1. Def of group

We construct a "group" from the basic conception "set"

Let S be a non-empty set

Def 1.1. If $a \cdot b$ is defined for all $a, b \in S$, then $\cdot$ is said to be a binary operation on S

Def 1.2. If $\forall\, a, b \in S$, $a \cdot b \in S$, then $\cdot$ is said to be a closed binary operation. i.e. $\cdot : S \times S \to S$ s.t. $(a, b) \mapsto a \cdot b$

Def 1.3. If $\forall\, a, b, c \in S$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, ($\cdot$ is a binary operation), the $\cdot$ is said to be associative.

Def 1.4 A non empty set S together with a associative closed binary operation $\cdot$, is a Semigroup. denoted by $(S, \cdot)$

E.g. $(\mathbb{Z}_{>0}, +)$ $(\{p^i \mid i \geq n\}, \times)$ where $n \in \mathbb{Z}_{>0}$, p prime $(S, \cdot)$

Def 1.5 A monoid is a semigroup which contains a two-sided identity $e \in S$ s.t $ae = ea = a$, $\forall\, a \in S$

E.g. $(\mathbb{Z}_{\geq 0}, +)$ $(\{cp^i \mid i \geq 0\}, \times)$

Exercise: this identity is unique.

pf: sps $e' \neq e$ $\forall\, a \in S$

$e' = e'e = e$ (we use "two sided" here)

Def 1.6 A group is a monoid $(S,\cdot)$ s.t $\forall a \in S$ there exist an (two-sided) inverse element $a^{-1} \in S$ s.t $a^{-1}a = aa^{-1} = e$

Ex 1. If e is two-sided then left inverse = right inverse, further inverse is unique

sps a', a'' all inverse of a. $\forall a \in S$

$$a' = a'e = a'aa'' = (a'a)a'' = ea'' = a''$$

Ex2*. Let $(S,\cdot)$ be a semigroup. satisfies:

① $\exists e \in S$ s.t $\forall a \in S$. $ae = a$ (right side identity)

② $\forall a \in S$, $\exists a' \in S$ s.t $aa' = e$ (right side inverse)

Then G must be a group. (The weaken def of group).

Step 1. we prove $\forall a \in S$, a' is also left side inverse.

for a', $\exists a''$ s.t $a'a'' = e$

Then $a'a = a'ae = a'aa'a'' = a'(aa')a'' = a'ea'' = (a'e)a'' = a'a'' = e$

Step 2. we prove e is also a left side identity.

$$ea = aa'a = a(a'a) = ae = a$$

Ex3*. If in Ex2* change right identity to left. still holds?

No, counterexample as follows:

define "$\cdot$" on S s.t $\forall x, y \in S$, $x \cdot y = y$

Then 1° fix arbitrary $a \in S$, a can by left identity

2° $\forall b \in S$, a is its right inverse

This structure is a special semigroup. called a "loop"

Ex4*. Let S be a finite semigroup, satisfying

① $\exists e \in S$ s.t $\forall a \in G$, $ae = a$ (right identity).

② $\forall a \in S$, if $ab = ac$ for some $b, c \in S$ then $b = c$ (left cancellation law)

Then S must be a group.

Only need to show a has right inverse then by Ex3* We are done.

Consider the sequence $a, a^2, \cdots$

Since G is finite, there exist r and s, $r<s$ s.t

$a^r = a^s$ then by left cancellation law

$$a^{r-1} = a^{s-1} \cdots a = a^{s-r+1}, \quad e = a^{s-r} \Rightarrow a \cdot a^{s-r-1} = e$$

$$\Downarrow \qquad \nearrow \text{left cancell} \qquad \Rightarrow a^{s-r-1} \text{ is right inverse}$$

$ae = a^{s-r+1}$

right inverse

□.

2. Subgroup. coset

Def 1. Let G be a group, $H, K \subseteq G$,

$$HK = \{hk \mid h \in H, k \in K\}$$

$$H^{-1} = \{h^{-1} \mid h \in H\}$$

$$H^n = \{h_1 \cdots h_n \mid h_i \in H\}$$

Ref 2. If $H \subseteq G$, $H \neq \emptyset$, $H^2 \subseteq H$ and $H^{-1} \subseteq H$, then $H \leq G$

Cor 3. Let G be a group. $H \subseteq G$, TFAE

(1) $H \leq G$

(2). $\forall a, b \in H$, $ab \in H$ and $a^{-1} \in H$

(3) $\forall a, b \in H$, $ab^{-1} \in H$ (or $a^{-1}b \in H$)

Def 4. Let G be a grp. $M \subseteq G$ (allow $M = \emptyset$) subgrup.

$$\bigcap_i H_i \quad , \quad M \subseteq H_i \leq G$$

is a subgrup generated by M, denoted by $\langle M \rangle$

In other words. $\langle M \rangle = \{ 1, a_1 \cdots a_n \mid a_i \in M \cup M^{-1}, n = 1, 2, \cdots \}$

If $\langle M \rangle = G$, then M is a generate system of G

or G is generated by M

if $|M| = 1$, i.e. $M = \{a\}$, and $G = \langle a \rangle$, G is called cyclic

if $\exists M \subseteq G$ s.t $\langle M \rangle = G$ and $|M| < \infty$, then

G is called finitely generated group

Obviously. finite grups are all finitely generated grup

E.g. $(\mathbb{Z}, +) = \langle 1 \rangle$ $(2\mathbb{Z}, +)$ is finitely generated

but not finite.

