Visualization of Algebraic Structures using MATLAB

Foster Teng

Topic: Cyclic group

Supervisor: Prof. Camelia Karimianpour

Summer 2025

Contents

1 Introduction **2**

2 Cyclic Groups $\mathbb{Z}/n\mathbb{Z}$ **2**

3 Direct Products of Cyclic Groups **4**

3.1 $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ for prime p 4

3.2 $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ for composite n 8

3.3 $(\mathbb{Z}/2\mathbb{Z})^n$ 11

4 Functions of Two Variables over Finite Fields $\mathbb{Z}/p\mathbb{Z}$ on $\mathbb{R}^2$ **11**

4.1 Comparison between $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{R}$ 12

5 Conclusion and Future Directions **16**

1 Introduction

We use the method of visualization to understand more the structure of finite groups, particularly cyclic groups and their products. And MATLAB becomes our main tool to generate the images we desire.

2 Cyclic Groups $\mathbb{Z}/n\mathbb{Z}$

Objective

- There exists a bijection between regular polygons on the unit circle and the subgroups of $\mathbb{Z}/n\mathbb{Z}$.
- Each element in $\mathbb{Z}/n\mathbb{Z}$ can be represented by a vertical line connecting all integers in the same equivalence class, with a distinct color, by wrapping the real line around a cylinder.

The group $\mathbb{Z}/n\mathbb{Z}$ consists of the integers 0, ..., n-1 modulo n with operation being additive. And by Theorem 7.(3), Dummit and Foote [1, p. 58]:

For every positive divisor k of n, there exists a cyclic subgroup H of $\mathbb{Z}/n\mathbb{Z}$ such that $|H| = k$. Moreover, this subgroup is unique up to its order.

In order to explore richer subgroup structures, we choose $n = 24$, so that the divisors $k = 1, 2, 3, 4, 6, 8, 12, 24$ yield distinct cyclic subgroups. Each subgroup is represented as a regular polygon, with its generators indicated by bold nodes. See the following video for a demonstration: `https://youtu.be/JsfWLnf7_GI`.

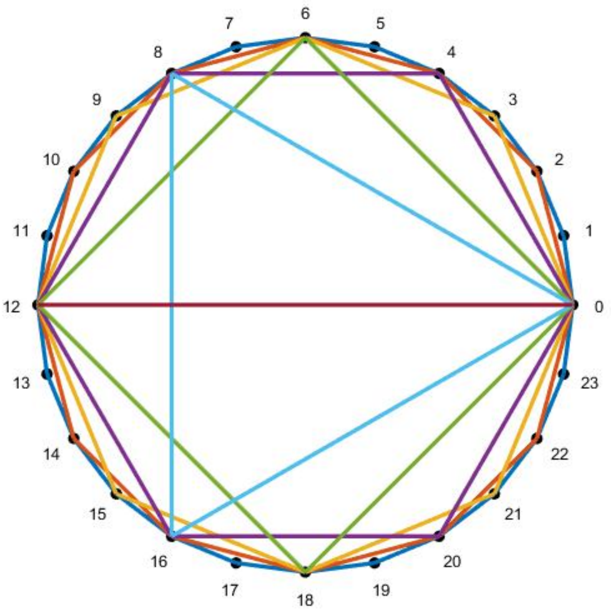

Figure 1: Overlay of all cyclic subgroups of $\mathbb{Z}/24\mathbb{Z}$. Each k-gon corresponds to the unique subgroup of order k

Our visualization provides a correspondence between polygons inclosed within a circle and subgroups of $\mathbb{Z}/n\mathbb{Z}$. Specifically, the unique subgroup of order k is identified by a k-gon formed by nodes labeled with the elements of this subgroup. To achieve this, we plot a unit circle in Figure 1 and label the nodes $0, 1, \ldots, 22, 23$ on it. These nodes represent the 24 elements of $\mathbb{Z}/n\mathbb{Z}$. Next, for each divisor k of n, we represent a cyclic subgroup of order k by a regular polygon with k vertices. This visualization was motivated by the nth roots of unity on the complex unit circle.

We can also define $\mathbb{Z}/24\mathbb{Z}$ as $\{[0], [1], \ldots, [23]\}$, that is, the set of equivalence classes. To visualize this, we wrap all the integers on the real line into an infinitely long cylinder, as shown in Figure 2 below. We consider only a segment of this infinite cylinder containing the numbers from 1 to 120, so that the cylinder displays exactly 5 complete periods. Each element in $\mathbb{Z}/24\mathbb{Z}$, which is an equivalence class of all integers mod 24, is represented by a vertical line with a specific color, and the gradient of 24 colors corresponds to the 24 elements of $\mathbb{Z}/24\mathbb{Z}$.

Interestingly, if we form the elements $1, 2, ..., 119, 120$ as a group, then each circular period represents a coset by taking the first period with elements $1, 2, ..., 23, 24$ as a normal subgroup.

