Solutions to Dummit and Foote's *Abstract Algebra*

Written by
James Ha

Contents

Chapter 2

Subgroups

2.1 Definition and Examples

1. (a) Clearly, this subset is not empty, since it contains $0 = 0 + 0i$. In addition, for any two elements $a + ai, b + bi$ in this subset, we have $(a + ai) + (-b - bi) = (a - b) + (a - b)i$ is also in this subset. Therefore this subset is a subgroup of $\mathbb{C}$.

1. (b) Let $H = \{z \in \mathbb{C} \mid |z| = 1\}$. H is clearly not empty since it contains 1. In addition, notice that for any $z \in H$, we have $|z^{-1}| = |z||z^{-1}| = |zz^{-1}| = 1$. So, for any $z_1, z_2 \in H$, we have $|z_1 z_2^{-1}| = |z_1||z_2^{-1}| = 1$ so $z_1 z_2^{-1} \in H$. H is therefore a subgroup of $\mathbb{C} \setminus \{0\}$.

1. (c) Name this subset H. H is not empty since $\frac{1}{n}$ is in H. In addition, for any two elements $\frac{a}{b}, \frac{c}{d} \in H$, with $n = \alpha b = \beta d$, we have $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd} = \frac{\alpha\beta ad - \alpha\beta bc}{\alpha\beta bd} = \frac{\alpha a - \beta c}{n}$ is also an element of H. Therefore, H is a subgroup of $\mathbb{Q}$.

1. (d) Name this subset H. H cannot be empty because 1 is coprime to every positive integer, so H contains all integers. In addition, for any two elements $\frac{a}{b}, \frac{c}{d} \in H$, we have $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}$ is also in H, since if $(b, n) = (d, n) = 1$, then $(bd, n) = 1$. Hence, H is a subgroup of $\mathbb{Q}$.

1. (e) Name this subset H. H cannot be empty, since 1 is in H. Furthermore, for any two elements $x, y \in H$, we have $(xy^{-1})^2 = x^2y^{-2}$ is an element of H since $\mathbb{Q} \setminus \{0\}$ is closed under division. It follows that H is a subgroup of $\mathbb{R} \setminus \{0\}$.

2. (a) This set is not closed under the group operation (e.g., $(1\ 2)(1\ 3) = (1\ 3\ 2)$) and so it cannot be a subgroup.

2. (b) This set is not closed under the group operation (e.g., $(sr)(sr^2) = s^2r = r$) and so it cannot be a subgroup.

2. (c) This set is not closed under the group operation (e.g., if a satisfies $a|n$, x^a cannot be in this subset) and so it cannot be a subgroup.

2. (d) This set is not closed under the group operation, since the sum of any two odd integers is an even integer. So, it cannot be a subgroup.

2. (e) This set is not closed under the group operation, since $\sqrt{2}, \sqrt{3}$ are in this subset, yet $\sqrt{2} + \sqrt{3}$ is not ($(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$).

3. (a) Since all of these elements are their own inverses, it suffices to show that the product of any two elements in this subset is also in this subset. We exclude products with the identity, since these are obviously in the subset. The products are as follows:

$$r^2s = sr^2 \quad r^2sr^2 = s \quad ssr^2 = r^2 \quad sr^2r^2 = s \quad sr^2s = r^2$$

All of these are in the subset, so this subset is a subgroup of D_8.

3. (b) Again, these elements are their own inverses. The products are as follows:

$$r^2sr = sr^3 \quad r^2sr^3 = sr = sr^3r^2 \quad srsr^3 = r^2 = sr^3sr$$

Thus, this subset is a subgroup of D_8.

4. $\mathbb{Z}$ is a group under addition, but the infinite subset $\mathbb{Z}^+$ is not a subgroup because it does not contain the identity element and it is not closed under inverses.

5. Assume there is such a subgroup H. Let $y \in G$ be the unique element satisfying $y \notin H$ and let $x \in H$ be any non-identity element. Then $x, x^{-1}y \in H$ but their product $x(x^{-1}y) = y$ is not. Thus, H is not a subgroup, which is a contradiction. We conclude that no such H exists.

