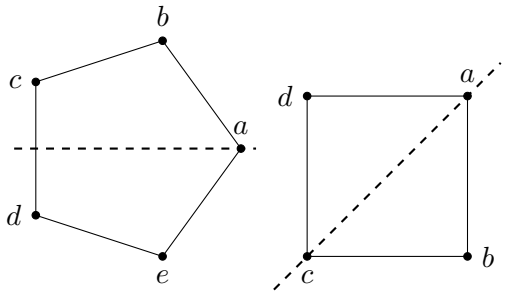
Modern Algebra 1

Grant Talbert
09/12/24
Dr. Duque-Rosero
MA 541 Section A1

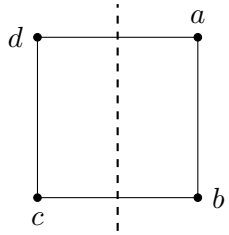
Boston University

Problem 1. Describe the elements of D_n. How many elements does D_n have?

Solution. There is a distinction between shapes with an even number of vertices and shapes with an odd number; for shapes with an even number, an angle bisector must necessarily pass through two angles, whereas a shape with an odd number must only go through one. Reflections across these lines give symmetries. Visual depiction because I'm bad at explaining:



In the case of an odd number of vertices, there are n symmetries given by reflections about lines bisecting angles. In the case of an even number of angles, there are $\frac{n}{2}$ symmetries given by the same reflections, but then another $\frac{n}{2}$ symmetries given by reflections about lines bisecting sides. Another visual depiction:



There are thus n symmetries given by reflections for any n-sided regular polygon, although their form varies slightly (angle bisectors for odd number of angles, angle OR side bisector for even number). Then, for any n-sided regular polygon, there exist n different rotations. Specifically, a rotation by $\frac{360}{n}$ degrees, a rotation by $2\frac{360}{n}$ degrees, and so on until a rotation by 360 degrees, which is the identity element. The Dihedral group thus has $2n$ elements, n of which are reflections (as described previously), and n of which are rotations. □

Problem 2. Let $n \geq 2$. Define R as the rotation of the regular n-gon by $360/n$ degrees, S as any reflection of the n-gon, and R_0 as the identity transformation (rotation by 0 degrees). Explain why

$$D_n = \left\{R_0, R^1, R^2, \ldots, R^{n-1}, S, RS, R^2S.., R^{n-1}S\right\}.$$

Note that $R^iS = SR^{-i}$ for all i.

Solution. As explained in part (a) of Problem 1, each rotation by $360/n$ degrees is a unique symmetry, UNTIL the nth rotation, since a 360 degree rotation is equivalent to the identity rotation R_0. This gives rise to n symmetries, R_0, and up to $n-1$ repeated applications of the rotation R. We write i applications of R as R^i, so $\left\{R_0, R^1, R^2, \ldots, R^{n-1}\right\} \subseteq D_n$. However, there also exist n different reflections of the polygon that are elements of D_n. Since the polygon is rigid, however, it only has two possible orientations: face-up, and face-down. Reflections differ from rotations in that they change the orientation of the shape, but reflections only differ from each other in where the angles end up after the change in orientation. Thus, they only differ by a rotation. So for some arbitrary reflection $S' \neq S$, there will exist some rotation R^i such that applying S and then applying this rotation is equivalent to applying S':

$$S' = R^iS.$$

Thus, we can represent each different reflection as

$$\left\{S, RS, R^2S, \ldots, R^{n-1}S\right\} \subseteq D_n.$$

Note that since function composition is applied left to right, this implies we are reflecting **before** rotating, which is how I described it. Finally, we have

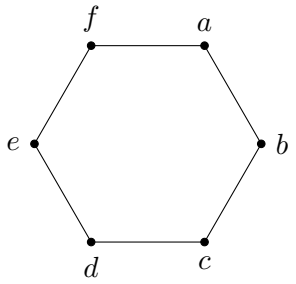
$$D_n = \left\{R_0, R^1, \ldots, R^{n-1}, S, RS, R^2S, \ldots, R^{n-1}S\right\}.$$

