Contents

Abstract Algebra Toolbox Solution File

Howard Xiao

1 Groups

Tool 1: Group Operation Checking

Solution 1.1: Exercise 1.1

1. Since $[(a_1, b_1) \star (a_2, b_2)] \star (a_3, b_3) = (a_1b_2 + b_1a_2, b_1b_2) \star (a_3, b_3) = (a_1b_2b_3 + b_1a_2b_3 + a_3b_1b_2, b_1b_2b_3)$, and $(a_1, b_1) \star [(a_2, b_2) \star (a_3, b_3)] = (a_1, b_1) \star (a_2b_3 + a_3b_2, b_2b_3) = (a_1b_2b_3 + a_2b_1b_3 + a_3b_1b_2, b_1b_2b_3)$, we know that $\star$ is associative.
2. Since $(a \star b) \star c = \frac{a}{b} \star c = \frac{a}{bc}$, and $a \star (b \star c) = a \star \frac{b}{c} = \frac{ac}{b} \neq \frac{a}{bc}$, we know that $\star$ is not associative.
3. From 1., we know that $(a_1, b_1) \star (a_2, b_2) = (a_1b_2 + b_1a_2, b_1b_2)$, and $(a_2, b_2) \star (a_1, b_1) = (a_1b_2 + b_1a_2, b_1b_2)$, hence $\star$ is commutative.
4. It is commutative, since $a \star b = \frac{a+b}{5} = \frac{b+a}{5} = b \star a$ for all $a, b \in \mathbb{Q}$.
5. Consider three residue classes $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$, then we know that $([a] + [b]) + [c] = [a + b + c] = [a] + ([b] + [c])$, hence addition is associative. Also, since $[a] + [b] = [a + b] = [b + a] = [b] + [a]$, we know that addition is also commutative.
6. Since $(ab)c = ac = a$ and $a(bc) = ab = a$, we know that this operation is associative. Since $ab = a \neq ba = b$, we know that it is not commutative.

Tool 2: Group or Not a Group?

Solution 1.2: Exercise 1.2

1. Since $e \cdot e = e$, we know that $e^{-1} = e$, e is invertible. Thus, $e \in S$. Also, for any invertible elements $a, b \in G$, $(ab) \star (b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = e$, we know that ab is invertible. Therefore, S is closed under $\star$. Since $\star$ is associative on G, it is also associative for S. Finally, for any invertible $a \in G$, we know that $a^{-1} \star a = e$, hence a^{-1} is also invertible.
2. For all $n > 1$, there is no multiplicative inverse for $0 \in \mathbb{Z}/n\mathbb{Z}$, hence $\mathbb{Z}/n\mathbb{Z}$ is not a group.
3.
(a) Not a group, since $\frac{1}{2} + \frac{1}{2} = 1$ which has absolute value equal to 1, hence this set is not closed under addition.
(b) Is a group, since addition in rational numbers is associative. The additive inverses of any rational number with denominator either 1 or 2 is another rational number with denominator either 1 or 2. Adding two rational numbers with denominator 1 or 2 results in another one with denominator 1 or 2. 0 can be think of $0 = \frac{0}{1}$, which is the identity element in this group.
(c) This is a group. Consider any two rational numbers $\frac{p_1}{q_1}, \frac{p_2}{q_2}$ in lowest terms such that q_1, q_2 are odd. Then, $\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1q_2+p_2q_1}{q_1q_2}$, which is a rational number with odd denominator, hence after reducing to lowest term, it still has odd denominator. Therefore, the set is closed under addition. Since the additive inverse of a rational with odd denominator is still a rational with odd denominator, and $0 = \frac{0}{1}$ has odd demonimator as above, also since addition is associative for $\mathbb{Q}$, we know that this set is a group.
4. Since given $0 \leq x, y < 1$, we know that $0 \leq x \star y < 1$, hence G is closed under $\star$. Next, since $x \star (1 - x) = 1 - \lfloor 1 \rfloor = 0$, we know that $x^{-1} = 1 - x$ for all $x \in G$, thus inverse exists for all $x \in G$ under $\star$. Then, for $x = 0$, $0 \star y = y - \lfloor y \rfloor = y - 0 = y$ for all $y \in G$, thus 0 is the identity element for operation $\star$. Finally, since $(x \star y) \star z = (x + y - \lfloor x + y \rfloor) \star z = (x + y - \lfloor x + y \rfloor) + z - \lfloor (x + y - \lfloor x + y \rfloor) + z \rfloor = x + y + z - \lfloor x + y + z \rfloor$ and $x \star (y \star z) = x \star (y + z - \lfloor y + z \rfloor) = x + (y + z - \lfloor y + z \rfloor) - \lfloor x + (y + z - \lfloor y + z \rfloor) \rfloor = x + y + z - \lfloor x + y + z \rfloor$, we know that $\star$ is associative. Therefore G is a group. Finally, since $x \star y = x + y - \lfloor x + y \rfloor = y + x - \lfloor y + x \rfloor = y \star x$, G is an abelian group.
5. Suppose $A \times B$ is an abelian group. Then, we know that $(a_1, b_1) \star (a_2, b_2) = (a_1 \star a_2, b_1 \star' b_2) = (a_2, b_2) \star (a_1, b_1) = (a_2 \star a_1, b_2 \star' b_1)$, hence $a_1 \star a_2 = a_2 \star a_1$ for all $a_1, a_2 \in A$, and $b_1 \star' b_2 = b_2 \star' b_1$ for all $b_1, b_2 \in B$, thus A, B are both abelian.
If A, B are both abelian, consider any $(a_1, b_1), (a_2, b_2) \in A \times B$, we know that $(a_1, b_1) \star (a_2, b_2) = (a_1 \star a_2, b_1 \star' b_2) = (a_2, b_2) \star (a_1, b_1) = (a_2 \star a_1, b_2 \star' b_1)$, hence $A \times B$ is abelian.
Note: in the above, we use $\star$ to symbolize operation on A and $A \times B$, and $\star'$ to denote operation on B.

