Math 3130 - Assignment 1

Due January 24, 2024

(1) Complete the multiplication table for the symmetries $1, a, b, c$ of a (nonsquare) rectangle.

A multiplication is *commutative* if order of the arguments does not matter, that is, $xy = yx$ for all x and y.

Is the multiplication of symmetries of a rectangle commutative?

Solution:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Note: every row and column is a permutation of $1, a, b, c$ and $x^2 = 1$ for all x.

Since the table is symmetric on the diagonal, the multiplication is commutative.

(2) With pictures and words describe the set of symmetries of an equilateral triangle.

How many symmetries are there?

For each symmetry, give its inverse.

Is the multiplication of symmetries of an equilateral triangle commutative?

Solution: Let r be the rotation by $2pi/3$ around the center. Then $1, r, r^2$ are 3 rotational symmetries. Additionally there are 3 reflections a, b, c in the lines through the center and one corner of the triangle.

These are all 6 symmetries by the argument as in 3(b).

$1^{-1} = 1, r^{-1} = r^2, r^{-2} = r$ and each reflection is its own inverse.

Since e.g. $ra \neq ar$, the multiplication is not commutative.

(3) A *regular n-gon* is a plane figure that has n sides of equal length and n equal angles. E.g., for $n = 4$ a regular n-gon is just a square.

(a) Describe the symmetries of the regular n-gon ($n \geq 3$).

Hint: Consider the cases of n even and n odd separately.

(b) How many symmetries are there for a regular n-gon ($n \geq 3$)?

The group of symmetries of a regular n-gon is called the *dihedral group of order* $2n$ and denoted D_{2n} for short.

Attention: In [1] and some other books this is denoted D_n instead.

Solution: (a) There are n rotations around the origin by angles $k * 2pi/n$ for $k = 0, 1, 2, \dots, n$ (rotation by 0 is the identity). For n odd there are n reflections each at an axis through the origin and one corner (as well as through the midpoint of the opposite side) of the n-gon.

For n even, there are $n/2$ reflections each at an axis through the origin and one corner of the n-gon as well as $n/2$ reflections each an axis through the origin and a midpoint of one side.

(b) Label corners of the n-gon $1, \dots, n$ counterclockwise. A symmetry s can move 1 to one of n total corners. Since $s(2)$ is a neighbor of $s(1)$, we then have 2 options for it. By the choices of $s(1), s(2)$ all other images are fixed. So there are at most $2n$ symmetries. In (a) we found $2n$ symmetries. So $|D_{2n}| = 2n$.

(4) (a) In D_{2n}, describe geometrically why the composition of two rotations is a rotation.
(b) In D_{2n}, describe geometrically why the composition of two reflections is a rotation.
Hint: What happens with the positions of two neighboring corners after one reflection? After two?

Solution: (a) If r_α, r_β are rotations by angles α, β with the same center, then their composition $r_\alpha r_\beta = r_{\alpha+\beta}$ is a rotation by $\alpha + \beta$.

(b) Label corners of the n-gon $1, \dots, n$ counterclockwise. For any rotation r the images $r(1), \dots, r(n)$ will still be labelled counterclockwise (same orientation).

For any reflection s, the orientation of $s(1), s(2)$ changes. Composing two reflections then results again in the original orientation. Hence the composition of two reflections cannot be a reflection, but is a rotation.

(5) Let $n \in \mathbb{N}, a, a', b, b' \in \mathbb{Z}$ such that $a \equiv_n a', b \equiv_n b'$. Show
$$a + b \equiv_n a' + b'.$$

Solution: Assume $a - a' = qn$, $b - b' = rn$ for $q, r \in \mathbb{Z}$. Then
$$a + b - (a' + b') = a - a' + b - b' = qn + rn$$
is a multiple of n. So $a + b \equiv_n a' + b'$.

(6) (a) Show that $\{1, 2, 3\}$ under multiplication modulo 4 is not a group.
(b) Show that $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ is a group.

Solution: (a) E.g. $2 \cdot 2 = 0 \notin \{1, 2, 3\}$. So multiplication modulo 4 is not an operation on $\{1, 2, 3\}$.

(b) $\mathbb{Z}_5 \setminus \{0\}$ is closed under multiplication since 5 is prime.

Associativity is inherited from the multiplication on $\mathbb{Z}$.

1 is the identity.

Every element has a multiplicative inverse $1^{-1} = 1, 2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 4$.

(7) Let $n \geq 2$ and a be integers. Show that $ax \mod n = 1$ has a solution iff $\gcd(a, n) = 1$.

Solution: $\Rightarrow$ Assume $ax \mod n = 1$ has a solution $x \in \mathbb{Z}$. That means $ax - 1$ is a multiple of n, say $ax - 1 = ny$ for $y \in \mathbb{Z}$. So

$$ax - ny = 1$$

Since $\gcd(a, n)$ divides the lefthand side, it follows that $\gcd(a, n) = 1$.

$\Leftarrow$ Assume $\gcd(a, n) = 1$. By Bezout's identity there exist $x, y \in \mathbb{Z}$ such that

$$ax + ny = \gcd(a, n) = 1.$$

Then $ax \equiv_n 1$ as required.

References

[1] Joseph A. Gallian. Contemporary Abstract Algebra. Houghton Mifflin Company, sixth edition, 2006.