# Chapter 1

**Exercise 1.1:**

$$(x+y)^2 = x^2 + 2xy + y^2$$
$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$
$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$
$$(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$$

For $n = 2, 3, 4, 5$, the coefficients of the terms in the expansion of $x + y)^n$ are the same as the entries of row $n$ for Pascal's Triangle.

**Exercise 1.2:** The top row of Pascal's triangle is indexed row $n = 0$ rather than $n = 1$ to keep the correspondence between the coefficients of the terms in the expansion of $(x + y)^n$ and the entries of row $n$ for Pascal's Triangle, as observed in Exercise 1.2. Note that $(x + y)^0 = 1$, so this correspondence even works for $n = 0$.

**Exercise 1.3:** For simplicity, label the four people $P_1$, $P_2$, $P_3$, and $P_4$:

- There are 4 ways to choose a one person subcommittee, that is, pick one of $P_1$, $P_2$, $P_3$, or $P_4$.

- The 6 possibilities for a two person subcommittee are

$$P_1, P_2 \qquad P_1, P_3 \qquad P_1, P_4 \qquad P_2, P_3 \qquad P_2, P_4 \qquad P_3, P_4$$

- There are 4 ways to choose a three person subcommittee. One way to do this is leave out $P_1$, $P_2$, $P_3$, or $P_4$:

$$P_1, P_2, P_3 \qquad P_1, P_2, P_4 \qquad P_1, P_3, P_4 \qquad P_2, P_3, P_4$$

Note that the number of outcomes for the different size subcommittees come from row 4 of Pascal's Triangle. They are also binomial coefficients.We see

$$\binom{4}{1} = \frac{4!}{1!3!} = 4 \qquad \binom{4}{2} = \frac{4!}{2!2!} = 6 \qquad \binom{4}{3} = \frac{4!}{3!1!} = 4$$

The order in which we choose students does not matter. For example, the subcommittee $P_1, P_2$ is the same as $P_2, P_1$, which is why we only list one when counting the two person subcommittees.

**Exercise 1.4:** The number of ways to choose 8 students from a group of 30 (again, the order in which we pick them does not matter) is the following.

$$\binom{30}{8} = 5,852,925.$$

**Exercise 1.5:** There is one way to choose a subcommittee with no students. Simply, do not pick anyone. In terms of a binomial coefficient, we can represent this as

$$\binom{n}{0} = \frac{n!}{0!n!} = 1$$

recalling that $0! = 1$. This is in agreement with the left edge of Pascal's Triangle consisting solely of ones.

**Exercise 1.7:**

| $\oplus$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $\oplus$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| $\oplus$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

Just as in $\mathbb{Z}_5$, 0 is the additive identity for $\mathbb{Z}_2$, $\mathbb{Z}_3$, and $\mathbb{Z}_5$. Likewise, for all three addition tables, we see that each element has an additive inverse, the addition is commutative, and each row and column in the table is a rearrangement (permutation) of the underlying set. One difference worth noting is that in $\mathbb{Z}_2$, each element is its own inverse. That is not true for the other sets.

**Exercise 1.11:** One such function is $f_1 : S \longrightarrow S$ given by $f_1(1) = 2$, $f_1(2) = 3$, $f_1(3) = 4$, $f_1(4) = 1$, $f_1(5) = 6$, $f_1(6) = 7$, $f_1(7) = 5$, $f_1(8) = 5$, $f_1(9) = 6$, and $f_1(10) = 7$.

Another such function is $f_2 : S \longrightarrow S$ given by $f_2(1) = 2$, $f_2(2) = 3$, $f_2(3) = 4$, $f_2(4) = 1$, $f_2(5) = 6$, $f_2(6) = 7$, $f_2(7) = 5$, $f_2(8) = 1$, $f_2(9) = 8$, and $f_2(10) = 9$.

Note that the directed graphs of $f_1$ and $f_2$ are not the same. There are many other functions that also satisfy the given criteria, but have different directed graphs.

**Exercise 1.12:** Let $f : S \longrightarrow S$. Since $|S| = 6$, there are six choices for $f(x)$ and, likewise, six choices for the images of the other five elements of $S$. Since these choices are independent, the multiplication principle gives $6^6 = 46,656$ total functions from $S$ to itself. Hence, there are the same number of directed graphs, although many will have the same structure (i.e., be graph isomorphic).

The minimum number of connected components for such a directed graph is 1. One example of a function that gives a graph with one connected component is

$f(x) = y$, $f(y) = u$, $f(u) = v$, $f(v) = w$, $f(w) = z$, and $f(z) = x$. There are many other examples as well.

The maximum number of connected components is 6. The only function which satisfies this condition is the identity map $f : S \longrightarrow S$ given by $f(a) = a$ for all $a \in S$.

**Exercise 1.13:** This exercise is a direct generalization of Exercise 1.12. By the same argument, there are $n^n$ functions from an $n-$element set to itself. The minimum number of connected components is 1, and there are many ways to construct functions whose directed graphs contain only one connected component. The maximum number of connected components is $n$ and this can only be achieved via the identity map.

**Exercise 1.15:** i) Let $\boldsymbol{s_{n+1}} \in S_{n+1}$. By definition, there is some $\boldsymbol{s_0} \in S_0$ such that $f^{n+1}(\boldsymbol{s_0}) = \boldsymbol{s_{n+1}}$. Then the directed graph of $f$ contains a path of length $n+1$ starting at $\boldsymbol{s_0}$ and ending at $\boldsymbol{s_{n+1}}$. Let $\boldsymbol{s_1} = f(\boldsymbol{s_0})$. This means that there is a path of length $n$ in the directed graph starting at $\boldsymbol{s_1}$ and ending at $\boldsymbol{s_0}$. But since $S_0 = S$, $\boldsymbol{s_1} \in S_0$, and thus $\boldsymbol{s_{n+1}} \in S_n$. It follows that $S_n \supseteq S_{n+1}$.

ii) We proceed by induction. $S = S_0 \supseteq S_1$ by definition. Next, assume $S_{n-1} \supseteq S_n$ for some $n \geq 1$ and let $\boldsymbol{s_{n+1}} \in S_{n+1}$. Then there exists some $\boldsymbol{s_n} \in S_n$ such that $f(\boldsymbol{s_n}) = \boldsymbol{s_{n+1}}$. By the induction hypothesis, $\boldsymbol{s_n} \in S_{n-1}$ which means $\boldsymbol{s_{n+1}} \in S_n$.

**Exercise 1.16:** i) Let $q_i = |S_i| \in \mathbb{N}$ for $i \geq 0$. By Exercise 1.15,

$$q_0 \geq q_1 \geq \cdots \geq q_n \geq q_{n+1} \geq \cdots$$

is a set of nonnegative integers. By the Well-Ordering Principle, this set must contain a smallest element $q_r = N$. Since the sequence is non-increasing, $q_i = N$ for all $i \geq r$. But since $S_n \supseteq S_{n+1}$, it must be the case that $S_n = S_N$ for all $n \geq N$.

ii) If $N = 0$, $S_n = S_0$ for all $n$, that is, all states lie on oriented cycles and there are no transients.

iii) The transient states are elements of $S_0 \backslash S_N$.

**Exercise 1.17:** Yes, it is possible to construct a function on $S$ without Garden-of-Eden states. Any function whose directed graph consists solely of states on cycles satisfies this.

It is not possible to construct a function where every state is a Garden-of-Eden state. If $x \in S$, then $f(x)$ is not a Garden-of-Eden state by definition.

For a set $S$ with $n$ elements, the largest possible number of Garden-of-Eden states is $n-1$. If $S = \{1, 2, ..., n\}$, a function that satisfies this condition is $f(x) = 1$ for all $x \in S$. Then $2, 3, ..., n$ are all Garden-of-Eden states.

**Exercise 1.18:** Let $S = \{1, 2, ..., 8\}$. Then $f_1(x) = 1$ for all $x \in S$ produces a directed graph with 7 transient states and a unique cycle of length 1. The graph has one connected component. A second function which satisfies these criteria is $f_2(x) = x + 1$ for $1 \leq x \leq 7$ and $f_2(8) = 8$. There are other functions as well. In all such cases, the corresponding directed graphs all have exactly one connected component since there is only one cycle state.

**Exercise 1.19:** The smallest positive integer $n$ such that $f^n$ is the identity map is the least common multiple of the cycle lengths, i.e., $\text{lcm}(1, 2, 3, 4, 5, 6, 8, 9, 12) = 360$.

**Exercise 1.21:** We denote the orbit of $u$ by $\text{orb}(u)$. For Example 1.10:

$\text{orb}(1)=\{1, 5, 5, 5, ...\}$
$\text{orb}(2)=\{2, 8, 4, 2, 8, 4, ...\}$
$\text{orb}(3)=\{3, 4, 2, 8, 4, 2, 8, ...\}$
$\text{orb}(4)=\{4, 2, 8, 4, 2, 8, ...\}$
$\text{orb}(5)=\{5, 5, 5, ...\}$
$\text{orb}(6)=\{6, 2, 8, 4, 2, 8, 4, ...\}$
$\text{orb}(7)=\{7, 8, 4, 2, 8, 4, 2, ...\}$
$\text{orb}(8)=\{8, 4, 2, 8, 4, 2, ...\}$

For Example 1.14:

$\text{orb}(1)=\{1, 2, 3, 4, 5, 6, 4, 5, 6, ...\}$
$\text{orb}(2)=\{2, 3, 4, 5, 6, 4, 5, 6, ...\}$
$\text{orb}(3)=\{3, 4, 5, 6, 4, 5, 6, ...\}$
$\text{orb}(4)=\{4, 5, 6, 4, 5, 6, ...\}$
$\text{orb}(5)=\{5, 6, 4, 5, 6, 4, ...\}$
$\text{orb}(6)=\{6, 4, 5, 6, 4, 5, ...\}$

# Chapter 2

**Exercise 2.1:** i) If a sub-row of $n$ consecutive 0s appears, then beneath it a sub-row of $n-1$ consecutive 0s must appear due to Pascal's Rule and the fact that $0 + 0 = 0$. Beneath this, a sub-row of $n-2$ consecutive 0s is found, and so on. This is what causes triangular regions of zeros in the mod 5 triangle.

ii) The values which appear above the first sub-rows of zeros are alternating 1s and 4s or 2s and 3s. When these pairs align in this way, a row of zeros results underneath since $1 + 4 \equiv 0 \bmod 5$ and $2 + 3 \equiv 0 \bmod 5$. In other words, 1 and 4

are additive inverses of each other with respect to mod 5 addition as are 2 and 3.

iii) The first 25 rows of the mod 5 triangle contain 15 sub-triangles of non-zero elements. The value down the side of each of these is the same as the one found in the corresponding position of the first five rows of the mod 5 triangle. The same is true of the analogous 15 sub-triangles in the first 125 rows.

**Exercise 2.2:** This question is subjective at this point, so there are no wrong answers. But the complexities of these images will soon be described in mathematically precise ways!

**Exercise 2.3:**
Simplest Visual Class: $n = 29$.
Middle Visual Class: $n = 9, 16, 27$.
Most Complex Visual Class: $n = 15, 18, 26$.

**Exercise 2.4:** If the modulus $n = p$ where $p$ is a prime, then it is best to display $p^n$ rows for $n \geq 1$ to see a "complete" pattern. If $n = p^q$ for some $q \geq 2$, then displaying $p^r$ rows for any $r \geq q$ works well. For the mod 6 triangle, there is no optimal number of rows to make all patterns in the triangle seem complete. This is also true for other moduli $n$ which are the products of two or more relatively prime factors.

**Exercise 2.5:** We proceed by induction.

Base case: $n = 2$.

The first four rows of the mod 2 triangle are shown below.

We see that these rows consist of 3 copies of the first two rows surrounding a single 0 in the middle.