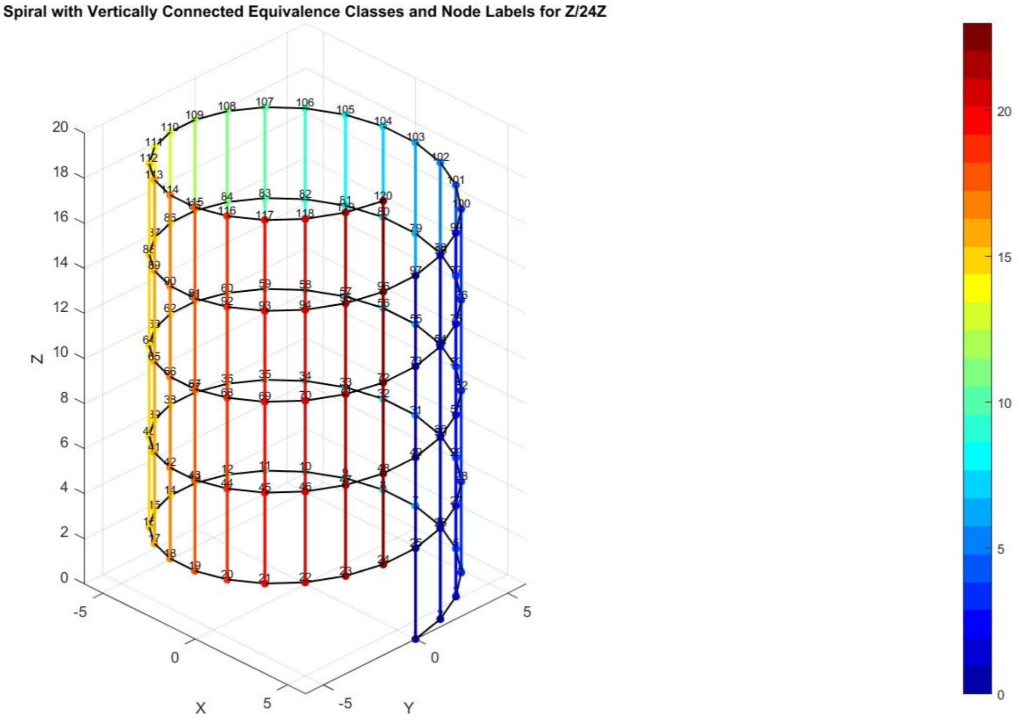

Figure 2: Visualization of $\mathbb{Z}/24\mathbb{Z}$ as equivalence classes on a cylinder. Each vertical line represents an equivalence class modulo 24, with elements stacked along the height of the cylinder. The color gradient distinguishes the 24 distinct classes, and 5 complete periods are shown corresponding to the integers from 1 to 120.

3 Direct Products of Cyclic Groups

3.1 $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ for prime p

Definition. The group $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ is the direct product of two copies of the cyclic group $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number. It consists of all ordered pairs of the form (a, b), where $a, b \in \mathbb{Z}/p\mathbb{Z}$, with componentwise addition modulo p:

$$(a, b) + (c, d) = (a + c, b + d) \mod p.$$

The identity element is $(0, 0)$, and each element (a, b) has an inverse $(-a, -b)$.

For each non-identity element $(g_1, g_2) \in (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$, where p is a prime number, the subgroup $\langle (g_1, g_2) \rangle$ generated by this element has order p by Lagrange's Theorem. This follows from the fact that $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ has order p^2 and is not cyclic.

Moreover, any two distinct subgroups of order p must intersect trivially. If their intersection contained a non-identity element, it would be a subgroup of order p contained in both, which implies the two subgroups are equal, contradicting the assumption.

Therefore, the group $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$, excluding the identity element, is partitioned into disjoint cyclic subgroups of order p. Since each such subgroup contains $p - 1$ non-identity elements, the total number of distinct subgroups is

$$\frac{p^2 - 1}{p - 1} = p + 1, \quad \text{where} \quad p^2 - 1 = \left| (\mathbb{Z}/p\mathbb{Z})^2 \setminus \{e\} \right|.$$

We visualize the group $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ for $p = 2, 3, 5$, and 7, where the group elements are arranged on a 2D grid to reveal structural patterns. The following notational conventions are used in the visualization:

- 1 the generator of $\mathbb{Z}/p\mathbb{Z}$.
- The elements of $\mathbb{Z}/p\mathbb{Z}$ are placed along the horizontal and vertical axes using the numbers from 0 to $p - 1$
- One generator (not unique) of each cyclic subgroup of $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ is circled.
- Each color represents a distinct cyclic subgroup of $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ of order p. There are $p + 1$ distinct non-white colors, and elements are colored according to the subgroup to which they belong.
- The identity element, which belongs to all subgroups, is uniquely colored in white.
- The order of each subgroup is indicated next to the colorbar.

For $p = 2$ in Figure 3 below, we can see that the group is isomorphic to Klein four-group.

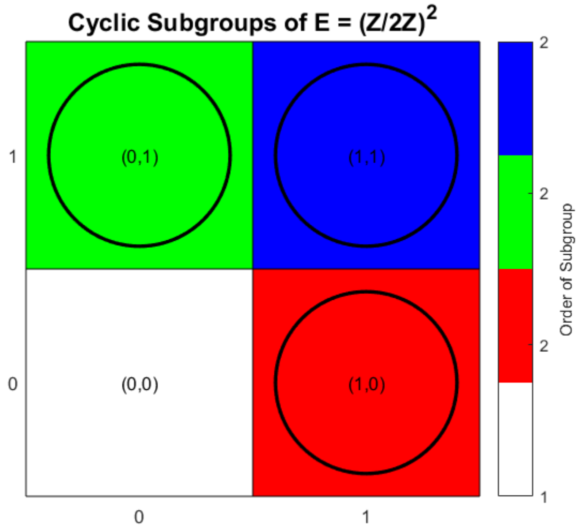

Figure 3: Visualization of the cyclic subgroups of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Each color represents a distinct cyclic subgroup of order 2. One generator of each subgroup is circled. The identity element is colored in white.

