

# MATH 3030 ALGEBRA I

## Lecture 1

### Free groups (Motivation)

Let  $A$  be a set.

Consider the category  $\mathcal{F}^A$  with

- $\text{Obj}(\mathcal{F}^A) = \{ (j, G) : G \text{ is a group and } j : A \rightarrow G \text{ is a map} \}$
- morphisms between  $(j_1, G_1)$  and  $(j_2, G_2)$  are comm. diagrams

$$\begin{array}{ccc} G_1 & \xrightarrow{\varphi} & G_2 \\ \uparrow j_1 & & \uparrow j_2 \\ & A & \end{array}$$

s.t.  $\varphi$  is a group homomorphism

A **free group**  $F(A)$  on  $A$  is then (the group component) of an initial object in  $\mathcal{F}^A$ . As such, it's unique up to isomorphism.

## Free groups (Construction)

Given a set  $A$ , let  $A^{-1}$  be a set disjoint from  $A$  and such that there is a bijection:

$$A \xrightarrow{\sim} A^{-1}, \quad a \leftrightarrow a^{-1}$$

A **word** on  $A$  is a finite ordered list  
 $(a_1, a_2, \dots, a_n)$

which we denote by juxtaposition  
 $w = a_1 a_2 \dots a_n$

where each "letter"  $a_i$  is either an elt  $a \in A$  or an elt  $a^{-1} \in A^{-1}$ .  
The set of words on  $A$  (including the empty word) is denoted by  $W(A)$ .  
The number of letters in a word  $w \in W(A)$  is called its **length**.

Note that there may be redundancy in a word, e.g.  
 $aba^{-1}abb^{-1}bbaa^{-1}$  should be the same as  $abb$ .

To resolve this, we introduce an elementary reduction map

$$r: W(A) \rightarrow W(A)$$

$w \mapsto$  removing the first occurred (from left to right)  
pair  $aa^{-1}$  or  $a^{-1}a$  from  $w$

e.g.  $r(aba^{-1}abb^{-1}bbaa^{-1}) = abb^{-1}bbaa^{-1}$

$$r^2(aba^{-1}abb^{-1}bbaa^{-1}) = abbaa^{-1}$$

$$r^3(aba^{-1}abb^{-1}bbaa^{-1}) = abb$$

We say that  $w \in W(A)$  is a **reduced word** if  $r(w) = w$ .

Lemma If  $w \in W(A)$  has length  $n$ , then  $r^{\lfloor \frac{n}{2} \rfloor}(w)$  is reduced.

Now we can define the reduction map

$$R: W(A) \rightarrow W(A)$$

$$w \mapsto r^{\lfloor \frac{n}{2} \rfloor}(w) \text{ if } \text{length}(w) = n.$$

Let  $F(A) = \text{Im } R =$  the set of all reduced words on  $A$ .

Define a binary operation on  $F(A)$  by **juxtaposition and reduction**:

$$w \cdot w' := R(ww')$$

Thm  $F(A)$  is a group under this operation.

Sketch of Pf :

- The operation is associative: this amounts to showing that reduction of words is independent of the order of iterating cancellations of pairs  $aa^{-1}$  or  $a^{-1}a$ .
- empty word is the identity
- inverse is given by reversing order of letters and replacing  $a$  by  $a^{-1}$  (or  $a^{-1}$  by  $a$ ). #

e.g.  $F(\emptyset) = \{e\}$  and if  $A = \{a\}$  is a singleton, then  $F(A) = \langle a \rangle \cong \mathbb{Z}$ .  
But if  $|A| \geq 2$ ,  $F(A)$  is quite complicated.

Rmk : We have a natural map  $j: A \rightarrow F(A)$ ,  $a \mapsto a$ , and the pair  $(j, F(A))$  is an initial object in  $\mathcal{F}^A$ .  
So  $F(A)$  gives the free group on  $A$ .

Rmk : Similarly, given a set  $A$ , we can define  
the free abelian group on  $A$

$$\mathbb{Z}^{\oplus A} := \{f: A \rightarrow \mathbb{Z} \mid f(a) \neq 0 \text{ for only finitely many } a \in A\}$$

and the free vector space (over a field  $F$ ) on  $A$

$$F^{\oplus A} := \{f: A \rightarrow F \mid f(a) \neq 0 \text{ for only finitely many } a \in A\}$$

## Normal subgroups & Quotient groups

Given  $H < G$ , it's natural to ask if one can define a group structure on the set of left cosets  $\{aH \mid a \in G\}$  by

$$(aH) \cdot (bH) := (ab)H \quad (*)$$

Rmk: We can of course replace left cosets by right cosets in this discussion.

It turns out that this is not well-defined unless  $H$  satisfies a condition:

Def A subgroup  $H < G$  is normal iff  $aH = Ha \ \forall a \in G$ .  
We denote a normal subgroup by  $H \triangleleft G$ .

