9/3/15

HW 1 due Tues Sept 15
(A mistake in Problem 3 has been corrected.)

I think we've seen enough abstract nonsense for now. Let's move on to the first real topic of the course:

Group Theory

What is a group?

There are two different points of view.

(1) A group is a structure

$$(G, \circ, 1)$$

such that G is a set, $\circ : G \times G \to G$ is a function, and $1 \in G$ is a special element satisfying three axioms:

— $\forall\, a, b, c \in G$ we have

$$a \circ (b \circ c) = (a \circ b) \circ c$$

— $\forall\, a \in G$ we have

$$a \circ 1 = 1 \circ a = a.$$

[Hence the "identity element" is unique. Given any other $1' \in G$ with

$$a \circ 1' = 1' \circ a = a$$

for all $a \in G$, it follows that

$$1' = 1' \circ 1 = 1. \;]$$

— $\forall\, a \in G$, $\exists\, b \in G$ such that

$$a \circ b = b \circ a = 1.$$

[This element b is unique. Indeed, given any $b' \in G$ such that

$$a \circ b' = b' \circ a = 1,$$

it follows that

$$\begin{aligned} b' &= b' \circ 1 \\ &= b' \circ (a \circ b) \\ &= (b' \circ a) \circ b \\ &= 1 \circ b \\ &= b. \end{aligned}$$

Since the element is unique we can give it a name. We write $b = "a^{-1}"$ and call it the inverse of a.]

---

(2) A group is the collection of automorphisms ("symmetries") of a structure X. We say that a function

$$f : X \to X$$

is an automorphism if

- f preserves structure.
- f is invertible
- its inverse preserves structure (in some cases this will be automatic)

Let $\mathrm{Aut}(X)$ be the collection of automorphisms. One can check that this is a group in the sense of (1):

1 = the identity function
$\circ$ = functional composition.

[Note that functional composition is automatically associative.]

Examples:

- $\mathrm{Aut}(\text{set } X) = S(X)$
  = permutations of X.

  called the "symmetric group"

- $\mathrm{Aut}(\text{vector space } \mathbb{R}^n) = GL_n(\mathbb{R})$.

  = invertible $n \times n$ matrices with matrix multiplication.

  called the "general linear group".
  [Hermann Weyl called it "her all-embracing majesty."]

- $\mathrm{Aut}(\text{inner product space } \mathbb{R}^n) = O(n)$.

  $= \text{orthogonal } n \times n \text{ matrices}$

  $= \{ A \in GL_n(\mathbb{R}) : A^T A = I \}$.

  called the "orthogonal group".

- $\mathrm{Aut}(\text{hermitian space } \mathbb{C}^n) = U(n)$

  $= \text{unitary matrices}$

  $= \{ A \in GL_n(\mathbb{C}) : A^* A = I \}$

  called the "unitary group".

[$A^* = \overline{A}^T$ is the complex conjugate transpose matrix.]

Note that definition (2) motivates the axioms in (1). The interaction between definitions (1) and (2) is called "representation theory".

Definition: Let $(G, \circ, 1)$ be a group.
A subset $H \subseteq G$ is called a subgroup if

- $1 \in H$.
- $\forall\, a \in H$ we have $a^{-1} \in H$.
- $\forall\, a, b \in H$ we have $a \circ b \in H$.

[In other words, if the triple $(H, \circ, 1)$ is itself a group.]

Remark: The three conditions of a a subgroup can be rolled into one.

- $\forall\, a, b \in H$ we have $a \circ b^{-1} \in H$

///

Definition: Given a group $(G, \circ, 1)$, let

$$\mathcal{L}(G) := \{ \text{subgroups of } G \}.$$

I claim that the poset $(\mathcal{L}(G), \subseteq)$ is actually a Lattice.

What do we need to show ?

Clearly the minimum and maximum are

$$0 = \{1\} \quad \text{and} \quad 1 = G.$$

What about $\wedge$ and $\vee$?

Claim: Given subgroups $H, K \subseteq G$ we have

$$H \wedge K = H \cap K.$$

Proof: It is trivial to check that the intersection $H \cap K$ is indeed a subgroup. We'll show that it satisfies the universal property of the meet. Indeed, we have $H \cap K \subseteq H$ and $H \cap K \subseteq K$. If $L \subseteq G$ is <u>any</u> subgroup satisfing

$$L \subseteq H \quad \text{and} \quad L \subseteq K,$$

it follows that $L \subseteq H \cap K$ as <u>sets</u>, hence also as <u>groups</u>. ///

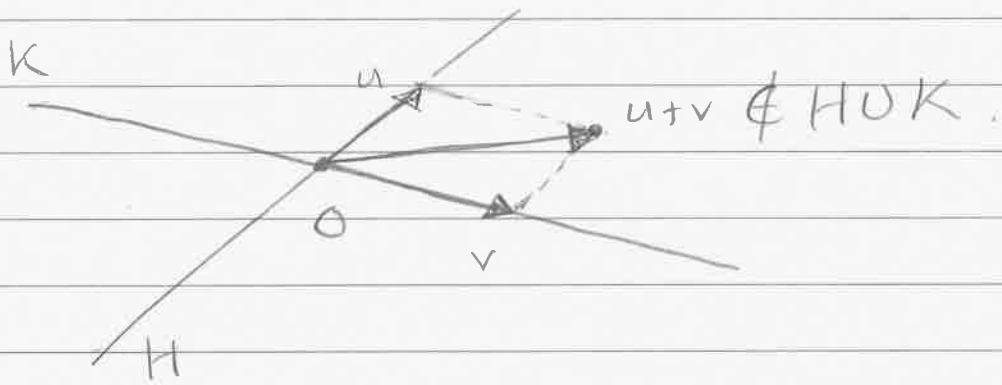
The existence of joins is not so obvious ...

Let $H, K \leq G$ be subgroups. If $H \cup K$ is also a subgroup then we will have

$$H \vee K = H \cup K,$$

but this almost never happens!

Example: Let $G = (\mathbb{R}^n, +, 0)$.
Let H and K by 1-dimensional subspaces.
If $H \neq K$ then $H \cup K$ is not a subgroup.



In linear algebra, we fix this by taking the span of H and K.

$$\begin{aligned} H \vee K &= \text{span}(H, K) \\ &= H + K \\ &= \{h + k : h \in H, k \in K\} \end{aligned}$$

///

A similar trick works for any "abelian" group.

Def: We say that group $(G, \circ, 1)$ is abelian if for all $a, b \in G$ we have

$$a \circ b = b \circ a .$$

When G is abelian we will usually call the operation "$+$" and the identity "0".

Given two subgroups H, K of an abelian group $(G, +, 0)$ we define

$$H + K = \{ h + k : h \in H, k \in K \} .$$

[Exercise: Check that this is a subgroup.]

Claim: In this case we have

$$H \vee K = H + K .$$

Proof: we will show that $H + K$ satisfies the universal property of join.

Indeed, since $h+0=h$ and $0+k=k$ we have $H \subseteq H+K$ and $K \subseteq H+K$. If L is any subgroup satisfying

$$H \subseteq L \quad \text{and} \quad K \subseteq L,$$

then for all $h \in H$ and $k \in K$ we have $h, k \in L$ and hence $h+k \in L$. It follows that

$$H+K \subseteq L. \qquad ///$$

But what if $(G, \circ, 1)$ is nonabelian?

[In a nonabelian group we will write

$$a \circ b = ab. \quad]$$

Given subgroups $H, K \subseteq G$ we can still define the subset

$$HK := \{ hk : h \in H, k \in K \} \subseteq G,$$

but this is not always a subgroup.

The best we can do is a sort of formal trick.

Lemma: Let $(P, \leq)$ be a poset. If for every subset $S \subseteq P$ (even for infinite subsets) there exists a meet

$$\bigwedge S \in P,$$

it follows that P also has arbitrary joins. [In this case we say that $(P, \leq)$ is a complete lattice.]

Proof: Given a subset $S \subseteq P$ we consider its set of upper bounds

$$S^{\vee} := \{ p \in P : s \leq p \ \forall s \in S \}.$$

Now we can define the join of S as the meet of all upper bounds of S,

$$\bigvee S := \bigwedge (S^{\vee}).$$

One can check that this satisfies the desired universal property //

Finally, we can apply this to define joins in the poset $(\mathcal{L}(G), \subseteq)$.

Def: Let G be a group and consider any subset $S \subseteq G$. We define

$$\langle S \rangle := \bigcap_{S \subseteq H} H$$

where the intersection is over all subgroups of G that contain S. One can check that an arbitrary intersection of subgroups is again a subgroup; in particular, $\langle S \rangle$ is a subgroup. We call it the subgroup of G generated by S.

In summary, the poset $(\mathcal{L}(G), \subseteq)$ is a complete lattice and the previous Lemma tells us that for all subgroups $H, K \subseteq G$ we have

$$H \vee K = \langle H \cup K \rangle.$$

//

9/8/15

HW 1 is due next Tues Sept 15 (hopefully all the mistakes have been ironed out now).

Recall from last time:

Let $(G, \circ, 1)$ be a group. We say that a subset $H \subseteq G$ is a subgroup if

$\forall a, b \in H$ we have $a \circ b^{-1} \in H$.

It is immediate that an arbitrary intersection of subgroups is again a subgroup. This allows us to make the following definition:

Given any subset $S \subseteq G$, we define

$$\langle S \rangle := \bigcap_{S \subseteq H} H,$$

where the intersection is over all subgroups containing S. This $\langle S \rangle$ is the smallest subgroup of G containing S; we call it the "subgroup generated by S".

Now let $(\mathcal{L}(G), \subseteq)$ be the set of subgroups of G, partially ordered by inclusion. The above remarks tell us that $\mathcal{L}(G)$ is a complete lattice.

Indeed, given a family of subgroups

$$\{H_i\}_{i \in I},$$

their meet is just the intersection

$$\bigwedge H_i = \bigcap H_i$$

and their join is the subgroup generated by their union

$$\bigvee H_i = \langle \bigcup H_i \rangle.$$

[If the index set is empty, $I = \emptyset$, then by convention we have

$$\bigwedge H_i = G \quad \text{and} \quad \bigvee H_i = \{1\}.$$

Compare: "The sum of no numbers is 0 and the product of no numbers is 1."]

Special Case: If $(G, +, 0)$ is an abelian group, we saw that

$$H \vee K = \langle H \cup K \rangle$$
$$= H + K$$
$$:= \{h + k : h \in H, k \in K\}.$$

If $(G, \circ, 1)$ is nonabelian, we can still define the subset

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

but in general this is not a subgroup.