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 0 & & 1 & \\ 1 & & 1 & & 1 & & 1 \end{array}$$

Now assume that the first $2^n$ rows consist of 3 copies of the first $2^{n-1}$ rows surrounding an inverted sub-triangle of zeros for some fixed $n \geq 2$. Then by this induction hypothesis the last row, i.e., row $2^n - 1$ consists of all $1s$ and there are $2^n$ of them. This means that row $2^n$ is the following:

$$1 \quad 0 \quad 0 \quad \cdots \quad 0 \quad 0 \quad 1$$

Here, there are $2^n - 1$ zeros between the $1s$. These zeros form the top row of an inverted sub-triangle of zeros with $2^n - 1$ rows. In addition, $1s$ must lie along

the left and right boundary of this zero sub-triangle. This creates two copies of the first $2^n$ rows to the left and right of the zero sub-triangle. Hence, the first $2^{n+1}$ rows must be 3 copies of the first $2^n$ rows surrounded by this inverted sub-triangle of zeros.

**Exercise 2.7:** The counts are shown in the table below. Initially, there are more 1s than 0s in the top portion of the mod 2 triangle. But somewhere between rows 16 and 32 this relationship flips. Once it does, the number of 0s in the first $n$ rows exceeds the number of 1s. This means that the number of even elements in the first $n$ rows of Pascal's Triangle, for $n$ large, exceeds the number of odd elements.

| number of rows | number $1s$ | number of $0s$ |
|---|---|---|
| $2^0 = 1$ | 1 | 0 |
| $2^1 = 2$ | 3 | 0 |
| $2^2 = 4$ | 9 | 1 |
| $2^3 = 8$ | 27 | 9 |
| $2^4 = 16$ | 81 | 55 |
| $2^5 = 32$ | 243 | 285 |
| $2^6 = 64$ | 729 | 1351 |

**Exercise 2.10:** The sum is 1 if $p > 2$ since the entries in row $p-1$ of the mod $p$ triangle are being added. This row consists of alternating pairs of 1 and $p-1$ until the last entry in the row, which is a 1, appears. For $p = 2$, the sum is zero.

**Exercise 2.11:** The products are as follows:

For $p = 13$, $12^6 \equiv 1 \bmod 13$.
For $p = 17$, $16^8 \equiv 1 \bmod 17$.
For $p = 19$, $18^9 \equiv 18 \bmod 19$.

As with the examples in the text before this exercise, the product is 1 or $p-1$, depending on $p$.

# Chapter 3

**Exercise 3.2:** i) $\mathbb{N}$ is closed under addition, since the sum of two positive integers is a positive integer.

ii) $\mathbb{N}$ is not closed under subtraction. For example, $2, 3 \in \mathbb{N}$ but $2 - 3 = -1 \notin \mathbb{N}$.

iii) The even integers are closed under addition. To see this, suppose $x = 2n$ and $y = 2m$ where $m, n \in \mathbb{Z}$. Then $x + y = 2n + 2m = 2(n + m)$ is an even integer since $m + n \in \mathbb{Z}$.

iv) The odd integers are not closed under addition. For example, 3 and 5 are odd integers, but $3 + 5 = 8$ is not odd.

v) The odd integers are closed under multiplication. To see this, suppose $x = 2n + 1$ and $y = 2m + 1$ where $m, n \in \mathbb{Z}$. Then $xy = (2n + 1)(2m + 1) = 4nm + 2m + 2n + 1 = 2(2nm + m + n) + 1$, which is odd since $2nm + m + n \in \mathbb{Z}$.

**Exercise 3.4:** Yes, $*$ is commutative on $V$. We can see from Table 3.1 that $x * y = y * x$ for all $x, y \in V$.

**Exercise 3.5:** Yes, each element in $V$ has a unique inverse. In fact, each element is its own inverse. This can be seen in Table 3.1 which shows $x * x = e$ for all $x \in V$. Note that the identity $e$ is the only entry on the main forward diagonal of the table, which is one way to see this.

**Exercise 3.6:** Yes, $*$ appears to be associative on $V$ by testing some cases. For example,

$$b * (a * b) = b * c = a = c * b = (b * a) * b.$$

Any other case you test also works, which means that $*$ is associative on $V$. However, if you wanted to test all possible cases from the table in this way, there are $4^3 = 64$ equations to be verified.

**Exercise 3.7:** This triangle resembles the mod 2 triangle. It is, in fact, the "same" as the mod 2 triangle in the sense that if you replace $a$ with 1 and $e$ with 0, Pascal's triangle mod 2 results.

**Exercise 3.11:** $r_1 \circ \mu_2 = \mu_1$ but $\mu_2 \circ r_1 = \mu_3$. This says that function composition is not a commutative operation on $S_3$ and, more generally, on $S_n$.

**Exercise 3.12:** i) Yes, we can see from Table 3.2 that the identity element is $r_0$.

ii) Yes, each element has a unique inverse. From Table 3.2 we have the following:

$$r_0^{-1} = r_0 \quad r_1^{-1} = r_2 \quad r_2^{-1} = r_1 \quad \mu_1^{-1} = \mu_1 \quad \mu_2^{-1} = \mu_2 \quad \mu_3^{-1} = \mu_3$$

iii) All of the previously examined finite sets under a binary operation have been commutative. $S_3$ under function composition is our first example that is not commutative.

**Exercise 3.14:** i) Closed subsets of $S_3$:

1-element: $\{r_0\}$

2-element: $\{r_0, \mu_1\}$, $\{r_0, \mu_2\}$, $\{r_0, \mu_3\}$
3-element: $\{r_0, r_1, r_2\}$
4-element: none
5-element: none
6-element: $S_3$

ii) The smallest closed subset that contains both $r_1$ and $\mu_1$ is $S_3$.

**Exercise 3.15:** The $\mu_1$ triangle is really Pascal's triangle mod 2, and the $r_1$ triangle is Pascal's triangle mod 3.

**Exercise 3.16:** Creating a triangle over $S_3$ with $r_1$ down the left and $r_2$ down the right will not produce all six elements of $S_3$. Rather, it will include only elements from $\{r_0, r_1, r_2\}$, which is the smallest closed subset containing $r_1$ and $r_2$. The triangle over $\mathbb{Z}_3$ with 1 down the left and 2 down the right is essentially the same as the triangle over $S_3$ with $r_1$ down the left and $r_2$ down the right. To see this, replace $r_0$, $r_1$, and $r_2$ by 0, 1, and 2, respectively.

**Exercise 3.17:**

$$r_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad r_{180} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad r_{270} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$f_V = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad f_H = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

**Exercise 3.18:**

| $\circ$ | $r_0$ | $r_{90}$ | $r_{180}$ | $r_{270}$ | $f_V$ | $f_H$ | $f_1$ | $f_2$ |
|---|---|---|---|---|---|---|---|---|
| $r_0$ | $r_0$ | $r_{90}$ | $r_{180}$ | $r_{270}$ | $f_V$ | $f_H$ | $f_1$ | $f_2$ |
| $r_{90}$ | $r_{90}$ | $r_{180}$ | $r_{270}$ | $r_0$ | $f_2$ | $f_1$ | $f_V$ | $f_H$ |
| $r_{180}$ | $r_{180}$ | $r_{270}$ | $r_0$ | $r_{90}$ | $f_H$ | $f_V$ | $f_2$ | $f_1$ |
| $r_{270}$ | $r_{270}$ | $r_0$ | $r_{90}$ | $r_{180}$ | $f_1$ | $f_2$ | $f_H$ | $f_V$ |
| $f_V$ | $f_V$ | $f_1$ | $f_H$ | $f_2$ | $r_0$ | $r_{180}$ | $r_{90}$ | $r_{270}$ |
| $f_H$ | $f_H$ | $f_2$ | $f_V$ | $f_1$ | $r_{180}$ | $r_0$ | $r_{270}$ | $r_{90}$ |
| $f_1$ | $f_1$ | $f_H$ | $f_2$ | $f_V$ | $r_{270}$ | $r_{90}$ | $r_0$ | $r_{180}$ |
| $f_2$ | $f_2$ | $f_V$ | $f_1$ | $f_H$ | $r_{90}$ | $r_{270}$ | $r_{180}$ | $r_0$ |

**Exercise 3.19:** i) $r_0$ is the identity.

ii) Yes, each element has a unique inverse. Six of the elements are their own inverse: $r_0$, $r_{180}$, $f_V$, $f_H$, $f_1$, and $f_2$. The remaining two elements $r_{90}$ and $r_{270}$ are inverses of each other.

iii) No, function composition is not a commutative operation on $D_4$. For example, $r_{90}f_V = f_2$ but $f_V r_{90} = f_1$.

iv) When defined, function composition is always associative and, hence, is associative on $D_4$.

**Exercise 3.20:** $f$ interchanges the corners of the square labeled 1 and 2, but fixes the other two corners. This results in a twist of the original square and so $f$ does not leave the square invariant.

**Exercise 3.22:** Placing a single value from $D_4$ down both sides will not generate all 8 elements. In all cases, you only get the smallest closed subset that contains that element. So, only 1, 2, or 4 elements appear, depending on which elements you choose for the sides. $r_{90}$ and $r_{270}$ are the only two that produce 4 of the elements.

**Exercise 3.23:** This is open-ended, and you should experiment with numerous combinations and summarize your observations. But the key takeaway here is that by placing two different elements down the sides, it is possible to get all 8 elements in $D_4$ (or 10 in $D_5$) to appear in the triangle in some cases.

# Chapter 4

**Exercise 4.2:** Let $A = (a_{ij}), B = (b_{ij}) \in M_{n\times n}(\mathbb{R})$ where $1 \leq i, j \leq n$. Then $A + B = (a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) \in M_{n\times n}(\mathbb{R})$, giving closure.

i) If $C = (c_{ij}) \in M_{n\times n}(\mathbb{R})$, then

$$\begin{aligned} A + (B + C) &= (a_{ij}) + ((b_{ij}) + (c_{ij})) \\ &= (a_{ij}) + (b_{ij} + c_{ij}) \\ &= (a_{ij} + (b_{ij} + c_{ij})) \\ &= ((a_{ij} + b_{ij}) + c_{ij}) \\ &= ((a_{ij}) + (b_{ij})) + (c_{ij}) \\ &= (A + B) + C \end{aligned}$$

which shows matrix addition is associative.

ii) The zero matrix $O = (0_{ij})$ is the identity for matrix addition.

iii) For inverses, let $-A = (-a_{ij})$. Then $A + (-A) = -A + A = O$, the zero matrix. Hence, each square matrix has an additive identity.

It follows that $M_{n\times n}(\mathbb{R})$ is a group under matrix addition.

$M_{n\times n}(\mathbb{R})$ is not a group under matrix multiplication. Closure and associativity are satisfied, and the $n \times n$ matrix $I_n$ with 1s down the main diagonal and zeros anywhere else is the multiplicative identity. However, not all square ma-

trices are invertible, i.e., have multiplicative inverses. In particular, those with determinant zero are not invertible.

**Exercise 4.3:** The irrationals $\mathbb{P}$ are not a group under addition. In fact, $\mathbb{P}$ is not closed under addition. For example, $\sqrt{2}, -\sqrt{2} \in \mathbb{P}$ but $-\sqrt{2} + \sqrt{2} = 0 \notin \mathbb{P}$. In addition, there is no additive identity.

**Exercise 4.5:** Let $A = (a_{ij}), B = (b_{ij}) \in M_{n\times n}(\mathbb{R})$. Then $A + B = (a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) = (b_{ij} + a_{ij}) = (b_{ij}) + (a_{ij}) = B + A$. Thus, $M_{n\times n}(\mathbb{R})$ is abelian.

It is not difficult to show that $M_{n\times m}(\mathbb{R})$ is an abelian group. In Exercise 4.2, the assumption that the matrices are square is never used, so the proof also works for $M_{n\times m}(\mathbb{R})$ when $n \neq m$. Likewise, the first part of this exercise generalizes to non-square matrices.

