4. Algebraic structures

4.1. Basic algebraic structures

Definition Let S be a set. A binary operation on S is a mapping

$$S \times S \mapsto S$$

Notation: $(x,y) \mapsto x+y,\ x\cdot y,\ x \circ y,\ x * y, \ \ldots$

Definition An operation

$$\cdot : S \times S \mapsto S$$

is called

- associative if $(x\cdot y)\cdot z = x\cdot(y\cdot z) \quad \forall x,y,z \in S$
- commutative if $x\cdot y = y \cdot x \quad \forall x,y \in S$

Definition A semigroup is a pair $(S,\cdot)$ where $\cdot$ is a associative operation on S.

If operation $\cdot$ is commutative then $(S,\cdot)$ is called commutative (abelian).

Examples of semigroups

- $(\mathbb{R},+)$, $(\mathbb{Z},+)$, $(\mathbb{N},+)$ (addition operation)
- $(\mathbb{R},\cdot)$, $(\mathbb{Z},\cdot)$, $(\mathbb{N},\cdot)$

- $(\mathbb{R}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{N}, \cdot)$
  (multiplication operation)
- $(M_n, +)$ $(M_n, \cdot)$
  $n \times n$ matrices with addition and matrix multiplication
- $(X^X, \circ)$
  Set X^X of all functions $f: X \to X$, where $\circ$ is the composition of functions.

- Not all operations are associative: $(\mathbb{R}, -)$

$$(x, y) \mapsto x - y$$

$$2 - (3 - 1) = 0$$

$$(2 - 3) - 1 = -2$$

Definition Let S be a set with binary operation $\cdot$.
An element $e \in S$ is called **neutral element (unit, identity)** if

$$x \cdot e = e \cdot x = x \quad \forall x \in S.$$

- There is at most one neutral element:

$e_1, e_2 \in S$ neutral $\Rightarrow$

$$e_1 = e_1 \cdot e_2 = e_2.$$

Definition: A semigroup that contains an identity is called **monoid**.

identity is [illegible]

Examples of monoids:

- $(\mathbb{R},+)$ $\quad e=0$
- $(\mathbb{R},\cdot)$ $\quad e=1$
- $(M_n,\cdot)$ $\quad e=\begin{pmatrix}1 & & 0\\ & \ddots & \\ 0 & & 1\end{pmatrix}$
- $(X^X,\circ)$ $\quad e=$ identity map

- $(S,\circ)$

S: all functions $f: S \mapsto S$, where S is infinite, whose range is finite

$\circ$: composition

It is not monoid: By contradiction, let $e: S \to S$ be a neutral element.

$$\Rightarrow \quad e(f(x)) = f(x), \; \forall f \in S, \; x \in X$$

So for a constant function

$$f(s) = x \quad \forall s$$

we have $\forall s \in S$:

$$e(x) = x$$

So e must be identity, but identity has not finite range.

__Definition__ Let $(S, \cdot)$ be monoid with unit e. We say that an element $x \in S$ has __an inverse__ y if

$$x \cdot y = y \cdot x = e$$

An element that has an inverse is called *invertible*.

---

notation: x^{-1} (if operation is $\cdot$)
$-x$ (if operation is $+$) $\quad$ ne)

There is at most one inverse element: y_1, y_2 are inverse elements of x, then

$$y_1 = y_1 e = y_1(x y_2) = (y_1 x) y_2 = e y_2 = y_2$$

__Examples__:

- $(\mathbb{R}, \cdot)$
  $x \neq 0$ is invertible and $x^{-1} = \frac{1}{x}$

- $(M_n, \cdot)$
  A is invertible $\Leftrightarrow$ A is regular ($\det A \neq 0$)

  A^{-1} is the inverse matrix

- $(X^X, \circ)$
  $f: X \to X$ is invertible $\Leftrightarrow$ f is a bijection
  f^{-1} is the inverse function.

$f: R \to R$

f^{-1} is the inverse function.

Proposition: $(S, \cdot)$ - monoid with a unit e.

Then

(i) $e^{-1} = e$

(ii) $x \in S$ is invertible $\Leftrightarrow$ x^{-1} is invertible and $(x^{-1})^{-1} = x$

(iii) $x, y \in S$ invertible, then

$$\boxed{(xy)^{-1} = y^{-1}x^{-1}}$$

Proof (ii) $x \cdot x^{-1} = x^{-1} \cdot x = e$

$\Rightarrow (x^{-1})^{-1} = x$

(iii) $xy \cdot (y^{-1}x^{-1}) = xx^{-1} = e$

$(y^{-1}x^{-1})(xy) = y^{-1}y = e$

Definition A monoid where every element is invertible is called a group.