Tool 3: Order of Group Elements

Solution 1.3: Exercise 1.3

1. Since $1^1 = 1$, $|1| = 1$. Since $2^n = 0 \in \mathbb{Z}/6\mathbb{Z}$, $|2| = \infty$. Since $3^n = 3 \in \mathbb{Z}/6\mathbb{Z}$, $|3| = \infty$. Since $4^n = 4 \in \mathbb{Z}/6\mathbb{Z}$, $|4| = \infty$. Since $5^2 = 1 \in \mathbb{Z}/6\mathbb{Z}$, $|5| = 2$.
2. Since $x^2 = e \in G$, we know that $|x| \leq 2$. Since if $x = e$, $e^2 = e$, and in this case x has order 1, $|x|$ is either 1 or 2.
3. Suppose $|x| = n$, i.e. $x^n = e$, and we know that $x^n \cdot (x^{-1})^n = e$, hence $(x^{-1})^n = e$, $|x^{-1}| \leq n$. If $|x^{-1}| = m < n$, we know that $(x^{-1})^m = e$, and since $(x^{-1})^m \cdot x^m = e$, $x^m = e$, which is impossible. Therefore, $|x^{-1}| = |x| = n$.
4. Firstly, since $x^n = x^{st} = (x^s)^t = e$, we know that $|x^s| \leq t$. Suppose $|x^s| = m < t$, then we know that $(x^s)^m = x^{sm} = e$, which is impossible since $sm < n = st$. Thus, $|x^s| = t$.
5. We simply need to show that $e, x, \ldots, x^{n-1}$ are all different to prove the claim. Suppose $x^i = x^j$ for some $0 \leq i, j \leq n-1$, suppose $i < j$. Then, we know that $x^{-i}x^i = x^{-i}x^j = x^{j-i} = e$, and we have $0 \leq j - i \leq n - 1 < n$, which is impossible.
6. Given any $a, b \in G$ where G is a group, suppose $|ab| = n < \infty$. Then, we know that $(ab)^n = a(ba)^{n-1}b = e$, thus $(ba)^{n-1} = a^{-1}b^{-1} = (ba)^{-1}$. Therefore, $(ba)^n = e$, $|ba| \leq n$. Suppose $|ba| = m < n$, then we know that $(ba)^m = b(ab)^{m-1}a = e$, similarly we know that $(ab)^m = e$, which is impossible since $m < n$. Hence, $|ba| = n = |ab|$.
Suppose $|ab| = \infty$ and $|ba| = n < \infty$, then from above, we know that $(ab)^n = e$, which is impossible. Hence, in this case, $|ab| = |ba| = \infty$.
7. Firstly we know that $(a, 1) \star (1, b) = (a \star 1, 1 \star b) = (1 \star a, b \star 1) = (1, b) \star (a, 1)$, hence they commutes in $A \times B$. Then, suppose $|(a, b)| = n$, thus $(a, b)^n = [(a, 1) \star (1, b)]^n = (a, 1)^n \star (1, b)^n = (a^n, b^n) = (1, 1)$. Therefore, we know that n is the smallest n satisfying $a^n = 1 = b^n$. Suppose $|a| = x$ and $|b| = y$. We know that for $m = lcm(x, y)$, $a^m = b^m = 1$, hence $n \leq m = lcm(x, y)$. Suppose $n < m$, then either $x \nmid n$ or $y \nmid n$. If $x \nmid n$, we can find $n = px + r$, where $r < x$, which means $a^n = a^{px+r} = a^{xp} \cdot a^r = a^r = 1$, which is impossible since $r < x$. Similarly for the case $y \nmid n$. Thus, we have shown that $n = lcm(x, y)$.
8. Suppose $x^i = x^j$ for some $i, j \in \mathbb{N}$, and suppose $i < j$. Then, we know that $x^{j-i} = e$, which means $|x| \leq j - i < \infty$, which is impossible.
9. Suppose the operation defined for G is $\star$. Then, G must be closed under $\star$. Consider $a \star b$, since $a \star b = a$ or $a \star b = b$ implies $b = 1$ or $a = 1$ respectively, which both are impossible, we know that $a \star b = c$. Similarly, $b \star a = c$, $a \star c = c \star a = b$, $b \star c = c \star b = a$. Consider a^2 under $\star$. $a^2 \neq a$ since $a \neq 1$. If $a^2 = b$ or $a^2 = c$, we know that $a^3 \neq 1$, which is impossible since $|a| \leq 3$. Therefore, $a^2 = 1 = b^2 = c^2$. Thus, the operation $\star$ is uniquely determined and from above we know that G is abelian under $\star$.

Tool 4: Arithmetic of Group Elements

Solution 1.4: Proof of Theorem 1.1

1. Suppose we have e, e' being identities of G. Then, we know that $ee' = e' = e$.
2. Suppose $g \in G$ has inverses $g^{-1}, g^{-1\prime}$. Then, we know that $g^{-1}g = e$, multiply both sides by $g^{-1\prime}$, we get $g^{-1}(gg^{-1\prime}) = g^{-1} = g^{-1\prime}$.
3. Since $g \cdot g^{-1} = e$, and by 2., we know that $g^{-1^{-1}} = g$.

Solution 1.5: Proof of Theorem 1.2

Suppose $g, x, y \in G$ for some group G and $gx = gy$, then multiply by g^{-1} on the left on both sides we get $x = y$. Similarly if $xg = yg$, multiply by g^{-1} on the right on both sides we get $x = y$.

Solution 1.6: Exercise 1.4

1. Since $(a_1 \star \cdots \star a_n) \star (a_n^{-1} \star \cdots a_1^{-1}) = e$ by associativity of $\star$, by Theorem 1.1, we know that $(a_1 \star \cdots \star a_n)^{-1} = (a_n^{-1} \star \cdots a_1^{-1})$.
2. Given group G, $x, y \in G$. Suppose $xy = yx$, then multiply both sides on the left by y^{-1}, we get $y^{-1}xy = x$. Multiply both sides on the left by $x^{-1}y^{-1}$, we get $x^{-1}y^{-1}xy = e$.
Suppose $y^{-1}xy = x$, multiply both sides on the left by y, we get $xy = yx$.
Suppose $x^{-1}y^{-1}xy = e$, multiply both sides on the left by yx, we get $xy = yx$.
3. Suppose $x^2 = e$ for all $x \in G$ for some group G. Hence, we know by Theorem 1.1 that $x = x^{-1}$ for all $x \in G$. Suppose $x, y \in G$. Then, $(xy)^2 = xyxy = e$, thus $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. Therefore, G is abelian.
4. If $xyz = e$, then we know that $yz = x^{-1}$ by Theorem 1.1. Hence, $yzx = x^{-1}x = e$. However yxz is not always true. Pick any non-abelian group where $xy \neq yx$, then we know that $xyz \neq yxz$ by Theorem 1.2.

Tool 5: Dihedral Group Computation

Solution 1.7: Proof of Theorem 1.3

We are trying to show that the composition of two reflections is either identity or a rotation.

We have several cases. Given reflections s and t, suppose $s = t$, then $st = s^2 = e$.

Suppose n is odd. Label clockwise each vertex from $1, 2, \dots n$. Then, we know that s fixes some point x and t fixes some point y. Suppose $x < y$ (case $x > y$ is exactly the same). Then, we know that $t \circ s : x \mapsto x \mapsto y+y-x = 2y-x$, $t \circ s : y \mapsto x-(y-x) = 2x-y \mapsto y-(2x-y)+y = 3y-2x$. Hence, both x and y rotates clockwise by $2y - 2x$. We can repeat above and verify other vertex as well, in this case $t \circ s$ is a rotation.