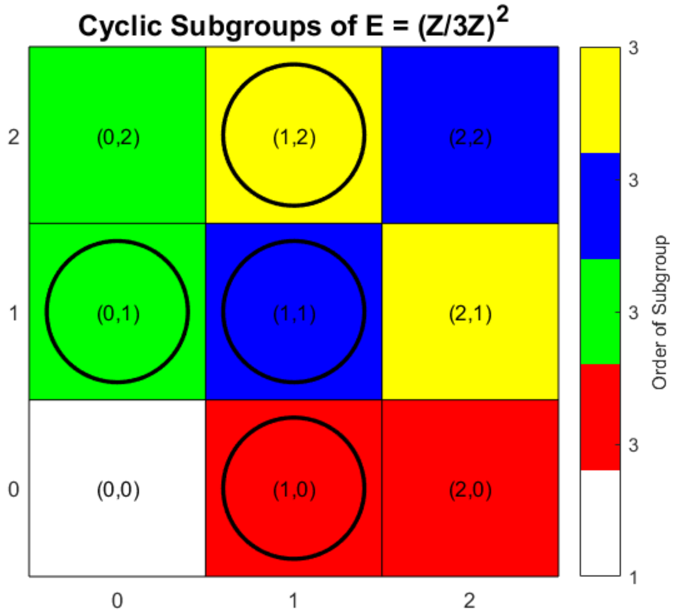

Figure 4: Visualization of the cyclic subgroups of $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$. Each color represents a distinct cyclic subgroup of order 3. One generator of each subgroup is circled. The identity element is colored in white.

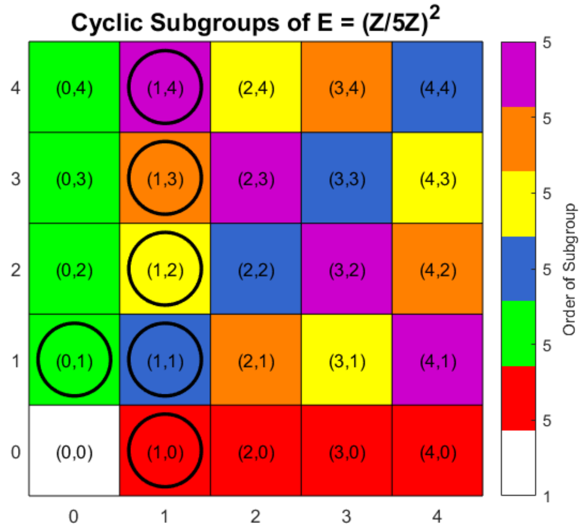

Figure 5: Visualization of the cyclic subgroups of $(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$. Each color represents a distinct cyclic subgroup of order 5. One generator of each subgroup is circled. The identity element is colored in white.

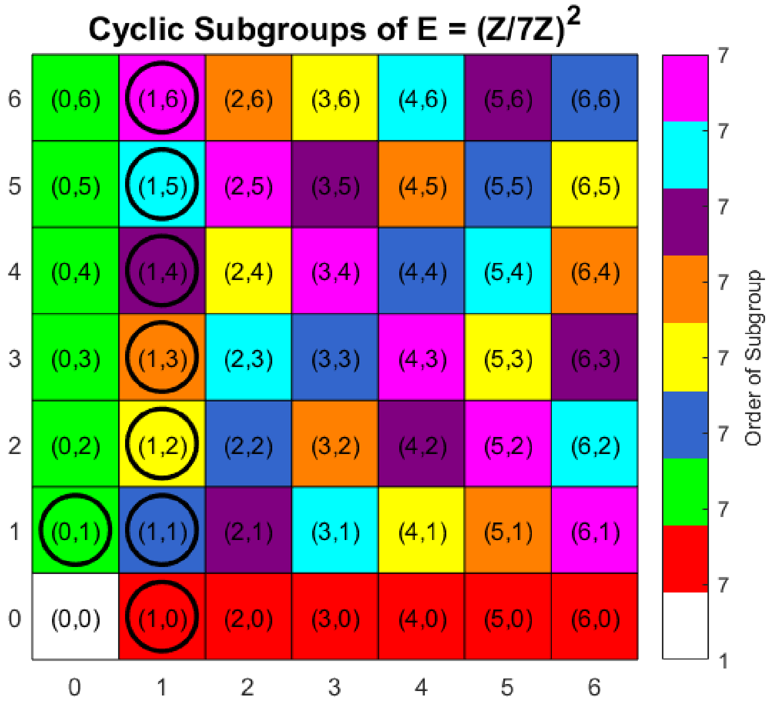

Figure 6: Visualization of the cyclic subgroups of $(\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})$. Each color represents a distinct cyclic subgroup of order 7. One generator of each subgroup is circled. The identity element is colored in white.

Conclusion

In general, for the group $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$, where p is prime, all subgroups are cyclic and pairwise disjoint except at the identity element. This property is clearly reflected in the visualization through the way subgroup elements are distributed.

For $p = 2$ (Figure 3), the group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ has 3 cyclic subgroups, so the visualization displays 3 distinct non-white colors.