Cor 5 Let G be a group, $H \subseteq G$, $|H| < \infty$ then

$$H \leq G \iff H^2 \subseteq H \quad (\text{do not need } H^{-1} \subseteq H)$$

$|H| < \infty$, $\forall a \in H$, $a, a^2, \cdots \Rightarrow a^i = a^j \Rightarrow a \cdot a^{j-i-1} = e$

$H^{-1} \subseteq H$

Thm 6 Let G be a grup. $H \leq G$, $K \leq G$,

then $HK \leq G \iff HK = KH$

Def Let G be a group, $H \leq G$, $a \in G$

aH is a H left coset in G

$aH = bH \iff a^{-1}b \in H$

Thm $H \leq G$. $a, b \in G$ then

(1) $|aH| = |bH|$

(2) $aH \cap bH \neq \emptyset \Rightarrow aH = bH$

In a word, the (left) coset of H in G is a partition of G

i.e. $G = a_1H \sqcup \cdots \sqcup a_nH$ for some $a_1, \ldots, a_n$

$\{a_1, \ldots, a_n\}$ is called a (left) coset representative system of H in G. the number of different coset of H in G is called the index of H in G, denoted by $|G:H|$ or $[G:H]$

Thm 8 (Lagrange) $|G| < \infty$, $H \leq G$, then

$$|G| = |H|\,|G:H|$$

Thm 9 Let G be a group. H, K are finite subgroup of G then

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

~~4~~. **Thm 10** Let G be a finite group, $H \leq G$. $K \leq G$, then

1) $|\langle H, K\rangle : H| \geq |K : H \cap K|$

2) $|G : H \cap K| \leq |G:H|\,|G:K|$

3) If $(|G:H|, |G:K|) = 1$, then $|G : H \cap K| = |G:H| \cdot |G:K|$

And $G = HK$

Proof: 1). $HK \subseteq \langle H,K\rangle \Rightarrow \frac{|\langle H,K\rangle|}{|H|} \geq \frac{|HK|}{|H|} = \frac{|K|}{|H\cap K|}$

2). $|G:H\cap K| = |G:K|\,|K:H\cap K|$

Since $|G:H| \geq |\langle H,K\rangle : H| \geq |K:H\cap K|$

$\Rightarrow |G:H\cap K| \leq |G:K|\,|G:H|$

3). By Lagrange Thm. $|G:H| \mid |G:H\cap K|$ and $|G:K| \mid |G:H\cap K|$

Furthermore. $\because |G:H|, |G:K| = 1 \Rightarrow$ and by 2)

$$|G:H\cap K| = |G:H|\,|G:K|$$

on the orther hand.

$$|G:H\cap K| = |G:K|\,|K:H\cap K|$$

$$= |G:K|\,|HK:H|$$

$$\Rightarrow \frac{|HK|}{|H|} = \frac{|G|}{|H|} \Rightarrow G = HK.$$

Def 11 Double coset. Let $|G| < \infty$. let $H, K \leq G$. (not necessary different)

HaK, $a \in G$. is a subset of G

$HaK = \{ hak \mid h \in H, k \in K \}$ is called a double coset of H and K in G.

Thm 12 $HaK \cap HbK \neq \emptyset \Rightarrow HaK = HbK$

Based on this. $G = Ha_1K \sqcup \cdots \sqcup Ha_nK$ for some $a_1, \ldots a_n \in G$.

proof: Sps. $hak = h'bk' \in HaK \cap HbK$

$$\Rightarrow a = h^{-1}h'bk'k^{-1}$$

$$\Rightarrow HaK = Hh^{-1}h'bk'k^{-1}K = HbK \quad \square$$

Thm 3 Any double coset HaK is an union of several right cosets of H in G, the number of those H cosets is $[K : H^a \cap K]$ where $H^a = a^{-1}Ha$. For $K, \dots, [H^a : H^a \cap K]$

Let $g \in HaK$, then $gK \subseteq HaK \cdot K = HaK$

Thus $HaK = \bigcup_{\text{for some } g \in G} gK$

Suppose HaK contains n K right cosets.

Then $n = |HaK| / |K|$

$$|HaK| = |a^{-1}HaK| = |H^aK|$$

$$\Rightarrow |H^aK| = \frac{|H^a| \cdot |K|}{|H^a \cap K|} \Rightarrow [H^a : H^a \cap K]$$

actually $|H^a| = |H|$, write this H^a here is aim to let this symbol well-defined.

Since $H^a \cap K \leq H^a$ but $H^a \cap K$ may not contained in H.