Examples:
- $(\mathbb{R} \setminus \{0\}, \cdot)$
- $((0, \infty), \cdot)$
- $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{N}, +)$
- $(M_n, +)$ is abelian group

$(M_n, \cdot)$ not

- $(GL_n, \cdot)$ is a group

invertible $n \times n$ matrices; matrix multiplication

- $(X^X, \circ)$ is not a group as non-injective functions have no inversion

- $(B(X), \circ)$ is a group.

bijections

Linear equations are solvable in groups

Theorem: Let $(S, \cdot)$ be a semigroup. $(S, \cdot)$ is a group $\Leftrightarrow$ the equations

$$(*) \quad \begin{aligned} a \cdot x &= b \\ y \cdot a &= b \end{aligned}$$

have solution (x, y) for every $a, b \in S$.

Proof $\Rightarrow$ If S is a group then $(*)$ have solution

$$x = a^{-1} b$$
$$y = b a^{-1}$$

$\Leftarrow$ First we show that S has a unit.

By assumption given $a \in S$ there is e_a, such that

$a e_a = a$

e_a, such that

$a \cdot e_e = a$

By assumption given $b \in S$ $\exists y \in S$ such that $b = ya$. Then

$$b e_a = y a e_a = ya = b$$

So for $e = e_a$ we have

$$b e = b \quad \forall b \in S$$

Similarly, there is $e' \in S$ with

$$e' b = b \quad \forall b \in S$$

Now

$$e = e' e = e'$$

So e is a unit.

Having unit e we see that, given $a \in S$ $\exists x, y \in S$ with

$$x a = e$$
$$a y = e$$

then $$y = e y = x \underbrace{a y}_{= e} = x$$

$\square$

<u>Definition</u> Let $(G_1, \cdot)$ and $(G_2, +)$ be groups. A bijection $\varphi : G_1 \to G_2$ is said to be isomorphism if

$$\varphi(a \cdot b) = \varphi(a) * \varphi(b) \quad \forall\, a, b \in G_1$$

G_1 and G_2 are isomorphic if there is an isomorphism between them.

<u>Example</u> $\varphi : (0, \infty) \to \mathbb{R} : \varphi(x) = \ln x$

is isomorphism from $G_1 = ((0,\infty), \cdot)$ onto $(\mathbb{R}, +)$

Indeed

$$\ln(xy) = \ln x + \ln y \qquad \forall x, y > 0$$

$[\ \varphi^{-1}(x) = e^{x}\ ]$

4.2. Subgroups

<u>Definition</u> Let $(S, \cdot)$ be a semigroup. A subset $T \subseteq S$ forms a subsemigroup if $a \cdot b \in T$ whenever $a, b \in T$.

Then $(T, \cdot)$ is a semigroup with the same operation.

Examples

- $((0,\infty),\cdot)$ is a subsemigroup of $(\mathbb{R},\cdot)$
- $(\mathbb{N},+)$ is a subsemigroup of $(\mathbb{R},+)$

Definition Let $(S,\cdot)$ be a monoid with a unit e. A subsemigroup T of S is a submonoid if $e \in S$.

Definition Let $(G,\cdot)$ be a group with a unit e. Then a subset $H \subset G$ forms a subgroup of G if

(i) $x, y \in H \Rightarrow x \cdot y \in H \quad \forall x, y \in H$

(ii) $e \in H$

(iii) $x \in H \Rightarrow x^{-1} \in H$

- $H \subset G$ is a subgroup $\Leftrightarrow x^{-1}y \in H, \forall x, y \in H$
- Intersection of subgroups is a subgroup again

Definition Let $g_1, g_2, \ldots, g_n \in (G,\cdot)$ where G is a group. Define

$$\langle g_1, g_2, \ldots, g_n \rangle$$

as the smallest subgroup containing $g_1, g_2, \ldots, g_n$.

It is called subgroup generated by $g_1, g_2, \ldots, g_n$.

Remark

$$\langle g_1, g_2, \ldots, g_n \rangle = \begin{cases} \text{intersection of all subgroups of } G \text{ containing } e \\ \text{set of all products } h_1^{\pm 1} h_2^{\pm 1} \ldots h_k^{\pm 1} \text{ where } h_1, h_2, \ldots, h_k \in \{g_1, g_2, \ldots, g_n\} \end{cases}$$

<u>Example</u>

- $(\mathbb{Z}, +)$

$\langle 1 \rangle = \mathbb{Z}$

$\langle 3 \rangle = \{3k \mid k \in \mathbb{Z}\}$

- $(\mathbb{R} \setminus \{0\}, \cdot)$

$a \in \mathbb{R} \setminus \{0\}$

$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} =$

$\{\ \ldots, \frac{1}{a^2}, \frac{1}{a}, 1, a, a^2 \ldots\ \}$

<u>Definition</u>: Let $(H, \cdot)$ be a subgroup of $(G, \cdot)$.
For any $g \in G$ define it's <u>left coset</u> with respect to H as

$$gH = \{gh \mid h \in H\}.$$

<u>Notation</u>: $G/H = \{gH \mid g \in G\}$

If we have $(G, +)$ $\quad G/H = \{g + H \mid g \in G\}$

Example $\cdot$ $G = (\mathbb{Z}, +)$

H = even integers

$$n + H = \begin{cases} H & \text{if } n \text{ is even} \\ \text{odd numbers} & \text{if } n \text{ is odd} \end{cases}$$