6. Let $H = \{g \in G \mid |g| < \infty\}$. H cannot be empty, since the identity element is order 1. Consider any two elements $g, h \in H$ with $|g| = n$ and $|h| = m$. Then $(gh^{-1})^{nm} = g^{nm}h^{-nm} = 1^m1^n = 1$, so $gh^{-1} \in H$. It follows that H is a subgroup of G.

This proof does not hold for the non-abelian group $G = \langle r, s \mid r^n = s^m = 1 \rangle$ since r, s are of finite order, but rs has infinite order.

7. The torsion subgroup is $\{(a, \overline{b}) \in \mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z}) \mid a = 0\}$. Consider $(1, \overline{b}), (-1, \overline{c}) \in \mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$, where $\overline{b} + \overline{c} \neq \overline{0}$. These two elements are of infinite order, but $(1, \overline{b}) + (-1, \overline{c}) = (0, \overline{b} + \overline{c})$ is a non-identity element of finite order. Thus, the set of elements of infinite order together with the identity is not a subgroup of this direct product.

8. Assume without loss of generality that $H \subseteq K$. Then $H \cup K = K$ so $H \cup K \leq G$.

Assume there exists $H \cup K \leq G$ such that $H \nsubseteq K$ and $K \nsubseteq H$. Consider any $h \in H \setminus K$ and any $k \in K \setminus H$. Observe that $hk \notin H \cup K$. For if it were, then $hk \in H$ or $hk \in K$. But $hk \in H$ implies $k \in H$ (since $h^{-1}(hk) = k$) and $hk \in K$ implies $h \in K$ (since $(hk)k^{-1} = h$). Clearly, this is impossible, so $hk \notin H \cup K$. Therefore, $H \cup K$ is not closed under the group operation. We have $H \cup K \nleq G$, which is a contradiction. So, no such $H \cup K$ exists.

9. $SL_n(F)$ clearly contains the identity I. $SL_n(F)$ is closed under the group operation, since $\det(AB) = \det(A)\det(B)$ for all $A, B \in GL_n(F)$. $SL_n(F)$ is also closed under inverses, since $\det(A^{-1}) = \det(A)^{-1}$ for all $A \in GL_n(F)$. Thus, $SL_n(F) \leq GL_n(F)$.

10. (a) $H \cap K$ must contain 1, since H and K are subgroups. For any element $a \in H \cap K$, we have $a \in H$ and $a \in K$ so that $a^{-1} \in H$ and $a^{-1} \in K$. It follows that $a^{-1} \in H \cap K$. For any two elements $a, b \in H \cap K$, we have $a, b \in H$ and $a, b \in K$. Therefore, $ab \in H$ and $ab \in K$ so $ab \in H \cap K$. Thus, $H \cap K \leq G$.

10. (b) Note that the intersection must contain the identity since all subgroups contain the identity. Any element a in the intersection must be in all of the subgroups of the collection. All of the subgroups must therefore contain a^{-1}, from which it follows that the intersection contains a^{-1}. Any two elements a, b in the intersection must be in all of the subgroups of the collection. All of the subgroups must therefore contain ab, from which it follows that ab is in the intersection. Thus, the intersection must also be a subgroup of G.

11. (a) Name this subset H. H is not empty, since $(1, 1) \in H$. For any two elements $(a, 1), (b, 1) \in H$, we have $(a, 1)(b, 1)^{-1} = (a, 1)(b^{-1}, 1) = (ab^{-1}, 1)$ is also in H. Therefore $H \leq A \times B$.

11. (b) The argument that this subset is a subgroup of $A \times B$ is nearly identical to the one in Exercise 11.(a).

11. (c) Name this subset H. H is not empty, since $(1,1) \in H$. For any two elements $(a,a),(b,b) \in H$, we have $(a,a)(b,b)^{-1} = (a,a)(b^{-1},b^{-1}) = (ab^{-1},ab^{-1})$ is also in H. Thus, $H \leq A \times A$.

12. (a) Name this subset H. H is not empty, since $1^n = 1$ is in H. For any two elements $a^n, b^n \in H$, we have $a^n b^{-n} = (ab^{-1})^n$ is also in H. Thus, $H \leq A$.