Q: When is HK a subgroup?

A: Suppose that HK is a subgroup and consider $h \in H$, $k \in K$. Since $k \in HK$ and $h \in HK$ this implies that $kh \in HK$. In other words, there exist $h' \in H$ and $k' \in K$ such that

$$kh = h'k'.$$

This implies that $KH \subseteq HK$.

$\{$

Conversely, given $h \in H$ and $k \in K$ we have $hk \in HK$ and hence $(hk)^{-1} = k^{-1}h^{-1} \in HK$. In other words, there exist $h'' \in H$ and $k'' \in K$ such that

$$k^{-1}h^{-1} = h''k''.$$

Take the inverse of both sides to get

$$hk = (k'')^{-1}(h'')^{-1}.$$

This implies that $HK \subseteq KH$.

★ In summary, we conclude that the subset HK is a subgroup if and only if

$$HK = KH.$$ //

[We will have more to say about this later.]

Let G be a group and consider a subset $S \subseteq G$.

Notation: If $S = \{s_1, s_2, \cdots, s_k\}$ is finite we will write

$$\langle S \rangle =: \langle s_1, s_2, \cdots, s_k \rangle .$$

If $G = \langle s_1, s_2, \cdots, s_k \rangle$ we say that G is a finitely generated group.

If $G = \langle a \rangle$ for a single element $a \in G$ we say that G is a cyclic group. In this case we can be quite explicit:

$$G = \{ \cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots \}.$$

[Here we use the notations $a^{-n} := (a^{-1})^n$ and $a^0 := 1$. This is very convenient because it means that

$$a^m a^n = a^{m+n}$$

for all integers $m, n \in \mathbb{Z}$.]

If G is finite then there must exist integers $m < n$ such that

$$\begin{aligned} a^n &= a^m \\ a^n (a^m)^{-1} &= 1 \\ a^n a^{-m} &= 1 \\ a^{n-m} &= 1. \end{aligned}$$

In other words, there must exist a positive integer $n-m$ such that $a^{n-m} = 1$. If r is the smallest such positive integer then $\forall\, m, n \in \mathbb{Z}$ we have

$$a^n = a^m \iff r \mid n-m$$

and it follows that

$$G = \{1, a, a^2, \ldots, a^{r-1}\}.$$

[If this reminds you of modular arithmetic, good.]

More generally, given any element x of a group G we say that $|\langle x \rangle|$ is the order of the element.

The internal structure of cyclic groups is completely described by the following theorem.

★ Fundamental Theorem of Cyclic Groups:

Let G be a cyclic group of order r. Then its subgroup lattice is isomorphic to the lattice of divisors of r,

$$(\mathcal{L}(G), \subseteq) \approx (\mathrm{Div}(r), |).$$

We could prove this now, but to give the correct proof we must first discuss the external structure of cyclic groups.

what?

Remarks on Internal vs. External Structure:

Starting in the 1930s, Øystein Ore and Garrett Birkhoff advocated the point of view that the structure of a group G ↓

should be studied through its lattice $\mathcal{L}(G)$ of subgroups. They attempted to say as much as possible about the group without ever referring to its elements, but only to its subgroups and the relationships between them.

It turned out that the subgroup lattice does not contain quite enough information about G [for example, there are two nonisomorphic groups of order 8 with isomorphic subgroup lattices] and this point of view has now been absorbed into the theory of "categories".

We say that $\mathcal{L}(G)$ describes the "internal" structure of G because it encodes the interrelationships between all the subgroups of G. To describe the "external" structure of G we should say how G interacts with all other groups. This information is encoded in the category of groups.

Let Grp denote the category of groups.
This consists of

- The collection of all groups.
- The collection of all morphisms between groups.

Definition: Given two groups G and H and a function $\varphi: G \to H$, we say that φ is a group morphism (or homomorphism) if $\forall\, a, b \in G$ we have

$$\varphi(\underbrace{ab}_{\text{in } G}) = \underbrace{\varphi(a)\varphi(b)}_{\text{in } H}.$$

We say that φ is a group isomorphism if (1) it is a group morphism, and (2) it is invertible.

[In this case it follows automatically that the inverse φ^{-1} is also a morphism. Indeed, let $\varphi(a) = c$ and $\varphi(b) = d$ so that $a = \varphi^{-1}(c)$ and $b = \varphi^{-1}(d)$. Then we have $\S$

$$\begin{aligned}\varphi^{-1}(cd) &= \varphi^{-1}(\varphi(a)\varphi(b)) \\ &= \varphi^{-1}(\varphi(ab)) \\ &= ab \\ &= \varphi^{-1}(c)\varphi^{-1}(d). \quad ///\end{aligned}$$

In category theory we draw morphisms as arrows

$$G \xrightarrow{\varphi} H.$$

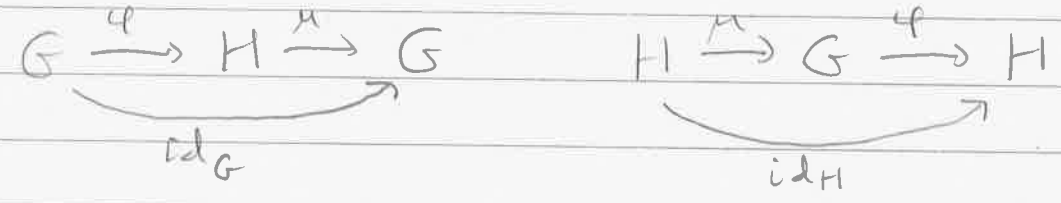
The "philosophy" of category theory is to argue with arrows and to avoid any mention of the elements of groups.

For example, we can give an arrow-theoretic definition of isomorphism.

Def: Consider an arrow $G \xrightarrow{\varphi} H$ between groups. We say that this arrow is an isomorphism if there exists another arrow

$$H \xrightarrow{\mu} G$$

such that the following diagrams commute:



In symbols, we have

$$\mu \circ \varphi = id_G \quad \text{and} \quad \varphi \circ \mu = id_H.$$

Note that the arrow μ is unique. Indeed, if $\exists\ H \xrightarrow{\mu'} G$ such that $\mu' \circ \varphi = id_G$ and $\varphi \circ \mu' = id_H$ then we have

$$\mu' = \mu' \circ id_H = \mu' \circ (\varphi \circ \mu)$$

$$= (\mu' \circ \varphi) \circ \mu = id_G \circ \mu = \mu. \quad ///$$

Since μ is unique we will write $\mu = \varphi^{-1}$ and call it the inverse of φ. When there exists an isomorphism between G and H we will write

$$G \approx H.$$

9/10/15

HW 1 due next Tues.

Last time I mentioned the word "category". Today I'll define it.

Def: A category $\mathcal{C}$ consists of

- a collection of objects
- a collection of arrows between objects (sometimes we call the arrows "morphisms" or "homomorphisms")

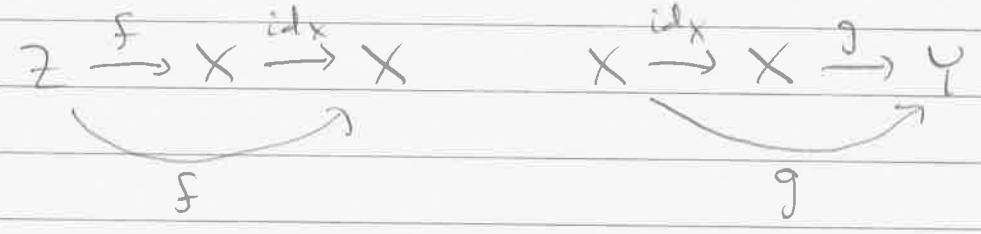
satisfying two axioms

- arrows can be composed and the composition is associative (just like functions)
- every object X has an "identity arrow" $X \xrightarrow{id_X} X$ such that for all arrows

$$Z \xrightarrow{f} X \quad \text{and} \quad X \xrightarrow{g} Y$$

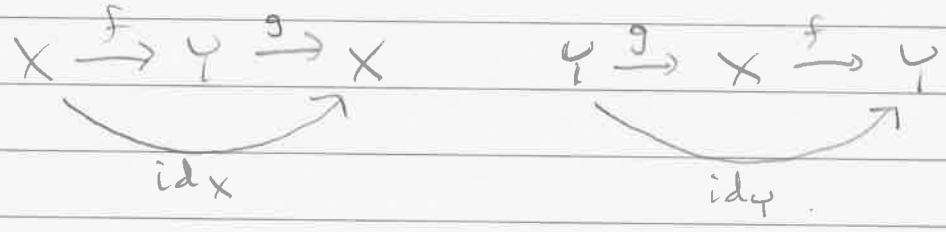
we have $id_X \circ f = f$ and $g \circ id_X = g$.

But we prefer to say this with "commutative diagrams":



Last time we saw the definition of isomorphism in a category

Def: An arrow $X \xrightarrow{f} Y$ is called an isomorphism if there exists an arrow $Y \xrightarrow{g} X$ such that



The arrow g (if it exists) is unique, so we call it f^{-1}.

Here is some common notation. Let X and Y be objects in a category $\mathcal{C}$.

We define:

- $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ = the collection of arrows from X to Y

  [a.k.a. "homomorphisms"]

- $\mathrm{End}_{\mathcal{C}}(X)$ = the collection of arrows from X to X

  [a.k.a. "endomorphisms"]

- $\mathrm{Aut}_{\mathcal{C}}(X)$ = the collection of isomorphisms from X to X.

  [a.k.a. "automorphisms"]

[Disclaimer: Without further comment I will always assume that Hom, End, and Aut are sets (i.e., not something bigger than a set). In other words, I will assume that all categories are

"locally small".]

Examples:

- A monoid is a category with one object, say, X. In this case we identify the category with the set $\mathrm{End}(X)$.

- A groupoid is a category in which every arrow is an isomorphism.

- A group is a groupoid with one object, say X. In this case we identify the category with the set $\mathrm{Aut}(X)$ $(= \mathrm{End}(X))$.

- A poset is a category such that for all objects X, Y we have

$$|\mathrm{End}(X)| = 1 \quad , \quad |\mathrm{Hom}(X,Y)| \in \{0,1\}.$$

We use the notation

$$\text{“}X \leq Y\text{”} \iff |\mathrm{Hom}(X,Y)| = 1$$

[Exercise: Verify the three axioms of partial order.]

- Given a field K, let K-Vect be the category whose objects are vector spaces over K and whose arrows are K-linear maps.