- $G = (\mathbb{Z}, +)$

$H = \{3k \mid k \in \mathbb{Z}\} = 3\mathbb{Z}$

$0 + \mathbb{Z} = H$

$1 + \mathbb{Z} = \{3k+1 \mid k \in \mathbb{Z}\} = \{z \in \mathbb{Z} \mid z \equiv 1 \pmod 3\}$

$2 + \mathbb{Z} = \{3k+2 \mid k \in \mathbb{Z}\} = \{z \in \mathbb{Z} \mid z \equiv 2 \pmod 3\}$

$(3 + \mathbb{Z} = 0 + \mathbb{Z}, \ldots)$

So $\mathbb{Z}/3\mathbb{Z}$ has 3 elements $[0], [1], [2]$

e.g. $[2] + [2] = [4] = [1]$.

- $(\mathbb{Q} \setminus \{0\}, \cdot)$

$H = \{1\}$

$zH = \{z\}$

- $(\mathbb{Q} \setminus \{0\}, \cdot)$

$H = \{2^k \mid k \in \mathbb{Z}\} = \langle 2 \rangle$

$zH = \{z \cdot 2^k \mid k \in \mathbb{Z}\} = \{\ldots \frac{z}{4}, \frac{z}{2}, 1, 2z, 4z, \ldots\}$

Theorem Let $(H,\cdot)$ be a subgroup of $(G,\cdot)$ then G/H is a partition of G.

Proof: • cosets are non-empty: $g = g\cdot 1 \in gH$

• $g \in gH$ and so

$$\bigcup_{g\in G} gH = G$$

• Suppose that $g_1H \cap g_2H \neq \emptyset$

So there is $h \in g_1H \cap g_2H$ i.e.

$$h = g_1h_1 \quad h_1 \in H$$
$$h = g_2h_2 \quad h_2 \in H$$

Take

$a \in g_1H$

$a = g_1u \quad u \in H$

Then

$$a = g_1u = hh_1^{-1}u = g_2\underbrace{h_2h_1^{-1}u}_{\in H} \in g_2H$$

Therefore $g_1H \subset g_2H$ and so $g_1H = g_2H$ by symmetry.

$\square$

In a similar way we define right cosets Hg. We obtain another partition of G

In a similar way we define right cosets Hg. We obtain another partition of G

Partition $\{gH \mid g \in G\}$ defines an equivalence on G

$$g_1 \sim g_2 \underset{\text{def}}{\equiv} g_1 H = g_2 H.$$

Observation: $g_1 \sim g_2 \Leftrightarrow g_2^{-1} g_1 \in H$

Indeed, $g_1 \in g_2 H \Rightarrow g_1 = g_2 h$, $h \in H$

$\Rightarrow g_2^{-1} g_1 = h \in H$.

Suppose that $g_2^{-1} g_1 \in H$. Then

$g_2^{-1} g_1 = h \in H$

$g_1 = g_2 h$

Let $k \in H$. Then $g_1 k = g_2 \underbrace{hk}_{\in H}$. Therefore $g_1 H \subseteq g_2 H$.

By symmetry $g_2 H \subset g_1 H$ and so $g_1 H = g_2 H$.

$\square$

Definition: Let $(H, \cdot)$ be a subgroup of $(G, \cdot)$.
H is called normal subgroup if

$$gH = Hg \quad \forall g \in G.$$

In this case we define the quotient group G/H

by defining for $[g_1] = g_1 H$
$[g_2] = g_2 H$

the operations

$[g_2] = g_2 H$

the operations

$$[g_1]\cdot[g_2] = [g_1 g_2].$$

Let us verify that G/H is a group

- operations are well defined, i.e not depending on the choice of g_1 and g_2

$$\left.\begin{array}{l} g_1' \in g_1 H \\ g_2' \in g_2 H \end{array}\right\} \overset{?}{\Rightarrow} [g_1 g_2] = [g_1' g_2'].$$

Indeed, $$(g_1' g_2')^{-1} g_1 g_2 = \underbrace{g_2'^{-1} \underbrace{g_1'^{-1} g_1}_{= h \in H} g_2}_{g_2' H = H g_2' \Rightarrow\, = k g_2'^{-1} \text{ for } k \in H} = k g_2'^{-1} g_2 = k \in H$$

- now axioms for groups are satisfied:

$$[e]\cdot[g] = [eg] = [g]$$

✓ so $[e]$ is the unit of G/H.