Suppose n is even. Then, we have several cases. The case when both s and t are Type II reflections is the same as if n is odd, since there are fixed points, we can repeat arguments above. Suppose s is a Type I reflection and t is a Type II reflection. Pick one of the side cut through by the reflection axis of s, namely $(x, x+1)$, and pick a fixed point of t, namely y. Suppose $y \geq x + 1$. ($y \leq x$ case is exactly the same) In this case, we know that $t \circ s : x \mapsto x + 1 \mapsto y + y - (x + 1) = 2y - x - 1$, and $t \circ s : y \mapsto x-(y-(x+1)) = 2x-y+1 \mapsto y+y-(2x-y+1) = 3y-2x-1$. Here both x and y rotates clockwise by $2y-2x-1$ sides. Finally, if both s, t are Type I reflections, we can pick one of the sides cut through by the reflection axis of s, namely $(x, x+1)$, and one of the sides cut through by the reflection axis of t, namely $(y, y+1)$, and suppose $x < y$. In this case, $t \circ s : x \mapsto x + 1 \mapsto y + 1 + y - (x + 1) = 2y - x$, and $t \circ s : y \mapsto 2x - y + 1 \mapsto y + 1 + 2y - 2x - 1 = 3y - 2x$, hence both x and y rotates clockwise by $2y - 2x$.

With all cases being above, we have verified the claim.

Solution 1.8: Exercise 1.5

1. Since r is a rotation, we can write r as ρ^k for some $k \in \mathbb{N}$. Label the n-gon clockwise by $1, 2, \ldots, n$. If n is odd, suppose the reflection fixes a point a. Then, we know that for any point x, under rs, $x \mapsto a-(x-a) = 2a - x \mapsto 2a - x - k$, and under sr^{-1}, $x \mapsto x + k \mapsto a - (x + k - a) = 2a - x - k$, thus we know that in this case $rs = sr^{-1}$.
If n is even, suppose the reflection s is a Type II reflection, then this is the same case as if n is odd. If the reflection s is a Type I reflection, pick one side $(a, a + 1)$ where the axis of reflection goes through. Then, we know that for any point x, under rs, $x \mapsto a-(x-a-1) = 2a-x+1 \mapsto 2a-x+1-k$, and under sr^{-1}, $x \mapsto x+k \mapsto a-(x+k-a-1) = 2a-x+1-k$, thus in this case we also have $rs = sr^{-1}$.
2. Let s be any element in D_{2n} that is not a power of r, then we know that s is not a rotation, hence a reflection. Then, this follows from 1.
3. If n is odd, consider an element $a \neq e$ in D_{2n}. If a is a rotation, let us write $a = \rho^k$. Consider any reflection s, we then know that $as = sa^{-1}$, however since $a = \rho^k$, $a^{-1} = \rho^{n-k} \neq \rho^k$ since n is odd, $a \neq a^{-1}$, hence $as = sa^{-1} \neq sa$, thus a does not commute with any reflection.
If a is a reflection, consider any rotation $r = \rho^k$, then we know that $ar = a(r^{-1})^{-1} = r^{-1}a$, however since $r \neq r^{-1}$, we know that $ar \neq ra$, hence a does not commute with any rotation using similar reason as above. Therefore, e is the only element that commutes with all other elements in D_{2n}.
4. Since x, y are elements of order 2, we know that $x^2 = y^2 = e$, thus $x = x^{-1}$, $y = y^{-1}$. Thus, $tx = xyx$ and $xt^{-1} = x(xy)^{-1} = xy^{-1}x^{-1} = xyx$. Similar for yt.

Tool 6: Rigid Motion Group Order for 3D Spaces

Solution 1.9: Exercise 1.6

1. For any rigid motion on the cube, a face of the cube is shifted to some face on the cube (6 possibilities). Fixing where this face is shifted, we also have 4 choices of sending a particular edge on this face to an edge on the target face, but then due to the constraint of rigid motions, we have only 1 choice of sending other edges, since we can not "twist" the cube. Therefore, the group of rigid motions of a cube has order $6 \cdot 4 = 24$.
2. For any rigid motion on a tetrahedron, a face of the tetrahedron is sent to some face of this tetrahedron (4 choices). Fixing where this face is sent, we also have 3 choices of sending a particular edge on this face to an edge on the target face. Due to constraint of rigid motions, we have only 1 choice of sending other edges, therefore, this group has order $4 \cdot 3 = 12$.
3. Repeat argument in 1., but replace with 8 faces and 3 edges, we know that the group order is $8 \cdot 3 = 24$. 4. Repeat above arguments with x faces and y edges, we get the answer.

Tool 7: Computations on Cycles and Permutations

Solution 1.10: Proof of Theorem 1.5

We know that S_n is the set of bijective permutations on the set $X = \{1, 2, \ldots, n\}$. There are n possibilities that 1 can be mapped to, but after 1 is mapped, 2 can't map to the same place since it is a bijection, so we are left with $n-1$ choices for 2. In the end, we have only 1 choice of mapping n, thus the order of S_n is $n!$.

Solution 1.11: Exercise 1.7

1. We have $S_3 = \{id, (12), (23), (13), (123), (132)\}$. The orders are $1, 2, 2, 2, 3, 3$ respectively.
2. We do the computation from right to left, we have $1 \mapsto 2 \mapsto 2$, $2 \mapsto 3 \mapsto 5$, $3 \mapsto 1 \mapsto 3$, $5 \mapsto 5 \mapsto 1$, hence the result is (125).
3. We first observe that the order of any n-cycle is n. The order should be a multiple of 2 since we contain a 2-cycle, should be a multiple of 3, since we also contain a 3-cycle, and should be a multiple of 5 as well, since we contain a 5 cycle. Therefore, the order should be the least common multiple of $2, 3, 5$, which is 30. The proof of second claim follows exact same logic as above.
4. Firstly, there are $n \cdot (n-1) \cdots (n-m+1)$ ways to choose m elements in X into a m-cycle. However, for any m-cycle, there are m ways to write it in the cycle notation. So the total number of different m-cycles should be $\frac{n \cdot (n-1) \cdots (n-m+1)}{m}$.
5. Firstly, there are $\frac{n \cdot (n-1)}{2}$ ways to choose the first cycle, and after the first 2-cycle is chosen, there are only $n-2$ elements left in X, hence only $\frac{(n-2) \cdot (n-3)}{2}$ choices to choose the second cycle. Further more, we know that $(ab)(cd)$ and $(cd)(ab)$ is the same cycle, we need to further divide by 2. Therefore, the number of permutation who can be written as the multiplication of two disjoint 2-cycles is $\frac{n \cdot (n-1)}{2} \cdot \frac{(n-2) \cdot (n-3)}{2} \cdot \frac{1}{2} = \frac{n(n-1)(n-2)(n-3)}{8}$.

