HK \Rightarrow kh \in HK \implies KH \subseteq HK$.

$$k^{-1}h^{-1} = HK \Rightarrow hk = (k^{-1}h^{-1})^{-1} \in (HK)^{-1} = K^{-1}H^{-1} = KH$$

So $HK \leq KH \implies HK = KH$.
If $HK = KH$, then $KH \subseteq HK$. If $KH \subseteq HK$, and $h_0, h_1 \in H, k_0, k_1 \in K$, then $(h_0k_0)(h_1k_1)^{-1} = h_0k_0k_1^{-1}h_1^{-1} = h_0h_2k_2$ for some $h_2 \in H, k_2 \in K$. Since $k_0k_1^{-1}h_1^{-1} \in KH \subseteq HK$, so $(h_0k_0)(h_1k_1)^{-1} \in HK$. So $HK \leq G$.

$\square$

Corollary

If $HK = KH$, then $[H : H \cap K] = [HK : K]$

When does $HK = KH$?

Sufficient condition for all $h \in H$,

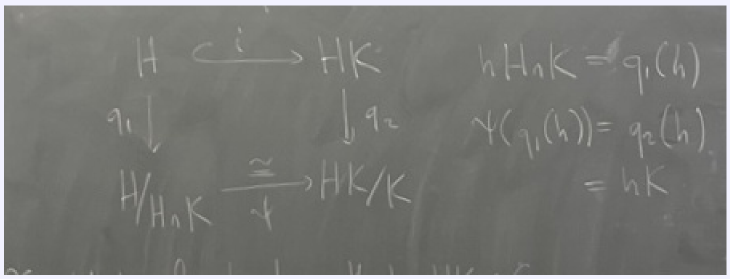
$$hK = Kh$$
$$hKh^{-1} = K \text{ for all } h \in H$$
$$H = N_G(K), \text{ the normalizer of } K \text{ in } G$$
$$H \subseteq N_G(K)$$
$$HK \leq G$$

Theorem Second Isomorphism Theorem

If $H, K \leq G$ and $H \leq N_G(K)$, then $HK \leq G$, $K \trianglelefteq HK$ and $H \cap K \trianglelefteq H$.
Furthermore, if $i : H \to HK$ is the inclusion,

$$q_1 : H \to H/H \cap K \text{ is the quotient map}$$
$$q_2 : HK \to HK/K \text{ is the quotient map}$$

Then there is an isomorphism $\psi : H/H \cap K \to HK/K$ such that $\psi \cdot q_1 = q_2 \cdot i$.



Proof

We have already shown that $HK \leq G$. IF $hk \in HK$, then

$$\begin{aligned} hkK(hk)^{-1} &= hkKk^{-1}h^{-1} \\ &= hKh^{-1} \text{ since } k \in K \\ &= K \text{ since } H \leq N_G(K) \end{aligned}$$

If $k \in H \cap K$ and $h \in H$, then $hkh^{-1} \leq H$ and $hkh^{-1} \in K$ since $K \trianglelefteq G$, so $hkh^{-1} \in H \cap K$.
So $hH \cap Kh^{-1} = H \cap K$, for all $h \in H \implies h \cap K \trianglelefteq H$.
Let ψ be the function $H/H \cap K \to HK/K$, $hH \cap K \mapsto hk$.
We're previously shown that this is a bijection, it satisfies $\psi \cot q_1 = q_2 \cdot i$.
If $h_0, h_1 \in H$, then $\psi(h_0 H \cap K \cdot h_1 H \cap K) = \psi(h_0 h_1 H \cap K) = h_0 h_1 K = h_0 K \cdot h_1 K = \psi(h_0 H \cap K) \cdot \psi(h_1 H \cap K)$.
So ψ is a homomorphism.

□

Example

$(H \cup K), P \leq GL_2(\mathbb{R})$, P permutation matrices. $N_{GL_n}(T) = PT$.
$P \cap T = \{e\}$. So $T \trianglelefteq PT$.

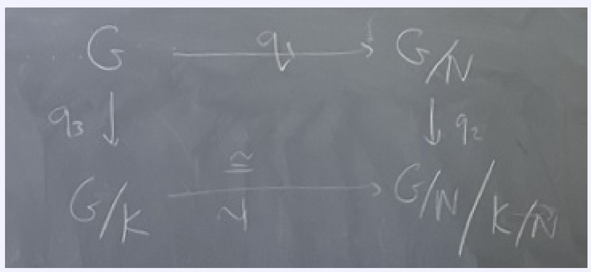
$$PT/T \cong P/(P \cap T) = P/\{e\} \cong P$$

From correspondence theorem, if $N \trianglelefteq G \iff K/N \trianglelefteq G/N$.

Suppose $K/N \trianglelefteq G/N$. What is $(G/N)/(K/N)$?

Theorem Third Isomorphism Theorem

If $N, K \trianglelefteq G$ and $N \leq K \leq G$, and $q_1 : G \to G/N$, $q_2 : G/N \to (G/N)/(K/N)$, $q_3 : G \to G/K$ are the quotient homomorphisms, then there is an isomorphism $\psi : G/K \to (G/N)/(K/N)$ such that $\psi \cdot q_3 = q_2 \cdot q_1$.



Example

$10\mathbb{Z} \leq 5\mathbb{Z} \leq \mathbb{Z}$

$$(\mathbb{Z}/10\mathbb{Z})/(5\mathbb{Z}/10\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$$

(**Note:** $5Z/10Z \cong \mathbb{Z}/2\mathbb{Z}$)

Proof

$Im\ q_2 \circ q_1 = (G/N)/(K/N)$.
$\ker q_2 \circ q_1 = q_1^{-1}(q_2^{-1}(\{e\})) = q_1^{-1}(K/N) = K$ by correspondence theorem.
By the 1st isomorphism theorem, there is an isomorphism

$$\psi : G/K \to (G/N)/(K/N) \text{ s.t. } \psi \cdot q_3 = q_2 \cdot q_1$$

□

xii. Group Actions

Permutation $\sigma, \pi \in S_n, \sigma \cdot \pi$

So, acts on $\{1, \ldots, n\}$. D_{2n} acts on P_n regards $n - gon$.

$GL_n\mathbb{R}$ acts on $\mathbb{R}^n$. We want an abstract notion of group action.

Definition

Let G be a group. A left action of G on a set X is function

$$\cdot : G \times X \to X : (g, x) \mapsto g \cdot x$$

Such that:

1. $g \cdot (h \cdot x) = (g \cdot h) \cdot x$ for all $g, h \in G, x \in X$ (associativity)
2. $e \cdot x = x$ for all $x \in X$ (identity)

Example

1. All the above.
2. G groups x any set, trivial action $g \cdot x = x$
3. If X is a set, $S_x = \{f : x \to X : f$ is a bijection $\}$ acts on X by $f \cdot x = f(x)$
4. D_{2n} acts on $\mathbb{R}^2$ and a $V(P_n) = \{v_1, \ldots, v_n\}$ (Vertex set of P_n)

Definition

G acts on X, and $Y \subseteq X$, we say that Y is invariant under the $G - action$ if $g \cdot y \in Y, \forall y \in Y$.

Lemma

If G acts on X, and $Y \subseteq X$ is invariant under the $G - action$, then G acts on Y via the action $G \times Y \to Y : (g, y) \mapsto g \cdot y$.(Same action as on X)

Example

$\{0\}$ is an invariant subset of the $GL_n\mathbb{R}$ action on $\mathbb{R}^n$. ($GL_n\mathbb{R}$ acts trivially on $\{0\}$)

Proposition

If G acts on X and Y, then G acts on $Fun(X,Y)$ via

$$G \times Fun(X,Y) \to Fun(X,Y) : (g,f) \mapsto x \mapsto g \cdot f(g^{-1} \cdot x)$$

$$g \cdot f(x) = g \cdot f(g^{-1} \cdot x)$$

Proof

Homework :p

□

Note

In many situations, we have an action on X, and take the trivial action on Y, so rule is $g \cdot f(x) = f(g^{-1} \cdot x)$.

Definition

Let G be a group. A right action of G on a set X is function

$$\cdot : X \times G \to X : (x,g) \mapsto x \cdot g$$

Such that:

1. $x \cdot (g \cdot h) = (x \cdot g) \cdot h$ for all $g, h \in G, x \in X$ (associativity)
2. $x \cdot e = x$ for all $x \in X$ (identity)

Example

If G acts on X with a left action, Y any set, then G has a right action on $Fun(X,Y)$ via $(f \cdot g)(x) = f(g \cdot x)$

Lemma

We'll concentrate a left action

If $\cdot$ is a right action of G on X, then $g \cdot x := x \cdot g^{-1}$ is a left action of G on X.

Proof

$$g \cdot (h \cdot x) = g \cdot (x \cdot h^{-1}) = (x \cdot h^{-1}) \cdot g^{-1} = x \cdot (h^{-1} \cdot g^{-1}) = (x \cdot h^{-1}) \cdot g^{-1} = (g \cdot h) \cdot x$$

$$e \cdot x = x \cdot e^{-1} = x \quad \forall g, h \in G, x \in X$$

□

Proposition

If G acts on a set X, then G acts a 2^X, by $g \cdot S = \{gs : s \in S\}$

Proof

$e \cdot S = \{e \cdot s : s \in S\} = S$ (identity)

$(g \cdot h) \cdot S = \{gh \cdot s : s \in S\} = g \cdot \{h \cdot s : s \in S\} = g \cdot (h \cdot S)$

□

Note

2^X is in bijection with $Fun(X, \{0, 1\})$,

$S \leftrightarrow X_s(x) = \begin{cases} 1 & \text{if } x \in S \\ 0 & \text{if } x \notin S \end{cases}$

Hmw, show that this bijection sends $G-action$ on 2^X to the $G-action$ on $Fun(X, \{0, 1\})$. (With the trivial action on $\{0, 1\}$)

Proposition

How can we get an action (non-trivial) of a group G on a set?

If G is a group, then the group operation $\cdot : G \times G \to G$ is a left/right action of G on itself.

We call this the left/right regular action of G on itself.

Proof

$g \cdot (h \cdot k) = (g \cdot h) \cdot k$ for all $g, h \in G, k \in G$ (associativity)

$e \cdot g = g$ for all $g \in G$ (identity)

□

Corollary

If $H \leq G$, then G acts on G/H by $g \cdot kH := gkH$.

Proof

G acts on G via the left regular action, so G acts in 2^G $g \cdot S = \{gs : s \in S\}$.

□

If $S \in G/H \subseteq 2^G$ and $g \in G$, then $g \cdot S \in G/H$. ($S = kH$ then $gS = gkH$)
So, G/H is an invariant subset of 2^G, so G acts on G/H via the actions.
(and this action does satisfy $g \cdot kH = gkH$)

Lemma

Let G act on X. Giving $g \in G$, let

$$l_g : X \to X : x \mapsto g \cdot x$$

Then:

1. $l_g l_h = l_{gh}$ for all $g, h \in G$.
2. $l_e = \mathrm{id}_X$ where e is the identity of G.
3. l_g is a bijection for all $g \in G$.

Proof

1. $l_g l_h(x) = g \cdot (h \cdot x) = (gh) \cdot x = l_{gh}(x)$, so $l_g l_h = l_{gh}$.
2. $l_e(x) = e \cdot x = x$, so $l_e = \mathrm{id}_X$. For all $x \in X$.
3. $l_g l_g^{-1} = l_g g^{-1} = l_e = \mathrm{id}_X$, $l_g^{-1} l_g = l_{g^{-1}g} = l_e = \mathrm{id}_X$. Thus, $l_g^{-1} = l_{g^{-1}}$

□

Corollary

If G acts on X, then the function
$G \to S_X = \{f : X \to X | f \text{ is a bijection}\}$
$g \mapsto l_g$ is a homomorphism.

Definition

A permutation representation of a group G on a set X is a homomorphism $G \to S_X$, if X is finite with $|X| = n$, then $S_x \cong S_n$.
So G action on X gives a homomorphism $G \to S_n$.

Example

Let D_{2n} act on the set $\{v_1, v_2, \ldots, v_n\}$ (the vertices of a regular n-gon). This action gives a homomorphism:

$$D_{2n} \to S_n$$

where each group element permutes the vertices. For example, $1 \mapsto v_1$, $2 \mapsto v_2$, …, $n \mapsto v_n$.

Theorem

1. If G acts on X, then there is a homomorphism $\phi : G \to S_X$ s.t. $\phi(g)(x) = g \cdot x$ for all $g \in G$ and $x \in X$.
2. If $\phi : G \to S_X$ is a homomorphism, then $g \cdot x = \phi(g)(x)$ defines an action of G on X.

Proof

1. $\phi(g) = l_g$, $l_g(x) = g \cdot x$
2. $$\begin{aligned} g \cdot (h \cdot x) &= g \cdot (\phi(h)(x)) \\ &= \phi(g)(\phi(h)(x)) \\ &= \phi(g) \cdot \phi(h)(x) \\ &= \phi(gh)(x) \\ &= (gh) \cdot x \end{aligned}$$

$$e \cdot x = \phi(e)(x) = \mathrm{Id}_X(x) = x \qquad \text{for all } x \in X, g, h \in G$$

So $\cdot$ is a group action.

□

Exercise: Proof that points 1 and 2 gives a bijection.

Group action of G on X $\leftrightsquigarrow$ Permutation representation of G on X.