✓ Obviously $[g_1]\cdot([g_2]\cdot[g_3]) = ([g_1]\cdot[g_2])\cdot[g_3]$ $\forall\, g_1, g_2, g_3 \in G$

✓ $$[g^{-1}]\cdot[g] = [g^{-1}g] = [e].$$
$$[g]\cdot[g^{-1}] = [g g^{-1}] = [e]$$

Therefore, $$[g]^{-1} = [g^{-1}].$$

<u>Example</u>: • If $H = \{e\}$ then

$$G/H = G$$

as $gH = \{g\}$

is $\quad gH = \{g\}$

- $G = (\mathbb{Z}, +)$

  H = even numbers $= 2\mathbb{Z}$

  For $x \in \mathbb{Z}$

  $[x] = \{x + 2k \mid k \in \mathbb{Z}\}$

  $[x] + [y] = [x+y] = \{x + y + 2k \mid k \in \mathbb{Z}\}$

So $[x] = $ even numbers if x is even $= [0]$; odd numbers if x is odd $= [1]$

$G/H = \{[0], [1]\}$

$[0] + [0] = [0]$

$[0] + [1] = [1]$

$[1] + [1] = [2] = [0]$

This is isomorphic to $\mathbb{Z}_2 = \{0, 1\}$ with $x \oplus y = (x+y) \bmod 2$

It will be investigated in a separate section

- More general example, $n \in \mathbb{N}$

  $G = \mathbb{Z}$

  $H = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$

$$\mathbb{Z}_n = G/H = \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}$$

$$[x] + [y] = [x+y]$$

<u>Definition</u> Let $(G, \cdot)$ be a group. Order of G is

Definition Let $(G,\cdot)$ be a group. Order of G is the number of its elements if it is finite and infinity if it infinite.

Let $H \leq G$ be a subgroup.

Then index of H, $[G:H]$, is the number of elements of G/H if G/H is finite and infinity if G/H is infinite.

Example $G = (\mathbb{Z},+)$

H = even integers

$[G:H] = 2$

Lagrange theorem Let $(G,\cdot)$ be a finite group and $(H,\cdot)$ its subgroup. Then

$$\boxed{|G| = [G:H]\cdot[H]}$$

Proof: We show that all left cosets have the same size.

Write $H = \{g_1, g_2, \dots, g_k\}$

Fix $g \in G$.

The map $\tau : H \to gH$

$\tau(g_i) = g g_i$

is an injective map mapping H onto gH.

$(g g_i = g g_j \Rightarrow g^{-1} g g_i = g^{-1} g g_j$, i.e. $g_i = g_j)$

($gg_i = gg_j \Rightarrow \underbrace{g^{-1}g}_{e}g_i = g^{-1}gg_j$, i.e. $g_i = g_j$)

Therefore $|H| = |gH|$.

Then $|G| = |H| \cdot$ number of cosets $= |H| \cdot [G:H]$

<u>Corollary</u> : If G is finite and H is a subgroup of G then both $|H|$ and $[G:H]$ divides $|G|$.

<u>Notation</u> $(G, \cdot)$ - group with identity e.

$a \in G$

$k \in \mathbb{N}$

We define the powers of a as follows

$a^0 = e$

$a^k = \underbrace{a \cdot a \cdot \ldots \cdot a}_{k\text{-times}}$

$a^{-k} = \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{k\text{-times}}$

Then $\langle a \rangle = \{ a^j \mid j \in \mathbb{Z} \}$

It is a subgroup as $a^j \cdot a^k = a^{j+k}$

Order of $a \underset{\text{def}}{\equiv} |\langle a \rangle|$

Example : $\cdot$ $G = (\mathbb{Z}, +)$

$\langle 0 \rangle = \{0\}$ order 1

Example : $\cdot$ $G = (\mathbb{Z}, +)$

$\langle 0 \rangle = \{0\}$ order 1

$\langle 1 \rangle = \mathbb{Z}$ order ∞

$\cdot$ $G = (\mathbb{R} \setminus \{0\}, \cdot)$

$\langle 1 \rangle = \{1\}$

$\langle -1 \rangle = \{1, -1\}$ order 2

$x \in \mathbb{R}$; $x \neq 0, 1, -1$

$\langle x \rangle = \{x^j \mid j \in \mathbb{Z}\}$ - infinite order

$x^j = x^k \Leftrightarrow x^{j-k} = 1$ $\quad j \neq k$

$\Rightarrow x \in \{1, -1\}$

Proposition: If $(G, \cdot)$ is a finite group and $a \in G$, then order of a divides order of G.

Proposition : Let $a \in (G, \cdot)$ have finite order r. Then r is the smallest positive integer such that

$$\boxed{a^r = e}$$

Proof : Suppose that $a \neq e$.

as $|\langle a \rangle|$ is finite then there must exist $j \in \mathbb{N}$ such that

$$a^j = e$$

Indeed, as $|\langle a \rangle|$ is finite there must exist $i < k$ integers such that

$$a^i = a^k$$

Then $$a^{-k}a^{i} = a^{i-k} = e$$
and we can put
$$j = i - k$$

Now let r be the smallest natural number such that $a^r = e$.

Then $a^{\ell} \neq a^{k}$ for all $0 \leq \ell < k \leq r$ for otherwise

$$a^{\ell} = a^{k} \text{ would imply } e = a^{\ell}a^{-\ell} = a^{k-\ell}$$

as $0 < k - \ell < r$ we have contradiction with definition of r.

