Chapter 3: 1d, 2bd, 3, 5, 7, 12.
Due date: Friday, 9/19

NOTE: the numbers listed above correspond to the printed version of the textbook, generated from 2013/08/16 source files.

1. Find all $x \in \mathbb{Z}$ satisfying the following equation: $9x \equiv 3 \pmod 5$.

Solution: By definition, an integer x satisfies $9x \equiv 3 \pmod 5$ if and only if $9x = 5y + 3$ for some $y \in \mathbb{Z}$.

To gain some intuition about which integers satisfy this relation, first consider the integers n for which $9n = 5m$ for some $m \in \mathbb{Z}$. Since $\gcd(5, 9) = 1$, the only such n that work are multiples of 5. That is, $n \in \{\dots, -5, 0, 5, 10, \dots\}$.

Consider the equation $9x = 5y + 3$. Is there a way to add some number to both the left and right sides so that we are back in the easy case of $9n = 5m$? Indeed, there is:

$$\begin{aligned} & 9x &=& 5y + 3 \\ \Leftrightarrow \quad & 9x - 18 &=& 5y + 3 - 18 \\ \Leftrightarrow \quad & 9x - 18 &=& 5y + -15 \\ \Leftrightarrow \quad & 9(x - 2) &=& 5(y - 3) \end{aligned}$$

So, the x that satisfy $9x \equiv 3 \pmod 5$ are those satisfying

$$x - 2 \in \{\dots, -5, 0, 5, 10, \dots\}.$$

That is, $x \in \{\dots, -3, 2, 7, 14, \dots\}$.

2. Which of the following multiplication tables defined on the set $G = \{a, b, c, d\}$ form a group? Support your answer in each case.

(b)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

(d)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	b	a	d
d	d	d	b	c

Solution:

(b) This is the multiplication table of a group. We prove this by checking that it satisfies the group properties:

Denote the universe by X, so $X = \{a, b, c, d\}$.

- (existence of identity) Clearly a behaves as an identity element.

- (existence of inverses) In this case, every element is its own inverse, since, for each $x \in X$, we have $x \circ x = a$.
- (closure) Clear, since all the elements in the table come from the set $\{a, b, c, d\}$.
- (associativity) We must show, for all $x, y, z \in X$, $(x \circ y) \circ z = x \circ (y \circ z)$. Fix three elements $x, y, z \in X$. We split the proof into cases.

Case 1: Suppose at least one of x, y, z is the identity element, a. Associativity is trivial in this case. (For example, $(x \circ a) \circ z = x \circ z = x \circ (z \circ z)$.)

Case 2: Suppose $x, y, z \in \{b, c, d\}$, and suppose the three elements are distinct. Then $x \circ y = z$, $x \circ z = y$, and $y \circ z = x$, so,

$$(x \circ y) \circ z = z \circ z = a = x \circ x = x \circ (y \circ z).$$

Case 3: Suppose exactly two of $x, y, z \in \{b, c, d\}$ are the same, say $x = y \neq z$. Let w be the third element in $\{b, c, d\}$–i.e., the element not equal to x or z. Then $w = x \circ z$ and $z = x \circ x$, so,

$$(x \circ y) \circ z = (x \circ x) \circ z = a \circ z = z = x \circ w = x \circ (x \circ z) = x \circ (y \circ z).$$

The cases $x = z \neq y$ and $x \neq y = z$ are handled similarly.

Case 4: Assume all three elements are the same, $x = y = z$. Then,

$$(x \circ y) \circ z = (x \circ x) \circ x = a \circ x = x = x \circ a = x \circ (x \circ x) = x \circ (y \circ z).$$

(d) This is not the Cayley table of a group. If it were, then a would have to be the identity, but then d has no inverse. (There are other ways to see that this Cayley table does not give a group.)

3. Write out Cayley tables for groups formed by the symmetries of a rectangle and for $(\mathbb{Z}_4, +)$. How many elements are in each group? Are the groups the same? Why or why not?

Solution:

Symmetries of a rectangle

The "universe" (or set of elements of the group) is $G = \{e, \mu_1, \mu_2, \rho\}$. This is a multiplicative group with identity element e, so the group is formally denoted as $\mathbf{G} = \langle G, \cdot, ^{-1}, e \rangle$.

The elements in the universe of $\mathbf{G}$ act on the set $\{1, 2, 3, 4\}$ by permuting the elements of this set in certain ways. To describe this action, imagine a rectangle with vertices labeled counter-clockwise: 1 in the south-west corner, 2 in the south-east corner, 3 in the north-east corner, and 4 in the north-west corner. The result looks something like this:

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

- The identity element (leaves all four corners of the square fixed) $e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$
- Reflection across a vertical line $\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

- Rotation by 180 degrees $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$
- Reflection across a horizontal line $\mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

The cyclic group $\mathbb{Z}_4$

For the group $\mathbb{Z}_4$, the universe is the set $\{(0), (1), (2), (3)\}$ of congruence classes of integers modulo 4. The binary operation is addition modulo 4, and the identity element is the class (0). Thus, we formally write this group as $\mathbb{Z}_4 = \langle\{(0), (1), (2), (3)\}, +, -, (0)\rangle$.

The Cayley tables

The Cayley tables below were generated using Sage.