12. (b) Name this subset H. H is not empty since 1 is in H. For any two elements $a, b \in H$, we have $(ab^{-1})^n = a^n b^{-n} = 1$, so $ab \in H$. Thus, $H \leq A$.

13. It suffices to show that if H is a subgroup with this property and $H \neq \{0\}$, then $H = \mathbb{Q}$. So let $H \neq \{0\}$ and suppose $H \neq \mathbb{Q}$. Consider any non-zero $h \in H$ and $q \in \mathbb{Q} \setminus H$. $\exists a,b,c,d \in \mathbb{Z}$ such that $(a,b) = (c,d) = 1$ and $h = \frac{a}{b}$, $q = \frac{c}{d}$. Given H's special property, $\frac{1}{h} \in H$. H must be closed under the group operation, so $a = bh$ and $b = \frac{a}{h}$ must be elements of H. Since $(a,b) = 1$, it follows that $1 \in H$, and therefore, so is all of $\mathbb{Z}$. But this implies that $\frac{1}{d} \in H$, and by closure under addition, so is q. This is a contradiction, so $H = \mathbb{Q}$ and we have the claim.

14. $|s| = |sr| = 2$, but $s(sr) = r$. Since $|r| \geq 3$, this set is not closed under the group operation. It cannot be a subgroup of D_{2n}.

15. Let $H = \bigcup_{i=1}^{\infty} H_i$. Since every subgroup contains the identity, H must also contain the identity, and is therefore non-empty. It is clear that for any element $h \in H$, $\exists N \in \mathbb{Z}^+$ such that $\forall n \geq N$, $h \in H_n$. Since $h \in H_N$, it follows that $h^{-1} \in H_N$ and therefore, $h^{-1} \in H$. Now consider any two $g, h \in H$. Let $N, M \in \mathbb{Z}^+$ be such that $\forall n \geq N$, $h \in H_n$ and $\forall n \geq M$, $g \in H_n$. Then $g, h \in H_{N+M}$ and therefore, $gh \in H_{N+M}$. It follows that $gh \in H$. Hence, $H \leq G$.

16. Name this subset H. Consider the product AB of any two elements $A, B \in H$. Note that the $(i,j)^{th}$ entry of AB is given by $(AB)_{ij} = \sum_k A_{ik}B_{kj}$. However, for $k < i$, $A_{ik} = 0$, and for $k > j$, $B_{kj} = 0$. So, $(AB)_{ij} = \sum_{i \leq k \leq j} A_{ik}B_{kj}$. If $i > j$, there is no non-zero term in this sum, so $(AB)_{ij} = 0$ for all $i > j$. This shows that H is closed under the group operation. Now, consider the matrix A^{-1} for any $A \in H$. We will show that $A^{-1}_{ij} = 0$ if $i > j$. For $j = 1$, we have $(A^{-1}A)_{i1} = \sum_{k \leq 1} A^{-1}_{ik}A_{k1} = A^{-1}_{i1}A_{11}$. But $A^{-1}A = I$, so $A^{-1}_{i1} = 0$ for all $i > 1$. Suppose this holds for all $j < \ell$ where $\ell > 1$. Then for $j = \ell$, we have $(A^{-1}A)_{i\ell} = \sum_{k \leq \ell} A^{-1}_{ik}A_{k\ell}$. From the inductive assumption, we have that $A^{-1}_{ik} = 0$ if $i > k$ for all $k < \ell$. Thus, for all $i > \ell$, $(A^{-1}A)_{i\ell} = A^{-1}_{i\ell}A_{\ell\ell}$. But $A^{-1}A = I$, so $A^{-1}_{i\ell}A_{\ell\ell} = 0$. Since $A_{\ell\ell} \neq 0$, it follows that $A^{-1}_{i\ell} = 0$. By induction on j, the claim holds. This implies that A^{-1} is in H. Therefore, $H \leq GL_n(F)$.

