Part I

Abstract Algebra

New Algebras from Old Ones

- Subalgebra
- Product Algebra
- Quotient Algebra

Definition

- Let
  - $(G, *)$ be a semigroup
  - T be a nonempty subset of G
- $(T, *)$ is called subsemigroup of $(G, *)$
  - if T is closed under the operation $*$

Example

- $(\mathbb{Z}, \times)$ and $(\mathbb{E}, \times)$
- $(\mathbb{Z}, +)$ and $(\mathbb{E}, +)$

Definition

- Let
  - $(G, *)$ be a monoid
  - T be a nonempty subset of G
- $(T, *)$ is called submonoid of $(G, *)$
  - if T is a subsemigroup and $e \in T$

Example

- $(\mathbb{Z}, \times)$ and $(\mathbb{E}, \times)$
- $(\mathbb{Z}, +)$ and $(\mathbb{E}, +)$

Definition

- Let
  - $(G, *)$ be a group
  - T be a nonempty subset of G
- $(T, *)$ is called subgroup of $(G, *)$
  - if T is a submonoid, and if $a \in T$, then $a^{-1} \in T$

Example

- $(\mathbb{Z}, \times)$ and $(\mathbb{E}, \times)$
- $(\mathbb{Z}, +)$ and $(\mathbb{E}, +)$

Definition

- Let
  - $(G, *)$ be a group
  - T be a nonempty subset of G
- $(T, *)$ is called subgroup of $(G, *)$
  - if T is a submonoid, and if $a \in T$, then $a^{-1} \in T$

Example

- $(\mathbb{Z}, \times)$ and $(\mathbb{E}, \times)$
- $(\mathbb{Z}, +)$ and $(\mathbb{E}, +)$

Trivial Subgroups

- Let
  - G be a group.
- Then
  - G and $H = \{e\}$ are subgroups of G, the trivial subgroups of G.

Subgroup of S_3

- Consider S_3, the group of symmetries of the equilateral triangle.
  - $H = \{f_1, f_2, f_3\}$ is a subgroup of S_3

$*$	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_1	f_2	f_3
g_2	g_2	g_3	g_1	f_3	f_1	f_2
g_3	g_3	g_1	g_2	f_2	f_3	f_1

Subgroup of S_3

- Consider S_3, the group of symmetries of the equilateral triangle.
  - $H = \{f_1, f_2, f_3\}$ is a subgroup of S_3

$*$	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_1	f_2	f_3
g_2	g_2	g_3	g_1	f_3	f_1	f_2
g_3	g_3	g_1	g_2	f_2	f_3	f_1

Definition (Powers of a)

- Let
  - G be a semigroup, monoid, or group
  - $a \in G$
- Define
  - a^n as $aa \ldots a$ (n factors), for $n \in \mathbb{Z}^+$
  - a^0 as e, in case of monoid
  - a^{-n} as $a^{-1}a^{-1} \ldots a^{-1}$ (n factors), in case of group

Theorem

- *If n and m are any integers, then $a^n a^m = a^{n+m}$.*

Example

- It is easy to show that
  - $H = \{a^i | i \in \mathbb{Z}^+\}$ is a subsemigroup of G
  - $H = \{a^i | i \in \mathbb{Z}^+$ or $i = 0\}$ is a submonoid of G
  - $H = \{a^i | i \in \mathbb{Z}\}$ is a subgroup of G

Theorem

- *Let*
  - $(G, \ *)$ *be a group*
  - H *be a nonempty subset of* G
- *If*
  - $\forall a, b \in H$ *implies* $a^{-1} * b \in H$
- *Then*
  - H *is a subgroup of* G

Theorem

- *If* $(S, *)$ *and* $(T, *')$ *are semigroups (monoid, group), then* $(S \times T, *'')$ *is a semigroup (monoid, group), where* $*''$ *is defined by*
  - $(s_1, t_1) *'' (s_2, t_2) = (s_1 * s_2, t_1 *' t_2)$

Proof.

- Omitted.

$\mathbb{Z}_2 \times \mathbb{Z}_2$

- Let G_1 and G_2 be the group $\mathbb{Z}_2$.
- For simplicity of notation, we shall write the elements of $\mathbb{Z}_2$ as $\overline{0}$ and $\overline{1}$, respectively, instead of $[0]$ and $[1]$.
- Then the multiplication table of $G = G_1 \times G_2$ is given in Table.

