

Homework Assignment 2

Due: Friday, February 5

1. Let $m \in \mathbb{N}$ be a natural number. Recall that the *residue of an integer x modulo m* is the remainder r when applying the division algorithm (HW1 #8) to divide x by m . We say that integers x and y are *congruent modulo m* if they have the same residue modulo m .

- (a) Show that x and y have the same residue modulo m if and only if m divides $x - y$.

Proof. Let $x = q_1m + r_1$ and $y = q_2m + r_2$ so that $x - y = (q_1 - q_2)m + r_1 - r_2$. Since $-m < r_1 - r_2 < m$, we observe that m divides $x - y$ if and only if $r_1 - r_2 = 0$ as desired. \square

- (b) Show that congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. We use part (a) to assert that x is congruent to y modulo m precisely when m divides $x - y$. For reflexivity observe that m divides $x - x = 0$. For symmetry we see that if $x \equiv y \pmod{m}$ then $x - y = km$ so that $y - x = -km$ implying that $y \equiv x \pmod{m}$. Finally we establish transitivity. Suppose $x \equiv y \pmod{m}$ and $y \equiv z \pmod{m}$. Then $x - y = km$ and $y - z = lm$ so that:

$$x - z = x - y - (z - y) = km + lm = (k + l)m,$$

so that $x \equiv z \pmod{m}$. \square

- (c) Suppose $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$. Show that:

$$a + b \equiv a' + b' \pmod{m} \quad \text{and} \quad ab \equiv a'b' \pmod{m}.$$

Proof. Assume assume that $a = a' + km$ and $b = b' + lm$. Then

$$a + b = a' + km + b' + lm = a' + b' + (k + l)m \equiv a' + b' \pmod{m}.$$

and

$$ab = (a' + km)(b' + lm) = a'b' + km b' + a' lm + kmlm = a'b' + m(kb' + a'l + klm) \equiv a'b' \pmod{m}.$$

\square

2. (a) Let p be a prime number, and let $x, y \in \mathbb{Z}/p\mathbb{Z}$ be nonzero. Show that xy is also nonzero.

Proof. Choose representatives $a, b \in \mathbb{Z}$ for x and y respectively. We prove the contrapositive. If $xy = 0$ then $p|ab$ so that $p|a$ or $p|b$ by Euclid's formula. Therefore either $x = 0$ or $y = 0$. \square

- (b) On the other hand, let m be a composite number greater than 3. Show that one can always find two nonzero elements of $\mathbb{Z}/m\mathbb{Z}$ whose product is zero.

Proof. As m is composite $m = ab$ for $1 < a, b < m$. Then \bar{a}, \bar{b} are nonzero in $\mathbb{Z}/m\mathbb{Z}$ but their product $\bar{a}\bar{b} = \overline{ab} = \bar{m} = 0$. \square

3. Fix a natural number m .

(a) Let $x, y \in (\mathbb{Z}/m\mathbb{Z})^\times$. Show that $xy \in (\mathbb{Z}/m\mathbb{Z})^\times$.

Proof. By definition, the elements of $(\mathbb{Z}/m\mathbb{Z})^\times$ are those with multiplicative inverses (recall that we showed this to be equivalent to a representative being coprime with m using the extended Euclidean algorithm). Therefore we fix inverses x^{-1} and y^{-1} respectively for x and y respectively. But then $y^{-1}x^{-1}$ is a multiplicative inverse for xy , so that $xy \in (\mathbb{Z}/m\mathbb{Z})^\times$. \square

(b) Show that $(\mathbb{Z}/m\mathbb{Z})^\times$ is a group under multiplication modulo m .

Proof. By part (a) multiplication mod m is a binary operation. Associativity is inherited from multiplication in \mathbb{Z} . Indeed, let $\bar{x}, \bar{y}, \bar{z} \in (\mathbb{Z}/m\mathbb{Z})^\times$. Then:

$$(\bar{x}\bar{y})\bar{z} = \overline{(xy)z} = \overline{x(yz)} = \bar{x}(\bar{y}\bar{z}).$$

The identity element is $\bar{1}$, and by definition, every element of $(\mathbb{Z}/m\mathbb{Z})^\times$ has a multiplicative inverse. \square

(c) Compute the order of each element of $(\mathbb{Z}/7\mathbb{Z})^\times$

Proof. For each $a = 1, 2, \dots, 6$ we Compute powers of a by repeatedly multiplying by a and reducing mod 7. Count how many steps it take to get to 1.

$|1| = 1$.

Powers of 2 mod 7. $2, 4, 8 \equiv 1$. So $|2| = 3$.

Powers of 3 mod 7. $3, 9 \equiv 2, 6, 18 \equiv 4, 12 \equiv 5, 15 \equiv 1$. So $|3| = 6$

Powers of 4 mod 7. $4, 16 \equiv 2, 8 \equiv 1$. So $|4| = 3$.