Definition

Let G act on X, and let $\phi : G \to S_X$ be the corresponding permutation representation. Then the kernel of the action is $\ker\phi$, and the action is faithful if $\ker\phi = \{e\}$.

Lemma

An action is faithful $\iff$ for all $g \in G\backslash\{e\}$, there is $x \in X = 1$. $g \cdot x \neq x$, so there is some $x \in X$ s.t. $\phi(g)(x) \neq x$.

Proof

$\Rightarrow$ If $g \in G\backslash\{e\}$, so there is some $x \in X$ s.t. $\phi(g)(x) \neq x$.
$\Leftarrow$ if $g \in G$ and $g \in \ker\phi$, then $\phi(g) = \mathrm{id}_X$, so $g \times x = \phi(g)(x) = x$ for all $x \in X$, so $g = e \Rightarrow \ker\phi = \{e\}$.

□

Example

- $S_x \curvearrowright X$ is faithful. (If $f(x) = x \forall x \in X$, then $f = \mathrm{id}_X$.)
- $GL_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$, $M \neq \mathrm{id}$, $M_v \neq v$. Faithful action.
- Trivial action of G on X is not faithful is G is not trivial.

Theorem Cayley's Theorem

The left regular action of a group G on itself is faithful. Consequently, G is isomorphic to a subgroup of S_G.
In particular, if $|G| = n < +\infty$, then G is isomorphic to a subgroup of S_n.

Example

- $\mathbb{Z}_2 \cong H = S_2 \subset S_2$. Because $|S_2| = 2$ and $|H| = 2$, so $H = S_2$.
- $D_6 \cong H \leq S_6$. 6!

Proof

If $g \in G$, t hen $g \cdot e = g \neq e$ if $g \neq e$, so the action is faithful.
Because is faithful, permutation $\phi : G \to S_G$ is injective, because 1st isomorphism theorem then $G \cong G/\langle e\rangle \cong \mathrm{Im}\,\phi \leq S_G$.
If $|G| = n < +\infty$, then $S_G \cong S_n$.

□

Definition

Suppose G acts on X, then the G-orbit of a point $x \in X$ is $\mathscr{O}_x = \{g \cdot x | g \in G\} \subseteq X$.
The G-orbit is sometimes denoted by $G \cdot x$.
An action is transitive if $X = \mathscr{O}_x$ for some $x \in X$.

Example

- Left regular action of $G \curvearrowright G$
  $g \in G$, $\mathscr{O}_g = \{hg : h \in G\} = Gg = G$ transitive.
- $H \leq G$. $H \curvearrowright G$ by left multiplication, $\mathscr{O}_g = Hg$ Transitive $\iff$ $H = G$.
- $GL_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$.

$$\begin{aligned}\mathscr{O}_v &= \{Mv : M \in GL_n(\mathbb{R})\} \\ &= \begin{cases} R^n \backslash \{0\} & \text{if } v \neq 0 \\ \{0\} & \text{if } v = 0 \end{cases}\end{aligned}$$

Note

action of S_n on $\{1, 2, \ldots, n\}$ is given by
Let $x = 1$

$$\mathscr{O}_1 = \{1, 2, \ldots, n\}$$

Another example:
Action of $\langle s \rangle = H$ on $\{1, \ldots, G\}$ $\sigma = (1, 4, 5)(2, 3)$

- $\mathscr{O}_1 = \{1, 4, 5\} = \mathscr{O}_4 = \mathscr{O}_5$
- $\mathscr{O}_2 = \{2, 3\} = \mathscr{O}_3$
- $\mathscr{O}_6 = \{6\}$

Lemma

If G acts on X, the relation $\tilde{G}$ on X defined by $x\tilde{G}y$ if and only if there is an element $g \in G$ such that $g \cdot x = y$ is an equivalence relation.

$$[x]_{\tilde{G}} = \mathscr{O}_x$$

Proof

If $x \in X$ then $x \sim x$ because $e \cdot x = x$. If $x \sim y$ then $y = g \cdot x$ for some $g \in X$ so $x = g^{-1} \cdot y \implies y \sim x$.
If $x \sim y$ and $y \sim z$, then $y = g \cdot x$ and $z = h \cdot y$ so $z = h \cdot (g \cdot x) = (hg) \cdot x \implies z \sim x$.
$\underbrace{[x]_\sim}_{\{y : x \sim y\}} = \mathscr{O}_x$ by definition of orbit.
Because orbits on equivalence classes, we know
e.g.

$$\mathscr{O}_x = \mathscr{O}_y \iff y \in \mathscr{O}_x, x \neq \emptyset$$

□

Corollary

An action of G on X is transitive if and only if $\mathscr{O}_x = X$ for all $x \in X$.

Proof

($\Leftarrow$) Clear
($\Rightarrow$) If $\mathscr{O}_x = X$ for some $x \in X$, then $y \in \mathscr{O}_x$ for all $y \in X$. $\implies \mathscr{O}_y = \mathscr{O}_x = X$ for all $x \in X$.

□

Definition

Let $\sim$ is an equivalence relation on a set X. A set of representatives for $\sim$ is a set S s.t. every equivalence class of $\sim$ contains exactly one element of S.

Example

$\{1, 2, 6\}$ is a set of representatives for $\langle\sigma\rangle \curvearrowright \{1, \ldots, 6\}, \sigma = (1, 4, 5)(2, 3)$.
So is $\{4, 3, 6\}$.

Proposition

Let G act on X, and S be a set of representatives for the action (i.e. for $\tilde{G}$) then

$$|X| = \sum_{x \in S} |\mathscr{O}_x|$$

Proof

Orbits partition X

□

Question: What is $\mathscr{O}_x$?

Definition

If G acts on X, and $x \in X$, then the stabilizer of x is

$$G_x = \{g \in G : g \cdot x = x\}$$

Proposition

$G_x \leq G$

Proof

$e \in G_x$, and if $g, h \in G_x$, then $(g \cdot h) \cdot x = g \cdot h \cdot x = g \cdot x = x$,
so $gh \in G_x$, and $h \cdot x = x \implies h^{-1}x = h^{-1} \cdot h \cdot x = x$.
so $h^{-1} \in G_x$.

□

Lemma

If G acts on X, then kernal is $\cap_{x \in X} G_x$.

Proof

g is in the kernel of the action
$\iff l_g = Id_X \iff g \cdot x = x$ for all $x \in X \iff g \in G_x$ for all $x \in X$.

□

Example

- $S_6 \curvearrowright \{1, 2, \ldots, 6\}$. Faithful action.
- $G_6 = \{\mathscr{O}(6) = 6\}$, $|G_6| = 5!$.

Theorem (Orbit-stabilize thm)

If G acts on X, and $x \in X$, then there is a bijection

$$\begin{aligned} \phi : G/G_x &\to \mathscr{O}_x \\ gG_x &\mapsto g \cdot x \end{aligned}$$

Proof

Suppose $gG_x = hG_x$, then $h^{-1}g \in G_x$, so $h^{-1}g \cdot x = x \implies h \cdot x = g \cdot x$.
So the function ϕ is well-defined.
Clearly ϕ is onto.
Suppose $\phi(gG_x) = \phi(hG_x)$, then

$$\begin{aligned} & g \cdot x = h \cdot x \\ \implies & h^{-1}g \cdot x = x \\ \implies & h^{-1}g \in G_x \\ \implies & gG_x = hG_x \end{aligned}$$

□

Corollary

(1) $|\mathscr{O}_x| = [G : G_x]$

(2) If S is a set of representatives for the G action, and X and G on finite,

$$|X| = \sum_{x \in S} \frac{|G|}{|G_x|} = |G| \cdot \sum_{x \in S} \frac{1}{|G_x|}$$

Lemma

Let $H \leq G$. Then

(1) the left multiplication action of G on G/H is transitive.

$$\boxed{G/H = G/G_{eH} \xrightarrow[\text{Orbit-Stabilizer}]{\sim} \mathscr{O}_{eH} = G/H}$$

Proof

$g \cdot eH = gH$ so action is transitive. $gH = g \cdot eH = eH \iff g \in H$.
So $G_{eH} = H$.

□

Theorem

If G is finite, and $H \leq G$, s.t. $[G : H] = p$ where p is the smallest prime p dividing $|G|$, then $H \trianglelefteq G$.

Proof

Let K be the kernel of the action of G on G/H by left multiplication.
We know $K = \cap_{x \in X} G_x \leq G_{eH} = H$.

Let $k = [H : K] = \frac{|H|}{|K|}$.
$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = p \cdot k$.

By first isomorphism theorem, $G/K \cong$ a subgroup of $S_{G/H} \cong S_p$.
So $kp = |G/K|$ divides $p! \implies k \mid (p-1)!$.
Also $k \mid |G| \implies k = 1$.

□

Lemma

$G \times G \to G \cdot (g, h) \mapsto ghg^{-1}$ is a left action of G on G.

Proof

$e \cdot h = ehe^{-1} = h$

$$g \circ (h \circ k) = g \circ (hkh^{-1}) = ghkh^{-1}g^{-1} = ghk(gh)^{-1}$$

□

Definition

This action of G on itself is called the conjugation action

$$\alpha : G \times G \to G, \quad (g, k) \mapsto g \cdot k = gkg^{-1}$$

The orbit of $k \in G$ under this action is called the conjugate class of k and is denoted by $\mathrm{Conj}_G(k) = \{gkg^{-1} \mid g \in G\}$. To stabilize of k is called the centralizer, and is denoted by $G_k = \{g \in G, gkg^{-1} = k\} \leq G \iff gk = kg$.

Example

Consider S_6 and let $\sigma = (1\ 4\ 5)(2\ 3)$.
Let us compute the conjugate $\sigma\tau\sigma^{-1}$ for some $\tau \in S_6$.
Recall that conjugation acts by relabeling: for any i, $\sigma(i)$ replaces i in the cycle notation.
For example, conjugating $(1\ 4\ 5)(2\ 3)$ by σ gives:

$$\sigma(1\ 4\ 5)(2\ 3)\sigma^{-1} = (\sigma(1)\ \sigma(4)\ \sigma(5))(\sigma(2)\ \sigma(3))$$

If we take $\tau = (1\ 4\ 5)(2\ 3)$, then:

$$\sigma\tau\sigma^{-1} = (\sigma(1)\ \sigma(4)\ \sigma(5))(\sigma(2)\ \sigma(3))$$

This shows that conjugation in S_n permutes the labels in the cycles according to σ.

Note: The cycle type of permutation Π is the list $(m_n, \ldots, m_1)$ when m_i = number of cycles of length i in Π.
Cyclic type of $(1\ 4\ 5)(2\ 3)$ is $(0, 0, 0, 1, 1, 1)$, meaning there are 1 cycles of length 3 and 1 cycle of length 2.
$(1\ 2\ 3)(4\ 5)(6)$ has the same cycle type.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 2 & 3 & 6 \end{pmatrix}$$

$$\mathrm{Conj}(\Pi) = \{\text{all elements of } S_n \text{ with the same cyclic type as } \Pi\}$$

Note

Conjugation action on G gives action on 2^G.
$N_G(S), S \leq G$ is the stabilizes of S in this action.

$GL_n(\mathbb{R})$ acts on $GL_n(\mathbb{R})$ by conjugation on $M_n(\mathbb{R})$ by $A \cdot B = ABA^{-1}$.
Orbits are called similarity classes.

A matrix is diagonal if and only if it is similarity class contains a diagonal matrix.
Jordan normal form determines the conjugate class of any matrix.

$|\mathrm{Conj}_G(k)| = 1 \iff gkg^{-1} = k$ for all $g \in G \iff g \in Z(G)$.

Theorem Class Equation

Let T be a set of representatives for the conjugation action not contained in $Z(G)$.
Then

$$|G| = |Z(G)| + \sum_{t \in T} |\mathrm{Conj}_G(t)|$$

Proof

$T \cup Z(G)$ is a set of representatives for the conjugation action so $|G| = \sum_{t \in T \cup Z(G)} |\mathrm{Conj}_G(t)|$.

□

Suppose $p \mid |G|, |G| < +\infty$. Is there an element of G of order p?

Lagrange's theorem: if $g \in G$, then $|g| \mid |G|$.

Theorem Cauchy's Theorem

If $|G| < +\infty$ and $p \mid |G|$, when p is prime, then G has an element of order p.

Proof

Let $|G| = pm$. Proof by induction on m.
Base case: $n = 1$, G is cyclic, so there is an element of order p.
Suppose theorem holds for order pk for $1 \leq k < m$.

Case 1: If G is cyclic, true by previous calculation for cyclic groups.

Case 2: If G is Abelian but not cyclic, choose $a \in G$, $a \neq e$. Since G is not cyclic, $|a| < |G|$.
If $p \mid |a|$, then $a^{\frac{|a|}{p}}$ is an element of order p.
If $p \nmid |a|$, let $\langle a \rangle =: N \trianglelefteq G$, since G is abelian.

Then

$$p \mid \frac{|G|}{|N|} = |G/N|$$

Since $|G/N| < |G|$ (because $a \neq e$, so $|N| > 1$), there is an element bN in G/N of order p by induction.
$q : G \to G/N$. $bN = q(N)$. So $p = |bN| \mid |b|$, and $b^{\frac{|b|}{p}}$ has order p.

Case 3: G is not abelian. Let T be a set of representatives for the conjugate class of G not contained in $Z(G)$.
If $p \nmid |\text{Conj}(g)|$ for some $g \in T$, then $p \mid |C_G(g)| = \frac{|G|}{|\text{Conj}_G(g)|}$, and since $g \notin Z(G)$, $|\text{Conj}_G(g)| > 1 \implies |C_G(g)| < |G|$.
By induction, $C_G(g)$ has an element of order p.