If V is an n-dimensional K-vector space then we have

$$\mathrm{End}_{K\text{-Vect}}(V) \approx \mathrm{Mat}_n(K) \text{ with matrix multiplication}$$

$$\mathrm{Aut}_{K\text{-Vect}}(V) \approx GL_n(K) \text{ with matrix multiplication.}$$

///

Enough general nonsense for now. Let's get back to the category of groups.

Let G, H be groups and consider a group homomorphism

$$\varphi : G \longrightarrow H.$$

This induces two interesting subgroups.

- The kernel

$$\ker\varphi := \{ g \in G : \varphi(g) = 1_H \}$$

Note that $\ker\varphi \subseteq G$ is a subgroup. More generally, if $K \subseteq H$ is any subgroup then its preimage

$$\varphi^{-1}(K) := \{ g \in G : \exists\, k \in K,\ \varphi(g) = k \}$$

is a subgroup of G.

Proof: Let $a, b \in \varphi^{-1}(K)$ so we have $\varphi(a) = c$ and $\varphi(b) = d$ for some $c, d \in K$.

First note that $\varphi(b)^{-1} = \varphi(b^{-1})$. Indeed, we have $1_G = 1_G 1_G$. Applying φ gives

$$\varphi(1_G) = \varphi(1_G)\varphi(1_G).$$

Then multiply on the left by $\varphi(1_G)^{-1}$ to get $\varphi(1_G) = 1_H$.

$\{$

Now apply φ to the equation $bb^{-1} = 1_G$ to get

$$\begin{aligned} bb^{-1} &= 1_G \\ \varphi(bb^{-1}) &= \varphi(1_G) \\ \varphi(b)\varphi(b^{-1}) &= 1_H \end{aligned}$$

Multiply on the left by $\varphi(b)^{-1}$ to get

$$\varphi(b^{-1}) = \varphi(b)^{-1}.$$

Finally, since $K \subseteq H$ is a subgroup we have

$$\begin{aligned} \varphi(ab^{-1}) &= \varphi(a)\varphi(b^{-1}) \\ &= \varphi(a)\varphi(b)^{-1} \\ &= cd^{-1} \qquad \in K \end{aligned}$$

and we conclude that $ab^{-1} \in \varphi^{-1}(K)$ as desired. ///

[Note that $\ker \varphi = \varphi^{-1}(\{1_H\})$.]

- The image

$$\operatorname{im}\varphi := \{ h \in H : \exists\, g \in G,\ \varphi(g) = h \}$$

Note that $\operatorname{im}\varphi \subseteq H$ is a subgroup. More generally, if $K \subseteq G$ is any subgroup then its image

$$\varphi(K) := \{ h \in H : \exists\, k \in K,\ \varphi(k) = h \}$$

is a subgroup of H.

Proof: Let $c, d \in \varphi(K)$ so we have $\varphi(a) = c$ and $\varphi(b) = d$ for some $a, b \in K$. Then since $K \subseteq G$ is a subgroup we have $ab^{-1} \in K$ and hence

$$\begin{aligned} cd^{-1} &= \varphi(a)\varphi(b)^{-1} \\ &= \varphi(a)\varphi(b^{-1}) \\ &= \varphi(ab^{-1}) \quad \in \varphi(K), \end{aligned}$$

as desired. ///

[Note that $\operatorname{im}\varphi = \varphi(G)$.]

Let $\mathcal{L}(G)$ and $\mathcal{L}(H)$ be the subgroup lattices of G and H. We have just defined two maps

$$\varphi : \mathcal{L}(G) \rightleftarrows \mathcal{L}(H) : \varphi^{-1}$$

Did you notice that this is a Galois connection? Well, it is.

Claim: For all subgroups $A \subseteq G$ and $B \subseteq H$ we have

$$\varphi(A) \subseteq B \iff A \subseteq \varphi^{-1}(B).$$

Proof: Note that

$$\begin{aligned}
\varphi(A) \subseteq B &\iff \forall a \in A,\ \varphi(a) \in B \\
&\iff \forall a \in A,\ \exists b \in B,\ \varphi(a) = b \\
&\iff \forall a \in A,\ a \in \varphi^{-1}(B) \\
&\iff A \subseteq \varphi^{-1}(B).
\end{aligned}$$

///

It follows from HW1 Problem 5 that we get an isomorphism between posets of "closed" subgroups.

Q: which subgroups are closed?

Let's examine the "closure" operators.

Claim: For all subgroups $A \leq G$, $B \leq H$ we have

- $\varphi^{-1}(\varphi(A)) = A \vee \ker\varphi$.
- $\varphi(\varphi^{-1}(B)) = B \wedge \mathrm{im}\,\varphi$.

[You will prove this on HW 2.]

It follows that the "closed" subgroups of G are those containing $\ker\varphi$ and the "closed" subgroups of H are those contained in $\mathrm{im}\,\varphi$.

Notation: For any subgroup $N \leq G$ we will write

$$\mathcal{L}(G, N) := \{ A \in \mathcal{L}(G) : N \leq A \}$$

Check that this is a sublattice of $\mathcal{L}(G)$.

Finally, we obtain the following theorem.

★ Lattice Isomorphism for Groups:

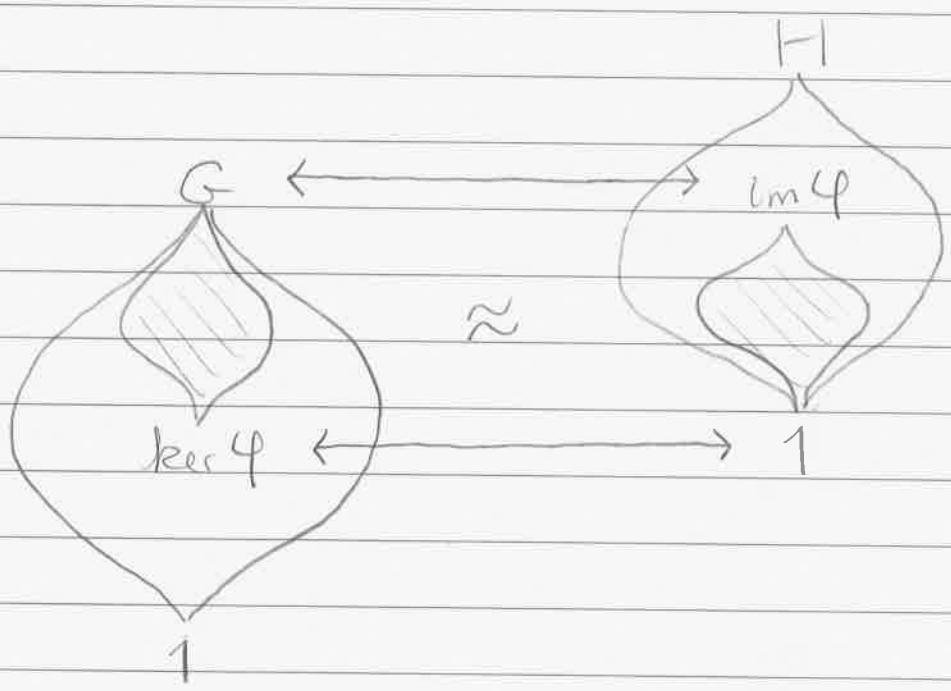
Let $\varphi: G \to H$ be a group homomorphism. This induces a Galois connection

$$\varphi : \mathcal{L}(G) \rightleftarrows \mathcal{L}(H) : \varphi^{-1},$$

which restricts to an isomorphism of lattices

$$\varphi : \mathcal{L}(G, \ker\varphi) \rightleftarrows \mathcal{L}(\mathrm{im}\varphi) : \varphi^{-1}$$

Picture:



9/15/15

HW 1 due now.
HW 2 TBA

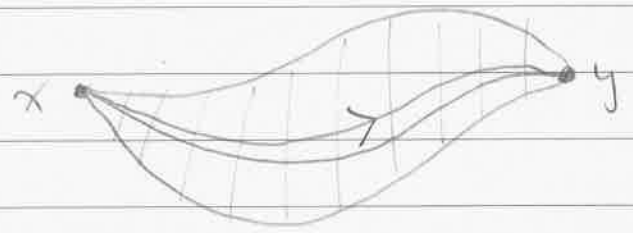
Last time I gave the following definition.

Def: A groupoid is a category in which every arrow is an isomorphism.

But I forgot to mention the most important example.

Example: Let X be a topological space. The fundamental groupoid $\pi_1(X)$ is the category with

- objects = points of X
- arrows $x \to y$ are homotopy classes of continuous paths



Arrows are composed by "concatenation".

If we choose a specific basepoint $x_0 \in X$ then we obtain the fundamental group

$$\pi_1(X, x_0) = Aut_{\pi_1(X)}(x_0).$$

[Remark: The fundamental group and groupoid are not "concretizable", i.e., it is not possible to view their objects as sets and their arrows as functions. Highbrow Translation: There does not exist a "faithful functor" to the category of sets,

$$U : \pi_1(X) \to Set.$$]

OK, enough of that for now.

Recall from last time:

Let G, H be groups and consider a group homomorphism

$$\varphi : G \longrightarrow H.$$

This induces a pair of maps

$$\varphi : \mathcal{L}(G) \rightleftarrows \mathcal{L}(H) : \varphi^{-1}$$

called image and preimage. We verified that for all subgroups $A \leq G$ and $B \leq H$ we have

$$\varphi(A) \subseteq B \iff A \subseteq \varphi^{-1}(B),$$

hence this is a Galois connection. You will show on HW 2 that the "Galois closures" are

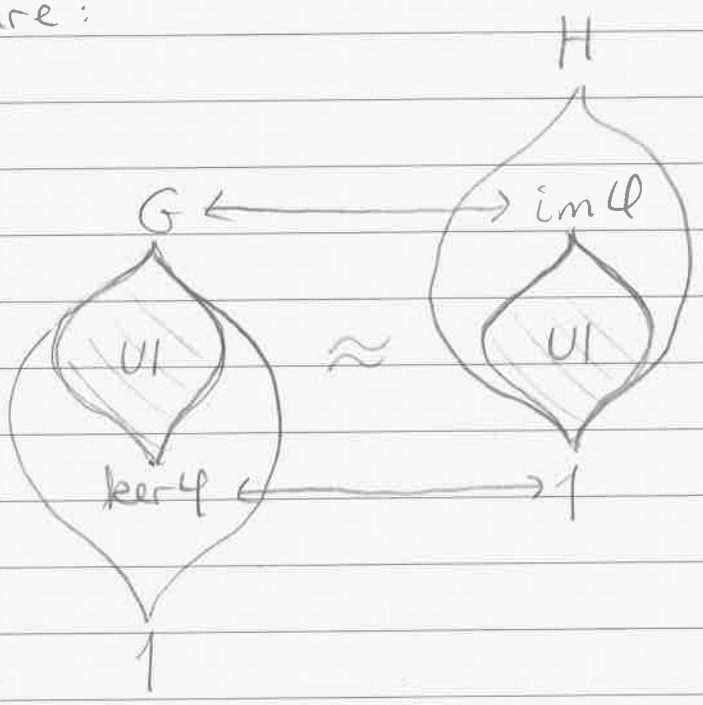
$$\varphi^{-1}(\varphi(A)) = A \vee \ker\varphi$$

$$\varphi(\varphi^{-1}(B)) = B \wedge \operatorname{im}\varphi$$

Hence we obtain an isomorphism of lattices

$$\varphi : \mathcal{L}(G, \ker\varphi) \rightleftarrows \mathcal{L}(\operatorname{im}\varphi) : \varphi^{-1}$$

Picture:



More generally, given any subgroup $N \subseteq G$ we can define the "relative" subgroup lattice

$$\mathcal{L}(G,N) := \{ A \in \mathcal{L}(G) : N \subseteq A \}.$$

Q: Under what conditions does there exist a group G' such that

$$\mathcal{L}(G,N) \approx \mathcal{L}(G') \; ?$$

To answer this we must take a detour into the theory of quotients.

