MATH 417 – THIRD WEEK

BRUCE REZNICK
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

September 9, 2020, in advance

Because of the technical problems in Friday's Zoom, I want to start with the worksheet problems.

I will continue with a few topics that I neglected to mention from sections four through six and give one more application from number theory.

I will skip section seven and move on to section eight, with permutations which give some non-abelian groups.

WORKSHEET PROBLEMS

1. Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{([a]_2, [b]_3)\}$, and define the operation $*$ by

$$([a]_2, [b]_3) * ([c]_2, [d]_3) = ([a+c]_2, [b+d]_3)$$

Thus, for example

$$([1]_2, [1]_3) * ([1]_2, [1]_3) = ([2]_2, [2]_3) = ([0]_2, [2]_3),$$

because $2 \equiv 0 \mod 2$ and $2 \equiv 2 \mod 3$.

Prove that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is a cyclic group of order 6 by working out $\langle([1]_2, [1]_3)\rangle$.

2. Same situation. Consider $C_6 = \langle a \rangle, a^6 = e$. There is an isomorphism Φ which takes C_6 to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and for which $\Phi(a) = ([1]_2, [1]_3)$. Write out the other values of $\Phi(a^k)$, and $\Phi(\langle a^2 \rangle)$ and $\Phi(\langle a^3 \rangle)$. These are subgroups of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ that will be "obviously" subgroups.

WORKSHEET SOLUTIONS

From the definition of the group

$$([1]_2, [1]_3)^1 = ([1]_2, [1]_3)$$
$$([1]_2, [1]_3)^2 = ([1]_2, [1]_3) * ([1]_2, [1]_3) = ([0]_2, [2]_3)$$
$$([1]_2, [1]_3)^3 = ([1]_2, [1]_3) * ([1]_2, [1]_3)^2 = ([1]_2, [0]_3)$$
$$([1]_2, [1]_3)^4 = ([1]_2, [1]_3) * ([1]_2, [1]_3)^3 = ([0]_2, [1]_3)$$
$$([1]_2, [1]_3)^5 = ([1]_2, [1]_3) * ([1]_2, [1]_3)^4 = ([1]_2, [2]_3)$$
$$([1]_2, [1]_3)^6 = ([1]_2, [1]_3) * ([1]_2, [1]_3)^5 = ([0]_2, [0]_3)$$

So the first five powers are different and the sixth gives the identity and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is a cyclic group of order 6.

2. If $\Phi(a) = ([1]_2, [1]_3)$, then because Φ is an isomorphism. $\Phi(a^k) = ([1]_2, [1]_3)^k$, so $\Phi(a^2) = ([0]_2, [2]_3)$, $\Phi(a^3) = ([1]_2, [0]_3)$, $\Phi(a^4) = ([0]_2, [2]_3)$, $\Phi(a^5) = ([1]_2, [2]_3)$ and $\Phi(e) = \Phi(a^6) = ([0]_2, [0]_3) = e_G$. Actually, $\Phi(a^k) = ([k]_2, [k]_3)$.

The images of $\Phi(\langle a^2 \rangle) = \Phi(\{e, a^2, a^4\})$ and $\Phi(\langle a^3 \rangle) = \Phi(\{e, a^3\})$ are then

$$\{([0]_2, [0]_3), ([0]_2, [1]_3), ([0]_2, [2]_3)\}$$

and

$$\{([0]_2, [0]_3), ([1]_2, [0]_3)\}$$

A couple of points worth mentioning from the book. The author uses a' where I have used a^{-1}. I don't know why.

He also has a slightly different definition of $\langle a \rangle$ than I do. The definitions coincide for finite groups (which is what we'll mostly study), but are subtly different for infinite groups.

Recall that I defined

$$\langle a \rangle = \{a, a^2, a^3, \dots\} = \{a^n \mid n \in \mathbb{N}\}$$

Fraleigh says that

$$\langle a \rangle = \{\dots a^{-2}, a^{-1}, e, a, a^2, a^3, \dots\} = \{a^n \mid n \in \mathbb{Z}\}.$$

Suppose G is finite, then there exists m so that $a^m = e$, hence $e \in \langle a \rangle$ by my definition and, since $a^{m-1} = a^{-1}$, $a^{-1} \in \langle a \rangle$ as well, the two definitions coincide.

However, when G is an infinite group, then they can be different. Consider $(\mathbb{Z}, +)$. In this case, my definition gives

$$\langle 1 \rangle = \{1, 2, 3, \dots\} = \{a^n \mid n \in \mathbb{N}\}$$

Clearly, we never get to the identity – 0 – this way, and this subset is not a subgroup. Fraleigh uses the more standard and correct definition so that

$$\langle 1 \rangle = \{-2, -1, 0, 1, 2, 3, \dots\} = \mathbb{Z}.$$

He also phrases this as saying that $\langle a \rangle$ is the "smallest subgroup of G containing a. The reason for this is twofold. First of all, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is a group and it is a subgroup of G. Second, if H is a subgroup of G and $a \in H$, so $a * a = a^2 \in H$, etc. But also $e \in H$ and $a^{-1} \in H$ because it's a subgroup, and so by an easy induction $a^n \in H$ for $n \in \mathbb{Z}$. Thus $\langle a \rangle \subseteq H$, so $\langle a \rangle$ is the smallest subgroup.

Before I get to permutations, one more application that is not in the book. This might be of interest to future math teachers. It involves infinite repeated decimals.

Ordinary pre-college infinite decimals have the following standard meaning. If all $a_i \in \{0, 1, ..., 9\}$, then

$$.a_1a_2a_3a_4\cdots = \frac{a_1}{10^1} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \frac{a_4}{10^4} + \cdots = \sum_{n=1}^{\infty} \frac{a_n}{10^n}.$$

Many fractions have a nice repeating pattern. Perhaps you know that

$$\frac{1}{7} = .142857\ 142857\ 142857\ 142857\ldots.$$

I'm putting artificial spaces in there and throughout so you can see where the blocks break up. Why is this formula true? Let me do a bit of algebra (trigger-warning: geometric series from calculus will be showing up.)

$$\begin{aligned}
&.142857\ 142857142857\ 142857\ldots \\
&= 142857 \times (.000001\ 000001\ 000001\ 000001\ldots) \\
&= 142857 \times \left(\frac{1}{10^6} + \frac{1}{10^{12}} + \frac{1}{10^{18}} + \frac{1}{10^{24}}\cdots\right) \\
&= 142857 \times \frac{1}{10^6} \times \left(1 + \frac{1}{10^6} + \frac{1}{10^{12}} + \frac{1}{10^{18}} + \ldots\right) \\
142857 \times \frac{1}{10^6} \times \frac{1}{1-\frac{1}{10^6}} &= \frac{142857}{10^6(1-\frac{1}{10^6})} = \frac{142857}{10^6-1} = \frac{142857}{999999}.
\end{aligned}$$

Finally, $999999 = 7 \cdot 142857$, so the sum is

$$\frac{142857}{999999} = \frac{142857}{7 * 142857} = \frac{1}{7}.$$

I was using the geometric series, but $|\frac{1}{10^6}| < 1$, so that's ok.