□

xiii. Classification of groups

Proposition

If G is a group of order 6, then G is isomorphic to either $\mathbb{Z}_6$ or $D_6 \cong S_3$.

Order	**Groups**
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6, D_6$
7	$\mathbb{Z}_7$
$\vdots$	$\vdots$

Proof

There is an element of order 2 and an element of order 3.
$|\langle a\rangle \cap \langle b\rangle| = 1$ by Lagrange's theorem,

$$|\langle a\rangle\langle b\rangle| = \frac{|\langle a\rangle| \cdot |\langle b\rangle|}{|\langle a\rangle \cap \langle b\rangle|} = 6$$

So every element of G can be written uniquely as $a^i b^j$ for $0 \le i \le 1$ and $0 \le j \le 2$, $a^{-1} = a$, $aba = ?$.
If $aba = 6 \implies ab = ba$ so a, b commute, $\implies G$ abelian

$$ab$$

$$(ab)^2 = a^2b^2 = b^2 \qquad (ab)^3 = a^3b^3 = a$$

$$(ab)^4 = a^4b^4 = b \qquad (ab)^5 = ab^2$$

$$(ab)^6 = a^6b^6 = e$$

Now $[G : \langle b\rangle] = \frac{6}{3} = 2$, $\langle b\rangle \trianglelefteq G \implies aba = b^i$.

(**Note**: if $aba = e \implies b = e$)
$i = 1$ abelian
$i = 2$ if $aba = b^2$, then $ab = b^{-1}a$. This is the same relation in get in the dihedral group $rs = s^{-1}r$.
So multiplication table for G is the same e multi table for $D_6 \implies G \cong D_6$.

□

Example

$\mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_6$

$$(1,1) \to (2,2) = (0,2) \to (1,0) \to (0,1) \to (1,2) \to (0,0)$$

$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ is the cyclic group of order m.

Lemma

If $\gcd(m,n) = 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

Proof

$k(1,1) = (0,0)$ in $\mathbb{Z}_m \times \mathbb{Z}_n \iff m \mid k, n \mid k \iff mn \mid k$.

□

So, $|(1,1)| = mn$.

Theorem (Classification of finite abelian groups)

If G is a finite abelian group, then

$$G_p \cong \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \cdots \times \mathbb{Z}_{p^{a_k}}$$

where $a_1 \leq a_2 \leq \cdots \leq a_k$ prime powers.
Furthermore, if $G \cong \mathbb{Z}_{b_1} \times \mathbb{Z}_{b_2} \times \cdots \times \mathbb{Z}_{b_l}$, then $k = l$ and $a_i = b_i$ for all i.

Example

- $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$
- $\mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_9 \ncong \mathbb{Z}_{27} \times \mathbb{Z}_7 \cong \mathbb{Z}_{27\times 7}$

xiv. Sylow's Theorems

Definition

An automorphism of a group G is an isomorphism $G \to G$.

Lemma

If $g \in G$, then $\phi : G \to G \cdot h \mapsto ghg^{-1}$ is an automorphism.

Proof

$\phi(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = \phi(h)\phi(k)$.

□

Corollary

If $H \leq G$ then $gHg^{-1} \leq G$ for all $g \in G$. (and $|gHg^{-1}| = |H|$)

Definition

Let p be a prime: A p-group is a group of order p^k for some $k \geq 1$.
A p-subgroup of G is a subgroup which is a p-group.

Proposition

If $|G| = p^k m$ where $p \mid m$ then by Lagrange's theorem, a p-subgroup of G has order p^l where $1 \leq l \leq k$.
A Sylow p-subgroup of G is a subgroup $H \leq G$ with order p^k.
We let $\text{Sylow}_p(G)$ denote the set of sylow p-subgroups of G.

$$n_p(G) = |\text{Sylow}_p(G)|$$

Theorem (Sylow Theorems)

Let G be a finite group, $|G| = p^k m$ where p is prime, $k \geq 1$, and $p \nmid m$. Then

(1) $\text{Sylow}_p(G) \neq \emptyset$. i.e., G has a Sylow p-subgroup.

(2) If Q is a p-subgroup and $P \in \text{Sylow}_p(G)$, then there is $g \in G$ s.t. $gPg^{-1} = Q$. In particular, all Sylow p subgroup on conjugate to each other.

(3) $n_p(G) = [G : N_G(P)]$ for any $P \in \text{Sylow}_p(G)$. In particular, $n_p(G) \mid |G|$ Also $n_p \equiv 1 \pmod{p}$.

Corollary

If $np = 1$ then there is a unique Sylow p-subgroup, and it is normal.

Proof

If $P \in \text{Sylow}_p(G)$, then $gPg^{-1} \in \text{Sylow}_p(G)$.
$np = 1 \implies gPg^{-1} = P$ for all $g \in G$.

$\square$

Example

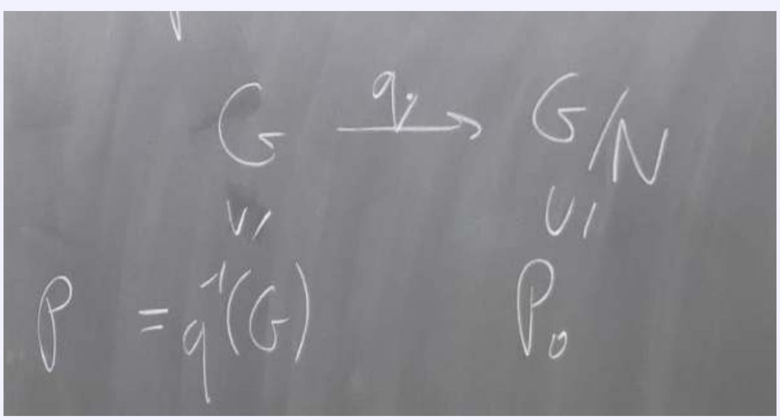
Applying the Sylow Theorems
Suppose $|G| = pq$ p, q are primes, $p < q$.
Let Q be a Sylow q-subgroup. Then $n_q(G) \mid p$ but $n_q(G) \equiv 1 \pmod q$, so $n_q(G) = 1 + kq$ for some $k \geq 0$.
Since $1 + kq \nmid p$ for $k \geq 1, n_q = 1$.
So Q is normal (since $gQ^{-1}g$ is a Sylow q-subgroup, $gQg^{-1} = Q$).

Proof

Sylow's Theorems Part 1:

Proof by induction on $|G|$.
Base case: $|G| = 1$. Trivially true, suppose that the Sylow theorem (1).
For all groups of order less than $|G|$, let $|G| = p^k m$.

Case 1: $p \mid |Z(G)|$
By Cauchy's theorem, $Z(G)$ contains an element a of order p, such that $N = \langle a \rangle$. Since $N \leq Z(G)$, $N \leq G$. $|G/N| = p^{k-1}m$.
By induction, G/N has a subgroup P_0 of order P^{k-1}.



P is a subgroup of G that contains N. $P/N \cong P_0$. $p^{k-1} = |P_0| = \frac{|P|}{|N|}$.

So $|P| = p^k \implies P$ is a Sylow p-subgroup.

Case 2: $p \nmid |Z(G)|$
Let T be a set of representations for any classes of G not contained in $Z(G)$.
As in the proof of Cauchy's theorem, since

$$|G| = |Z(G)| + \sum_{C \in T} |\text{Conj}(t)| \text{ and } p \nmid |Z(G)|$$

Then is some $t \in T$ s.t. $p \nmid |\text{Conj}(t)|$.
Since $|\text{Conj}(t)| = \frac{|G|}{|C_G(t)|}$, we have

$$p^k \mid |C_G(t)|$$

Since $t \notin Z(G)$, $C_G(t) \neq G$.
So by induction, $C_G(t)$ has a Sylow p-subgroup P.

$$P \leq C_G(t) \leq G \implies P \leq G$$

Since $|P| = p^k$, P is a Sylow p-subgroup of G.

□

Lemma

Suppose $P \in \text{Sylow}_p(G)$, Q p-subgroup of G. Then $Q \cap N_G(P) = P \cap Q$.

Proof

We know $P \leq N_G(P)$, so $Q \cap P \leq Q \cap N_G(P)$.
Let $H = Q \cap N_G(P)$. Since $H \leq Q$, $|Q| \leq p^l$ for some l.
So H is a p-subgroup. $H \leq N_G(P)$, from 2nd isomorphism theorem, $HP \leq G$.
Also,

$$|HP| = \frac{|P| \cdot |H|}{|P \cap H|}$$

power of p.
So $|HP| = p^{l'}$ for some l'. But $HP \geq P \implies HP \cdot P$ since P has maximal order for a p-group.
So $H \subseteq HP = P$. $\implies Q \cap N_G(P) = P \cap Q$.

□

Proof

Sylow's Theorems Part 2/3:

Let P be some Sylow p-subgroup of G. Let $\mathscr{O}_p = \{gPg^{-1} : g \in G\}$ be the orbit of P under

the conjugation action of G on 2^G.
Suppose Q is a p-subgroup Q acts by conjugation on $\mathscr{O}_p$.
Let T be a set of representatives for this action, so

$$|\mathscr{O}_p| = \sum_{p' \in T} |Q \cdot p'|$$
$$Q \cdot p' = \{gPg^{-1} : q \in Q\} \quad Q \text{ is orbit of } p'$$

Stabilize of p' is

$$\begin{aligned} C_Q(p') &= \{q \in Q : qP'q^{-1} = P'\} \\ &= Q \cap N_G(P') \\ &= Q \cap P' \end{aligned}$$

Because all elements of $\mathscr{O}_p$ a Sylow p-subgroup.
So $|Q \cdot p'| = \frac{|Q|}{|Q \cap P'|} = [Q : Q \cap P']$.
Notice that $Q \cap P'$ is a p-subgroup if $Q \nsubseteq P'$, then $|Q \cap P'| < |Q|$.
$\implies p \mid [Q : Q \cap P']$.

Claim 1: $|\mathscr{O}_p| \equiv 1 \mod p$

Proof

Take $Q = P$, choose T s.t. $P \in T$.
$P \cap P = P \implies |Q \cdot P| = 1$.
For $P' \in T \backslash \{P\}, P \notin P' \implies p | [P : P \cap P']$.
So,

$$\begin{aligned} |\mathscr{O}_p| &= \sum_{p' \in T} [Q \cdot P'] \\ &= 1 + \sum_{p' \in T \backslash \{P\}} [Q \cdot P'] \\ &\equiv 1 \mod p \end{aligned}$$

□

Claim 2: Every p-subgroup Q is contained in P' for some $P' \in \mathscr{O}_p$.

Proof

Suppose Q is a p-subgroup, s.t. $Q \nsubseteq P'$ for all $P \ \in \mathscr{O}_p$.
Then,

$$p \mid |Q \cdot P'| \implies p \mid \sum_{p' \in T} |Q \cdot P'| = |\mathscr{O}_p|$$

This contradicting claim 1, then must be some $P' \in \mathscr{O}_p$ such that $\underline{Q \subseteq P'}$.

□

Sylow's Theorem Part 2:
If p' is a Sylow p-subgroup, then by (2) there is $P'' \in \mathscr{O}_p$ such that, $P' \subseteq P''$. Since $|P'| = |P''|$, $P' = P''$. So, $o' \in \mathscr{O}_p$. We conclude that $\mathscr{O}_p = \text{Sylow}_p(G)$.

So $n_p(G) = |\mathscr{O}_p| \equiv 1 \mod p$ by Claim 1.

$$\begin{aligned} n_p(G) &= \frac{|G|}{|\text{stabilizer of } P}| \\ &= \frac{|G|}{|N_G(P)|} \\ &= [G : N_G(P)] \end{aligned}$$

because $N_G(P) = \{g : gPg^{-1} = P\}$ is the stabilizer of P.

□

Note

Classification of finite abelian groups:

- Statement only (exam)
- Proof see videos (won't be on exam)

II. Ring Theory

i. Rings

Definition

A ring is a tuple $(R, +, \cdot)$ where

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

(2) $\cdot$ is an associative binary operation on R.

$$\text{s.t.} \begin{cases} a \cdot (b + c) = a \cdot b + a \cdot c \\ (b + c) \cdot a = b \cdot a + c \cdot a \quad \text{for all } a, b, c \in R \end{cases}$$

A ring is commutative if $\cdot$ is commutative (i.e., $a \cdot b = b \cdot a$ for all $a, b \in R$).
In a ring, O is usually and for the additive identity (i.e., the identity in $(R, +)$).
x is used for the inverse of x in $(R, +)$, i.e., $x + (-x) = O$.
Denote $a \cdot b$ as ab for all $a, b \in R$.

A multiplicative identity in a ring R is an element $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.
We know from before that a multiplicative identity is unique if it exists. Usually, denote it by 1 (or $\mathbb{1}$ or I) if it exists.

Definition

A unital ring is a ring with a multiplicative identity.

Note

In this course, ring $\equiv$ unital ring.
Ring (with no multiplicative identity) is non-unital ring.

Example

(1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ commutative rings

$\mathbb{N}$ is not a ring no addition inverse

(2) $M_n(\mathbb{R})$ non-commutative ring, R any ring $M_n(R)$ $n \times n$ matrices over R.

(3) $\mathbb{Z}_n\mathbb{Z}$ commutative ring.