**Exercise 4.6:** Every group $G$ contains at least one element that is its own inverse, namely the identity $e$.

**Exercise 4.7:** In the group $\mathbb{Z}_n$, 0 is its own inverse regardless of $n$ since it is the identity. For $m \neq 0$ to be its own inverse in $\mathbb{Z}_n$, $m + m = 0$. Since $m \in \{1, 2, ..., n-1\}$, this equation only has a solution if $n$ is even. In this case, $n = 2m$. If $n$ is odd, only the identity 0 is its own inverse.

**Exercise 4.8:** If you focus on the sub-triangles with the light blue in Figure 4.2, it is easy to see four different elements (colors) that must be their own inverse. Note that light blue is the identity that is its own inverse. To find the others, just look for two occurrences of the same color side by side with a light blue underneath. Such an element is its own inverse by definition. In the figure, it is easy to see that dark blue has this property. Likewise, the rust and tan colors sitting in the row before the light blue sub-triangles share this property. If you look at the $D_4$ Cayley table, there are actually six elements that are their own inverses.

**Exercise 4.12:** i) First, consider $\{0, 2, 4, 6\} \subset \mathbb{Z}_8$. It is easy to see this set is closed under addition mod 8 by inspection (an even plus on even is always even). Since associativity is inherited by any subset of a group, we need not check it. 0 is the identity of $\{0, 2, 4, 6\}$. Finally, we see that each element in the subset has an inverse back in the set: 0 is its own inverse, as is 4; $-2 = 6$ and $-6 = 2 \bmod 8$. It follows that $\{0, 2, 4, 6\}$ is a subgroup of $\mathbb{Z}_8$.

Since $\{0, 4\}$ is a closed subset of $\{0, 2, 4, 6\}$ containing the identity, 0 and 4 are their own inverses, $\{0, 4\}$ is a subgroup of $\{0, 2, 4, 6\}$.

Since the singleton set $\{0\}$ is trivially a group, the result follows.

ii) Answers will vary depending upon what you see! But you should see subgroup triangles forming and nesting insider of each other due to closure.

**Exercise 4.13:** Both $\{0\}$ and $\mathbb{Z}_5$ are subgroups of $\mathbb{Z}_5$ by definition. Suppose that there is another subgroup, call it $H$. Then $H$ must contain at least one nonzero value:

case 1: $1 \in H$. Then, by closure, $1+1=2 \in H$, $1+2=3 \in H$, $1+3=4 \in H$, and $1+4=0 \in H$. Hence, $H = \mathbb{Z}_5$.

case 2: $2 \in H$. Then, by closure, $2+2+2=1 \in H$ which means $H = \mathbb{Z}_5$ by case 1.

case 3: $3 \in H$. Then since $H$ is a group, $-3=2 \in H$ and $H = \mathbb{Z}_5$ by case 2.

case 4: $4 \in H$. Then $-4=1 \in H$ and $H = \mathbb{Z}_5$ by case 1.

So, if $H$ is a subgroup of $\mathbb{Z}_5$ that contains a nonzero element, $H$ must equal $\mathbb{Z}_5$. The result follows.

**Exercise 4.14:** Consider a subgroup of $\mathbb{Z}_6$ which contains 2. Then by closure the subgroup must contain $2+2=4$ and $2+2+2=0$. Let $H_1 = \{0,2,4\}$. Then $H_1$ is closed under addition mod 6. In addition, $H_1$ contains the identity. Since $-2=4$ and $-4=2 \bmod 6$, each element of $H_1$ has an inverse in $H_1$. Hence, this is a proper subgroup of $\mathbb{Z}_6$ containing 2.

By a similar argument, $H_2 = \{0,3\}$ is a proper subgroup of $\mathbb{Z}_6$ containing 3. As always, the singleton set containing the identity, $\{0\}$ in this case, is always a proper subgroup of a non-trivial group. Note that any subgroup containing 1 and/or 5 must be all of $\mathbb{Z}_6$ due to closure. If a subgroup contains 2 and 3, then it must also contain $2+3=5$, meaning we have all of $\mathbb{Z}_6$ once again. Hence, all of the subgroups are $\mathbb{Z}_6$, $H_1$, $H_2$, and $\{0\}$, the last three being proper subgroups.

**Exercise 4.15:** The exponents of $a$ throughout the triangle are precisely the values from Pascal's Triangle, including their respective locations. Hence, the exponents are binomial coefficients. The $n^{th}$ row of this triangle will have as exponents the binomial coefficients from the $n^{th}$ row of Pascal's Triangle.

**Exercise 4.18:** ii) The triangles you drew in i) should look like the mod 3 and mod 4 triangles, respectively.

iii) For $n=3$, $\langle a \rangle$ is a disguised version of $\mathbb{Z}_3$. Likewise for $n=4$, $\langle a \rangle$ is a disguised version of $\mathbb{Z}_4$.

**Exercise 4.20:** ii) What you should see (empirically only) from i) is that the generators for $\mathbb{Z}_n$ are those group elements whose integer equivalent is relatively prime to $n$.

iii) If $n$ is prime, every nonzero value generates $\mathbb{Z}_n$ since each of these is relatively prime to $n$.

**Exercise 4.21:** We proceed by induction. The base case $n = 1$ is verified in Figure 4.9. Now assume for some fixed $n$ that the $n^{th}$ row has the following form:

$$a \qquad a^{\binom{n}{1}}b^{\binom{n}{0}} \qquad a^{\binom{n}{2}}b^{\binom{n}{1}} \qquad \dots \qquad a^{\binom{n}{n-1}}b^{\binom{n}{n-2}} \qquad a^{\binom{n}{n}}b^{\binom{n}{n-1}} \qquad b$$

The the $(n+1)^{st}$ row starts with $a$ by construction. The next entry is found by multiplying $a = a^{\binom{n}{0}}$ and $a^{\binom{n}{1}}b^{\binom{n}{0}}$ using the group multiplication. Since the operation is commutative, this yields

$$a^{\binom{n}{0}}a^{\binom{n}{1}}b^{\binom{n}{0}} = \left(a^{\binom{n}{0}+\binom{n}{1}}\right)b^{\binom{n}{0}} = a^{\binom{n+1}{1}}b^{\binom{n+1}{0}}$$

.

This last equality follows from Pascal's Rule and the fact that $\binom{n}{0} = \binom{n+1}{0}$.

Next, consider entries $j$ and $j+1$ of the $n^{th}$ row, $j = 1, ..., n-1$:

$$a^{\binom{n}{j}}b^{\binom{n}{j-1}} \qquad\qquad a^{\binom{n}{j+1}}b^{\binom{n}{j}}$$

Then the entry in position $j+1$ of the $(n+1)^{st}$ row is obtained by multiplying these two entries using the group multiplication. Since the underlying group is abelian, this yields

$$\left(a^{\binom{n}{j}+\binom{n}{j+1}}\right)\left(b^{\binom{n}{j-1}+\binom{n}{j}}\right) = a^{\binom{n+1}{j+1}}b^{\binom{n+1}{j}}.$$

The second to last entry of row $n+1$ is obtained by multiplying $a^{\binom{n}{n}}b^{\binom{n}{n-1}}$ and $b = b^{\binom{n}{n}}$, yielding

$$a^{\binom{n}{n}}b^{\binom{n}{n-1}}b^{\binom{n}{n}} = a^{\binom{n}{n}}\left(b^{\binom{n}{n-1}+\binom{n}{n}}\right) = a^{\binom{n+1}{n+1}}b^{\binom{n+1}{n}}.$$

The last entry of this row is $b$ by construction, and the result follows.

# Chapter 5

**Exercise 5.1:** Addition mod 6 on the subsets in the partition $P$ is not well-defined. For example, consider $\{0, 1\}$ and $\{2, 4\}$. We see $0 + 2 = 2 \in \{2, 4\}$ but $1 + 4 = 5 \in \{3, 5\}$.

**Exercise 5.2:** Yes, $\bigoplus$ is commutative and associative on $S$. These properties are inherited from the mod 6 addition and so cases do not need to be enumerated. This means $S$ is an abelian group of order 3.

**Exercise 5.3:** $H + 3 = H + 0 = H$ and $H + 5 = H + 2$. So, neither of these are new cosets. They are just different names for already constructed cosets.

**Exercise 5.4:** i) $0 + H = 3 + H = H \qquad 1 + H = 4 + H \qquad 2 + H = 5 + H.$

ii) Yes, the left cosets also form a group.

ii) Yes, the left and right cosets are the same sets. If $a \in \mathbb{Z}_6$, then

$$a + H = \{a + h \mid h \in H\} = \{h + a \mid h \in H\} = H + a$$

since addition mod 6 is a commutative operation.

**Exercise 5.5:** i) The right cosets are $K = K + 0 = \{0, 2, 4\}$ and $K + 1 = \{1, 3, 5\}$.

ii) Yes, the addition is well-defined:

| $+$ | $K$ | $K+1$ |
|---|---|---|
| $K$ | $K$ | $K+1$ |
| $K+1$ | $K+1$ | $K$ |

iii) Yes, the cosets form a group that is a disguised version of $\mathbb{Z}_2$. $K$ is the identity and $K + 1$ is the nonzero element. So $K$ and $K + 1$ are analogous to 0 and 1 in $\mathbb{Z}_2$, respectively.

iv) The mod 2 growth in Figure 5.2 results from the fact that the cosets $K$ and $K+1$, which partition $\mathbb{Z}_6$, form a group that is structurally the same as $\mathbb{Z}_2$ and the mod 6 triangle must follow the coset multiplication.

iv) Since the left and right cosets are the same, there is no difference in using the left cosets instead of the right.

**Exercise 5.11:** i) Since $H_1 = G$, it must be the only right coset of $H_1$ in $G$. Recall that the right cosets for any subgroup partition the original group and, thus, must be disjoint. If we start with a subgroup that is the entire group, there cannot be other right cosets.

Let $g \in G$. Then $H_2 + g = \{e_G + g\} = \{g\}$ since $H_2$ only contains the identity of $G$. Thus, the right cosets of $H_2$ in $G$ are singleton sets, one for each $g \in G$.

ii) $G/H_1 = \{H_1\}$, i.e., it a group with only one element. $G/H_2 = \{\{g\} \mid g \in G\}$ and the elements are in a 1-1 correspondence with the elements of $G$.

iii) Relative to $G$, $G/H_1$ is a group that is the same as $\{e_G\}$, just in a different notation. Likewise, $G/H_2$ is really the same group as $G$.

**Exercise 5.12:** For a prime $p$, $\mathbb{Z}_p$ only has the subgroups $\{0\}$ and $\mathbb{Z}_p$. So, there are only two quotient groups. By the previous exercise, $\mathbb{Z}_p/\mathbb{Z}_p$ is structurally the same group as $\{0\}$ and $\mathbb{Z}_p/\{0\}$ is really just another description of $\mathbb{Z}_p$.

**Exercise 5.13:** The subgroups of $\mathbb{Z}_{10}$ are $\{0\}$, $H = \{0, 5\}$, $K = \{0, 2, 4, 6, 8\}$, and $\mathbb{Z}_{10}$. By Exercise 5.11, we know that using the trivial subgroup or the entire group does not produce interesting quotients. So, let us focus on $H$ and $K$.

The cosets of $H$ are $H$, $H + 1 = \{1, 6\}$, $H + 2 = \{2, 7\}$, $H + 3 = \{3, 8\}$, and $H + 4 = \{4, 9\}$. Hence, $\mathbb{Z}_{10}/H$ is a group with 5 elements. By constructing the Cayley table for this quotient, it is clear that this group is really the same as $\mathbb{Z}_5$.

The cosets of $K$ are $K$ and $K + 1 = \{1, 3, 5, 7, 9\}$. This means $\mathbb{Z}_{10}/K = \{K, K + 1\}$ is a 2-elements group which acts like $\mathbb{Z}_2$.