Here's a wonderful fact that we are about to prove: Suppose $n \equiv 1, 3, 7, 9 \mod 10$ and $\frac{c}{n} \in (0, 1)$, then the decimal expression for $\frac{c}{n}$ always repeats! For example,

$$\frac{1}{417} =$$

.002398081534772182254196642685851318944844124 7 002398...

The block that repeats has 46 digits.

The proof of the wonderful fact is not that hard and will follow from the group theory we've been doing.

LEMMA 1: If $n \equiv 1, 3, 7, 9 \mod 10$, then there exists $r \in \mathbb{N}$ so that $10^r \equiv 1 \mod n$.

PROOF: We've seen that $(\mathbb{Z}/10\mathbb{Z})^* = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$, so that the hypothesis means that $[n]_{10} \in (\mathbb{Z}/10\mathbb{Z})^*$. But this means that $gcd(n, 10) = 1$ so $gcd(10, n) = 1$, so that $[10]_n \in (\mathbb{Z}/n\mathbb{Z})^*$.

We also know that $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$ is a finite group, so there exists r so that $([10]_n)^r = [10^r]_n = [1]_n$ is the identity in $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$; that is, $10^r \equiv 1 \mod n$. □

(We will later have a result which implies that $r \mid \phi(n)$, but that's not important right now.)

LEMMA 2: For any $r \in \mathbb{N}$,

$$\frac{1}{10^r} + \frac{1}{10^{2r}} + \frac{1}{10^{3r}} + \frac{1}{10^{4r}} + \cdots = \frac{1}{10^r - 1}.$$

PROOF: As we saw above with $r = 6$,

$$\frac{1}{10^r} + \frac{1}{10^{2r}} + \frac{1}{10^{3r}} + \frac{1}{10^{4r}} + \cdots =$$
$$\frac{1}{10^r} \cdot \left(1 + \frac{1}{10^r} + \frac{1}{10^{2r}} + \frac{1}{10^{3r}} + \ldots\right)$$
$$\frac{1}{10^r} \cdot \sum_{k=0}^{\infty} \frac{1}{(10^r)^k} = \frac{1}{10^r} \cdot \frac{1}{1 - \frac{1}{10^r}} = \frac{1}{10^r - 1}.$$

□

Again, I was using the geometric series, but $|\frac{1}{10^r}| < 1$, so it's valid.

THEOREM: Suppose $n \equiv 1, 3, 7, 9 \mod 10$ and $\frac{c}{n} \in (0, 1)$, then there exists r so that the decimal expansion of $\frac{c}{n}$ will repeat in a block of size r.

PROOF: By Lemma 1, there exists r so that $10^r \equiv 1 \mod n$. This means that $n \mid 10^r - 1 \iff 10^r - 1 = n \cdot t$ for some integer t. Therefore, by Lemma 2,

$$\frac{c}{n} = \frac{ct}{nt} = \frac{ct}{10^r - 1} = ct \cdot (.00\ldots01\ 00\ldots01\ 00\ldots01\ldots)$$

Since $\frac{c}{n} < 1$, we have $ct < nt = 10^r - 1$ and this means that there is no carryover when we multiply into the block. □

Here's an example. Since $10^6 - 1 = 999999 = 13 \cdot 76923$,

$$\frac{4}{13} = \frac{4 \cdot 76923}{13 \cdot 76923} = \frac{307692}{999999} =$$

$$307692 * (.000001\ 000001\ 000001\ 000001\ 000001 \dots)$$

$$= .307692\ 307692\ 307692\ 307692 \dots$$

We have $10^{46} \equiv 1 \mod 417$, which explains the blocks of 46 above, and also

$$\phi(417) = \phi(3 \cdot 139) = (3-1)(139-1) = 2 \cdot 138 = 276 = 6 \cdot 46,$$

and

$$10^{46} - 1 = 417 \times$$
$$2398081534772182254196642685851318944844124 7,$$

Also, you can get these fractions in many different ways probably know that $\frac{1}{11}$ has a nice decimal expression

$$.0909090909 \cdots = .09\ 09\ 09\ 09\ 09\ 09 \cdots = .0909\ 0909\ 0909 \dots .$$

So we can think of it in two ways:

$$\frac{1}{11} = \frac{9}{99} = \frac{9}{10^2 - 1} = 9 \cdot (.01\ 01\ 01\ 01 \dots)$$

or

$$\frac{1}{11} = \frac{909}{9999} = \frac{909}{10^4 - 1} = 909 \cdot (.0001\ 0001 \dots).$$

Now a complete change of topics. Let $A = \{a_1, \dots, a_n\}$ be a finite set, and let σ be a bijection of A to A. That is

$$\{\sigma(a_1), \sigma(a_2), \dots, \sigma(a_n)\} = \{a_1, \dots, a_n\} = A.$$

We say that σ is a *permutation* of A. At the beginning at least, we will take $A = \{1, \dots n\}$. As an example, if $n = 5$, then we might have

$$\sigma(1) = 3, \quad \sigma(2) = 2, \quad \sigma(3) = 5, \quad \sigma(4) = 1, \quad \sigma(5) = 4.$$

There are two ways to write this in a compressed form. The first is to consider a kind of matrix in which j lies above $\sigma(j)$. In this case

$$\sigma = \begin{pmatrix} 12345 \\ 32514 \end{pmatrix}.$$

Another way would use an arrow to designate the way σ acts on the set. Here

$$1 \mapsto 3 \mapsto 5 \mapsto 4 \mapsto 1, \quad 2 \mapsto 2.$$

This can be written as $\sigma = (1354)(2)$. Whenever there is a block of terms, each one goes to the next one and the last one goes to the first. There are a lot of different ways to write this, and they are all equivalent:

$$\sigma = (1354)(2) = (5413)(2) = (2)(3541) \quad \text{etc.}$$

As you probably suspect, there is a group at work here. We need to figure out how to combine them, and the order can be confusing. Let me give another permutation of $\{1, 2, 3, 4, 5\}$

$$\rho(1) = 4, \quad \rho(2) = 3, \quad \rho(3) = 5, \quad \rho(4) = 1, \quad \rho(5) = 2.$$

so we would write

$$\rho = \begin{pmatrix} 12345 \\ 43512 \end{pmatrix}.$$

Since ρ acts as follows

$$1 \mapsto 4 \mapsto 1, \quad 2 \mapsto 3 \mapsto 5 \mapsto 2,$$

we have $\rho = (14)(235) = (352)(41)$, etc.