(4) $(M_n, +, \odot)$, $A \odot B = \frac{AB+BA}{2}$, (From hmw, not associative). It's not a ring. (It called Jordan algebra)

(5) $Fun(X, R)$, X set, R ring, $(+, \cdot)$ point wise operations.

- $(f+g)(x) = f(x) + g(x)$
- $(f \cdot g)(x) = f(x) \cdot g(x)$

This is a ring.

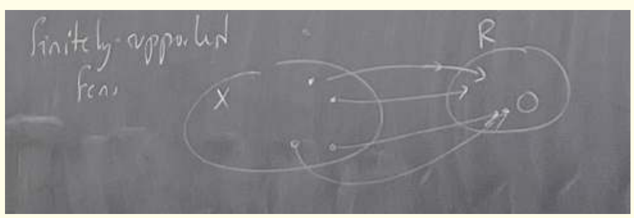
Note

- Commutative $\iff$ R is commutative.
- Identity: $x \to 1_R$ (constant function).

(6) Non-unital ring: $Fun(X, R) = \{f : x \to R | f^{-1}(R \backslash \{0\}) \text{ is finite}\}$.

Note

This is a non-unital ring, since $f(x) = 0$ for all $x \in X$ does not have a multiplicative identity.



If X is infinite, $x \mapsto 1 \notin Fun_{\text{finite}}(X, R)$.

1. Basic properties of rings

Proposition

Let R be a ring,

(1) $0 \cdot x = x \cdot 0 = 0$ for all $x \in R$.

Proof

$0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x = 0$ and $x \cdot 0 = x \cdot (0+0)$

$\square$

(2) $(-a) \cdot (b) = a \cdot (-b) = -ab$

Proof

$0 = 0 \cdot \underset{\leq 0}{b} = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$
so $(-a) \cdot b = -ab$.

$\square$

(3) $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-a \cdot b)$

(4) $-x = (-1) \cdot x$ for all $x \in R$.

Proof

$(-1) \cdot x = -(1 \cdot x) = -x$.

$\square$

Lemma

If $1 = 0$, then $R = \{0\}$

Proof

If $x \in R$ then $x = 1 \cdot x = 0 \cdot x = 0$.

$\square$

Definition

Let R be a ring, a subset $S \subseteq R$ is a subring if

(1) S is subgroup of $(R, +)$

(2) if $a, b \in S$, then $a \cdot b \in S$.

(3) $1 \in S$.

If just (1) and (2) hold, then S is a non-unital subring.

Example

The center of a ring R is

$$Z(R) = \{x \in R \mid xy = yx \text{ for all } y \in R\}$$

Homework: Prove that $Z(R)$ is a subring of R.

Example

$Z(M_n(\mathbb{C})) = \mathbb{C} \cdot \mathbb{1} \cong \mathbb{C}$.

2. Polynomial rings

Definition

If R is a ring, then

$$R[x] = \{(a_i)_{i=0}^{\infty} \in R^{\infty} \mid \text{ there is some } k \geq 0 \text{ s.t. } a_i = 0 \text{ for } i \geq k\}$$

If $(a_i)_{i=0}^{\infty} \in R[x]$ with $a_i = 0$ for $i \geq k$, we write $(a_i)_{i=0}^{\infty} = \sum_{i=0}^{k} a_i x^i$.

Example

$\mathbb{Z}[x]$,

- $1 + 2x + 3x^2 + 4x^3 + 0 \cdot x^4 \in \mathbb{Z}[x]$.
- $1 + x + x^2 + x^3 + \cdots \notin \mathbb{Z}[x]$ (infinite sum).

Note

- Addition: $(a_i)_{i=0}^{\infty} + (b_i)_{i=0}^{\infty} = (a_i + b_i)_{i=0}^{\infty}$.
- Multiplication: $(a_i)_{i=0}^{\infty} \cdot (b_j)_{j=0}^{\infty} = (c_k)_{k=0}^{\infty}$, where

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

Proposition

$(R[x], +, \cdot)$ is a ring with identity $1 = 1 \cdot x^0$.
If R is a commutative then $R[x]$ is commutative.

Definition

Terminology

$$\deg(\sum_{i=0}^{k} a_i x^i) = \max\{0 \le i \le k \mid a_i \neq 0\} \cup \{-\infty\}$$

Example

$\deg(0) = -\infty, \deg(7) = 0, \deg(1 + 7x^{10}) = 10$

a_i is the coefficient of x^i in $\sum a_i x^i$.

Definition

Monomial: poly of the form $x^i, i \ge 0$.

Term: poly of the form $ax^i, i \ge 0, a \in R$.

$a_i x^i, i = 0, 1, \ldots, k$ are the term of $\sum_{i=0}^{k} a_i x^i$.

If

$$k = \deg(\sum_{i=0}^{k} a_i x^i)$$

then $a_k x^k$ is the leading term and a_k is the leading coefficient of $\sum_{i=0}^{k} a_i x^i$.

Lemma

The constant polynomials $\{a \cdot x^0 : a \in \mathbb{R}\}$ form a subring of $R[x]$.

Definition

Group rings If R is a ring, G is a group
Let

$$RG = \{(a_g)g \mid g \in G, a_g \in R, \forall g \in G \text{ and } |\{g \in G : a_g \neq 0\}| < \infty\}$$

While $(a_g)_{g\in G}$ as $\sum_{g\in G} a_g g$ (drop terms that a zero)

Example

$D_6 = G$, $2 \cdot e + 7 \cdot s - 6sr = 2e + 7s - 6sr + 0s^2 - 0r + 0s^2 r$

Example

$G = \mathbb{Z} = R$

- $2 \cdot \underline{1} + 7 \cdot \underline{2} - 6 \cdot \underline{3} \in \mathbb{Z}[\mathbb{Z}]$
- $1 \cdot \underline{1} + 1 \cdot \underline{2} + 1 \cdot \underline{3} + \ldots \notin \mathbb{Z}[\mathbb{Z}]$ (infinite sum).

Proposition

$$\sum a_g g + \sum b_g g = \sum (a_g + b_g) g, \forall a_g, b_g \in R$$

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{g\in G} b_g g\right) = \sum_{g,h} a_g b_h (gh) = \sum_{k\in G} \left(\sum_{g\in G} a_g b_{g^{-1}k}\right) k$$

Example

$G = D_6, (2 \cdot e + 7 \cdot s) + (2s - 3r) = 2e + 9s - 3r$
$(2e + 7s) \cdot (2s - 3r) = 4s + 14s^2 - 6r - 21sr.$

Example

$\mathbb{Z}[\mathbb{Z}]$

$$(3 \cdot \underline{1} + 4 \cdot \underline{2}) - (7 \cdot \underline{2} + 3 \cdot \underline{-8}) = 3 \cdot \underline{1} - 3 \cdot \underline{2} - 3 \cdot \underline{-8}$$
$$(3 \cdot \underline{1} + 4 \cdot \underline{2}) \cdot (7 \cdot \underline{2} + 3 \cdot \underline{-8}) = 21 \cdot \underline{3} + 28 \cdot \underline{4} + 9 \cdot \underline{-7} + 12 \cdot \underline{-6}$$
$$(3 \cdot x^1 + 4 \cdot x^2) \cdot (7 \cdot x^2 + 3 \cdot x^{-8})$$

Proposition

$(RG, +, \cdot)$ is a ring with identity $1 = e$

Proof

See videos.

$\square$

Note

G group $\to RG$
R ring (e.g. $R = \mathbb{Z} \cdot \mathbb{Q}$ (e.g. $\mathbb{Z}G$))
$R \to (R, +) =: R^+$ (e.g. $\mathbb{Z}^+$, $\mathbb{Q}^+$)
$0 \times x = 1$ $(R \backslash \{0\}, \cdot)$
$\mathbb{Z} \backslash \{0\}$

Definition

An element of a ring R is called a unit if it is invertible with respect to the multiplication. The set of units is denoted by $R^\times$.

Example

- $\mathbb{Q}^\times = \mathbb{Q} \backslash \{0\}$,
- $\mathbb{Z}^\times = \{\pm 1\}$,

$R^\times$ is always a group.

Definition

Let R and S be rings. A function $\phi : R \to S$ is a ring homomorphism if

(1) $\phi(a + b) = \phi(a) + \phi(b)$

(ϕ is a homomorphism for $(R, +)$ and $(S, +)$),

(2) $\phi(ab) = \phi(a)\phi(b)$

(3) $\phi(1_R) = 1_S$

If only (1) and (2) hold, say that ϕ is a non-unital ring

Example

(1) If R is any ring, then $R \to \{0\}$, $r \mapsto 0$ is a ring homomorphism.

zero homomorphism

(2) If R, S on rings, then $R \to S : r \mapsto 0_S$. This is a non-unital ring homomorphism, but not a homomorphism unless $S = \{0\}$.

Not necessarily the case that then is a ring homomorphism between two rings R and S.

(3) Let R be a ring. If $p = \sum_{i=0}^{k} a_i x^i \in R[x]$, and $x \in R$, let $p(\alpha) = \sum_{i=0}^{k} a_i \alpha^i \in R$.

$p(\alpha)$ is the evaluation of p at α.

Lemma

Let R be commutative, then

$$ev_\alpha : R[x] \to R, \quad p \mapsto p(\alpha)$$

is a ring homomorphism.

Proof

We want to show that if $p \cdot q \in R[x]$,

$$\begin{aligned}(p+q)(\alpha) &= p(\alpha) + q(\alpha) \\ (pq)(\alpha) &= p(\alpha)q(\alpha) \\ 1(\alpha) &= 1_R(1 \cdot (x) = 1 \cdot \alpha^0 = 1)\end{aligned}$$

Suppose $p = \sum_{i=0}^k a_i x^i$ and $q = \sum_{j=0}^l b_j x^j$.
By taking $a_i = 0$ for $i \geq k$, $b_j = 0$ for $j \geq l$, can assume WLOG that $k = l$.
Then

$$\begin{aligned}(p+q)(\alpha) &= \left(\sum_{i=0}^k (a_i + b_i)\, x^i\right)(\alpha) \\ &= \sum_{i=0}^k (a_i + b_i)\, \alpha^i \\ &= \sum_{i=0}^k a_i \alpha^i + \sum_{i=0}^k b_i \alpha^i \\ &= p\,(\alpha) + q\,(\alpha)\end{aligned}$$

For the second part, we have

$$\begin{aligned}(pq)(\alpha) &= \left(\sum_{m=0}^{k+l} \left(\sum_{k=0}^m a_k b_{m-k}\right) x^m\right)(\alpha) \\ &= \sum_{m=0}^{k+l} \left(\sum_{k=0}^m a_k b_{m-k}\right) \alpha^m \\ &= \left(\sum_{i=0}^k a_i \alpha^i\right)\left(\sum_{j=0}^l b_j \alpha^j\right) \\ &= p\,(\alpha)\, q\,(\alpha)\end{aligned}$$

□

Proposition

If $\phi : G \to H$ is a group homomorphism, R is a ring, then there is a ring homomorphism

$$RG \to RH : \sum_{g \in G} a_g g \mapsto \sum_{h \in H} \left(\sum_{g \in G, \phi(g) = h} a_g \right) h$$

$$\phi\left(\sum a_g g\right) = \sum_{g \in G} a_g \phi(g)$$

(There are finitely many terms in not zero, so the sum is finite.)

Definition

If R is a ring, and $n \geq 2$, then <u>multivariable polynomial (over R)</u> is a function

$$R[x_1, x_2, \ldots, x_n] := R[x_1, x_2, \ldots, x_{n-1}][x_n]$$

Example

$R[x, y] = R[x][y]$
Elements of this ring look like $(1 + x^2)y^0 + (1 - x^2)y + x^{100}y^2$

Note

If $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in R^n$, then

$$\begin{aligned} ev_\alpha : & R[x_1, x_2, \ldots, x_n] \to R \\ & R[x_1, x_2, \ldots, x_{n-1}][x_n] \xrightarrow{ev_{\alpha n}} R[x_1, x_2, \ldots, x_{n-1}] \\ & \xrightarrow{ev_{\alpha_{n-1}}} \cdots \xrightarrow{ev_{\alpha_1}} R \end{aligned}$$

is defined by setting $ev_\alpha(p) = ev_{\alpha_1} \cdot ev_{\alpha_2} \cdots ev_{\alpha_n}(p)$.

Example

$p = (1 + 2x) - (7 + x^2)y^3 \in Z[x, y]$, what is $ev_{(1,2)}(p)$?

$$ev_2(p) = 1 + 2x - (7 + x^2) \cdot 2^3 = -55 + 2x - 8x^2$$

$$ev_1(ev_2(p)) = -55 + 2 - 8 = -61$$

Definition

A bijective ring homomorphism is called an isomorphism.

Lemma

If $\phi : R \to S$ is a ring isomorphism, then $\phi^{-1} : S \to R$ is also a ring isomorphism
i.e. $\phi : R \to S$ is a ring isomorphism if and only if there is a ring homomorphism $\phi : R \to S$ s.t. $\phi \cdot \psi = id$, $\psi \cdot \phi = id$.

