

# Homework 1 Solutions

## Chapter 0: 4, 11, 13, 31, 46, 47, 48

4. Find all integers  $s, t$  such that  $1 = 7s + 11t$ .

There is a nice method called the *Extended Euclidean Algorithm* that hands you a pair  $s$  and  $t$ . [Here are some notes on this topic.](#)

In general, notice that if  $0 < a < b$ , then

$$\gcd(a, b) = \gcd(b \bmod a, a)$$

From the Euclidean Division Algorithm, we know that  $0 \leq b \bmod a < a$ , so we set  $d_0 = b > d_1 = a > d_2 = b \bmod a > d_3 = d_1 \bmod d_2 > \dots > d_k > d_{k-1} \bmod d_k = 0$ . When this happens we have  $\gcd(a, b) = \gcd(d_k, d_{k-1}) = d_k > 0$  since  $d_k \mid d_{k-1}$ . This is a very quick method to find the GCD of two numbers. Now, if we look a bit harder, this method actually provides a pair  $(s_i, t_i)$  so that  $as_i + bt_i = d_i$  for all  $i$  and thus  $d = \gcd(a, b) = d_k = as_k + bt_k$ . We start with  $a \cdot 0 + b \cdot 1 = b = d_0$  and  $a \cdot 1 + b \cdot 0 = a = d_1$  so  $(s_0, t_0) = (0, 1)$  and  $(s_1, t_1) = (1, 0)$ . Now suppose  $d_i = as_i + bt_i$  for  $i = 0, \dots, j$  and so  $d_{j-1} = d_j q_j + d_{j+1}$  where  $q_j = \lfloor \frac{d_{j-1}}{d_j} \rfloor$  and so

$$d_{j+1} = d_{j-1} - d_j q_j = (as_{j-1} + bt_{j-1}) - q_j(as_j + bt_j) = a(s_{j-1} - q_j s_j) + b(t_{j-1} - q_j t_j)$$

So we have  $(s_{j+1}, t_{j+1}) = (s_{j-1}, t_{j-1}) - q_j(s_j, t_j)$  where  $q_j = \lfloor \frac{as_{j-1} + bt_{j-1}}{as_j + bt_j} \rfloor$ . This is a simple recursion. When  $d_{j+1} = 0$  we stop and know that  $d_j = \gcd(a, b) = as_j + bt_j$ .

So with 11 and 7 we have:  $d_0 = 11 > d_1 = 7$ ,  $(s_0, t_0) = (0, 1)$ , and  $(s_1, t_1) = (1, 0)$ . Now  $11 = 7(1) + 4$  so  $d_2 = 4$ ,  $q_1 = 1$ , and  $(s_2, t_2) = (0, 1) - (1)(1, 0) = (-1, 1)$ . Notice  $d_2 = 4 = (-1)(7) + (1)(11)$ . Now  $7 = 4(1) + 3$ , so  $d_3 = 3$ ,  $q_2 = 1$ , and  $(s_3, t_3) = (1, 0) - (1)(-1, 1) = (2, -1)$ . Again, notice  $d_3 = 3 = (2)(7) + (-1)(11) = 3$ . Continuing,  $4 = (3)(1) + 1$  so  $d_4 = 1$ ,  $q_3 = 1$ , and  $(s_4, t_4) = (-1, 1) - (1)(2, -1) = (-3, 2)$ . We have now  $1 = (-3)(7) + (2)(11)$ . Clearly, this is what we were looking for. So  $s = -3$  and  $t = 2$  works.

Taking one more step, we get  $3 = 1(3) + 0$  and so  $d_5 = 0$ ,  $q_4 = 3$ , and  $(s_5, t_5) = (2, -1) - (3)(-3, 2) = (11, -7)$ , and so  $(11)(7) + (-7)(11) = 0$ , but then  $(11k)(7) + (-7k)(11) = 0$  and clearly

$$1 = (11k - 3)(7) + (2 - 7k)(11)$$

for any  $k \in \mathbb{Z}$ . So any pair  $(s, t)$  of the form  $(11k - 3, 2 - 7k)$  works. Is that all pairs  $(s, k)$ ?

**11.** Let  $n > 1$  be a fixed integer. Show that if  $a = a' \bmod n$  and  $b = b' \bmod n$ , then  $a+b = (a'+b') \bmod n$  and  $ab = a'b' \bmod n$ . Note that from this we get that  $a^k = (a')^k \bmod n$ , but it is not true that  $c^a = c^{a'} \bmod n$ . So, you do have to be cautious.

It is clear that  $a = a' \pmod n \iff n \mid a - a'$  so we have  $n \mid a - a'$  and  $n \mid b - b'$  and we want to see that  $n \mid (a + b) - (a' + b')$  and  $n \mid ab - a'b'$ . The first is trivial since  $(a + b) - (a' + b') = (a - a') + (b - b')$ . For the second  $ab - a'b' = (a - a')(b + b') - ab' + a'b = (a - a')(b + b') - ab' + ab - ab + a'b = (a - a')(b + b') + a(b - b') - b(a - a')$  and since  $n$  divides each summand we have that  $n$  divides  $ab - a'b'$ .

**13.** Let  $a$  and  $n$  be positive integers and  $d = \gcd(a, n)$ . Show that there is an integer  $x$  such that  $ax \pmod n = 1$  iff  $d = 1$ .

If  $x$  exists, then we have  $ax = bn + 1$ , so  $ax - bn = 1$ . But now if  $d \mid a, n$ , then  $d \mid 1$ , so  $d = 1$ . Conversely, if  $\gcd(a, n) = 1$ , then we know there are integers  $x$  and  $y$  such that  $ax + ny = 1$  and so  $ax = -ny + 1$  so  $ax \pmod n = 1$ .