Since

$$\sigma = \begin{pmatrix} 12345 \\ 32514 \end{pmatrix}, \qquad \rho = \begin{pmatrix} 12345 \\ 43512 \end{pmatrix},$$

we define $\sigma \circ \rho$ by reading from left to right as it acts on the various elements

$$\begin{aligned}
&\sigma(1) = 3 \quad \rho(3) = 5 \implies (\sigma \circ \rho)(1) = 5, \quad 1 \mapsto 3 \mapsto 5; \\
&\sigma(2) = 2 \quad \rho(2) = 3 \implies (\sigma \circ \rho)(2) = 3, \quad 2 \mapsto 2 \mapsto 3; \\
&\sigma(3) = 5 \quad \rho(5) = 2 \implies (\sigma \circ \rho)(3) = 2, \quad 3 \mapsto 5 \mapsto 2; \\
&\sigma(4) = 1 \quad \rho(1) = 4 \implies (\sigma \circ \rho)(4) = 4, \quad 4 \mapsto 1 \mapsto 4; \\
&\sigma(5) = 4 \quad \rho(4) = 1 \implies (\sigma \circ \rho)(5) = 1, \quad 5 \mapsto 4 \mapsto 1.
\end{aligned}$$

Thus

$$\sigma \circ \rho = \begin{pmatrix} 12345 \\ 53241 \end{pmatrix} = (15)(23)(4).$$

It's important to observe that this is not commutative!

$$\begin{aligned}
&\rho(1) = 4 \quad \sigma(4) = 1 \implies (\rho \circ \sigma)(1) = 1, \quad 1 \mapsto 4 \mapsto 1; \\
&\rho(2) = 3 \quad \sigma(3) = 5 \implies (\rho \circ \sigma)(2) = 5, \quad 2 \mapsto 3 \mapsto 5; \\
&\rho(3) = 5 \quad \sigma(5) = 4 \implies (\rho \circ \sigma)(3) = 4, \quad 3 \mapsto 5 \mapsto 4; \\
&\rho(4) = 1 \quad \sigma(1) = 3 \implies (\rho \circ \sigma)(4) = 3, \quad 4 \mapsto 1 \mapsto 3; \\
&\rho(5) = 2 \quad \sigma(2) = 2 \implies (\rho \circ \sigma)(5) = 2, \quad 5 \mapsto 2 \mapsto 2;
\end{aligned}$$

Thus

$$\rho \circ \sigma = \begin{pmatrix} 12345 \\ 15432 \end{pmatrix} = (1)(25)(34), \quad \sigma \circ \rho = \begin{pmatrix} 12345 \\ 53241 \end{pmatrix} = (15)(23)(4).$$

They look similar but are different. In fact, there is no i for which $(\sigma \circ \rho)(i) = (\rho \circ \sigma)(i)$

Here's the tricky part: if you think of these as functions, $(\sigma \circ \rho)(j) = \rho(\sigma(j))$, so if you write in functional terms, it looks like we've written it in the wrong direction. I'm sorry, stuff happens. This is just the way the notation is in this book, but not in all algebra books. Whenever you look at a group theory book, you have to see which direction is used. You can find both.

In the next lecture, I'll prove that the set of permutations of $\{1, \ldots, n\}$, called S_n, forms a group of order $n!$.

On Wednesday, I will answer your questions (please send them) and also have some worksheet activities on multiplying permutations. It does get easier with practice. If there is time, I will completely describe the elements of S_3, the non-abelian group of permutations of $\{1, 2, 3\}$, which can also be interpreted as the motions of an equilateral triangle.

If you can, cut (or fold) a triangle out of paper so you can follow along. Hope to see you then.

September 9, 2020, in class

First a few elaborations on the material I sent out Tuesday.

Given that $n \equiv 1, 3, 7, 9 \mod 10$, it follows that $[n]_{10} \in (\mathbb{Z}/10\mathbb{Z})^*$, so $gcd(n, 10) = 1 = gcd(10, n)$, so that $[10]_n \in (\mathbb{Z}/n\mathbb{Z})^*$.

Rather than appealing to a previous theorem, I'll give the proof again. We know that $(\mathbb{Z}/n\mathbb{Z})^*$ is a finite set, so the sequence

$$[10]_n, \quad [10^2]_n, \quad [10^3]_n, \quad [10^4]_n, \ldots$$

can't all be different.

Thus, we can find $i < j$ so that $[10^i]_n = [10^j]_n$. (This is kind of the Pigeonhole Principle.) Thus, since $gcd(n, 10) = 1$,

$$n \mid 10^j - 10^i = 10^i(10^{j-i} - 1) \implies$$
$$n \mid (10^{j-i} - 1) \implies 10^{j-i} \equiv 1 \mod n \implies [10^{j-i}]_n = [1]_n.$$

I've also gotten requests for a refresher on the geometric series.

Here's one derivation. Suppose $x \neq 1$ and $n \in \mathbb{N}$. Then there is an exact identity which you can verify by cross-multiplying.

$$1 + x + x^2 + \cdots + x^n = \frac{1 - x^{n+1}}{1 - x} = \frac{1}{1 - x} - \frac{x^{n+1}}{1 - x}.$$

If $|x| < 1$, then $x^{n+1} \to 0$, and so we have the geometric series formula:

$$1 + x + x^2 + \cdots + x^n + \cdots = \sum_{k=0}^{\infty} x^k = \frac{1}{1-x} \quad \text{if} \quad |x| < 1.$$

What about the series we saw in decimals?

$$x + x^2 + x^3 + \cdots = x(1 + x + x^2 + \dots) = \frac{x}{1-x}.$$

In the special case that $x = \frac{1}{N}$ (our case is $N = 10^r$), we have

$$\frac{1}{N} + \frac{1}{N^2} + \frac{1}{N^3} + \cdots = \frac{\frac{1}{N}}{1 - \frac{1}{N}} = \frac{1}{N-1}.$$

For example, if $n = 13$, then Mathematica tells me that the sequence of $10^k \mod 13$ is:

$$10^0 \equiv 1,\ 10^1 \equiv 10,\ 10^2 \equiv 9,\ 10^3 \equiv 12,\ 10^4 \equiv 3,\ 10^5 \equiv 4,\ 10^6 \equiv 1$$

Here, $i = 0,\ j = 6$, and $10^6 - 1 = 999999 = 13 \cdot 76923$.