The subgroups of $\mathbb{Z}_{12}$ are $\{0\}$, $H = \{0, 6\}$, $K = \{0, 4, 8\}$, $L = \{0, 3, 6, 9\}$, $M = \{0, 2, 4, 6, 8, 10\}$, and $\mathbb{Z}_{12}$. The quotients of interest involve $H$, $K$, $L$, and $M$:

The cosets of $H$ are $H$, $H + 1 = \{1, 7\}$, $H + 2 = \{2, 8\}$, $H + 3 = \{3, 9\}$, $H + 4 = \{4, 10\}$, and $H + 5 = \{5, 11\}$. This means $\mathbb{Z}_{12}/H$ is a group with 6 elements. By constructing the Cayley table for this quotient, we see that this group is really $\mathbb{Z}_6$.

The cosets of $K$ are $K$, $K + 1 = \{1, 5, 9\}$, $K + 2 = \{2, 6, 10\}$, and $K + 3 = \{3, 7, 11\}$. $\mathbb{Z}_{12}/H$ is a group with 4 elements which you can check is $\mathbb{Z}_4$.

The cosets of $L$ are $L$, $L + 1 = \{1, 4, 7, 10\}$, and $L + 2 = \{2, 5, 8, 11\}$. $\mathbb{Z}_{12}/L$ acts like $\mathbb{Z}_3$ as a group.

The cosets of $M$ are $M$ and $M + 1 = \{1, 3, 5, 7, 9, 11\}$ and $\mathbb{Z}_{12}/M$ is really $\mathbb{Z}_2$.

**Exercise 5.15:** The cosets of $H_2 = \{e, a\}$ in $V$ are $H_2$ and $H_2 + b = \{e * b, a * b\} = \{b, c\}$. Likewise, the cosets of $H_3 = \{e, b\}$ in $V$ are $H_3$ and $H_3 + a = \{a, c\}$. Then $V/H_2 = \{H_2, H_2 + b\}$ and $V/H_3 = \{H_3, H_3 + a\}$. In both cases, the quotient is a two-element group, really just copies of $\mathbb{Z}_2$.

# Chapter 6

**Exercise 6.4:** Let us denote the first group $G_1 = \{a, b, c\}$ and the second group $G_2 = \{H, H + 1, H + 2\}$. Define a map $f_1 : G_1 \longrightarrow G_2$ by $f_1(a) = H$, $f_1(b) = H + 1$, and $f_1(c) = H + 2$. Then $f_1$ is clearly 1-1 and onto. We just need to check that the map preserves the operation, i.e., satisfies condition iii) in the definition of an isomorphism. We check a few cases:

$$f_1(a * b) = f_1(b) = H + 1 = (H + 0) + (H + 1) = f_1(a) + f_1(b)$$

$$f_1(b * c) = f_1(a) = H + 0 = (H + 1) + (H + 2) = f_1(b) + f_1(c)$$

$$f_1(c * c) = f_1(b) = H + 1 = (H + 2) + (H + 2) = f_1(c) + f_1(c)$$

There are other cases to check, but you can verify they all work. Hence, $f_1$ is an isomorphism and $G_1 \simeq G_2$.

The third group is $\mathbb{Z}_3$. Define $f_2 : G_1 \longrightarrow \mathbb{Z}_3$ by $f_2(a) = 0$, $f_2(b) = 1$, and $f_2(c) = 2$. By the same argument as above, $f_2$ is an isomorphism and $G_1 \simeq \mathbb{Z}_3$.

Since $G_2$ and $\mathbb{Z}_3$ are isomorphic to the same group, they must be isomorphic to each other. An isomorphism between $G_2$ and $\mathbb{Z}_3$ should also be clear at this point.

**Exercise 6.7:** The only automorphism of $\mathbb{Z}_2$ is the identity map. The reason is that automorphisms map the identity to itself. Since $\mathbb{Z}_2$ only contains one other element, any automorphism must map that element to itself as well.

**Exercise 6.8:** $f$ is 1-1 and onto, so we just need to make sure $f$ preserves the operation. We check a few cases:

$$f(1+2) = f(0) = 0 = 2+1 = f(1) + f(2)$$
$$f(1+1) = f(2) = 1 = 2+2 = f(1) + f(1)$$
$$f(1+0) = f(1) = 2 = 2+0 = f(1) + f(0)$$

There are other cases to check, but you can verify they all work. Hence, $f$ is an automorphism. The identity map and $f$ are the only automorphisms of $\mathbb{Z}_3$. Since an automorphism must map the identity to itself, there are only two choices for the image of 1. If 1 is mapped to itself, the identity map results since 2 must then map to 2. If 1 is mapped to 2, $f$ result.

**Exercise 6.11:** Since $\phi_3(1) = 3$, we have the following:

$$\phi_3(2) = \phi_3(1+1) = \phi_3(1) + \phi_3(1) = 3+3 = 1 \bmod 5$$
$$\phi_3(3) = \phi_3(1+2) = \phi_3(1) + \phi_3(2) = 3+1 = 4 \bmod 5$$
$$\phi_3(4) = \phi_3(1+3) = \phi_3(1) + \phi_3(3) = 3+4 = 2 \bmod 5$$
$$\phi_3(0) = \phi_3(1+4) = \phi_3(1) + \phi_3(4) = 3+2 = 0 \bmod 5$$

Since $\phi_4(1) = 4$, we have the following:

$$\phi_4(2) = \phi_4(1+1) = \phi_4(1) + \phi_4(1) = 4+4 = 3 \bmod 5$$
$$\phi_4(3) = \phi_4(1+2) = \phi_4(1) + \phi_4(2) = 4+3 = 2 \bmod 5$$
$$\phi_4(4) = \phi_4(1+3) = \phi_4(1) + \phi_4(3) = 4+2 = 1 \bmod 5$$
$$\phi_4(0) = \phi_4(1+4) = \phi_4(1) + \phi_4(4) = 4+1 = 0 \bmod 5$$

Since automorphisms of $\mathbb{Z}_5$ are always determined uniquely by the image of the generator 1, we have exhausted all of the possibilities.

**Exercise 6.12:** For a prime $p$, any automorphism of $\mathbb{Z}_p$ is determined by the image of 1 under the map. If $1 \longrightarrow i$, then the structure preserving requirement from the definition of an isomorphism uniquely determines the rest of the map $\phi_i : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$. Since 1 cannot be mapped to 0 (only 0 gets mapped to 0 by any automorphism), the allowable choices for $i$ are 1, 2,..., $p-1$. This is why $\text{Aut}(\mathbb{Z}_p) = \{\phi_1, \phi_2, ..., \phi_{p-1}\}$. Also, each $\phi_i$ is 1-1 and onto since $p$ is prime.

**Exercise 6.15:** The proof in Section 6.1 does not use the fact that the map is 1-1 or onto. It only relies on iii) from the definition of an isomorphism, i.e., that the map is structure preserving. But this is exactly the definition of an homomorphism.

**Exercise 6.16:** If $f$ is an isomorphism, then $\ker(f) = \{e_G\}$. Since $f$ is an isomorpihsm, $e_G \in \ker(f)$. But since $f$ is 1-1, no other element can map to $e_H$ and, hence, the kernel can only contain one element.

**Exercise 6.19:** i) If $|G| = |H| = n$, there are $n^n$ functions $f : G \longrightarrow H$.

ii) Of the functions from i), $n^{n-1}$ of them map $e_G$ to $e_H$.

**Exercise 6.22:** In $\mathbb{Z}_2 \times \mathbb{Z}_3$, $(1,1) + (1,1) = (0,2)$, $(1,1) + (0,2) = (1,0)$, $(1,1) + (1,0) = (0,1)$, $(1,1) + (0,1) = (1,2)$, and $(1,1) + (1,2) = (0,0)$. Hence, $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,1) \rangle$.

**Exercise 6.23:** i) The color assignment, recoloring the left figure into the right, is as follows:

white $\longrightarrow$ white
black $\longrightarrow$ blue
green $\longrightarrow$ light purple
blue $\longrightarrow$ black
light purple $\longrightarrow$ green
orange $\longrightarrow$ orange

This color correspondence defines the following map $\phi : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$:

$\phi(0) = (0,0)$
$\phi(1) = (1,1)$
$\phi(2) = (0,2)$
$\phi(3) = (1,0)$
$\phi(4) = (0,1)$
$\phi(5) = (1,2)$

iii) The map is clearly 1-1 and onto. Note how the image of 1 determines the rest of the map. That is, since $\phi(1) = (1,1)$, for $\phi$ to be structure preserving (a homomorphism), we must have the following:

$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = (1,1) + (1,1) = (0,2)$
$\phi(3) = \phi(1+2) = \phi(1) + \phi(2) = (1,1) + (0,2) = (1,0)$
$\phi(4) = \phi(1+3) = \phi(1) + \phi(3) = (1,1) + (1,0) = (0,1)$
$\phi(5) = \phi(1+4) = \phi(1) + \phi(4) = (1,1) + (0,1) = (1,2)$
$\phi(0) = \phi(1+5) = \phi(1) + \phi(5) = (1,1) + (1,2) = (0,0)$

which is exactly the way the map is defined in ii). Hence, $\phi$ is an isomorphism and $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$.

**Exercise 6.24:** By placing $(1,2)$ down both sides of the $\mathbb{Z}_2 \times \mathbb{Z}_3$ triangle, it appears to be just a recoloring of the $\mathbb{Z}_6$ triangle once again. The color correspondence defines the map $\phi : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$ which is as follows:

$\phi(0) = (0,0)$
$\phi(1) = (1,2)$
$\phi(2) = (0,1)$
$\phi(3) = (1,0)$
$\phi(4) = (0,2)$
$\phi(5) = (1,1)$

This map is an isomorphism using the same argument as in the previous exercise. The generators of $\mathbb{Z}_6$ are 1 and 5. The generators of $\mathbb{Z}_2 \times \mathbb{Z}_3$ are $(1,1)$ and $(1,2)$. Since the two groups are isomorphic, they must both have the same number of generators.

**Exercise 6.25:** ii) No. The most colors you can obtain is 4.

iii) $\mathbb{Z}_4 \times \mathbb{Z}_2$ cannot be generated by one element.

iv) You should obtain triangles that look like the mod 2 and mod 4 triangles, depending on which element is placed down the sides.

v) $\mathbb{Z}_8$ and $\mathbb{Z}_4 \times \mathbb{Z}_2$ are not isomorphic since the first is cyclic whereas the latter is not.

# Chapter 7

**Exercise 7.5:** The radius of the update rule is $R = 4$. This system simply shifts states 4 cells to the right.

**Exercise 7.6:** The following is obtained:

1
1 1
1 0 1
1 1 1 1
1 0 0 0 1

$$\begin{array}{cccccccc} 1 & 1 & 0 & 0 & 1 & 1 & & \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}$$

Note that this can be arranged symmetrically to obtain

$$\begin{array}{c} 1 \\ 1 \quad 1 \\ 1 \quad 0 \quad 1 \\ 1 \quad 1 \quad 1 \quad 1 \\ 1 \quad 0 \quad 0 \quad 0 \quad 1 \\ 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \\ 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \\ 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \end{array}$$

which is clearly the first 8 rows of Pascal's triangle mod 2.

**Exercise 7.13:** The rule number is

$$1 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 229.$$

**Exercise 7.14:** We first decompose 167 into binary form:

$$167 = 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0.$$

This corresponds to the following update for each of the eight 3-cell binary arrangements:

| 111 | 110 | 101 | 100 | 011 | 010 | 001 | 000 |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |

**Exercise 7.15:** In this case the left-most cell uses the last cell as its 'left neighbor' and the right-most cell uses the first cell as its 'right neighbor'. In other words, the lattice identifies the ends of the lattice as if it is wrapped into a circular array.