**19.** Let  $a, b, s, t$  be integers and  $a \pmod{st} = b \pmod{st}$ , show that  $a \pmod s = b \pmod s$  and  $a \pmod t = b \pmod t$ . What conditions on  $s$  and  $t$  are required for the converse to hold?

$$a = b \pmod{st} \iff st \mid a - b \implies (s \mid a - b \wedge t \mid a - b)$$

For the converse, we need  $(s \mid a - b \wedge t \mid a - b) \implies st \mid a - b$ . If  $s$  and  $t$  are relatively prime, then this is true. On the other hand, if  $\gcd(s, t) = d$ , then let  $m = \text{lcm}(s, t)$  and  $a - b = m$ , then  $s \mid a - b$ ,  $t \mid a - b$ , but  $st \nmid a - b$ . Since  $st = |\mathbb{Z}_{st}| = |\mathbb{Z}_s \times \mathbb{Z}_t| = |\mathbb{Z}_s| |\mathbb{Z}_t| = st$ . We know that the map is surjective as well.

Note that this shows that the map  $f : \mathbb{Z}_{st} \rightarrow \mathbb{Z}_s \times \mathbb{Z}_t$  given by  $n \pmod{st} \mapsto (n \pmod s, n \pmod t)$  is injective if  $\gcd(s, t) = 1$ .

**31.** Use the Generalized Euclidean Lemma to establish the uniqueness of the Fundamental Theorem of Arithmetic.

Suppose uniqueness fails. Let  $n$  be the least positive failure. So  $n = p_1 \cdots p_k = q_1 \cdots q_l$  do primes  $p_i$  and  $q_j$ . Since  $p_1$  is prime, we know  $p_1 \mid q_j$  for some  $j$ . By rearranging, we may assume  $j = 1$ . This means that  $p_1 = q_1$  and thus we have  $m = p_2 \cdots p_k = q_2 \cdots q_l$ . But  $0 < m < n$ , and now  $m$  has a non-unique factorization into primes. This is a contradiction, so no such  $n$  could exist in the first place.

**46.** Suppose that an ISBN-10 has a smudged entry where the question mark appears in the number 0-716?-2841-9. Determine the missing digit.

You have to look at (45) where the ISBN-10 is defined as  $a_1, \dots, a_9$  can be any number 0-9 with  $a_{10}$  can be any of 0-10 with 'X' used when the number is 10 and  $a_{10}$  is a check digit and is chosen so that

$$\text{ISBN-10} = \langle (a_1, a_2, \dots, a_{10}), (10, 9, 8, \dots, 1) \rangle \pmod{11} = \sum_{i=1}^{10} (11-i)a_i \pmod{11} = 0$$

So here we have

$$(10)(0) + (9)(7) + (8)(1) + (7)(6) + (6)(?) + (5)(2) + (4)(8) + (3)(4) + (2)(1) + 9 \pmod{11} = 0$$

This reduces to  $178 + 6? = 0 \pmod{11}$  which is the same as  $6? = -178 \pmod{11}$ . Now  $178 \pmod{11} = 2$  and so  $-178 \pmod{11} = 11 - 2 = 9$ , thus we are solving  $6? = 9 \pmod{11}$  which is the same as  $2? = 3 \pmod{11}$ . So we are looking for  $?$  so that  $11 \mid 2? - 3$  and we see 7 works,  $(2)(7) - 3 = 11$ , so  $? = 7$ . So we need

47. Suppose three consecutive digits  $abc$  of an ISBN-10 are scrambled as  $bca$ . Which such errors will go undetected?

Here what we know is that  $N + (m)(a) + (m - 1)b + (m - 2)c + s = 0 \pmod{11}$  or that  $N + (m)(a) + (m - 1)b + (m - 2)c = -s \pmod{11} = 11 - s$ . Since  $-k = n - k \pmod{n}$ . Now what we compute from the scrambled code is  $N + (m)b + (m - 1)c + (m - 2)a - (N + (m)(a) + (m - 1)b + (m - 2)c) = b - 2a + c$ . If  $N + (m)b + (m - 1)c + (m - 2)a = s \pmod{11}$ , then we will not detect an error. Otherwise, we know there is some error, but we don't know how to fix it. So if  $b - 2a + c = 0 \pmod{11}$  we will **not** detect an error.

48. Here we define a relation  $s \sim t$  on  $\mathbb{R}$  by  $s \sim t \iff s - t \in \mathbb{Z}$ . We need to show that this is an equivalence relation. There are three things to show

**Symmetry**  $s \sim t \iff s - t \in \mathbb{Z} \iff t - s \in \mathbb{Z} \iff t \sim s$ .

**Transitivity** Assume  $s \sim t \wedge t \sim r$ , so  $s - t, t - r \in \mathbb{Z}$  and from this  $s - r = (s - t) - (t - r) \in \mathbb{Z}$ , and so we have  $s \sim r$ .

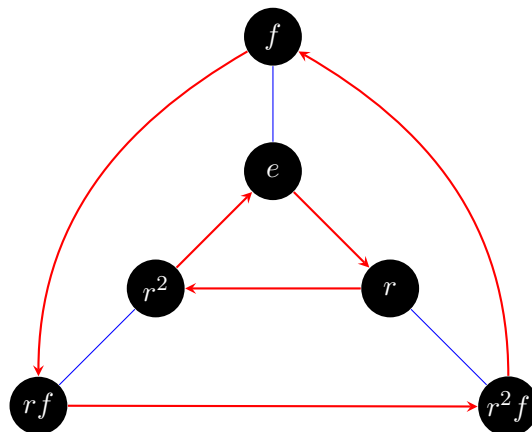
**Reflexive**  $s - s \in \mathbb{Z}$ , so  $s \sim s$ .