□

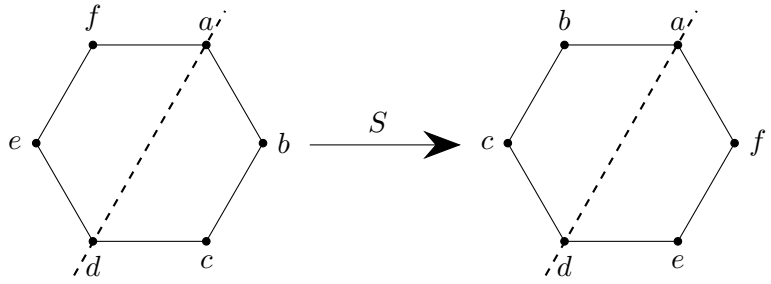
Problem 3. For this problem, recall that D_6 is the dihedral group of order 12, the group of symmetries of the hexagon.

- Find elements $A, B \in D_6$ such that $AB \neq BA$.
- Find elements $A, B, C \in D_6$ such that $AB = BC$ but $A \neq C$.

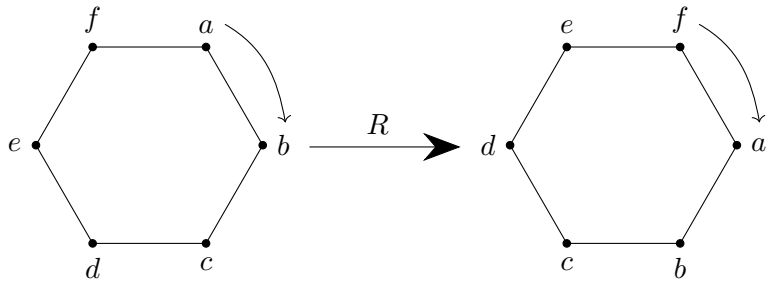
Solution. For simplicity, consider the visualization below.



Take S to be the reflection fixing points a and d.

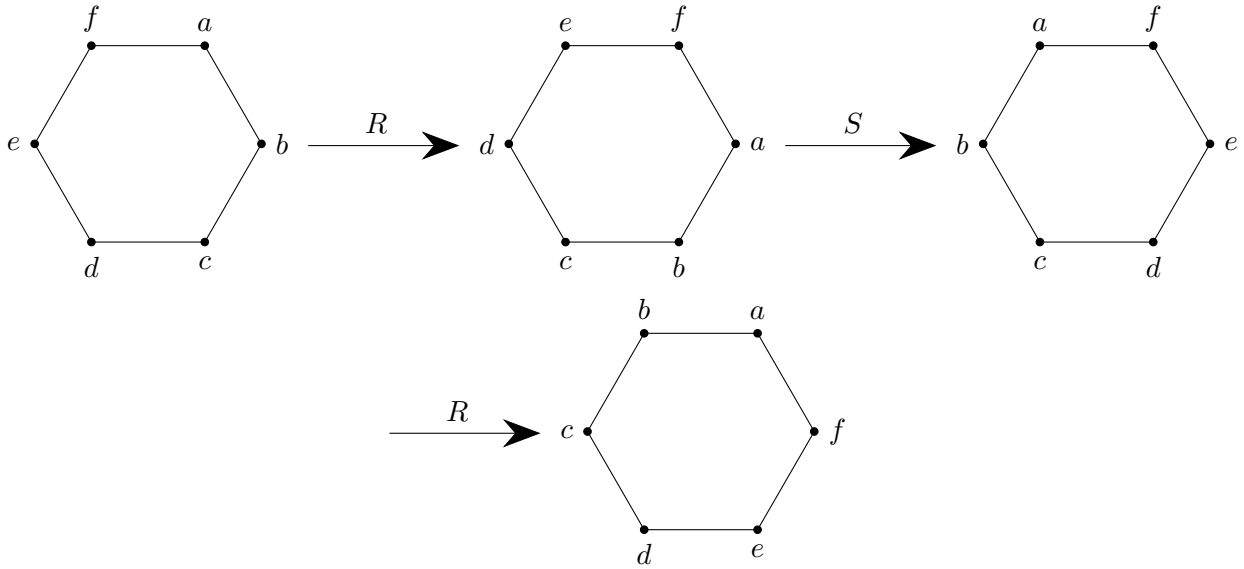


From the visualization, we know S maps b to f, e to c, and vice versa. Now take R to be a clockwise rotation by 60°.

