- It's time for us to move onto a fresh topic which has had an enormous impact on both theory and applications.
- A *binary operation* on a set S is a function $\varphi : S \times S \longrightarrow S$. Essentially it's a way of combining a pair of elements in S (in a specific order) to get a result in S. Typically we eschew the function notation and write instead $s * t$ for $\varphi(s, t)$. Examples might be multiplication or addition of numbers, or combinations of rotations and reflections in three dimensional space.
- A *group* is a non-empty set G together with a binary operation satisfying*

  (i) $a * (b * c) = (a * b) * c \quad \forall\, a, b, c \in G$

  (ii) $\exists\, e \in G$ such that $a * e = a = e * a \quad \forall\, a \in G$

  (iii) $a \in G \implies \exists\, a' \in G$ such that $a * a' = e = a' * a$
- Typically we'll write a^{-1} for a', and write 1 for e (although we might choose to use 0 if working with addition on numbers, just for our sanity!).
- A group is said to be *Abelian* if it also satisfies the *commutative* axiom

  (iv) $a * b = b * a \quad \forall\, a, b \in G$
- Standard examples are $\mathbb{Z}$ under addition, $\mathbb{Q}^*$ and $\mathbb{R}^*$ under multiplication**, $\mathbb{Z}_5^*$ but not $\mathbb{Z}_6^*$ under multiplication (*why is 6 bad?*), and for a non-commutative example, the set comprising all rotations about the origin and all reflections through lines through the origin in the plane. We'll consider many more examples as we work through this material.

---

* These axioms are called *associative, identity,* and *inverse,* respectively.

** Recall that the use of the star here means deletion of 0, so $\mathbb{R}^* = \mathbb{R} - \{0\}$.

- Of course, once we have a structure, we can play the usual games with structures and functions amongst them.
- A *subgroup* H of a group G is a subset of H which is itself a group (using the same binary operation as G).* Given any non-empty subset $S \subseteq G$, we can extend S to a subgroup of G by 'multiplying' its various elements together until it becomes self-contained and has all its inverses. In this situation we say the subgroup H is *generated* by S, and will write $H = \langle S \rangle$.
  - *Example*: Let $G = \mathbb{Z}_{12}$ under addition, and let $S = \{4, 6\}$, then since $4 + 4 = 8$, $4 + 8 = 0$, $4 + 6 = 10$. $4 + 10 = 2$, etc.. In the end, we get $H = \langle 4, 6 \rangle = \{0, 2, 4, 6, 8, 10\}$.
  - Let G = { all acts of permuting *4* things }. Clearly, it seems reasonable to assume that { all acts of permuting *3* things } should be a subgroup of G, since any permutation of just *3* things can be thought of as a permutation of *4* things where one of the things is kept fixed, and so must be self-contained.
- The *permutation group* S_n is the group of all permutations** of *n* objects. Let's illustrate this in the case of $n = 5$.
  - Certainly there are $5! = 120$ possible permutations of the five objects *a, b, c, d, e* (*5* choices for the first one, leaving *4* options for the second, *3* for the third, *2* for the fourth, and only *1* for the last one).
  - *Notation*: We'll denote the act of moving, for example, *abcde* to *baced* by the 'symbol' (*12*)(*3*)(*45*), which we interpret as meaning "swap the things in *positions 1* and *2*, leave *position 3* fixed, and swap the things in *positions 4* and *5*". Then the 'symbol' (*134*)(*25*) means "cycle the things in positions *1*, *3* and *4*, and swap those in positions *2* and *5*". Notice that the first example permutation is its own inverse, and the second one, when performed *6* times, get us back to the identity action.
  - The subsets { (*12*) , (*23*) } and { (*12*) , (*34*) } each generate their own subgroups of S_5. You might like to try writing out the multiplication table for S_4 and seeing if you can spot the subgroups sitting inside it.

---

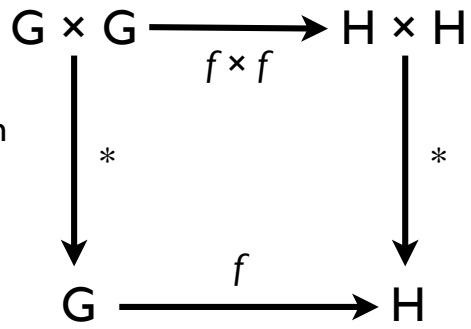
* A consequence of this is that H must also contain the identity of G.

** We abuse notation and language by using the word *permutation* both for the end product of moving stuff around, as well as the actual *act* of moving them.

- Functions between groups G and H are of course functions between sets, but since we have the added structure of a binary operation, it's convenient to insist that group functions *preserve* that structure. In particular, we define a group *homomorphism* $f : G \longrightarrow H$ to be a function f which also satisfies

  - $f(a *_G b) = f(a) *_H f(b)$

    Notice that in our commutative diagram, we've expressed the homomorphism condition as equivalent to saying that going across the top followed by going down the RHS yields the same answer as first going down and then going across the bottom. In other words, it doesn't matter if you multiply before mapping to H or afterwards.



- Our other function labels can be applied to homomorphisms; so *epimorphism*, *monomorphism*, *isomorphism*, *endomorphism*, and *automorphism* all carry the same additional meanings.

- Moreover, we can repeat the equivalence relation factoring that we'd done for functions once we've ensured that the relations respect the additional structure. So, for example, if we have a relation ~ defined on elements in a group G, then we get G/~ as the *set* of equivalence classes, so can try to see if it can be made into a *group* in its own right under the following natural extension of the original binary operation

  - define $*$ on G/~ by $[a] * [b] = [a * b]$

    Although this worked well for $\mathbb{Z}$ under addition, and having a ~ b iff (b – a) is divisible by *5*, this is actually less benign than it appears. Simply because we used the word 'define', doesn't automatically make it a good definition. We have to show that it's *well-defined*. In particular, since $[a]$ and $[b]$ are sets merely *labelled* by a and b, yet the definition uses those labels *explicitly*, we need to show that we'd get the same answer if those same sets had different labels. In particular, does $[a] = [a'] \text{ and } [b] = [b'] \implies [a] * [b] = [a'] * [b']$?

    Our natural definition will then only make sense if $a * b \sim a' * b'$, and that will depend on the choice of ~ .