17. Name this subset H. Drawing on the work from Exercise 16, we just need to show that $(AB)_{ii} = A_{ii}^{-1} = 1$ for all i and any $A, B \in H$. So consider the product of any two elements $A, B \in H$. We have $(AB)_{ii} = \sum_k A_{ik}B_{ki}$ for all i. But since $A_{ik} = 0$ for all $k < i$ and $B_{ki} = 0$ for all $k > i$, we have $(AB)_{ii} = A_{ii}B_{ii} = 1$ for all i. Thus, H is closed under the group operation. Now consider A^{-1}. We already know from Exercise 16 that A^{-1} is upper triangular. Thus, $(AA^{-1})_{ii} = \sum_k A_{ik}A_{ki}^{-1} = A_{ii}A_{ii}^{-1}$. But since $AA^{-1} = I$, we must have $A_{ii}A_{ii}^{-1} = A_{ii}^{-1} = 1$ for all i. Thus, H is closed under inverses. It follows that $H \leq GL_n(F)$.

2.2 Centralizers and Normalizers, Stabilizers and Kernels

1. The centralizer $C_G(A)$ is the set $\{g \in G \mid gag^{-1} = a, \forall a \in A\}$. But if g satisfies $a = gag^{-1}$ for all $a \in A$, then $g^{-1}ag = g^{-1}gag^{-1}g = a$ for all $a \in A$. Similarly, if $a = g^{-1}ag$ for all $a \in A$, then $gag^{-1} = gg^{-1}agg^{-1} = a$ for all $a \in A$. Thus, $C_G(A) = \{g \in G \mid g^{-1}ag = a, \forall a \in A\}$.

2. We have $C_G(Z(G)) = \{g \in G \mid gzg^{-1} = z, \forall z \in Z(G)\}$. For any element $g \in G$, we have $gz = zg$ for all $z \in Z(G)$ by definition of $Z(G)$. But if $gz = zg$ for all $z \in Z(G)$, then $gzg^{-1} = z$ for all $z \in Z(G)$. Therefore, $G \subseteq C_G(Z(G))$. Since $C_G(Z(G)) \subseteq G$ by definition, we have $C_G(Z(G)) = G$.

3. Note that for any $g \in C_G(B)$, we must have $g \in C_G(A)$, since g satisfies $gbg^{-1} = b$ for all $b \in B$ and $A \subseteq B$. So, $C_G(B) \subseteq C_G(A)$. $C_G(B)$ cannot be empty because it must contain the identity. In addition, for any two elements $g, h \in C_G(B)$, the product gh^{-1} satisfies $gh^{-1}b(gh^{-1})^{-1} = gh^{-1}bhg^{-1} = gbg^{-1} = b$ for all $b \in B$, so $gh^{-1} \in C_G(B)$. Thus, $C_G(B) \leq C_G(A)$.

4. We start with S_3:

$$C_{S_3}(\{1\}) = S_3 \quad C_{S_3}(\{(1\,2)\}) = \{1, (1\,2)\} \quad C_{S_3}(\{(1\,3)\}) = \{1, (1\,3)\}$$

$$C_{S_3}(\{(2\,3)\}) = \{1, (2\,3)\} \quad C_{S_3}(\{(1\,2\,3)\}) = \{1, (1\,2\,3), (1\,3\,2)\}$$

$$C_{S_3}(\{(1\,3\,2)\}) = \{1, (1\,2\,3), (1\,3\,2)\} \quad Z(S_3) = \{1\}$$

Next we examine D_8:

$$C_{D_8}(\{1\}) = D_8 \quad C_{D_8}(\{r\}) = \{1, r, r^2, r^3\} \quad C_{D_8}(\{r^2\}) = D_8 \quad C_{D_8}(\{r^3\}) = \{1, r, r^2, r^3\}$$

$$C_{D_8}(\{s\}) = \{1, r^2, s, sr^2\} \quad C_{D_8}(\{sr\}) = \{1, r^2, sr, sr^3\} \quad C_{D_8}(\{sr^2\}) = \{1, r^2, s, sr^2\}$$

$$C_{D_8}(\{sr^3\}) = \{1, r^2, sr, sr^3\} \quad Z(D_8) = \{1, r^2\}$$

Finally, for Q_8, we have:

$$C_{Q_8}(\{1\}) = Q_8 \quad C_{Q_8}(\{-1\}) = Q_8 \quad C_{Q_8}(\{i\}) = \{1, -1, i, -i\} \quad C_{Q_8}(\{-i\}) = \{1, -1, i, -i\}$$

$$C_{Q_8}(\{j\}) = \{1, -1, j, -j\} \quad C_{Q_8}(\{-j\}) = \{1, -1, j, -j\} \quad C_{Q_8}(\{k\}) = \{1, -1, k, -k\}$$

$$C_{Q_8}(\{-k\}) = \{1, -1, k, -k\} \quad Z(Q_8) = \{1, -1\}$$

5. (a) Drawing on the results of Exercise 4, we find that $C_{S_3}(A) = A$. Next, note that since $C_{S_3}(A) \leq N_{S_3}(A)$ and $|A| = 3$, by Lagrange's theorem, either $N_{S_3}(A) = A$ or $N_{S_3}(A) = S_3$. Since $(1\,2)(1\,2\,3)(1\,2) = (2\,3)(1\,2) = (1\,3\,2)$ and $(1\,2)(1\,3\,2)(1\,2) = (1\,2)(2\,3) = (1\,2\,3)$, we have $N_{S_3}(A) = S_3$.

5. (b) Drawing on the results of Exercise 4, we find that $C_{D_8}(A) = A$. Again, since $C_{D_8}(A) \leq N_{D_8}(A)$ and $|A| = 4$, by Lagrange's theorem, we have either $N_{D_8}(A) = A$ or $N_{D_8}(A) = D_8$. Since $rsr^{-1} = sr^{-2} = sr^2$, $rr^2r^{-1} = r^2$, and $rsr^2r^{-1} = s$, we find that $N_{D_8}(A) = D_8$.

5. (c) All powers of r commute with each other, so $A \leq C_{D_{10}}(A)$. By Lagrange's theorem, either $C_{D_{10}}(A) = A$ or $C_{D_{10}}(A) = D_{10}$. Since $srs = r^{-1} \neq r$, we have $C_{D_{10}}(A) = A$. Lagrange's theorem allows us to determine that either $N_{D_{10}}(A) = A$ or $N_{D_{10}}(A) = D_{10}$. Since $srs = r^4$, $sr^2s = r^3$, $sr^3s = r^2$, and $sr^4s = r$, we have $N_{D_{10}}(A) = D_{10}$.

6. (a) Consider any element $g \in H$. We will show that $gHg^{-1} = H$. First, pick any element $h \in H$. We have $g^{-1}hg \in H$, since H is a group. It follows that gHg^{-1} contains the element $g(g^{-1}hg)g^{-1} = h$, so $H \subseteq gHg^{-1}$. But H is closed under its group operation, so $gHg^{-1} \subseteq H$. Therefore, $H = gHg^{-1}$ and $g \in N_G(H)$. We conclude that $H \leq N_G(H)$.

This is not true if H is merely a subset of G. Take, for example, the subset $\{1, r, s\}$ of D_8. The normalizer of this subset is $N_{D_8}(\{1, r, s\}) = \{1, r^2\}$, and $\{1, r, s\}$ is not even a subset of its normalizer.

6. (b) If H is abelian, then for any element $g \in H$, we have $gh = hg$ for all $h \in H$. This implies that $ghg^{-1} = h$ for all $h \in H$. Therefore, $H \leq C_G(H)$.

If $H \leq C_G(H)$, then for any element $g \in H$, $ghg^{-1} = h$ for all $h \in H$. This implies that $gh = hg$ for all $h \in H$. Therefore, H must be abelian.

7. (a) First, we show that an element of the form sr^i cannot be in $Z(D_{2n})$. If there were such an element in $Z(D_{2n})$, then we would require $sr^ir = rsr^i$. Since $sr^ir = sr^{i+1}$ and $rsr^i = sr^{i-1}$, it must be that $sr^{i+1} = sr^{i-1}$. This can only be true if $sr^2 = s$. But $n \geq 3$ so $sr^2 \neq s$. Therefore, no such element exists in $Z(D_{2n})$, which contains only powers of r.

