CHAPTER 1

Introduction to Groups

1. Three rotations: 0°, 120°, 240°, and three reflections across lines from vertices to midpoints of opposite sides.
2. Let $R = R_{120}$, $R^2 = R_{240}$, F be a reflection across a vertical axis, $F' = RF$, and $F'' = R^2F$

	R_0	R	R^2	F	F'	F''
R_0	R_0	R	R^2	F	F'	F''
R	R	R^2	R_0	F'	F''	F
R^2	R^2	R_0	R	F''	F	F'
F	F	F''	F'	R_0	R^2	R
F'	F'	F	F''	R	R_0	R^2
F''	F''	F'	F	R^2	R	R_0

3. **a.** V **b.** R_{270} **c.** R_0 **d.** $R_0, R_{180}, H, V, D, D'$ **e.** none
4. Five rotations: 0°, 72°, 144°, 216°, 288°, and five reflections across lines from vertices to midpoints of opposite sides.
5. D_n has n rotations of the form $k(360°/n)$, where $k = 0, \ldots, n-1$. In addition, D_n has n reflections. When n is odd, the axes of reflection are the lines from the vertices to the midpoints of the opposite sides. When n is even, half of the axes of reflection are obtained by joining opposite vertices; the other half, by joining midpoints of opposite sides.
6. A nonidentity rotation leaves only one point fixed – the center of rotation. A reflection leaves the axis of reflection fixed. A reflection followed by a different reflection would leave only one point fixed (the intersection of the two axes of reflection), so it must be a rotation.
7. A rotation followed by a rotation either fixes every point (and so is the identity) or fixes only the center of rotation. However, a reflection fixes a line.
8. In either case, the set of points fixed is some axis of reflection.
9. Observe that $1 \cdot 1 = 1$; $1(-1) = -1$; $(-1)1 = -1$; $(-1)(-1) = 1$. These relationships also hold when 1 is replaced by a "rotation" and -1 is replaced by a "reflection."
10. Reflection.

11. Thinking geometrically and observing that even powers of elements of a dihedral group do not change orentation, we note that each of a, b and c appears an even number of times in the expression. So, there is no change in orentation. Thus, the expression is a rotation. Alternatively, as in Exercise 9, we associate each of a, b and c with 1 if they are rotations and -1 if they are reflections and we observe that in the product $a^2b^4ac^5a^3c$ the terms involving a represent six 1s or six -1s, the term b^4 represents four 1s or four -1s, and the terms involving c represent six 1s or six -1s. Thus the product of all the 1s and -1s is 1. So the expression is a rotation.
12. n is even.
13. In D_4, $HD = DV$ but $H \neq V$.
14. D_n is not commutative.
15. R_0, R_{180}, H, V
16. Rotations of $0°$ and $180°$; Rotations of $0°$ and $180°$ and reflections about the diagonals.
17. R_0, R_{180}, H, V
18. Let the distance from a point on one H to the corresponding point on an adjacent H be one unit. Then, a translations of any number of units to the right or left are symmetries; a reflection across the horizontal axis through the middle of the H's is a symmetry; and a reflection across any vertical axis midway between two H's or bisecting any H is a symmetry. All other symmetries are compositions of finitely many of those already described. The group is non-Abelian.
19. In each case the group is D_6.
20. D_{28}
21. First observe that $X^2 \neq R_0$. Since R_0 and R_{180} are the only elements in D_4 that are squares we have $X^2 = R_{180}$. Solving $X^2Y = R_{90}$ for Y gives $Y = R_{270}$.
22. $X^2 = F$ has no solutions; the only solution to $X^3 = F$ is F.
23. The n rotations of D_n are $R_0, R_{360/n}, R^2_{360/n}, \ldots, R^{n-1}_{360/n}$. Suppose that $n = 2k$ for some positive integer k. Then $R^k_{360/n} = R_{360k/2k} = R_{180}$. Conversely, if $R^k_{360/n} = R_{180}$ then $360k/n = 180$ and therefore $2k = n$.
24. Z_4, D_5, D_4, Z_2
D_4, Z_3, D_3, D_{16}
D_7, D_4, D_5, Z_{10}