**Exercise 7.16:** In this example, the ends of the lattice are identified as in the last exercise. Next, apply rule 30 to a few states:

$$0000 \longrightarrow 0000 \text{ and } 1111 \longrightarrow 0000$$

In addition,

$$1010 \longrightarrow 1010 \text{ and } 0101 \longrightarrow 0101$$

This accounts for 4 of the states, so 12 remain. One is 1000. Let us find its orbit:

$$1000 \longrightarrow 1101 \longrightarrow 0001 \longrightarrow 1011 \longrightarrow 0010 \longrightarrow 0111 \longrightarrow 0100 \longrightarrow 1110 \longrightarrow 1000$$

Note that the first and last states are the same, but the states between are all distinct. Hence, this orbit defines an 8-cycle in the state transition diagram. There are 4 states remaining, and they evolve as follows:

$$0110 \longrightarrow 1101$$
$$1100 \longrightarrow 1011$$
$$1001 \longrightarrow 0111$$
$$0011 \longrightarrow 1110$$

The 4 output states have already been identified as being on the 8-cycle, equally spaced. We have already identified three 1-cycles and the state 1111 evolving to the zero state which is one of the fixed points. Hence, the state transition diagram shown in Figure 7.17 results.

**Exercise 7.17:** The states corresponding to $t = 4, 5, ., 9$ are shown in Figure 1. The top row gives $t = 4, 5, 6$ (reading from left to right) and the bottom row $t = 7, 8, 9$. Observe that the states for times $t = 0, .., 7$ are all distinct, but the states at times $t = 6, 8$ are the same. This means that the system enters a 2-cycle at this point. For $n \geq 6$ states with odd time index are the same as the $t = 7$ state and states with an even time index are the same as the $t = 6$ state. This includes the specified times of $t = 1000$ and $t = 1001$.

**Exercise 7.19:** The states are shown in Figure 2. Here black represents 1 and light blue represents 0.

**Exercise 7.22:** For the state with a single 1 and zeros everywhere else, it takes 32 time steps for this initial state to evolve to the zero state. For other initial states, you should see experimentally that it takes at most 32 time steps to evolve to the zero state.

**Exercise 7.23:** This exercise is experimental and open-ended. But if you try a variety of initial states, should find numerous examples of states on 27 and 81 cycles.

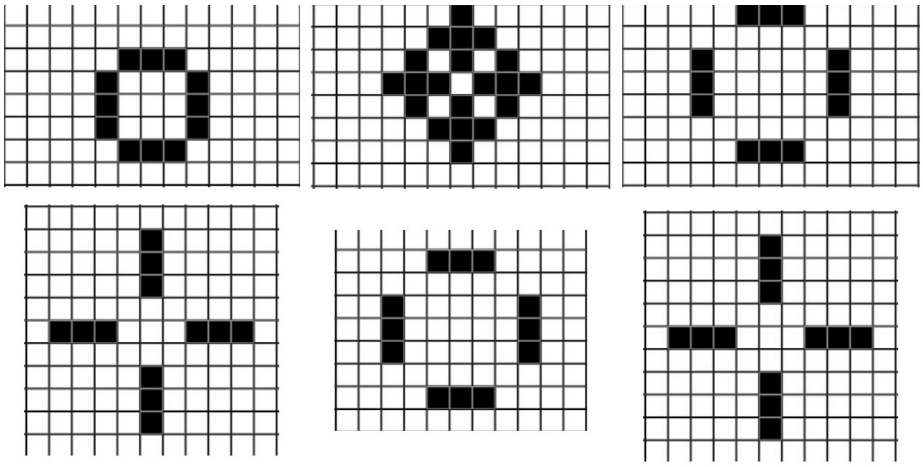

Figure 1: The next six time steps which follow the $t = 3$ state.

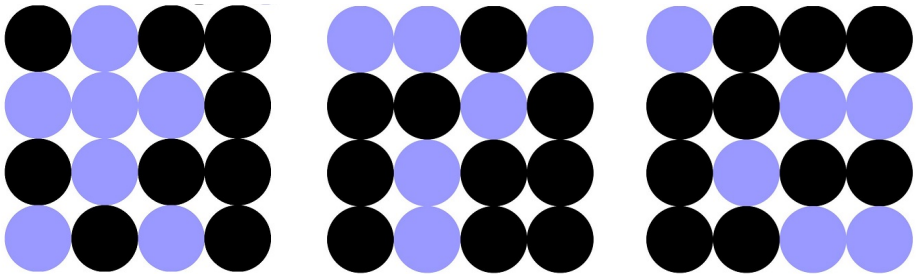

Figure 2: The initial state (left) along with next states using i) null boundary (middle) and ii) periodic boundary (right)

**Exercise 7.27:** The transition matrix for the system is

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Let $\boldsymbol{s} = (a_1, a_2, a_3, a_4)$ be a state in the system. Then in one time-step $\boldsymbol{s}$ evolves to

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} = \begin{bmatrix} a_1 + a_4 \\ a_1 + a_2 \\ a_2 + a_3 \\ a_3 + a_4 \end{bmatrix}$$

If $\boldsymbol{s} \in \text{Nul}(M)$, then $a_1 + a_4 = a_1 + a_2 = a_2 + a_3 = a_3 + a_4 = 0$. Solving this system over $\mathbb{Z}_2$ gives two solutions: $\boldsymbol{s} = (0, 0, 0, 0)$ and $\boldsymbol{s} = (1, 1, 1, 1)$.

Row reducing $M$ mod 2 yields

$$M \sim \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

This is a rank 3 matrix so the image of the time evolution map, i.e., the column space of $M$, of the span of the first three columns of $M$:

$$\text{Col}(M) = \{x(1,1,0,0) + y(0,1,1,0) + z(0,0,1,1) | x, y, z \in \mathbb{Z}_2\}$$

By substituting all possible values of $x$, $y$, and $z$, then following states are obtained for the column space:

$$0 \equiv 0000$$

$$3 \equiv 0011$$

$$6 \equiv 0110$$

$$5 \equiv 0101$$

$$12 \equiv 1100$$

$$15 \equiv 1111$$

$$10 \equiv 1010$$

$$9 \equiv 1001$$

These are precisely the states in the system after one time step. The other 8 states are Garden-of-Eden states. Finally, by direct computation, it is easy to see that $M$, $M^2$, and $M^3$ mod 2 are all distinct and $M^4$ is the zero matrix mod 2. This says that all states in the system evolve to the zero state in at most 4 time steps. So, the zero state is the only fixed point of the system, and there are no other cycles. All of this analysis is in agreement with the state transition diagram of the system given in Figure 7.26 from Chapter 7 of the book.

**Exercise 7.29:** i) Row reducing the augmented matrix mod 2 results in the following:

$$(M|I_4) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Since the left $4 \times 4$ submatrix of the reduced augmented matrix is $I_4$, $M$ is invertible and the right $4 \times 4$ submatrix is $M^{-1}$.

ii) First, compute $M$, $M^2$, $M^3$, and $M^4$ mod 2 either by hand or using software. Note that they are all different and $M^4 = MM^3 = I_4$. This means $M^3 = M^{-1}$. As expected $M^3$ agrees with $M^{-1}$ just found in i).

# Chapter 8

**Exercise 8.2:** $S_0$ is closed under component-wise mod 4 addition. Since associativity in each component results from associativity in $\mathbb{Z}_4$, the binary operation on $S_0$ is associative. The identity is $(0,0,0,0,0)$ and if $\boldsymbol{s} = (a_1, a_2, a_3, a_4, a_5) \in S_0$ then $-\boldsymbol{s} = (-a_1, -a_2, -a_3, -a_4, -a_5) \in S_0$ since $-a_i \in \mathbb{Z}_4$ for $i = 1, .., 5$. It follows that $S_0$ is a group, which is also abelian since the addition is commutative in each component. Finally, $S_0 \simeq \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$.

**Exercise 8.5:** We proceed by induction. The base case is covered by the assumption that $\phi(\boldsymbol{s_1} + \boldsymbol{s_2}) = \phi(\boldsymbol{s_1}) + \phi(\boldsymbol{s_2})$ for all $\boldsymbol{s_1}, \boldsymbol{s_2} \in S_0$. Now assume that $\phi(\boldsymbol{s_1} + \boldsymbol{s_2} + \cdots + \boldsymbol{s_n}) = \phi(\boldsymbol{s_1}) + \phi(\boldsymbol{s_2}) + \cdots + \phi(\boldsymbol{s_n})$ for all $\boldsymbol{s_1}, \boldsymbol{s_2}, ..., \boldsymbol{s_n} \in S_0$. Let $\boldsymbol{s_1}, \boldsymbol{s_2}, ..., \boldsymbol{s_n}, \boldsymbol{s_{n+1}} \in S_0$. Then

$$\begin{aligned}\phi(\boldsymbol{s_1} + \cdots + \boldsymbol{s_n} + \boldsymbol{s_{n+1}}) &= \phi(\boldsymbol{s_1} + \cdots + \boldsymbol{s_n}) + \phi(\boldsymbol{s_{n+1}}) \text{ by the initial assumption} \\ &= \phi(\boldsymbol{s_1}) + \phi(\boldsymbol{s_2}) + \cdots + \phi(\boldsymbol{s_n}) + \phi(\boldsymbol{s_{n+1}})\end{aligned}$$

by the induction hypothesis.

**Exercise 8.6:** Assuming that $\phi(\boldsymbol{s_1} + \boldsymbol{s_2}) = \phi(\boldsymbol{s_1}) + \phi(\boldsymbol{s_2})$ for all $\boldsymbol{s_1}, \boldsymbol{s_2} \in S_0$, we need to show that $\phi^n(\boldsymbol{s_1} + \boldsymbol{s_2}) = \phi^n(\boldsymbol{s_1}) + \phi^n(\boldsymbol{s_2})$ for all $\boldsymbol{s_1}, \boldsymbol{s_2} \in S_0$ and $n \geq 1$. We proceed by induction. The base case $n = 1$ is satisfied by assumption. Now assume $\phi^n(\boldsymbol{s_1} + \boldsymbol{s_2}) = \phi^n(\boldsymbol{s_1}) + \phi^n(\boldsymbol{s_2})$ for all $\boldsymbol{s_1}, \boldsymbol{s_2} \in S_0$ for some $n \geq 1$. Then

$$\begin{aligned}\phi^{n+1}(\boldsymbol{s_1} + \boldsymbol{s_2}) &= \phi(\phi^n(\boldsymbol{s_1} + \boldsymbol{s_2})) \\ &= \phi(\phi^n(\boldsymbol{s_1}) + \phi^n(\boldsymbol{s_2})) \qquad \text{by the induction hypothesis} \\ &= \phi(\phi^n(\boldsymbol{s_1})) + \phi(\phi^n(\boldsymbol{s_2})) \\ &= \phi^{n+1}(\boldsymbol{s_1}) + \phi^{n+1}(\boldsymbol{s_2}).\end{aligned}$$

**Exercise 8.8:** Let $\boldsymbol{s_1} = (a_1, a_2, ..., a_9, a_{10})$ and $\boldsymbol{s_2} = (b_1, b_2, ..., b_9, b_{10})$ be states. Then

$$\begin{aligned}&\phi(\boldsymbol{s_1} + \boldsymbol{s_2}) \\ &= \phi((a_1 + b_1, a_2 + b_2, ..., a_9 + b_9, a_{10} + b_{10})) \\ &= (a_{10} + b_{10} + a_1 + b_1, a_1 + b_1 + a_2 + b_2, ..., a_8 + b_8 + a_9 + b_9, a_9 + b_9 + a_{10} + b_{10}) \\ &= (a_{10} + a_1, a_1 + a_2, ..., a_8 + a_9, a_9 + a_{10}) + (b_{10} + b_1, b_1 + b_2, ..., b_8 + b_9, b_9 + b_{10}) \\ &= \phi(\boldsymbol{s_1}) + \phi(\boldsymbol{s_2}).\end{aligned}$$

Note that addition in each component is done mod 3. It follows that $\phi$ commutes with the addition on states for this system.

**Exercise 8.10** We start by considering the 2-D case. Let $\mathcal{A}$ be a finite cellular

automaton over an abelian group alphabet $\mathbb{A}$. Then a state in this system has the form $\boldsymbol{s} = (a_{i,j})$ where $1 \leq i \leq n$ and $1 \leq j \leq m$.