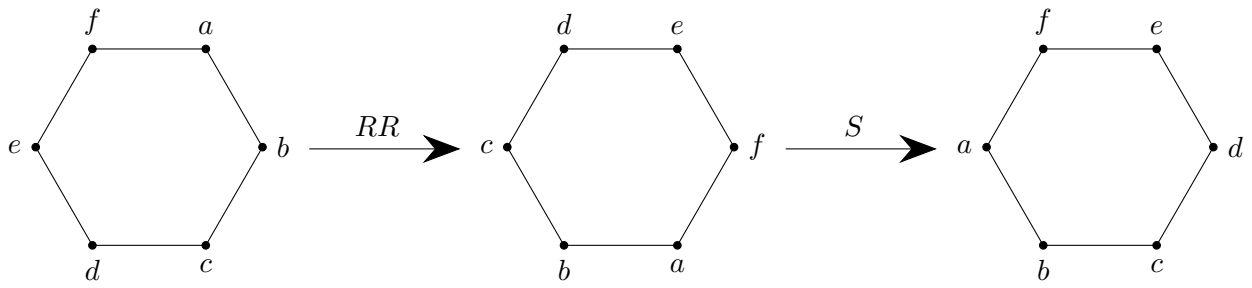


Consider the symmetries $A \coloneqq SR$ and $B \coloneqq R$. We have $AB = SRR$ and $BA = RSR$. Function composition is applied from right to left, so we apply the rightmost transformation first. Rather than tediously explain what point maps to what position, a visual proof has been given.

$BA = RSR$

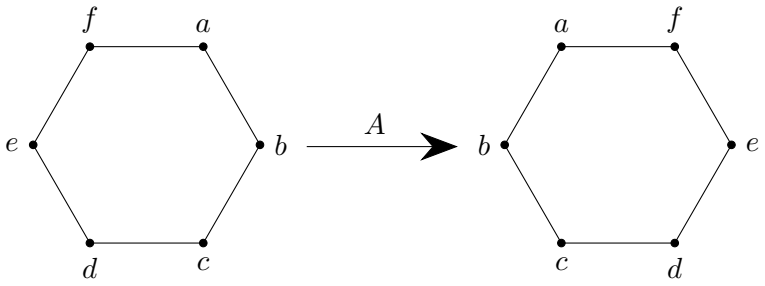


$AB = SRR$

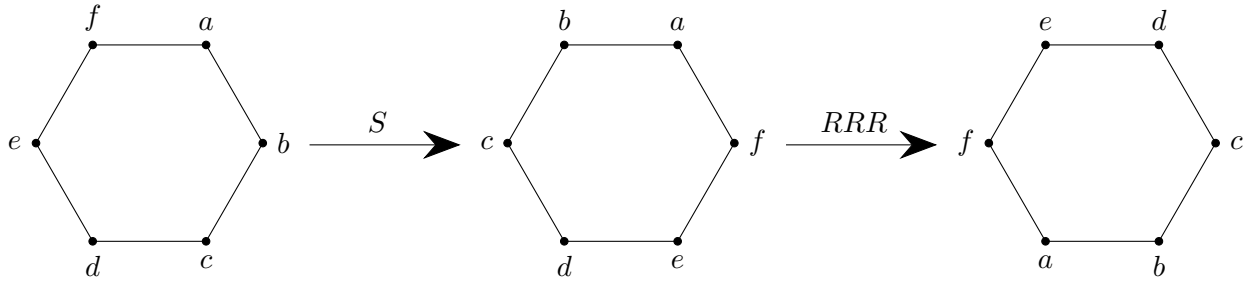


Clearly these hexagons are not in the same orientation, and as such $AB \neq BA$.

For the second part of the problem, let A and B be as previously defined. Notice that the symmetry AB is equivalent to reflecting once and then rotating 4 times. Define $C \coloneqq RRRS$. With this definition, $BC = RRRRS$, one reflection and four rotations. Thus, $AB = BC$. However, it's not necessarily implied that $A \neq C$, since SR and $RRRS$ may simply be different representations of the same symmetry. The result of the transformation A can be seen as the result of the first two transformations present in BA. For simplicity, it has been redrawn below.



Now consider the transformation C:



Clearly, $A \neq C$. As such, we have an example of $AB = BC$ for $A \neq C$. □

Problem 4. Let $G = \{1, 2, 3, 4\}$ with binary operation given by multiplication modulo n. Show that G is a group under this operation.