Tool 8: Order of Cycles

Solution 1.12: Exercise 1.8

1. Firstly, since the element has order 4 in S_4, its disjoint cycle decomposition has cycles with length's least common multiple 4, hence are either 4-cycles or product of 2 disjoint 2-cycles. Thus, we have $(1234), (1243), (1324), (1342), (1423), (1432)$ being the 4-cycles, and $(12)(34)$, $(13)(24)$, $(14)(23)$ being the products of 2 disjoint 2-cycles.
2. Firstly, $\sigma : a_x \mapsto a_{(x+1) \mod m}$. Suppose $\sigma^i : a_x \mapsto a_{(x+i) \mod m}$, then we know that $\sigma^{i+1} = \sigma \circ \sigma^i : a_x \mapsto a_{(x+i) \mod m} \mapsto a_{(x+i+1) \mod m}$. Thus, by induction the claim is proved.
3. Consider the disjoint cycle decomposition of this element. We know that the lengths of the disjont cycle decomposition of this element must have least common multiple 2, hence it must has the cycle decomposition of commuting(disjoint) 2-cycles, since we do not write 1-cycles in cycle decomposition.
4. Firstly we observe that this element is not identity, since identity has order 1. Thus, it must has a cycle decomposition with some n-cycles, $n \geq 2$. Consider the disjoint cycle decomposition of this element. We know that the lengths of the disjont cycle decomposition of this element must have least common multiple p, hence it must has the cycle decomposition of commuting(disjoint) p-cycles, since no other number $1 < x \leq n, x \neq p$ divide p and we do not write 1 cycles. Therefore, it must have a cycle decomposition of commuting p-cycles. This is wrong when p is not a prime. Consider $p = 6 = n$ and $x = (12)(345)$, x is still order 6 but does not have 6-cycles.
5. Suppose $n > 8$, then it is not possible that one of the element of the n-cycle "vanishes" as we compute σ^k to get τ while the other $1, 2, \ldots 8$ stays in the cycle decomposition. Thus, $n = 8$. Since a 8-cycle has order 8, but τ has order 2, we must have k being a multiple of 4, but not a multiple of 8, since otherwise this will result identity. Consider $k = 4$, then we can find $\sigma = (13572468)$.
6. Similar as in 5, $n = 5$. However, τ has order 6, but a 5-cycle has order 5, hence it is not possible that $\tau = \sigma^k$, since $|\sigma^k| \leq |\sigma| = 5$.

Tool 9: Usage of Various Examples of Groups

Solution 1.13: Exercise 1.9

1. We need the determinant of the matrix to be not equal 0, hence we have: $\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}$. Since $\begin{pmatrix}1&1\\0&1\end{pmatrix} \cdot \begin{pmatrix}1&0\\1&1\end{pmatrix} = \begin{pmatrix}0&1\\1&1\end{pmatrix}$, and $\begin{pmatrix}1&0\\1&1\end{pmatrix} \cdot \begin{pmatrix}1&1\\0&1\end{pmatrix} = \begin{pmatrix}1&1\\1&0\end{pmatrix}$, we know that $GL_2(\mathbb{F}_2)$ is non-abelian. 2. Consider any matrix A such that $A_{11} = x \in F$, and $A_{jj} = 1$ for all $1 < j \leq n$, and all other entries not on the diagonal is 0. We know that $\det(A) \neq 0$, hence $A \in GL(n, F)$, but we have a infinite amount of choices for x if F is infinite. If F is finite, the total number of $n \times n$ matrices is finite, hence $GL(n, F)$ must be finite.
3. Firstly, the identity matrix is an upper triangular matrix. Secondly, we know that:

$$\begin{pmatrix}a&b\\0&c\end{pmatrix} \cdot \begin{pmatrix}d&e\\0&f\end{pmatrix} = \begin{pmatrix}ad&ae+bf\\0&cf,\end{pmatrix}$$

which is also upper triangular. Given $\begin{pmatrix}a&b\\0&c\end{pmatrix}$, we know that the matrix $\begin{pmatrix}\frac{1}{a}&-\frac{b}{ac}\\0&\frac{1}{c}\end{pmatrix}$ is the inverse by above formula, which is also upper-triangular.
3. The order of 1 is 1, order of -1 is 2, order of i, j, k is 4.

Tool 10: Group Homomorphisms and their Properties

Solution 1.14: Proof of Theorem 1.8

1. Since ϕ is a homomorphism, we know that $\phi(e_G g) = \phi(e_G)\phi(g) = \phi(g)$, hence $\phi(e_G) = e_H$ since the identity is unique.
2. Since ϕ is a homomorphism, we have $\phi(gg^{-1}) = \phi(g)\phi(g^{-1}) = \phi(e_G) = e_H$, we have $\phi(g^{-1}) = \phi(g)^{-1}$ by uniqueness of inverses.

Solution 1.15: Exercise 1.10

1. Consider $g, g' \in G$, then we know that $\phi(gg') = g_0 g g' {g_0}^{-1} = g_0 g {g_0}^{-1} g_0 g' {g_0}^{-1} = \phi(g)\phi(g')$, thus ϕ is a homomorphism.
2. Suppose ϕ is a group homomorphism, then we know that for all $x, y \in G$, $xy = \phi((xy)^{-1}) = \phi(y^{-1}x^{-1}) = \phi(y^{-1})\phi(x^{-1}) = yx$, hence G is abelian. Suppose G is abelian, then we know that for all $x, y \in G$, we have $\phi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \phi(x)\phi(y)$, thus ϕ is a homomorphism.
3. Firstly, $n = 1$ is trivially true. Suppose for some $n \in \mathbb{N}$, we have $\phi(g^n) = (\phi(g))^n$. Then, $\phi(g^{n+1}) = \phi(g^n g) = \phi(g^n)\phi(g) = (\phi(g))^n \phi(g) = \phi(g)^{n+1}$, thus by induction the claim is true for all $n \in \mathbb{N}$.
4. Let $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$, then we know that $\pi(x + y) = \pi((x_1 + y_1, \ldots, x_n + y_n)) = x_1 + y_1 = \pi(x) + \pi(y)$, thus π is a homomorphism.
5. Suppose $x, y \in G'$. Then, we know that $x = \phi(g), y = \phi(g')$ for some $g, g' \in G$. Thus we have $xy = \phi(g)\phi(g') = \phi(gg') = \phi(g'g) = \phi(g')\phi(g) = yx$, hence G' is abelian.
6. Since for all $x, x' \in \mathbb{R}$, we have $f(x + x') = e^{i(x+x')} = e^{ix} \cdot e^{ix'} = f(x) \cdot f(x')$, thus f is a homomorphism.
7. Consider $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $\begin{pmatrix} d & e \\ 0 & f \end{pmatrix}$. Then, we know that $\phi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}) = \phi(\begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix} = (ad)^2 = a^2 d^2 = \phi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}) \cdot \phi(\begin{pmatrix} d & e \\ 0 & f \end{pmatrix})$.
8. Consider any homomorphism $\phi : G \to H$, and $Im(\phi) \subset H$. Suppose $x, y \in Im(\phi)$, then $x = \phi(g), y = \phi(g')$ for some $g, g' \in G$, thus $xy = \phi(gg') \in Im(\phi)$, hence $Im(\phi)$ is closed under group operation of H, since $x^{-1} = (\phi(g))^{-1} = \phi(g^{-1})$, we know that $x{-}1 \in Im(\phi)$, $Im(\phi)$ is closed under inversion of H. Finally, we know that $\phi(e_G) = e_H$, hence $e_H \in Im(\phi)$, and the associativity follows from the group operation of H, thus $Im(\phi)$ is a group.

