Math 417 – Seventh Day

Bruce Reznick
University of Illinois at Urbana-Champaign

September 8, 2020

Welcome back. I hope you had a restful break.

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.

SOLUTION to 1. 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.

SOLUTION to 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

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

You could write these as $\{[0]_2\} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \{[0]_3\}$

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

$$\langle 1 \rangle = \{1, 2, 3, \dots\} = \mathbb{N}$$

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

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

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.)

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

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,

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

.002398081534772182254196642685851318944844 1247 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 $r = 6$,

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

$$\frac{1}{10^r} \cdot \left(1 + \frac{1}{10^r} + \frac{1}{10^{2r}} + \frac{1}{10^{3r}} + \cdots\right)$$

$$\frac{1}{10^r} \cdot \sum_{k=0}^{\infty} \frac{1}{(10^r)^k} = \frac{1}{10^r} \cdot \frac{1}{1 - \frac{1}{10^r}} = \frac{1}{10^r - 1}.$$

□

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. $\square$

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

$$\frac{4}{13} = \frac{4 \cdot 76923}{13 \cdot 76923} = \frac{307692}{999999} = 307692 \cdot \frac{1}{999999}$$

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

$$= .307692\ 307692\ 307692\ 307692 \ldots$$

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. You probably know that $\frac{1}{11}$ has a nice decimal expression

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

So we can think of it in two ways:

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

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

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

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

We say that σ is a *permutation* of A.

At the beginning at least, we will take $A = \{1, \ldots n\}$. 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 have

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

Since ρ acts as follows

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

we'd write $\rho = (14)(235) = (352)(41)$, 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

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

Let's do it the other way

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

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 give 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.