## Chapter 1: 2, 5 - 8, 15, 18, 22, 24

2. Give the multiplication table for  $D_3$ . Here  $f$  is a horizontal flip, and  $r$  is  $120^\circ$  clockwise rotation. The multiplication is row  $\times$  column, and we are rewriting everything as one of this set  $\{e, r, r^2, f, rf, r^2f\}$ ,

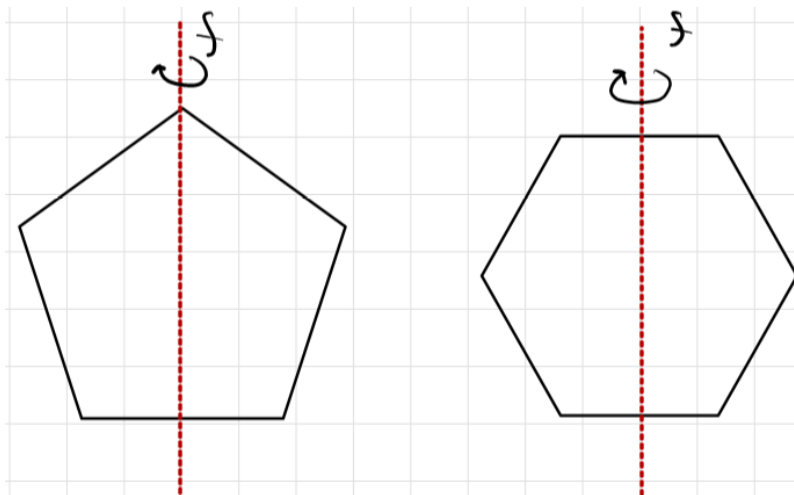
$\cdot$	$e$	$r$	$r^2$	$f$	$rf$	$r^2f$
$e$	$e$	$r$	$r^2$	$f$	$rf$	$r^2f$
$r$	$r$	$r^2$	$e$	$rf$	$r^2f$	$f$
$r^2$	$r^2$	$e$	$r$	$r^2f$	$f$	$rf$
$f$	$f$	$r^2f$	$rf$	$e$	$r^2$	$r$
$rf$	$rf$	$f$	$r^2f$	$r$	$e$	$r^2$
$r^2f$	$r^2f$	$rf$	$f$	$r^2$	$r$	$e$

To complete this table, it is useful to use the following Cayley Diagram for  $D_3$ .



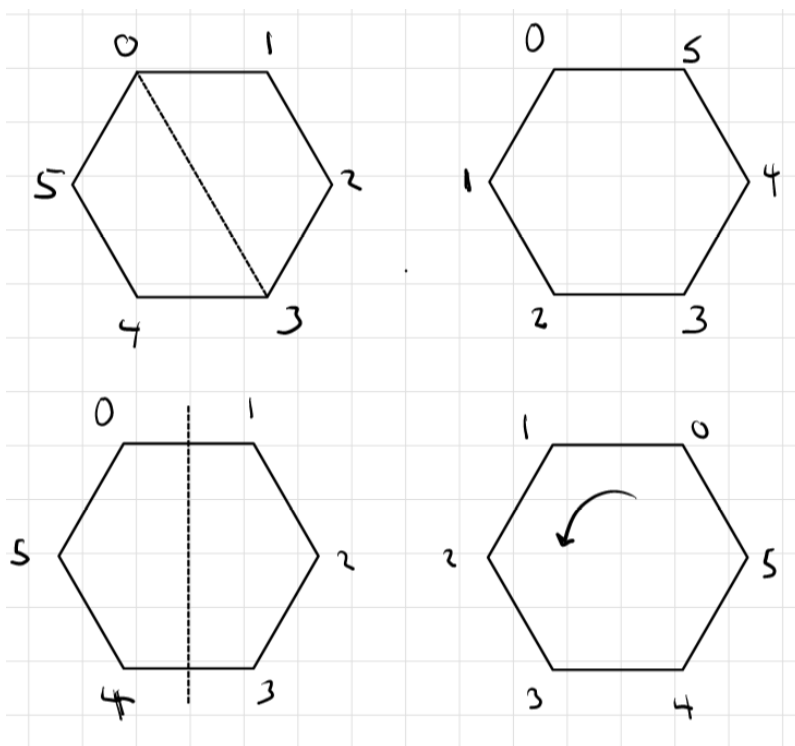
This is not abelian, for example,  $rf = fr^2 \neq fr = r^2f$ .

5. For  $n$  odd or even, there are the  $n$  rotations of  $k \cdot \frac{2\pi}{n} = r^k$  for  $k = 0, \dots, n-1$ .  $r^0 = e$ . Then there are the **flips** or **reflections**. For  $n$  odd, reflect about the line passing through a vertex and the midpoint of the side opposite that vertex. If  $n$  is even, then the reflections are through the midpoints of opposite sides as well as through opposite sides.

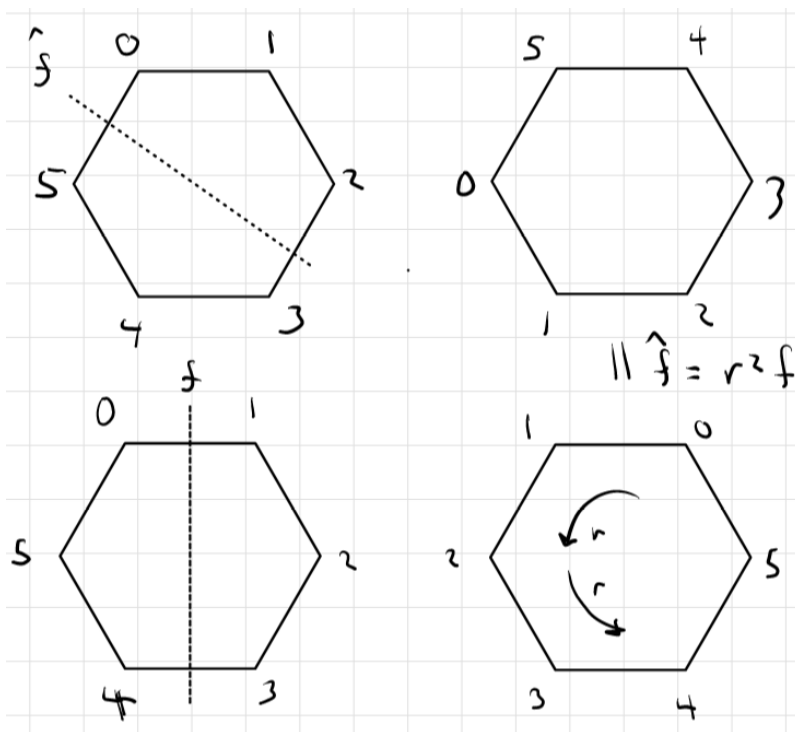


Pick any one of the reflections and call it  $f$ , then all other reflections can be achieved using just  $r$  and  $f$ .