One more question was about the order of composition, and I think it would be easiest if I used two functions which aren't permutations.

Suppose $f(x) = x + 3$ and $g(x) = x^2$ and you apply f first and then do g. Then you get $x \mapsto x + 3 \mapsto (x+3)^2$. For comparison,

$$f(g(x)) = f(x^2) = x^2 + 3,$$
$$g(f(x)) = g(x+3) = (x+3)^2.$$

So in this case too: if we act in the order written, it gets written in the reverse. It's confusing but this is how it works here.

The symmetric group we will get to know best is S_3, which has $6 = 3!$ elements. I will write them down and then give them all names (the same ones in Fraleigh) and say a little bit about each one. They can also be viewed as symmetries of an equilateral triangle.

Here is the triangle:

1 2

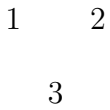
3

Each element of S_3 gets its own page.

This is the first element, ρ_0. Under ρ_0,

$$1 \mapsto 1, \quad 2 \mapsto 2, \quad 3 \mapsto 3$$

$$\rho_0 = \begin{pmatrix}123\\123\end{pmatrix} = (1)(2)(3),$$

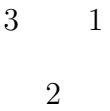


Thus $\rho_0 = e$ is the identity element. The triangle at the end to show the motions of these permutations and this is the starting configuration. Think of the numbers as labels that can move, and also indicate the name of the position.

This is the second element, ρ_1. Under ρ_1,

$$1 \mapsto 2, \quad 2 \mapsto 3, \quad 3 \mapsto 1$$

$$\rho_1 = \begin{pmatrix}123\\231\end{pmatrix} = (123),$$

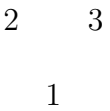


The permutation ρ_1 rotates the triangle clockwise by $\frac{2\pi}{3}$. The triangle shows that the label 1 goes to the position 2, the label 2 goes to the position 3 and label 3 goes to the position 1.

This is the third element, ρ_2. Under ρ_2,

$$1 \mapsto 3, \quad 2 \mapsto 1, \quad 3 \mapsto 2$$

$$\rho_2 = \begin{pmatrix}123\\312\end{pmatrix} = (132),$$



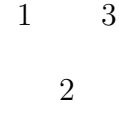
The permutation ρ_2 rotates clockwise by $\frac{4\pi}{3}$ or counterclockwise by $\frac{2\pi}{3}$. The triangle shows that the label 1 goes to the position 3, the label 2 goes to the position 1 and label 3 goes to the position 2.

I hope you can see that $\rho_2 = \rho_1^2$ and $\rho_1 = \rho_2^2$, $\rho_1^3 = \rho_2^3 = \rho_0 = e$. It follows that $\{\rho_0, \rho_1, \rho_2\}$ is a cyclic group of order 3, and a subgroup of S_3.

This is the fourth element, μ_1. Under μ_1,

$$1 \mapsto 1, \quad 2 \mapsto 3, \quad 3 \mapsto 2$$

$$\mu_1 = \begin{pmatrix}123\\132\end{pmatrix} = (1)(23),$$

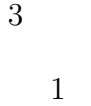


The permutation μ_1 flips 2 and 3 and fixes 1. This type of permutation is called a *transposition*. Notice that $\mu_1^2 = \rho_0 = e$. It's equivalent to flipping the triangle on a diameter through 1.

This is the fifth element, μ_2. Under μ_2,

$$1 \mapsto 3, \quad 2 \mapsto 2, \quad 3 \mapsto 1$$

$$\mu_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (13)(2),$$

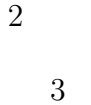


The permutation μ_2 flips 1 and 3 and fixes 2. Also a transposition. Notice that $\mu_2^2 = \rho_0 = e$. It's equivalent to flipping the triangle on a diameter through 2.

This is the sixth element, μ_3. Under μ_3,

$$1 \mapsto 2, \quad 2 \mapsto 1, \quad 3 \mapsto 3$$

$$\mu_3 = \begin{pmatrix} 123 \\ 213 \end{pmatrix} = (12)(3),$$



The permutation μ_3 flips 1 and 2 and fixes 3. Also a transposition. Again, $\mu_3^2 = \rho_0 = e$. It's equivalent to flipping the triangle on a diameter through 3.

We'll finish the multiplication table later, but I wanted to show that the operation $\circ$ is *not* always commutative. In one simple case:

$$\mu_1 \circ \mu_2 = \begin{pmatrix} 123 \\ 132 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 321 \end{pmatrix} \implies$$

$$1 \mapsto 1 \mapsto 3, \quad 2 \mapsto 3 \mapsto 1, \quad 3 \mapsto 2 \mapsto 2, \implies$$

$$\mu_1 \circ \mu_2 = \begin{pmatrix} 123 \\ 312 \end{pmatrix} = \rho_2;$$

$$\mu_2 \circ \mu_1 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 132 \end{pmatrix} \implies$$

$$1 \mapsto 3 \mapsto 2, \quad 2 \mapsto 2 \mapsto 3, \quad 3 \mapsto 1 \mapsto 1, \implies$$

$$\mu_1 \circ \mu_2 = \begin{pmatrix} 123 \\ 231 \end{pmatrix} = \rho_1.$$

So the product of each flip is a rotation, but they are different rotations: $\mu_1 \circ \mu_2 \neq \mu_2 \circ \mu_1$.

One more point on these before we go on. Imagine that the triangle is, say, red on the front and blue on the back. We start with it as red. Any rotation (or the identity) (that is, any ρ_i) will keep it red. Any flip (that is, any μ_i) will switch it so the front is blue.

If you think about that, then you can convince yourself, **without any calculation**, that $\rho_i \circ \rho_j$ will be some ρ_k and $\rho_i \circ \mu_j$ or $\mu_i \circ \rho_j$ will

be some μ_k. Finally, two flips will turn the triangle twice, so it's in its original color position. Thus, $\mu_i \circ \mu_j$ will be some ρ_k. (We saw that twice above.) This shows up in table 8.8 on p.79 of the book. We'll talk about this on Friday.

WORKSHEET PROBLEMS

1. It is a fact from arithmetic that $77 \cdot 12987 = 999999$. Use this information to give the decimal expansion of

$$\frac{50}{77}.$$

2. Recall that

$$\rho_2 = \begin{pmatrix} 123 \\ 312 \end{pmatrix} = (132), \qquad \mu_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (13)(2)$$

Calculate $\rho_2 \circ \mu_2$ and $\mu_2 \circ \rho_2$.