For $p = 3$ (Figure 4), the group $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ has 4 cyclic subgroups, resulting in 4 distinct non-white colors. Notice that these 4 subgroups are displayed as vertical, horizontal, diagonal, and anti-diagonal components on the grid, generated respectively by $(0, y)$, $(x, 0)$, (x, y), and (x, y^2).

For $p = 5$ (Figure 5), the group $(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ has 6 cyclic subgroups, resulting in 6 distinct non-white colors. In this case, two additional subgroups appear compared to Figure 4, forming windmill-shaped patterns on the grid, generated by (x, y^2) and (x, y^3), respectively.

For $p = 7$ (Figure 6), the group $(\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})$ has 8 cyclic subgroups, resulting in 8 distinct non-white colors. In this case, four additional subgroups appear compared to Figure 4, forming stretched windmill-shaped patterns on the grid, generated by (x, y^2), (x, y^3), (x, y^4), and (x, y^5), respectively.

For each case, we can observe certain embedding structures. For example, in Figure 5, there are 6 such structures, corresponding to the 6 cyclic subgroups. These can be viewed as embedding maps $\varphi : \mathbb{Z}/5\mathbb{Z} \to (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$, defined as follows:

- $g \mapsto (g, 0)$, corresponding to $\langle (x, 0) \rangle$
- $g \mapsto (0, g)$, corresponding to $\langle (0, y) \rangle$
- $g \mapsto (g, g)$, corresponding to $\langle (x, y) \rangle$
- $g \mapsto (g, g^2)$, corresponding to $\langle (x, y^2) \rangle$
- $g \mapsto (g, g^3)$, corresponding to $\langle (x, y^3) \rangle$
- $g \mapsto (g, g^4)$, corresponding to $\langle (x, y^4) \rangle$

where $g \neq 0$

These embeddings correspond, respectively, to the horizontal red, vertical green, diagonal blue, windmill-shaped yellow, windmill-shaped orange, and anti-diagonal purple components in the grid.

3.2 $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ for composite n

For composite values of n, the subgroups are no longer disjoint due to the increased number of divisors. Instead of visualizing distinct subgroups, we represent the order of each element in the group by assigning a color corresponding to its order. This allows us to observe the distribution of elements with different orders across the group.

For $n = 4$ in Figure 7 below, there are three types of elements of orders 1, 2, and 4.

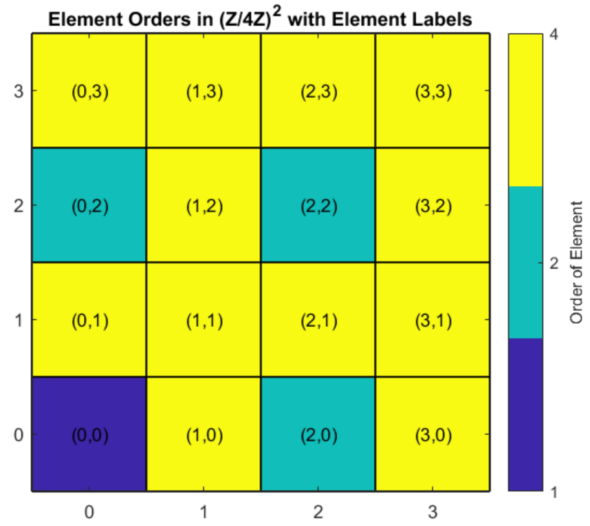

Figure 7: Order of elements in $(\mathbb{Z}/4\mathbb{Z})^2$.

For $n = 6$ in Figure 8 below, the elements can have one additional order, as shown by the appearance of one additional color.

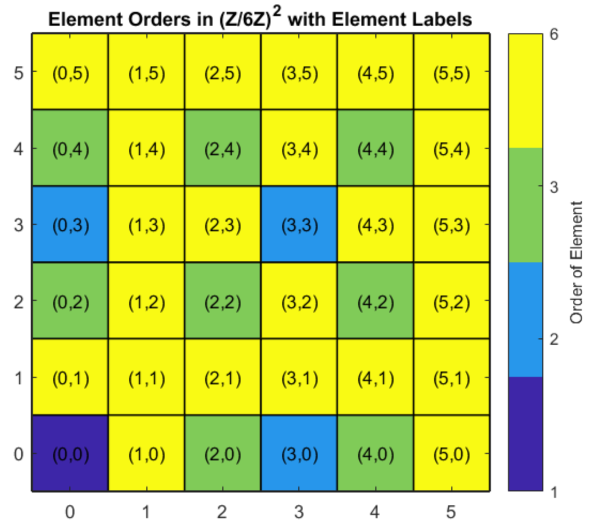

Figure 8: Order of elements in $(\mathbb{Z}/6\mathbb{Z})^2$.

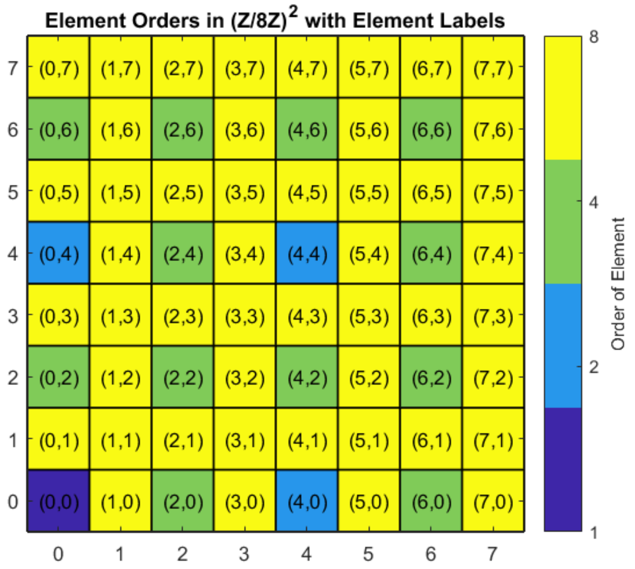

Figure 9: Order of elements in $(\mathbb{Z}/8\mathbb{Z})^2$.

