Section 2: Groups

The point of abstract algebra is to "abstract", i.e., isolate the important properties of several different contexts at once so that we can make statements that are true about all of them, and to give a name to the context so that it can be recognized and applied elsewhere. The more details and requirements we add to the context we create, the more restrictive it is, i.e., the fewer examples of it there are, but the more true and provable statements we can make about all the examples of it at once. "Semigroup" (set with associative operation) is a very general concept; there are many, many examples, and it is difficult to say much that is true about every one of them. In this section we add two conditions, giving a concept that has proved to be very general, with lots of examples, and very fruitful, with many general statements that apply to all of them.

Def: A *group* is a set G with an associative operation $*$ for which

(i) there is an element e in G such that $e * g = g = g * e$ for every element g of G, and

(ii) for each g in G there is an element g^{-1} in G for which $g * g^{-1} = e = g^{-1} * g$

The e in (i) is an *identity* for G, and the g^{-1} is an *inverse* for g in G.

We already know lots of groups, especially if the operation is some form of addition:

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ — but not $(\mathbb{Z}^+, +)$, etc., because there is no identity or inverses.

- $\mathbb{R}^n$ under vector addition, and similarly $M_{m\times n}(R)$, the set of $m \times n$ matrices with entries from $\mathbb{R}$, under matrix addition.

- The set of real-valued functions defined on a common domain D (which might be an interval $[a, b]$, but it can be any set), under pointwise addition, is a group. The identity is the constant function 0, and the inverse $-f$ of a function f is given by $(-f)(x) = -(f(x))$ for every x in D.

- For any positive integer n, $(\mathbb{Z}_n, \oplus)$ (the integers modulo n and addition mod n) form a group.

How about if the operation is some form of multiplication? Well, usually there is an identity, a 1 of some sort; but there may not be inverses, i.e., reciprocals:

- Multiplication is an associative operation on $\mathbb{R}$, and 1 is an identity for this operation; but 0 does not have an inverse in $\mathbb{R}$, so $(\mathbb{R}, \cdot)$ is not a group. Everything else has a reciprocal, though, and the product of two nonzero reals is again nonzero, so multiplication is also an operation on $\mathbb{R} - \{0\}$, and $(\mathbb{R} - \{0\}, \cdot)$ is a group. Similarly for $\mathbb{Q}$, but not $\mathbb{Z}$, because $\mathbb{Z}$ doesn't include reciprocals of its elements. In fact, the only elements of $\mathbb{Z}$ with reciprocals in $\mathbb{Z}$ are ± 1; and, sure enough, $(\{1, -1\}, \cdot)$ is a group.

- For a particular positive integer n, multiplication mod n is an associative operation on $\mathbb{Z}_n$, and 1 acts as an identity; but there are elements of Z_n — 0, for example, but also examples like 2 and 4 in $\mathbb{Z}_6$ — that have no multiplicative inverses, so $(\mathbb{Z}_n, \odot)$ is not a group. But we can recall some facts from Math 250: If k is relatively prime to n, then there are integers r, s for which $rk + sn = 1$, and hence $\overline{r} \odot k = 1$ in $\mathbb{Z}_n$ (where overbar means remainder on division by n), i.e., k has a "reciprocal" $\overline{r}$ in $\mathbb{Z}_n$. The converse also holds: If k has a "reciprocal" in $\mathbb{Z}_n$, then k is relatively prime to n. Now the product ab of two numbers a, b relatively prime to n is also relatively prime to n, and so is the remainder $\overline{ab}$, so multiplication mod n is an operation on the set $U(\mathbb{Z}_n)$ of elements of $\mathbb{Z}_n$ that are relatively prime to n, and $(U(\mathbb{Z}_n), \odot)$ is a group.