WORKSHEET PROBLEM SOLUTIONS

1.

$$\frac{50}{77} = \frac{50 \cdot 12987}{77 \cdot 12987} = \frac{649350}{999999} = 649350 \times \frac{1}{999999} =$$
$$649350 \times (.000001\ 000001\ 000001\ \dots)$$
$$= .649350\ 649350\ 649350\ \dots$$

2. Again, for reference,

$$\rho_2 = \begin{pmatrix} 123 \\ 312 \end{pmatrix} = (132), \qquad \mu_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (13)(2)$$

So $\rho_2 \circ \mu_2$ takes $1 \mapsto 3 \mapsto 1$, $2 \mapsto 1 \mapsto 3$ and $3 \mapsto 2 \mapsto 2$ and

$$\rho_2 \circ \mu_2 = \begin{pmatrix} 123 \\ 132 \end{pmatrix} = (1)(23)$$

Similarly, $\mu_2 \circ \rho_2$ takes $1 \mapsto 3 \mapsto 2$, $2 \mapsto 2 \mapsto 1$ and $3 \mapsto 1 \mapsto 3$ and

$$\mu_2 \circ \rho_2 = \begin{pmatrix} 123 \\ 213 \end{pmatrix} = (12)(3)$$

That is, $\rho_2 \circ \mu_2 = \mu_1$ and $\mu_2 \circ \rho_2 = \mu_3$.

September 11, 2020, in advance

We're first going to talk about the general symmetric group S_n and then go back to a much more detailed examination of S_3.

Okay. I have to start with an embarrassing confession. I gave you the multiplication of permutations as I was taught it and I told you that there are books in which it can go in different directions. Well, I looked up *Fraleigh*, and **he does it the other way**, and I'm going to follow him. So I'm going to redo the examples from yesterday.

I think it's less confusing for me to fix about 30 minutes of class than for you to have to correct the book every time you read it.

Definition. Fix an integer $n \geq 2$ and consider permutations of $\{1, \ldots, n\}$. We write S_n for the set of permutations of $\{1, \ldots, n\}$ with the operation $\circ$ as defined so that, if $\sigma, \pi \in S_n$, then $\sigma \circ \pi$ operates right to left, with $i \mapsto \pi(i) \mapsto \sigma(\pi(i))$: $(S_n, \circ)$ is called the *n-th symmetric group* or *the symmetric group on n letters.*

In other words, it is consistent with functional notation, but you do the second permutation first and then apply the first permutation.

Here are corrected versions of our earlier instances

First, from Tuesday night, recall

$$\sigma = \begin{pmatrix} 12345 \\ 32514 \end{pmatrix}, \qquad \rho = \begin{pmatrix} 12345 \\ 43512 \end{pmatrix};$$

we define $(\sigma \circ \rho)(i) = \sigma(\rho(i))$ so

$$\begin{aligned}
&\rho(1) = 4 \quad \sigma(4) = 1 \implies (\sigma \circ \rho)(1) = 1, \quad 1 \mapsto 4 \mapsto 1; \\
&\rho(2) = 3 \quad \sigma(3) = 5 \implies (\sigma \circ \rho)(2) = 5, \quad 2 \mapsto 3 \mapsto 5; \\
&\rho(3) = 5 \quad \sigma(5) = 4 \implies (\sigma \circ \rho)(3) = 4, \quad 3 \mapsto 5 \mapsto 4; \\
&\rho(4) = 1 \quad \sigma(1) = 3 \implies (\sigma \circ \rho)(4) = 3, \quad 4 \mapsto 1 \mapsto 3; \\
&\rho(5) = 2 \quad \sigma(2) = 2 \implies (\sigma \circ \rho)(5) = 2, \quad 5 \mapsto 2 \mapsto 2; \\
&\implies \sigma \circ \rho = \begin{pmatrix} 12345 \\ 15432 \end{pmatrix} = (1)(25)(34),
\end{aligned}$$

Similarly,

$$\begin{aligned}
&\sigma(1) = 3 \quad \rho(3) = 5 \implies (\rho \circ \sigma)(1) = 5, \quad 1 \mapsto 3 \mapsto 5; \\
&\sigma(2) = 2 \quad \rho(2) = 3 \implies (\rho \circ \sigma)(2) = 3, \quad 2 \mapsto 2 \mapsto 3; \\
&\sigma(3) = 5 \quad \rho(5) = 2 \implies (\rho \circ \sigma)(3) = 2, \quad 3 \mapsto 5 \mapsto 2; \\
&\sigma(4) = 1 \quad \rho(1) = 4 \implies (\rho \circ \sigma)(4) = 4, \quad 4 \mapsto 1 \mapsto 4; \\
&\sigma(5) = 4 \quad \rho(4) = 1 \implies (\rho \circ \sigma)(5) = 1, \quad 5 \mapsto 4 \mapsto 1; \\
&\implies \rho \circ \sigma = \begin{pmatrix} 12345 \\ 53241 \end{pmatrix} = (15)(23)(4)
\end{aligned}$$

These are just the reverses of what we had earlier.

And we did this in class on Wednesday. Recall

$$\mu_1 = \begin{pmatrix} 123 \\ 132 \end{pmatrix} = (1)(23), \qquad \mu_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (13)(2),$$

Thinking about these as functions, and $(\mu_1 \circ \mu_2)(i) = \mu_1(\mu_2(i))$, so we do μ_2 first:

$$(\mu_1 \circ \mu_2)(1) = \mu_1(\mu_2(1)) = \mu_1(3) = 2$$
$$(\mu_1 \circ \mu_2)(2) = \mu_1(\mu_2(2)) = \mu_1(2) = 3$$
$$(\mu_1 \circ \mu_2)(3) = \mu_1(\mu_2(3)) = \mu_1(1) = 1$$
$$\implies \mu_1 \circ \mu_2 = \begin{pmatrix} 123 \\ 231 \end{pmatrix} = \rho_1$$

Similarly,

$$(\mu_2 \circ \mu_1)(1) = \mu_2(\mu_1(1)) = \mu_2(1) = 3$$
$$(\mu_2 \circ \mu_1)(2) = \mu_2(\mu_1(2)) = \mu_2(3) = 1$$
$$(\mu_2 \circ \mu_1)(3) = \mu_2(\mu_1(3)) = \mu_2(2) = 2$$
$$\implies \mu_1 \circ \mu_2 = \begin{pmatrix} 123 \\ 312 \end{pmatrix} = \rho_2$$

So the product of each flip is a rotation, but they are different rotations: $\mu_1 \circ \mu_2 \neq \mu_2 \circ \mu_1$.

