Groups

1 Binary operations

A closed *binary operation* on a set A is a function from $A \times A$ to A. The modifier *closed* indicates that every pair of elements in A maps to another element of A, as opposed to being undefined. This, of course, is required for it to be a function.

binary operation
closed

There are loads of examples of binary operations:

- $+$, $\cdot$, and $-$ on $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}$.
- $\cup$, $\cap$, and $-$ on the powerset of any set.
- $\wedge$ and $\vee$ on any lattice.
- Matrix multiplication on $n \times n$ matrices.
- Concatenation on strings.

$\div$ is not closed on $\mathbb{R}$, $\mathbb{Q}$ or $\mathbb{Z}$ because division by zero is not defined. $\div$ is closed, however, on $\mathbb{R} - \{0\}$ and $\mathbb{Q} - \{0\}$. It is still not closed on $\mathbb{Z} - \{0\}$, though.

We will use the symbol $*$ to denote a generic binary operation. ($\cdot$ will be for plain old arithmetic multiplication, and $\times$ for cartesian product.) We know a variety of properties that binary operations may or may not have:

- *Commutativity.* $\forall\ a, b \in A,\ a * b = b * a$. $+$ on $\mathbb{Z}$ is commutative, concatenation on strings is not.
- *Associativity.* $\forall\ a, b, c \in A,\ (a * b) * c = a * (b * c)$. Concatenation on strings is associative, $-$ on $\mathbb{R}$ is not.
- *Idempotency.* $\forall\ a \in A,\ a * a = a$. $\cup$ on a powerset is idempotent, $\cdot$ on $\mathbb{Q}$ is not.

2 Semigroups

We have a special name for a set with an associative binary operation: *semigroup*. The odd name is because it's a generalization of the idea of a *group*, which gets the top billing. Here's a diverse handful of examples (most selected from the previous list): *semigroup*

- For a set A, $\mathscr{P}(A)$ with $\cup$
- Any lattice with $\vee$
- For a set A, the set of functions $\{f : A \to A\}$ with $\circ$ (composition).
- $\mathbb{Z}$ with $+$.
- For an alphabet A, the set of strings on A with concatenation.

Many semigroups (say, A with $*$) have a distinguished element e with the property that

$$\forall\ a \in A,\ a * e = e * a = a$$

We call such an element an *identity*. A semigroup that has an identity is called a *monoid*, but we won't use that term very often. Not all semigroups have an identity, but all of the examples above do; respectively: $\emptyset$, $\perp$, $f(x) = x$ (by freakish coincidence called the "identity function"), 0, and ε (that is, the empty string). *identity* *monoid*

Note that if we take the set $\mathbb{Z}^+$ with $+$, we still have a semigroup, but it no longer has an identity. Note also that on number sets with multiplication, 1 is the identity. By the way, should we say *the* identity or *an* identity? I suppose we should say *an* until we prove that

Theorem 1 *If A with $*$ is a semigroup, then e, if it exists, is unique.*

> **Proof** Suppose A with $*$ is a semigroup, and suppose further that e and e' are both identities. Then by definition of identity, $e * e' = e$ and $e * e' = e'$. By substitution, $e = e'$. □

Now we can (and should) say *the*.

3 Homomorphisms

Let A and A' be semigroups with $*$ and $*'$, respectively. Let ϕ be a function $A \to A'$. We say that ϕ is a *homomorphism* if for all $a, b \in A$, $\phi(a * b) = \phi(a) *' \phi(b)$. *homomorphism*

For example, take the sets $\{1, 2, 3\}$ and $\{1, 2\}$. Define $\phi : \mathscr{P}(\{1, 2, 3\}) \to \mathscr{P}(\{1, 2\})$ so that

$$\phi(X) = X - \{3\}$$

So, for instance, $\phi(\{1, 3\}) = \{1\}$ and $\phi(\{1, 2\}) = \{1, 2\}$. Notice

$$\begin{aligned} \phi(\{1,3\} \cup \{1,2\}) &= \phi(\{1,2,3\}) \\ &= \{1,2\} \\ &= \{1\} \cup \{1,2\} \\ &= \phi(\{1,3\}) \cup \phi(\{1,2\}) \end{aligned}$$

This makes it look like ϕ is a homomorphism, and you can probably do a quick proof of this in your head.

What's the difference between a homomorphism and an *isomorphism*? That thing about "$\phi(a * b) = \phi(a) *' \phi(b)$" is the structure-preserving (iso)morphic property for semigroups, analogous to the ones we've seen for graphs and lattices, but a homomorphism doesn't need to be a one-to-one correspondence. In the example above, ϕ isn't: $\phi(3) = \emptyset = \phi(\emptyset)$. A homomorphism lets us preserve

the structure of a semigroup even though we compress it into another semigroup that's truly smaller than the first.

Just as with groups verses semigroups, isomorphisms get top billing rather than homomorphisms. But when we prove properties of isomorphisms in the coming two weeks, make sure you take note of whether or not your proof relies on the fact the the 'morphism is one-to-one. If it *doesn't*, then the result is true for homomorphisms as well as for isomorphisms. For example:

Theorem 2 *Let A with $*$ and A' with $*'$ be monoids with identities e and e', respectively and ϕ be an isomorphism from A to A'. Then $\phi(e) = e'$*

Proof. Suppose the first sentence. Suppose further that $b \in A'$. Since ϕ is onto, there exists an $a \in A$ such that $\phi(a) = b$. Now,

$$\begin{array}{rcll} \phi(e) *' b & = & \phi(e) *' \phi(a) & \text{by substitution} \\ & = & \phi(e * a) & \text{by the (iso)morphic property} \\ & = & \phi(a) & \text{by the definition of identity} \\ & = & b & \text{by substitution again} \end{array}$$

Similarly $b *' \phi(e) = b$. Therefore, by definition of identity and the face that identities are unique, $\phi(e) = e'$. □

Did we use the fact that ϕ was a one-to-one correspondence? Well, we used onto, but not one-to-one. So, we can say, more generally,

Corollary 1 *Let A with $*$ and A' with $*'$ be monoids with identities e and e', respectively and ϕ be an onto homomorphism from A to A'. Then $\phi(e) = e'$*

Note that our earlier example, though not an isomorphism, was an onto homomorphism.