- For a particular positive integer n, we know that multiplication of $n \times n$ matrices is an associative operation on $M_n(\mathbb{R})$, and that the identity matrix (1's on the main diagonal, 0's elsewhere) is an identity for this operation. But some square matrices do not have inverses (i.e., are "singular"), so $M_n(\mathbb{R})$ is not a group. Yes, but let's be inspired by the examples above: If we look only at the $n \times n$ matrices that have inverses, do we get a group? Well, the question is whether matrix multiplication is an operation on this set, because, if so, it is clearly associative, has an identity (the identity matrix, which is its own inverse) and inverses for each of its elements. So the question becomes, is the product of two invertible matrices again invertible? In the case of square matrices, there is the logical equivalent of a big, ugly club to decide that question: the determinant. That is, a square matrix is invertible iff its determinant is nonzero, and the determinant of a product is the product of the determinants of the factors. So: If A, B are invertible $n \times n$ matrices, then $\det(A), \det(B)$ are nonzero, so $\det(AB) = \det(A)\det(B)$ is also nonzero (because the product of nonzero numbers is nonzero), so AB is invertible. Therefore, the set of invertible $n \times n$ matrices (with real entries) forms a group (which is denoted $GL(n, \mathbb{R})$ and called the *general linear group* of order n) under matrix multiplication.

Okay, we have seen the same idea three times in a row now, verified in three different ways, but always true; it is time to abstract it to get a general result. It seems to be the case that, if we have a set with an associative operation and an identity, then, even if some of the elements do not have inverses, the subset of elements that do have inverses (with respect to that operation) form a group. Well, they certainly do if combining two that have inverses, using the operation, gives another that has an inverse; because then the operation on the big set, restricted to the smaller set, is still an operation, it inherits associativity and the identity from the big set, and all the elements have inverses — if an element x has an inverse x', then x' also has an inverse, namely the original x; so x' is also in the smaller set. So let's write down the result, to establish some notation and hypotheses, and see if we can complete a proof:

Prop: Let S be a set with an associative operation $*$ and an identity e, and consider the set G of elements x of S for which there is an element x' in S with the property that $x * x' = e = x' * x$. Then G is a group under the restriction of $*$ to G.

Pf: By the discussion before the statement of the proposition, we only need to show that, if x, y in S have inverses (say x', y' respectively) in S, then $x * y$ also has an inverse in S. The first choice for an inverse of $x * y$ is $x' * y'$, but verifying $(x * y) * (x' * y') = e$ doesn't seem to work — x' is "in the way" between y and y'. So let's reverse x' and y' and see how it goes: Putting in all the ugly parens, we get

$$(x * y) * (y' * x') = x * (y * (y' * x')) = x * ((y * y') * x') = x * (e * x') = x * x' = e \ ,$$

and similarly $(y' * x') * (x * y) = e$.

[Pedagogically, it probably would have been better for me to write it out giving reasons for each step:

$$\begin{aligned}
(x * y) * (y' * x') &= x * (y * (y' * x')) && \text{(associativity)} \\
&= x * ((y * y') * x') && \text{(associativity)} \\
&= x * (e * x') && \text{(y' is an inverse of y)} \\
&= x * x' && \text{(e identity)} \\
&= e && \text{(x' is an inverse of x)}
\end{aligned}$$

I will certainly do so if I think there are questionable steps along the way, and I encourage you to do so anytime you think there might be a question about how a step is justified.]

So $y' * x'$ is an element of S that serves as an inverse for $x * y$. The $*$ of two elements in G is again in G, so G is a group under the restriction of $*$.//

So here is the kind of result we get from the abstraction process:

Cor: Let X be a set. Then the set $\mathcal{S}(X)$ of all one-to-one functions from X $\underline{\text{onto}}$ X (which are the functions X $\underline{\text{into}}$ X that have inverse functions) is a group under composition.

The group $\mathcal{S}(X)$ is called the *symmetric group* on X. Later we will study in some detail the case where $X = \{1, 2, \ldots, n-1, n\}$ for n a positive integer; in this case $\mathcal{S}(X) = \mathcal{S}_n$ is called the *symmetric group of order* n.