Since powers of r commute with each other, to prove that a specific power r^k is in $Z(D_{2n})$, it suffices to show that it commutes with all elements of the form sr^i. For r^k to be an element of $Z(D_{2n})$, it must satisfy $sr^ir^k = r^ksr^i$ for all $i \in \mathbb{Z}$. That is, it must satisfy $s = sr^{2k}$. It follows that $n|2k$. But if n is odd, n must divide k. Therefore, $r^k = 1$ and $Z(D_{2n}) = \{1\}$.

7. (b) We draw on the work for Exercise 7.(a). If n is even, then $2k$ can be any multiple of n. This allows the new possibility $2k = n$, so we have $Z(D_{2n}) = \{1, r^k\}$ where $n = 2k$.

8. First, note that G_i is not empty, since every stabilizer contains id. Consider any two elements $\sigma, \tau \in G_i$. It is obvious that $\tau^{-1}(i) = \tau^{-1}(\tau(i)) = i$. Since the action of G on $\{1, ..., n\}$ is a group action, we have $(\sigma \circ \tau^{-1}) \cdot i = \sigma \cdot (\tau^{-1} \cdot i) = \sigma \cdot i = i$. Therefore, $\sigma \circ \tau^{-1} \in G_i$ as well. We may conclude that $G_i \leq G$. If we require that i be fixed, that leaves us $n - 1$ elements of $\{1, ..., n\}$ that we can freely permute. It is therefore easy to see that $|G_i| = (n-1)!$.

9. Note that $N_H(A) \subseteq H$ by definition. Let h be any element of $N_H(A)$. Then $hAh^{-1} = A$. Since $H \leq G$, $h \in G$. It follows that $h \in N_G(A)$. Since $N_H(A) \subseteq H$ and $N_H(A) \subseteq N_G(A)$, we find that $N_H(A) \subseteq N_G(A) \cap H$. Next consider any element $g \in N_G(A) \cap H$. By definition, $g \in H$ and $g \in N_G(A)$. Since $gAg^{-1} = A$ and $g \in H$, necessarily, $g \in N_H(A)$. So, $N_G(A) \cap H \subseteq N_H(A)$. We conclude that $N_H(A) = N_G(A) \cap H$.

10. If H is a subgroup of order two, there is exactly one non-identity element of H. Call this element h. For any $g \in N_G(H)$, we must have $\{g1g^{-1}, ghg^{-1}\} = \{1, h\}$. But since $g1g^{-1} = 1$ for all $g \in G$, this means that g must satisfy $ghg^{-1} = h$. Since $gxg^{-1} = x$ for all $x \in H$, we have $g \in C_G(H)$ and therefore, $N_G(H) \leq C_G(H)$. It was shown in the text that $C_G(H) \leq N_G(H)$, so we have $N_G(H) = C_G(H)$.

If $N_G(H) = G$, then $C_G(H) = G$ and every $g \in G$ satisfies $ghg^{-1} = h$ for all $h \in H$. In other words, for each $h \in H$, $gh = hg$ for all $g \in G$. Therefore, if $h \in H$, then $h \in Z(G)$. It follows that $H \leq Z(G)$.

11. Let A be any subset of G, and consider any element $z \in Z(G)$. Since $zg = gz$ for all $g \in G$ and A is a subset of G, we must have $z \in C_G(A)$. So, $Z(G) \leq C_G(A)$. It was shown in the text that $C_G(A) \leq N_G(A)$. By transitivity of $\leq$, we find that $Z(G) \leq N_G(A)$.