Table: Multiplication Table of $\mathbb{Z}_2 \times \mathbb{Z}_2$

$\circledast$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$

B^n

- Let $B = \{0, 1\}$ be the group with $+$ defined as below

$+$	0	1
0	0	1
1	1	0

- Then $B^n = B \times B \times \cdots \times B$ (n factors) is a group with operation $\oplus$ defined by
  - $(x_1, x_2, \ldots, x_n) \oplus (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$
- The identity of B^n is $(0, 0, \ldots, 0)$, and every element is its own inverse.

Definition (Congruence Relation)

- An equivalence relation R on the groupoid $(G, \ *)$ is called a congruence relation
  - if $a \ R \ a'$ and $b \ R \ b'$ imply $(a * b) \ R \ (a' * b')$

Example

- Consider the group $(\mathbb{Z}, +)$ and the equivalence relation R on $\mathbb{Z}$ defined by
  - $a\ R\ b$ if and only if $a \equiv b \pmod 2$
  - If $a \equiv b \pmod 2$, then $2|(a-b)$
- Show that this relation is a congruence relation.

Proof.

- R is an equivalence relation (omitted).
- R is a congruence relation
  - If $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$
  - $2|a-b$ and $2|c-d$
  - So $a-b=2m$ and $c-d=2n$, where m and n are integers.
  - $(a-b)+(c-d)=2m+2n$
  - $(a+c)-(b+d)=2(m+n)$
  - so $a+c \equiv b+d \pmod 2$.
  - Hence the relation is a congruence relation

Proof.

- R is an equivalence relation (omitted).
- R is a congruence relation
  - If $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$
  - $2|a-b$ and $2|c-d$
  - So $a-b=2m$ and $c-d=2n$, where m and n are integers.
  - $(a-b)+(c-d)=2m+2n$
  - $(a+c)-(b+d)=2(m+n)$
  - so $a+c \equiv b+d \pmod 2$.
  - Hence the relation is a congruence relation

Proof.

- R is an equivalence relation (omitted).
- R is a congruence relation
  - If $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$
  - $2|a-b$ and $2|c-d$
  - So $a-b=2m$ and $c-d=2n$, where m and n are integers.
  - $(a-b)+(c-d)=2m+2n$
  - $(a+c)-(b+d)=2(m+n)$
  - so $a+c \equiv b+d \pmod 2$.
  - Hence the relation is a congruence relation

Proof.

- R is an equivalence relation (omitted).
- R is a congruence relation
  - If $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$
  - $2|a-b$ and $2|c-d$
  - So $a-b=2m$ and $c-d=2n$, where m and n are integers.
  - $(a-b)+(c-d)=2m+2n$
  - $(a+c)-(b+d)=2(m+n)$
  - so $a+c \equiv b+d \pmod 2$.
  - Hence the relation is a congruence relation

Proof.

- R is an equivalence relation (omitted).
- R is a congruence relation
  - If $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$
  - $2|a-b$ and $2|c-d$
  - So $a-b=2m$ and $c-d=2n$, where m and n are integers.
  - $(a-b)+(c-d)=2m+2n$
  - $(a+c)-(b+d)=2(m+n)$
  - so $a+c \equiv b+d \pmod 2$.
  - Hence the relation is a congruence relation

Proof.

- R is an equivalence relation (omitted).
- R is a congruence relation
  - If $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$
  - $2|a-b$ and $2|c-d$
  - So $a-b=2m$ and $c-d=2n$, where m and n are integers.
  - $(a-b)+(c-d)=2m+2n$
  - $(a+c)-(b+d)=2(m+n)$
  - so $a+c \equiv b+d \pmod 2$.
  - Hence the relation is a congruence relation

Proof.

- R is an equivalence relation (omitted).
- R is a congruence relation
  - If $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$
  - $2|a - b$ and $2|c - d$
  - So $a - b = 2m$ and $c - d = 2n$, where m and n are integers.
  - $(a - b) + (c - d) = 2m + 2n$
  - $(a + c) - (b + d) = 2(m + n)$
  - so $a + c \equiv b + d \pmod 2$.
  - Hence the relation is a congruence relation

Proof.

- R is an equivalence relation (omitted).
- R is a congruence relation
  - If $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$
  - $2|a-b$ and $2|c-d$
  - So $a-b=2m$ and $c-d=2n$, where m and n are integers.
  - $(a-b)+(c-d)=2m+2n$
  - $(a+c)-(b+d)=2(m+n)$
  - so $a+c \equiv b+d \pmod 2$.
  - Hence the relation is a congruence relation

Proof.