CHAPTER 2

Groups

1. **c, d**
2. **c, d**
3. none
4. **a, c**
5. 7; 13; $n-1$; $\frac{1}{3-2i} = \frac{1}{3-2i}\frac{3+2i}{3+2i} = \frac{3}{13} + \frac{2}{13}i$
6. **a.** $-31-i$ **b.** 5 **c.** $\dfrac{1}{12}\begin{bmatrix} 2 & -3 \\ -8 & 6 \end{bmatrix}$ **d.** $\begin{bmatrix} 2 & 4 \\ 4 & 6 \end{bmatrix}$.
7. Let $A = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$. Then $A \in G_1$ and det $A = 2$ but det $A^2 = 0$. So G_1 is not closed under multiplication. Also $A \in G_2$ but $A^{-1} = \begin{bmatrix} 1/2 & 0 \\ 0 & 1 \end{bmatrix}$ is not in G_2. G_3 is a group.
8. Say, x is the identity. Then, $0 - x = 0$. So, $x = 0$. But $0 - 1 \neq 1$.
9. If $5x = 3$ multiply both sides by 4, we get $0 = 12$. If $3x = 5$ multiply both sides by 7, we get $x = 15$. Checking, we see that $3 \cdot 15 = 5$ mod 20.
10. $1, 3, 7, 9, 11, 13, 17, 19. 1, 9, 11,$ and 19 are their own inverses; 3 and 7 are inverses of each other as are 11 and 13.
11. One is Socks-Shoes-Boots.
12. The set does not contain the identity; closure fails.
13. Under multiplication modulo 4, 2 does not have an inverse. Under multiplication modulo 5, $\{1, 2, 3, 4\}$ is closed, 1 is the identity, 1 and 4 are their own inverses, and 2 and 3 are inverses of each other.Modulo multiplication is associative.
14. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.
15. a^{11}, a^6, a^4, a^1
16. The identity is 25.
17. (a) $2a + 3b$; (b) $-2a + 2(-b + c)$; (c) $-3(a + 2b) + 2c = 0$
18. $(ab)^3 = ababab$ and $(ab^{-2}c)^{-2} = ((ab^{-2}c)^{-1})^2 = (c^{-1}b^2a^{-1})^2 = c^{-1}b^2a^{-1}c^{-1}b^2a^{-1}$.

19. Observe that $a^5 = e$ implies that $a^{-2} = a^3$ and $b^7 = e$ implies that $b^{14} = e$ and therefore $b^{-11} = b^3$. Thus, $a^{-2}b^{-11} = a^3b^3$. Moreover, $(a^2b^4)^{-2} = ((a^2b^4)^{-1})^2 = (b^{-4}a^{-2})^2 = (b^3a^3)^2$.
20. $K = \{R_0, R_{180}\};\ L = \{R_0, R_{180}, H, V, D, D'\}$.
21. The set is closed because det $(AB) =$ (det A)(det B). Matrix multiplication is associative. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity. Since $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ its determinant is $ad - bc = 1$.
22. $1^2 = (n-1)^2 = 1$.
23. Using closure and trial and error, we discover that $9 \cdot 74 = 29$ and 29 is not on the list.
24. All we need do is find an x with the property $xab = bax$. The solution is $x = b$.
25. For $n \geq 0$, we use induction. The case that $n = 0$ is trivial. Then note that $(ab)^{n+1} = (ab)^n ab = a^n b^n ab = a^{n+1}b^{n+1}$. For $n < 0$, note that $e = (ab)^0 = (ab)^n(ab)^{-n} = (ab)^n a^{-n}b^{-n}$ so that $a^n b^n = (ab)^n$. In a non-Abelian group $(ab)^n$ need not equal $a^n b^n$.
26. The "inverse" of putting on your socks and then putting on your shoes, is taking off your shoes then taking off your socks. Use D_4 for the examples. (An appropriate name for the property $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$ is "Socks-Shoes-Boots Property.")
27. Suppose that G is Abelian. Then by Exercise 26, $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$. If $(ab)^{-1} = a^{-1}b^{-1}$ then by Exercise $24 e = aba^{-1}b^{-1}$. Multiplying both sides on the right by ba yields $ba = ab$.
28. By definition, $a^{-1}(a^{-1})^{-1} = e$. Now multiply on the left by a.
29. The case where $n = 0$ is trivial. For $n > 0$, note that $(a^{-1}ba)^n = (a^{-1}ba)(a^{-1}ba)\cdots(a^{-1}ba)$ (n terms). So, cancelling the consecutive a and a^{-1} terms gives $a^{-1}b^n a$. For $n < 0$, note that $e = (a^{-1}ba)^n(a^{-1}ba)^{-n} = (a^{-1}ba)^n(a^{-1}b^{-n}a)$ and solve for $(a^{-1}ba)^n$.
30. $(a_1a_2\cdots a_n)(a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}) = e$
31. By closure we have $\{1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45\}$.
32. $f(x) = x$ for all x. See Theorem 0.8.
33. Suppose x appears in a row labeled with a twice. Say $x = ab$ and $x = ac$. Then cancellation gives $b = c$. But we use distinct elements to label the columns.
34. Z_{105}; $Z_{40}, D_{20}, U(41)$
35. Closure and associativity follow from the definition of multiplication;

$a = b = c = 0$ gives the identity; we may find inverses by solving the equations $a + a' = 0$, $b' + ac' + b = 0$, $c' + c = 0$ for a', b', c'.