In other words, the set
$$H = \{e, a, a^2, \ldots, a^{r-1}\}$$
has r elements

Let us show that H is a subgroup of G.

For this, for $0 \leq i, j \leq r-1$ we have
$$i + j = kr + r', \quad r' = 0, 1, \ldots, r-1$$
and so
$$a^{i+j} = a^{kr+r'} = \underbrace{a^{kr}}_{e^k = 1} \cdot a^{r'} = a^{r'}$$

Also, if $0 \leq i \leq r-1$, then
$$a^i \cdot a^{r-i} = a^{r-i}a^i = a^r = e$$
and so
$$(a^i)^{-1} = a^{r-i} \in H$$

Therefore $H = \langle a \rangle$

and $|\langle a \rangle| = |H| = r$. $\square$

(♡) Corollary: Let $a \in (G, \cdot)$ where G is a finite group. Then the order r of a equals r if and only if

(i) $a^r = e$

(ii) if $a^s = e$, then $r | s$

(T)

> Corollary: Let $(G, \cdot)$ be a finite group and $a \in G$. Then
>
> (a) $|\langle a \rangle|$ devides $|G|$
>
> (b) $a^{|G|} = e$

Proof: (a) It follows from Lagrange theorem

(b) From (a)

$$|G| = \underset{\text{integer}}{K} \cdot \underset{\text{order of } a}{r}$$

So

$$a^{|G|} = a^{K \cdot r} = (a^r)^K = e^K = e.$$

$\square$

> Proposition: Let $(G, \cdot)$ be a finite group.
>
> Let $a \in G$ has order $r(a)$. Then
>
> $$r(a^i) = \frac{r(a)}{\gcd(r(a), i)}$$

Proof: We shall apply ♡ Corollary:

Put $r = r(a)$

$d = \gcd(r, i)$.

So $i = d i'$

$r = d r'$

where $i' \perp r'$

(1) in ♡

$$(a^i)^{r'} = a^{ir'} = a^{i'dr'} = a^{(dr')i'} = (a^r)^{i'} = e.$$

(2) assume $a^{is} = e$

Then $r \mid is$

Further,

$$is = kr$$
$$i'ds = kr'd$$

and $i's = kr'$

Euclid: $r' \mid s \Rightarrow r'$ is the order of a^i.

Example: What is order of $[3]$ in $\mathbb{Z}_{15}$?

$$\text{order of }([3]) = \frac{15}{\gcd(3,15)} = 5$$

and indeed $[3]^5 = [5 \cdot 3] = [15] = [0]$.

Definition group $(G, \cdot)$ is called cyclic if there is $a \in G$ such that

$$\langle a \rangle = G.$$

In this case, a is called generator of G.

Example
- $(\mathbb{Z}, +)$ is cyclic with generator 1.
- $(\mathbb{R}, +)$ is not cyclic as any subgroup generated by $a \neq 0$ is countable

---

Theorem Any finite cyclic group is isomorphic to $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$

where $[i] + [j] = [(i+j) \bmod n]$

Proof: $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

where n is order of G (and a).

Define
$$\varphi : G \to \mathbb{Z}_n$$
$$\varphi(a^i) = i$$

φ is a bijection

$$\varphi(a^i \cdot a^j) = \varphi(a^{i+j}) = \varphi\left(a^{(i+j) \bmod n}\right)$$
$$= (i+j) \bmod n = \varphi(a^i) \oplus \varphi(a^j).$$

- Infinite cyclic group is isomorphic to $(\mathbb{Z},+)$.

4.3. Groups associated with $\mathbb{Z}_n$

__Definition:__ Let $n \in \mathbb{N}$ and $\equiv_n$ congruence relation on $\mathbb{Z}$ modulo n.

Define

$$\mathbb{Z}_n = \mathbb{Z}/\equiv_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$$

$$[i]_n = \{x \in \mathbb{Z} \mid x \equiv i \pmod{n}\}$$

We shall define operation $+$ on $\mathbb{Z}_n$ by

$$[i] + [j] = [i+j]$$

- Observation:

$$(\mathbb{Z}_n, +) = \mathbb{Z}/n\mathbb{Z} \quad \text{quotient group}$$

($n\mathbb{Z}$ is a normal subgroup)

It is an abelian group

__Examples:__ $G = \mathbb{Z}_4$

- $[3] + [2] = [5] = [1]$

- $[3] + [1] = [4] = [0]$

i.e.

$[1]$ is the inverse element of $[3]$

- In general $\mathbb{Z}_n$

$$-[i] = [n-i] = [-i]$$

$\uparrow$

inverse of i in $\mathbb{Z}_n$

$(\mathbb{Z}_n, +)$ is a cyclic group.