Let S be a set. We say that a relation $\sim \subseteq S \times S$ is an equivalence if

- $\forall x \in S,\ x \sim x$
- $\forall x, y \in S,\ x \sim y \Rightarrow y \sim x$
- $\forall x, y, z \in S,\ x \sim y \ \& \ y \sim z \Rightarrow x \sim z$.

For each $x \in S$ we define its equivalence class

$$[x]_\sim := \{ y \in S : x \sim y \}.$$

Given $x, y \in S$, check that the following are equivalent:

i) $x \sim y$
ii) $[x]_\sim = [y]_\sim$
iii) $[x]_\sim \cap [y]_\sim \neq \emptyset$.

Now it often happens in math that we have a function $\varphi : S \to T$

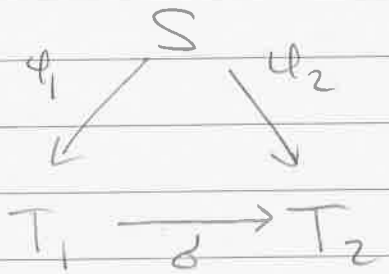
that is constant on $\sim$ classes, i.e., for all $x, y \in S$ we have

$$x \sim y \implies \varphi(x) = \varphi(y).$$

We will call any such pair (φ, T) a

"$\sim$ class function".

Now let's define a category whose "objects" are class functions (φ, T) and whose "arrows" $(\varphi_1, T_1) \xrightarrow{\sigma} (\varphi_2, T_2)$ are commutative diagrams



It turns out that there is a special object in this category called the quotient of S by $\sim$.

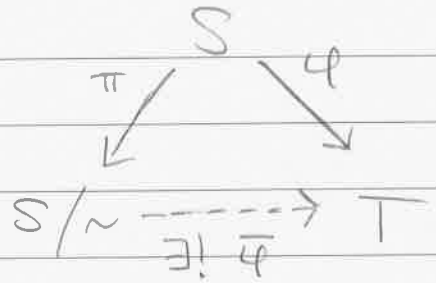
We define it as follows:

{

Let $S/\sim := \{ [x]_\sim : x \in S \}$ and
Let $\pi : S \to S/\sim$ be defined by

$$\pi(x) := [x]_\sim .$$

Theorem: The object $(\pi, S/\sim)$ is "initial" in the category of class functions
In other words, given any class function (φ, T), there exists a unique arrow



Proof: Let $[x]_\sim$ be an arbitrary element of $S/\sim$. By commutativity we must have

$$\text{(*)} \qquad \bar{\varphi}([x]_\sim) = \varphi(x).$$

Thus if $\bar{\varphi}$ exists at all then it must be unique. To show that $\bar{\varphi}$ exists we just have to show that the prescription (*) is well-defined.

Indeed, for all $[x]_\sim, [y]_\sim \in S/\sim$ we have

$$[x]_\sim = [y]_\sim \implies x \sim y \implies \varphi(x) = \varphi(y).$$ //

Def: We say that an object X in a category $\mathcal{C}$ is initial if for all objects Y we have

$$|\mathrm{Hom}_{\mathcal{C}}(X, Y)| = 1.$$

[Example: The 0 element of a poset (if it exists) is initial.]

It follows from general nonsense that initial objects are unique up to isomorphism. Thus the quotient

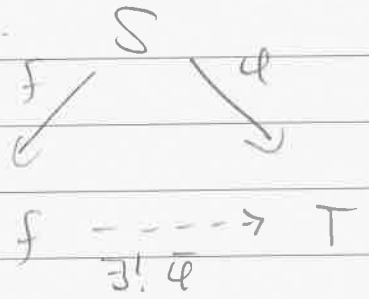
$$S \xrightarrow{\pi} S/\sim$$

is unique up to isomorphism in the category of class functions. //

Application: Let $f: S \to S'$ be any function of sets. We will define an equivalence relation on S by declaring

$$x \sim_f y \iff f(x) = f(y).$$

Note that the function $S \xrightarrow{f} \operatorname{im} f$ is constant on $\sim_f$ classes (by definition). Note also that for all "$\sim_f$ class functions" $S \xrightarrow{\varphi} T$ we have



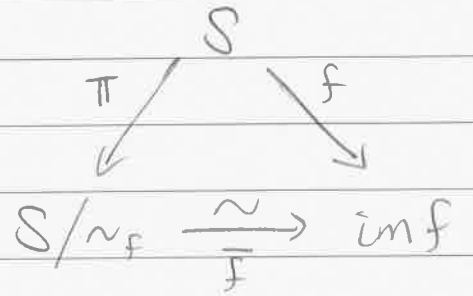
where the unique function is (well-) defined by the prescription

$$\bar{\varphi}(f(x)) := \varphi(x).$$

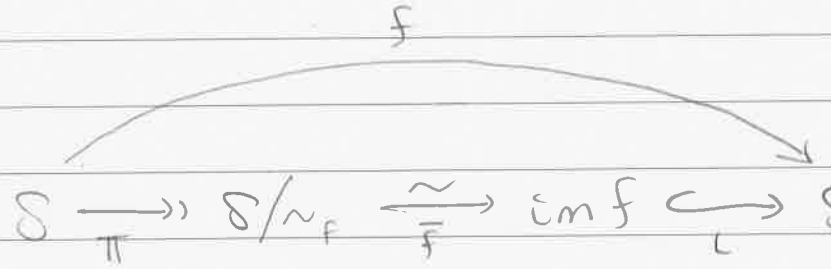
In other words, $S \xrightarrow{f} \operatorname{im} f$ is an initial object in the category of $\sim_f$ class functions.

$\{$

By uniqueness of initial objects we obtain an isomorphism of $\sim_f$ functions:



In other words we have taken the original set function $f : S \to S'$ and factored it into a surjection followed by a bijection followed by an injection:



Our goal is to lift this construction from the category of sets to the category of groups.

Let G be a group and consider any equivalence relation $\sim \subseteq G \times G$. Under what conditions is the quotient map

$$G \xrightarrow{\pi} G/\sim$$

a group homomorphism? Note that for all $a, b \in G$ we have

$$\pi(a) = [a]_\sim, \quad \pi(b) = [b], \quad \pi(ab) = [ab]_\sim.$$

Thus to turn π into a group hom we must have

$$\pi(a)\pi(b) = \pi(ab)$$
$$[a]_\sim \cdot [b]_\sim = [ab]_\sim.$$

The problem, of course, is that this "product" operation on $G/\sim$ might not be well-defined. To be well-defined in the first factor we require the following:

Given $[a]_\sim = [a']_\sim$ we have for all $b \in G$ that $[ab]_\sim = [a'b]_\sim$.

In other words, for all $a, a', b \in G$ we have

$$a \sim a' \implies ab \sim a'b.$$

[We say that the relation is right-invariant under the group operation.]

Similarly for the operation $[a]_\sim \cdot [b]_\sim = [ab]_\sim$ to be well-defined in the second factor we require that for all $a, b, b' \in G$ we have

$$b \sim b' \implies ab \sim ab'.$$

[We say the relation is left-invariant.].

So Let's make a definition.

Def: An equivalence relation $\sim$ on a group G is called G-invariant if for all $a, b, g \in G$ we have

$$a \sim b \implies ag \sim bg$$
$$a \sim b \implies ga \sim gb.$$

//

And here's the theorem.

☆ Theorem: Let $\sim$ be an equivalence relation on a group G. The prescription

$$[a]_\sim \circ [b]_\sim = [ab]_\sim$$

defines a group structure on the quotient $G/\sim$ if and only if the relation $\sim$ is G-invariant.

Proof: We already saw that group structure implies G-invariance.

Conversely, assume that $\sim$ is G-invariant. If $[a]_\sim = [a']_\sim$ and $[b]_\sim = [b']_\sim$ then by G-invariance we have

$$\left.\begin{array}{l} a \sim a' \implies ab \sim a'b \\ b \sim b' \implies a'b \sim a'b' \end{array}\right\} \implies ab = a'b'$$

hence $[ab]_\sim = [a'b']_\sim$. We conclude that the operation is well-defined.

As for group structure, associativity in $G/\sim$ is inherited from G:

For all $a, b, c \in G$ we have

$$\begin{aligned}([a]\circ[b])\circ[c] &= [ab]\circ[c] \\ &= [(ab)c] \\ &= [a(bc)] \\ &= [a]\circ[bc] \\ &= [a]\circ([b]\circ[c])\end{aligned}$$

The identity is $[1]$. Indeed, $\forall\, a \in G$ we have

$$[a]\circ[1] = [a1] = [a]$$
$$[1]\circ[a] = [1a] = [a].$$

And for all $a \in G$ we have $[a]^{-1} = [a^{-1}]$. Indeed, note that

$$[a]\circ[a^{-1}] = [aa^{-1}] = [1]$$
$$[a^{-1}]\circ[a] = [a^{-1}a] = [1].$$

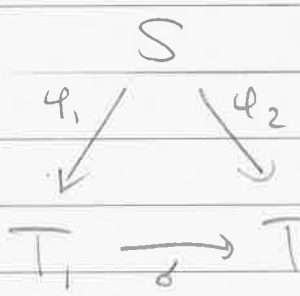
9/17/15

HW 2 still TBA.