Rmk: TFAE (why?)

(a)  $H \triangleleft G$  i.e.  $aH = Ha \quad \forall a \in G$

(b)  $aH \subset Ha \quad \forall a \in G$

(c)  $aHa^{-1} \subset H \quad \forall a \in G$

(d)  $aHa^{-1} = H \quad \forall a \in G$

Thm Let  $H < G$ . Then the operation on left cosets

$$(aH)(bH) = (ab)H \quad (*)$$

is well-defined iff  $H \triangleleft G$ .

Pf: (\*) is well-defined iff  $aH = a'H \ \& \ bH = b'H \Rightarrow (ab)H = (a'b')H$   
 $\forall$  possible choices of  $a, a', b, b'$ .

iff  $(ahbh')H = (ab)H \quad \forall a, b \in G \ \& \ \forall h, h' \in H$ .

( $\Rightarrow$ ): Suppose that the operation  $(*)$  is well-defined.

This means that

$$(ahbh')H = (ab)H \quad \forall h, h' \in H \text{ and } \forall a, b \in G.$$

In particular,  $ahb \in abH \quad \forall h \in H \text{ and } \forall a, b \in G$

So  $aha^{-1} \in H \quad \forall h \in H \text{ and } \forall a \in G.$

$\Rightarrow aHa^{-1} \subset H \quad \forall a \in G.$  Hence  $H \triangleleft G.$

( $\Leftarrow$ ): Suppose that  $H$  is normal.

Let  $h, h' \in H$  and let  $a, b \in G.$

Then  $H \triangleleft G \Rightarrow \exists h'' \in H$  s.t.  $hb = bh''$

So  $ahbh' = ah''h'$  which implies  $ahbh' \in (ab)H.$



Then  $(ahbh')H \cap (ab)H \neq \emptyset$ .

So we must have  $(ahbh')H = (ab)H$ .

Since  $a, b \in G$  and  $h, h' \in H$  are arbitrary,  
this shows that  $(*)$  is well-defined. #

|| Cor Let  $H \triangleleft G$ . Then the cosets of  $H$  form a group  $G/H$ , called the quotient group of  $G$  by  $H$ , under the binary operation  $(*)$ .

Pf: Associativity follows from that in  $G$ .  $H = eH$  is the identity.  
The inverse of  $aH$  is given by  $a^{-1}H$ . #

Examples: • If  $G$  is an abelian group, then any subgroup is normal.

e.g.  $n\mathbb{Z} \triangleleft \mathbb{Z}$ ,  $\mathbb{Z} \triangleleft \mathbb{R}$  and  $W \triangleleft V$ .

$\mathbb{Z} \triangleleft \mathbb{Q} \triangleleft \mathbb{R} \triangleleft \mathbb{C}$ , and

$W < V$  for any vector subspace  $W \subset V$

Rmk  $V/W$  can be equipped with the structure of a vector space, called the quotient space of  $V$  by  $W$ .

•  $\{e\} \triangleleft G$ ,  $G \triangleleft G$ .  $G/\{e\} \cong G$ ,  $G/G \cong \{e\}$ .

• (i)  $A_n \triangleleft S_n$  for any positive integer  $n$ .

(ii) Let  $a \in D_n$  (the  $n$ -th dihedral group) be the rotation by  $\frac{2\pi}{n}$ .

Then the cyclic subgroup  $\langle a \rangle$  in  $D_n$  is normal.

(iii)  $SO_n(\mathbb{R}) \triangleleft O_n(\mathbb{R})$

More generally, if  $H < G$  has index  $[G:H] = 2$ , then  $H \triangleleft G$   
(reason:  $\forall a \in G \setminus H$ , we have  $H \cup aH = G = H \cup Ha \Rightarrow aH = Ha$ .)  
In this case,  $C/H \cong \mathbb{Z}_2$ .

- $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$

- (Non-example)

For  $S_3 = \{id, \rho, \rho^2, \mu, \rho\mu, \rho^2\mu\}$  where  $\rho = (1\ 2\ 3)$ ,  $\mu = (1\ 2)$ , and  
 $H = \langle \mu \rangle < S_3$ . We've seen that  $\rho H \neq H\rho$  and  $\rho^2 H \neq H\rho^2$ .  
So  $H$  is not normal in  $S_3$ .

## Kernel of a homomorphism

Prop Let  $\phi: G \rightarrow G'$  be a homomorphism.

(1)  $\phi(e_G) = e_{G'}$

(2)  $\forall a \in G, \phi(a^{-1}) = \phi(a)^{-1}$ .

(3)  $N \triangleleft G \Rightarrow \phi(N) \triangleleft \phi(G)$ .

(4)  $M \triangleleft G' \Rightarrow \phi^{-1}(M) \triangleleft G$ .

