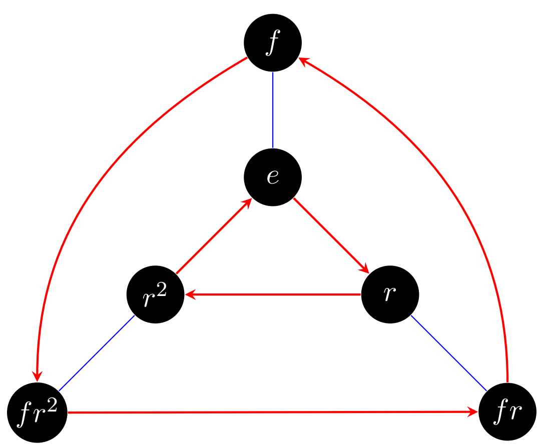
Homework 1 Solutions

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

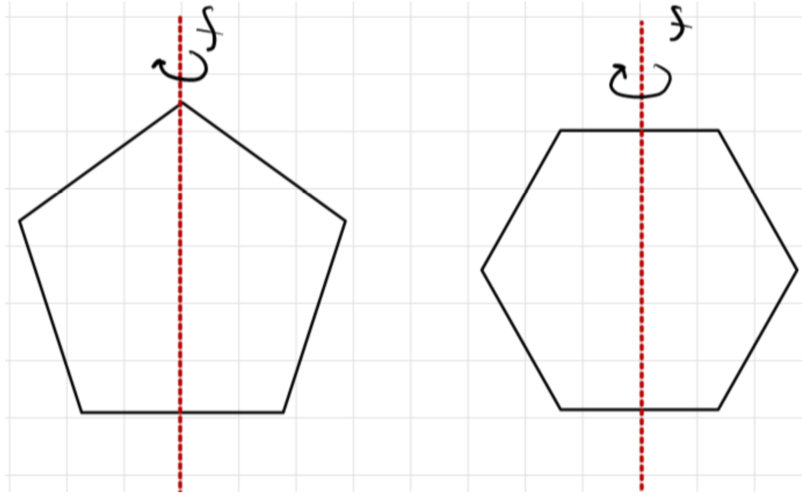
2. Give the multiplication table for D_3.

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

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

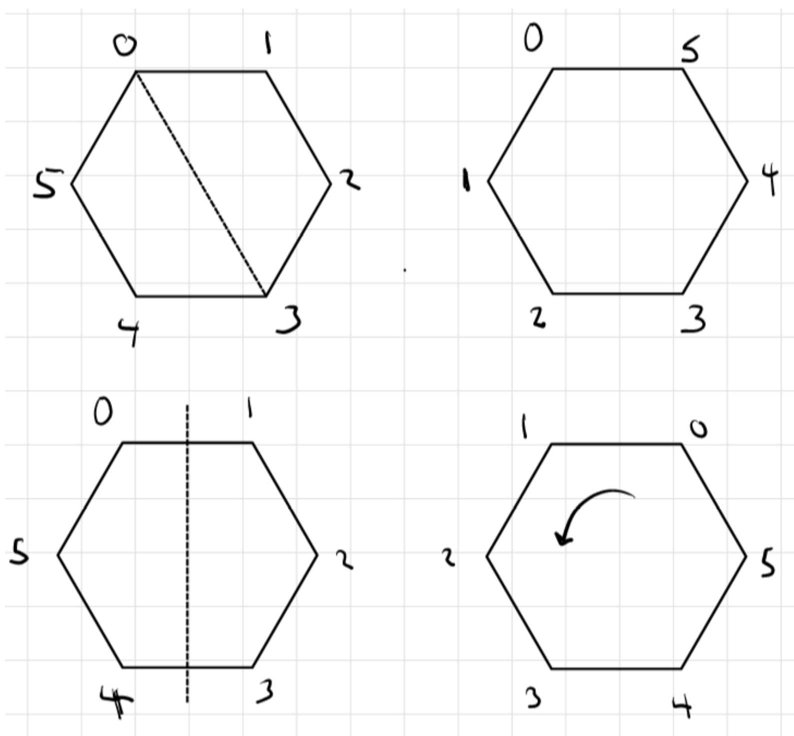


5. For n odd or even, there are the n rotations of $k \cdot \frac{2\pi}{n} = r^k$ for $k = 0, \dots, n-1$. $r^0 = e$. Then there are the **flips** or **reflections**. For n odd, reflect about the line passing through a vertex and the midpoint of the side opposite that vertex. If n is even, then the reflections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