36. $(ab)^2 = a^2b^2 \Leftrightarrow abab = aabb \Leftrightarrow ba = ab$.
$(ab)^{-2} = b^{-2}a^{-2} \Leftrightarrow b^{-1}a^{-1}b^{-1}a^{-1} = b^{-1}b^{-1}a^{-1}a^{-1} \Leftrightarrow a^{-1}b^{-1} = b^{-1}a^{-1} \Leftrightarrow ba = ab$.

37. Since e is one solution, it suffices to show that nonidentity solutions come in distinct pairs. To this end, note that if $x^n = e$ and $x \neq e$, then $(x^{-1})^n = e$ and $x \neq x^{-1}$. So if we can find one nonidentity solution we can find a second one. Now suppose that a and a^{-1} are nonidentity elements that satisfy $x^n = e$ and b is a nonidentity element such that $b \neq a$ and $b \neq a^{-1}$ and $b^n = e$. Then, as before, $(b^{-1})^n = e$ and $b \neq b^{-1}$. Moreover, $b^{-1} \neq a$ and $b^{-1} \neq a^{-1}$. Thus, finding a third nonidentity solution gives a fourth one. Continuing in this fashion, we see that we always have an even number of nonidentity solutions to the equation $x^n = e$.

38. Note that $(\frac{1}{2}, \frac{1}{3}) = (\frac{2}{4}, \frac{1}{3})$, but $(\frac{1}{2}, \frac{1}{3})$ corresponds to $\frac{2}{5}$ whereas $(\frac{2}{4}, \frac{1}{3})$ corresponds to $\frac{3}{7}$. So, the correspondence is not a function from $Q^+ \times Q^+$ to Q^+.

39. If $F_1F_2 = R_0$ then $F_1F_2 = F_1F_1$, and by cancellation $F_1 = F_2$.

40. Observe that $F_1F_2 = F_2F_1$ implies that $(F_1F_2)(F_1F_2) = R_0$. Since F_1 and F_2 are distinct and F_1F_2 is a rotation it must be R_{180}.
Alternate proof. Observe that $(F_1F_2)^{-1} = F_2^{-1}F_1^{-1} = F_2F_1 = F_1F_2$ implies that (F_1F_2) is its own inverse. Since F_1 and F_2 are distinct and F_1F_2 is a rotation it must be R_{180}.

41. Since FR^k is a reflection we have $(FR^k)(FR^k) = R_0$. Multiplying on the left by F gives $R^kFR^k = F$.

42. Since FR^k is a reflection, we have $(FR^k)(FR^k) = R_0$. Multiplying on the right by R^{-k} gives $FR^kF = R^{-k}$. If D_n were Abelian, then $FR_{360^\circ/n}F = R_{360^\circ/n}$. But $(R_{360^\circ/n})^{-1} = R_{360^\circ(n-1)/n} \neq R_{360^\circ/n}$ when $n \geq 3$.

43. Using Exercise 42 we obtain the solutions R and $R^{-1}F$.

44. $R_{\beta-\alpha}$; $R_{\alpha-\beta}$

45. Since $a^2 = b^2 = (ab)^2 = e$, we have $aabb = abab$. Now cancel on left and right.

46. If a satisfies $x^5 = e$ and $a \neq e$, then so does a^2, a^3, a^4. Now, using cancellation we have that a^2, a^3, a^4 are not the identity and are distinct from each other and distinct from a. If these are all of the nonidentity solutions of $x^5 = e$, we are done. If b is another solution that is not a power of a, then by the same argument b, b^2, b^3 and b^4 are four distinct nonidentity solutions. We must further show that b^2, b^3 and b^4 are distinct from a, a^2, a^3, a^4. If $b^2 = a^i$ for some i, then cubing both sides we have $b = b^6 = a^{3i}$, which is a contradiction. A

similar argument applies to b^3 and b^4. Continuing in this fashion, we have that the number of nonidentity solutions to $x^5 = e$ is a multiple of 4. In the general case, the number of solutions is a multiple of 4 or is infinite.