**closure:** Let $\boldsymbol{s_1} = (a_{i,j}), \boldsymbol{s_2} = (b_{i,j}) \in S_0$. Then $\boldsymbol{s_1} + \boldsymbol{s_2} = (a_{i,j}) + (b_{i,j}) = (a_{i,j} + b_{i,j}) \in S_0$ since $a_{i,j} + b_{i,j} \in \mathbb{A}$ for each $i$ and $j$ using the closure of $+$ in $\mathbb{A}$. Note that $+$ is being used to refer to two different (but related) binary operations. The $+$ on $S_0$ is defined as component-wise addition using the $+$ on $\mathbb{A}$ in each coordinate.

**associativity:** Let $\boldsymbol{s_1} = (a_{i,j}), \boldsymbol{s_2} = (b_{i,j}), \boldsymbol{s_3} = (c_{i,j}) \in S_0$.

$$\begin{aligned}
\text{Then } (\boldsymbol{s_1} + \boldsymbol{s_2}) + \boldsymbol{s_3} &= ((a_{i,j}) + (b_{i,j})) + (c_{i,j}) \\
&= (a_{i,j} + b_{i,j}) + (c_{i,j}) \\
&= ((a_{i,j} + b_{i,j}) + c_{i,j}) \\
&= (a_{i,j} + (b_{i,j} + c_{i,j})) \qquad \text{by associativity in } \mathbb{A} \\
&= (a_{i,j}) + (b_{i,j} + c_{i,j}) \\
&= (a_{i,j}) + ((b_{i,j}) + (c_{i,j})) \\
&= \boldsymbol{s_1} + (\boldsymbol{s_2} + \boldsymbol{s_3}).
\end{aligned}$$

**identity:** Let 0 denote the identity of $\mathbb{A}$ and $\mathbf{0} \in S_0$ be the state that contains 0 in each component. Then if $\boldsymbol{s} = (a_{i,j}) \in S_0$, $\boldsymbol{s} + \mathbf{0} = (a_{i,j}) + \mathbf{0} = (a_{i,j} + 0) = (a_{i,j}) = \boldsymbol{s} = (0 + a_{i,j}) = \mathbf{0} + (a_{i,j}) = \mathbf{0} + \boldsymbol{s}$. Hence, $\mathbf{0}$ is the identity of $S_0$.

**inverses:** Let $\boldsymbol{s} = (a_{i,j}) \in S_0$. Since $\mathbb{A}$ is a group and $a_{i,j} \in \mathbb{A}$ for each $i$ and $j$, $-a_{i,j} \in \mathbb{A}$. Define $-\boldsymbol{s} = (-a_{i,j}) \in S_0$. Then $\boldsymbol{s} + -\boldsymbol{s} = (a_{i,j}) + (-a_{i,j}) = (0) = \mathbf{0}$. Likewise, $-\boldsymbol{s} + \boldsymbol{s} = \mathbf{0}$. So, $\boldsymbol{s}$ and $-\boldsymbol{s}$ are inverses of each other in $S_0$.

It follows that $S_0$ is a group under component-wise addition. To see that it is an abelian group, observe that $\boldsymbol{s_1} + \boldsymbol{s_2} = (a_{i,j}) + (b_{i,j}) = (a_{i,j} + b_{i,j}) = (b_{i,j} + a_{i,j}) = (b_{i,j}) + (a_{i,j}) = \boldsymbol{s_2} + \boldsymbol{s_1}$.

To generalize this proof to other dimensions, we really only need to adjust the indexing to match the lattice. Suppose $\mathcal{A}$ is finite a D-dimensional cellular automaton. Then a state has the form $(a_{i_1,i_2,\ldots,i_D}) \in S_0$ where $1 \leq i_1 \leq n_1$, $1 \leq i_2 \leq n_2$, ..., $1 \leq i_D \leq n_D$ for some positive integers $n_1, n_2, \ldots, n_D$. Now just follow the same proof for the 2-D case replacing states of the form $(a_{i,j})$ with $(a_{i_1,i_2,\ldots,i_D})$.

**Exercise 8.15:** The transition matrix for the system is

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Let $\boldsymbol{s} = (a_1, a_2, a_3, a_4, a_5, a_6)$ be a state in the system. Then in one time-step $\boldsymbol{s}$ evolves to

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{bmatrix} = \begin{bmatrix} a_1 + a_6 \\ a_1 + a_2 \\ a_2 + a_3 \\ a_3 + a_4 \\ a_4 + a_5 \\ a_5 + a_6 \end{bmatrix}$$

If $\boldsymbol{s} \in \text{Nul}(M)$, then $a_1 + a_6 = a_1 + a_2 = a_2 + a_3 = a_3 + a_4 = a_4 + a_5 = a_5 + a_6 = 0$. Solving this system over $\mathbb{Z}_2$ gives two solutions: $\boldsymbol{s} = (0, 0, 0, 0, 0, 0)$ and $\boldsymbol{s} = (1, 1, 1, 1, 1, 1)$.

Row reducing $M$ mod 2 yields

$$M \sim \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

This is a rank 5 matrix so the image of the time evolution map, i.e., the column space of $M$, is the span of the first five columns of $M$ which tells us there are $2^5 = 32$ non-Garden-of-Eden states.

Finally, by direct computation, it is easy to see that $M$, $M^2$,..., and $M^7$ mod 2 are all distinct and $M^8 = M^2$. This is consistent with the fact that all states in the system are mapped to cycle states in at most two time steps and and then at that point all states are on cycles whose length divides 6, the maximum cycle length.

**Exercise 8.16:** For $|ker(\phi_1)| = |ker(\phi_2)| = \cdots = |ker(\phi_N)|$, all paths from Garden-of-Eden states to the zero state (for an irreversible system) must have the same length.

**Exercise 8.20:** Using an appropriate software system, note that $M^9 - I_9 \sim I_9$, which means the only state that is mapped to itself after nine time steps is the zero state. Hence, there are no 9-cycles.

**Exercise 8.21:** Since this is a reversible cellular automaton and all cycle lengths divide 18, every state in the system is fixed after 18 time steps, i.e., $M^{18}\boldsymbol{s} = \boldsymbol{s}$ for each state $\boldsymbol{s}$. This is equivalent to saying each $\boldsymbol{s}$ is in the nullspace of $M^{18} - I_9$.

**Exercise 8.23:** Enter the $8 \times 9$ augmented matrix $(M|s)$ mod 5 using a computer algebra system and row reduce for each of the four given states $\boldsymbol{s}$. In each case, the reduced matrix will have a row starting with 8 zeros and then ending

with a 1 (assuming a reduced echelon form). This indicates that the system is inconsistent and, hence, the four states in question are Garden-of-Eden.

**Exercise 8.28:** The rule distance for this system is $d = 3$. Let

$$\boldsymbol{s} = (a_1, a_2, \cdots, a_8)$$

be a state such that $\boldsymbol{s} \longrightarrow \mathbf{0}$. Then $a_1, \cdots, a_8$ must satisfy the following:

$$\begin{cases} & & & a_4 & & & & + a_8 = 0 \\ a_1 & & & + a_5 & & & & = 0 \\ & a_2 & & & + a_6 & & & = 0 \\ & & a_3 & & & + a_7 & & = 0 \\ & & & a_4 & & & & + a_8 = 0 \\ a_1 & & & + a_5 & & & & = 0 \\ & a_2 & & & + a_6 & & & = 0 \\ & & a_3 & & & + a_7 & & = 0 \end{cases}$$

Note that each equation shows up twice in this system leading to the following:

$$a_1 = -a_5 \qquad a_2 = -a_6 \qquad a_3 = -a_7 \qquad a_4 = -a_8$$

Since this has nonzero solutions over $\mathbb{Z}_n$, this system is irreversible.

**Exercise 8.29:** The rule distance for this system is $d = 2$. Let $\boldsymbol{s} = (a_1, a_2, \cdots, a_{12})$ be a state such that $\boldsymbol{s} \longrightarrow \mathbf{0}$. Then $a_1, \cdots, a_{12}$ must satisfy the following:

$$\begin{cases} a_1 + a_4 = 0 \\ a_2 + a_5 = 0 \\ a_3 + a_6 = 0 \\ a_4 + a_7 = 0 \\ a_5 + a_8 = 0 \\ a_6 + a_9 = 0 \\ a_7 + a_{10} = 0 \\ a_8 + a_{11} = 0 \\ a_9 + a_{12} = 0 \\ a_1 + a_{10} = 0 \\ a_2 + a_{11} = 0 \\ a_3 + a_{12} = 0 \end{cases}$$

This system leading to the following:

$$a_1 = -a_4 = a_7 = -a_{10}$$

$$a_2 = -a_5 = a_8 = -a_{11}$$

$$a_3 = -a_6 = a_9 = -a_{12}$$

Since this has nonzero solutions over $\mathbb{Z}_n$, this system is irreversible.

# Chapter 9

**Exercise 9.1:** i)

| | **# segments** | **length** |
|---|---|---|
| n=2 | $16=4^2$ | $\frac{16}{9} = \frac{4^2}{3^2}$ |
| n=3 | $64=4^3$ | $\frac{64}{27} = \frac{4^3}{3^3}$ |
| n=4 | $256=4^4$ | $\frac{256}{81} = \frac{4^4}{3^4}$ |

ii) The number of line segments for the $n^{th}$ iteration is $4^n$. The length is $\left(\frac{4}{3}\right)^n$.

iii) The length of the Koch Curve is

$$\lim_{n\to\infty} \left(\frac{4}{3}\right)^n = \infty.$$

**Exercise 9.2:** i) Let $a_i$ denote the area of $A_i$. Then

$a_1 = \frac{3}{4}a_0$,
$a_2 = \frac{3}{4}a_1 = \left(\frac{3}{4}\right)^2 a_0$
$a_3 = \frac{3}{4}a_2 = \left(\frac{3}{4}\right)^3 a_0$
$a_4 = \frac{3}{4}a_3 = \left(\frac{3}{4}\right)^4 a_0$

ii) The remaining area of the $n^{th}$ iteration is $a_n = \frac{3}{4}a_{n-1} = \left(\frac{3}{4}\right)^n a_0$.

iii) No area remains:

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} \left(\frac{3}{4}\right)^n a_0 = 0.$$

iv) Let $l_i$ denote the length of the boundary of $A_i$. Then

$l_0 = 3$
$l_1 = 3 \cdot 3\left(\frac{1}{2}\right)$
$l_2 = 3 \cdot 9\left(\frac{1}{4}\right)$
$l_3 = 3 \cdot 27\left(\frac{1}{8}\right)$
$l_4 = 3 \cdot 81\left(\frac{1}{16}\right)$

v) The total length for the boundary of the $n^{th}$ iteration is $l_n = \frac{3^{n+1}}{2^n}$.

vi) The total length of the Sierpinski Triangle is

$$L = \lim_{n\to\infty} l_n = \lim_{n\to\infty} = \frac{3^{n+1}}{2^n} = \infty.$$

**Exercise 9.3:** i)

| | **# segments** | **length** |
|---|---|---|
| n=3 | 8 | $8 \cdot \frac{1}{27} = \frac{2^3}{3^3}$ |
| n=4 | 16 | $16 \cdot \frac{1}{81} = \frac{2^4}{3^4}$ |
| n=5 | 32 | $32 \cdot \frac{1}{243} = \frac{2^5}{3^5}$ |

ii) For the $n^{th}$ iteration, the total number of line segments is $2^n$ and the total length is $L_n = \left(\frac{2}{3}\right)^n$.

iii) The Cantor set has zero length:

$$L = \lim_{n\to\infty} \left(\frac{2}{3}\right)^n = 0.$$

**Exercise 9.4:** The volume of the $n^{th}$ iteration is $V_n = \left(\frac{20}{27}\right)^n$ and the surface area is $A_n = 2\left(\frac{20}{9}\right)^n + 4\left(\frac{8}{9}\right)^n$. Taking the limit of both expressions shows that the Menger Sponge has zero volume and infinite surface area.