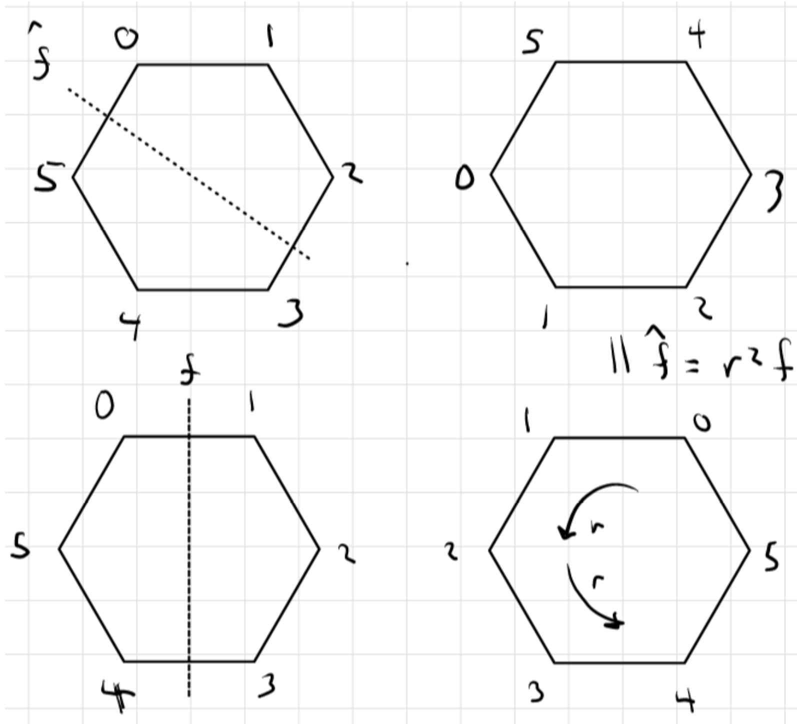


Pick any one of the reflections and call it f, then all other reflections can be achieved using just r and f.

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



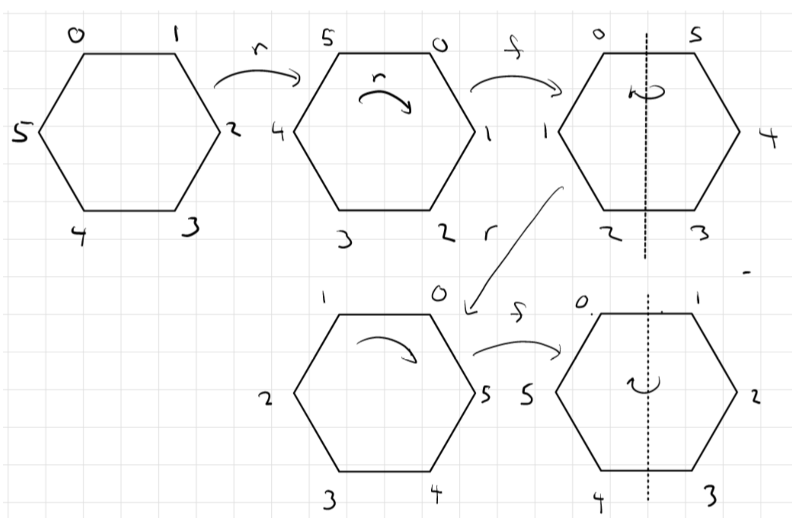
The following shows how a flip across a line adjoining two opposite sides can be achieved with a horizontal flip and rotations.