Let $\sim$ be an equivalence relation on a set S. We say that $\varphi : S \to T$ is a class function if for all elements $x, y \in S$ we have

$$x \sim y \implies \varphi(x) = \varphi(y).$$

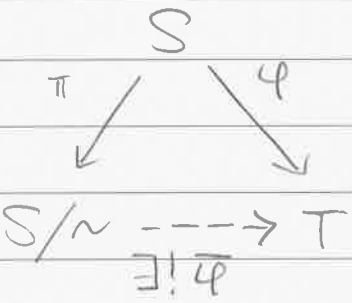
Last time we defined a category whose objects are class functions (φ, T) and whose morphisms $(\varphi_1, T_1) \to (\varphi_2, T_2)$ are functions $\delta : T_1 \to T_2$ satisfying the commutative diagram



We proved that this category has an initial object $(\pi, S/\sim)$ called the quotient of S by $\sim$.

[An initial object X in category $\mathcal{C}$ satisfies $|\mathrm{Hom}_{\mathcal{C}}(X, Y)| = 1$ for all objects Y. You will show on HW 2 that initial objects are unique up to (a unique) isomorphism.]

In other words, the quotient is defined by the "universal property"



Now if $S = G$ is a group we would like to know whether the "set quotient" $G/\sim$ can be lifted to a "group quotient".

We can define a category as before where the objects are group homomorphisms $\varphi : G \to H$ satisfying $\forall\, a, b \in G$

$$a \sim b \implies \varphi(a) = \varphi(b).$$

Q: For which equivalence relations $\sim$ does this category have an initial object?

[If an initial object $(\pi, G/\sim)$ exists we call it the quotient group.]

A: We proved last time that the quotient group exists if and only if $\sim$ is "G-invariant", i.e., for all $a, b, c \in G$ we have

$$a \sim b \implies ac \sim bc$$
$$a \sim b \implies ca \sim cb.$$

///

For this reason we are very interested in studying G-invariant equivalence relations.

☆ Theorem: Let $\sim$ be G-invariant. Then

- $[1]_\sim \subseteq G$ is a subgroup.
- For all $a, b \in G$ we have

$$a \sim b \iff a^{-1}b \in [1]_\sim$$
$$\iff ab^{-1} \in [1]_\sim$$

Proof: To show that $[1]_\sim$ is a subgroup, consider any $a, b \in [1]_\sim$. By definition this means $a \sim 1$ and $b \sim 1$. Apply b^{-1} to $b \sim 1$ to get $bb^{-1} \sim b^{-1}$, hence $b^{-1} \sim 1$. Then apply a to $b^{-1} \sim 1$ to get $ab^{-1} \sim a$. Since $ab^{-1} \sim a$ and $a \sim 1$, transitivity implies $ab^{-1} \in [1]_\sim$ as desired.

For the second part we will only prove that $a \sim b \iff ab^{-1} \in [1]_\sim$. The proof of $a \sim b \iff a^{-1}b \in [1]_\sim$ is similar.

Consider any $a, b \in G$. Then we have

$$a \sim b \overset{\cdot b^{-1}}{\implies} ab^{-1} \sim 1 \implies ab^{-1} \in [1]_\sim.$$

Conversely, we have

$$ab^{-1} \in [1]_\sim \implies ab^{-1} \sim 1 \overset{\cdot b}{\implies} a \sim b. \quad //$$

$\int$

Notation: Let $\sim$ be G-invariant and define the subgroup $N := [1]_\sim$. Then we will write

$$G/N := G/\sim$$

and we will call this the "quotient of G by the subgroup N". The equivalence relation becomes

$$a \sim_N b \iff a^{-1}b \in N \iff ab^{-1} \in N.$$

The equivalence classes are

$$\begin{aligned}
[a]_N &= \{ b \in G : a \sim_N b \} \\
&= \{ b \in G : a^{-1}b \in N \} \\
&= \{ b \in G : \exists n \in N,\ a^{-1}b = n \} \\
&= \{ b \in G : \exists n \in N,\ b = an \} \\
&= \{ an : n \in N \} \\
&=: aN.
\end{aligned}$$

We call this the left coset of N generated by $a \in G$. On the other hand, we also have

$\}$

$$[a]_N = \{ b \in G : ab^{-1} \in N \}$$
$$= \{ na : n \in N \}$$
$$=: Na.$$

We call this the right coset of N generated by $a \in G$.

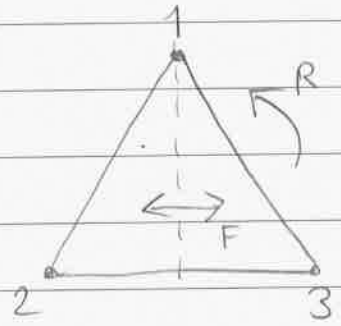
Thus for all $a \in G$ we have

$$aN = Na :$$

Definition: Any subgroup with this property will be called normal (following Galois), but a better name might be "G-invariant subgroup".

Example: Not all subgroups are normal.

Clearly all subgroups of abelian groups are normal so we must look to the smallest non-abelian group for an example. This is the dihedral group D_6 of symmetries of an equilateral triangle:



We can identify group elements with permutations of the vertices $\{1, 2, 3\}$.

Let F be the "flip" switching $2 \leftrightarrow 3$ and let R be the "rotation" $1 \to 2 \to 3 \to 1$.

The six elements of the group are

$$D_6 = \{1, R, R^2, F, FR, FR^2\}.$$

We observe that the subgroup $\langle F \rangle = \{1, F\}$ is <u>not</u> normal. Indeed, the cosets

$$\langle F \rangle R = \{R, FR\}$$
$$R\langle F \rangle = \{R, RF\}$$

are not equal because $RF = FR^2 \neq FR$.

Hence the symbol $D_6/\langle F \rangle$ can mean two different things (the set of left cosets or the set of right cosets.), neither of which is a group. ///

More generally, we can define the dihedral group D_{2n}. It is generated by two elements F & R satisfying

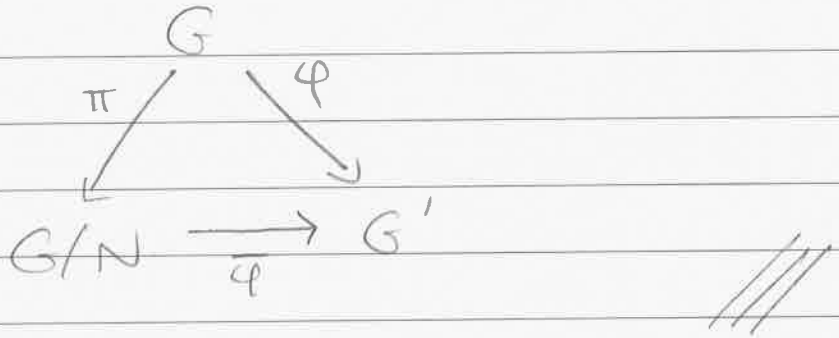
$$F^2 = R^n = 1 \quad \text{and} \quad RF = FR^{n-1}.$$

We can think of D_{2n} as the group of symmetries of a regular n-gon; where F = "flip" and R = "rotate".

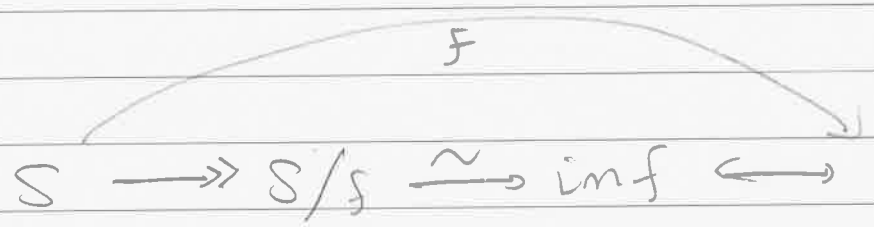
Let's summarize what we've learned.

☆ Universal Property of Group Quotient:

Let G be a group with normal subgroup N and consider the quotient homomorphism $G \xrightarrow{\pi} G/N$. If $\varphi: G \to G'$ is any group hom that is constant on cosets of N then there exists a unique group homomorphism $\overline{\varphi}: G/N \to G'$ such that the following diagram commutes



Recall that in the category of sets we used quotients to factor any set function $f : S \to S'$ as



Next time we will lift this factorization to the category of groups.

9/22/15

HW2 due Thurs Oct 1.

Recall from last time:

Let $H \subseteq G$ be a subgroup. We can use H to define two equivalence relations on G:

$$a \sim_H b \iff ab^{-1} \in H$$

$$a {}_H\!\sim b \iff a^{-1}b \in H.$$

The equivalence classes

$$[a]_{\sim_H} = Ha = \{ha : h \in H\}$$

$$[a]_{H\sim} = aH = \{ah : h \in H\}$$

are called right and left H-cosets, respectively. If the two equivalence relations coincide, that is, if we have $aH = Ha$ for all $a \in G$, then we say H is a <u>normal</u> subgroup and we write

$$H \trianglelefteq G.$$

But to prove that a subgroup is normal, it is more convenient to use the following criterion.

★ Normal Subgroup Criterion:

Let $H \subseteq G$ be a subgroup. Then we have $H \trianglelefteq G$ if and only if

$$\boxed{\forall\, a \in G,\ \forall\, h \in H,\ aha^{-1} \in H}$$

Proof: Suppose that $\forall\, a \in G, \forall\, h \in H$ we have aha^{-1}. Now consider any element $ah \in aH$. Then we have

$$ah = (aha^{-1})a \in Ha.$$

Conversely, given any element $ha \in Ha$ we have

$$\begin{aligned} ha &= a(a^{-1}ha) \\ &= a((a^{-1})h(a^{-1})^{-1}) \in aH. \end{aligned}$$

//

↓

Next suppose that $aH = Ha \ \forall a \in G$. Then given $a \in G$ and $h \in H$ we have $ah \in aH = Ha$, hence there exists $h' \in H$ such that $ah = h'a$. We conclude that

$$aha^{-1} = h' \in H. \qquad ///$$

But the easiest way to prove that a subgroup is normal is the following.

★ Normal Subgroup Criterion:

Let $H \subseteq G$ be a subgroup. Then we have $H \trianglelefteq G$ if and only if there exists a group homomorphism

$$\varphi : G \to G'$$

such that $H = \ker \varphi$.