Solution. This could be easily brute forced with a Cayley Table, but that's boring (and I still did it at the end incase I got something wrong). Instead, I have proven for any $G = \{1, 2, \ldots, n-1\}$, G is a group under multiplication modulo n **if and only if** n is prime. I have denoted the set of prime numbers as $\mathbb{P}$. Since 5 is a prime number, this being true implies that $\{1, \ldots, 4\}$ is a group under multiplication modulo 5. Credit to my friend Cathy for teaching me what a prime decomposition was.

First, we show that if G is a group, then $n \in \mathbb{P}$. Let G be a group. Note that since $0 \notin G$, there cannot be any $a, b \in G$ such that $ab = n$, because this impliess $ab \equiv 0 \mod n \notin G$. For any $n \in \mathbb{Z}$, we

know there exists primes $p_1, \ldots, p_k$ such that

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Suppose $n \notin \mathbb{P}$. Then the prime decompositon of n must contain at least two distinct prime numbers, since otherwise n would be prime. Call these primes $p_1, \ldots, p_k$. It follows that $p_i < n$ for all i, and thus $p_i \in G$ for all i. But then, there would exist numbers p_i in G such that

$$\prod_{i=1}^{k} p_i^{\alpha_i} = n \equiv 0 \mod n.$$

This would imply that G is not a group due to not being closed, which is a contradiction. Thus, we conclude n must be prime to ensure closure under multiplication modulo n, since by definitoin of a prime number there do not exist elements of G that multiply to form n. Therefore, G being a group implies n is prime.

Now we prove $n \in \mathbb{P}$ implies G is a group. Associativity and identity follow immediately from the integers; since all elements of G are integers, and integers are associative under multiplication, G is associative. Additionaly, the identity under multiplication in the integers, 1, is also an element of G. Thus, G has an identity element.

We will now show that multiplication modulo n is indeed a binary operation on G. It will only fail to be a binary operation if there exists $a, b \in G$ such that

$$ab = \lambda n$$

for an arbitrary nonzero integer $\lambda > n$, since any multiple of n would be equivalent to 0 modulo n, and $0 \notin G$. Since every integer has a **unique** prime decomposition, we know both that λ has a prime decomposition

$$\lambda = \prod_{i=1}^{k} p_i^{\alpha_i},$$

and λn must have a prime decomposition that is equivalent to

$$\lambda n = n \prod_{i=1}^{k} p_i^{\alpha_i},$$

since n is a prime number. Since this prime decomposition is **unique**, any factorization of $n\lambda$ must also have this exact prime decomposition, meaning n is either a factor of some number in any factorization of λn, or n must be explicitly present in this factorization. Since ab is a factorization of λn, and since $n \notin G \implies a, b \neq n$, we know that n must be a factor of either a or b. However, $a, b \in G$ implies that $n > a, b$, which cannot be true if n is a factor of a or b. Thus, such an $a, b \in G$ do not exist, and the set is closed under multiplication modulo n.

Finally, we show inverses exist. Credit to https://math.stackexchange.com/a/76676 for solving it because I couldn't figure it out. Bezout's Lemma states for any $a, b, c \in \mathbb{N}$, there exist $u, v \in \mathbb{Z}$ such that $au + bv = c$ if and only if $\gcd(a, b)|c$. Obviously, since n is prime and any $g \in G$ has $g < n$, we have $\gcd(g, n) = 1$. Therefore, there exist u, v such that $gu + nv = 1$. However, adding any multiple of n does not change the value of the number modulo n, so

$$gu + nv \equiv gu \mod n \equiv 1 \mod n.$$

Since 1 is the identity, we know for any $g \in G$ there will exist a corresponding u such that $g^{-1} = u$. However, it's not obvious that $u \in G$. We know that u cannot be a multiple of n, as this would imply $ug = 0 \mod n$, which would be a contradiction. However, this is all we know. It's possible still that $u > n$, and thus $u \notin G$. There would, however, exist $u' \in G$ such that $u \equiv u' \mod n$, since u is not a multiple of n. Proving that for $u \equiv u' \mod n$, $ug \equiv u'g \mod n$ follows from the fact that $u = u' + \alpha n$ for some $\alpha \in \mathbb{Z}$, and is fairly trivial. Therefore, there exists some $u' \in G$ such that $u'g = gu' = 1$ for all $g \in G$, and thus G is a group.