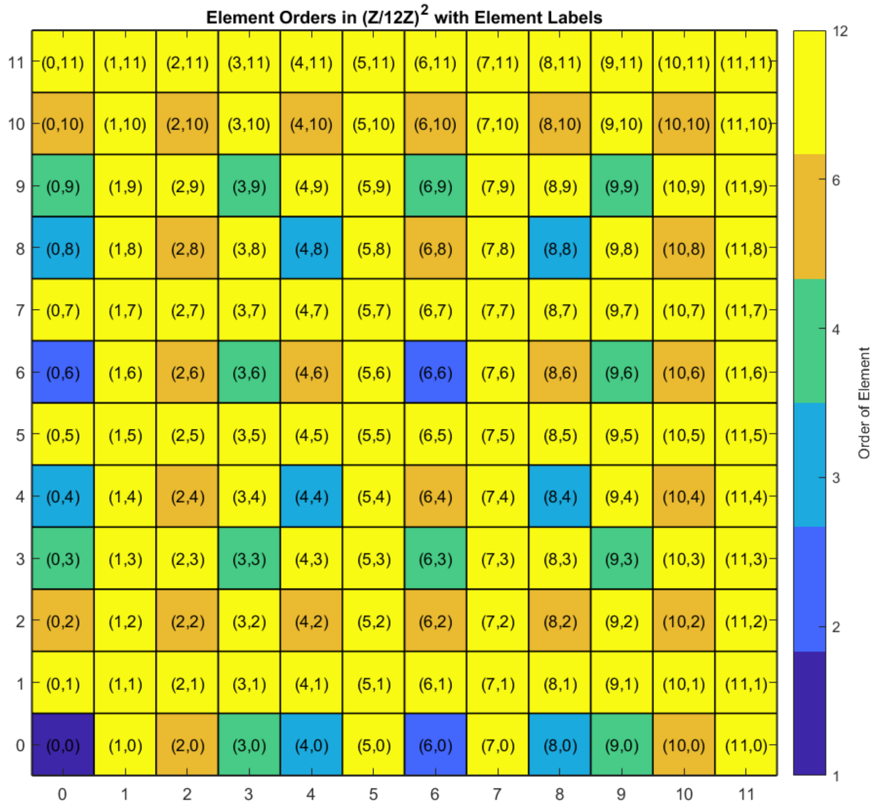

Figure 10: Order of elements in $(\mathbb{Z}/12\mathbb{Z})^2$.

Conclusion

For any composite n above, we can immediately conclude that the group $(\mathbb{Z}/n\mathbb{Z})^2$ is not cyclic, since the greatest order of its elements is n (colored yellow).

For $n = 4$ in Figure 7, elements of order 2 are rare: in fact, fewer than one fourth of the elements have order 2. Although $|(\mathbb{Z}/4\mathbb{Z})^2| = 16$ and $8 \mid 16$, there is no element of order 8, implying that there is no cyclic subgroup of order 8. This again proves that $(\mathbb{Z}/4\mathbb{Z})^2$ cannot be cyclic by Theorem 7.3(3) in Dummit and Foote [1, p. 58]. Finally, we observe that the non-yellow elements (0, 0), (0, 2), (2, 0) and (2, 2) form a subgroup $\langle(0, 2),(2, 0)\rangle \leq (\mathbb{Z}/4\mathbb{Z})^2$ generated by (0, 2) and (2, 0).

For $n = 6$ in Figure 8, note that $4, 9, 12, 18, 36 \mid \left|(\mathbb{Z}/6\mathbb{Z})^2\right|$, yet no elements of these orders appear, which will be explained shortly. As before, the subgroups $\langle(2, 0),(0, 2)\rangle$ and $\langle(3, 0),(0, 3)\rangle \leq (\mathbb{Z}/6\mathbb{Z})^2$ consist entirely of elements that are not yellow.

For $n = 8$ in Figure 9, we observe the subgroup chain $\langle(4, 0),(0, 4)\rangle \leq \langle(2, 0),(0, 2)\rangle \leq (\mathbb{Z}/8\mathbb{Z})^2$.

For $n = 12$ in Figure 10, we observe two subgroup chains $\langle(4, 0),(0, 4)\rangle \leq \langle(2, 0),(0, 2)\rangle \leq (\mathbb{Z}/12\mathbb{Z})^2$ and $\langle(6, 0),(0, 6)\rangle \leq \langle(3, 0),(0, 3)\rangle \leq (\mathbb{Z}/12\mathbb{Z})^2$.

From the observations above, we draw the following conclusions.