Example

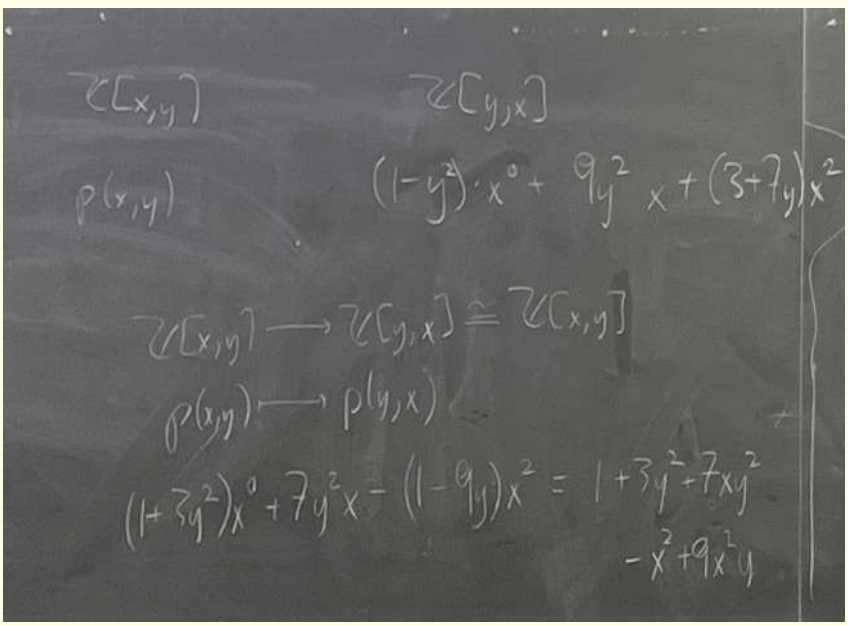
(1) $R[x] \cong R[y]$, doesn't matter what variable we use in polynomial rings.

(2) If we have a permutation $\sigma \in S_n$, then

$$R[x_1, x_2, \dots, x_n] \cong R[x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}]$$

Example

Typically elements of $\mathbb{Z}[x, y](1 + 3x^2)y^0 + 7x^2y - (1 - 9x)y^2$
If $\sigma \in S_n$, then $R[x_1, \dots, x_n] = R[x_{\sigma(1)}, \dots, x_{\sigma(n)}]$.



Proposition

Properties of Ring Homomorphisms

Let $\phi : R \to S$ be a ring homomorphism.

(1) $\phi(a^n) = \phi(a)^n$ for all $n \geq 0$

Proof

By induction.

□

(2) If $u \in R^\times$m then $\phi(u) \in S^\times$ and $\phi(u^{-1}) = \phi(u)^{-1}$.

Proof

$1_S = \phi(1_R) = \phi(u \cdot u^{-1}) = \phi(u) \cdot \phi(u^{-1})$,
so $1_S = \phi(u) \cdot \phi(u^{-1})$ implies $\phi(u)^{-1} = \phi(u^{-1})$.

□

(3) $Im\phi$ is a subring of S.

Note

$\phi : (R, +) \to (S, +)$ is a group homomorphism, $Im\phi$ and $\ker \phi$ denote image and kernel of ϕ respectively.

(4) If $a \in R, b \in \ker \phi$, then $ab, ba \in \ker \phi$.

Proof

$\phi(a \cdot b) = \phi(a) \cdot \phi(b) = \phi(a) \cdot 0_S = 0_S$ and similarly for ba.

□

Note

If $S \leq R$, $x \in R$, then $xS = \{xs \mid s \in S\}$.
Property (4) can be rewritten ($x \neq S$) to say that $x \ker \phi \subseteq \ker \phi$ for all $x \in R$.
(4) $\implies$ $\ker \phi$ is a non-unital subring of R.

ii. Ideals

Definition

A subset $I \subseteq R$ is an ideal if

1. I is a subring of $(R, +)$, and
2. $xI, Ix \subseteq I$ for all $x \in R$.

Example

(1) If $\phi : R \to S$ is a ring homomorphism, then $\ker \phi$ is an ideal of R.

(2) $I = \{0\}$ and $I = R$ are ideals since $r \cdot 1 \in I, \forall r \in R$.
Zero ideal, **Note** $I = R \iff 1 \in I$.

(3) Every ideal is a non-unital subring, **converse is not true**.
$R[x]$ has R as a subring, $R \cdot x^0$ constant polynomials, not an ideal $x \cdot rx^0 = rx \notin R[x]$.

(4) $n\mathbb{Z} = \{ka : k \in \mathbb{Z}\}$ is an ideal in $\mathbb{Z}$.

Lemma

If R is a common ring and $x \in R$, then $xR = Rx$ is an ideal in R.

Proof

$0 = x \cdot 0 \in xR$. If $xa, xb \in xR$,
then $xa + xb = xR$, $-xa = x \cdot (-a) \in xR$.
So xR is a subring of R.

□

If $xa \in xR, y \in R$ then $y \cdot xa = x(ay) \in xR$, so xR is an ideal in R.
An ideal of the form xR is called a principal ideal.

Proposition

Properties of Ideals

Let I be an ideal in R.

1. If I, J are ideals in a ring R, then $I + J = \{x + y : x \in I, y \in J\}$ is an ideal of R.
2. If F is a family of ideals then $\bigcap_{I \in F} I$ is an ideal of R.
3. If $\phi : R \to S$ is a surjective homomorphism, and I is an ideal of R, then $\phi(I)$ is an ideal of S.

Proof

We proof that I and J is a subgroup of $(R, 1)$, $(I \subseteq N_{(R,1)}(J))$.
If $x \in I, y \in J, r \in R$, then $r(x + y) = rx + ry \in I + J$ because $rx \in I, ry \in J$.
Similarly, $(x + y)r = xr + gr \in I + J$. So $I + J$ is an ideal of R.
$(2) - (4)$ Hwk.

□

Definition

If R is a ring and $S \subseteq R$, then the ideal generated by S is

$$(S) := \bigcap_{S \subseteq I \subseteq R, I \text{ ideal}} I$$

This is an ideal by part (2) of the properties of ideals. Also $S \subseteq (S)$.

Lemma

If K is a commutation ring, and $S = \{f_1, f_2, \ldots, f_n\}$then

$$(S) = \{F_1 R + F_2 R + \ldots + F_n R : F_i \in R\}$$

Lemma

If R commutative ring, $S = \{f_1, \dots, f_n\} \subseteq R$
Then $(S) = f_1 R + \cdots + f_n R$ is the ideal generated by S. $I + J = \{a + b \mid a \in I, b \in J\}$ is an ideal.

Proof

$I = f_1 R + \cdots + f_n R$. We know that I is an ideal and $f_1, \dots, f_n \in I$, so $(S) \subseteq I$.
Since $S \subseteq (S), f_1, \dots, f_n \in (S)$.
If $f_1 r_1 + \cdots + f_n r_n \in (S)$ for some $r_1, \dots, r_n \in R$, then $f_i r_i \in (S)$ so $f_1 r_1 + \cdots + f_n r_n \in (S)$.
We conclude that $I \subseteq (S)$.

□

Corollary

$xR = (x)$

Example

Suppose R is commutative, $c \in R$
$f = x - c \in R[x]$ is a polynomial.
Then $(f) = R[x]f = \{g(x)(x - c) \mid g(x) \in R[x]\}$ is the ideal generated by f.
If $h(x) = g(x)(x - c)$, then $ev_c(h(x)) = g(c)(c - c) = 0$.
So $(f) = \ker(ev_c)$.

Lemma

If $h \in R[x]$, $\deg h \subseteq n$, then there are $a_0, a_1, \ldots, a_n \in R$ such that

$$h = \sum_{i=0}^{n} a_i (x-c)^i$$

where $(x-c)^0 := 1$.

Proof

Let a_n be the coefficient of x^n in h.
Then $h(x) = a_n x^n + \text{lower degree terms}$.
So, $h(x) = a_n (x-c)^n = \text{polynomial of degree } \leq n-1$.

$$a_n x^n + \text{lower degree terms}$$

So we can make an individual argument to show,

$$h - a_n(x-c)^n = \sum_{i=0}^{n-1} a_i (x-c)^i$$
$$\implies h = \sum_{i=0}^{n} a_i (x-c)^i$$

□

Corollary

$\ker(ev_c) = (x - c)$

Proof

$(x - c) \subseteq \ker(ev_c)$.
Suppose $h \in \ker(ev_c)$, we can write

$$h = \sum_{i=0}^{n} a_i (x - c)^i$$

$$\begin{aligned} ev_c(h) &= \sum_{i=1}^{n} a_i (ev_c(x - c))^i + ev_c(a_0) \\ &= a_0 \end{aligned}$$

Since $h \in \ker(ev_c)$, $a_0 = 0$, so

$$\begin{aligned} h &= \sum_{i=1}^{n} a_i (x - c)^i \\ &= (x - c) \sum_{i=1}^{n} a_i (x - c)^{i-1} \\ &\in (x - c) \end{aligned}$$

□

Example

Not all ideals are principal.
$(x, y) \subseteq \mathbb{Z}[x, y]$. Suppose $(x, y) \subseteq (f)$.
Then there is $pq \in \mathbb{Z}[x, y]$ such that

$$x = pf, \quad y = qf$$

Hmw: $f = \pm 1 \implies (f) = \mathbb{Z}[x, y]$.
Only principal ideal containing (x, y) is $\mathbb{Z}[x, y]$.

Example

$I = (2, x) \subseteq \mathbb{Z}[x]$ If $I \subseteq (f)$, then
$Z = pf$ for some $p \in \mathbb{Z}[x]$.
Hwk: $f = \{\pm 1, \pm 2\}$
Hwk: $x \notin (f)$ if $f = \pm 2$.
So only principal ideals containing I is $\mathbb{Z}[x]$.

iii. Quotient Rings

Recall

If R is a ring, $S \subseteq (R,+) =: R^k$ then

$$R^+/S = \{a + S \mid a \in R^+\}$$

Since R^+ is an abelian group, R^+/S is a group with operation $(a+S)+(b+S) = (a+b)+S$.

Theorem

Let I be an ideal in a ring R.
Theorem R/I is a ring with operations.

$$(a + I) + (b + I) = a + b + I$$
$$(a + I)(b + I) = ab + I$$

and identity: $1 + I$.
Furthermore, the quotient map, $q : R \to R/I$ is a ring homomorphism with $\ker q = I$.

Corollary

A subset $I \subseteq R$ is an ideal iff $I = \ker \phi$ for some ring homomorphism $\phi : R \to S$.

Proof

We already know that R/I is an addition group with the group operation.
To show $\cdot$ is well-defined, suppose $a_1 + I = a_2 + I$ and $b_1 + I = b_2 + I$.
Then $a_1 - a_2 \in I$ and $b_1 - b_2 \in I$. So,

$$\begin{aligned} a_1 b_1 - a_2 b_2 &= a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 \in I \\ &= a_1 \underbrace{(b_1 - b_2)}_{\in I} + b_2 \underbrace{(a_1 - a_2)}_{\in I} \in I \end{aligned}$$

Suppose $a + I, b + I, c + I \in R/I$.
Then $(a + I)(b + I) = ab + I$, and

- is associative:

$$\begin{aligned} (a+I)((b+I)(c+I)) &= (a+I)(bc+I) \\ &= abc + I \text{ as associative in } R \\ &= (ab+I)(c+I) \\ &= ((a+I)(b+I))(c+I) \end{aligned}$$

- is distributive:

$$\begin{aligned} (a+I)((b+I)+(c+I)) &= (a+I)(b+c+I) \\ &= a(b+c)+I \\ &= ab+ac+I \\ &= (ab+I)+(ac+I) \\ &= (a+I)(b+I)+(a+I)(c+I) \end{aligned}$$

  Similarly, $((b+I)+(c+I))(a+I) = (b+I)(a+I)+(c+I)(a+I)$.

- $1 + I$ is the identity:

$$\begin{aligned} (a+I)(1+I) &= (1 \cdot a) + I \\ &= a + I \\ &= (a+I)(1+I) \\ &= a + I \end{aligned}$$

So R/I is a ring. We also know that q is a group homomorphism.
$R^k \to (R/I, +)$ with $\ker q = I$.
Since $q(ab) = ab + I = (a+I)(b+I) = q(a)q(b)$, $q(1) = 1 + I$.
So q is a ring homomorphism with $\ker q = I$.

□

Recall

$x + I$ is an equivalence class can also denote it by $[x]$.
With the notation with $x + I = [x]$, we can write

$$[x] + [y] = [x + y]$$
$$[x][y] = [xy]$$
$$1_{R/I} = [1]$$

Example

$\mathbb{Z}/n\mathbb{Z}$ is a quotient ring.

$$[a] + [b] = [a + b]$$
$$[a][b] = [ab]$$

iv. Isomorphism Theorems for Rings

Theorem (Universal property of quotient rings)

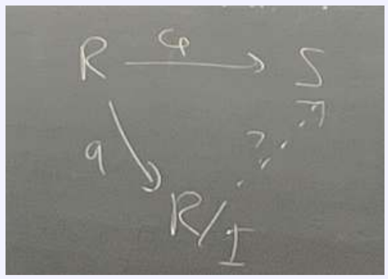
Let $\phi : R \to S$ be a ring homomorphism, I be an ideal of R, and $q \cdot R \to R/I$ be a quotient homomorphism.
Then there is a homomorphism

$$\psi : R/I \to S$$

with

$$\psi \cdot q = \phi \iff I \subseteq \ker \phi$$

If ψ exists, it is unique.