Powers of 5 mod 7. $5, 25 \equiv 4, 20 \equiv 6, 30 \equiv 2, 10 \equiv 3, 15 \equiv 1$. So $|5| = 6$.

Powers of 6 mod 7. $6, 36 \equiv 1$. So $|6| = 2$. \square

4. Let $*$ denote multiplication modulo 15, and consider the set $\{3, 6, 9, 12\}$. Fill in the following multiplication table.

*	3	6	9	12
3	9	3	12	6
6	3	6	9	12
9	12	9	6	3
12	6	12	3	9

Use the table to prove that $(\{3, 6, 9, 12\}, *)$ is a group. What is the identity element?

Proof. Associativity follows from associativity of multiplication in \mathbb{Z} (just like in 3(b) above). The identity element here is 6. As 6 appears once in each column, every element has an inverse (it suffices to check columns as multiplication is commutative, or leveraging 7(a) below). \square

5. Let A be a nonempty set, and define $S_A := \{f : A \rightarrow A \mid f \text{ is bijective}\}$. Define a binary operation on S_A using composition of functions. Explicitly, for any $f, g \in S_A$ we define their product as follows: $f * g := f \circ g$. Show that S_A is a group. We will call this the *permutation group of A* .

Proof. First we must show that composition on S_A is a binary operation. We will show something slightly more general as it will come in handy in the future as well.

Lemma 1. *Let $f : A \rightarrow B$ and $g : B \rightarrow C$ be two bijective functions. Then the composition $g \circ f : A \rightarrow C$ is bijective as well.*

Proof. In HW1#4(c) we showed that a function is bijective if and only if it has an inverse, so we must show $g \circ f$ has an inverse. Let f^{-1} and g^{-1} be the inverses to f and g respectively (which we know exist because they are bijective). Then:

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ id_B \circ g^{-1} = g \circ g^{-1} = id_C,$$

and

$$(f^{-1} \circ g^{-1}) \circ g \circ f = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ id_B \circ f = f^{-1} \circ f = id_A.$$

Therefore $g \circ f$ has inverse $f^{-1} \circ g^{-1}$ and is therefore bijective. \square

Lemma 1 tells us that if $f, g \in S_A$ then $g \circ f \in S_A$ so that composition is in fact a binary operation on S_A .

To show S_A is a group we must now show that this operation (i) is associative, (ii) has an identity, and (iii) has inverses. Associativity is clear because composition of functions is associative. The identity function id_A is bijective, and for all $f \in S_A$ we have $id_A \circ f = f \circ id_A = f$, so the identity function serves as the identity element of the group. Finally, we showed HW1#4(c) that f is bijective if and only if it has an inverse f^{-1} , which naturally serves as the inverse element of f in S_A . \square

6. Let $(A, *)$ and (B, \cdot) be two groups. Define multiplication on the Cartesian product $A \times B$ via the following rule:

$$(a_1, b_1)(a_2, b_2) = (a_1 * a_2, b_1 \cdot b_2).$$

Show that this makes $A \times B$ into a group. We call this group the *direct product of A and B* .

Proof. We begin by checking associativity of the binary operation. This is inherited from the associativity of the operations on A and B :

$$((a_1, b_1)(a_2, b_2))(a_3, b_3) = ((a_1 * a_2) * a_3, (b_1 \cdot b_2) \cdot b_3) = (a_1 * (a_2 * a_3), b_1 \cdot (b_2 \cdot b_3)) = (a_1, b_1)((a_2, b_2)(a_3, b_3)).$$

Then one easily checks that $(1_A, 1_B)$ is an identity. Indeed

$$(1_A, 1_B)(a, b) = (1_A * a, 1_B \cdot b) = (a, b)$$

and the other side is identical. Finally, we observe that $(a, b)^{-1} = (a^{-1}, b^{-1})$. Indeed:

$$(a, b)(a^{-1}, b^{-1}) = (a * a^{-1}, b * b^{-1}) = (1_A, 1_B),$$

and the other side is identical. \square

7. Fix elements x, y of a group G .

- (a) Show that if $xy = e$ then $x^{-1} = y$ and $y^{-1} = x$.

Proof. Multiplying on the left of both sides by x^{-1} gives:

$$y = x^{-1}xy = x^{-1}e = x^{-1}.$$

Multiplying on the right of both sides by y^{-1} gives:

$$x = xy y^{-1} = ey^{-1} = y^{-1}.$$

□

- (b) Show that $(xy)^{-1} = y^{-1}x^{-1}$.

Proof. Observe that $(xy)(y^{-1}x^{-1}) = xey^{-1} = e$, so that leveraging part (a) gives the result. □

- (c) Show that $(x^n)^{-1} = x^{-n}$.