Tool 11: Group Isomorphisms and their Properties

Solution 1.16: Exercise 1.11

1. Suppose by contradiction that they are isomorphic, i.e. there exists an isomorphism ϕ between $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$. Suppose $\phi(x) = i$, then we know that $\phi(x^4) = (\phi(x))^4 = 1$, which means $x^4 = 1$ for some $x \in, x \neq 1$ since $\phi(1) = 1$. We can only have $x = -1$. However, we also need $\phi(y) = -1$, where $\phi(y^2) = 1$, $y^2 = 1$ and have $y \neq x$, but $y \neq 1$. This is impossible and we reached a contradiction.
2. Suppose there is an isomorphism ϕ between $\mathbb{R}$ and $\mathbb{Q}$. Consider $\phi|_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Q}$, this cannot be surjective since otherwise ϕ can't be injective. However, $\phi|_{\mathbb{Q}}$ is injective since ϕ is injective. Therefore, we have found a function from $\mathbb{Q}$ to $\mathbb{Q}$ that is injective but not surjective, which is impossible.
3. Suppose there is an isomorphism between D_8 and Q_8. Consider the 8-cycle in D_8. This element x has order 8, meaning that $\phi(x), \phi(x^2), \ldots, \phi(x^7)$ do not equal to the identity, which means $\phi(x)$ also has order 8. However, there is no element of order 8 in Q_8, thus we get a contradiction.
4. Consider the map $\phi : A \times B \to B \times A$ such that $\phi(a, b) = (b, a)$. It is very easy to see that this map is bijective. We need to show ϕ is a homomorphism. Consider $\phi((a_1 + a_2, b_1 + b_2)) = (b_1 + b_2, a_1 + a_2) = (b_1, a_1) + (b_2, a_2) = \phi((a_1, b_1)) + \phi((a_2, b_2))$, hence ϕ is indeed an isomorphism, and $A \times B \cong B \times A$.
5. Suppose ϕ is an isomorphism. Then, ϕ is bijective. Since $\phi(e) = e$, we know that the kernel of ϕ is $\{e\}$. Suppose ϕ is a surjective homomorphism with kernel $\{e\}$. Then, suppose $\phi(x) = \phi(y)$, then we know that $\phi(x)(\phi(y))^{-1} = \phi(xy^{-1}) = e$, however, this means $xy^{-1} = e, x = y$, thus ϕ is injective. Therefore, ϕ is a bijective homomorphism, hence an isomorphism.
6. First of all, if ϕ is an isomorphism, we know that ϕ is bijective, hence ϕ^{-1} is also bijective. Next, consider $\phi^{-1}(xy) = \phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(x)\phi^{-1}(y)$, for some a, b such that $\phi(a) = x, \phi(b) = y$, thus ϕ^{-1} is a bijective homomorphism, thus isomorphism.
7. Suppose ϕ is any homomorphism from $\mathbb{Z}^+$ to itself. Then, $\phi(0) = 0$. Consider $\phi(x)$ for some $x \in \mathbb{Z}^+$, we know that $\phi(x) = \phi(x \cdot 1) = \phi(1) + \phi(1) + \ldots + \phi(1) = x \cdot \phi(1)$ for all $x \in \mathbb{Z}$, and $\phi(-x) = -\phi(x) = -x\phi(1)$. Hence, as soon as $\phi(1)$ is defined, we have defined ϕ for all $x \in \mathbb{Z}$. Therefore, we can summarize that $\phi_a(x) = a \cdot x$ for any $a, x \in \mathbb{Z}$. Among these ϕ, for $\phi(x) = 0$ for all x, we know that this ϕ is neither injective or surjective. Otherwise ϕ_a is injective for all $a \neq 0$. However, $a \mid \phi_a(x)$ for all $a \in \mathbb{Z}$, so the only surjective and hence bijective ϕ_a's are $\phi(x) = x$ and $\phi(x) = -x$.

Tool 12: Automorphisms and their Properties

Solution 1.17: Proof of Theorem 1.10

Firstly, we know that id can be seen as C_e as $ege^{-1} = g$ for all $g \in G$, thus $id \in inn(G)$. Next, suppose $C_g, C_{g'} \in inn(G)$, then we know that $)C_g \circ C_{g'})(x) = gg'xg'^{-1}g^{-1} = (gg')x(gg')^{-1} = C_{gg'}(x)$, thus $C_g \circ C_{g'} \in inn(G)$. Thus, we also know that $C_g \circ C_{g^{-1}} = C_e(x) = id$, hence ${C_g}^{-1} \in inn(G)$. Then since function composition is associative, we know that $inn(G)$ is indeed a group. If G is abelian, we know that for any inner automorphism $C_g(x) = gxg^{-1} = gg^{-1}x = x$, thus $inn(G) = \{id\}$.

Solution 1.18: Exercise 1.12

1. Since we know that $(AB) \mapsto (AB)^{T^{-1}} = (B^TA^T)^{-1} = (A^T)^{-1}(B^T)^{-1}$, we know that this map is a homomorphism. Next, suppose $A \neq B$, then we know that $A^T \neq B^T$, hence $(A^T)^{-1} \neq (B^T)^{-1}$ by uniqueness of inverses, therefore, this map is injective. Consider any $X \in GL(n, \mathbb{R})$, then we know that $(X^{-1})^T \mapsto X$, hence this map is surjective, hence bijective. Therefore, this map is an automorphism.
2. Firstly, we know that the identity is an automorphism from Theorem 1.10. Next, associative laws hold for function composition. Then, if we have two automorphisms ϕ, ϕ', we know that $\phi \circ \phi'(xx') = \phi(\phi'(xx')) = \phi(\phi'(x)\phi'(x')) = \phi\phi'(x) \cdot \phi\phi'(x') = \phi \circ \phi'(x) \cdot \phi \circ \phi'(x')$, hence $\phi \circ \phi'$ is a homomorphism. Further more since ϕ, ϕ' are all bijective, $\phi \circ \phi'$ is also bijective. Thus, we know that $\phi \circ \phi'$ is another automorphism. We also know that from Exercise 1.11.6, that ϕ^{-1} is an isomorphism, hence automorphism. Therefore, the set of automorphims is a group.
3. Consider $q_1, q_2 \in \mathbb{Q}$, then we know that $q_1 + q_2 \mapsto k(q_1 + q_2) = kq_1 + kq_1$, thus this map is homomorphism. Next, this is a linear function on $\mathbb{Q}$, which is clearly bijective. Therefore, we know that this map is a automorphism. Suppose this map is an inner automorphism, then since $\mathbb{Q}$ is abelian, this map must be identity. However, $k \neq 1$, hence this map is an outer automorphism for $k \neq 1$.

Tool 13: Group Action: Does this act?