And from the worksheet

$$\rho_2 = \begin{pmatrix} 123 \\ 312 \end{pmatrix} = (132), \qquad \mu_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (13)(2)$$

So $\mu_2 \circ \rho_2$ takes $1 \mapsto 3 \mapsto 1$, $2 \mapsto 1 \mapsto 3$ and $3 \mapsto 2 \mapsto 2$ and

$$\mu_2 \circ \rho_2 = \begin{pmatrix} 123 \\ 132 \end{pmatrix} = (1)(23) = \mu_1$$

Similarly, $\rho_2 \circ \mu_2$ takes $1 \mapsto 3 \mapsto 2$, $2 \mapsto 2 \mapsto 1$ and $3 \mapsto 1 \mapsto 3$ and

$$\rho_2 \circ \mu_2 = \begin{pmatrix} 123 \\ 213 \end{pmatrix} = (12)(3) = \mu_3$$

I owe you a fresh example. Suppose $n = 4$ and

$$\sigma(1) = 2, \sigma(2) = 4, \sigma(3) = 1, \sigma(4) = 3; \ \sigma = \begin{pmatrix} 1234 \\ 2413 \end{pmatrix} = (1243),$$
$$\pi(1) = 4, \pi(2) = 1, \pi(3) = 3, \pi(4) = 2; \ \pi = \begin{pmatrix} 1234 \\ 4132 \end{pmatrix} = (142)(3).$$

Then (with a lot of redundancy):

$$\begin{array}{llll} \sigma(1)=2 & \pi(2)=1 \implies (\pi\circ\sigma)(1)=1, & 1\mapsto 2\mapsto 1;\\ \sigma(2)=4 & \pi(4)=2 \implies (\pi\circ\sigma)(2)=2, & 2\mapsto 4\mapsto 2;\\ \sigma(3)=1 & \pi(1)=4 \implies (\pi\circ\sigma)(3)=4, & 3\mapsto 1\mapsto 4;\\ \sigma(4)=3 & \pi(3)=3 \implies (\pi\circ\sigma)(4)=3, & 4\mapsto 3\mapsto 3; \end{array}$$

$$\implies$$

$$\pi\circ\sigma = \binom{1234}{1243} = (1)(2)(34).$$

THEOREM: The symmetric group S_n is a group of order $n!$.

PROOF: First, how many elements are there in S_n? There are n choices for $\sigma(1)$, and we know that there are $n-1$ choices for $\sigma(2)$ (because it can't equal $\sigma(1)$) and then $n-2$ choices for $\sigma(3)$ (because it can't equal $\sigma(1)$ or $\sigma(2)$), etc., so altogether, there are $n\cdot(n-1)\cdot(n-2)\cdots = n!$ possible permutations, and $|S_n| = n!$.

First we need an identity element. Let e be defined so that $e(j)=j$ for all j; that is,

$$e = \binom{12\ldots n}{12\ldots n} = (1)(2)\cdots(n).$$

Then it should be clear that for every $\sigma\in S_n$, $\sigma\circ e = e\circ\sigma = \sigma$.

Next we need inverses, and here we use functional inverses. For $\sigma\in S_n$, define ρ by $\sigma(i)=j \implies \rho(j)=i$, that is, $\rho(j)=\sigma^{-1}(j)$ *as a function*. Then $\sigma\circ\rho$ takes $i\mapsto j\mapsto i$, and similarly for $\rho\circ\sigma$. That is, $\sigma\circ\rho=\rho\circ\sigma=e$, and so $\rho=\sigma^{-1}$.

The last thing we have to check is associativity, and this is ugly. We need to show that

$$(\sigma_1\circ\sigma_2)\circ\sigma_3 = \sigma_1\circ(\sigma_2\circ\sigma_3).$$

Let's work through the definition. For $i\in\{1,\ldots,n\}$,

$$((\sigma_1\circ\sigma_2)\circ\sigma_3)(i) = (\sigma_1\circ\sigma_2)(\sigma_3(i)) = \sigma_1(\sigma_2(\sigma_(3)))(i)$$
$$(\sigma_1\circ((\sigma_2\circ\sigma_3))(i) = \sigma_1((\sigma_2\circ\sigma_3)(i)) = \sigma_1(\sigma_2(\sigma_(3)))(i)$$

so they're equal. Yes, this is tedious, , because taking functions is associative. but we only have to do this once, and now we can say we have a group. $\square$.

A bit about how to find inverses in practice. Let's recall σ:

$$\sigma(1)=2,\sigma(2)=4,\sigma(3)=1,\sigma(4)=3; \quad \sigma = \binom{1234}{2413} = (1243)$$

If as a function, $\rho = \sigma^{-1}$, then we can just reverse this:

$$\rho(2) = 1,\ \rho(4) = 2,\ \rho(1) = 3,\ \rho(3) = 4;\ \Longleftrightarrow$$
$$\rho(1) = 3,\ \rho(2) = 1,\ \rho(3) = 4,\ \rho(4) = 2,$$

or ake the matrix for σ, flip it over and then rearrange columns:

$$\rho = \begin{pmatrix} 2413 \\ 1234 \end{pmatrix} = \begin{pmatrix} 1234 \\ 3142 \end{pmatrix}$$

Or take the cycles and just run them in reverse. If, previously, under a permutation, we had $a_1 \mapsto a_2 \cdots \mapsto a_n \mapsto a_1$, then in the inverse we have $a_1 \leftarrow a_2 \cdots \leftarrow a_n \leftarrow a_1$, so (1243) becomes (3421) or (1342).

It's also worth mentioning that $S_1 = \{(1)\}$ is just the trivial group and $S_2 = \{(1)(2), (12)\}$ is a cyclic group of order 2. We're about to spend a lot of time with S_3. There is something we can say generally about symmetric groups.

THEOREM If $n \geq 3$, then S_n is not abelian.

PROOF All we need to show is that there are always $\alpha, \beta \in S_n$ so that $\alpha \circ \beta \neq \beta \circ \alpha$. Consider these two transpositions:

$$\alpha(1) = 2, \alpha(2) = 1; k \in \{3, 4, \ldots, n\} \implies \alpha(k) = k,$$
$$\beta(1) = 3, \beta(3) = 1; k \in \{2, 4, \ldots, n\} \implies \beta(k) = k,$$

In other words, $\alpha = (12)$ switches $\{1, 2\}$ and leaves everything else alone and $\beta = (13)$ switches $\{1, 3\}$ and leaves everything else alone. These are both elements of S_n for $n \geq 3$.