Pf: (3) Suppose  $N \triangleleft G$ . We already know that  $\phi(N) < G'$ .

Now  $\phi(g)\phi(N)\phi(g)^{-1} = \phi(gNg^{-1}) = \phi(N) \forall g \in G$ . So  $\phi(N) \triangleleft \phi(G)$ .

(4) Suppose  $M \triangleleft G'$ . Again we know that  $\phi^{-1}(M) < G$ .

Now  $\phi(ga g^{-1}) = \phi(g)\phi(a)\phi(g)^{-1} \in M \forall g \in G$  and  $a \in \phi^{-1}(M)$ .

So  $g\phi^{-1}(M)g^{-1} \subset \phi^{-1}(M) \forall g \in G$ . Hence  $\phi^{-1}(M) \triangleleft G$ . #

Cor For any homomorphism  $\phi: G \rightarrow G'$ ,  $\text{Ker}(\phi) \triangleleft G$ .

Examples • Recall that  $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_n$   
 $k \mapsto r := \begin{matrix} \text{remainder of } k \\ \text{when it's divided by } n \end{matrix}$   
is a surjective homomorphism.  $\text{Ker}(\phi) = n\mathbb{Z}$ .

•  $\phi: \mathbb{R} \rightarrow \text{U}(1)$   
 $t \mapsto e^{2\pi i t}$

is a surjective homomorphism.  $\text{Ker}(\phi) = \mathbb{Z}$ .

•  $\phi: \mathbb{C}^* \rightarrow \mathbb{R}_{>0}$  (use multiplication for both  
 $z \mapsto |z|$   $\mathbb{C}^* \nrightarrow \mathbb{R}_{>0}$ )

is a surjective homomorphism.

$$\text{Ker}(\phi) = \{z \in \mathbb{C}^* \mid |z| = 1\} = \text{U}(1) < \mathbb{C}^*.$$

•  $\det: \text{GL}_n(F) \rightarrow F^*$  is a surjective homomorphism.  $\text{Ker} = \text{SL}_n(F)$ .

Prop Let  $H \triangleleft G$ . Then the map  $\pi: G \rightarrow G/H$  defined by  
$$\pi(a) := aH$$
is a homomorphism with  $\text{Ker}(\pi) = H$ .

Pf:  $\forall a, b \in G, \pi(ab) = (ab)H = (aH)(bH) = \pi(a)\pi(b)$ .

So  $\pi$  is a homomorphism.

$$\text{Ker}(\pi) = \{a \in G \mid aH = H\} = H. \#$$

Hence any normal subgroup is the kernel of a homomorphism.

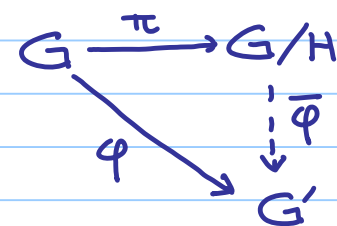
$\pi: G \rightarrow G/H$  is called the projection map or canonical map.

Thm Let  $\varphi: G \rightarrow G'$  be a homomorphism. Let  $H = \text{Ker}(\varphi)$ .

Then the map  $\bar{\varphi}: G/H \rightarrow \varphi(G)$  defined by

$$\bar{\varphi}(aH) = \varphi(a)$$

is an isomorphism such that  $\varphi = \bar{\varphi} \circ \pi$ .



Pf: First of all, we need to show that  $\bar{\varphi}$  is well-defined.

If  $aH = a'H$ , then  $a = a'h$  for some  $h \in H$ .

$$\text{So } \bar{\varphi}(aH) = \varphi(a) = \varphi(a'h) = \varphi(a')\varphi(h) = \varphi(a') = \bar{\varphi}(a'H).$$

Hence,  $\bar{\varphi}$  is well-defined.

Since  $\varphi$  is a homomorphism, we have

$$\bar{\varphi}(aH)(bH) = \bar{\varphi}(abH) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(aH)\bar{\varphi}(bH)$$

Thus  $\bar{\varphi}$  is a homomorphism.

$$\text{Ker}(\bar{\varphi}) = \{aH \in G/H \mid \varphi(a) = e'\} = \{aH \in G/H \mid a \in H\} = H.$$

So  $\bar{\varphi}$  is 1-1. It is clearly onto since  $\forall \varphi(a) \in \varphi(G)$ ,  $\bar{\varphi}(aH) = \varphi(a)$ . Hence  $\bar{\varphi}$  is an isomorphism.