Solution 1.19: Exercise 1.13

1. Consider $a, b \in F$, $v \in V$, we know that $av \in V$, $(ab)v = a(bv)$ by definition of scalar multiplication and $1v = v$. Thus, F acts on V by scalar multiplication.
2. Since $(z_1 \cdot z_2) \cdot a = z_1 + z_2 + a = z_1 + (z_2 + a) = z_1 \cdot (z_2 \cdot a)$ for all $z_1, z_2 \in \mathbb{Z}$ and $0 \cdot a = a$ for all $a \in \mathbb{Z}$, hence we know that $\mathbb{Z}^+$ acts on itself by $z \cdot a = z + a$.
3. Suppose the permutation representation of this action is ϕ, then we know that $g \cdot a = \phi(g)(a)$ for all $g \in G, a \in A$. Suppose $g \cdot a = e$, then $\phi(g)(a) = e$, a in the kernel of $\phi(g)$. Similarly vice versa.
4. The group of rigid motions G of a tetrahedron acts on the set of 4 vertices $\{1, 2, 3, 4\}$ and has a permutation representation $\phi : G \to S_4$. ϕ is injective by construction, but may not be surjective due to rigid motion constraint, hence since ϕ is an isomorphism G is isomorphic to some group $Im(\phi)$ inside S_4.
5. Consider $g, g', h \in G$, then we know by associativity that $(gg')h = g(g'h)$, and $eh = h$, thus group multiplication is a self-action on G.

Tool 14: Orbits, Stablizer and Centralizer

Solution 1.20: Exercise 1.14

. Since we know that the only element in D_{2n} for odd n that commutes with all other element is e, the center of D_{2n} for n odd is $\{e\}$ by definition.
2. Since identity is a rotation, and just leaves every point on S^3 unchanged, and rotations compose with each other, we can see that $SO(2)$ acts on S^3 by rotation in the x-y plane, leaving z-axis fixed. For any $s \in S$, if $s = N$ or $s = S$, then this point is fixed under rotation, hence the orbit of s in this case is $\{s\}$. Otherwise, the orbit of s is the circle on the x-y plane of points in S^3 passing through s. For any point $s \neq N, S$, we know that $Stab_G(s)$ can only be the identity transformation, since all other rotation change the position of s under this action.
3. Firstly, we know that $C_G(Z(G)) \subset G$ by definition. Then, for any $g \in G$, $a \in Z(G)$, we know that $ga = ag$ by definition of $Z(G)$, thus $C_G(Z(G)) = G$.
4. We are trying to answer the question of what is the matrix that commutes with all matrices in $GL(n, \mathbb{R})$, and we know that it can only be a diagonal matrix such that nonzero real numbers are on the diagonal (to make sure it is invertible).

Tool 15: Subgroup or Not a Subgroup?

Solution 1.21: Exercise 1.15

1. Consider $a + ai, b + bi$ in this set. Then, we know that $a, b \in \mathbb{R}$. Since we also know that $a + ai - (b + bi) = (a - b) + (a - b)i$ is in this set, by criterion of subgroup, we know this set is a subgroup of complex numbers.
2. Let S be the set of rational numbers whose denominators divide n. Then, consider any $\frac{p_1}{q_1}, \frac{p_2}{q_2} \in S$, we have $\frac{p_1}{q_1} - \frac{p_2}{q_2} = \frac{p_1 k}{n} - \frac{p_2 m}{n} = \frac{p_1 k - p_2 m}{n}$ for some $m, k \in \mathbb{Z}$ since q_1, q_2 divide n. Thus, the result is still in S, hence by subgroup criterion this set is a subgroup of $\mathbb{Q}$.
3. The set of reflections of D_{2n} is not a subgroup, since as shown in tool 5, composition of two reflections can be a rotation, hence the set of reflections is not closed under composition.
4. This is not a subgroup. Consider $\sqrt{2}, \sqrt{3}$ in this group. They both square to rational numbers, but $(\sqrt{2}+\sqrt{3}) = 2+3+2\sqrt{2}\sqrt{3} = 5+2\sqrt{6}$, which is not a rational number as $\sqrt{6}$ is irrational. Therefore, this set is not closed under addition.
5. Let g be the element in G but not in H. Consider $< g >= \{g, g^2, g^3, \ldots\}$. Then, we know that this is a subgroup of G, and since G is finite, we know that the order of g is finite, namely m. However, we know that $g^2, g^3, \ldots \in H$, which means that $g^{2^{-1}} = g^{-2} \in H$ as H is a subgroup. Then, this means that either $m = 1$, i.e. $g = e \in H$, or $g^3 \cdot g^{-2} = g \in H$ as H is a subgroup, but both are impossible by our assumption. Therefore, we have reached a contradiction.
6. Suppose G is abelian, g, g' in the torsion subgroup. Then, we know that $|g| = m$, $|g'| = |g'^{-1}| = n$, and since G is abliean, we know that $(gg'^{-1})^{mn} = g^m(g'^{-1})^n = e$, thus $|gg'^{-1}| < \infty$, gg'^{-1} is in the torsion group.
7. Suppose $H \subset K$ or $K \subset H$, then we know that $H \cup K$ is either H, or K, which are both subgroups of G. Suppose $H \cup K$ is a subgroup of G, meaning that for all $h \in H, k \in K$, $hk^{-1} \in H \cup K$. Suppose $H \not\subset K$ and $K \not\subset H$, suppose $k \in K$ but $k \notin H$. Suppose $h \in H$ and $h \notin K$. Then, we know that $hk^{-1} \in H \cup K$, which means $hk^{-1} \in H$ or $hk^{-1} \in K$, but this gives either $k \in H$ or $h \in K$, which reaches a contradiction.
8. Suppose H is abliean, since $C_G(H)$ is a group, and we know that for all $h, h' \in H$, $hh' = h'h$, thus $H \leq C_G(H)$. Suppose $H \leq C_G(H)$, this means for all $h, h' \in H$, $hh' = h'h$, which exactly means H is abelian.