One of the generators is $[1]$:

$$\langle [1] \rangle = \{[1], [2], [3], \dots, [n-1], [n] = [0]\}$$

Let us recall that any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

<u>Example</u> $G = (\mathbb{Z}_{35}, +)$

- Find $\langle [5] \rangle$

$\langle [5] \rangle = \{[5], [10], [15], [20], [25], [30], [35] = 0\}$

This subgroup has order 7

$(7 | n$ as order of any element should do!$)$

- $\langle [6] \rangle$

as $[1] = [36] \in \langle [6] \rangle$

we conclude that

$\langle [6] \rangle = \mathbb{Z}_{35}$

i.e. $[6]$ is another generator of $(\mathbb{Z}_{35}, +)$

<u>Proposition</u> Any $[i] \in (\mathbb{Z}_n, +)$ has order $\frac{n}{\gcd(i,n)}$

<u>Proof</u>: $[i] = [1] + [1] + \dots + [1]$

and we can use Proposition $(**)$ for $a = [1]$, $ia = [i]$,
"a^i"

<u>Example</u>: • $G = (\mathbb{Z}_{35}, +)$

$$|\langle[7]\rangle| = \frac{35}{\gcd(35,7)} = \frac{35}{7} = 5$$

$$|\langle[6]\rangle| = \frac{35}{\gcd(6,35)} = \frac{35}{1} = 35$$

$\Rightarrow$ $[6]$ is a generator of G

Observation: $[i] \in \mathbb{Z}_n$ is a generator of G $\Leftrightarrow$ $i \perp n$

Now we shall consider multiplication on $\mathbb{Z}_n$:

Definition: We define multiplication on $\mathbb{Z}_n$ by

$$\boxed{[i]\cdot[j] = [ij]}$$

Definition is correct: $\left.\begin{array}{l} i \equiv i' \pmod n \\ j \equiv j' \pmod n \end{array}\right\} \Rightarrow ij \equiv i'j' \pmod n$

Proposition: $(\mathbb{Z}_n, \cdot)$ is a commutative monoid with unit $[1]$.

Warning: $(\mathbb{Z}_n, \cdot)$ is not always group. For example, in $(\mathbb{Z}_4, \cdot)$ we have

$$[2]\cdot[2] = [4] = [0]$$

So for a inverse $[j]$ of $[2]$ we would have

$$j\cdot([2]\cdot[2]) = (\underbrace{j\cdot[2]}_{=[1]})\cdot[2] = [2]$$

but
$$j \cdot ([2]\cdot[2]) = j\cdot[0] = [0] \quad \text{- contradiction}$$

Question: When is an element $[i]$ invertible in $(\mathbb{Z}_n, \cdot)$?

Answer: $[i]$ is invertible if and only if

$i \perp n$

Proof: $[i]$ has an inversion $[j]$ if and only if
$$[i]\cdot[j] = [ij] = [1].$$

$\Leftrightarrow \quad ij \equiv 1 \pmod{n}$

$\Leftrightarrow \quad \gcd(i,n) \mid 1 \Leftrightarrow \gcd(i,n) = 1$

see number theory

Example: $(\mathbb{Z}_6, \cdot)$ has invertible elements all $[i]$ with $i \perp j$:

$[1], [5]$

General fact: Let $(S, \cdot)$ be monoid. Then the set
$$S^\times = \{ s \in S \mid s \text{ is invertible} \}$$
endowed with multiplication $\cdot$ is a group

Proof: If $x, y \in S^\times$ with inversions x^{-1}, y^{-1} then $xy \in S^\times$ with inversion $y^{-1}x^{-1}$!

Observation: $[0]$ is never invertible in $(\mathbb{Z}_n, \cdot)$ as
$$[0]\cdot[x] = [0] \neq [1] \quad \forall x \in \mathbb{Z}_n$$

Corollary: $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ is group if and only if n is prime.

Proof: Every element of $\mathbb{Z}_n$ is inventible $\Leftrightarrow$
$\forall\, i \in \{1, 2, \dots, n-1\}$ we have $i \perp n$ $\Leftrightarrow$ n is prime

---

Definition Euler function $\varphi : N \to N$ is defined as

$$\boxed{\varphi(n) = \#\{k \in N \mid k \leq n,\ k \perp n\}}$$

In other words,

$$\varphi(n) = |\mathbb{Z}_n^\times|$$

Proposition:

(1) If p is prime then

$$\varphi(p^k) = p^k - p^{k-1} \quad \forall\, k = 1, 2, \dots,$$

Especially, $\phi(p) = p - 1$

Proof divisors of p^k : $1, p, p^2, \dots, p^k$

Therefore $\gcd(p^k, m) > 1 \Leftrightarrow p^\ell \mid m$ for some ℓ $\Leftrightarrow m$ is multiple of p

For $0 \leq m \leq p^k$ we have $\gcd(p^k, m) > 1 \Leftrightarrow$

$$m = p, 2p, \dots, p^{k-1}p = p^k.$$

We have p^{k-1} such m's.