47. The matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is in $\mathrm{GL}(2, Z_2)$ if and only if $ad \neq bc$. This happens when a and d are 1 and at least 1 of b and c is 0 and when b and c are 1 and at least 1 of a and d is 0. So, the elements are $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.
$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ do not commute.

48. If n is not prime, we can write $n = ab$, where $1 < a < n$ and $1 < b < n$. Then, a and b belong to the set $\{1, 2, \ldots, n-1\}$, but $0 = ab \mod n$ does not. If n is prime, let c be any element in the set. Then by the Corollary of Theorem 0.2 there are integers s and t such that $cs + nt = 1$. So, mod n we have $cs = 1$.

49. Proceed as follows. By definition of the identity, we may complete the first row and column. Then complete row 3 and column 5 by using Exercise 33. In row 2 only c and d remain to be used. We cannot use d in position 3 in row 2 because there would then be two d's in column 3. This observation allows us to complete row 2. Then rows 3 and 4 may be completed by inserting the unused two elements. Finally, we complete the bottom row by inserting the unused column elements.

CHAPTER 3

Finite Groups; Subgroups

1. $|Z_{12}| = 12; |U(10)| = 4; |U(12)| = 4; |U(20)| = 8; |D_4| = 8.$
   In Z_{12}, $|0| = 1; |1| = |5| = |7| = |11| = 12; |2| = |10| = 6; |3| = |9| = 4; |4| = |8| = 3; |6| = 2.$
   In $U(10)$, $|1| = 1$; $|3| = |7| = 4$; $|9| = 2$.
   In $U(20)$, $|1| = 1$; $|3| = |7| = |13| = |17| = 4$; $|9| = |11| = |19| = 2$.
   In D_4, $|R_0| = 1$; $|R_{90}| = |R_{270}| = 4$;
   $|R_{180}| = |H| = |V| = |D| = |D'| = 2$.
   In each case, notice that the order of the element divides the order of the group.

2. In Q, $\langle 1/2 \rangle = \{n(1/2) |\ n \in Z\} = \{0, \pm 1/2, \pm 1, \pm 3/2, \ldots\}$. In Q^*, $\langle 1/2 \rangle = \{(1/2)^n |\ n \in Z\} = \{1, 1/2, 1/4, 1/8, \ldots; 2, 4, 8, \ldots\}$.

3. In Q, $|0| = 1$. All other elements have infinite order since $x + x + \cdots + x = 0$ only when $x = 0$.

4. Observe that $a^n = e$ if and only if $(a^n)^{-1} = e^{-1} = e$ and $(a^n)^{-1} = (a^{-1})^n$. The infinite case follows from the infinite case.
   Alternate solution. Suppose $|a| = n$ and $|a^{-1}| = k$. Then $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$. So $k \leq n$. Now reverse the roles of a and a^{-1} to obtain $n \leq k$. The infinite case follows from the finite case.

5. By the corollary of Theorem 0.2 there are integers s and t so that $1 = ms + nt$. Then $a^1 = a^{ms+nt} = a^{ms}a^{nt} = (a^m)^s(a^n)^t = (a^t)^n$.

6. In Z, the set of positive integers. In Q, the set of numbers greater than 1.

7. In Z_{30}, $2 + 28 = 0$ and $8 + 22 = 0$. So, 2 and 28 are inverses of each other and 8 and 22 are inverses of each other. In $U(15)$, $2 \cdot 8 = 1$ and $7 \cdot 13 = 1$. So, 2 and 8 are inverses of each other and 7 and 13 are inverses of each other.

8. a. $|6| = 2, |2| = 6, |8| = 3$; b. $|3| = 4, |8| = 5, |11| = 12$;
   c. $|5| = 12, |4| = 3, |9| = 4$. In each case $|a + b|$ divides $\text{lcm}(|a|, |b|)$.

9. $(a^4c^{-2}b^4)^{-1} = b^{-4}c^2a^{-4} = b^3c^2a^2$.

10. $aba^2 = a(ba)a = a(a^2b)a = a^3(ba) = a^5b$.

11. For F any reflection in D_6, $\{R_0, R_{120}, R_{240}, F, R_{120}F, R_{240}F\}$.

12. In D_4, $K = \{R_0, R_{180}\}$, which is a subgroup; in D_3, $K = \{R_0, F_1, F_2, F_3\}$. But F_1F_2 is a rotation not R_0, so K is not closed. In D_6, $K = \{R_0, R_{180}, F_1, F_2, \ldots, F_6\}$. If K were a subgroup