Finally,  $\forall a \in G$ , we have  $(\bar{\varphi} \circ \pi)(a) = \bar{\varphi}(\pi(a)) = \bar{\varphi}(aH) = \varphi(a)$ . #

Thus, any group homomorphism  $\varphi: G \rightarrow G'$  can be decomposed as

$$G \xrightarrow{\varphi} G/\text{Ker } \varphi \xrightarrow{\cong} \text{Im } \varphi \hookrightarrow G'$$

(Actually, any set-theoretic map  $\varphi: A \rightarrow B$  can be decomposed as

$$A \xrightarrow{\varphi} \text{Im } \varphi \hookrightarrow B.)$$



Rmk: This is usually called the First Isomorphism Theorem, and is a useful tool in establishing isomorphisms.

Rmk: Given a group  $G$  and the equivalence relation  $\sim_L$  defined by  $H \triangleleft G$ , we can consider the category with

- objects = pairs  $(H, \varphi)$ , where  $H$  is a group and  $\varphi: G \rightarrow H$  is a homomorphism
- morphisms are comm. diagrams

$$\begin{array}{ccc} & G & \\ \varphi_1 \swarrow & & \searrow \varphi_2 \\ H_1 & \xrightarrow{\psi} & H_2 \end{array}$$

where  $\psi$  is a homomorphism

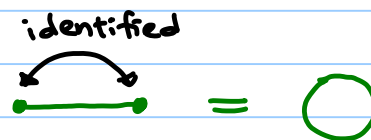
Then the pair  $(G/H, \pi)$  is an initial object in this category.

e.g. •  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

(The isom. is given by mapping  $k+n\mathbb{Z}$  to  $k$  for  $k=0,1,\dots,n-1$ .)

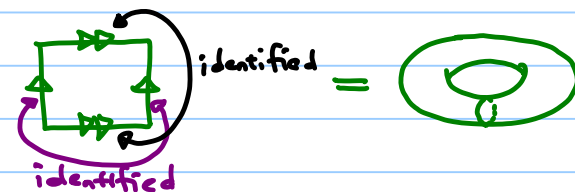
•  $\mathbb{R}/\mathbb{Z} \cong U(1)$

(The isom. is  $\mathbb{R}/\mathbb{Z} \longrightarrow U(1)$   
 $t + \mathbb{Z} \longmapsto e^{2\pi i t}$ )



For  $\mathbb{Z}^2 \triangleleft \mathbb{R}^2$ ,  $\mathbb{R}^2/\mathbb{Z}^2$  is a torus

(and similarly for higher dimensions)



•  $\mathbb{C}^*/U(1) \cong \mathbb{R}_{>0}$

•  $GL_n(F)/SL_n(F) \cong F^\times$

Example (Converse of Theorem of Lagrange is false)

We claim that  $A_4$  has no subgroup of order 6.

Pf: Suppose that  $\exists H < A_4$  with  $|H|=6$ .

Then  $H \triangleleft A_4$  and  $A_4/H \cong \mathbb{Z}_2$ .

This implies that  $\forall \sigma \in A_4, (\sigma H)(\sigma H) = H$ .

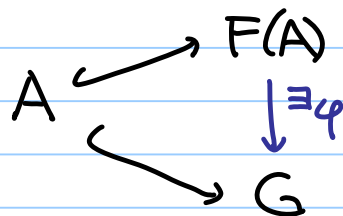
In other words,  $\sigma^2 \in H \quad \forall \sigma \in A_4$ .

Now  $(p, q, r) = (p, r, q)^2 \quad \forall$  distinct  $p, q, r \in \{1, 2, 3, 4\}$ .

There are 8 such elements and they are all inside  $H$ ,  
contradicting  $|H|=6$ .

## Presentations

Let  $G$  be a group. Then we can always find a subset  $A \subset G$  s.t.  $G = \langle A \rangle$  (at least we can take  $A = G$ ). By the universal property of free groups,  $\exists!$  group homomorphism  $\varphi: F(A) \rightarrow G$ , where  $F(A)$  is the free group on  $A$ , s.t. the following diagram commutes:



So every group (resp. abelian group) is a quotient of a free group (resp. free abelian group).

Def A **presentation** of a group  $G$  is an (explicit) isomorphism

$$G \cong F(A)/R$$

where  $F(A)$  is the free group on a set  $A$ .

Elements of  $A$  are called **generators** and elements of  $R$  are called **relations**.

If we can find a **finite** set  $A$  and a **finite** set  $R \subset F(A)$  of words s.t.  $R = \langle R \rangle$ , then we say that  $G \cong F(A)/R$  is **finitely presented**. In this case, we write  $G = \langle A | R \rangle$ .

Rmk A group can have many different presentations.

e.g. •  $F(A) = \langle A \mid \emptyset \rangle$

•  $\mathbb{Z}_n = \langle 1 \mid n \rangle$

•  $D_n = \langle a, b \mid a^n, b^2, abab \rangle$

•  $S_3 = \langle \sigma, \tau \mid \sigma^3, \tau^2, \sigma\tau\sigma\tau \rangle$