Therefore,

$$\varphi(p^k) = \underbrace{p^k}_{\substack{\#\text{ of all}\\ \text{naturals} \leq \\ p^k}} - \underbrace{p^{k-1}}_{\substack{\#\text{ of all}\\ \text{naturals}\\ \text{not coprime}\\ \text{to } p^k}}$$

<u>Theorem</u> Euler function is multiplicative in a sense

$$\boxed{\begin{array}{c}\varphi(nm) = \varphi(n)\varphi(m) \\ \text{whenever } \; n \perp m\end{array}}$$

<u>Proof</u> difficult, omitted

<u>Corollary</u> If $n = pq$ where p, q are different prime numbers, then

$$\varphi(n) = (p-1)(q-1)$$

This is expression used in RSA coding

<u>Proof</u>:
$$\varphi(pq) \underset{\substack{\uparrow \\ p \perp q}}{=} \varphi(p)\varphi(q) = (p-1)(q-1)$$

$\square$

Multiplicativity enables to compute Euler function for any natural number.

<u>Exercise</u>: Find $|\mathbb{Z}_{105}^{\times}| = \varphi(105)$

$$105 = 5 \cdot 21 = 5 \cdot 7 \cdot 3$$

$105 = 5 \cdot 21 = 5 \cdot 7 \cdot 3$

$\varphi(105) = 4 \cdot 6 \cdot 2 = 48$

Euler theorem: Consider $a, n \in \mathbb{N}$, $a \perp n$. Then

$$\boxed{a^{\phi(n)} \equiv 1 \pmod{n}}.$$

For $n = p$ prime we obtain Fermat little theorem. So we shall have another proof of Fermat theorem.

Proof: Let $G = (\mathbb{Z}_n^\times, \cdot)$

If $a \perp n$ then $[a] \in G$. By Theorem (T) above we have

$$a^{|G|} = \underset{\substack{\uparrow \\ \text{unit}}}{e}.$$

In our case

$$[a^{\phi(n)}] = [a]^{\phi(n)} = [1]$$

or equivalently

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

$\square$

Proposition $(\mathbb{Z}_p^\times, \cdot)$ is cyclic whenever p is prime

Proof: Difficult, omitted

If p is not prime then this does not hold:

$n = 8$:

$$\mathbb{Z}_8^{\times} = \{[1],[3],[5],[7]\}$$

$$[3]^2 = [1]$$

$$[5]^2 = [1]$$

$$[7]^2 = [1]$$

So all elements, except for $[1]$, has order 2.

4.4. Lattices and Boolean algebras

Let us recall that a lattice is a poset $(L, \leq)$ in which there exists supremum and infimum of any pair of elements

Notation: $\sup\{a,b\} = a \vee b$
$\inf\{a,b\} = a \wedge b$

This are the operations on L satisfying the following rules:

- $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ associativity
- $a \wedge b = b \wedge a \quad a \vee b = b \vee a$ commutativity
- $a \wedge (a \vee b) = a \quad a \vee (a \wedge b) = a$ absorbtion law

Definition: Let $(L, \wedge, \vee)$ be a lattice. Then an element 0 is called the least element if

$$0 \leq a \quad \forall a \in L$$

An element 1 is called the greatest element if

$$a \leq 1 \quad \forall a \in L.$$

0 - bottom

1 - top

Vizualization: $\quad a \leq b \ : \quad a \to b$

and if there is no c with $\quad \begin{array}{c} b \\ | \\ a \end{array}$

$$a \leq c \leq b$$

Then $a \leq b$ if there is a path from a to b

Examples: $\bullet \ (\mathbb{R}, \leq)$

$$a \cup b = \max(a, b)$$

$$a \wedge b = \inf(a, b)$$

There is no greatest and least element

$\bullet \quad ([a, b], \leq) \qquad a < b$

$0 = a$

$1 = b$

$\bullet \quad X$ - nonempty set

$P(X)$ - subsets of X with inclusion $\subseteq$

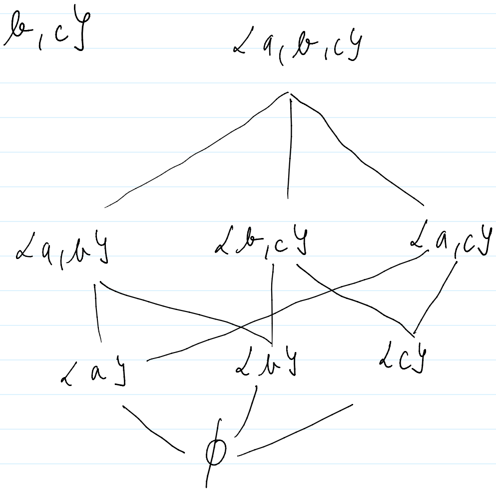
$$Z \vee Y = Z \cup Y$$

$$Z \wedge Y = Z \cap Y$$

$0 = \emptyset$

$1 = X$

$X = \{a, b, c\}$



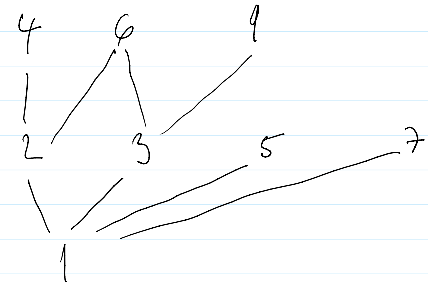
• $(\mathbb{N}, \preceq_d)$ $\qquad$ $n \preceq_d m$ if $n | m$

