12.9 An example, $\mathcal{U}(n)$

Let $\mathcal{U}(n)$ be the set of all positive integers less than n and relatively prime to n. For examples, $\mathcal{U}(5) = \{1, 2, 3, 4\}$ and $\mathcal{U}(8) = \{1, 3, 5, 7\}$. (Notice that we consider 1 to be relatively prime to anything.)

Theorem 12.3 *For $n \in \mathbb{Z}^+$, $\mathcal{U}(n)$ with multiplication modulo n is a group.*

Let's take $\mathcal{U}(8)$.

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Looks closed. Everything has an inverse (itself in this case, but not always; try $\mathcal{U}(5)$ on your own). 1's the identity. We already know multiplication is associative. Let's prove it.

Proof. As mentioned already, we know that multiplication is associative and that 1 will be the identity for any kind of multiplication. We need to prove closure and inverses.

Suppose $a, b \in \mathcal{U}(n)$. The quotient-remainder theorem tells us that there exist $q, r \in \mathbb{Z}^+$ such that $a \cdot b = n \cdot q + r$, where $0 < r \leq n$. The definition of modular arithmetic says that $a \cdot b \bmod n = r$. What we need to show is that r is relatively prime with n.

Suppose r is not relatively prime with n. That means there exists an $x \in Z^+$ such that x is a common factor of r and n (ie, $x|r$ and $x|n$). That would mean $x|(n \cdot q + r)$, and hence $x|(a \cdot b)$. Then x is a factor of either a or b, and thus either a or b is not relatively prime with n; either $a \notin \mathcal{U}(n)$ or $b \notin \mathcal{U}(n)$. Contradiction. Hence r is relatively prime with n, and multiplication mod n is closed on $\mathcal{U}(n)$.

Showing inverses is a bit more complicated. First, a lemma:

Lemma 12.1 *If $a, b, c \in \mathcal{U}(n)$ and $b \neq c$, then $a * b \neq a * c$.*

Proof (of lemma). Suppose $a, b, c \in \mathcal{U}(n)$ and $b \neq c$. (Notice that it could be that $a = b$ or $a = c$.)

Suppose further that $(a \cdot b) \bmod n = (a \cdot c) \bmod n$. Then there exist q_1, q_2, and r such that $a \cdot b = q_1 \cdot n + r$ and $a \cdot c = q_2 \cdot n + r$.

Say (without loss of generality) b is the greater of the two, i.e., $b > c$. Then we can subtract equations

$$\begin{array}{rrcl} & a \cdot b & = & q_1 \cdot n + r \\ - & a \cdot c & = & q_2 \cdot n + r \\ \hline & a \cdot (b - c) & = & (q_1 - q_2) \cdot n \end{array}$$

Since a is relatively prime with n, a can't divide n, so it must divide $q_1 - q_2$. Now, solving for b:

$$b = \frac{q_1 - q_2}{a} \cdot n + c$$

Since we said $a|(q_1 - q_2)$, then $\frac{q_1 - q_2}{a} > 1$, and so $b > n$. This is a contradiction because we assumed $b \in \mathcal{U}(n)$. □

What this lemma says is that given $a \in \mathcal{U}(n)$, every element in $\mathcal{U}(n)$ must take a to something different. This further means that for every element in $\mathcal{U}(n)$, something must take a to it, simply because otherwise we'd run out of elements (technically, this uses what's called "The Pigeonhole Principle"). This has to include 1, the identity, therefore a's inverse must exist in $\mathcal{U}(n)$.

This accounts for all the requirements for $\mathcal{U}(n)$ to be a group. □

If you're frustrated by that proof, especially the part about inverses, it might be because we didn't actually tell how to find the inverse of a given a, we just said it had to exist. (In CS 243 terms, it's like proving there exists a unicorn by showing it's impossible for a unicorn not to exist, as opposed to brining a unicorn into the room.) There are other proofs of this theorem out there (mostly using stuff we haven't covered), but I don't know of a constructive one.

12.10 Cyclic subgroups

Suppose A with $*$ is a group, and $a\ inA$. Let $\langle a \rangle$ be the set $\{a^n \mid n \in \mathbb{Z}\}$ For example, if the group is $\mathbb{Q}$ with addition and $a = \frac{1}{2}$, then $\langle \frac{1}{2} \rangle$ is

$$\ldots \quad \frac{1}{2}^{-2} = -1, \quad \frac{1}{2}^{-1} = -\frac{1}{2}, \quad \frac{1}{2}^{0} = 0, \quad \frac{1}{2}^{1} = \frac{1}{2}, \quad \frac{1}{2}^{2} = 1, \frac{1}{2}^{3} = \frac{3}{2}, \quad \frac{1}{2}^{4} = 2 \quad \ldots$$

cyclic group

generator

If it so happens that $A = \langle a \rangle$ for some a, then A is called a *cyclic group* and a is called the *generator* of A. For example, 1 is the generator of $\mathbb{Z}$ with addition. It's possible that a cyclic group has more than one generator.

12.11 Permutations

In combinatorics, we think of a permutation of a set as simply a (re)arrangement of the elements in the set. It's like a way to shuffle the cards. Thus, for the set $\{1, 2, 3, 4\}$, the permutations are

1, 2, 3, 4	1, 2, 4, 3	1, 3, 2, 4	1, 3, 4, 2	1, 4, 3, 2	1, 4, 2, 3
2, 1, 3, 4	2, 1, 4, 3	2, 3, 1, 4	2, 3, 4, 1	2, 4, 1, 3	2, 4, 3, 1
3, 1, 2, 4	3, 1, 4, 2	3, 2, 1, 4	3, 2, 4, 1	3, 4, 1, 2	3, 4, 2, 1
4, 1, 2, 3	4, 1, 3, 2	4, 2, 1, 3	4, 2, 3, 1	4, 3, 1, 2	4, 3, 2, 1

But we're going to forge a new definition. We'll say that a *permutation* of a set A is a one-to-one correspondence from A to A.

permutation

What fellowship does that definition have with our intuitive understanding of permutations? Well, consider an example. Let's define the following one-to-one correspondence, α, on $\{1, 2, 3, 4\}$:

x	$\alpha(x)$
1	2
2	1
3	3
4	4

Looks just like one of the "permutations" we listed above. Moreover, if we extend our notion of α so that it can be applied to lists of elements of A (sort of like the image of a set under a function, except the elements or ordered; more like the `map` function in ML), then

$$\alpha([1, 2, 3, 4]) = [2, 1, 3, 4]$$

There's a standard matrix-looking way to represent a permutation. The one above (α) would be written

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{bmatrix}$$

Read that by finding the input on top and the corresponding output on the bottom: 1 maps to 2, 2 maps to 1, 3 maps to 3, 4 maps to 4. We also have a ready binary operation to apply to permutations: function composition. Let β be the permutation listed originally as 3, 4, 1, 2. Then

$$\alpha \circ \beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix}$$

To get your mind around this, you need to read from right to left. What is $\alpha \circ \beta(1)$? Well, we feed 1 into β , which gets 3; feed 3 into α, and we still get 3. Hence $\alpha \circ \beta(1) = 3$.

permutation group

A set of permutations that forms a group under function composition is called a *permutation group*. We've already seen one: Think about the rotations and symmetries of an equilateral triangle–they're just permutations of ways to list the corners, say, going clockwise from the top.