Proof

($\Rightarrow$)
If ψ exists, then $I = \ker q \subseteq \ker \psi \cdot q = \ker \phi$.
($\Leftarrow$)
If $I \subseteq \ker \phi$, then there is a unique group homomorphism ψ with $\psi \cdot q = \phi$ by the universal property of quotient groups.
If $a + I, b + I \in R/I$, then

$$\begin{aligned} \phi((a+I)(b+I)) &= \phi(q(ab)) \\ &= \phi(ab) = \phi(a)\phi(b) \\ &= \psi(a+I)\psi(b+I) \end{aligned}$$

$$\psi(1+I) = \phi(q(1)) = \phi(1) = 1_S$$

So ψ is a ring homomorphism.

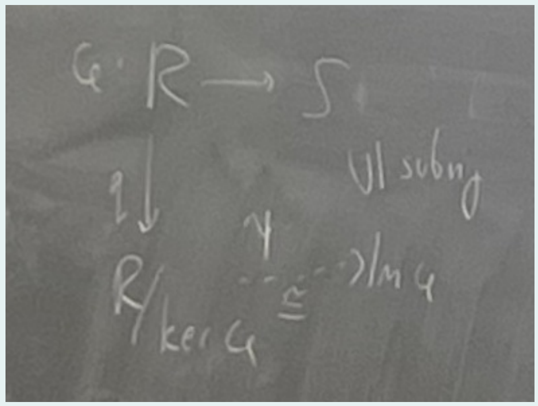
□

Corollary (1st isomorphism theorem for rings)

If $\phi : R \to S$ is a ring homomorphism, then there is an isomorphism

$$\psi : R/\ker\phi \to \operatorname{im}\phi \quad \text{s.t. } \psi \cdot q = \phi$$

where $q : R \to R/\ker\phi$ is the quotient homomorphism.



Proof

$\ker\phi \leq \ker q$, by the universal property of quotient rings, there is a unique homomorphism $\psi : R/\ker\phi \to S$ such that $\psi \cdot q = \phi$. By the 1st isomorphism theorem for groups, there is a group isomorphism

$$\psi' : R/\ker\phi \to \operatorname{im}\phi$$

s.t. $\psi \cdot q = \phi$.
So,

$$\begin{aligned}\phi(a+I) &= \psi(q(a)) = \phi(a) \\ &= \psi' \cdot q(a) = \psi'(a+I) \forall a \in R\end{aligned}$$

So $\psi = \psi'$.

□

Example

If R commutation, then

$$R[x]/(x-c) = R[x]/\ker ev_c \cong R(\text{ by first isomorphism theorem})$$

$\operatorname{im}(ev_c : R[x] \to R : x \mapsto c) = R$.

Example

$(y - x^2) \subseteq \mathbb{Z}[x, y] = \mathbb{Z}[x][y] \quad (c = x^2 \in R, R = \mathbb{Z}[x])$.
$\mathbb{Z}[x, y]/(y - x^2) \cong \mathbb{Z}[x]$.

Remark

If $I \subseteq R[x], p \in I$

$$R[x]/I, \quad \bar{x} = x + I$$

$\sum a_i x^i + I \in R[x]$, $q(\sum a_i x^i) = \sum a_i \bar{x}^i$.

$$0 = q(o) = \sum_i [b_i] \bar{x}^i := p(\bar{x})$$

Where $p = \sum b_i x^i$ $\bar{x}$ satisfies the equation $p = 0$.

Example

Let $p = x^2 + 1 \in \mathbb{R}[x]$
$\bar{x}^2 + 1 = 0$ in $\mathbb{R}[x]/(p) \implies \bar{x}^2 = -1$.
Let $q : \mathbb{R}[x] \to \mathbb{R}[x]/(p)$ be the quotient map.
Then $q(\bar{x}) = i$ in $\mathbb{R}[x]/(p)$.

Lemma

Every element of $\mathbb{R}[x]/(p)$ can be written uniquely as $a + bx + (p)$ for some $a, b \in \mathbb{R}$.

Proof

Suppose $\alpha \in \mathbb{R}[x]/(p)$, so $a = f(x) + (p)$ for some polynomial $f \in \mathbb{R}[x]$. Choose f to have minimal degree. Let $f = \sum_{i=0}^{n} a_i x^i$, where n is the degree. If $n \geq 2$, then

$$f = a_n p x^{n-2} + (p) = \alpha$$

because $a_n p x^{n-2} \in (p)$.
Since $f - a_n p x^{n-2}$ has degree $< n$,
So, $f = a + bx$

Suppose

$$\begin{aligned} a + bx + (p) &= c + dx + (p) \\ \implies (a-c) + (b-d)x &\in (p) \\ \implies (a-c) + (b-d)x g(x) p(x) &\text{ for some } g(x) \in \mathbb{R}[x] \end{aligned}$$

In $\mathbb{R}[x], \deg gp \deg g + \deg p = \deg g + 2$.
So by $gp = \deg((a-c) + (b-d)x)$, $\deg g + 2 \leq 1$.
$\implies \deg g = -\infty \implies a = c, b = d$.
So $a + bx$ is the unique representable for α.

□

Proposition

$\mathbb{R}[x]/(p) \cong \mathbb{C}$

Proof

Since $\mathbb{R}$ is a subring of $\mathbb{C}$, so $\mathbb{R}[x]$ is a subring of $\mathbb{C}[x]$.
Let $\phi : \mathbb{R}[x] \to \mathbb{C}[x]$ be the inclusion map. (a ring homomorphism)
Let $\phi : \mathbb{R}[x] \to \mathbb{C} : f \mapsto ev_{x=i}(\psi(f))$
Then $\phi(x^2+1) = i^2 + 1 = -1 + 1 = 0$.

$$(\phi(x) = ev_{x=i}(\psi(x)) = i)$$

$x^2 + 1 \in \ker\phi \implies (x^2+1) \leq \ker\phi$.
By universal property of quotient rings, there is a homomorphism

$$\tilde{\phi} : \mathbb{R}[x]/(p) \to \mathbb{C} : f + (p) \mapsto f(i)$$

$\tilde{\phi}(a + bx + (p)) = a + bi$.
Since every element of $\mathbb{R}[x]/(p)$ can be written uniquely as $a+bx+(p)$, for $a, b \in \mathbb{R}$, and every element of $\mathbb{C}$ can be written uniquely as $a+bi$ for $a, b \in \mathbb{R}$, $\tilde{\phi}$ is an isomorphism.

□

Note

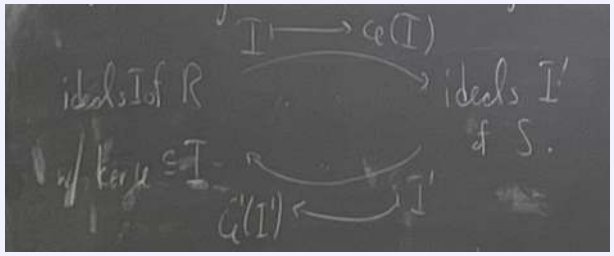
Method for constructing a ring homomorphism from old rings:

1. Start with some ring R.
2. Add some variables $x_1, x_2, \dots, x_n$
3. Choose some polynomials $p_1, p_2, \dots, p_m$ in $R[x_1, x_2, \dots, x_n]$, that we want $x_1, x_2, \dots, x_n$ to satisfy.
4. Take $S \in R[x_1, x_2, \dots, x_n]/(p_1, p_2, \dots, p_m)$. The elements $\bar{x_1}, \bar{x_2}, \dots, \bar{x_n}$ satisfy $p_1, p_2, \dots, p_m$.

We can use this method to construct $\mathbb{C}$ from $\mathbb{R}$ and many other examples.
Conclusion: S could be the zero ring.

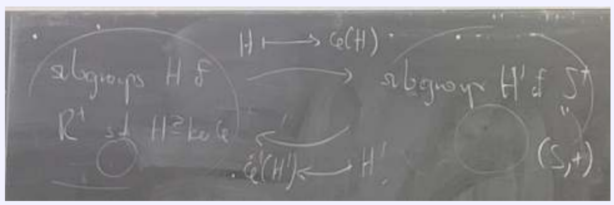
Theorem (Correspondence Theorem)

Let $\phi : R \to S$ be a surjective ring homomorphism. There is a bijection,



Proof

By Correspondence Theorem for groups, we have



From homework, if I is an ideal of R and $\ker \phi \subseteq I$ (Optional), then $\phi(I)$ is an ideal of S.
If I is an ideal of S then $\phi^{-1}(I')$ is an ideal of R containing $\ker \phi$.
So the bijection restrict to bijection on the subsets.

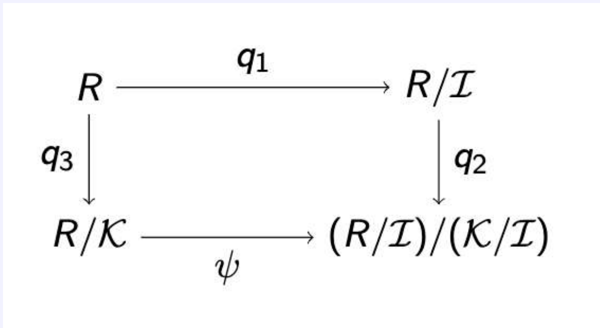
□

Theorem (3rd isomorphism theorem)

If $I \subseteq K$ an ideals in a ring R, and

$$\begin{aligned} q_1 :& R \to R/I, \\ q_2 :& R/I \to R/I \;/\; K/I \\ q_3 :& R \to R/K \end{aligned}$$

Then there is a homomorphism $\psi : R/K \to R/I \;/\; K/I$ such that



Proof

We know from the 3rd isomorphism for group that there is a group isomorphism ψ with $\psi \circ q_3 = q_2 \circ q_1$.
If $a, b \in R$, then

$$\begin{aligned} \psi([a] \cdot [b]) &= \psi(q_3(a \cdot b)) \\ &= q_2(q_1(a \cdot b)) \\ &= q_2(q_1(a) \cdot q_1(b)) \\ &= q_2(q_1(a)) \cdot q_2(q_1(b)) \\ &= \psi([a]) \cdot \psi([b]) \end{aligned}$$

Similarly, $\psi([1]) = [1]$. $R/I/\; K/I$ is a ring, so ψ is a ring homomorphism.

$\square$

Note

Second isomorphism theorem for rings: In video

v. Commutative Rings

Example

Like $\mathbb{Q}, \mathbb{Z}, \ldots$

Definition

A field is a commutative ring R in which $1 \neq 0$ and $R^\times = R \setminus \{0\}$.

Example

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

Example

$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$
$[m]$ has an inverse if and only if $\gcd(m, n) = 1$.
So

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times &= \{[m] \mid \gcd(m,n) = 1, 0 \leq m \leq n-1\} \\ &= \mathbb{Z}_n \setminus \{[0]\} \iff n \text{ is prime}\end{aligned}$$

Proposition

Let R be a commutative ring, then R is a field if and only if $1 \neq 0$, and the only ideals of R are $\{0\}$ and R.

Proof

$(\Rightarrow)$
Suppose R is a field, $I \subseteq R$ is an ideal.
Suppose $I \neq \{0\}$, so there is $r \in I$ such that $r \neq 0$.
Since $r \neq 0, r \in R^\times$, so there is $t \in R$ such that $rt = 1 \implies I = R$.
$(\Leftarrow)$
Suppose the only ideal of R on $\{0\}$ and R. (on d $1 \neq 0$)
Let $r \in R \setminus \{0\}$. Then $rR \neq \{0\}$, because $r \neq 0$, so $rR = R$. So $1 = r \cdot s$ for some $t \in R$. So $r \in R^\times$.

□

Corollary

If $\phi : \mathbb{K} \to R$ is a homomorphism, $\mathbb{K}$ is a field, and $R \neq 0$. Then ϕ is injective.

Proof

$\ker \phi \neq \mathbb{K}$ because $\phi(1) = 1 \neq 0$ because $R \neq 0$.
So $\ker \phi = \{0\}$, and ϕ is injective.

$\square$

Note

Question: When is a quotient ring R/I a field?

Example

$\mathbb{R}[x]/(x^2 + 1)$ is a field, $\mathbb{C}$.

Answer: R/I is a field if and only if $[1] \neq [0]$ and the only ideal of R/I are $\{0\}$ and R/I.

Lemma

Let I be an ideal in a commutative ring R. Then,

1. $[1] \neq [0] \iff I \neq R$.

   Pf: Exercise

2. The only ideals of R/I on $\{0\}$ and R/I if and only if the only ideals of R containing I are I and R.

   Proof

   Correspondence Theorem for rings,
   [FIXME: Diagram]

   $\square$

Definition

An ideal I of R is maximal if

1. $I \neq R$, and
2. the only ideals of R containing I are I and R.

Corollary

Let I be an ideal in a commutative ring. Then R/I is a field if and only if I is a maximal ideal of R.

Example

$(x-c) \subseteq R[x]$, $c \in R$ is a maximal ideal.
$R[x]/(x-c) \cong R$, $(x-c)$ is maximal if and only if R is a feild.
$(x) \leq \mathbb{Z}[x]$ is not maximal, $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$.

Note

Q: Is $\mathbb{R}[x]/(x^2 - c)$ a field?
$c < 0$: Yes, because $x^2 - c$ is irreducible over $\mathbb{R}$.
$c > 0$: No, because $x^2 - c$ is reducible over $\mathbb{R}$ (it factors as $(x - \sqrt{c})(x + \sqrt{c})$).
Hint: check if $x^2 - c$ is maximal ideal in $\mathbb{R}[x]$.