$0 = 1$

1 - does not exist

$n \vee m = lcm(n, m)$

$n \wedge m = gcd(n, m)$



• p is a prime number if and only if

$p \wedge q = 1$ for all $q = 1, 2, 3, \dots, p-1$

Definition a lattice L is distributive if

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (b \vee c)$$

- One law implies the other one. Indeed, assume the first one

$$(a \vee b) \wedge (a \vee c) = \big[(a \vee b) \wedge a\big] \vee \big[(a \vee b) \wedge c\big] =$$

$$= a \vee \big[(a \vee b) \wedge c\big] =$$

$$= a \vee \big[(a \wedge c) \vee (b \wedge c)\big] =$$

$$= \big[a \vee (a \wedge c)\big] \vee \big[b \wedge c\big] =$$

$$= a \vee (b \wedge c)$$

Examples:

- $(P(X), \subseteq)$ is a distributive lattice

- X – linear space

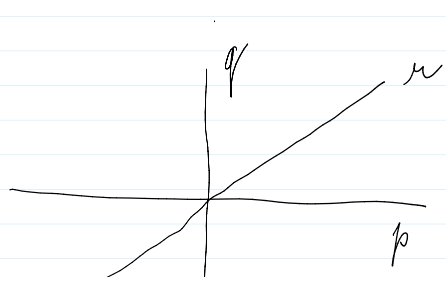
  $(L(X), \subseteq)$ ... linear subspaces of X

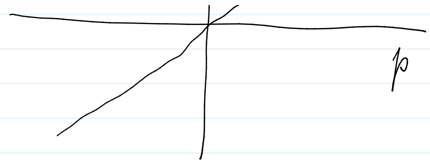
$$Y \vee Z = Y + Z = \{ y + z \mid y \in Y,\ z \in Z \}$$

$$Y \wedge Z = Y \cap Z$$

It is not distributive in general:

$X = \mathbb{R}^2$





$$r \wedge \underbrace{(p \vee q)}_{= X} = r \wedge X = r$$

$$\underbrace{(r \wedge p)}_{= \{0\}} \vee \underbrace{(r \wedge q)}_{= \{0\}} = \{0\}$$

<u>Definition</u>: Let $(L, \leq)$ be a lattice with $\mathbb{0}, \mathbb{1}$.

Let $a \in L$. Then $b \in L$ is **a complement of a**

if
$$a \wedge b = \mathbb{0}$$
$$a \vee b = \mathbb{1}$$

<u>Proposition</u>: If $(L, \leq)$ is a distributive lattice, then there is at most one complement of any $a \in L$.

<u>Proof</u>: Suppose b and c are complements of a.

Then
$$b = \underbrace{(a \vee b)}_{= 1} \wedge b = (a \vee c) \wedge b = (a \wedge b) \vee (b \wedge c)$$
$$= \mathbb{0} \vee (b \wedge c) = b \wedge c$$

In the same way
$$c = b \wedge c$$

so $\qquad c = b$

<u>Notation</u>: L - distributive lattice with $\mathbb{0}, \mathbb{1}$

Then $a^{\perp} \equiv$ complement of a

Example: • $(X, \mathcal{P}(X))$

$$A \in \mathcal{P}(X) : A^{\perp} = X \setminus A$$

Definition: Boolean algebra is

a distributive lattice with $\mathbf{0}$ and $\mathbf{1}$

such that every element has (unique) complement

Example: For any nonempty set X is

$(\mathcal{P}(X), \subseteq)$ a Boolean algebra

with $\mathbf{0} = \emptyset$

$\mathbf{1} = X$

$A^{\perp} = X \setminus A$

Smallest Boolean algebra

$$B_2 = \{0, 1\}$$

$0 \vee 0 = 0$

$0 \vee 1 = 1$

$0 \wedge 1 = 0 \wedge 0 = 0$

$0^{\perp} = 1$

$1^{\perp} = 0$.

$\equiv$ Subsets of 1-point sets

$$X = \{x\}$$

$$P(X) = \{\emptyset, X\}.$$

$$B_n \equiv B_2 \times B_2 \times \cdots \times B_2$$

$$(a_1, a_2, \dots, a_n) \le (b_1, b_2, \dots, b_n) \iff a_i \le b_i \quad \forall i$$

$$(a_1, a_2, \dots, a_n) \vee (b_1, b_2, \dots, b_n) = (a_1 \vee b_1, a_2 \vee b_2, \dots, a_n \vee b_n)$$

$$(a_1, a_2, \dots, a_n) \wedge (b_1, b_2, \dots, b_n) = (a_1 \wedge b_1, a_2 \wedge b_2, \dots, a_n \wedge b_n).$$

$$(a_1, a_2, \dots, a_n)^{\perp} = (a_1^{\perp}, a_2^{\perp}, \dots, a_n^{\perp})$$

- All finite Boolean algebras are isomorphic to B_n.

  (without proof)
