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.** $\frac{1}{12}\begin{bmatrix} 2 & -3 \\ -8 & 6 \end{bmatrix}$ **d.** $\begin{bmatrix} 2 & 4 \\ 4 & 6 \end{bmatrix}$.
7. The set does not contain the identity; closure fails.
8. 1, 3, 7, 9, 11, 13, 17, 19.
9. 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.
10. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.
11. a^{11}, a^6, a^4, a^1
12. $5, 4, 8$
13. (a) $2a+3b$; (b) $-2a+2(-b+c)$; (c) $-3(a+2b)+2c=0$
14. $(ab)^3 = ababab$ and
$(ab^{-2}c)^{-2} = ((ab^{-2}c)^{-1})^2 = (c^{-1}b^2a^{-1})^2 = c^{-1}b^2a^{-1}c^{-1}b^2a^{-1}$.
15. 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,
$(a^2b^4)^{-2} = ((a^2b^4)^{-1})^2 = (b^{-4}a^{-2})^2 = (b^3a^3)^2$.
16. The identity is 25.
17. Since the inverse of an element in G is in G, $H \subseteq G$. Let g belong to G. Then g^{-1} belongs to G and therefore $(g^{-1})^{-1} = g$ belong to G. So, $G \subseteq H$.
18. $K = \{R_0, R_{180}\}$; $L = \{R_0, R_{180}, H, V, D, D'\}$.

19. 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 $ad - bc = 1$.

20. $1^2 = (n-1)^2 = 1$.

21. Using closure and trial and error, we discover that $9 \cdot 74 = 29$ and 29 is not on the list.

22. Consider $xyx = xyx$.

23. 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 $a^n b^n$.

24. 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.")

25. Suppose that G is Abelian. Then by Exercise 24, $(ab)^{-1} = b^{-1} a^{-1} = a^{-1} b^{-1}$. 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 $ba = ab$.

26. By definition, $a^{-1}(a^{-1})^{-1} = e$. Now multiply on the left by a.

27. 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 $(a^{-1}ba)^n$.

28. $(a_1 a_2 \cdots a_n)(a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}) = e$

29. By closure we have $\{1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45\}$.

30. Z_{105}; Z_{44} and D_{22}.

31. 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.

32.

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

33. 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 31. 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.

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

35. $axb = c$ implies that $x = a^{-1}(axb)b^{-1} = a^{-1}cb^{-1}$; $a^{-1}xa = c$ implies that $x = a(a^{-1}xa)a^{-1} = aca^{-1}$.

36. Observe that $xabx^{-1} = ba$ is equivalent to $xab = bax$ and this is true for $x = b$.

37. Since e is one solution it suffices to show that nonidentity solutions come in distinct pairs. To this end note that if $x^3 = e$ and $x \neq e$, then $(x^{-1})^3 = e$ 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 $x^3 = e$ and b is a nonidentity element such that $b \neq a$ and $b \neq a^{-1}$ and $b^3 = e$. Then, as before, $(b^{-1})^3 = e$ 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 $x^3 = e$.

    To prove the second statement note that if $x^2 \neq e$, then $x^{-1} \neq x$ and $(x^{-1})^2 \neq e$. So, arguing as in the preceding case we see that solutions to $x^2 \neq e$ come in distinct pairs.

38. In $D_4, HR_{90}V = DR_{90}H$ but $HV \neq DH$.

39. Observe that $aa^{-1}b = ba^{-1}a$. Cancelling the middle term a^{-1} on both sides we obtain $ab = ba$.

40. $X = VR_{270}D'H$.

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

42. 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}.

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

44. 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 $n \geq 3$.

45. **a.** R^3 **b.** R **c.** R^5F

46. 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'.

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

48. 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.

49. 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.

50. 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 $0 = ab \bmod n$ does not.

51. Let a be any element in G and write $x = ea$. Then $a^{-1}x = a^{-1}(ea) = (a^{-1}e)a = a^{-1}a = e$. Then solving for x we obtain $x = ae = a$.

52. Suppose that $ab = e$ and let b' be the element in G with the property that $bb' = e$. Then observe that
$ba = (ba)e = ba(bb') = b(ab)b' = beb' = (be)b' = bb' = e$.