Definition

A partial order on a set X is a relation if

1. $x \leq x$ for all $x \in X$ (reflexive),
2. if $x \leq y$ and $y \leq x$, then $x = y$ (antisymmetric), for all $x, y \in X$,
3. if $x \leq y$ and $y \leq z$, then $x \leq z$ (transitive), for all $x, y, z \in X$.

We say $x < y$ if $x \leq y$ and $x \neq y$.
A maximal element of a subset $S \subseteq X$ is an element $x \in S$ such that if $y \geq x$ and $y \in S$ then $y = x$.
An upper bound on a subset $S \in X$ is an element $x \in X$ such that for all $y \in S$.
A maximum element of a subset S is an element of S which is an upper bound. A set has a unique maximum element if one exists maximum and maximal element do not have to exist.

Example

If X is a set, then 2^X is a partial ordered under subset inclusion.

$$X = \{1, 2\} \quad S = \{\emptyset, \{1\}, \{2\}\}$$

$\{1, 2\}$ is an upper bound not maximal element of S.

Note

The set of ideals is a ring R is partially ordered under subset inclusion.
The set of all ideals has a maximum element, R. The set of proper ideals is also partially ordered under subset inclusion. A maximal ideal is a maximal element of the set of proper ideals.

Definition

A subset S of a partially ordered set $(X, \leq)$ is a chain if for every $x, y \in S$ either $x \leq y$ or $y \leq x$.

Proposition

Every commutative ring R has a maximal ideal.

Proof

Let X be the set of proper ideals of R, and let S be a chain of ideals in X.

$$J = \bigcup_{I \in S} I$$

$1 \in J \iff 1 \in I$ for some $I \in S$, which can't happen because all ideals in S are proper.
So, $J \in X$.

□

Since any chain in X has an upper bound in X, X has a maximal element by Zorn's lemma.

Corollary

If T is a commutative ring with $1 \neq 0$, then there is a homomorphism $R \to \mathbb{K}$ where $\mathbb{K}$ is a field.

Proof

Let I be a maximal ideal in R, $\mathbb{K} = R/I$ have homomorphism $R \to R/I$.
$\mathbb{Z} \to Q : x \mapsto x$, $\mathbb{Z} \mapsto \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$, $n \mapsto [n]$

□

vi. Integral Domains

If $\mathbb{K}$ is a field, $p, q \in \mathbb{K}[x]$ then

$$\deg(pq) = \deg(p) + \deg(q)$$

This doesn't happen in $\mathbb{Z}_6[x]$:

$$(1+2x)(1+3x) = 1 + 5x + 6x^2 = 1 - x$$

The problem in $\mathbb{Z}_6[x]$ is that 2 and 3 are zero divisors, so $\mathbb{Z}_6[x]$ is not an integral domain.

Definition

Let R be a ring, and element $x \in R \backslash \{0\}$ is a zero divisor if there is $y \in R\backslash\{0\}$ such that $xy = 0$.

Example

$\mathbb{Z}_n$ if $d \mid n$ then $[d] = [\frac{n}{d}] = [n] = 0$ is a zero divisor.
$0 < d < n$, $[d] \neq 0$.
If $\gcd(d, n) = g > 1$, then

$$[d] \cdot \left[\frac{n}{g}\right] = [0]$$

Example

$\mathbb{R} \times \mathbb{R}$, $(a, 0), (0, b)$ for $a, b \neq 0$ are zero divisors.

Example

$\mathbb{Q}[x]/(x^2)$ $[x] \cdot [x] = [0]$ is a zero divisor. $[x] \neq 0$.

Example

$\mathbb{Q}[x, y]/(xy)$, $[x] \cdot [y] = [xy] = 0$, so $[x]$ and $[y]$ are zero divisors.

Definition

A commutative ring R is an integral domain (or domain) if

1. $1 \neq 0$ in R
2. R has no zero divisors.

Lemma

If n is a unit, then u is not a zero divisor.

Proof

If $u \cdot x = 0$ then $\underbrace{u^{-1}}_{=0} \cdot (u \cdot x) = 1 \cdot x = 0$.

□

Example

Any field is a integral domain

Example

$\mathbb{Z}$ is on integral domain. $\mathbb{Z}$ is a subring of $\mathbb{Q}$.
First, any subring if an integral domain is a integral domain

Example

$\mathbb{Z}/n\mathbb{Z}$ is an integral domain $\iff$ n is primes $\iff$ $\mathbb{Z}/n\mathbb{Z}$ is a field.

Proposition

If T is a finite integral domain, then R is a field.

Lemma (Cancellation Law)

If $x \in R \backslash \{0\}$ is not a zero divisor, and $xa = xb$ or $ax = bx$, then $a = b$.

Proof

If $xa = xb$ then $x(a - b) = 0$, so $a - b = 0$.

□

Proposition

If R is a field integral domain, then R is a field.

Proof

Suppose $x \in R\backslash\{0\}$. (Note: $1 \neq 0$ because R is a domain.)
Because R is finite, the sequence $x, x^2, x^3, \ldots$ must repeat.
Suppose $x^n = x^m$ for some $n < m$. Then

$$x^m(x^{n-m}) = x^m - 1$$

Suppose $x^m = 0$, then $x \cdot x^{m-1} = x \cdot 0 \implies x^{m-1} = 0$.
To interacting this, we conclude that $x = 0$, this contradicts the fact that $x \neq 0$, so $x^m \neq 0/$
So

$$x^m(x^{n-m}) = x^m - 1 \implies x^{n-m} = 1$$

If $n = m+1$, then $1 \in R^\times$. If $n > m+1$, then x^{n-m-1} is an inverse for x, so $x \in R^\times$.

□

Proposition

If R is an integral domain, then

1. $f, g \in R[x]$ then $\deg(fg) = \deg(f) + \deg(g)$.
2. $R[x]$ is an integral domain.

Proof

1. $f = a_n x^n + \cdots$ and $g = b_m x^m + \cdots$. (Leading coefficients are non-zero.)
   Then $fg = a_n b_m x^{n+m} + \cdots$.
   Since $a_n, b_m \neq 0$, $a_n b_m \neq 0$, so $\deg(fg) = n + m = \deg(f) + \deg(g)$.
   (this covers the case when $f, g \neq 0$, f or g is zero will proof as exercise.)
2. If $f, g \in R[x]\backslash\{0\}$, then $\deg(fg) = \deg(f) + \deg(g) \geq 0$, since $\deg(f), \deg(g) \geq 0$.
   So, $fg \neq 0$, also $1 \neq 0 \in R[x]$.
   So $R[x]$ is an integral domain.

□

Question: When is R/I an integral domain?

Definition

Let R be a commutative ring. An ideal $I \in R$ is a prime if $I \neq R$, and if $ab \in I$ for some $a, b \in R$, then either $a \in I$ or $b \in I$. (or both)

Example

$R = \mathbb{Z}$, $k \in m\mathbb{Z} \iff m \mid k$.
If p is prime, then $ab \in p\mathbb{Z} \iff p \mid ab \iff p \mid a$ or $p \mid b \iff a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.
$I \subseteq R$ is an ideal.

Theorem

If R is a commutative ring, then R/I is an integral domain if and only if I is a prime.

Proof

($\Rightarrow$)
Since $[1] \neq [0], I \neq R$. If $a, b \in R$ s.t. $ab \in I$, then $[ab] = 0$ in R/I.
Since R/I does not have any zero divisors, must have $[a] = 0$ or $[b] = 0$.
So either $a \in I$ or $b \in I$. So I is a prime.
($\Leftarrow$)
Suppose I is prime, since $I \subsetneq R, [1] \neq [0]$ in R/I.
Also, if $[a] \cdot [b] = [0]$ in R/I, then $ab \in I$.
Since I is prime, either $a \in I \implies [a] = [0]$ or $b \in I \implies [b] = [0]$.
So, R/I does not have zero divisors $\implies R/I$ is an integral domain.

□

Example

$\mathbb{Z}/m\mathbb{Z}$ is a domain for $m \geq 1$ if and only if m is prime.
So $m\mathbb{Z}$ is prime if and only if m is prime.

Example

If $I \subseteq R$ is maximal then R/I is a field $\Rightarrow R/I$ is a domain $\iff I$ is prime.

Example

Previously, saw $\mathbb{Q}[x, y]/(y - x^2) \cong \mathbb{Q}[x]$
$x \notin \mathbb{Q}[x]^*$, $\mathbb{Q}[x]$ is a domain but not a field.
So, $(y - x^2)$ is a prime, but not maximal.

Corollary

Let R be a commutative ring, then R is a domain $\iff$ $I = \{0\}$ is prime.

Proof

$R/\{0\} \cong R$, so R is a domain $\iff$ $\{0\}$ is prime.
If R is a domain, then whether $f(x)R[x]$ is prime is a field where f factors.

□

Lemma

If $g, h \in R[x]$ have deg ≥ 1, then $I = ghR[x]$ is not prime.

Proof

$gh \in I$, if $f \in I$ then $f = ghk$ so either

$$f = 0$$

or

$$\deg(f) = \deg(g) + \deg(h) + \deg(k) \geq \deg(g) + \deg(h) > \max(\deg(g), \deg(h))$$

So, $g, h \notin I$.

□

Example

$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ so (x^2+1) is maximal $\implies$ x^2+1 is prime.

$$(\pm i)^2 = -1, \quad (\pm[x])^2 = -1$$

$\mathbb{C}[x]/(x^2+1)$ is not a domain, since $x^2+1 = (x-i)(x+i)$ in $\mathbb{C}[x]$, so (x^2+1) is not prime by the previous lemma.

Question: Can we find a domain R containing $\mathbb{C}$ as a subring, s.t. R has $x \in R \backslash C$ such that $x^2 = -1$?

Lemma

If R is a domain and $x^2 = t^2$ in R then $x = t$ or $x = -t$ in R.

Proof

$x^2 = 1^2 \implies x^2 - t^2 = (x-t)(x+t) = 0$, so $x - t = 0$ or $x + t = 0$ in R, implies $x = t$ or $x = -t$.
Apply thing this with $t = i$ gives $x^2 = -1$ in R.

□

Lemma

Let R be an integral domain. The integral domain. The relation $\sim$ on $R \times (R \setminus \{0\})$ defined by

$$(a, b) \sim (c, d) \iff ad = bc$$

is an equivalence relation.

Proof

$a \in R, b \in R \setminus \{0\}, ab = ab$ so $(a, b) \sim (a, b)$

- If $(a, b) \sim (c, d)$ then $ad = bc$ so $bc = ad$ and $(c, d) \sim (a, b)$
- If $(a, b) \sim (c, d) \sim (e, f)$ $a, b, c \in R, b, d, f \in R \setminus \{0\}$ $ad = bc$ and $cf = dc$ si $adf = bcf = bdc$ so $af = be$ by cancellation law so $(a, b) \sim (e, f)$

□

Definition

If R is an integral domain, $a \in R, b \in R \setminus \{0\}$, set

$$\frac{a}{b} = [(a, b)] \in R \times (R \setminus \{0\}) / \sim$$

The field of fractions of R is $\left\{\frac{a}{b} \mid a \in R, b \in R \setminus \{0\}\right\}$

Theorem

Let Q be the field of fraction of R, the Q is a field with operation

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}, \quad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$$

Zero in Q is $\frac{0}{1}$ and the identity is $\frac{1}{1}$.
$-\frac{a}{b}=\frac{-a}{b}$

Proof

1. $+$ and $\cdot$ are well-defined
2. $(Q,+)$ is an abelian group
3. $\cdot$ is associative and distributive and commutative
4. $+$ is an identity for multiplication
5. Every non-zero element is invertible $(ab,ab)\sim(1,1)$ so $\frac{a}{b}\neq 0$ has an inverse

$$\frac{a}{b}\frac{b}{a}=\frac{ab}{ab}=\frac{1}{1}$$

□

Corollary

Every domain is a subring of a field

Proof

Given a domain R, let Q be the field of fraction of R, and let $R_0=\{\frac{a}{b}: a\in R\}$ Then R_0 is a subring and

$$R\to R_0 : a\mapsto\frac{a}{1} \text{ is an isomorphism}$$

□

Example

$R=\mathbb{Z}$ field and fraction in $\mathbb{Q}$.

Example

If R is a field, the field of fraction of $\mathbb{K}[x]$ is denoted by $\mathbb{K}(x)$.

vii. Chinese Remainder Theorem (In video)

viii. Principal Ideal Domain (PID)

Definition

If R is a commutative ring, we say $f \mid g$ or f divides g if there is some $h \in R$ with $g = fh$ (or $g \in fR$).

Note

1. If $x \mid y$ then $x \mid yz$ for all $z \in R$
2. $x \mid 0$ for all $x \in R$
3. $u \mid 1$ if and only if $u \in R^\times$ If $u \in R^\times$, then $u \mid x$ for all $x \in R$.

$$x = xu^{-1} \cdot u$$

4. If $x, y \in R$, $u \in R^\times$, then $x \mid y \implies ux \mid y, ux \mid x, x \mid ux$.

Definition

If R is commutative, then two elements $x, y \in R$ are associates if $y = ux$ for some $u \in R^\times$. Note: $x \sim y$.

Lemma

$\sim$ is an equivalence relation.

1. $\sim$ is a transitive relation.

$$x \sim y \sim z, y = ux, z = vy, z = uvx$$

2. If $x_1 \sim x_2$ and $y_1 \sim y_2$, then $x_1 \mid y_1 \iff x_2 \mid y_2$.
3. If $x \sim y$, then $x \mid y \iff y \mid x$.