Let's look at $\alpha \circ \beta$ and $\beta \circ \alpha$. I should look at 1, 2, 3 and $k \geq 4$ separately when we compute $\alpha(\beta(i))$ and $\beta(\alpha(i))$

$$\begin{aligned}
\beta(1) = 3 \quad \alpha(3) = 3 &\implies (\alpha \circ \beta)(1) = 3, \quad 1 \mapsto 3 \mapsto 3; \\
\beta(2) = 2 \quad \alpha(2) = 1 &\implies (\alpha \circ \beta)(2) = 1, \quad 2 \mapsto 2 \mapsto 1; \\
\beta(3) = 1 \quad \alpha(1) = 2 &\implies (\alpha \circ \beta)(3) = 2, \quad 3 \mapsto 1 \mapsto 2; \\
\beta(k) = k \quad \alpha(k) = k &\implies (\alpha \circ \beta)(k) = 3, \quad k \mapsto k \mapsto k; \\
&\implies \alpha \circ \beta = (132)(4) \cdots (n).
\end{aligned}$$

$$\begin{aligned}
\alpha(1) = 2 \quad \beta(2) = 2 &\implies (\beta \circ \alpha)(1) = 2, \quad 1 \mapsto 2 \mapsto 2; \\
\alpha(2) = 1 \quad \beta(1) = 3 &\implies (\beta \circ \alpha)(2) = 3, \quad 2 \mapsto 1 \mapsto 3; \\
\alpha(3) = 3 \quad \beta(3) = 1 &\implies (\beta \circ \alpha)(3) = 1, \quad 3 \mapsto 3 \mapsto 1; \\
\alpha(k) = k \quad \beta(k) = k &\implies (\beta \circ \alpha)(k) = 3, \quad k \mapsto k \mapsto k; \\
&\implies \beta \circ \alpha = (123)(4) \cdots (n).
\end{aligned}$$

The two calculations is very similar, but notice that $\beta \circ \alpha$ is like $\alpha \circ \beta$ if we just switched the 2 and the 3.

Since $(132) \neq (123)$, it follows that $(12) \circ (13) \neq (13) \circ (12)$ and S_n is not abelian. $\square$

The argument we made above can work more generally. Suppose i, j, k are three different elements of $\{1, 2, \ldots, n\}$. Then $(ij) \circ (ik) = (ikj)$.

Let's review what we've seen of S_3:

$$\rho_0 = \begin{pmatrix} 123 \\ 123 \end{pmatrix} = (1)(2)(3), \quad \rho_1 = \begin{pmatrix} 123 \\ 231 \end{pmatrix} = (123),$$

$$\rho_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (132), \quad \mu_1 = \begin{pmatrix} 123 \\ 132 \end{pmatrix} = (1)(23),$$

$$\mu_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (13)(2), \quad \mu_3 = \begin{pmatrix} 123 \\ 213 \end{pmatrix} = (12)(3).$$

We also know that ρ_0 is the identity element, $\{\rho_0, \rho_1, \rho_2\}$ form a cyclic group of order 3 and $\mu_j^2 = \rho_0$ for $j = 1, 2, 3$. We've argued by looking at whether the triangle is flipped, we've seen that $\rho_i \circ \rho_j$ will be some ρ_k and $\rho_i \circ \mu_j$ or $\mu_i \circ \rho_j$ will be some μ_k. Unless we know the answer, the subscript is mysterious. This is enough to fill in 18 of the 36 places.

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	$\mu_?$	$\mu_?$	$\mu_?$
ρ_2	ρ_2	ρ_0	ρ_1	$\mu_?$	$\mu_?$	$\mu_?$
μ_1	μ_1	$\mu_?$	$\mu_?$	ρ_0	$\rho_?$	$\rho_?$
μ_2	μ_2	$\mu_?$	$\mu_?$	$\rho_?$	ρ_0	$\rho_?$
μ_3	μ_3	$\mu_?$	$\mu_?$	$\rho_?$	$\rho_?$	ρ_0

We know a few more things that have been worked out in class yesterday, and corrected today. For example, we showed that $\mu_1 \circ \mu_2 = \rho_1$ and $\mu_2 \circ \mu_1 = \rho_2$, and from the worksheet $\rho_2 \circ \mu_2 = \mu_3$ and $\mu_2 \circ \rho_2 = \mu_1$. Let's put these in (in red for the lecture, though it won't show up in the end of the week document.)

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	$\mu_?$	$\mu_?$	$\mu_?$
ρ_2	ρ_2	ρ_0	ρ_1	$\mu_?$	μ_3	$\mu_?$
μ_1	μ_1	$\mu_?$	$\mu_?$	ρ_0	ρ_1	$\rho_?$
μ_2	μ_2	$\mu_?$	μ_1	ρ_2	ρ_0	$\rho_?$
μ_3	μ_3	$\mu_?$	$\mu_?$	$\rho_?$	$\rho_?$	ρ_0

There are still 14 question marks, but I claim that we are actually done, provided we remember the rules that elements in all rows and columns have to be different.

Let's look at $\rho_2 \circ \mu_1$. It can't be ρ_2, ρ_0, ρ_1 or μ_3, because they already appear in the row, and it can't be μ_1, because it's already in the column, so *without any calculation!* we know that $\rho_2 \circ \mu_1 = \mu_2$ – it's the only choice left.

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	$\mu_?$	$\mu_?$	$\mu_?$
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	$\mu_?$
μ_1	μ_1	$\mu_?$	$\mu_?$	ρ_0	ρ_1	$\rho_?$
μ_2	μ_2	$\mu_?$	μ_1	ρ_2	ρ_0	$\rho_?$
μ_3	μ_3	$\mu_?$	$\mu_?$	$\rho_?$	$\rho_?$	ρ_0

Looking at the same row now forces is to see that $\rho_2 \circ \mu_3 = \mu_1$, because it's the only element left!

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	$\mu_?$	$\mu_?$	$\mu_?$
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	$\mu_?$	$\mu_?$	ρ_0	ρ_1	$\rho_?$
μ_2	μ_2	$\mu_?$	μ_1	ρ_2	ρ_0	$\rho_?$
μ_3	μ_3	$\mu_?$	$\mu_?$	$\rho_?$	$\rho_?$	ρ_0

Since the columns are different, we can fill out the ρ_1 row, and this completes the $\rho \circ \mu$ block. Identical reasoning lets us fill out the $\mu \circ \rho$ block as well, leaving only $\mu \circ \mu$, which is by now really forced.

You might enjoy copying this table and trying to finish it on your own.

Maybe not.

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

As a check, let's do $\mu_3 \circ \rho_1$:

$$\mu_3 \circ \rho_1 = \begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 231 \end{pmatrix} \implies$$

$$1 \mapsto 2 \mapsto 1, \quad 2 \mapsto 3 \mapsto 3, \quad 3 \mapsto 1 \mapsto 2, \implies$$

$$\mu_3 \circ \rho_1 = \begin{pmatrix} 123 \\ 132 \end{pmatrix} = \mu_1.$$

September 11, 2020, in class

A few general remarks about homeworks.