Proof. We freely use that $x^a x^b = x^{a+b}$ for any $a, b \in \mathbb{Z}$. This follows essentially by definition, leveraging associativity, but I encourage you to check it if you are skeptical. We then proceed by induction, noticing that the base case $n = 1$ is trivial. We then observe that by induction:

$$x^n x^{-n} = x^{n-1} x x^{-1} x^{-(n-1)} = x^{n-1} x^{-(n-1)} = e.$$

Then by part (a) we are done. □

8. Fix an element x of a group G and suppose $|x| = n$.

- (a) Show that x^{-1} is a nonnegative power of x .

Proof. Notice that $xx^{n-1} = x^n = e$. Therefore $x^{-1} = x^{n-1}$ by 7(a). Since $n \geq 1$, we are done. □

- (b) Show that the all of $1, x, x^2, \dots, x^{n-1}$ are distinct. Conclude that $|x| \leq |G|$. (We will later show that if $|G|$ is finite then $|x|$ divides $|G|$.)

Proof. Suppose otherwise, so that $x^i = x^j$, and assume without loss of generality that $j \geq i$. Multiplying both sides by x^{-i} and leveraging 7(c) gives $x^{j-i} = e$. Since $j - i < n$ we must have $j - i = 0$, otherwise this would contradict that n is the minimal positive power of x which is the identity. This implies $j = i$ to begin with.

Notice that we have produced n distinct elements of G , so that $n \leq |G|$. □

- (c) Show that $x^i = x^j$ if and only if $i \equiv j \pmod n$.

Proof. We freely use that if $x^{ab} = (x^a)^b$. If b is positive, this is clear, as

$$x^{ab} = x^{\overbrace{a + a + \cdots + a}^{b\text{-times}}} = \underbrace{x^a x^a \cdots x^a}_{b\text{-times}} = (x^a)^b.$$

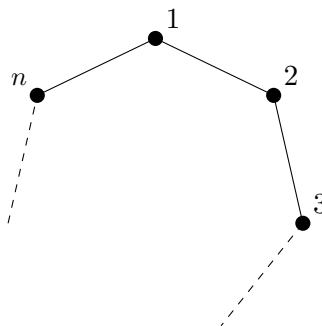
I encourage you to work out the b is negative case if you are skeptical. If $i \equiv j \pmod n$, then $i - j = kn$, so that $x^{i-j} = x^{kn} = (x^n)^k = e$. Therefore multiplying both sides by x^j gives $x^i = x^j$.

Conversely, if $x^i = x^j$ then $x^{i-j} = e$. Apply the division algorithm to divide $i - j$ by n , so $i - j = kn + r$ for $0 \leq r < n$. Then:

$$e = x^{i-j} = x^{kn+r} = x^{kn} x^r = e x^r = x^r.$$

Since $|x| = n$, and $r < n$, this implies $r = 0$. Thus $n|(i - j)$ as desired. \square

9. In class we developed the theory of the group D_{12} of rigid symmetries of the regular hexagon. In fact, everything we developed should go through almost exactly the same way for D_{2n} : the rigid symmetries of regular n -sided polygon, pictured below:



- (a) Explain why D_{2n} is a group under composition of symmetries.

Proof. The definition of symmetry is rather qualitative in nature, so an explanation in plain language here suffices. Essentially by definition, the composition of rigid symmetries is again a rigid symmetry. Also: 'doing nothing' is a rigid symmetry. By definition, a symmetry is reversible implying that inverses exist. Associativity is most easily seen by observing that a symmetry is a type of function from the n -gon to itself. As composition of functions is associative, we win. \square

- (b) Show that there are exactly $2n$ rigid symmetries of the regular n -gon.

Proof. Fix a symmetry α . We say $\alpha(i) = j$ if the vertex labelled i goes to the point j under the symmetry. Notice that a symmetry can take the vertex labelled 1, to any of the vertices $1, 2, \dots, n$. This is n choices. So let's make such a choice say $\alpha(1) = i$. Now, we are not allowed to break the n -gon, so that in particular the vertex labeled 2 must end up next to the vertex labeled 1. In particular, $\alpha(2) = i - 1$ or $\alpha(2) = i + 1$ (where we replace the number with the residue mod n where necessary, i.e., if $i = n$ or $i = 1$.) This is 2 choices. Now observe that once these two choices are made, the rest of the symmetry is fixed by rigidity. Indeed, if $\alpha(1) = i$ and $\alpha(2) = i + 1$, then $\alpha(3) = i + 2$

and $\alpha(4) = i + 3$ and so on. On the other hand, if $\alpha(1) = i$ and $\alpha(2) = i - 1$, then $\alpha(3) = i - 2$ and so on. In each case, we can freely choose from n choices for vertex 1, and then 2 choices for vertex 2, before the symmetry becomes completely determined. This gives precisely $2n$ symmetries. \square

- (c) Let r be the rotation by $2\pi/n$ in the clockwise direction, and s be the reflection along the vertical line going through the vertex labelled '1'. Compute the elements of D_{2n} in terms of r and s in the following steps:

- i. Compute the order of r and s (justifying your answers).