**Exercise 9.5:** For the Menger Sponge, $N = 20$ and $r = \frac{1}{3}$. Hence, the similarity dimension is

$$d = \frac{\log(20)}{\log(3)} \approx 2.7268.$$

**Exercise 9.6:** Applying $f_2, f_2$ to this set yields

$$C_3 = \left[0, \frac{1}{27}\right] \cup \left[\frac{2}{27}, \frac{1}{9}\right] \cup \left[\frac{2}{9}, \frac{7}{27}\right] \cup \left[\frac{8}{27}, \frac{1}{3}\right] \cup \left[\frac{2}{3}, \frac{19}{27}\right] \cup \left[\frac{20}{27}, \frac{7}{9}\right] \cup \left[\frac{8}{9}, \frac{25}{27}\right] \cup \left[\frac{26}{27}, 1\right].$$

The limiting value of this construction is the Cantor Set.

**Exercise 9.7:** Applying the IFS yields 9 sub-traingles of side length $\frac{1}{4}$ with the following coordinates:

**Bottom-Left Region:**

Triangle 1: $(0,0),\ \left(\frac{1}{4},0\right),\ \left(\frac{1}{8}, \frac{\sqrt{3}}{8}\right)$

Triangle 2: $\left(\frac{1}{4},0\right),\ \left(\frac{1}{2},0\right),\ \left(\frac{3}{8}, \frac{\sqrt{3}}{8}\right)$

Triangle 3: $\left(\frac{1}{8}, \frac{\sqrt{3}}{8}\right),\ \left(\frac{3}{8}, \frac{\sqrt{3}}{8}\right),\ \left(\frac{1}{4}, \frac{\sqrt{3}}{4}\right)$

**Bottom-Right Region:**

Triangle 4: $\left(\frac{1}{2},0\right),\ \left(\frac{3}{4},0\right),\ \left(\frac{5}{8}, \frac{\sqrt{3}}{8}\right)$

Triangle 5: $\left(\frac{3}{4},0\right),\ (1,0),\ \left(\frac{7}{8}, \frac{\sqrt{3}}{8}\right)$

Triangle 6: $\left(\frac{5}{8}, \frac{\sqrt{3}}{8}\right),\ \left(\frac{7}{8}, \frac{\sqrt{3}}{8}\right),\ \left(\frac{3}{4}, \frac{\sqrt{3}}{4}\right)$

**Top Region:**

Triangle 7: $\left(\frac{1}{4}, \frac{\sqrt{3}}{4}\right),\ \left(\frac{1}{2}, \frac{\sqrt{3}}{4}\right),\ \left(\frac{3}{8}, \frac{3\sqrt{3}}{8}\right)$

Triangle 8: $\left(\frac{1}{2}, \frac{\sqrt{3}}{4}\right),\ \left(\frac{3}{4}, \frac{\sqrt{3}}{4}\right),\ \left(\frac{5}{8}, \frac{3\sqrt{3}}{8}\right)$

Triangle 9: $\left(\frac{3}{8}, \frac{3\sqrt{3}}{8}\right),\ \left(\frac{5}{8}, \frac{3\sqrt{3}}{8}\right),\ \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$

**Exercise 9.8:** An Iterated Function System (IFS) for the Koch curve is defined as follows:

$$T_1\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}\frac{1}{3} & 0\\ 0 & \frac{1}{3}\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} + \begin{pmatrix}0\\0\end{pmatrix}$$

$$T_2\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}\frac{1}{6} & -\frac{\sqrt{3}}{6}\\ \frac{\sqrt{3}}{6} & \frac{1}{6}\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} + \begin{pmatrix}\frac{1}{3}\\0\end{pmatrix}$$

$$T_3\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}\frac{1}{6} & \frac{\sqrt{3}}{6}\\ -\frac{\sqrt{3}}{6} & \frac{1}{6}\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} + \begin{pmatrix}\frac{1}{2}\\\frac{\sqrt{3}}{6}\end{pmatrix}$$

$$T_4\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}\frac{1}{3} & 0\\ 0 & \frac{1}{3}\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} + \begin{pmatrix}\frac{2}{3}\\0\end{pmatrix}$$

The corresponding fractal dimension is the unique number $d$ such that $4\left(\frac{1}{3}\right)^d = 1$. Solving for $d$ yields

$$d = \frac{\log 4}{\log 3} \approx 1.26.$$

**Exercise 9.11:** The table is as follows:

| **number of rows** | **number of nonzero elements** |
|---|---|
| 3 | 6 |
| 9 | 36 |
| 27 | 216 |
| $\vdots$ | $\vdots$ |
| $3^n$ | $6^n$ |

The corresponding growth rate dimension is $\frac{\log(6)}{\log(3)} \approx 1.63$.

**Exercise 9.12:** In the mod 4 case, there is no constant growth factor. This is observed in the second column. Hence, the growth rate dimension formula, in its simplest form from Definition 9.10, cannot be applied directly. Geometrically, this occurs due to the mixing of the 2s in the (otherwise) zero subtriangles.

# Chapter 10

**Exercise 10.2:** $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a group of order 4 and, by definition, a subgroup of itself. All subgroups contain the identity, so $\{(0,0\})$ is the unique subgroup of

order 1. Since every element in this group is its own inverse, the following are subgroups of order 2:

$$\{(0,0),(1,0)\} \qquad \{(0,0),(0,1)\} \qquad \{(0,0),(1,1)\}$$

Note that each of these three subsets is closed, one of the requirements for a subgroup. Any subset of order three is not closed, which you can easily check. Hence, all the subgroups have been found.

**Exercise 10.3:** We know $r_0$ is the group identity of $S_3$, so for closure we focus on $r_1$ and $r_2$:

$$r_1 \circ r_1 = r_2 \qquad r_2 \circ r_2 = r_1 \qquad r_1 \circ r_2 = r_2 \circ r_1 = r_0.$$

Thus, $K$ is a closed subset that contains the identity. Associativity is inherited from $S_3$. Since $r_1$ and $r_2$ are inverses of each other, all requirements for a subgroup are satisfied, and $K \leq S_3$.

**Exercise 10.7:** For $H = \{r_0, \mu_1\}$, consider the following:

$$r_1 H \mu_2 H = r_1 \mu_2 H = \mu_1 H = H$$

and

$$\mu_3 H r_2 H = \mu_3 r_2 H = \mu_2 H = r_2 H.$$

Since $r_2 H \neq H$, we arrive at

$$r_1 H \mu_2 H \neq \mu_3 H r_2 H$$

even though $r_1 H = \mu_3 H$ and $\mu_2 H = r_2 H$. It follows that left coset multiplication is not well-defined for $H$.

**Exercise 10.8:** For $K = \{r_0, r_1, r_2\}$, there are only two left (or right) cosets, namely $K$ and $\mu_1 K = \{\mu_1, \mu_2, \mu_3\}$. To show that left coset multiplication is well-defined, we could check each product for all possible pairs of coset representatives. But here is the key observation: In $S_3$, $K$ is closed; any two elements (possibly the same) from $\mu_1 K$ composed produce an element from $K$; and an element from $K$ composed with an element of $\mu_1 K$ (in either order) yield an element from $\mu_1 K$. This means left coset multiplication is well-defined for $K$, and likewise for right.

**Exercise 10.9:** Define $\phi : H \longrightarrow Ha$ by $\phi(h) = ha$. Note that

$$\phi(h_1) = \phi(h_2) \implies h_1 a = h_2 a \implies h_1 = h_2.$$

The last implication follows from multiplying both sides of the equation by $a^{-1}$ on the right side (or using the right cancellation law for groups). Hence, $\phi$ is

1-1. If $ha \in Ha$, then $h \in H$ and $\phi(h) = ha$. So, $\phi$ is onto. It follows that $|H| = |Ha|$. This argument does not depend on $G$ and/or $H$ being finite. The result holds for infinite groups as well. The proof does apply to left cosets as well.

**Exercise 10.11:** If $G$ is finite and $H \leq G$, then there are a finite number of cosets of $H$ in $G$. Suppose $[G : H] = n$. Since the cosets partition $G$, we can write

$$G = Ha_1 \dot{\cup} Ha_{a_2} \dot{\cup} \cdots \dot{\cup} Ha_n.$$

Note that this is a disjoint union, that is, $Ha_i \cap Ha_j = \emptyset$ whenever $i \neq j$. Thus,

$$|G| = |Ha_1 \dot{\cup} Ha_{a_2} \dot{\cup} \cdots \dot{\cup} Ha_n| = |Ha_1| + |Ha_{a_2}| + \cdots + |Ha_n| = [G : H]|H|$$

since $|H| = |Ha_i|$ for $i = 1, .., n$. Lagrange's Theorem follows immediately from this.

**Exercises 10.14 and 10.15:** Since the composition of any two (possibly the same) rotations always yields a rotation, $R_7$ is closed. As always, associativity is inherited. The zero degree rotation is the identity and an element of $R_7$ by definition. As we have already seen with the dihedral groups, the inverse of any rotation is a rotation. Hence, $R_7 \leq D_7$.

To see that $R_7$ is normal in $D_7$, consider the left cosets. One is $R_7$, which consists of half of the group elements, i.e., the rotations. Since the cosets must all be the same size by Exercise 10.9, there can be only one other coset that consists of the reflections, call it $fR_7$, where $f$ is one of the reflections. The same argument applies to right cosets. Hence, the left and right cosets are equal (one contains the rotations, the other the relections) and it follows that $R_7 \lhd D_7$.

# Chapter 11

**Exercise 11.2:** Let $(n, p-n), (m, p-m) \in \mathbb{Z}_p \times \mathbb{Z}_p$, where $0 \leq n, m < p$. Then $(n, p-n)+(m, p-m) = (n+m, 2p-n-m)) = (n+m, p-(n+m)) \in H$. Clearly, $(0, 0) = (0, p-0) \in H$. If $(n, p-n) \in H$, then $(p-n, p-(p-n)) = (p-n, n) \in H$. In addition, $(n, p-n) + (p-n, n) = (0, 0)$. Thus, $-(n, p-n) = (p-n, n)$ and $H$ contains inverses for all of its elements. It follows that $H \leq \mathbb{Z}_p \times \mathbb{Z}_p$.

**Exercise 11.3:** i) Note that $\langle(1, 4)\rangle$ contains $(1, 4) + (1, 4) = (2, 3)$, $(1, 4) + (1, 4) + (1, 4) = (3, 2)$, $(1, 4) + (1, 4) + (1, 4) + (1, 4) = (4, 1)$, and $(1, 4) + (1, 4) + (1, 4) + (1, 4) + (1, 4) = (0, 0)$. Hence, $\langle(1, 4)\rangle = H$.

ii) Since $\langle(1, 4)\rangle$ is a cyclic group of order 5, it must be isomorphic to $\mathbb{Z}_5$. For an explicit isomorphism, one option is $(1, 4) \longrightarrow 1$ and then define the rest of

the map to preserve the operation.

iii) The resulting triangle after the coset identification is Pascal's triangle mod 5.

iv) Since $H = \{(0,0),(1,4),(2,3),(3,2),(4,1),$

$$(0,1) + H = \{(0,1),(1,0),(2,4),(3,3),(4,2)\} = (1,0) + H.$$

v) Since $(\mathbb{Z}_5 \times \mathbb{Z}_5)/H$ is a group or order 5, and $\mathbb{Z}_5$ is the only group of order 5, they must be isomorphic. Note: You can show that $(0,1) + H$ generates the quotient if that helps.

**Exercise 11.5:** i) The identity element is $\phi_1$.

ii) Yes, each element in the set has a unique inverse: $\phi_1^{-1} = \phi_1$, $\phi_2^{-1} = \phi_3$, $\phi_3^{-1} = \phi_2$, and $\phi_4^{-1} = \phi_4$.

iii) Closure is required. This is clearly satisfied, as seen in the table. Associativity is also needed. Since function composition (when defined) is always associative, this criterion is also met.

iv) By inspection, the table shows that $\mathrm{Aut}(\mathbb{Z}_5)$ is abelian. Observe that $\phi_i \circ \phi_j = \phi_{ij}$, where $ij$ is reduced mod 5. Since $ij = ji$, commutativity follows.

v) Since $\mathrm{Aut}(\mathbb{Z}_5)$ is a group of order 4, it must be isomorphic to $\mathbb{Z}_4$ or the Klein 4-group $(\mathbb{Z}_2 \times \mathbb{Z}_2)$. In the Klein 4-group, each element is its own inverse. That is not the case here, so $\mathrm{Aut}(\mathbb{Z}_5)$ must be isomorphic to $\mathbb{Z}_4$. Alternatively, you could also show that it is cyclic—it is generated by each of its non-identity elements.

