Chapter VIII - part II

QUOTIENTS ALGEBRA and MORPHISMS OF ALGEBRAIC STRUSTURES

From the existing Alg. structures, we can build new systems. From a set-theoritical perspective we consider products and quotients. We assume that sets are monoids and groups, and determine what is necessary to obtain a monoid or group on the product set and on the certain types of partitions.

8.2 Quotient Algebras:

8.2.1 Relation Congruence modulo n:

In the set of all integers $\mathbb{Z}$, x and y are congruent modulo n (for any positive integer n) denoted $x \equiv y \pmod{n}$ if $x - y = k.n$, $k \in \mathbb{Z}$, integral multiple of n.

Congruence modulo n is an Equivalence Relation.

Exple: Congruence mod 4 in $\mathbb{Z}$.

Verify that it is an Eq. Rel.

Equivalence Classes. congruence classes mod4.

$[0] = \{\dots -8, -4, 0, 4, 8, \dots\}$ $\quad [2] = \{\dots -6, -2, 2, 6, 10, \dots\}$

$[1] = \{\dots -7, -3, 1, 3, 5, 9, \dots\}$ $\quad [3] = \{\dots -5, -1, 3, 7, 11, \dots\}$

As we see and as we saw the equivalence classes define a partition on the set.

8.2.2 Quotient Algebra:

Idea is that given the monoid $(S, \cdot)$ with identity e. Let $\pi = \{B_1, B_2, \dots, B_n\}$ be a partition on S we seek a way to make π a monoid with a "block-by-block" operation of the form $A_i \cdot A_j = A_k$

Exple ①: $(\mathbb{Z}, \cdot)$, $\pi = \{\text{even}, \text{odd}\}$

$\cdot$	even	odd
even	even	even
odd	even	odd

From the table we see that there is an identity that is "odd".

Exple ②: $S = \{0, 1, 2, 3\}$ $(S, +_4)$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1

Let $\pi = \{A, B\}$ $\quad A = \{0, 1\}$ $\quad B = \{2, 3\}$

$x \in A$	$y \in B$	$x+y$
1	2	$3 \in B$
1	3	$0 \in A$

$1+2 = 3 \in B \Rightarrow \quad A+B = B$
$1+3 = 0 \in A \Rightarrow \quad A+B = A$

This partition does not work
which partition should we consider?

$[x]$ be the equivalence class represented by x induced by the relation R
$[y]$ " " " " " y " " " " R.

each class represents a block in a given partition. Thus what we want is
$[x]\cdot[y] = [x\cdot y]$ which failed in exple 2, when x and y are from the same class.

in terms of relation the criterion should be: if $x\,R\,a$ and $y\,R\,b$
then $x\cdot y\,R\,a\cdot b$. Any Eqn. Rel. that satisfies this criterion is called Congruence Relation.

<u>Theorem 8.3</u>: Let $(S,\cdot)$ be a monoid with identity e. Let R be an equivalence Relation on S. Then the partition of S induced by R is a monoid under the operation $[x]\cdot[y] = [x\cdot y]$ <u>iff</u> R is a congruence Relation, and the identity element is $[e]$.

The monoid induced by the partition of a congruence relation is called a <u>Quotient monoid</u>. The partition "factors" the set into blocks of "similar" elements.

We denote the resulting Quotient Monoid by S/R.

<u>Exple</u>: Same as before define R_4 on the set $\mathbb{Z}$ by $m\,R_4\,n$ <u>iff</u> $m-n$ is a multiple of 4.
1) Show that R_4 is a congruence relation on $(\mathbb{Z},+)$
2) Find the partition of $\mathbb{Z}$ induced by R_4.
3) Write the table for the corresponding quotient operation.

1) R, S, T, suppose that $x\,R_4\,a$ and $y\,R_4\,b$ show that $x+y\,R\,a+b$.

$x-a = 4k_1$
$y-b = 4k_2$ $\Rightarrow (x+y)-(a+b) = 4K = 4(k_1-k_2)$
$\Rightarrow (x+y)\,R_4\,(a+b)$

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\Rightarrow (\mathbb{Z}_n, +_n)$

If $(G,\cdot)$ is a group then $\forall x \in G$, $\exists x^{-1} \in G$ $\quad [x]\cdot[x^{-1}] = [x\cdot x^{-1}] = [e]$

<u>Theorem 8.4</u> Let $(G,\circ)$ with identity element e.