Tool 16: Cyclic Subgroups and Their Generators

Solution 1.22: Exercise 1.16

1. Finding all subgroups of Z_{45} is equivalent of finding factors of 45, as all cyclic subgroups must have order divisible by 45. Hence, we can find $< x >, < x^3 >, < x^5 >, < x^9 >, < x^{15} >, < e >$ as the subgroups.
2. Finding generators of $\mathbb{Z}/202\mathbb{Z}$ is equivalent of finding numbers that are coprime with 202, which can be every number from 1 to 201 except 2 and 101.
3. We know that $< e >$ is a cyclic group, and $< \rho >$ is another cyclic group of rotations. $< \rho^2 >$ is another cyclic group. Similarly, given any reflection r, the group $< r >$ is cyclic. Consider the two Type II reflections (reflection with diagonal axis) a, b and the group $\{e, a, b, \rho^2\}$. This group is not cyclic, but is a proper subgroup of D_8.
4. We know that $\mathbb{Z}/48\mathbb{Z} =< 1 >$, hence finding the integers a where ϕ_a extends to a homomorphism onto $_{36}$ is equivalent of finding a number a such that $x^{48a} = e$, thus we know that $36 \mid 48a$, hence $3 \mid a$, and we have $a = 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36$. Since none of the a's have greatest common divisor with 36 being 1, we know that none of the x^a's are generators of Z_{36}, hence this map is not surjective.
5. Suppose $\phi : \mathbb{Z} \to \mathbb{H}$ such that $\phi(1) = h \in H$. Then, we know that $\phi(a) = h^a$ for all $a \in \mathbb{Z}$ and $\phi(0) = e \in H$. Thus, ϕ is completely defined based on the condition $1 \mapsto h$, hence ϕ is unique.
6. Suppose $Z_n =< x >$. Then, we know that in order for this map to be bijective homomorphism, $\sigma_a(x) = x^a$ must also be a generator of Z_n, which only happens when (a, n) is 1. Similarly, if $(a, n) = 1$, we know that $\sigma_a(x) = x^a$ is bijective, what lefts is to show that σ_a is a homomorphism, which is straightforward as Z_n is cyclic.
7. For all $x \in Z_n$, $\sigma_a(\sigma_b(x)) = \sigma_a(x^b) = x^{ab}$ since σ_a, σ_b are homomorphisms. Therefore, $\sigma_a \circ \sigma_b = \sigma_{ab}$. Then, we first need to know that in order for $\phi : Z_n \to Z_n$ be an automorphism between cyclic groups $Z_n =< x >$, $\phi(x) = x^a$ for some a, hence $\phi = \sigma_a$ for some integer a, therefore, the group of automorphisms on Z_n is the set of σ_a for all $a \in \mathbb{Z}$. Next, consider $\psi(a) = \sigma_a$. Since $\psi(ab) = \sigma_{ab} = \sigma_a \circ \sigma_b$, we have shown that ψ is a homomorphism. Furthermore, from above, we know that every automorphism on Z_n is in the form of σ_x for some $x \in \mathbb{Z}$, hence equals to $\psi(x)$, and $\sigma_a \neq \sigma_b$ since they map differently on the generators for $a, b \in \mathbb{Z}/n\mathbb{Z}$, ψ is bijective. Thus, we know that ψ is an isomorphism.
8. Suppose G does not have any proper subgroup. Our first case is $G = \{e\}$. Next, suppose $x \in G, x \neq e$. Then, consider $< x >$, we must have $< x >= G$, hence G is cyclic. Suppose $|x| = n < \infty$, then we know that every element in $< x >$, namely x^a for some $a \in \mathbb{N}$ is a generator, thus $gcd(a, n) = 1$ for all $a < n$, which means n is a prime number. Suppose $|x| = \infty$, then we know that $< x^2 > \neq < x >$, since $x^{2a} \neq x$ for all $a \in \mathbb{Z}$ as $|x| = \infty$, and hence $< x^2 >$ is a proper subgroup of $< x >= G$, which is impossible. Hence $|x| \neq \infty$. Therefore, we know that G is either $\{e\}$ a cyclic group of prime order.

Tool 17: Cyclic or Not Cyclic?

Solution 1.23: Exercise 1.17

1. Firstly, consider $Z_2 \times Z_2$. Since $< (0,0 >= \{(0,0)\}$, $< (1,0) >= \{(1,0),(0,0)\}$, $< (0,1) >= \{(0,1),(0,0)\}$, and $< (1,1) >= \{(0,0),(1,1)\}$. We know that $Z_2 \times Z_2$ is not cyclic. Next, suppose $\mathbb{Z} \times \mathbb{Z}$ is cyclic, then we know that $< (a,b) >= \mathbb{Z} \times \mathbb{Z}$, thus $(a, b+1) = m(a,b) = (ma, mb)$, but then $m = 1$, $b+1 = b$, which is impossible.
2. We will show that $\mathbb{Z} \times Z_2$ is not cyclic. Suppose $\mathbb{Z} \times \mathbb{Z}_{\not=}$ is generated by a single element (a,b), then similar as above proof, we know that $(a+1,b)$ cannot be generated, hence this group is not cyclic. However, we know that $\mathbb{Z}$ is cyclic, and hence $\mathbb{Z} \times Z_2$ is not isomorphic to $\mathbb{Z}$.
3. Suppose $\mathbb{Q} \times \mathbb{Q}$ is cyclic, then it is generated by $(\frac{p}{q}, \frac{p'}{q'})$. Hence, we know that $(\frac{p+1}{q}, \frac{p'}{q'}) = m(\frac{p}{q}, \frac{p'}{q'})$, however $m = 1$, but $p \neq p+1$, hence this is not possible.
4. Suppose a is a generator of $(\mathbb{Z}/2^n\mathbb{Z})^\times$. Firstly, if a is odd, then we know that a^n is odd for all $n \in \mathbb{Z}$, thus 2 is not generated by a. If a is even, then we know that a^n is even for all $n \in \mathbb{Z}$, and thus 1 is not generated by a. Therefore, $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic.

Tool 18: Understanding Groups from Generators

Solution 1.24: Exercise 1.18

1. Firstly, since H is a subgroup of G, H is closed under group operation. Thus, $H =< H >$. Next, Since $H \neq \{1\}$, we can pick $h \neq 1 \in < H - \{1\} >$, and hence $h^{-1} \in < H - \{1\} >$, and $hh^{-1} = 1 \in < H - \{1\} >$, therefore, $< H - \{1\} >=< H >= H$.
2. Firstly, we know that $(12)(13)(24) = (1324)$, hence we have an element of order 4, which can correspond to a rotation. The next thing is to find a reflection. Since we have $(1324)(12) = (14)(32)$ and $(12)(1423) = (14)(23) = (14)(32)$, we know that $(1324)(12) = (12)(1324)^{-1}$, which satisfies $D_8 =< r, s : rs = sr^{-1} >$.
3. Suppose $\mathbb{Q}$ is finitely generated, namely the generators are $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$ and are in lowest terms. Let $d = lcm(q_1, \ldots, q_n) = p_1 \cdots p_k$ for some primes $p_1, \ldots, p_k$. Let $e = d + 1$, then we know that for all $x \in < \frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n} >$, x can be written as $\frac{m}{d}$ for some $m \in \mathbb{Z}$, however, suppose $\frac{m}{d} = \frac{1}{d+1}$, then we know that $m(d+1) = d$, thus $d+1 \mid d$, which means $d = 0$. Hence we have a contradiction.