The following shows how a reflection across the line adjoining opposite vertices can be written as a combination of a rotation and horizontal flip.



The following shows how a flip across a line adjoining two opposite sides can be achieved with a horizontal flip and rotations.

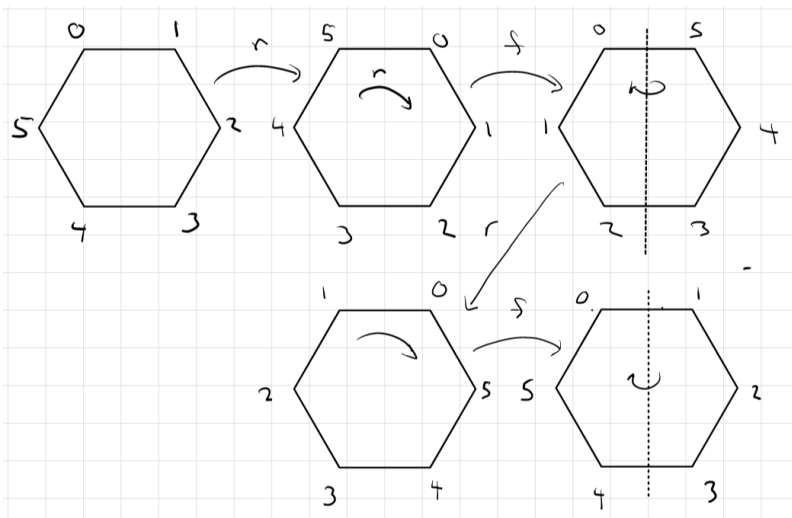


Thus all you need to describe all of the actions is  $r^k$  ( $k < n$ ) and  $f$ . It is also clear that  $r^n = e$ ,

$f^2 = e$ , and  $rfrf = e$ . From these three **relations**, we can deduce all other relations. For example,  $rf = fr^{-1}$  and since  $r^{-1} = r^{n-1}$ ,  $rf = fr^{n-1}$  as can be seen by

$$rf = (rf)^{-1} = f^{-1}r^{-1} = fr^{-1}.$$

The following illustrates  $rfrf = e$ .



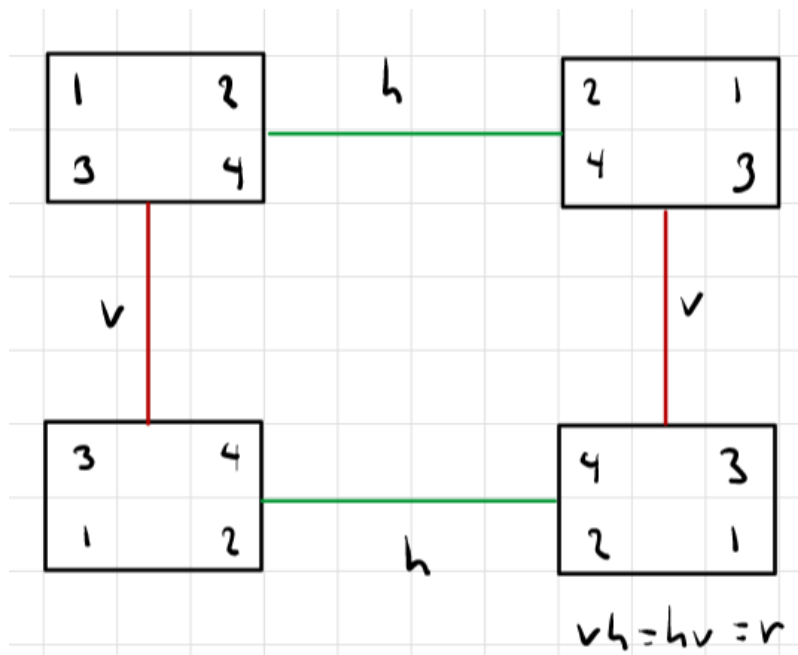
6. It is clear that all actions that preserve positive orientation (labels increasing clockwise) are just rotations. A flip changes the orientation, so two flips restore orientation and hence must just be a rotation.