Proof: First suppose that $H = \ker \varphi$ for some homomorphism $\varphi : G \to G'$.

Then for all $a \in G$, $h \in \ker\varphi = H$.

$$\begin{aligned}\varphi(aha^{-1}) &= \varphi(a)\varphi(h)\varphi(a^{-1}) \\ &= \varphi(a)\varphi(h)\varphi(a)^{-1} \\ &= \varphi(a)\,1\,\varphi(a)^{-1} \\ &= \varphi(a)\varphi(a)^{-1} \\ &= 1,\end{aligned}$$

hence $aha^{-1} \in \ker\varphi = H$. ///

Conversely, suppose that $H \trianglelefteq G$. We need to construct a group G' and a homomorphism $\varphi: G \to G'$ such that $H = \ker\varphi$.

We have already done the work for this. Since $H \trianglelefteq G$, the equivalence relation $\sim_H$ is G-invariant and we obtain a canonical quotient map

$$\begin{aligned}\pi: G &\to G/H \\ a &\mapsto [a]_H.\end{aligned}$$

Note that $a \in \ker\varphi \iff [a]_H = [1]_H$
$\iff a1^{-1} \in H$
$\iff a \in H$ ///

We have shown that

normal subgroup $\equiv$ kernel of group hom.

Combining this with HW 2 Problem 4 will give a purely arrow-theoretic characterization of normal subgroups.

[Constrast this with the subgroup lattice point of view. If $H \in \mathcal{L}(G)$ is normal then it is a modular element of $\mathcal{L}(G)$. By definition this means that for all $K, L \in \mathcal{L}(G)$ we have

$$\boxed{K \subseteq L \implies (H \vee K) \wedge L = (H \wedge L) \vee K}.$$

However, not all modular elements of $\mathcal{L}(G)$ are normal and in general there is no lattice-theoretic characterization of normal subgroups. This is one good reason why Ore's program was abandoned. However, the concept of "modularity" is still useful to know.]

Now we are ready to prove the category theory analogue of the Lattice Isomorphism Theorem. It is based on the following universal property of group quotients.

Let $N \trianglelefteq G$. Then a group homomorphism $\varphi: G \to G'$ is constant on N-cosets if and only if $N \subseteq \ker \varphi$.

Indeed, note that

$$[a]_N = [b]_N \iff a^{-1}b \in N.$$

Also, we have

$$\begin{aligned} \varphi(a) = \varphi(b) &\iff \varphi(a)^{-1}\varphi(b) = 1 \\ &\iff \varphi(a^{-1}b) = 1 \\ &\iff a^{-1}b \in \ker \varphi. \end{aligned}$$

Finally, note that the statement

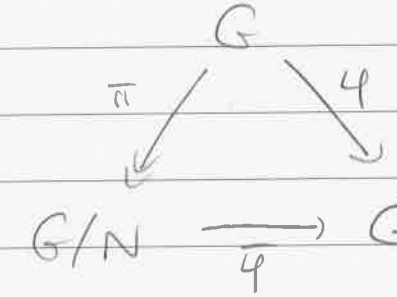
$$\forall a, b \in G, \ [a]_N = [b]_N \implies \varphi(a) = \varphi(b)$$

is equivalent to the statement

$$\forall a, b \in G,\ a^{-1}b \in N \Rightarrow a^{-1}b \in \ker\varphi,$$

which is equivalent to $N \subseteq \ker\varphi$. //

Thus if $\varphi : G \to G'$ is a group hom such that $N \subseteq \ker\varphi$, we obtain a unique set function $\overline{\varphi} : G/N \to G'$



defined by $\overline{\varphi}([a]_N) = \varphi(a)$. And this set function is actually a group homomorphism because

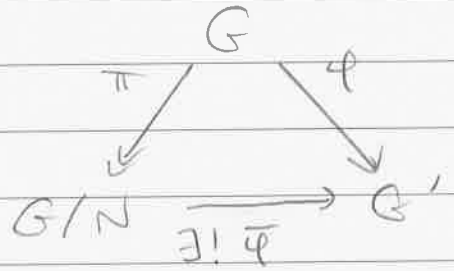
$$\begin{aligned}\overline{\varphi}([a]_N[b]_N) &= \overline{\varphi}([ab]_N) \\ &= \varphi(ab) \\ &= \varphi(a)\varphi(b) \\ &= \overline{\varphi}([a]_N)\overline{\varphi}([b]_N).\end{aligned}$$

//

In summary:

✡ Universal Property of Group Quotients:

Let $N \trianglelefteq G$. If $\varphi: G \to G'$ is a group hom. satisfying $N \subseteq \ker \varphi$ then there exists a unique group hom $\overline{\varphi}: G/N \to G'$ such that



[In other words, the map $\pi: G \to G/N$ is the initial object in a certain category of "N-homomorphisms" $\varphi: G \to G'$.]

Finally we have the famous

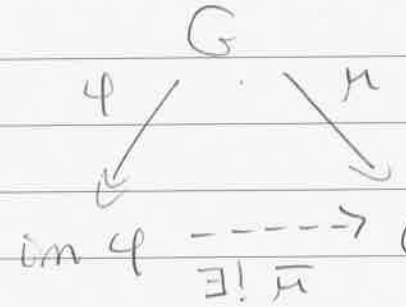
✡ First Isomorphism Theorem (E. Noether):

Let $\varphi: G \to G'$ be any group homomorphism. Then this induces a canonical group isomorphism

$$\overline{\varphi} : G/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi$$

Proof: I went through the universal properties so I could give the "correct" proof of this. We will show that the map $\varphi : G \longrightarrow \operatorname{im}\varphi$ is another initial object in the category of $\ker\varphi$-homomorphisms.

Indeed, $\varphi : G \to \operatorname{im}\varphi$ is a $\ker\varphi$-hom because $\ker\varphi \subseteq \ker\varphi$. Now let $\mu : G \to G'$ be any other group hom satisfying $\ker\varphi \subseteq \ker\mu$. We will show that



By commutativity we must have

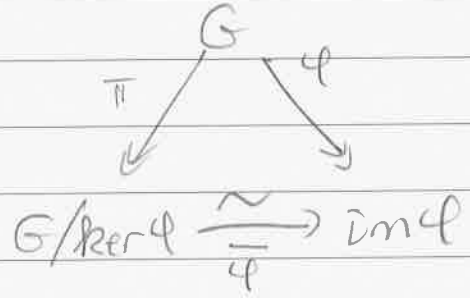
$$\overline{\mu}(\varphi(a)) = \mu(a),$$

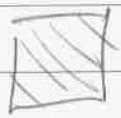
and this is well defined because

$$\begin{aligned} \varphi(a) = \varphi(b) &\Longrightarrow \varphi(a^{-1}b) = 1 \\ &\Longrightarrow a^{-1}b \in \ker \varphi \\ &\Longrightarrow a^{-1}b \in \ker \mu \\ &\Longrightarrow \mu(a^{-1}b) = 1 \\ &\Longrightarrow \mu(a) = \mu(b). \end{aligned}$$

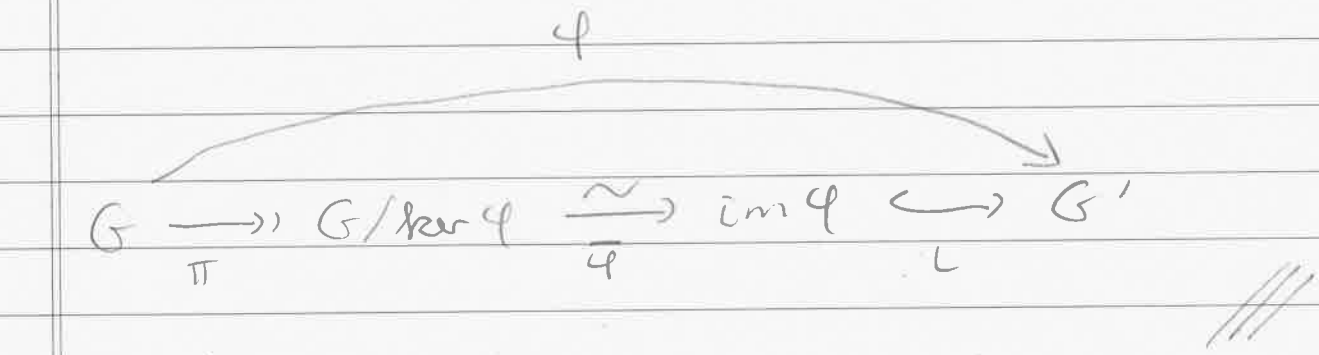
//

By uniqueness of initial objects we obtain a canonical (i.e. unique) isomorphism





In other words, for all morphisms $\varphi: G \to G'$ in the category of groups there is a canonical factorization



I think now maybe I've gone too far in the direction of category theory, so let's take a break and process what we have done.

Let $\varphi : G \to G'$ be a group hom. Combining the Lattice Isomorphism Theorem

$$\mathcal{L}(G, \ker\varphi) \approx \mathcal{L}(\operatorname{im}\varphi)$$

with the First Isomorphism Theorem

$$\operatorname{im}\varphi \approx G/\ker\varphi$$

gives us an isomorphism of Lattices

$$\mathcal{L}(G, \ker\varphi) \approx \mathcal{L}(G/\ker\varphi).$$

"excision"

This is often very useful.

Example: Let $G = \langle a \rangle$ be a cyclic group and consider the group hom

$$\varphi : (\mathbb{Z}, +, 0) \longrightarrow \langle a \rangle$$
$$s \longmapsto a^s$$

[we defined the exponential notation just for this purpose.]