1) If $x R y \Rightarrow x^{-1} R y^{-1}$
2) $[e]$ is a subgroup.
3) For $x, y \in G$, $x R y$ <u>iff</u> $x\circ y^{-1} \in [e]$ (or $x^{-1}\circ y \in [e]$)

omit * 4) $\forall x \in G$, $\{x\circ y \,;\, y \in [e]\} = \{y\circ x \,;\, y \in [e]\} = [e]$

<u>Proof</u>: ① Suppose xRy. $x^{-1}Rx^{-1}$ (Reflexivity) $\Rightarrow x\circ x^{-1} R y\circ x^{-1} \Rightarrow e R y\circ x^{-1}$
also $y^{-1}Ry^{-1} \Rightarrow x\circ y^{-1} R x\circ y^{-1} \Rightarrow x\circ y^{-1}\circ e \, R \, xy^{-1}\cdot y\cdot x^{-1} \Rightarrow xy^{-1} R e$
$\Rightarrow xy^{-1} R y\circ x^{-1} \Rightarrow y^{-1} R x^{-1} \Rightarrow x^{-1} R y^{-1}$

② ~~if $x, y \in [e]$~~. $e \in [e]$ if $x, y \in [e] \Rightarrow x R e$ and $y R e$
$\Rightarrow xy R e\cdot e \Rightarrow xy R e. \Rightarrow$ closed.
if $x \in [e]$ $\quad xRe \Rightarrow x^{-1} R e^{-1} \Rightarrow x^{-1} R e \Rightarrow x^{-1} \in [e]$

③ ~~$xRy \Rightarrow x^{-1}Ry^{-1} \Rightarrow x^{-1}\circ x R x y^{-1} \Rightarrow e R xy^{-1} \Rightarrow xy^{-1} \in e.$~~
~~$xy^{-1} \in e \Rightarrow xy^{-1} R e \Rightarrow x\cdot y^{-1} R \cdot y \cdot x^{-1}$ $x^{-1}Rx$ and yRx^{-1}~~

If $xRy \Leftrightarrow x^{-1}Ry^{-1} \Leftrightarrow x\cdot x^{-1} R x y^{-1} \Leftrightarrow e R x\circ y^{-1} \Leftrightarrow xy^{-1} \in [e]$

<u>Exple</u>: $(S,\cdot)$, where $S = \{\alpha, \beta, \gamma, \delta\}$ and "$\cdot$" defined by

$\cdot$	α	β	γ	δ
α	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	α	β
δ	δ	γ	β	α

$R = \{(\alpha,\alpha), (\alpha,\beta), (\beta,\alpha), (\beta,\beta), (\gamma,\gamma), (\gamma,\delta), (\delta,\gamma), (\delta,\delta)\}$ on S

$[\alpha] = \{\alpha, \beta\} = [\beta]$
$[\gamma] = \{\gamma, \delta\} = [\delta]$

$\cdot_R$	$[\alpha]$	$[\gamma]$
$[\alpha]$	$[\alpha]$	$[\gamma]$
$[\gamma]$	$[\gamma]$	$[\alpha]$

8.2.3 **Cosets**: Let $(H,\circ)$ be a subgroup of $(G,\circ)$.

a left coset, $x.H$, of H is $x.H = \{x.h : h \in H\}$

a right coset, $H.x$, of H is $H.x = \{h.x : h \in H\}$.

$(H,\circ)$ is said to be normal if for all x in G, $xH = Hx$

Exple: ① $S = \{1, 5, 8, 12\}$ forms a subgroup of $(\mathbb{Z}_{13}, \bullet_{13})$

The left coset $3S$ is:

$$3S = \{3 \circ_{13} 1,\ 3 \circ_{13} 5,\ 3 \cdot_{13} 8,\ 3 \circ_{13} 12\} = \{3, 2, 11, 10\}$$

② $S = \{0, 4, 8\}$ is a subgroup of $[\mathbb{Z}_{12}, +_{12}]$

find $6 + S = \{6, 10, 2\}$

Theorem 8.5 Let $(G,\circ)$ be a group with identity element e. Let H be a subgroup of G.