3. Normal subgroup, Quotient, IsoThm (Omit), Direct product.

Def 1 If $N \leq G$ and $\forall g \in G$. $N^g \subseteq N$, then N is called the normal subgroup of G, denoted by $N \trianglelefteq G$

Prop 2 TFAE

1). $N \trianglelefteq G$

2). $N^g = N$, $\forall g \in G$ (So N is self-conjugate)

3) $N_G(N) = G$

4)* If $n \in N$, then $\underline{C(n)} \subseteq N$, i.e. N is a union of several conjugacy classes. (the conjugacy class of n)

5) $\forall g \in G$. $gN = Ng$

6) Any right coset of N in G is also a left coset.

Additionally, G and $\{e\}$ are called the trivial normal subgroup of G.

Def3 A simple group is a group has no non-trivial normal subgroup.

Since any subgroup of an abelian group is a normal subgroup.

Thus, any simple abelian group is a p-cyclic group.

Prop4 Let $N \trianglelefteq G$, $H \leq G$, then $\langle H, N \rangle = NH = HN$

($N \leq G$. $H \leq G$, $\langle H, N \rangle$ may not equal to NH, in fact. NH may not equal to HN, But if one of N, H is normal, then it's equal)

Prop5 Let $N_1, \ldots, N_s$ all normal subgroups of G

the $\bigcap_{i=1}^{s} N_i \trianglelefteq G$ and $\prod_{j=1}^{s} N_i \trianglelefteq G$

Def 6 Let G be a group. $M \subseteq G$

$$M^G = \langle m^g \mid m \in M, g \in G \rangle$$

is called the normal closure of M in G. $M^G \trianglelefteq G$

Furthermore, $M^G = \bigcap_{\substack{H_i \trianglelefteq G \\ M \subseteq H_i}} H_i$, i.e M^G is the smallest normal subgroup of G which contains M.

Def 7 Let $N \trianglelefteq G$, $\overline{G} = \{Ng \mid g \in G\}$

define $(Ng)(Nh) = N(gN)h = N(Ng)h = Ngh$

In other words. $\cdot : \overline{G} \times \overline{G} \longrightarrow \overline{G}$

$$(Ng_1, Ng_2) \mapsto Ng_1g_2$$

Under this binary operation. $(\overline{G}, \cdot)$ is a group (Check it!)

$\overline{G}$ is called the quotient group of G by N, denoted by $\overline{G} = G/N$

Def 8 direct product. (outside)

$$G \times H = \{(g, h) \mid g \in G, h \in H\}.$$

multiplication: $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$

for n groups: $G = G_1 \times \cdots \times G_n$ for $i = 1, \ldots, n$

let $H_i = \{(1, \ldots, g_i, \ldots 1) \mid g_i \in G_i\}$.

(g_i: ith position)

then $H_i \cong G_i$, and.

1) $H_i \trianglelefteq G$, $\forall i$

2) $G = \langle H_1, \dots, H_n \rangle = \prod_{i=1}^{n} H_i$ i.e. $= H_1 H_2 \cdots H_n$

3) for all $i \neq j$, elements in H_i and H_j is commutative.

4) $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = 1$, $\forall i$

5) $\forall g \in G$, $g = h_1 \cdots h_n$, $h_i \in H_i$ and this form is unique

Usually we use "inside product"

if $G = H \times K$ then $G = HK$ is natural

Consider: $\varphi: H \times K \longrightarrow HK$ is iso
$(h, k) \longmapsto hk$

and $(h_1, k_2)(h_2, k_2) = (h_1 h_2, k_1 k_2)$

$h_1 k_2 h_2 k_2$ $\qquad$ $h_1 h_2 k_1 k_2$

Consider. $H \trianglelefteq G$, $K \trianglelefteq G$, $H \cap K = \{e\}$.

if $hk \neq kh$, then $\exists\, g \in G$ s.t. $g \neq e$ and

$g = \underbrace{hkh^{-1}k^{-1}}_{k_1}$ $\quad \downarrow \Rightarrow g \in K$ $\quad \Big\downarrow \Rightarrow g \in K \cap H$ but $g \neq e$. ↯

$g = \underbrace{hkh^{-1}k^{-1}}_{h_1}$ $\quad \downarrow \Rightarrow g \in H$

Thm G is the inside direct product of its subgroups $H_1, \dots, H_n$. iff:

1) $H_i \trianglelefteq G$, $i = 1, \dots, n$

2) $G = H_1 \cdots H_n$.

3) $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = 1$, $\forall i \in \{1, \cdots n\}$.

weaken 3) $H_i \cap H_1 \cdots H_{i-1} = 1$, $i = 2, \cdots n$.

OR

1) $H_i \trianglelefteq G$, $i = 1, \cdots n$

2) $G = H_1 \cdots H_n$

4) $\forall g \in G$, $g = h_1 \cdots h_n$ where $h_i \in H_i$, and it's unique.

weaken 4) $1 = 1 \cdots 1$ is unique.

i.e if $1 = h_1 \cdots h_n$ then $h_1 = \cdots = h_n = 1$.

4. Permutations. Sym grup. elementary introduction

Joseph. J. Rotman

A first course in abstract algebra. Page. 103–122.

This part of his book. is the BEST introduction of permutations. I can't be better than him.

So just follow this book!