The kernel is $n\mathbb{Z}$, where

$$n = \begin{cases} |\langle a \rangle| & \text{if } |\langle a \rangle| < \infty \\ 0 & \text{if } |\langle a \rangle| = \infty. \end{cases}$$

We obtain an isomorphism of groups

$$\overline{\varphi} : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \langle a \rangle$$

and an isomorphism of lattices

$$\mathcal{L}(\langle a \rangle) \approx \mathcal{L}(\mathbb{Z}/n\mathbb{Z}) \approx \mathcal{L}(\mathbb{Z}, n\mathbb{Z}).$$

The good thing about this is that we already understand the structure of

$$\mathcal{L}(\mathbb{Z}, n\mathbb{Z}).$$

Recall that the subgroups of $(\mathbb{Z}, +, 0)$ are precisely $d\mathbb{Z}$ for $d \in \mathbb{Z}$ [by the Division Algorithm] and we have

$$n\mathbb{Z} \subseteq d\mathbb{Z} \iff d \mid n.$$

Thus we obtain an isomorphism

$$\mathcal{L}(\mathbb{Z}, n\mathbb{Z}) \cong \mathrm{Div}(n)^{op}.$$

and hence,

✡ Fundamental Theorem of Cyclic Groups:

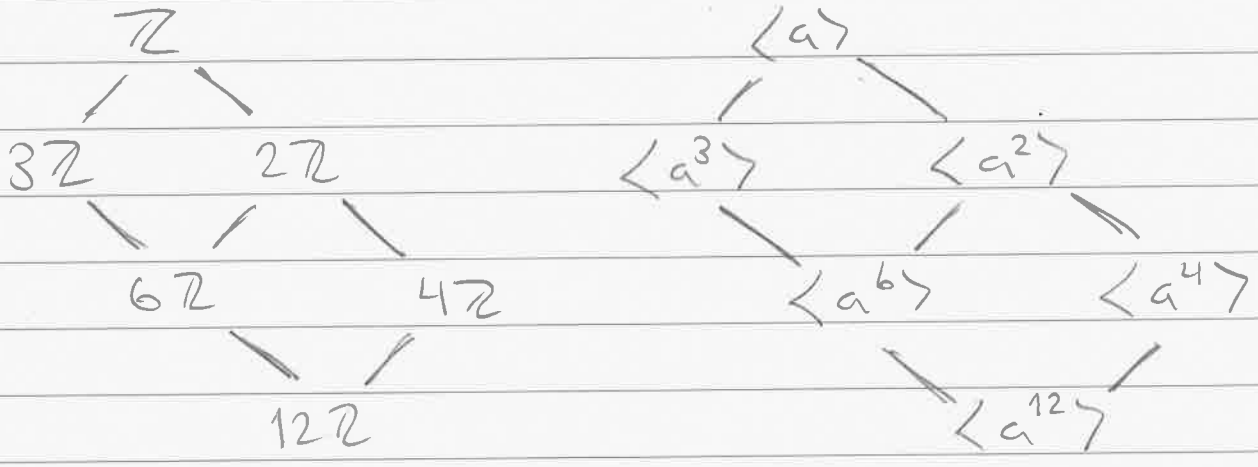
Every cyclic group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{Z}$ and we have

$$\mathcal{L}(\mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Div}(n)^{op}.$$

///

Picture for $|\langle a \rangle| = 12$:

$\mathcal{L}(\mathbb{Z}/12\mathbb{Z}) \quad \cong \quad \mathcal{L}(\langle a \rangle)$.



Remark: Certainly there are quicker ways to prove the Fundamental Theorem of Cyclic Groups, but doing it this way gave us the theorem for free.

I like getting theorems for free.

9/24/15

HW2 is due next Thurs Oct 1.

==

Let $\varphi: G \to G'$ be an arbitry group homomorphism. It will be an isomorphism in the category of groups if and only if it is bijective as a function. [Note: this doesn't work in all categories; e.g., it fails in the category of topological spaces.]

We can force φ to be surjective by taking the pullback onto the image

$$\varphi: G \twoheadrightarrow \text{im}\varphi$$

Q: How can we force φ to be injective?

A: Note that φ is injective if and only if the kernel is trivial.

[Proof: Recall that $\varphi(a) = \varphi(b) \iff a^{-1}b \in \ker\varphi$. If $\ker\varphi = \{1\}$ then $\varphi(a) = \varphi(b) \implies a^{-1}b \in \ker\varphi$ $\implies a^{-1}b = 1 \implies a = b$. If φ injective then $1^{-1}b \in \ker\varphi \implies \varphi(1) = \varphi(b) \implies b = 1$.]

Thus we can make φ injective by "killing the kernel", i.e., taking the quotient

$$\overline{\varphi} : G/\ker\varphi \hookrightarrow \operatorname{im}\varphi.$$

Now it's an isomorphism. //

Next we will discuss "products" in the category of groups.

Let $H, K \subseteq G$ be subgroups. Recall that the subset

$$HK = \{hk : h \in H, k \in K\} \subseteq G$$

is a subgroup if and only if

$$HK = KH,$$

and in this case we have $H \vee K = HK$.

↓

Definition: Given a subgroup $H \subseteq G$ we define its normalizer in G to be

$$N_G(H) := \{ g \in G : gH = Hg \}.$$

[Exercise: Prove that this is a subgroup of G; in fact, the largest subgroup of G in which H is normal.]

Claim: Let $H, K \subseteq G$ be subgroups. If either $H \subseteq N_G(K)$ or $K \subseteq N_G(H)$ then we have $HVK = HK$.

Proof: If $H \subseteq N_G(K)$ then we have

$$HK = \bigcup_{h \in H} hK = \bigcup_{h \in H} Kh = KH$$

and if $K \subseteq N_G(H)$ then we have

$$HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH.$$

In either case we conclude that $HVK = HK$.

///

Now consider the "multiplication map" from the Cartesian product set $H \times K$ into G,

$$\mu : H \times K \longrightarrow G$$
$$(h, k) \longmapsto hk.$$

Note that μ is injective if and only if $H \cap K = 1$.

Proof: Suppose $H \cap K \neq 1$, so there exists $1 \neq g \in H \cap K$. Then we have $g \in H$, $g^{-1} \in K$ and $(g, g^{-1}) \neq (1, 1)$. But

$$\mu(g, g^{-1}) = gg^{-1} = 1 = \mu(1, 1),$$

and hence μ is not injective.

Conversely, suppose that $H \cap K = 1$ and consider $(h_1, k_1), (h_2, k_2) \in H \times K$ such that $h_1 k_1 = h_2 k_2$. Then we have $h_2^{-1} h_1 = k_2 k_1^{-1} \in H \cap K$, which implies that $h_2^{-1} h_1 = k_2 k_1^{-1} = 1$, hence $h_1 = h_2$ and $k_1 = k_2$. Since $(h_1, k_1) = (h_2, k_2)$ we conclude that μ is injective.

Since the image of μ is HK, we conclude that μ is a bijection if and only if

$$\underset{\text{(injective)}}{H \cap K = 1} \quad \& \quad \underset{\text{(surjective)}}{HK = G} \quad ;$$

in other words, if and only if

$$H \wedge K = 1 \quad \& \quad H \vee K = G.$$

In this case we say that H & K are complementary subgroups of G.

If H & K are complementary then there is a unique way to define a group operation on the set $H \times K$ such that the bijection μ becomes a group isomorphism

$$\mu : H \times K \xrightarrow{\sim} G.$$

Let's investigate a few cases:

(1) Suppose that $H \wedge K = 1$, $HVK = G$, and $H \subseteq N_G(K)$.

[Note that $H \subseteq N_G(K)$ and $HVK = G$ together imply $K \trianglelefteq G$.]

Then for all $(h_1, k_1), (h_2, k_2) \in H \times K$ we must define a product

$$(h_1, k_1) \cdot (h_2, k_2) = (h, k)$$

such that

$$\mu(h_1, k_1)\,\mu(h_2, k_2) = \mu(h, k)$$
$$h_1 k_1 h_2 k_2 = hk.$$

Since $H \subseteq N_G(K)$ we have $h_2^{-1} k_1 h_2 \in K$. If we define $h = h_1 h_2 \in H$ and $k = (h_2^{-1} k_1 h_2) k_2 \in K$ then we have

$$hk = h_1 h_2 (h_2^{-1} k_1 h_2) k_2$$
$$= h_1 h_2 k_1 k_2$$

as desired. By uniqueness, this is the only solution for (h, k).

The set $H \times K$ together with the operation

$$(h_1, k_1) \circ (h_2, k_2) := (h_1 h_2, (h_2^{-1} k_1 h_2) k_2)$$

is called the (internal) semi-direct product of H & K. We will denote it by

$$H \rtimes K = (H \times K, \circ, (1,1))$$

[Mnemonic: The triangle pointing at K indicates that K is normal.]

(2) Suppose that $H \wedge K = 1$, $H \vee K = G$, and $K \subseteq N_G(H)$ [hence also $H \trianglelefteq G$].

Similar reasoning shows that the group operation on $H \times K$ is

$$(h_1, k_1) \circ (h_2, k_2) = (h_1 (k_1 h_2 k_1^{-1}), k_1 k_2).$$

In this case we write

$$H \ltimes K = (H \times K, \circ, (1,1))$$

This is also called an (internal) semi-direct product.

(3) Suppose that $H \cap K = 1$, $HK = G$, $H \subseteq N_G(K)$, and $K \subseteq N_G(H)$ [hence also $H \trianglelefteq G$ and $K \trianglelefteq G$].

Then for all $h \in H$, $k \in K$ we have $hkh^{-1} \in K$ (because $H \subseteq N_G(K)$) and $kh^{-1}k^{-1} \in H$ (because $K \subseteq N_G(H)$), hence

$$h(kh^{-1}k^{-1}) = (hkh^{-1})k^{-1} \in H \cap K.$$

Since $H \cap K = 1$ we conclude that

$$hkh^{-1}k^{-1} = 1$$
$$hk = kh.$$

This implies that the group operation on $H \times K$ is the most obvious one,

$$(h_1, k_1) \circ (h_2, k_2) = (h_1 h_2, k_1 k_2).$$

In this case we write

$$H \times K = (H \times K, \circ, (1,1))$$

and call this the (internal) direct product of H & K.

What do I mean by "internal"? This suggests that there is also an "external" perspective on direct and semi-direct products.

✡ Problem: Given two (isomorphism classes of) groups H & K, construct a group G (up to isomorphism) containing (isomorphic copies of) H & K such that

$$G = H \rtimes K, \quad G = H \rtimes K, \text{ or } G = H \times K,$$

respectively. This G will be called the "external" direct or semi-direct product of H & G.

Solution: See HW2 Problem 6. ///

So "internal" means that H & K are given as subgroups of some group G. "External" means that H & K are given abstractly and we have to construct the group G for ourselves out of thin air.

Discussion:

- Let $H, K \leq G$ be subgroups such that

$$H \wedge K = 1 \quad \& \quad HVK = G.$$

In this case we say that G is the internal product of H & K. Not all internal products are sem.-direct [I'll show you an example next time.] After doing HW2 Problem 6 you might wonder if internal products can be characterized "externally".