12. (a) We have:

$$\sigma \cdot p = 12x_1x_2^5x_3^7 - 18x_3^3x_4 + 11x_1^{23}x_2^6x_3x_4^3$$

$$\tau \cdot (\sigma \cdot p) = 12x_1^7x_2x_3^5 - 18x_1^3x_4 + 11x_1x_2^{23}x_3^6x_4^3$$

$$(\tau \circ \sigma) \cdot p = 12x_1^7x_2x_3^5 - 18x_1^3x_4 + 11x_1x_2^{23}x_3^6x_4^3$$

$$(\sigma \circ \tau) \cdot p = 12x_1x_3^5x_4^7 - 18x_2x_4^3 + 11x_1^{23}x_2^3x_3^6x_4$$

12. (b) Consider any two elements $\sigma, \tau \in S_4$ and any $p \in R$. We have $\sigma \cdot (\tau \cdot p(x_1, x_2, x_3, x_4)) = \sigma \cdot p(x_{\tau(1)}, x_{\tau(2)}, x_{\tau(3)}, x_{\tau(4)}) = p(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, x_{\sigma(\tau(3))}, x_{\sigma(\tau(4))}) = p(x_{\sigma\circ\tau(1)}, x_{\sigma\circ\tau(2)}, x_{\sigma\circ\tau(3)}, x_{\sigma\circ\tau(4)}) = (\sigma \circ \tau) \cdot p(x_1, x_2, x_3, x_4)$. In addition, $\mathrm{id} \cdot p(x_1, x_2, x_3, x_4) = p(x_{\mathrm{id}(1)}, x_{\mathrm{id}(2)}, x_{\mathrm{id}(3)}, x_{\mathrm{id}(4)}) = p(x_1, x_2, x_3, x_4)$. So, these definitions give a group action of S_4 on R.

12. (c) These are the permutations that fix 4. They are id, $(1\ 2)$, $(1\ 3)$, $(2\ 3)$, $(1\ 2\ 3)$, $(1\ 3\ 2)$. These are exactly the permutations of S_3, so they obviously satisfy the group axioms. Call this subgroup G, and note that the homomorphism $\varphi : S_3 \to G$ defined by $\varphi(\sigma) = \sigma$ is a bijection. Thus, this subgroup is isomorphic to S_3.

12. (d) A permutation that stabilizes $x_1 + x_2$ either fixes both 1 and 2, or sends 1 to 2 and vice versa. These permutations are id, $(1\ 2)$, $(3\ 4)$, $(1\ 2)(3\ 4)$. It is easy to see that this subset is closed under the group operation and under inverses (every element is order 2), so this subset must be a subgroup of S_4 of order 4. It is also obvious that every element commutes with every other element, so this subgroup is abelian.

12. (e) These permutations are id, $(1\ 2)$, $(3\ 4)$, $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$, $(1\ 3\ 2\ 4)$, $(1\ 4\ 2\ 3)$. The stabilizer of $x_1x_2 + x_3x_4$ in S_4 is a subgroup of S_4 as proven in the text. Call this stabilizer S. Now, note that $|(1\ 3)(2\ 4)| = 2$, $|(1\ 4\ 2\ 3)| = 4$, and $(1\ 4\ 2\ 3)(1\ 3)(2\ 4) = (1\ 3)(2\ 4)(1\ 3\ 2\ 4) = (1\ 3)(2\ 4)(1\ 4\ 2\ 3)^{-1}$. So, $(1\ 3)(2\ 4)$ and $(1\ 4\ 2\ 3)$ satisfy the same relations as $r, s \in D_8$. Thus, there is a unique homomorphism $\varphi : D_8 \to S$. It is easy to see that $(1\ 3)(2\ 4)$ and $(1\ 4\ 2\ 3)$ generate S. Simply note that $(1\ 4\ 2\ 3)(1\ 3)(2\ 4) = (3\ 4)$, $(1\ 3)(2\ 4)(1\ 4\ 2\ 3) = (1\ 2)$, $(1\ 4\ 2\ 3)^3 = (1\ 3\ 2\ 4)$, and $(1\ 3\ 2\ 4)(1\ 2) = (1\ 4)(2\ 3)$. So, φ is a surjection, and since $|D_8| = |S|$, φ is a bijection. This means that φ is an isomorphism, and $S \cong D_8$.

12. (f) It is easy to realize that these permutations are identical to those listed in Exercise 12.(e).