7. There is really nothing to say here; if we rotate and then rotate again, the end result is just a rotation.

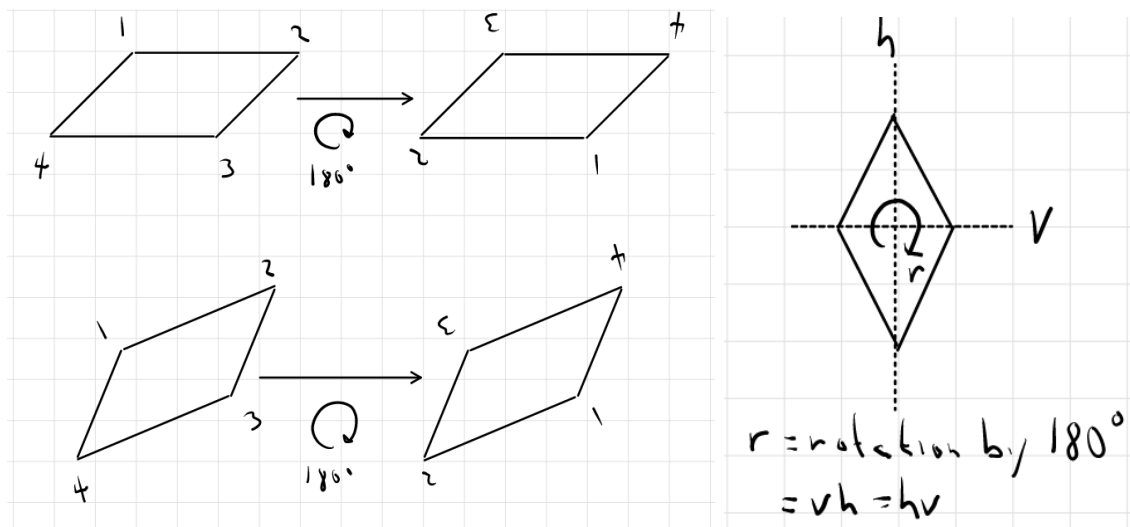
8. This is like 6. A flip corresponds to changing orientation, so a flip then a rotation changes the orientation once and hence is just a flip.

15. There is  $h$  (horizontal reflection),  $v$  (vertical reflection),  $r$  (rotation by  $\pi$ ), and of course  $e$  (do nothing).

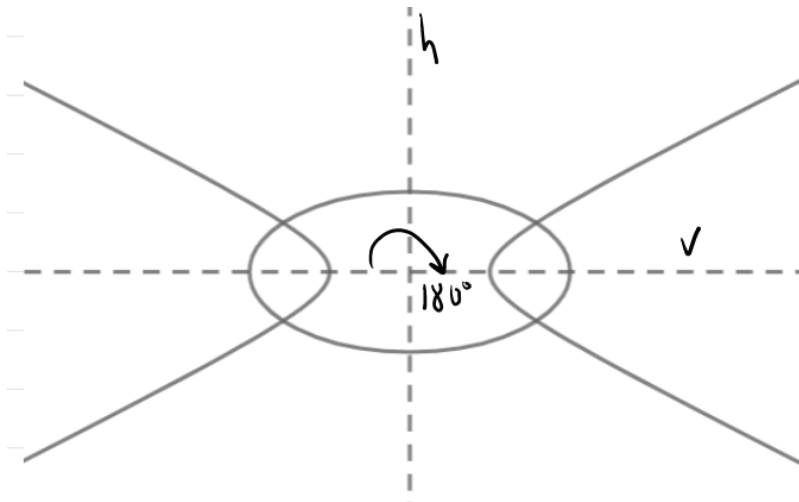
$\cdot$	$e$	$r$	$v$	$h$
$e$	$e$	$r$	$v$	$h$
$r$	$r$	$e$	$h$	$v$
$v$	$v$	$h$	$e$	$r$
$h$	$h$	$v$	$r$	$e$



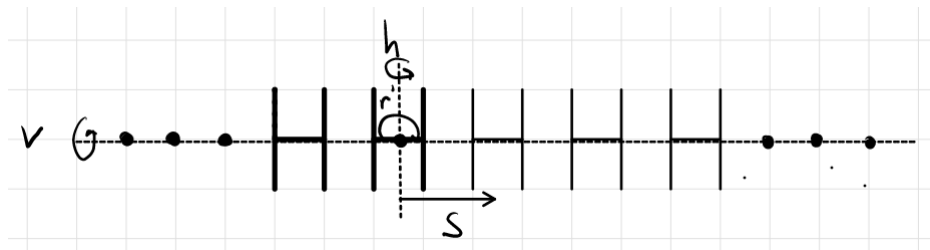
16. A non-rhombus parallelogram has only  $e$  (do nothing) and  $r$  (rotate  $180^\circ$ ) as actions. The non-rectangular rhombus has the same groups as the non-square rectangle.



17. Both these shapes have exactly the same group as the rectangle.



**18.** Here, we can shift 1 to the right; call this action  $s$ . Shifting  $n$  to the right is  $s^n$  and shifting  $n$  to the left is  $s^{-n}$ . We can vertically reflect about the horizontal axis ( $v$ ) and horizontally reflect about the vertical lines through the center of an  $H$  ( $h$ ). Also, a  $180^\circ$  rotation about the point  $p$  ( $r$ ) and  $p'$  ( $r'$ ). Clearly,  $r = hv = vh$ .



This is an infinite group.

**22.** Here I have used  $C_n$  for the order  $n$  cyclic group, the book uses  $Z_n$  (which is probably better).





24. If  $X^2$  is a rotation, regardless of what  $X$  is so  $X^2 = F$  has no solutions. If  $X = R^m F$ , then  $(R^m F)^3 = R^m F R^m F R^m F =$

Chapter 2: 4, 7, 18, 20, 21, 26, 29, 30, 41 - 44

4.

a. Closed.

$+_{16}$	0	4	8	12
0	0	4	8	12
4	4	8	12	0
8	8	12	0	4
12	12	0	4	8

b. Not closed.  $4 + 12 \equiv 1 \pmod{15}$

c. Closed.

$\cdot_{15}$	1	4	7	13
1	1	4	7	13
4	4	1	13	7
7	7	13	4	1
13	13	7	1	4

d. Not closed.  $4 \cdot 5 \equiv 2 \pmod{9}$ .