Yes they can. This concept is called the "knit product" or the "Zappa-Szép" product. It starts with two group homomorphisms

$$\alpha : H \longrightarrow Aut(K), \quad \beta : K \longrightarrow Aut(H)$$

[subject to certain conditions] and then defines

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 \alpha_{k_1}(h_2), \beta_{h_2}(k_1) k_2),$$

The notation

$$H \bowtie_{(\alpha,\beta)} K = (H \times K, \circ, (1_H, 1_K))$$

is used, which I think is really terrible since the symbol $\bowtie$ seems to suggest that both subgroups are normal, when in reality neither of them is normal.

If I ran the world I would switch the symbols

$$\times \leftrightarrows \bowtie$$

(Sigh...)

- The situation is much easier in the category of abelian groups. Let G be abelian and let $H, K \leq G$ be subgroups such that

$$H \wedge K = 1 \quad \& \quad H \vee K = G$$

$$\Downarrow$$

Since every subgroup of an abelian group is normal we must have $H \trianglelefteq G$ & $H \trianglelefteq K$, hence G is the direct product of H & K.
In this case we write

$$G = H \oplus K$$

and we say G is the direct sum of H & K.

[Sadly we can't use the symbol $\otimes$ for nonabelian direct products because this symbol is being used for other purposes . . .]

9/21/15

HW2 due Thursday

Recall: Let $H, K \subseteq G$ be subgroups. Then the following are equivalent:

- $HK \subseteq G$ is a subgroup,
- $H \vee K = HK$,
- $HK = KH$.

Any of these is implied by

- $H \subseteq N_G(K)$ or $K \subseteq N_G(H)$,

but this last statement is not equivalent to the others [as we will see].

Now consider the multiplication function

$$\mu : H \times K \longrightarrow G$$
$$(h, k) \longmapsto hk$$

This function is a bijection if and only if

$$H \wedge K = 1 \quad \& \quad H \vee K = G,$$

(injective) (surjective).

in which case the bijection induces a group structure on the set. There are 4 cases, but first note that since $G = H \vee K = HK$ we have

$$H \leq N_G(K) \iff K \trianglelefteq G$$
$$K \leq N_G(H) \iff H \trianglelefteq G.$$

Case 1: $H \trianglelefteq G$ and $K \trianglelefteq G$. In this case we write

$$G = H \times K$$

and say that G is the (internal) direct product of H & K.

Case 2: If $H \trianglelefteq G$ and $K \not\trianglelefteq G$ we write

$$G = H \rtimes K$$

and say G is the (internal) semi-direct product of H & K.

Case 3: If $H \trianglelefteq G$ and $K \leq G$ we write

$$G = H \rtimes K.$$

This is also called semi-direct.

Case 4: If $H \not\trianglelefteq G$ and $K \not\leq G$ we write

$$G = H \bowtie K$$

and we call this the (internal) Zappa-Szép product of H & K.

[The notation is bad but it seems kind of standard. I choose to remember it as follows: open side = normal, closed side = not normal.]

Finally, if G is abelian then all four cases collapse into one, called the direct sum of H & K:

$$G = H \oplus K.$$

Each of these situations also has an "external" characterization. That is, given two abstract groups H & K, we can construct a group G containing isomorphic copies of H & K such that

$$G = H \times K,\ H \rtimes K,\ H \ltimes K,\ \text{or}\ H \bowtie K,$$

respectively. The construction of $H \times K$ is unique up to isomorphism, but there are many ways to construct the others.

Case 1: Let H, K be groups. We define a group structure on the set $H \times K$ by

$$(h_1, k_1) \cdot (h_2, k_2) := (h_1 h_2, k_1 k_2).$$

Call this group G. There are natural injective morphisms $i_1 : H \hookrightarrow G$, $i_2 : K \hookrightarrow G$ defined by $i_1(h) = (h, 1_K)$, $i_2(k) = (1_H, k)$.

Denote the images by

$$\tilde{H} = \mathrm{im}(i_1),\ \tilde{K} = \mathrm{im}(i_2) \subseteq G.$$

Then one can check that

$$G = \tilde{H} \times \tilde{K}.$$

Cases 2 & 3: Let H, K be groups and consider any group hom $\varphi: K \to \mathrm{Aut}_{\mathrm{Grp}}(H)$.

Thus, for each $k \in K$ we get a bijection $\varphi_k: H \to H$ with the properties

- $\forall k \in K, h_1, h_2 \in H$, we have

$$\varphi_k(h_1 h_2) = \varphi_k(h_1)\varphi_k(h_2).$$

- $\forall k_1, k_2 \in K, h \in H$, we have

$$\varphi_{k_1 k_2}(h) = \varphi_{k_1}(\varphi_{k_2}(h)).$$

Then we define a group structure on the set $H \times K$ by

$$(h_1, k_1) \circ (h_2, k_2) := (h_1 \varphi_{k_1}(h_2), k_1 k_2).$$

Let G denote this group and let $\tilde{H}, \tilde{K} \subseteq G$ be the images of H & K inside G, as before.

You will show on HW2 Problem 6 that

$$G = \tilde{H} \rtimes \tilde{K}$$

Moreover, for all $h \in H$, $k \in K$ with images $\tilde{h} \in \tilde{H}$, $\tilde{k} \in \tilde{K}$ we have

$$\widetilde{\varphi_k(h)} = \tilde{k}\,\tilde{h}\,\tilde{k}^{-1}.$$

[Thus we have turned the abstract homomorphism φ into "conjugation".]

Case 4: Let H, K be groups and consider two group homomorphisms

$$\alpha : K \to Aut_{Set}(H), \quad \beta : H \to Aut_{Set}(K)^{op}$$

[The "op" in $Aut_{Set}(K)^{op}$ means the order of the group operation is reversed.]

If the maps α, β satisfy the "compatibility conditions"

- $\alpha_k(h_1 \cdot h_2) = \alpha_k(h_1) \cdot \alpha_{\beta_{h_1}(k)}(h_2)$
- $\beta_h(k_1 \cdot k_2) = \beta_{\alpha_{k_2}(h)}(k_1) \cdot \beta_h(k_2)$

then we can define a group operation on the set $H \times K$ by

$$(h_1, k_1) \circ (h_2, k_2) := (h_1 \alpha_{k_1}(h_2), \beta_{h_2}(k_1) k_2).$$

Let G denote this group. We will use the notation

$$G = H \,{}_{\alpha}\!\bowtie_{\beta} K$$

and call this the (external) Zappa-Szép product with respect to α & β

One can show [we won't!] that $G = \hat{H} \bowtie \tilde{K}$ and that every internal Zappa-Szép product arises in this way.

Examples:

(1) Consider two cyclic groups

$$\mathbb{Z}/m\mathbb{Z} = \langle a \rangle \quad \& \quad \mathbb{Z}/n\mathbb{Z} = \langle b \rangle$$

Note that a group homomorphism $\psi : \langle b \rangle \to \langle b \rangle$ is determined

by how it acts on the generator b, say

$$\varphi(b) = b^k, \text{ for some } k \in \mathbb{Z}.$$

This homomorphism will be invertible [and hence an automorphism] if and only if $\gcd(k, n) = 1$. It follows that we have an isomorphism

$$\begin{aligned} \mathrm{Aut}_{\mathrm{Grp}}(\mathbb{Z}/n\mathbb{Z}) &\cong (\mathbb{Z}/n\mathbb{Z})^\times. \\ (b \mapsto b^k) &\longleftrightarrow k. \end{aligned}$$

Now observe that a homomorphism

$$\varphi : \langle a \rangle \longrightarrow \mathrm{Aut}_{\mathrm{Grp}}(\langle b \rangle)$$

is determined by how it acts on the generator a. Thus it is determined by choosing $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ and defining

$$\varphi_a(b) = b^k.$$

One can check that the resulting semi-direct product has the presentation

$$\langle a, b : a^m = b^n = 1 \;,\; aba^{-1} = b^k \rangle .$$

[Think: What happens if $n = 0$?]

(2) Dihedral groups are a special case of this construction. Let $m = 2$ and $k = -1$. Then we have

$$\begin{aligned} D_{2n} &= \langle a \rangle \rtimes_4 \langle b \rangle \\ &= \langle a, b : a^2 = b^n = 1, \; aba = b^{-1} \rangle . \end{aligned}$$

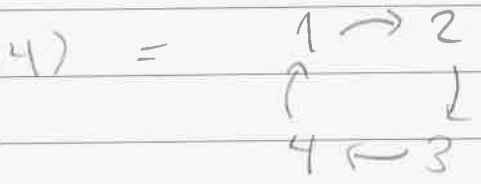
One can show that this is isomorphic to the group of symmetries of a regular n-gon in the plane.

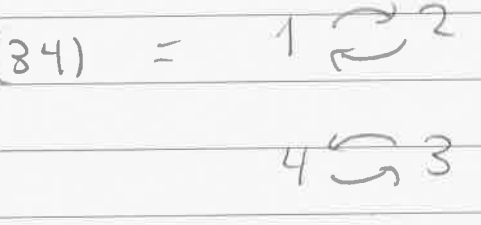
(3) Consider the set $[4] = \{1, 2, 3, 4\}$. Its automorphism group

$$S_4 := \mathrm{Aut}_{\mathrm{set}}([4])$$

is called a symmetric group. Its elements are the bijections $[4] \to [4]$, also called permutations of $[4]$.

We will denote a permutation by listing its oriented "cycles", e.g.,

$(1234) =$ 

$(12)(34) =$ 

$(123)(4) =$ 

Normally we will drop singleton cycles from the notation, so that $(123) = (123)(4)$.

Now consider the subgroups

$$H = \langle (1234), (12)(34) \rangle$$
$$K = \langle (123) \rangle.$$

One can show that $H \approx D_8$, $K \approx \mathbb{Z}/3\mathbb{Z}$, and that

$\{$

$$S_4 = H \bowtie K,$$

i.e., neither subgroup is normal.

(4) Let V be a vector space over a field K. In particular, V is an abelian group. We can express this by defining a "forgetful functor"

$$grp : K\text{-}Vec \longrightarrow Grp$$

that sends each K-vector space to its underlying abelian group.
[This functor "forgets" how to do scalar multiplication.].

Recall that the general linear group is defined by

$$GL(V) := Aut_{K\text{-}vec}(V).$$

This automatically gives us a group homomorphism

$$\{$$

$$\varphi : GL(V) \longrightarrow Aut_{Grp}(grp(V)).$$

That is, for all $X \in GL(V)$ and $\alpha, \beta \in V$ we have

$$X(\alpha + \beta) = X\alpha + X\beta .$$

The resulting semi-direct product is called the general affine group

$$\boxed{GA(V) := GL(V) \rtimes_{\varphi} grp(V)}$$

we will discuss its geometric meaning later.