Cor: For any common domain D, the family of all real-valued functions on D for which $f(x) \neq 0$ for all x in D is a group under pointwise multiplication. The identity is the constant function 1, and the inverse $1/f$ of f is defined by $(1/f)(x) = 1/(f(x))$ for all x in D.

Why did I say the use of determinants to prove the invertible $n \times n$ matrices form a group is using “a big ugly club”? Because (1) it uses some results that are difficult to prove to get to something that is easy to prove, and (2) after the proof is complete, we have only proved it for matrices, not for the set of invertible elements in any semigroup. Mathematicians would call the proof I gave for the general case as more “elegant”, because it uses only the basic assumptions and gives a general result. Proving the basic facts about determinants have ugly, subscript-laden proofs, so avoiding them is good. (It also makes good sense in practice, because determinants require a lot of arithmetic to compute.)

Let’s mention a couple of other easy examples of groups:

- For any set X, $(\mathcal{P}(X), \triangle)$ is a group: For any subset A of X, $\emptyset \triangle A = A = A \triangle \emptyset$, so $\emptyset$ is an identity; and $A \triangle A = \emptyset$, so every subset of X is its own inverse (!).

- $\mathbb{R}^+$ and $\mathbb{Q}^+$ are groups under multiplication, because the product of two positive numbers is positive, and the reciprocal of a positive number is positive. So the restriction of multiplication to these sets is still an operation, and the inverses are still there.

- The set $2\mathbb{Z}$ of even integers is a group under addition, because the sum of two even numbers is even, so addition is an operation even when restricted to the even integers; and the negative of an even number is even, so the inverses of elements in the smaller set are also in the smaller set.

Of course, our text gives us some weird examples that need to be checked from scratch. Here is a similar one: Is $\mathbb{R} - \{-1\}$, under the operation $a * b = a + b + ab$, a group? The first question is whether $*$ is an operation on $\mathbb{R} - \{-1\}$, i.e. if we find the $*$ of two numbers different from -1, will the result be different from -1? Let’s see: If it were ever true that $-1 = a * b = a + b + ab$, then $-(1 + a) = (1 + a)b$, so either b would have to be -1 or $1 + a$ would have to be 0, i.e., a would have to be -1. So the $*$ of two non-(-1)’s is again a non-(-1). Next, we need to check associativity:

$$\begin{aligned}
a * (b * c) &= a * (b + c + bc) = a + (b + c + bc) + a(b + c + bc) = a + b + c + bc + ab + ac + abc \\
(a * b) * c &= (a + b + ab) * c = (a + b + ab) + c + (a + b + ab)c = a + b + ab + c + ac + bc + abc
\end{aligned}$$

and these are equal because $+$ is commutative. Is there an identity? We need, for every a in $\mathbb{R}$, $a = a * e = a + e + ae$, so $(1 + a)e = 0$, and because this has to hold for every a, we see that $e = 0$ is the only hope; and it does work: $a * 0 = a + 0 + a0 = a$ — we only need to check it on one side because $*$ is clearly commutative. Does every integer a have an inverse? Well, $0 = a * b = a + b + ab$ yields $-a = (1 + a)b$, so $b = -a/(1 + a)$ is the hope; it exists because a was not -1, and this b does work. So $(\mathbb{R} - \{-1\}, *)$ is a group.

Whatever became of the commutative property? Well, most of the groups above have had a commutative operation, but there are plenty of useful groups that do not, like $GL(n, \mathbb{R})$ and $\mathcal{S}(X)$, so we are carefully not making it part of the definition. If the operation in a group is commutative, the group is called *abelian* (sometimes capitalized), in honor of the Norwegian mathematician Niels Henrik Abel, who realized an obscure but important consequence of commutativity in groups before groups were even invented.