First, For Figures 7 to 10, an element $(g_1, g_2) \in (\mathbb{Z}/n\mathbb{Z})^2$ is non-yellow if and only if $\gcd(g_1, n) \neq 1$ and $\gcd(g_2, n) \neq 1$. The converse follows by assuming, without loss of generality, that $\gcd(g_1, n) = 1$, then $|g_1| = n$, which implies $|(g_1, g_2)| = n$ and thus (g_1, g_2) is yellow. This little theorem helps us understand which elements are yellow and which are not.

Second, if p is a prime divisor of n such that $p^k \mid n$, then the subgroup $\langle(p, 0),(0, p)\rangle$ forms a single large square. For example, in Figure 8, when $p = 2$, this square includes all green elements together with $(0, 0)$. If n has at least two distinct prime divisors, say p_1 and p_2, then the union of the two corresponding squares yields a star-shaped pattern. In Figure 8, for $p_1 = 2$ and $p_2 = 3$, the combined blue and green regions, together with the identity, produce the points $(2, 2)$, $(2, 4)$, $(3, 3)$, $(4, 2)$, and $(4, 4)$.

3.3 $(\mathbb{Z}/2\mathbb{Z})^n$

We now turn to the n-fold direct product of $\mathbb{Z}/2\mathbb{Z}$, denoted $(\mathbb{Z}/2\mathbb{Z})^n$. This is an elementary abelian 2-group of order 2^n, with group operation given by componentwise addition modulo 2. The Cayley table of this group for $n = 4$ is shown below, visualized as a heat map where the group elements are ordered canonically.

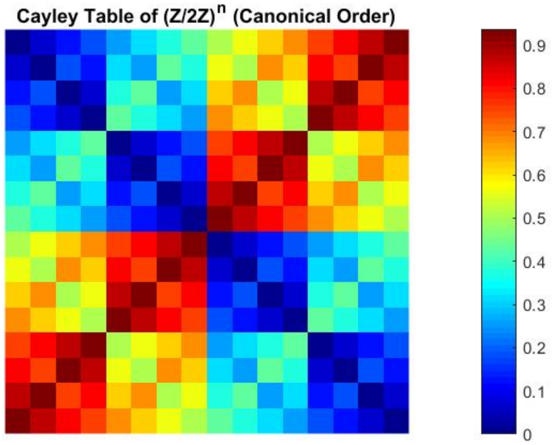

Figure 11: Cayley table of $(\mathbb{Z}/2\mathbb{Z})^4$ in canonical order. Colors represent normalized values for visual contrast.

Conclusion

Each time we take the direct product of $\mathbb{Z}/2\mathbb{Z}$, we reveal a deeper internal structure. For $n = 4$ in Figure 11 above, the first factor in $(\mathbb{Z}/2\mathbb{Z})^n$ is represented by the four largest squares in blue and red. The second factor is represented by the sixteen next-largest squares in varying shades of blue and red, and so on. There are four layers of such structure since $n = 4$. More blue coloration indicates the addition of elements with lower order, while more red coloration indicates the addition of elements with higher order.

4 Functions of Two Variables over Finite Fields $\mathbb{Z}/p\mathbb{Z}$ on $\mathbb{R}^2$

Instead of focusing on each element of the group $(\mathbb{Z}/k\mathbb{Z}) \times (\mathbb{Z}/k\mathbb{Z})$, where k is an integer, we now consider defining a function of two variables

$$f : (\mathbb{Z}/k\mathbb{Z}) \times (\mathbb{Z}/k\mathbb{Z}) \to \mathbb{Z}/k\mathbb{Z}$$

over a finite field. To ensure that $\mathbb{Z}/k\mathbb{Z}$ forms a field, we require k to be a prime number; from this point onward, we will denote it as $\mathbb{Z}/p\mathbb{Z}$.

Before moving on, we introduce two ways of visualizing this construction, as shown in Figure 12 below. For illustration, we take $f(x, y) = x + y$ for $p = 5$ as an example. Throughout this section, we will take the left-hand version to be our way of the visualization.

Notice that in Figure 12, we see five distinct colors, as we are working with $\mathbb{Z}/5\mathbb{Z}$. The image therefore contains exactly five distinct values, which behave like level sets of a function of two variables.

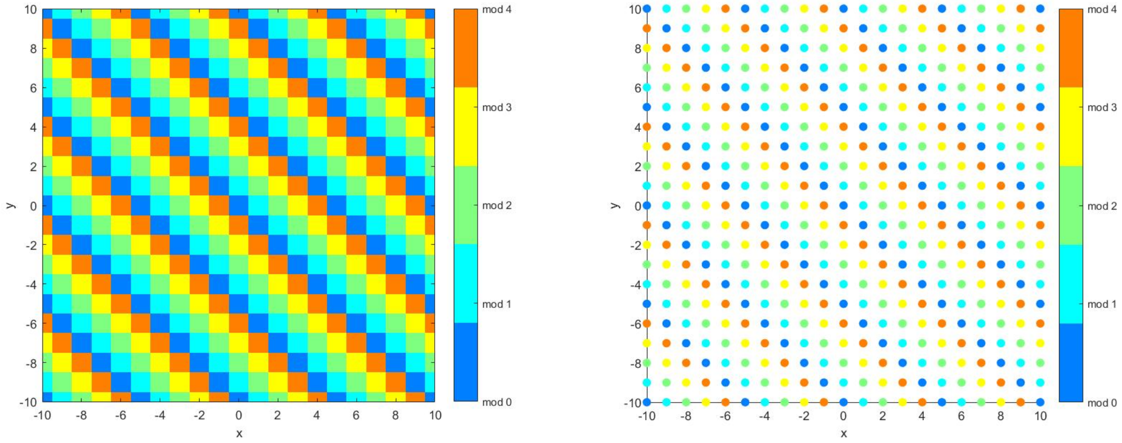

Figure 12: Comparison between scatter plot and grid plot for $x+y \mod 5$ visualized on $\mathbb{R}^2$.