- R is an equivalence relation (omitted).
- R is a congruence relation
  - If $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$
  - $2|a-b$ and $2|c-d$
  - So $a-b=2m$ and $c-d=2n$, where m and n are integers.
  - $(a-b)+(c-d)=2m+2n$
  - $(a+c)-(b+d)=2(m+n)$
  - so $a+c \equiv b+d \pmod 2$.
  - Hence the relation is a congruence relation

Non-congruence Relation

- Consider the group $(\mathbb{Z}, +)$
  - $f(x) = x^2 - x - 2$
- Define
  - $a \; R \; b$ if and only if $f(a) = f(b)$
- It is easy to verify that R is an equivalence relation, but R is not a congruence relation
  - $-1 \; R \; 2$, since $f(-1) = f(2) = 0$
  - $-2 \; R \; 3$, since $f(-2) = f(3) = 4$
  - but $(-1 + -2) \not R \; (2 + 3)$, since $f(-3) = 10 \neq f(5) = 18$

Theorem (Quotient Groupoid)

- *Let*
  - R *be a congruence relation on the groupoid* $(G, *)$
  - $\circledast$ *be a relation from* $G/R \times G/R$ *to* G/R *in which the ordered pair* $([a], [b])$ *is related to* $[a * b]$ *for* $a, b \in G$
- *Then*
  - $\circledast([a], [b]) = [a] \circledast [b] = [a * b]$, *is a function from* $G/R \times G/R$ *to* G/R
  - *So,* $(G/R, \circledast)$ *is a groupoid.*
    - *called the quotient groupoid or factor groupoid.*

Proof.

- $\circledast$ is a binary operation
  - Suppose that $([a], [b]) = ([a'], [b'])$, different forms
  - $a \; R \; a'$ and $b \; R \; b'$
  - $a * b \; R \; a' * b'$, since R is a congruence relation.
  - Thus $[a * b] = [a' * b']$, that is $[a] \circledast [b] = [a'] \circledast [b']$
  - $\circledast$ is a function, is a binary operation on G/R.
- Hence G/R is a groupoid.

Corollary

- *Let*
  - R *be a congruence relation on the groupoid* $(G, *)$
  - G/R *is the quotient groupoid*
- *Then*
  - *If* G *is a semigroup (monoid, group), So is* $(G/R, \circledast)$.

Corollary.

1. If $*$ is associative, so is $\circledast$
   - $[a] \circledast ([b] \circledast [c]) = [a] \circledast [b * c] = [a * (b * c)] = [(a * b) * c] = [a * b] \circledast [c] = ([a] \circledast [b]) \circledast [c]$
2. If e is the identity in G, $[e]$ is the identity in G/R
   - $[a] \circledast [e] = [a * e] = [a] = [e * a] = [e] \circledast [a]$
3. If a^{-1} is the inverse of a in G, then $[a^{-1}]$ is the inverse of $[a]$ in G/R
   - $[a^{-1}] \circledast [a] = [a^{-1} * a] = [e] = [a * a^{-1}] = [a] \circledast [a^{-1}]$

Corollary.

1. If $*$ is associative, so is $\circledast$
   - ☛ $[a] \circledast ([b] \circledast [c]) = [a] \circledast [b * c] = [a * (b * c)] = [(a * b) * c] = [a * b] \circledast [c] = ([a] \circledast [b]) \circledast [c]$
2. If e is the identity in G, $[e]$ is the identity in G/R
   - ♫ $[a] \circledast [e] = [a * e] = [a] = [e * a] = [e] \circledast [a]$
3. If a^{-1} is the inverse of a in G, then $[a^{-1}]$ is the inverse of $[a]$ in G/R
   - ♫ $[a^{-1}] \circledast [a] = [a^{-1} * a] = [e] = [a * a^{-1}] = [a] \circledast [a^{-1}]$

❀

Corollary.

1. If $*$ is associative, so is $\circledast$
   - $[a] \circledast ([b] \circledast [c]) = [a] \circledast [b * c] = [a * (b * c)] = [(a * b) * c] = [a * b] \circledast [c] = ([a] \circledast [b]) \circledast [c]$
2. If e is the identity in G, $[e]$ is the identity in G/R
   - $[a] \circledast [e] = [a * e] = [a] = [e * a] = [e] \circledast [a]$
3. If a^{-1} is the inverse of a in G, then $[a^{-1}]$ is the inverse of $[a]$ in G/R
   - $[a^{-1}] \circledast [a] = [a^{-1} * a] = [e] = [a * a^{-1}] = [a] \circledast [a^{-1}]$

Corollary.