1. The left cosets (or the right cosets) of H form a partition of G
2. $\forall x, y \in G$, $|xH| = |Hy| = |H|$.

③ Let $(G,\circ)$ be a group defined by

$\cdot$	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	q	e	s	t	r
q	q	e	p	t	r	s
r	r	t	s	e	q	p
s	s	r	t	p	e	q
t	t	s	r	q	p	e

find all the left and right cosets of the subgroup.

$H = \{e, r\}$

$eH = H = \{e, r\}$, $He = H = \{e, r\}$

$pH = \{p, s\}$, $Hp = \{p, t\}$

$qH = \{q, t\}$, $Hq = \{q, s\}$

$rH = \{r, e\}$, $Hr = \{r, e\}$

$sH = \{s, p\}$, $Hs = \{s, q\}$

$tH = \{t, q\}$, $Ht = \{t, p\}$

Not a normal subgroup.

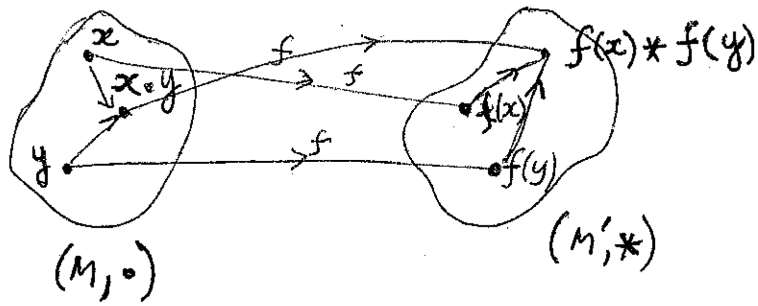
Theorem 8.6: Let $(G,\circ)$ be a finite group. Let H be a subgroup of $(G,\circ)$. Then the order of ~~G~~ divides the order of G.

$|G| = k\,|H|$. $\quad$ k: index of H in G

8.3 Morphisms of Algebraic Structures: The morphisms are the subject of the mechanism we describe the likenesses or "similarities" between two structures

8.3.1 - Homomorphisms between Monoids: Let $(M, \circ)$ and $(M', *)$ be monoids with identities e and e'. A Homomorphism between $(M, \circ)$ and $(M', *)$ is a fct $f: M \to M'$ such that:

1. $f(e) = e'$
2. $\forall x, y \in M \quad f(x \circ y) = f(x) * f(y)$



Exple: ① $f: \mathbb{Z}^+ \longrightarrow \mathbb{N}$; $f(m) = 2^m$, $m = 0, 1, 2, \ldots$

$(\mathbb{Z}^+, +)$ is a monoid with identity "0"
$(\mathbb{N}, \circ)$ " " " " "1"

first $f(0) = 2^0 = 1$ second $\forall x, y \in \mathbb{Z}^+$, $f(x+y) = f(x) \circ f(y)$

$\Rightarrow f$ is a homomorphism - $\quad 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y)$

② $(\mathbb{Z}, +) \longrightarrow (B = \{0, 1\}, +)$ $\quad f: \mathbb{Z} \to B \quad$ $f(m) = 0$ if m is even, $f(m) = 1$ if m is odd

if f a homomorphism;

m	n	$m+n$	$f(m+n)$	$f(m)+f(n)$
even	even	even	0	$0+0 = 0$
even	odd	odd	1	$0+1 = 1$
odd	even	odd	1	$1+0 = 1$
odd	odd	even	0	$1+1 =$ [illegible]

$\Rightarrow$ not a homomorphism

Theorem 8.7 : Let $(M, \circ)$ and $(M', \circ)$ be monoids with identities e and e' respectively : Let $f : M \to M'$ be a monoid homomorphism

1. The image of M by f is a submonoid of $(M', \circ)$
2. $f^{-1}(e')$ is a submonoid of $(M, \circ)$
3. Let R_f be the relation on M defined by $x R_f y$ iff $f(x) = f(y)$.