6. In each case perform the indicated operation.

(a.) In  $\mathbb{C}^*$ ,  $(7 + 5i)(-3 + 2i)$ .

$$\begin{aligned}
(7 + 5i)(-3 + 2i) &= (((7)(-3) + (5i)(2i)) + ((7)(2) + (5)(-3))i \\
&= (-21 - 10) + (14 - 15)i = -31 - i
\end{aligned}$$

(b.) In  $\text{GL}(2, \mathbb{Z}_{13})$ ,  $\det \begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix}$

$$\det \begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix} \equiv_{13} ((7)(5) - (1)(4)) \equiv_{13} (-1 - 4) \equiv_{13} 8$$

(c.) In  $\text{GL}(2, \mathbb{R})$ ,  $\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1}$ .

$$\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1} = \frac{1}{(6)(2) - (8)(3)} \begin{bmatrix} 2 & -3 \\ -8 & 6 \end{bmatrix} = -\frac{1}{12} \begin{bmatrix} 2 & -3 \\ -8 & 6 \end{bmatrix}$$

(d.) In  $\text{GL}(2, \mathbb{Z}_7)$ ,  $\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}^{-1}$ .

$$\begin{aligned}
\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix}^{-1} &\equiv_7 ((2)(3) - (1)(1))^{-1} \begin{bmatrix} 3 & -1 \\ -1 & 2 \end{bmatrix} \\
&\equiv_7 5^{-1} \begin{bmatrix} 3 & -1 \\ -1 & 2 \end{bmatrix} \\
&\equiv_7 3 \begin{bmatrix} 3 & -1 \\ -1 & 2 \end{bmatrix} \equiv_7 \begin{bmatrix} 9 & -3 \\ -3 & 6 \end{bmatrix} \\
&\equiv_7 \begin{bmatrix} 2 & 4 \\ 4 & 6 \end{bmatrix}
\end{aligned}$$

7. I am going to discuss closure separately.  $\det(AB) = \det(A)\det(B)$  is true over any ring. We can verify this directly for  $2 \times 2$ . Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ and } B = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

$$\begin{aligned}
&\det \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \right) \\
&= \det \begin{bmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{bmatrix} \\
&= (a\alpha + b\gamma)(c\beta + d\delta) - (c\alpha + d\gamma)(a\beta + b\delta) \\
&= a\alpha c\beta + a\alpha d\delta + b\gamma c\beta + b\gamma d\delta - c\alpha a\beta - c\alpha b\delta - c\alpha a\beta - c\alpha b\delta \\
&= a\alpha c\beta + a\alpha d\delta + b\gamma c\beta + b\gamma d\delta - a\alpha c\delta - b\alpha c\delta - a\alpha c\beta - b\alpha d\delta \\
&= (a\alpha d\delta + b\gamma c\beta - a\alpha c\delta - b\alpha d\delta) + (a\alpha c\beta - a\alpha c\beta) + (b\gamma d\delta - b\alpha d\delta) \\
&= a\alpha d\delta + b\gamma c\beta - a\alpha c\delta - b\alpha d\delta
\end{aligned}$$

and

$$\begin{aligned}\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} &= (ad - bc)(\alpha\delta - \beta\gamma) \\ &= ad\alpha\delta - ad\beta\gamma - bc\alpha\delta + bc\beta\gamma\end{aligned}$$

So it is true that mod 4:

$$\det(AB) \equiv \det(A)\det(B) \pmod{4}$$

Now the problem is that if  $\det(A) \equiv 2 \pmod{4}$  and  $\det(B) \equiv 2 \pmod{4}$  so  $A, B \in G_1$ , but then  $\det(AB) \equiv 0 \pmod{4}$ . So  $G_1$  is not closed. As a specific example

$$A = B = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \text{ so } AB = \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}$$

$G_2$  and  $G_3$  is closed since  $\det(A)\det(B) = 0 \iff \det(A) = 0$  or  $\det(B) = 0$  in  $\mathbb{Z}$  and in  $\mathbb{Q}^+$ .

Clearly,  $G_2$  does not have inverses, for example  $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \in G_2$  would have inverse  $\begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix} \notin G_2$ .

In terms of being a group,  $I$  needs to be included so in  $G_3$  let's assume that positive should be non-negative rationals. The inverse of a  $2 \times 2$  is given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

This shows that  $G_3$  is closed under inverses. So  $G_3$  is a group.

**18.**  $(ab)^3 = ababab$  and  $((ab^{-2}c)^2)^{-1} = (ab^{-2}cab^{-2}c)^{-1} = c^{-1}b^2a^{-1}c^{-1}b^2a^{-1}$

**20.** Here is the table for  $D_4$

MULTIPLICATION TABLE IN  $D_4$

	$R_0$	$R_{180}$	$R_{90}$	$R_{270}$	$H$	$V$	$D$	$D'$
$R_0$	$R_0$	$R_{180}$	$R_{90}$	$R_{270}$	$H$	$V$	$D$	$D'$
$R_{180}$	$R_{180}$	$R_0$	$R_{270}$	$R_{90}$	$V$	$H$	$D'$	$D$
$R_{90}$	$R_{90}$	$R_{270}$	$R_{180}$	$R_0$	$D'$	$D$	$H$	$V$
$R_{270}$	$R_{270}$	$R_{90}$	$R_0$	$R_{180}$	$D$	$D'$	$V$	$H$
$H$	$H$	$V$	$D$	$D'$	$R_0$	$R_{180}$	$R_{90}$	$R_{270}$
$V$	$V$	$H$	$D'$	$D$	$R_{180}$	$R_0$	$R_{270}$	$R_{90}$
$D$	$D$	$D'$	$V$	$H$	$R_{270}$	$R_{90}$	$R_0$	$R_{180}$
$D'$	$D'$	$D$	$H$	$V$	$R_{90}$	$R_{270}$	$R_{180}$	$R_0$

$K = \{R_0, R_{180}\}$  (the diagonal elements) and  $L = \{R_0, R_{180}, H, V, D, D'\}$

**21.** We did most of the work for this in (7).  $\det(AB) = \det(A)\det(B) = 1$  so the set is closed under product.  $\det(A)\det(A^{-1}) = 1$  so  $\det(A^{-1}) = \frac{1}{\det(A)} = 1$  so the set is closed under inverse, and  $I$  is in the set.