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 $rfrf = e$.



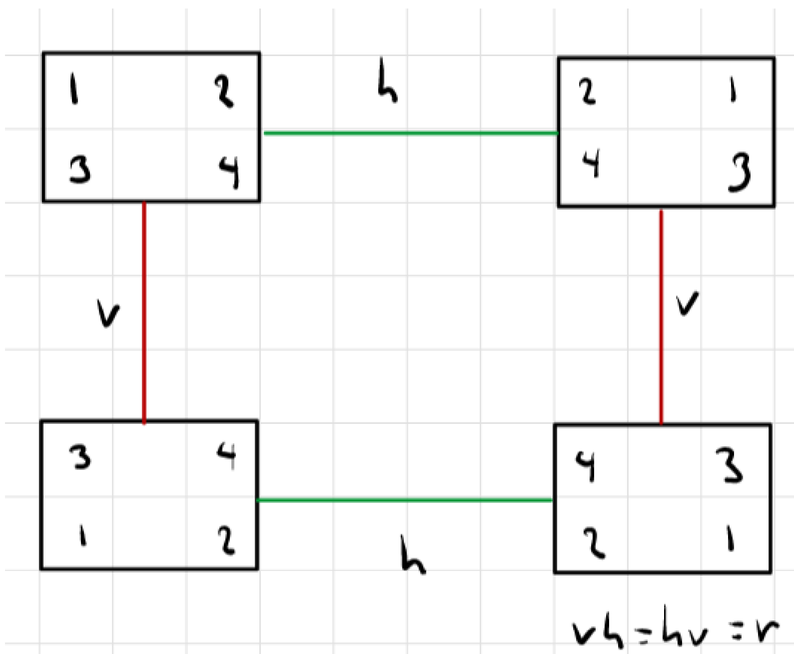
6. It is clear that all actions that preserve positive orientation (labels increasing clockwise) are just rotations. A flip changes the orientation, so two flips restore orientation and hence must just be a rotation.

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

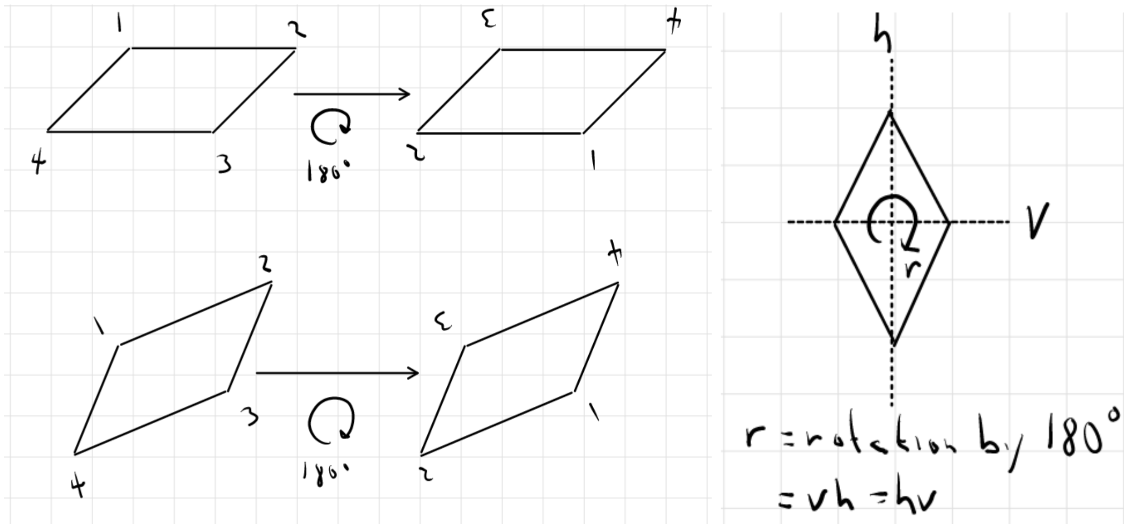
8. This is like 6. A flip corresponds to changing orientation, so a flip then a rotation changes the orientation once and hence is just a flip.