4.1 Comparison between $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{R}$

The motivation for using this style of visualization is illustrated in Figure 13 below. We expect the function $f(x, y) = x^2 + y^2$ to exhibit circular symmetry, as shown by the level sets of this function when defined over the real numbers (right-hand side of the figure). In contrast, when the function is defined over a finite field (left-hand side), the pattern instead shows vertical and horizontal symmetry. Similarly, we observe distinct patterns between $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{R}$, depending on the domain over which the functions are defined, as shown in Figures 14, 15, and 16 below.

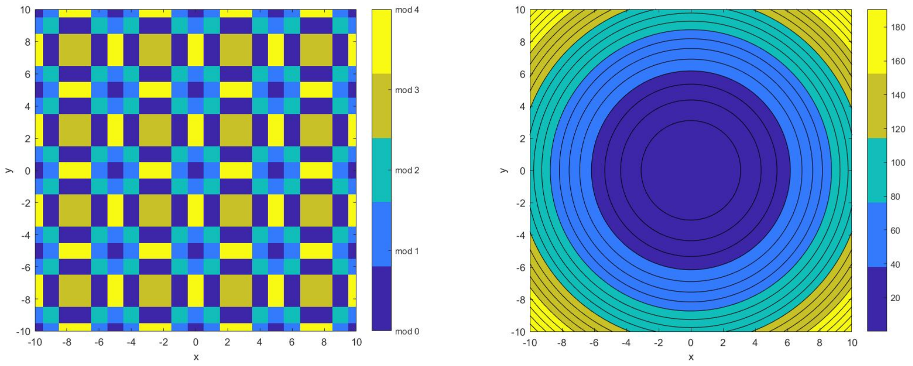

Figure 13: Comparison of the function $f(x, y) = x^2 + y^2$ defined over $\mathbb{Z}/5\mathbb{Z}$ (left) and over $\mathbb{R}$ (right).

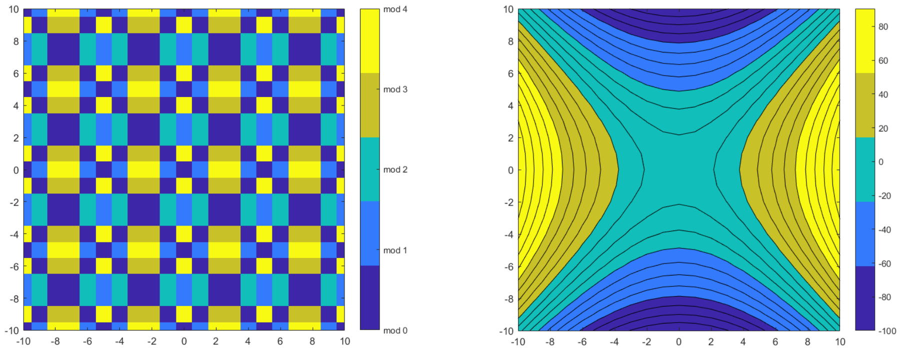

Figure 14: Comparison of $f(x, y) = x^2 - y^2$ over $\mathbb{Z}/5\mathbb{Z}$ (left) and over $\mathbb{R}$ (right).

Notice that in Figures 15 and 16 below, although the left-hand plots lose vertical and horizontal symmetry, they exhibit a new form of symmetry within each 4 × 4 region.

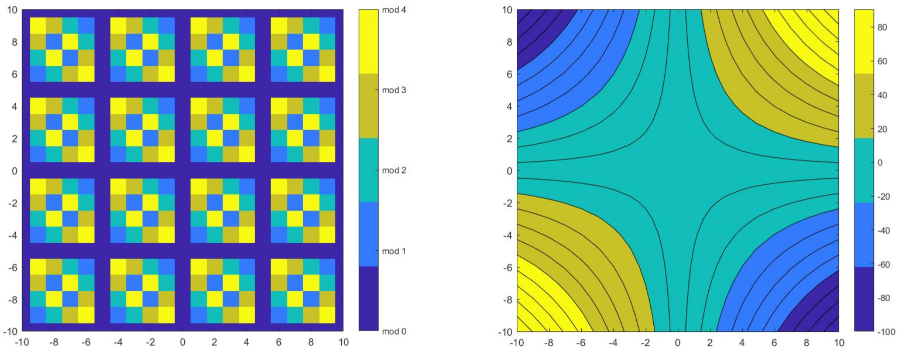

Figure 15: Comparison of $f(x, y) = xy$ over $\mathbb{Z}/5\mathbb{Z}$ (left) and over $\mathbb{R}$ (right).