**26.** You put on your socks, then your shoes, but you take off your shoes, then your socks.

For the second item, notice that if  $a^{-1}b^{-1} = (ab)^{-1}$  holds, then

$$ab = ((ab)^{-1})^{-1} = (a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1} = ba$$

so  $a$  and  $b$  must commute. So, for example, using  $a = r$  and  $b = r^2$  in  $D_3$  would suffice for an example.

For the third thing, we want to see that  $(ab)^{-2} \neq b^{-2}a^{-2}$ . Now here,  $a$  and  $b$  must not commute. Again, in  $D_3$ , take  $a = r$  and  $b = f$ , then

$$(rf)^{-2} = ((rf)^2)^{-1} = (rfrf)^{-1} = e^{-1} = e \neq f^{-2}r^{-2} = (f^2)^{-1}(r^2)^{-1} = r$$

**29.** This one is easy to see, but formally would require induction:

$$\begin{aligned} (a^{-1}ba)^n &= (a^{-1}ba)(a^{-1}ba) \cdots (a^{-1}ba)(a^{-1}ba) \\ &= a^{-1}b(aa^{-1})b(aa^{-1})b \cdots (aa^{-1})ba = a^{-1}bebebe \cdots eba = a^{-1}b^n a \end{aligned}$$

**30.**  $(a_1a_2 \cdots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1} \cdots a_2^{-1}a_1^{-1}$  (again induction is required to formalize this)

**41.** We know  $rfrf = e$  for any rotation  $r$ . This can be written,  $rf = f^{-1}r^{-1} = fr^{-1}$ , since  $f^2 = e$  and hence  $f^{-1} = f$ . But this is clear. If we rotate and then flip, then to undo this action, flip, and then rotate backward.

This shows that  $rfr = f$  and hence that  $r^kfr^k = f$  which is what we wanted.

**42.** This one also follows from the above, since  $e = rfrf$ , so  $e = (rfrf)^{-1} = fr^{-1}fr^{-1}$ . But this holds for any rotation  $r$  so it holds for  $r^{-1}$  and we have  $frrf = e$  and hence  $fr^kfr^k = e$  (again as  $r$  can be taken as  $r^k$ ). So  $fr^kf = r^{-k}$ .

If  $D_n$  were abelian, then we would have  $frr = f^2r = r = r^{-1}$

**43.**

$$R^6FRFR^{-3}FRF = R^6(R^{-1})R^{-3}R^{-1} = R$$

and

$$FR^4FR^5FR^2 = R^{-4}R^5FR^2 = RFRR = FR$$

**44.**  $FR_\alpha FR_\beta = R_{-\alpha}R_\beta = R_{\beta-\alpha}$  and  $R_\alpha FR_\beta F = R_\alpha R_{-\beta} = R_{\alpha-\beta}$ . So these are inverses of each other.

## Chapter 3: 4, 5, 12, 14, 17, 31, 45, 53, 62, 64, 71, 74, 82, 87, 89

**4.** If  $(a^{-1})^n = e$ , then  $(a^n)^{-1} = e$  so  $a^n = e$ , thus  $|a^{-1}| \leq |a|$ . Similarly,  $|a| \leq |a^{-1}|$  so the orders are the same.

**5.**  $\gcd(m, n) = 1$  so there are integers  $x$  and  $y$  so that  $xn + ym = 1$  and thus  $a^1 = a^{xn+ym} = (a^n)^x (a^m)^y = (a^n)^x = (a^x)^n$ .

**12.** The members of  $D_4$  are  $r^i$  and  $r^i f$  for  $i = 0, 1, 2, 3$ . So  $K = D_4^2$  consists of  $r^{2i}$  and  $r^i f r^i f = e$  (since  $r^i f$  is a reflection). But then Thus  $K = \{e, r^2\}$ , this is a subgroup, isomorphic to  $\mathbb{Z}_2$ .

In  $D_3$ , we have  $e, r, r^2, f, rf, r^2 f$ . The cubes of these are  $e, f, r f r f r f = f^2 r f = r f$  ( $r^2 f r^2 f r^2 f = f^2 r^2 f = r^2 f$ ). Now  $r^2 f r f = r r f r f = r f^2 = r$ , so  $K = D_3^3$  is not a group.

Consider  $D_6^2, D_6^2$  will have  $r^{2i}$  and as  $r^k f r^k f = e$ . No reflection can be a square, so  $D_6^2 = \langle r^2 \rangle$  is a subgroup. In fact, it is clear that  $D_n^2 = \langle r^2 \rangle$  is always a subgroup.

What about  $D_6^3$ ? Clearly,  $D_n^3$  contains all reflections. So, if it contains a single rotation, then it can't be a subgroup unless it is the entire group, in other words,  $r = r^{3m}$  must obtain for some  $m$ , so  $3m = 1 \pmod n$ . This will hold iff  $\gcd(3, n) = 1$ . so  $D_6^3$  is not a subgroup as  $\gcd(3, 6) = 3$ .

$D_5^3$  would be the entire group,  $D_5$ . Etc.

**14.**  $D_4$  has three subgroups of order 4, namely,  $\langle r \rangle = \{e, r, r^2, r^3\}$  and  $\langle h, v \rangle = \{e, h, v, r^2\}$ , and  $\langle d, d' \rangle = \{e, d, d', r^2\}$ . To help see this, notice,  $dd' = d'd = hv = vh = r^2$ ,  $hr^2 = r^2 h = v$ ,  $vr^2 = d^2 v = h$ , and  $d'r^2 = d = r^2 d' = d$ , and  $dr^2 = r^2 d = d'$ .

**17.** If  $a^n = e$ , then  $(xax^{-1})^n = xa^n x^{-1} = xx^{-1} = e$  and if  $(xax^{-1})^n = xa^n x^{-1} = e$ , then  $a^n = x^{-1} e x = e$ . So clearly,  $|xax^{-1}| \leq |a| \leq |xax^{-1}|$ .

