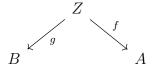
We discuss a little bit more before moving on to "abstract nonsense".

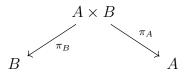
Recall that we have the universal property of the product, where something is a product if maps to projections factor through the product. Diagramatically, create a category whose morphisms are the σ such that the below diagram commutes,

$$\begin{array}{c}
Z_1 \\
\downarrow \sigma \\
B \xleftarrow{g_1} Z_2 \xrightarrow{f_2} A
\end{array}$$

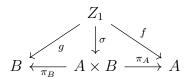
and the objects are things of the type



Then notice that, in this cattegory, the product



Is final, with morphisms



Where $\sigma(z) = (f(z), g(z))$. Here it is clear that the product map is unique, so this truly is final.

Definition 0.1. We say that a category C has products if $\forall A, B \in \text{Obj}(C)$, then $C_{A,B}$ has a final object. in SET, final objects are disjoint unions.

1 Groups

Definition 1.1 (Group). G is a set with a closed binary operation

$$(\cdot):G\times G\to G \quad \cdot (g,h)\mapsto g\times h$$

such that

- $1. \cdot is associative$
- 2. $\exists e_G \in G$ such that $\forall g \in G \ g \cdot e = e \cdot g = g$
- 3. We get inverses: $\forall g \in G$, there exists $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e_G$.

Example 1.2. The trivial group. Yep.

Example 1.3. $(\mathbb{Z}, +)$, $(\mathbb{C}, +)$, $(\pm 1, \cdot)$. Notice that all of these groups are abelian.

Example 1.4. Matrix groups: $(GL_n(F), \cdot)$, the multiplicative group of invertible $n \times n$ matrices over a field. Notice that matrix multiplication doesn't commute: a trivial fact.

Proposition 1.5. Both the identity and g^{-1} are unique.

Proof. Trivial. Suppose $\exists e_1, e_2$ both identities for the sake of contradiction. But then their product blah blah. And likewise for inverses.

Notation. By associativity, we can justify that

$$g^n = \underbrace{g \cdot g \cdot \dots \cdot g}_{n \text{times}}$$

As always, a group is called *Abelian* if the binary operation is commutative.

Example 1.6. The Commutator group for a non-abelian group is such that the binary op. is

$$[a,b] = aba^{-1}b^{-1}$$

Likewise the commutator subgroup is a subgroup generated by all commutators of elements from G.

Definition 1.7. The order of an element $g \in G$ is finite if $\exists n \in \mathbb{N}$ such that $g^n = \text{Id}$. The order of the element is the least such n. An element has infinite order otherwise.

Lemma 1.8. If $g^n = e$ for some n > 0, then |g| divides n.

Proof. Trivial exercise in number theory.

Corollary 1.9.

$$g^N \Leftrightarrow N$$
 is a multiple of $|g|$.

Definition 1.10. |G| is the number of elements in G, potentially ∞ .

Proposition 1.11. If gh = hg then |gh| divides lcm(|g|, |h|)

Example 1.12. The Symmetric group S_n with order n!. Notice that permutational composition goes in lexicagraphic order, which stinks. Also obviously S_n is not generally (in fact hardly ever) abelian. If so prompted, we can investigate the structure of S_3 , and write down a presentation of 6 generators.

Example 1.13. The Dihedral groups D_n are the groups that are isometries of a regular n-sided polygon¹ in \mathbb{R}^2 .

Example 1.14. Also of course we have the cyclic groups $\mathbb{Z}/n\mathbb{Z}$ which we will write as cosets under addition of cosets.

Likewise we can define $(\mathbb{Z}/p\mathbb{Z})^*$, the multiplicative group mod p. This is a group because trust me. Notice that it's kinda hard to find generators for this in general. It is sometimes cyclic.

Notice that groups together with group homomorphisms form a category called GRP.

$$\begin{array}{ccc} G \times G & \xrightarrow{\varphi \times \varphi} & H \times H \\ & \downarrow \cdot_G & & \downarrow \cdot_H \\ G & \xrightarrow{\varphi} & H \end{array}$$

https://www.youtube.com/watch?v=fV7zFzhqYps