Then R_f is a congruence relation on $(M, \circ)$

Proof : ① $f(e) = e' \in M \Rightarrow$ identity $\exists$ ii) closed under $\circ$, $f(x) \circ f(y) = f(x * y)$ $\exists$, since f is a monoid homomorphism

② i) since $f(e) = e' \Rightarrow e \in f^{-1}(e')$; ii) closed, $x, y \in f^{-1}(e') \Rightarrow f(x) = e', f(y) = e'$
$\Rightarrow f(x) \circ f(y) = f(x * y) = e' \circ e' = e' \Rightarrow x, y \in f^{-1}(e')$

③ R_f is an equivalence relation show it ! need to show that $x R_f y$, $a R_f b$ then $x \cdot a \, R_f \, y \cdot b$
$x R_f y \Rightarrow f(x) = f(y)$
$a R_f b \Rightarrow f(a) = f(b)$
hence $f(x \cdot a) = f(x) \circ f(a) = f(y) \circ f(b) = f(y \cdot b)$
$\Rightarrow R_f$ is a congruence relation

8.3.2 Isomorphisms of Monoids :

In the Example

$\cdot$	p	q	r	s
p	p	q	r	s
q	q	p	s	r
r	r	r	r	r
s	s	s	s	s

$\circ$	e	a
e	e	a
a	a	a

$\Downarrow$

$[p] \to e$
$[q] \to e$
$[r] \to a$
$[s] \to a$

$\Rightarrow$

$\circ$	[p]	[r]
[p]	[p]	[r]
[r]	[r]	[r]

classes by using the congruence Relation.

$[p] \to e$
$[r] \to a$

A monoid isomorphism is a bijective monoid homomorphism

If $(M, \circ)$ is isomorphic to $(M', \circ)$ we write $M \cong M'$

8.3.3 Fundamental Theorem of Homomorphisms for Monoids :

Theorem 8.8 : Let f be a surjective homomorphism from the monoid $(M, \cdot)$ to $(M', \circ)$. Then R_f is a congruence relation on $(M, \cdot)$ and $M/R_f \cong M'$.
Conversely, if R is a congruence on the monoid $(M, \circ)$, then there exists a surjective monoid homomorphism $h : M \to M/R$ such that $R = R_h$

8.3.4 Group Homomorphism: since groups are monoids all what was found as a result will apply to groups also.

Def: Let $(G, \circ, e)$ and $(G', *, e')$ be groups. ~~we~~ say that $f: G \to G'$ is a group homomorphism if the following conditions are met:

1. $f(e) = e'$
2. $f(x \cdot y) = f(x) * f(y) \quad \forall x, y \in G$.
3. $f(x^{-1}) = [f(x)]^{-1} \quad \forall x \in G$.

A group isomorphism is a bijective group homomorphism.

Exple: $[\mathbb{Z}, +]$, $[12\mathbb{Z}, +]$ where $12\mathbb{Z} = \{12z \mid z \in \mathbb{Z}\}$.

define $f: \mathbb{Z} \to 12\mathbb{Z} \quad f(x) = 12x$

(i) $f(0) = 0$

(ii) $f(x+y) = 12(x+y) = 12x + 12y = f(x) + f(y)$

(iii) $\forall x \in \mathbb{Z}$, $x^{-1} = -x \Rightarrow f(x^{-1}) = f(-x) = -12x = -f(x) = f(x)^{-1}$

8.3.4. The Kernel of f: Let $(G, \circ, e)$ and $(G', *, e')$ be groups, Given a group homomorphism $f: G \to G'$

The Kernel K of f is the set $f^{-1}(e')$ ~~where~~ $K = f^{-1}(e')$ where e' is the identity of ~~in~~ G'.

Theorem 8.9 Let $(G, \circ, e)$ and $(G', *, e')$ be groups. and let $f: G \to G'$ be a group homomorphism.

1. K_f is a normal subgroup of G.
2. f is an injection if $K_f = \{e\}$

8.3.5 Fundamental Theorem of Homomorphisms for Groups:

Theorem 8.10: Let f be a surjective homomorphism from the group $(G, \cdot, e)$ to $(G', \circ, e')$. Then K_f is a normal subgroup of G and $G/K_f \cong G'$. Conversely, if K is a normal subgroup of G, there exists a surjective group homomorphism $h: G \to G/K$ such that $K = K_h$.