I'm not very happy when I see an answer with no explanation. A good explanation can give substantial partial credit when the answer has a glitch. I can also help you understand better when I know what you are thinking.

As I've said, I encourage you to work together on the homework, but please check your work before you submit it. It's awkward for me to see the identical silly typo in several papers!

On HW 1, I will weight problem 5 less, but usually all problems have equal weight.

Just some quick review. Suppose you have a group $(G, *)$ and its multiplication table. For any $x \in G$, you can write down the powers from only looking at the table $x^2 = x * x, x^3 = x * (x^2)$.

In some cases, you are luck and find that $e, x, x^2, \cdots, x^{m-1}$ are distinct and are the elements of G in some order and that $x^m = e$. In this case, $(G, *)$ is a cyclic group of order m.

So, for example, you showed in HW1 that $((\mathbb{Z}/14\mathbb{Z})^*, \odot)$ is a cyclic group of order 6 with generators $[3]_{14}$ or $[5]_{14}$. You can work out the powers just from looking at the table. You don't have to calculate 5^5 and reduce it mod 14.

	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	15	3	1

Look at the powers: $5^2 = 5 * 5 = 11$, $5^3 = 5 * 5^2 = 5 * 11 = 13$, $5^4 = 5 * 5^3 = 5 * 13 = 9$, $5^5 = 5 * 5^4 = 5 * 9 = 3$, $5^6 = 5 * 3 = 1$.

Also, $11^2 = 11 * 11 = 9$, $11^3 = 11 * 11^2 = 9 * 11 = 1$, so $\langle \{[11]_{14} \rangle$ is a cyclic subgroup of order 3.

For fun, notice that $13 \equiv -1 \mod 14$,

How do you make an isomorphism from a $G = \langle x \rangle$ that is cyclic with order m and generator x with the more familiar $C_m = \langle a \rangle$? It is very easy: define Φ so that

$$\Phi(a^k) = x^k.$$

Then $\Phi(a^k * a^j) = \Phi(a^{k+j}) = x^{k+j} = x^k * x^j$, $\Phi(a^m) = x^m = e$, etc.

So to give an isomorphism from C_6 to $((\mathbb{Z}/14\mathbb{Z})^*, \odot)$, one is

$$\Phi(e) = [1]_{14}, \Phi(a) = [3]_{14}, \Phi(a^2) = [3^2]_{14} = [9]_{14},$$
$$\Phi(a^3) = [3^3]_{14} = [9 * 3]_{14} = [13]_{14}\Phi(a^4) = [3^4]_{14} = [13 * 3]_{14} = [11]_{14},$$
$$\Phi(a^5) = [3^5]_{14} = [11 * 3]_{14} = [5]_{14}.$$

You could give a second isomorphism Φ' by $\Phi'(a) = [5]_{14}$, because $(\mathbb{Z}/14\mathbb{Z})^* = \langle [3]_{14} \rangle = \langle [5]_{14} \rangle$. Any generator will do.

How do you check that a subset H of a group $(G, *)$ is a subgroup? You check that it is closed under $*$, that it contains the identity and that it contains the inverses of every element in it.

One type of subgroup works for every group $(G, *)$. For $x \in G$ take $\langle x \rangle$. This will always be closed under $*$, it has the identity and inverses.

When G is a cyclic group, this is the only possible kind of subgroup: The subgroups of C_n are $\langle x^k \rangle$, where k divides n.

It is possible for G to be not a cyclic group and this is true for proper subgroups too: take V or S_3.

I think we already saw that the only subgroups of V are

$$\{e\}, \{e, X\}, \{e, Y\}, \{e, Z\}, \{e, X, Y, Z\}$$

Here's the multiplication table for S_3

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Let's find all the subgroups of S_3.

The identity ρ_0 is in every subgroup. Suppose H is a subgroup of G and $\rho_1 \in H$. Then $\rho_1 \circ \rho_1 = \rho_2 \in H$ and since $\rho_1^3 = \rho_0$, $\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$ is a subgroup of S_3. You can also check that $\langle \rho_2 \rangle = \{\rho_0, \rho_1, \rho_2\}$. Suppose H is a subgroup that contains ρ_2. The same argument shows that H contains $\{\rho_0, \rho_1, \rho_2\}$.

Now suppose a subgroup H contains all the ρ_j's and one of the μ_i's. One look at the multiplication table shows that you get the other two μ_i's as well, so $H = S_3$.

So any other subgroup cannot have ρ_1 or ρ_2. If it has one μ_j, since $\mu_j \circ \mu_j = \rho_0$, we have the three subgroups $\langle \mu_j \rangle = \{\rho_0, \mu_j\}$. Suppose a subgroup H has two different μ_j's, say μ_j and μ_k. Then it has $\mu_j \circ \mu_k$, which will be ρ_1 or ρ_2, so we get all of S_3.

This gets harder as the groups get larger.

WORKSHEET PROBLEM

1. Suppose α and β are two permutations in S_5 given by

$$\alpha = \begin{pmatrix} 12345 \\ 24135 \end{pmatrix} = (1243)(5), \qquad \beta = \begin{pmatrix} 12345 \\ 35124 \end{pmatrix},$$

a. Write β in cycle form.

b. Compute $\alpha \circ \beta$. (Remember that $(\alpha \circ \beta)(i) = \alpha(\beta(i))$.)

WORKSHEET PROBLEM SOLUTION

For reference:

$$\alpha = \begin{pmatrix} 12345 \\ 24135 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 12345 \\ 35124 \end{pmatrix},$$

a. So $\alpha = (1243)(5)$ and $\beta = (13)(254)$ and $\alpha(\beta(i))$ is given by

$$\begin{aligned}
\alpha(1) = 2 \quad \beta(1) = 3 &\implies (\alpha \circ \beta)(1) = \alpha(3) = 1 \\
\alpha(2) = 4 \quad \beta(2) = 5 &\implies (\alpha \circ \beta)(2) = \alpha(5) = 5 \\
\alpha(3) = 1 \quad \beta(3) = 1 &\implies (\alpha \circ \beta)(3) = \alpha(1) = 2 \\
\alpha(4) = 3 \quad \beta(4) = 2 &\implies (\alpha \circ \beta)(4) = \alpha(2) = 4 \\
\alpha(5) = 5 \quad \beta(5) = 4 &\implies (\alpha \circ \beta)(5) = \alpha(4) = 3.
\end{aligned}$$

so

$$\alpha \circ \beta = \begin{pmatrix} 12345 \\ 15243 \end{pmatrix} = (1)(253)(4).$$