**Exercise 11.6:** This is to be done by inspection using *PascGaloisJE*.

**Exercise 11.7:** This is also to be done visually using *PascGaloisJE*. The takeaway is that, regardless of the prime and the nonzero value placed down both sides, automorphisms describe the triangle. Take the first $p$ rows and then apply the automorphisms by index following the first $p$ rows Pascal's Triangle. This will generate the first $p^2$ rows. The same result applies for the first $p^n$ and $p^{n+1}$ rows, $n \geq 1$.

# Chapter 12

**Exercise 12.4:** The tables are as follows:

| $\odot$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

| $\odot$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

| $\odot$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

| $\odot$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

Using either the definition of $\odot$ or by direct inspection in the tables, we can see that $\odot$ is commutative on these sets. 1 is the unity in each case. The units in each set are as follows:

$\mathbb{Z}_4$: 1,3
$\mathbb{Z}_5$: 1,2,3,4
$\mathbb{Z}_5$: 1,5
$\mathbb{Z}_5$: 1,2,3,4,5,6

The units are the values that are relatively prime to $n$. In the prime cases, all nonzero values are units. $\mathbb{Z}_n$ is a field for $n = 5, 7$.

**Exercise 12.5:** From linear algebra we know $2 \times 2$ matrices with real entries are closed under both matrix addition and matrix multiplication. Both operations are associative as well. The $2 \times 2$ zero matrix is the additive identity.

If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $a, b, c, d \in \mathbb{R}$, then $-A = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$. Since matrix addition is commutative, $M_{2\times 2}(\mathbb{R})$ is an abelian group. The last requirements for a ring are the two distributive properties. These are well-established facts from linear algebra, but also very easy to check with a few matrix computations.

**Exercise 12.6:** i) $S$ is not commutative under matrix multiplication. For example:

$$\text{Let } A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} (1)(0)+(0)(0) & (1)(1)+(0)(0) \\ (0)(0)+(0)(0) & (0)(1)+(0)(0) \end{bmatrix}$$
$$= \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$BA = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} (0)(1)+(1)(0) & (0)(0)+(1)(0) \\ (0)(1)+(0)(0) & (0)(0)+(0)(0) \end{bmatrix}$$
$$= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

ii) Yes, $S$ has unity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

iii) The units of $S$ are the invertible matrices. This means that they have determinant zero. Equivalently, they are of rank 2.

iv) $S$ is not a field, since not all $2 \times 2$ matrices are invertible. For example, $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ has determinant zero and is not invertible.

**Exercise 12.7:** i) If 0 is placed down both sides of the triangle, the triangle of all zeros results since $0 \cdot 0 = 0$.

$\mathbb{Z}_3$: $a = 2$ produces a copy of the mod 2 triangle.

$\mathbb{Z}_4$: $a = 2$ produces a triangle of zeros beneath the edges; $a = 3$ produces a copy of the mod 2 triangle.

$\mathbb{Z}_5$: $a = 2, 3$ produces a copy of the mod 4 triangle; $a = 4$ produces a copy of the mod 2 triangle.

$\mathbb{Z}_6$: $a = 2$ produces a copy of the mod 2 triangle, $a = 3$ gives a solid triangle consisting only of 3's; $a = 4$ gives a solid triangle consisting only of 4's; $a = 5$ produces a copy of the mod 2 triangle.

$\mathbb{Z}_7$: $a = 2$ produces a copy of the mod 3 triangle; $a = 3$ produces a copy of the mod 6 triangle; $a = 4$ produces a copy of the mod 3 triangle; $a = 5$ produces a copy of the mod 6 triangle; $a = 6$ produces a copy of the mod 2 triangle.

You can check $n = 8, 9, 10$ yourself, but should observe similar behaviors. In all cases, think about closed subsets under multiplication and any group structure that results from this multiplication.

ii) If $a = 1$, then a triangle of all 1's results regardless of $n$ since 1 is the multiplicative identity. This is analogous to using 0 down both sides under addition mod $n$.

iii)-v) Experiment with these on your own. In some cases, you will see patterns identical to those generated over groups. In other cases, new patterns will be revealed. In particular, look for examples where the top portion of the triangle is nonzero, but then the triangle eventually "dies out" into a subtriangle of 0's. Pay close attention to how the ring elements line up right before this happens. Also, not the modulus in each case. This is addressed further in Exercise 12.10.

**Exercise 12.10:** i) The triangles using composite moduli can produce the propagating zeros, depending on which values are placed down the sides. Anytime a pair of zero divisors are next to each other in a triangle, a zero appears beneath them. Since multiplication by 0 always yields 0, the propagation results.

ii) When placing a single value $a$ down both sides using a prime modulus, a structure equivalent to a mod $m$ triangle under addition will result. If $n$ is prime, $\mathbb{Z}_n$ is a field and has no zero divisors. If $n$ is composition, mod $m$ triangles under addition can still occur, but it depends on the choice of $a$ and $n$. When placing two different values down the side, the relationship is more complicated but worth further experimentation!

**Exercise 12.11:** The $T_{\mathbb{Z}_{10}}(6, 8)$ triangle under multiplication mod 10 is the same as the mod 4 triangle with an extra edge of zeros down the left side. Given that 10 is composite and 6,8, and 10 are all divisible by two (hence, not relatively prime), one may expect zero divisors to align and cause the propagating zeros. But that does not occur in this case and a mod 4 additive structure results.

**Exercise 12.13:** i) Consider the set $U_5 = \{1, 2, 3, 4\} \subset \mathbb{Z}_5$. Here is the Cayley table:

| $\odot$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

We see $U_5$ is closed under multiplication and 1 is the identity. Modular multiplication is always associative. For inverses, we have $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, and $4^{-1} = 4$. Hence, $U_5$ is a group under multiplication mod 5.

ii) In $\mathbb{Z}_5$ under multiplication, all nonzero elements have multiplicative inverses and, hence, are units.

iii) Since there are only two groups of order 4, $\mathbb{Z}_4$ and the Klein 4-group, $U_5$ must be isomorphic to one of these. By i) we see that only two of the elements

are their own inverses. So $U_5 \simeq \mathbb{Z}_4$. Alternatively, you could also show that $U_5$ is generated by 2 (or 3), making it a cyclic group.

For an explicit isomorphism, define $\phi : U_5 \longrightarrow \mathbb{Z}_5$ by $\phi(1) = 0$, $\phi(2) = 1$, $\phi(3) = 3$, and $\phi(4) = 2$.

iv) If 4 is placed down both sides, the resulting triangle looks like the mod 2 triangle, rather than the mod 4. The reason is that 4 is not a generator for $U_5$. It only generates a cyclic subgroup of order 2. As the isomorphism from iii) shows, 4 plays the same role in $U_5$ as 2 does in $\mathbb{Z}_4$. Similarly, 2 only generates a cyclic subgroup of order 2 in $\mathbb{Z}_4$.

**Exercise 12.14:** The triangle generated with mod 18 multiplication and 5 down both sides, produces 6 colors and appears to be the mod 6 triangle (under addition). The elements produced are 1, 5, 7, 11, 13, and 17. These are the elements of $U_{18}$. For an isomorphism, define $\phi : U_{18} \longrightarrow Z_6$ by $\phi(5) = 1$. Here, we are mapping a generator to a generator and the rest of the isomorphism uniquely follows by using the 'preserves the operation property'. Alternatively, you can use *PascGaloisJE* and see the isomorphism by placing the two triangles side-by-side.

**Exercise 12.17:** The techniques discussed so far do not provide a meaningful way to assign a fractal dimension to the entire spacetime diagram. However, there is an obvious split in the diagram and the two subtriangles formed could be investigated by the growth rate dimension and its generalization allowing for substructures that scale. You can investigate this idea further in the Projects.

**Exercise 12.18:** If row 27 is added, it will consist of all zeros except for the two 1's on the ends. This suggests the binomial identity

$$\binom{3^n}{k} \equiv 0 \qquad \text{mod } p \qquad \text{for } 0 < k < 3^n$$

for all $n \geq 1$. This will soon be generalized in the text.

**Exercise 12.21:** For $p = 3$:

$5 = (12)_3$ and $7 = (21)_3$. So, $(12)_3 + (21)_3 = (110)_3$

which results in 2 carries. Hence, $3^2 \mid \binom{12}{5}$.

For $p = 5$:

$5 = (10)_5$ and $7 = (12)_5$. So, $(10)_5 + (12)_5 = (22)_5$

which results in no carries. Hence, $5 \nmid \binom{12}{5}$.

For $p = 11$:

$5 = (5)_{11}$ and $7 = (7)_{11}$. So, $(5)_{11} + (7)_{11} = (11)_{11}$

which results in one carry. Hence, $11 \mid \binom{12}{5}$.

**Exercise 12.23:** This proof is the same as the proof for Proposition 2.9, just adjusting for the number of rows.

**Exercise 12.24:** This proof is the same as the proof for Proposition 2.12, just adjusting for the number of rows.

**Exercise 12.25:** i) First, assume that $p \equiv 3 \bmod 4$ and $n$ is odd. Note that $3^n \equiv 1 \bmod 4$ when $n$ is even and $3^n \equiv 3 \bmod 4$ when $n$ is odd. Thus, $p^n \equiv 3^n \equiv 3 \equiv -1 \bmod 4$. We can rewrite this as $p^n - 1 \equiv -2 \equiv 2 \bmod 4$. This means $p^n - 1 = 4k + 2 = 2(2k + 1)$ for some integer $k$. Hence, $\frac{p^n-1}{2}$ is odd.

For the forward direction, first note that $p^2 \equiv 1 \bmod 4$ for any odd prime. If $n = 2m$ is even, then $p^{2m} = (p^2)^m \equiv 1 \bmod 4$ and so $p^{2m} - 1 \equiv 0 \bmod 4$, which means that $\frac{p^{2m}-1}{2}$ is even.

Now assume $\frac{p^n-1}{2}$ is odd. Then $\frac{p^n-1}{2} = 2q + 1$ and, equivalently, $p^n - 1 = 4q+2$ for some integer $q$. This can be rewritten as $p^n - 3 = 4q$ and, thus, $p^n \equiv 3 \bmod 4$. From the argument in the previous paragraph, we know $n$ must also be odd.

ii) The condition in the product formula can be updated using $p \equiv 3 \bmod 4$ and $n$ rather than $\frac{p^n-1}{2}$.

**Exercise 12.26:** For a prime $p$,

$$\sum_{k=0}^{p^n-1} \binom{p^n - 1}{k} \equiv 1 \bmod p.$$

This is a generalization of Exercise 2.10. The proof is basically the same: The sum is 1 since the entries in row $p^n - 1$ of the mod $p$ triangle are being added. This row consists of alternating pairs of 1 and $p - 1$ until the last entry in the row, which is a 1, appears.

**Exercise 12.28:** For $p = 7$:

$$\binom{14}{14}\binom{21}{14}\binom{28}{14}\binom{35}{14}\binom{42}{14} \equiv 1 \cdot 3 \cdot 6 \cdot 3 \cdot 1 \equiv 5 \bmod 7.$$

For $p = 11$ :

$$\binom{22}{22}\binom{33}{22}\binom{44}{22}\binom{55}{22}\binom{66}{22}\binom{77}{22}\binom{88}{22}\binom{99}{11}\binom{110}{22}$$

$$\equiv 1 \cdot 3 \cdot 6 \cdot 10 \cdot 4 \cdot 10 \cdot 6 \cdot 3 \cdot 1 \equiv 9 \bmod 11.$$