1. If $*$ is associative, so is $\circledast$
   - $[a] \circledast ([b] \circledast [c]) = [a] \circledast [b * c] = [a * (b * c)] = [(a * b) * c] = [a * b] \circledast [c] = ([a] \circledast [b]) \circledast [c]$
2. If e is the identity in G, $[e]$ is the identity in G/R
   - $[a] \circledast [e] = [a * e] = [a] = [e * a] = [e] \circledast [a]$
3. If a^{-1} is the inverse of a in G, then $[a^{-1}]$ is the inverse of $[a]$ in G/R
   - $[a^{-1}] \circledast [a] = [a^{-1} * a] = [e] = [a * a^{-1}] = [a] \circledast [a^{-1}]$

Corollary.

1. If $*$ is associative, so is $\circledast$
   - $[a] \circledast ([b] \circledast [c]) = [a] \circledast [b * c] = [a * (b * c)] = [(a * b) * c] = [a * b] \circledast [c] = ([a] \circledast [b]) \circledast [c]$
2. If e is the identity in G, $[e]$ is the identity in G/R
   - $[a] \circledast [e] = [a * e] = [a] = [e * a] = [e] \circledast [a]$
3. If a^{-1} is the inverse of a in G, then $[a^{-1}]$ is the inverse of $[a]$ in G/R
   - $[a^{-1}] \circledast [a] = [a^{-1} * a] = [e] = [a * a^{-1}] = [a] \circledast [a^{-1}]$

Corollary.

1. If $*$ is associative, so is $\circledast$
   - ♫ $[a] \circledast ([b] \circledast [c]) = [a] \circledast [b * c] = [a * (b * c)] = [(a * b) * c] = [a * b] \circledast [c] = ([a] \circledast [b]) \circledast [c]$
2. If e is the identity in G, $[e]$ is the identity in G/R
   - ♫ $[a] \circledast [e] = [a * e] = [a] = [e * a] = [e] \circledast [a]$
3. If a^{-1} is the inverse of a in G, then $[a^{-1}]$ is the inverse of $[a]$ in G/R
   - ☛ $[a^{-1}] \circledast [a] = [a^{-1} * a] = [e] = [a * a^{-1}] = [a] \circledast [a^{-1}]$

❀

Example

- $(\mathbb{Z}, +)$
  - $a\ R\ b$ if and only if $a \equiv b \pmod{n}$
  - R is an equivalence relation
- $\equiv \pmod{4}$ is a congruence relation
  - $[0] = \{\dots, -8, -4, 0, 4, 8, 12, \dots\} = [4] = [8] = \dots$
  - $[1] = \{\dots, -7, -3, 1, 5, 9, 13, \dots\} = [5] = [9] = \dots$
  - $[2] = \{\dots, -6, -2, 2, 6, 10, 14, \dots\} = [6] = [10] = \dots$
  - $[3] = \{\dots, -5, -1, 3, 7, 11, 15, \dots\} = [7] = [11] = \dots$

Theorem

- $\mathbb{Z}/\equiv \pmod 4$ *or* $\mathbb{Z}_4$ *is a group with*
  - *identity* $[0]$
  - *operation* $[a] \oplus [b] = [a+b]$

$\oplus$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Theorem (群的一个例子, Group of Symmetries of A Square)

- $(S_4, *)$ *is a group, where*
  - $S_4 = \{$张英哲, 杨珂, 张永恒, 蔡玉生, 郭帅, 易鸿伟, 彭聪, 柏洋$\}$
  - *The operation* $*$ *on the set* S_4 *is defined as follows:*

$*$	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聪	柏洋
张英哲	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聪	柏洋
杨珂	杨珂	张永恒	蔡玉生	张英哲	柏洋	彭聪	郭帅	易鸿伟
张永恒	张永恒	蔡玉生	张英哲	杨珂	易鸿伟	郭帅	柏洋	彭聪
蔡玉生	蔡玉生	张英哲	杨珂	张永恒	彭聪	柏洋	易鸿伟	郭帅
郭帅	郭帅	彭聪	易鸿伟	柏洋	张英哲	张永恒	杨珂	蔡玉生
易鸿伟	易鸿伟	柏洋	郭帅	彭聪	张永恒	张英哲	蔡玉生	杨珂
彭聪	彭聪	易鸿伟	柏洋	郭帅	蔡玉生	杨珂	张英哲	张永恒
柏洋	柏洋	郭帅	彭聪	易鸿伟	杨珂	蔡玉生	张永恒	张英哲