Therefore, $\{1, \ldots, n-1\}$ is a group under multiplication modulo n if and only if n is prime. Since 5 is prime, the set $\{1, 2, 3, 4\}$ is a group under multiplication modulo 5.

Upon review prior to submitting, this appears to be a special case of the proof in Homework 2 that $U(n)$ is a group, although the method of proof appears to be different than what will be done for that problem.

Incase I got something horribly wrong, here's my original proof, which brute forces the solution for $n = 5$ using a Cayley Table.

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	1	1

From this table, it can also be seen that 1 is an identity element in G, so there exists an identity element in G. It can also be seen that every element has an inverse; 1 is it's own inverse since $1 \cdot 1 = 1 \mod 5$, but also $2 \cdot 3 = 1 \mod 5$, $3 \cdot 2 = 1 \mod 5$, and $4 \cdot 4 = 1 \mod 5$. So under multiplication modulo 5, the inverse of 2 is 3, the inverse of 3 is 2, and the inverse of 4 is 4, all of which are elements of G. Finally, we show associativity. We know that associativity holds in $\mathbb{Z}$, and $\{1, 2, 3, 4\} \subseteq \mathbb{Z}$. Thus, associativity holds for all elements of G, since all elements of G are also integers, which are known to be associative. Therefore, G is a group under the operation of multiplication modulo 5. □

Problem 5.

Solution.

- The set $\{1, 4, 7, 13\}$ is a group under multiplication modulo 15.
  - The set is closed under multiplication modulo 15:

$\cdot$	1	4	7	13
1	1	4	7	13
4	4	1	13	7
7	7	13	4	1
13	13	7	1	4

  - The set is associative by the same logic discussed in Problem 4: since $\{1, 4, 7, 13\} \subset \mathbb{Z}$, and since associativity holds in $\mathbb{Z}$, associativity holds for $\{1, 4, 7, 13\}$.
  - As can be seen in the above Cayley table, every element has some inverse. 1 and 4 are their own inverses, while 7 and 13 are inverses of each other.
  - As can be seen in the above Cayley table, 1 is an identity element in the set.

  All properties of a group are satisfied.

- The set of even integers $\{2n \mid n \in \mathbb{Z}\}$ is a group under addition. I have used the shorthand $2\mathbb{Z}$ to denote this set.

- The set is clearly closed. Let $a, b \in 2\mathbb{Z}$. By definition, there exist integers $m, n \in \mathbb{Z}$ such that $a = 2m$ and $b = 2n$. Thus, by the distributive property of multiplication over addition, which holds in $\mathbb{Z}$,
$$a + b = 2m + 2n = 2(m + n).$$
Since $m + n \in \mathbb{Z}$, then $2(m + n) \in 2\mathbb{Z}$, and thus $a + b \in 2\mathbb{Z}$.
- Associativity follows from the integers. Since $2\mathbb{Z} \subseteq \mathbb{Z}$, and since $\mathbb{Z}$ is associative over addition, $2\mathbb{Z}$ must also be associative.
- There exists an identity element $0 \in 2\mathbb{Z}$. From the properties of $\mathbb{Z}$, we know for any $a \in 2\mathbb{Z}$,
$$a + 0 = 0 + a = a.$$
Therefore, 0 is an identity element.
- For any $a \in 2\mathbb{Z}$, the number $-a \in 2\mathbb{Z}$ is the inverse of a. To prove they are inverses,
$$a + (-a) = (-a) + a = 0.$$
To prove $-a \in 2\mathbb{Z}$, let $n \in \mathbb{Z}$ such that $a = 2n$. It follows that $-a = -(2n) = 2(-n)$ since $\mathbb{Z}$ is commutative. Since $-n$ is an integer, $2(-n)$ must be an even integer, and thus $-a \in 2\mathbb{Z}$.

All the properties of a group are satisfied.

- $\mathbb{Z}$ under the operation $\star$ is not a group due to failiure to be associative. Let $a, b, c \in \mathbb{Z}$.
$$a \star (b \star c) = a - (b - c) = a - b + c.$$
$$(a \star b) \star c = (a - b) - c = a - b - c.$$
$$a - b - c \neq a - b + c.$$

□