(See the worksheet SymmetriesOfRectangle.sagews, in our GitHub repository:
https://github.com/williamdemeo/Math301-Fall2014/tree/master/sage)

$*$	e	μ_1	ρ	μ_2
e	e	μ_1	ρ	μ_2
μ_1	μ_1	e	μ_2	ρ
ρ	ρ	μ_2	e	μ_1
μ_2	μ_2	ρ	μ_1	e

$+$	(0)	(1)	(2)	(3)
(0)	(0)	(1)	(2)	(3)
(1)	(1)	(2)	(3)	(0)
(2)	(2)	(3)	(0)	(1)
(3)	(3)	(0)	(1)	(2)

It is clear from inspection of the two Cayley tables that these two groups are not the same. For example, every element of the group **G** is its own inverse, so has order 2. On the other hand $\mathbb{Z}_4$ has two elements of order 4, (namely (1) and (3)), which generate the whole group. Another way to see that the groups are different from inspecting the Cayley table is to notice that $\mathbb{Z}_4$ has only one proper nontrivial subgroup, with universe $\{(0), (2)\}$, whereas **G** has three proper nontrivial subgroups, with universes $\{e, \mu_1\}$, $\{e, \mu_2\}$, and $\{e, \rho\}$, respectively.

5. Describe the symmetries of a square and prove that the set of symmetries is a group. Give a Cayley table for the symmetries. How many ways can the vertices of a square be permuted? Is each permutation necessarily a symmetry of the square? The symmetry group of the square is denoted by D_4.

Solution: The group of symmetries of a square is also known as the dihedral group on four letters and is denoted by D_4. Here "letters" are the points that are moved under the rigid motion, in this case, the vertices of the square. Below, we will label the vertices of the square with numbers 1, 2, 3, 4, so for us the set of letters will be $\{1, 2, 3, 4\}$.

Important Note: The set $\{1, 2, 3, 4\}$ is *not* the universe of elements of this group! It is merely a set that the group elements "act upon."

In fact, the dihedral group acting on the set $\{1, 2, 3, 4\}$ has 8 elements. To identify the elements of this group, imagine a square with vertices labeled counter-clockwise: 1 in the south-west corner, 2 in the south-east corner, 3 in the north-east corner, and 4 in the north-west corner. The result

looks something like this:

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

The universe of this group is $\{e, \mu_1, \mu_2, \mu_3, \mu_4, \rho_1, \rho_2, \rho_3\}$, the elements of which are defined as follows:

- The identity element (leaves all four corners fixed) $e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$
- Reflection across a 45 degree line $\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$
- Reflection across a vertical line $\mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$
- Rotation by 90 degrees $\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$
- Reflection across a -45 degree line $\mu_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$
- Rotation by 180 degrees $\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$
- Rotation by 270 degrees $\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$
- Reflection across a horizontal line $\mu_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

The Cayley table of the group on symmetries of a square is the following:

$*$	e	μ_1	μ_2	ρ_1	μ_3	ρ_2	ρ_3	μ_4
e	e	μ_1	μ_2	ρ_1	μ_3	ρ_2	ρ_3	μ_4
μ_1	μ_1	e	ρ_1	μ_2	ρ_2	μ_3	μ_4	ρ_3
μ_2	μ_2	ρ_3	e	μ_3	ρ_1	μ_4	μ_1	ρ_2
ρ_1	ρ_1	μ_4	μ_1	ρ_2	μ_2	ρ_3	e	μ_3
μ_3	μ_3	ρ_2	ρ_3	μ_4	e	μ_1	μ_2	ρ_1
ρ_2	ρ_2	μ_3	μ_4	ρ_3	μ_1	e	ρ_1	μ_2
ρ_3	ρ_3	μ_2	μ_3	e	μ_4	ρ_1	ρ_2	μ_1
μ_4	μ_4	ρ_1	ρ_2	μ_1	ρ_3	μ_2	μ_3	e

The number of ways to permute any set of four elements (including the labels on four corners of a square) is $4! = 24$. However, we see from the foregoing description of D_4 that only 8 of these 24 permutations represent symmetries of a square.

7. Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

Solution: It follows from commutativity of addition and multiplication that $*$ is commutative. The identity element is $0 \in S$, since $a * 0 = a + 0 + a0 = 0 + a + 0a = 0 * a$. For each $a \in S$, we have

$$a + b + ab = 0 \Leftrightarrow a + (1 + a)b = 0 \Leftrightarrow -a/(1 + a) = b.$$

So, $-a/(1 + a)$ is an inverse for a, which always exists because $-1 \notin S$. (Associativity of $*$ was proved in lecture.)

12. Let $\mathbb{Z}_2^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{Z}_2\}$. Define a binary operation on $\mathbb{Z}_2^n$ by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

Prove that $\mathbb{Z}_2^n$ is a group under this operation. This group is important in algebraic coding theory.

Solution:

- (existence of identity) Clearly $\bar{0} = (0, 0, \ldots, 0)$ is the identity element.
- (existence of inverses) If $\bar{a} = (a_1, a_2, \ldots, a_n)$, then note that $\bar{a} + \bar{a} = (a_1 + a_1, a_2 + a_2, \ldots, a_n + a_n) = (0, 0, \ldots, 0)$, so every element is its own inverse.
- (associativity) Obvious, since addition modulo 2 is associative.
- (closure) Obvious, since the set $\{0, 1\}$ is closed under addition modulo 2.