Check it by yourself

- Closure, Associativity, Identity, Inverse
- Commutative

$(S_4, *)$

*	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聪	柏洋
张英哲	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聪	柏洋
杨珂	杨珂	张永恒	蔡玉生	张英哲	柏洋	彭聪	郭帅	易鸿伟
张永恒	张永恒	蔡玉生	张英哲	杨珂	易鸿伟	郭帅	柏洋	彭聪
蔡玉生	蔡玉生	张英哲	杨珂	张永恒	彭聪	柏洋	易鸿伟	郭帅
郭帅	郭帅	彭聪	易鸿伟	柏洋	张英哲	张永恒	杨珂	蔡玉生
易鸿伟	易鸿伟	柏洋	郭帅	彭聪	张永恒	张英哲	蔡玉生	杨珂
彭聪	彭聪	易鸿伟	柏洋	郭帅	蔡玉生	杨珂	张英哲	张永恒
柏洋	柏洋	郭帅	彭聪	易鸿伟	杨珂	蔡玉生	张永恒	张英哲

A Subgroup of $(S_4, *)$

*	张英哲	张永恒
张英哲	张英哲	张永恒
张永恒	张永恒	张英哲

$(S_4, *)$

*	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聪	柏洋
张英哲	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聪	柏洋
杨珂	杨珂	张永恒	蔡玉生	张英哲	柏洋	彭聪	郭帅	易鸿伟
张永恒	张永恒	蔡玉生	张英哲	杨珂	易鸿伟	郭帅	柏洋	彭聪
蔡玉生	蔡玉生	张英哲	杨珂	张永恒	彭聪	柏洋	易鸿伟	郭帅
郭帅	郭帅	彭聪	易鸿伟	柏洋	张英哲	张永恒	杨珂	蔡玉生
易鸿伟	易鸿伟	柏洋	郭帅	彭聪	张永恒	张英哲	蔡玉生	杨珂
彭聪	彭聪	易鸿伟	柏洋	郭帅	蔡玉生	杨珂	张英哲	张永恒
柏洋	柏洋	郭帅	彭聪	易鸿伟	杨珂	蔡玉生	张永恒	张英哲

An equivalence relation on S_4, which is a congruence relation

- $\pi = \{\{$张英哲,张永恒$\}, \{$杨珂,蔡玉生$\}, \{$郭帅,易鸿伟$\}, \{$彭聪,柏洋$\}\}$

Equivalence classes

- [张-张], [杨-蔡], [郭-易], [彭-柏]

Quotients - Example

$(S_4, *)$

*	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聪	柏洋
张英哲	张英哲	杨珂	张永恒	蔡玉生	郭帅	易鸿伟	彭聪	柏洋
杨珂	杨珂	张永恒	蔡玉生	张英哲	柏洋	彭聪	郭帅	易鸿伟
张永恒	张永恒	蔡玉生	张英哲	杨珂	易鸿伟	郭帅	柏洋	彭聪
蔡玉生	蔡玉生	张英哲	杨珂	张永恒	彭聪	柏洋	易鸿伟	郭帅
郭帅	郭帅	彭聪	易鸿伟	柏洋	张英哲	张永恒	杨珂	蔡玉生
易鸿伟	易鸿伟	柏洋	郭帅	彭聪	张永恒	张英哲	蔡玉生	杨珂
彭聪	彭聪	易鸿伟	柏洋	郭帅	蔡玉生	杨珂	张英哲	张永恒
柏洋	柏洋	郭帅	彭聪	易鸿伟	杨珂	蔡玉生	张永恒	张英哲

The Quotient Group, $(S_4/R, \circledast)$

$\circledast$	[张-张]	[杨-蔡]	[郭-易]	[彭-柏]
[张-张]	[张-张]	[杨-蔡]	[郭-易]	[彭-柏]
[杨-蔡]	[杨-蔡]	[张-张]	[彭-柏]	[郭-易]
[郭-易]	[郭-易]	[彭-柏]	[张-张]	[杨-蔡]
[彭-柏]	[彭-柏]	[郭-易]	[杨-蔡]	[张-张]