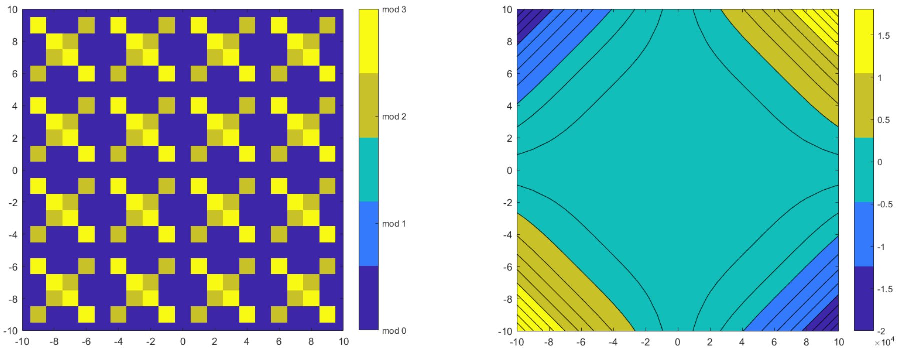

Figure 16: Comparison of $f(x, y) = (x^2 + y^2) \cdot x \cdot y$ over $\mathbb{Z}/5\mathbb{Z}$ (left) and over $\mathbb{R}$ (right).

In Figures 17 and 18 below, the choice of functions results in similar patterns between the left and right plots, which is an interesting observation.

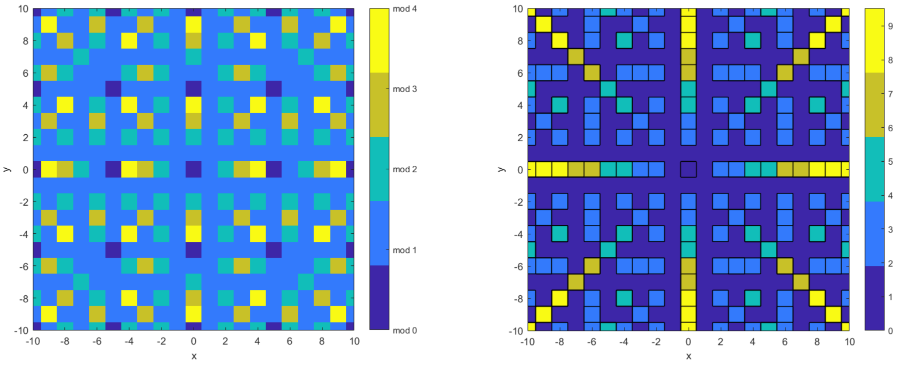

Figure 17: Comparison of the function $f(x, y) = \gcd(x, y)$ defined over $\mathbb{Z}/5\mathbb{Z}$ (left) and over $\mathbb{R}^2$ (right).

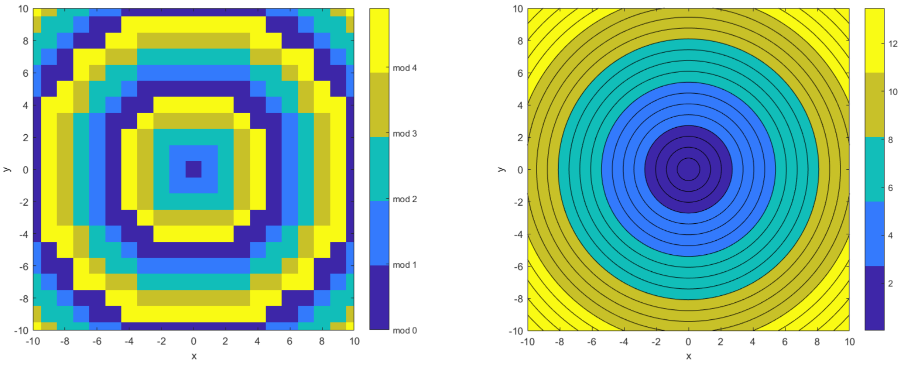

Figure 18: Comparison of the function $f(x, y) = \sqrt{x^2 + y^2}$ defined over $\mathbb{Z}/5\mathbb{Z}$ (left) and over $\mathbb{R}^2$ (right).

Conclusion

When comparing the level sets of two-variable functions defined over different fields, $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{R}^2$, it becomes clear that the choice of function plays a significant role. In particular, functions defined over the finite field $\mathbb{Z}/5\mathbb{Z}$ often produce additional types of symmetry, as seen in Figures 13–16. Moreover, certain functions yield similar patterns across both fields, as illustrated in Figures 17 and 18.

5 Conclusion and Future Directions

The plots of the direct product $(\mathbb{Z}/k\mathbb{Z}) \times (\mathbb{Z}/k\mathbb{Z})$ help us better understand the order and other properties of each element, as we saw in Sections 3.1 and 3.2.

For two-variable functions defined over finite fields $(\mathbb{Z}/p\mathbb{Z})$, we can immediately see that new kinds of symmetry appear. This is interesting in itself, but it also suggests that by changing the choice of functions, we might be able to explore more theoretical questions in the future. For example, it could be worth investigating whether results like Cauchy's theorem, the converse of Lagrange's theorem, or Sylow's theorems could somehow be visualized or better understood using these kinds of function plots. More generally, it raises the question of whether we could find subgroups of certain orders just by looking at patterns in the plots, which seems like a plausible idea, since extra symmetries often show up when we switch to functions over finite fields.

Another possible direction for further exploration is to study the patterns themselves more carefully. For example, in the level sets defined over finite fields in Figures 15 and 16, there might be another way to explain how these patterns form. It would also be interesting to see what happens when we move to a larger field like $\mathbb{Z}/11\mathbb{Z}$ where we might find even more internal structure in each 11×11 region.

References

[1] David S. Dummit and Richard M. Foote, *Abstract Algebra*, 3rd Edition, Wiley, 2004.