Tool 19: Normal Subgroups

Solution 1.25: Exercise 1.19

1. For all $h \in H, k \in K$, we know that $hkh^{-1} \in K$. Consider $x \in G$, $m \in \phi^{-1}(K)$, we know that $\phi(xmx^{-1}) = \phi(x)\phi(m)\phi(x)^{-1} \in K$ since $\phi(m) \in K$, $\phi(x) \in H$. Therefore, $xmx^{-1} \in \phi^{-1}(K)$.
2. Consider $x \in N \cap H$, $h \in H$, then we know that $hxh^{-1} \in H$ since H is a subgroup of G, also $hxh^{-1} \in N$ since $N \trianglelefteq G$, therefore $hxh^{-1} \in N \cap H$, and $N \cap H \trianglelefteq H$.
3. If $gNg^{-1} = N$, then $gNg^{-1} \subset N$ this is just trivial. Suppose $gNg^{-1} \subset N$. Consider the map $f : N \to N$ such that $f(x) = gxg^{-1}$. Firstly, since that $gxg^{-1} = gyg^{-1}$ means $x = y$, we know that f is injective. Then, this means f is surjective as f maps N to N. Thus, $gNg^{-1} = f(N) = N$.
4. If $g \in N_G(N)$, then we know that for all $n \in N$, $gng^{-1} \in N$, i.e. $gNg^{-1} \subset N$, hence $gNg^{-1} = N$, $gN = Ng$. If $gN = Ng$, we know that $gNg^{-1} = N$l hence $g \in N_G(N)$.
5. Suppose $A \in GL_n(F)$, $X \in SL_n(F)$, then we know that $AXA^{-1} \in GL_n(F)$ and $\det(AXA^{-1}) = \det(A)\det(X)\det(A^{-1}) = \det(X) = 1$, hence $AXA^{-1} \in SL_n(F)$. Thus, $SL_n(F) \trianglelefteq GL_n(F)$.
6. For any $g \in G$, we know that $g(x^{-1}y^{-1}xy)g^{-1} = (gx^{-1}g^{-1})(g(y^{-1})g^{-1})(gxg^{-1})(gyg^{-1}) = (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) \in < x^{-1}y^{-1}xy : x, y \in G >$. Thus, we know that $g(x^{-1}y^{-1}xy)g^{-1}$ is still in the commutator for all $g, x, y \in G$. Then, it remains to show that if we have generators $x_1, \dots$ for a group N, as long as for all $g \in G$, $gx_ig^{-1} \in N$, N is normal. In fact, we can show that for all $n \in N$, $n = \prod_{i=1} x_i^{a_i}$, hence $gng^{-1} = \prod_{i=1}(gx_ig^{-1})^{a_i} \in N$, thus N is normal. THerefore, since we have already shown that $g(x^{-1}y^{-1}xy)g^{-1}$ is still in the commutator for all $g, x, y \in G$, the commutator subgroup is normal in G.
7. Given $x \in H, y \in K$, we know that $x^{-1}y^{-1}xy = x^{-1}(y^{-1}xy) \in H$, and $x^{-1}y^{-1}xy = (x^{-1}y^{-1}x)y \in K$, thus $x^{-1}y^{-1}xy = 1$, $xy = yx$.

Tool 20: Cosets and Lagrange

Solution 1.26: Proof of Theorem 1.21

Since G is abelian, we know that for all $g \in G$, $h \in H$, $gh = hg \in Hg$, thus $gH \subset Hg$. Similarly, $hg = gh \in gH$, $Hg \subset gH$, hence $gH = Hg$.

Solution 1.27: Exercise 1.20

1. Suppose $x \in G \setminus H$. Consider the left coset xH, since $x \notin H$, this is different as H, hence xH, H partition G by Lagrange Theorem. Similarly, right cosets Hx, H partition G, thus $xH = Hx = G \setminus H$ for all $x \in G \setminus H$. For all $x \in H$, $xhx^{-1} \in H$ for all $h \in H$, therefore, $H \trianglelefteq G$.
2. Since $|H||13$, we know that $H = \{e\}$ or $H = G$.
3. Suppose G is a group with order being a power of p, namely p^k. Suppose $x \in G$. If $G = \{e\}$, $|G| = p^0$, but G does not have an element of order p. However, if $G \neq \{e\}$, suppose $x \neq e$. Consider $< x >$. We know that $| < x > | = |x||p^k$. Also we know that $x \neq e$, so $|x| = p^m$ for some $1 \leq m \leq k$. Thus, consider $| < x^{p^{m-1}} > |$, we know that $|x^{p^{m-1}}| = | < x^{p^{m-1}} > | = p$.
4. Let G be a group of order 35. Pick $x \in G$ such that $x \neq e$, consider $< x >$. We know that $| < x > | = |x| \mid 35$ and $|x| \neq 1$, hence $|x| = 5$ or 7 or 35. If $|x| = 35$, $|x^7| = 5$, $|x^5| = 7$. If $|x| = 7$, suppose there are no elements of order 5 (or 35 since otherwise we already have an element of order 5), then we know that we have subgroups of cardinality 7. However, 7 is a prime, meaning that these groups do not have proper subgroups. Hence we know that we can find several order 7 subgroups that intersect trivially but union to G. However, this would mean $35 = 6n + 1$ for n being the number of order 7 subgroups, which is impossible. If $|x| = 5$, suppose there are no elements of order 7 (or 35 since otherwise we already have an element of order 7), then we know that we have subgroups of cardinality 5. However, 5 is a prime, meaning that these groups do not have proper subgroups. Hence we know that we can find several order 7 subgroups that intersect trivially but union to G. However, this would mean $35 = 6n + 1$ for n being the number of order 7 subgroups, which is impossible.
5. Since we know that $H \cap K \subset H, K$ and $H \cap K$ is closed under group operation with identity, we know that $H \cap K$ is a subgroup of both H and K. Thus, $|H \cap K| \mid |H|$ and $|H \cap K| \mid |K|$, however this means $|H \cap K| = 1$, hence $H \cap K = 1$.
6. Let this map be ϕ. Given coset xH, suppose $xh \in xH$, then we know that $(xh)^{-1} = h^{-1}x^{-1} \in Hx^{-1}$. Thus, $\phi(xH) \subset Hx^{-1}$, and we know that $(hx^{-1})^{-1} = xh^{-1} \in xH$, $\phi^{-1}(Hx^{-1}) = \phi(Hx^{-1}) \subset \phi(xH)$. Hence, $\phi(xH) = Hx^{-1}$, hence ϕ maps a left coset to a right coset. Since ϕ is a bijection by definition, it gives a bijection between left and right cosets.
7. Firstly since $N \trianglelefteq G$, we would like to show that the set of cosets is a group itself. Firstly, for g_1N, g_2N where $g_1, g_2 \in G$, we find that $g_1N \cdot g_2N = g_1g_2(g_2)^{-1}Ng_2N = (g_1g_2)(g_2^{-1}Ng_2)N = g_1g_2N$. Thus, the group associativity for G still holds here, and we have $eN = N$ as the identity. This group has order n since $[G : N] = n$. Consider $h \in H$, and $|hN| = |N|$, suppose for some h, $hN \neq N$, then $h \neq e$. Then, we know that $hN \cap N = \emptyset$. Then, firstly $| < h > | \mid m$, then $h^mN \neq hN$ for all $1 < m \leq |h|$, thus $\{N, hN, h^2N, \ldots\}$ is a subgroup of the set of cosets. Thus, $| < h > | = |h| \mid n$, which suggests $|h| = 1$, $h = e$, but this is impossible. Hence, for all $h \in H$, $hN = N$, which means for all $h \in H$, $he = h \in N$, $H \leq N$.
8. For any a relatively prime to n, consider the subgroup $< a >$. Then we know that $| < a > | \mid |\mathbb{Z}/n\mathbb{Z}^\times| = \phi(n)$, by definition of Euler's totient function. Thus, $a^{\phi(n)} \equiv 1(\mod n)$.