Lemma

If R is a commutative ring, then $x \mid y$ and $y \mid x$ if and only if $(x) = (y)$, where (x) is the ideal generated by x.

Proof

$x \mid y$ and $y \mid x$ if and only if $y \in (x)$ and $x \in (y)$ iff $(y) \subseteq (x)$ and $(x) \subseteq (y)$ iff $(x) = (y)$.

□

Lemma

If R is a domain, then $x \mid y$ iff $x \mid y$ and $y \mid x$.

Proof

$(\Rightarrow)$
holds in any ring,
$(\Leftarrow)$
If $x = 0$ then $x \mid y \implies y = 0 \implies x \sim y$.
Suppose $x \neq 0$ and set $y = ux$ for some $u \in R$ and $x = vy$ for some $v \in R$.
Then $vux = vy = x$. Since R is a domain, $vu = 1$ so $v, u \in R^{\times} \implies x \sim y$.

□

Definition

An element $d \in R$ is a common divisor of $a, b \in R$ if $d \mid a$ and $d \mid b$.
A common divisor is a greatest common divisor of a, b if $d' \mid d$ for every common divisor d' of a, b.
Note: $d = \gcd(a, b)$ to mean d is a gcd of a and b.

Example

$2 = \gcd(6, 8), -2 = \gcd(-6, 8), 2 = \gcd(6, -8), -2 = \gcd(-6, -8)$.

Definition

Common divisor of a and b is a number $d \in R$ such that $d \mid a$ and $d \mid b$.
Greatest common divisor of a and b is a common divisor d such that for any common divisor d' of a and b, we have $d' \mid d$.

Example

$2 = \gcd(6, 8)$, $-2 = \gcd(6, 8)$

Note

1. $0 = \gcd(a, b)$ if and only if $a = 0$ or $b = 0$.
2. If $u \in R^\times$, then any divisor of u is a unit.

   (If $x \mid u$, then $u = hx \implies 1 = u^{-1}u = u^{-1}hx \implies \gcd(u, a) = u'$ for any $u' \in R^\times$)
3. If $d = \gcd(a, b)$ and $d' \sim d, a' \sim a, b' \sim b$, then $f' = \gcd(a', b')$.
4. If $d = \gcd(a, b)$, and $d' = \gcd(a, b)$ then $f \mid f'$ and $f' = d$.

In a domain, $d \sim d'$. We say gcd is unique up to units.

Lemma (Basic Property of Common Divisor)

Let $a, b, d \in R$, then TFAE:

1. $d \mid a$ and $d \mid b$.
2. $d \mid xa + yb$ for all $x, y \in R$.
3. $(a, b) = (d)$

Proof

1. (1) $\implies$ (2): If $d \mid a$ then $a = gd$ and if $d \mid b$ then $b = hd$. If $x, y \in R$ then $xa + yb = xgd + ghd = (xg + yh)d$, so $d \mid xa + yb$.
2. (2) $\implies$ (3): If $f \in (a, b)$ then $f = xa + yb$ for some $x, y \in R$,

   so $d \mid f \implies f \in (d)$.
3. (3) $\implies$ (1): $a, b \in (a, b) = (d) \implies d \mid a$ and $d \mid b$.

□

Proposition

Let $a, b \in R$, R commutative. Then a, b have a gcd iff there is a principal ideal I with $(a,b) \subseteq I$ and such that if J is a principal ideal with $(a,b) \subseteq J$, then $I \subseteq J$.

If I exists, then there is a unique and $I = (d) \iff d = \gcd(a,b)$.
[FIXME: Graphical]

Proof

$d = \gcd(a,b) \iff (a,b) \subseteq (d)$ and for any other principal ideal $J = (d')$ with $(a,b) \subseteq (d')$, $(d) \subseteq (d')$. (This is because $d' \mid a$ and $d' \mid b$ implies $d' \mid d$.)
If I and I' both satisfy the property of proposition, then $I \subseteq I'$ and $I' \subseteq I$ so $I = I'$.

□

Corollary

1. If $(a,b) = (d)$ then $d = \gcd(a,b)$.
2. If $(a,b) = (d) \iff d = xa + yb$ for some $x, y = R$ and $d \mid a$ and $d \mid b$.

Proof

1. Clear
2.

$$\begin{aligned}
(a,b) = (d) &\iff (d) \subseteq (a,b) \text{ and } (a,b) \subseteq (d) \\
&\iff d \in (a,b) \text{ and } d \mid a, d \mid b \\
&\iff d = xa + yb \text{ for some } x, y \in R \text{ and } d \mid a, d \mid b
\end{aligned}$$

□

Definition

A principal ideal domain or PID is an integral domain in which all ideals are principal ideals.

Corollary

If R is a PID, then every pair of elements has a gcd, and $d = \gcd(a,b) \iff d = xa + yb$ for some $x, y \in R$ and $d \mid a, d \mid b$.

Example

$\mathbb{Z}$ is a PID, ideal $\subseteq$ subgroups, for $\mathbb{Z}$, subgroup $= \{a\mathbb{Z} : a \in \mathbb{Z}\} =$ ideals.

Example

$\mathbb{Z}[x]$, $(2, x)$ is not a PID because $(2, x)$ is not principal.
$\mathbb{Q}[x, y]$, (x, y) is not a PID because (x, y) is not principal.

Lemma

If $\mathbb{K}$ is a field, and $f, g \in \mathbb{K}[x]$, $f \neq 0$ then there are $q, r \in \mathbb{K}[x]$ such that $g = qf + r$ where $\deg(r) < \deg(f)$

Proof

By induction on $\deg g$. If $\deg g < \deg f$, then set $q = 0$ and $r = g$.
Suppose that the lemma is true for $\deg(g) < k$.
If $\deg(g) = k$, then $g = ax^k + \underbrace{\cdots}_{\text{Lower degree terms}}$
Let $f = bx^m + \underbrace{\cdots}_{\text{Lower degree terms}}$
Let $h = g - \frac{a}{b}x^{k-m}f = (ax^k + \cdots) - (ax^k + \cdots)$
Then $\deg(h) < k$, so by induction, there are $q', r' \in \mathbb{K}[x]$ such that $h = q'f + r'$ where $\deg(r') < \deg(f)$

$$
\begin{aligned}
g &= \frac{a}{b}x^{k-m}f + h = \frac{a}{b}x^{k-m}f + q'f + r' \\
&= (\frac{a}{b}x^{k-m} + q')f + r'
\end{aligned}
$$

Take $q = \frac{a}{b}x^{k-m} + q'$ and $r = r'$, then $\deg(r) < \deg(f)$.

$\square$

Proposition

If $\mathbb{K}$ is a field then $\mathbb{K}[x]$ is a PID.

Proof

Suppose I is an ideal in $\mathbb{K}[x]$ iff $I = 0 = (0)$, so I is principal.
Suppose $I \neq 0$, let $k = \min\{n : \text{I has a non-zero element of degree n}\}$, and let $f \in I$ be an element of degree k.

Claim: $I = (f)$. We know $(f) \subseteq I$.
Suppose $g \in I$, $g \neq 0$, then there exists $q, r \in \mathbb{K}[x]$ such that $g = qf + r$ where $\deg(r) < \deg(f)$.
But $r = g - qf \in I$, so $r = 0$ and $g = qf \in (f)$, so $I \subseteq (f)$.

□

Note

$n\mathbb{Z}$ is prime if and only if n is prime or $n = 0$.

Proposition

If R is a PID, every non-zero prime ideal is maximal.

Proof

Let I be a non-zero prime ideal $J \neq R$.
Suppose J is a proper ideal with $I \subseteq J$.
Want to show $I = J$.
Since R is a PID, $I = (a)$ and $J = (b)$ for some $a \neq 0, b \neq 0$.
Since $I \subseteq J$, $a = br$ for some $r \in R, r \neq 0$.
Since I is prime, either $b \in I$ or $r \in I$.
If $b \in I$, then $J \subseteq I$ and $I = J$.
Suppose $r \in I$. Then $r = at$ for some $t \in R$, so $a \mid r$ and $r \mid a$.
Since R is a domain, $a \sim r$ associates, i.e. there is a unit $u \in R$ at $a = ur$. But then $ur = a = br \implies u = b$ by cancellation.
So $J = (b) = (a) = R$, which is a contradiction.
Thus, $b \in I$ and $I = J$.

□

Corollary

If $R[x]$ is a PID, then R is a field.

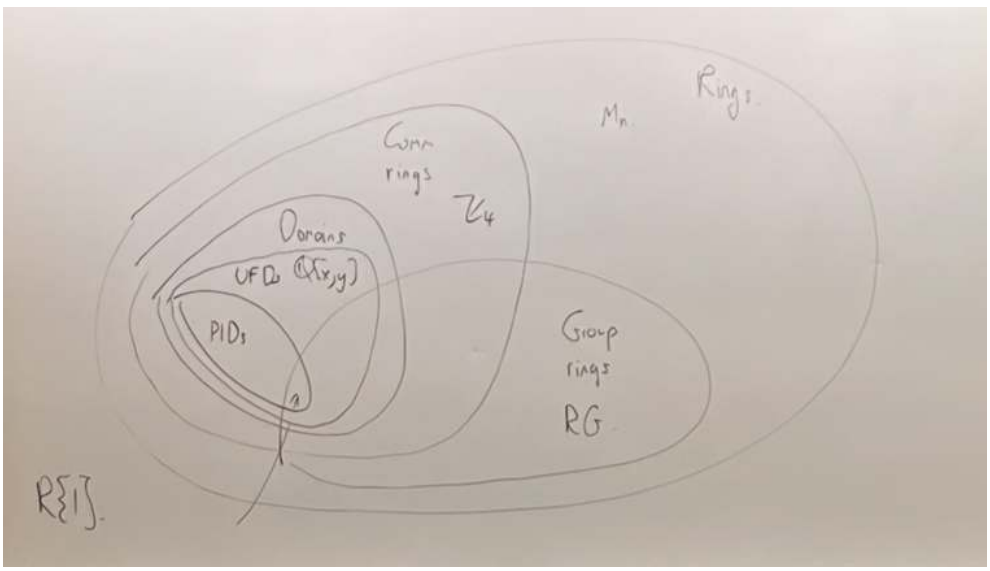
Proof

$R \subseteq R[x]$ is a subring, so R is a domain.

$$ev_0 : R[x] \to R, f(x) \mapsto f(0) \text{ is a ring homomorphism.}$$

With $Im_{ev_0} = R$ and $\ker_{ev_0} = (x)$.
By the First Isomorphism Theorem, $R[x]/(x) \cong R$, so (x) is prime.
By proposition, (x) is maximal, so $R[x]/(x)$ is a field.

□



III. Final Notes

Definition

Let R be a domain, $P \in R$, $p \neq 0$, $p \subseteq R^{\times}$.
Then p is prime if $p \mid ab \implies p \mid a$ or $p \mid b$ for all $a, b \in R$.
p is irreducible if $p = ab$, either a or b is a unit.
p is reducible if p is not irreducible.

Lemma

(1) p is prime if and only if (p) is a prime ideal.

(2) If $p \sim p'$ then p is prime (irreducible) if and only if p' is prime (irreducible).

(3) Ir p is prime, then p is irreducible.

Proposition

If p is an irreducible in a PID R, then p is prime.

Definition

Let R be a domain. We say that R has complete factorization into irreducible if for any $r \in R \setminus (R^\times \cup \{0\})$, there are irreducible $r_1, r_2, \ldots, r_k$ s.t. $r = r_1 r_2 \cdots r_k$ $(= (ur_1)(u^{-1}r_2)\cdots)$

Proposition

Complete factorization are unique if for any two sequences $f_1, \ldots, f_n$ and $g_1, \ldots, g_m$ of irreducible $n, m \geq 1$.
if

$$f_1 f_2 \cdots f_n = g_1 g_2 \cdots g_m$$

then $n = m$ and there is a permutation $\sigma \in S_n$
s.t. $f_1 \sim g_{\sigma(i)}$ for all $i = 1, \ldots, n$.

Definition

R is unique factorization domain (UFD) if R has complete factorization into irreducible and the complete factorization are unique.

Theorem (Big Theorem)

If R is a UFD, then $R[x]$ is a UFD.

Proposition

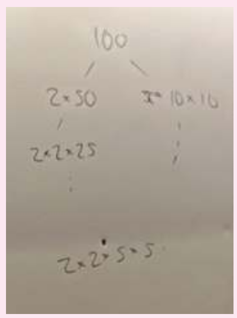
If R is a PID, then R is a UFD.

$\mathbb{Q}$	$\mathbb{Q}[x]$	$\mathbb{Q}[x,y]$	$\mathbb{Q}[x,y,z]$
field	PID	UFD	UFD

In PID, $\gcd(a,b) = k$ where $(k) = (a,b)$, gcd is existed in UFDs.
$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$,$b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$
$\gcd(a,b) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$ where $c_i = \min(a_i, b_i)$.

Proposition

If R is a domain, and every irreducible element is prime, then R has unique factorization.



Theorem

R is a UFD if and only if all irreducible elements are prime and R satisfies the ascending chain condition on principal ideals.

Note

Domain not a UFD
Not unique factorization, complete factorization do not exist.

Example

$\mathbb{Q}[x,t,z,w]/(xy - zw)$ $zw = xy$, x, y, z, w are irreducible.

Example

$\mathbb{Z}[i\sqrt{5}]$ $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$.

End of Class