**31.** If  $H < D_n$  and  $|H|$  is odd. Suppose  $g \in H$  is a reflection and let  $K = \{e, g\} < H$ . For  $h \in H$  let  $hK = \{h, hg\}$ , then for any  $h, h' \in H$ , either  $hK = h'K$  or  $hK \cap h'K = \emptyset$ . This is because if  $h \in h'K$ , then either  $h = h'$  or  $h = h'g$  so that  $hK = \{h, hg\} = \{h'g, h'gg\} = \{h'g, h'\} = h'K$ . So we have partitioned  $H$  into a collection of  $N$  disjoint two element sets, but then  $|H| = 2N$ .

Here is a second argument. Let  $r^i$  be such that  $0 < i < n$  is least with  $r^i \in H$ . For any other  $j$  such that  $r^j \in H$  we have  $j = ki + l$  and since  $(r^i)^{-k} \in H$  we have  $r^l \in H$ , but since  $l < i$  we must have  $l = 0$ , do  $j = ki$  and thus  $\langle r \rangle \cap H = \langle r^i \rangle$ . Let  $h \in H$  be any reflection, then let's see that  $H = \langle r^i \rangle h$ . Suppose  $h' \in H$  is also a reflection, then  $h'h = r^{ik}$  since this is a rotation in  $H$ . But then  $h' = r^{ik} h$  as desired. Moreover, the map  $r^{ik} \mapsto r^{ik} h$  is one-one so  $H = \langle r^i \rangle \cup \langle r^i \rangle h$  and so  $|H| = 2|r^i|$ .

**45.** It is easy to see that if  $H_i < H$  for  $i \in I$  (any index set), then  $H' = \bigcap_{i \in I} H_i < H$ . Thus

$$\langle S \rangle = \bigcap \{K \mid K < H \text{ and } S \subset K\}$$

is the smallest subgroup of  $H$  containing  $S$ . It is clear that  $s_1^{m_1} s_2^{m_2} \cdots s_k^{m_k} \in \langle S \rangle$  for  $s_i \in S$  and  $m_i \in \mathbb{Z}$ .  $L = \{s_1^{m_1} s_2^{m_2} \cdots s_k^{m_k} \mid s_i \in S \text{ and } m_i \in \mathbb{Z}\}$  is a subgroup, thus  $L = \langle S \rangle$ .

**53.** Check that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n+1 \\ 0 & 1 \end{bmatrix}$$

so  $A$  has infinite order in  $\text{SL}(2, \mathbb{R})$  and order  $p$  in  $\text{SL}(2, \mathbb{Z}_p)$ .

**62.** If  $2\theta = r\pi$  where  $r$  is irrational, then  $R_\theta^n = R_{nr\pi}$  and the question is is there any  $n$  and  $k$  so that  $nr\pi = 2k\pi$ . The answer is no, since then  $r = 2k/n$ . So  $\theta = \sqrt{2}\pi$  would work. So  $F$  and  $F'$  can intersect at an angle of  $\theta = \sqrt{2}\pi$ .

64.

a.  $U(3) = \{1, 2\}$ ,  $U(4) = \{1, 3\}$ ,  $U(12) = \{1, 5, 7, 11\}$ .

b.  $U(5) = \{1, 2, 3, 4\}$ ,  $U(7) = \{1, 2, 3, 4, 5, 6\}$ ,

$U(35) = \{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34\}$ .

c.  $U(4) = \{1, 3\}$ ,  $U(5) = \{1, 2, 3, 4\}$ ,  $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ .

d.  $U(4) = \{1, 2\}$ ,  $U(10) = \{1, 3, 7, 9\}$ ,  $U(40) = \{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39\}$ .

A reasonable guess here is that  $|U(n \cdot m)| = |U(m)| \cdot |U(n)|$  if  $\gcd(m, n) = 1$ .

71.  $xHx^{-1}$  is a group since  $(xh_1x^{-1})(xh_2x^{-1}) = x(h_1h_2)x^{-1}$  and  $(xh_1x^{-1})^{-1} = xh_1^{-1}x^{-1}$ .

If  $H = \langle a \rangle$ , then  $xHx^{-1} = \langle xax^{-1} \rangle$ . (See above Ch 2 problem 29.)

If  $H$  is abelian, then  $(xax^{-1})(xbx^{-1}) = x(ab)x^{-1} = x(ba)x^{-1} = (xbx^{-1})(xax^{-1})$ .

74.  $H = \{A \in \text{GL}(2, \mathbb{R}) \mid \det(A) = 2^n \text{ for some } n \in \mathbb{Z}\}$ . Show that  $H$  is a subgroup of  $\text{GL}(2, \mathbb{R})$ .

This is trivial from  $\det(AB) = \det(A)\det(B)$ . There is nothing special about being a power of 2 here.

82. In  $D_3$  consider  $K = \langle f \rangle$  and  $H = \langle rf \rangle$ . Then  $HK = \{e, f, rf, r\}$ , which is not a group.

87. Let  $H < G$ , then  $HZ(G) = \{hz \mid h \in H \text{ and } z \in Z(G)\}$ . Show that  $HZ(G) < G$ .

- $1 \in HZ(G)$
- $h_1z_1, h_2z_2 \in HZ(G)$ , then  $(h_1z_1)(h_2z_2) = h_1(z_1h_2)z_2 = h_1(h_2z_1)z_2 = (h_1h_2)(z_1z_2) \in HZ(G)$ .
- $(hz)^{-1} = z^{-1}h^{-1} = h^{-1}z^{-1} \in HZ(G)$ .

89. Let  $H < (\mathbb{Q}, +)$  and  $H \neq \{0\}$ . Let  $q \in H$ , then  $2\mathbb{Z}q < \mathbb{Z}q \leq H$ . Here  $\mathbb{Z}q = \{nq \mid n \in \mathbb{Z}\} = \langle q \rangle_H$  and  $2\mathbb{Z}q = \langle q + q \rangle$ .