Proof. Notice that r^n is rotation by $\frac{2\pi}{n}n = 2\pi$ so it is the identity function. Suppose $0 < i < n$. Then r^i takes 1 to the $i + 1$ 'st position so that r^i is not the identity. Thus $|r| = n$. For s notice that reflection undoes itself, so that s^2 is the identity. But, for example, $s(2) = n$, so that s is not the identity. Therefore $|s| = 2$. \square

- ii. Let $i_1, i_2 \in \{0, 1\}$ and $j_1, j_2 \in \{0, 1, \dots, n-1\}$. Show that:

$$s^{i_1}r^{j_1} = s^{i_2}r^{j_2} \text{ if and only if } i_1 = i_2 \text{ and } j_1 = j_2.$$

(Hint: You could first show $s \neq r^i$ for any i using geometry. The rest of the cases should follow from this and part (i) by using cancellation and 8(b).)

Proof. We follow the hint and first show that $s \neq r^i$ for any i . To see this, we first use 8(c) to reduce i modulo n without changing r^i , so that we may freely assume that $i = 0, 1, \dots, n-1$. Suppose $s = r^i$. Notice that $s(1) = 1$. Since $r^i(1) = i + 1$, we deduce that $i = 0$ as well. But this means r^i is the identity, and s is not the identity, which is a contradiction.

From this we may immediately deduce that $sr^i \neq r^j$ for any i, j . If not $s = r^{j-i}$, contradicting the previous paragraph.

Lastly, assume $sr^i = sr^j$. Then by cancellation $r^i = r^j$. By 8(c) we see that $i \equiv j \pmod n$ so that $i = j$ since they are both between 0 and $n-1$. \square

- iii. Conclude that $D_{2n} = \{s^i r^j \mid i = 0, 1 \text{ and } j = 0, 1, \dots, n-1\}$. In particular, r and s generate D_{2n} .

Proof. We saw in (c)(ii) that each $s^i r^j$ in the given set is distinct, thus enumerating $2n$ distinct elements of D_{2n} . But by part (b), there are exactly $2n$ elements of D_{2n} , so this must be all of them. \square

- (d) Show that $rs = sr^{-1}$. Deduce inductively from this that $r^n s = sr^{-n}$ for all n .

Proof. As in part (b), it suffices to show that rs and sr^{-1} agree on 1 and 2. One can observe geometrically that $r(i) = i + 1$ (appropriately reduced mod n), and that s fixes 1 and swaps n and 2. Then we observe:

$$\begin{aligned} r(s(1)) &= r(1) = 2 & s(r^{-1}(1)) &= s(n) = 2 \\ r(s(2)) &= r(n) = 1 & s(r^{-1}(2)) &= s(1) = 1, \end{aligned}$$

This serves as the base case for our induction. For the general case we may assume that $r^{n-1}s = sr^{1-n}$. Then we compute:

$$r^n s = r r^{n-1} s = r s r^{1-n} = s r^{-1} r^{1-n} = s r^{-n},$$

as desired. □

We now completely understand the algebraic structure of D_{2n} . In particular, we know what every element looks like (in terms of r and s) by (c), and we know how to multiply any two elements using the relation in part (d). We summarize this by saying that D_{2n} has the following presentation:

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

- (e) Use this presentation to give an algebraic proof that every element which is not a power of r has order 2.

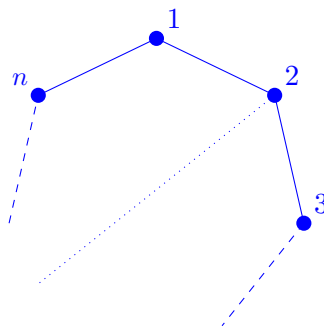
Proof. By (c)(iii), the elements which are not powers of r are all sr^i for some i , for the same reason they are nonzero. Then we may compute:

$$(sr^i)^2 = (sr^i)(sr^i) = s(r^i s)r^i = s(sr^{-i})(r^i) = (s^2)(r^{-i}r^i) = 1.$$

□

- (f) Bonus: Can you give a geometric interpretation of part (e)?

Proof. For each i one can consider the line bisecting vertex i , pictured below for $i = 2$.



Reflecting about this line gives a symmetry of order 2. This gives n more symmetries, each which clearly have order two, and which correspond precisely to the sr^j . For this reason, the sr^j are called the *reflections* in the dihedral group. □