15. There is h (horizotal reflection), v (vertical reflection), r (rotation by π), and of course e (do nothing).

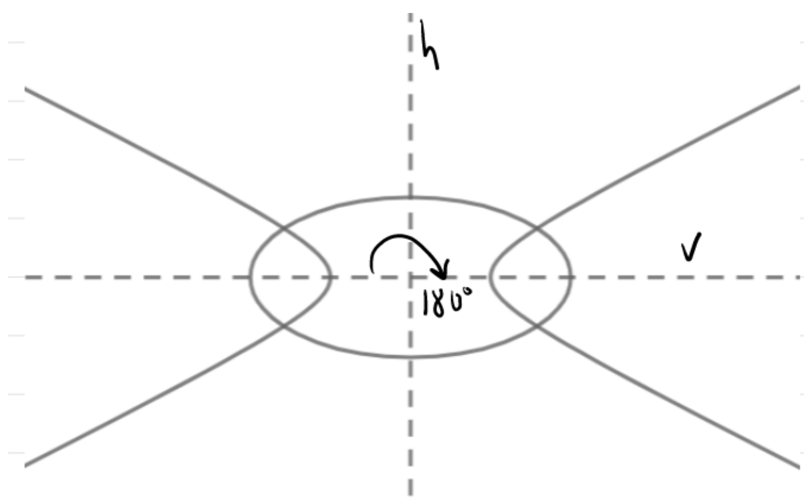
$\cdot$	e	r	v	h
e	e	r	v	h
r	r	e	h	v
v	v	h	e	r
h	h	v	r	e



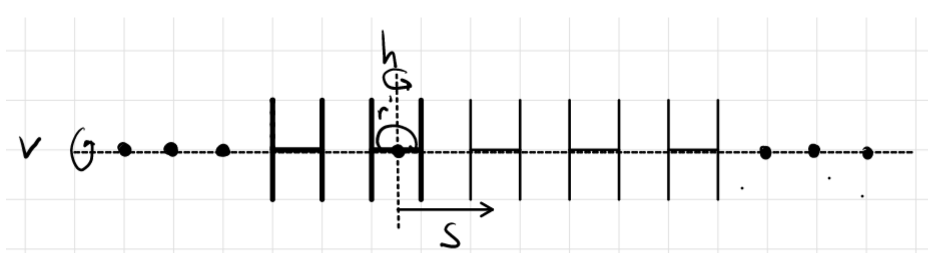
16. A non-rhombus parallelogram has only e (do nothing) and r (rotate 180°) as actions. The non-rectangular rhombus has the same groups as the non-square rectangle.



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

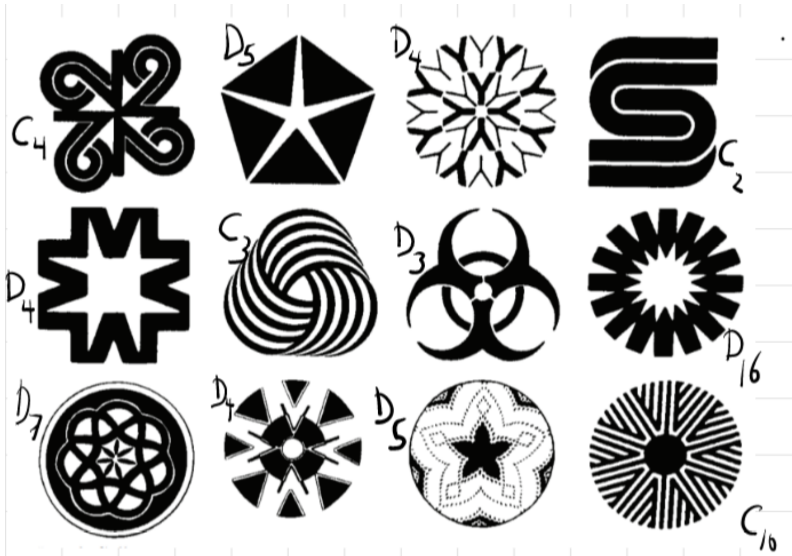


18. Here, we can shift 1 to the right; call this action s. Shifting n to the right is s^n and shifting n to the left is s^{-n}. We can vertically reflect about the horizontal axis (v) and horizontally reflect about the vertical lines through the center of an H (h). Also, a 180° rotation about the point 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. $4 + 12 \equiv 1 \bmod 15$

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. $4 \cdot 5 \equiv 2 \bmod 9$.

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 2×2.

$$\begin{aligned}
\det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} A & B \\ C & D \end{bmatrix}\right)& \\
&= \det\begin{bmatrix} aA + bC & aB + bD \\ cA + dC & cB + dD \end{bmatrix} \\
&= (aA + bC)(cB + dD) - (cA + dC)(aB + bD) \\
&= aAcB + aAdD + bCcB + bCdD - cAaB - cAbD - cAaB - cAbD \\
&= acAB + adAD + bcBC + bdCD - acAD - bcAD - acAB - bdCD \\
&= (adAD + bcBC - adBC - bcAD) + (acAB - acAB) + (bdCD - bdCD) \\
&= adAD + bcBC - adBC - bcAD
\end{aligned}$$

and

$$\begin{aligned}
\det\begin{bmatrix} a & b \\ c & d \end{bmatrix}\det\begin{bmatrix} A & B \\ C & D \end{bmatrix} &= (ad - bc)(AD - BC) \\
&= adAD - adBC - bcAD + bcBC
\end{aligned}$$

So it is true that mod 4:

$$\det(AB) \equiv \det(A)\det(B) \bmod 4$$

Now the problem is that $\det(A) \equiv 2 \bmod 4$ and $\det(B) \equiv 2 \bmod 4$ so $A, B \in G_1$, but then $\det(AB) \equiv 0 \bmod 4$. 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 $\left[\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right] \in G_2$ would have inverse $\left[\begin{smallmatrix} 1/2 & 0 \\ 0 & 1/2 \end{smallmatrix}\right] \notin G_2$.

In terms of being a group, I needs to be included so in G_3 let's assume that we mean non-negative rationals instead of positive rationals. The inverse of a 2×2 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 not closed under inverse since

$$\begin{bmatrix} 1 & 4 \\ 2 & 1 \end{bmatrix}^{-1} = \frac{1}{1 - 8}\begin{bmatrix} 1 & -4 \\ -2 & 1 \end{bmatrix} = \begin{bmatrix} -1/7 & 4/7 \\ 2/7 & -1/7 \end{bmatrix} \notin G_3$$

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:

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

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 $r^k fr^k = f$ 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 $frfr = e$ 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 $frf = f^2r = r = r^{-1}$

43.

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

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 $|a^{-1}| \le |a|$. Similarly, $|a| \le |a^{-1}|$ 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^if for $i = 0,1,2,3$. So K consists of r^{2i} and $r^ifr^if = e$ (since r^if is a reflection). 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^r, f. The cubes of these are e,f, $rfrfrf = f^2rf = rf$ $(r^2fr^2fr^2f = f^2r^2f = r^2f$. Now $r^2frf = rrfrf = rf^2 = r$, so not a group.

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, $dd' = d'd = hv = vh = r^2$, $hr^2 = r^2h = v$, $vr^2 = d^2v = h$, and $d'r^2 = d = r^2d' = d$, and $dr^2 = r^2d = d'$.

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

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 $|H| = 2N$.

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 $\mathrm{SL}(2,\mathbb{R})$ and order p in $\mathrm{SL}(2,\mathbb{Z}_p)$.

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 $(xhx^{-1})^{-1} = xh^{-1}x^{-1}$.

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

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

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

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 $H\,Z(G) < G$.

- $1 \in HZ(G)$
- $h_1z_1, h_2z_2 \in HZ(G)$, 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 $2\mathbb{Z}q = \langle q + q \rangle$.