13. The proof is almost identical to the one in Exercise 12.(b).

14. Consider any element $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ in $Z(H(F))$. For all $B \in H(F)$, A must satisfy

$$\begin{aligned} AB &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a+d & e+b+af \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a+d & e+b+dc \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \\ &= BA \end{aligned}$$

This requires $af = dc$ for all $d, f \in F$. This is only possible if $a = c = 0$. Thus, we have $Z(H(F)) = \{A \in H(F) \mid A_{12} = A_{23} = 0\}$. There is a natural homomorphism $\varphi : Z(H(F)) \to F$ defined by $\varphi(A) = A_{13}$ for all $A \in Z(H(F))$. Indeed, for all $A, B \in Z(H(F))$, we have

$$\begin{aligned} \varphi(AB) &= \varphi\left(\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right) \\ &= \varphi\left(\begin{pmatrix} 1 & 0 & a+b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right) \\ &= a + b \\ &= \varphi(A) + \varphi(B) \end{aligned}$$

Note that φ has a two-sided inverse $\varphi^{-1} : F \to Z(H(F))$ defined by

$$\varphi^{-1}(a) = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

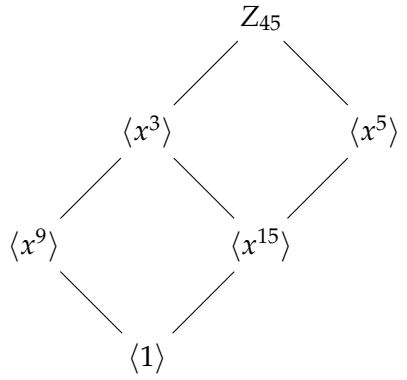
for all $a \in F$. It follows that φ is a bijection, and thus, an isomorphism. Therefore, $Z(H(F)) \cong F$.

2.3 Cyclic Groups and Cyclic Subgroups

1. The subgroups are

$$Z_{45} = \langle x \rangle \quad \langle x^3 \rangle \quad \langle x^5 \rangle \quad \langle x^9 \rangle \quad \left\langle x^{15} \right\rangle \quad \langle 1 \rangle$$

These satisfy



where a line drawn upwards from $\langle x^n \rangle$ to $\langle x^m \rangle$ means $\langle x^n \rangle \leq \langle x^m \rangle$.

2. Since $x \in G$, and G is a group, $\langle x \rangle \leq G$. In addition, $|G| < \infty$ and $|G| = |x| = |\langle x \rangle|$, so $\langle x \rangle = G$.

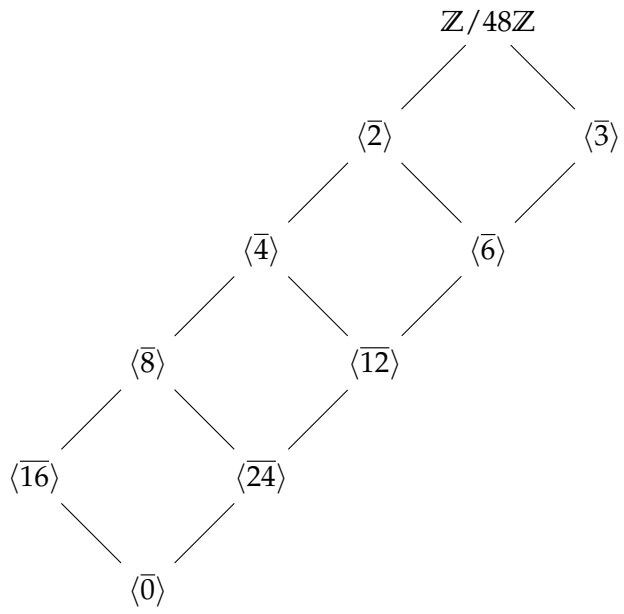
This is not necessarily true if G is an infinite group. For example, the infinite group $\mathbb{Z}$ contains the element 2, which is of infinite order, but $\langle 2 \rangle \neq \mathbb{Z}$.

3. The generators are $\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{29}, \overline{31}, \overline{35}, \overline{37}, \overline{41}, \overline{43}, \overline{47}$.

4. The generators are $\overline{2k+1}$ for $0 \leq k \leq 100$ except $\overline{101}$.

5. Let φ be Euler's totient function. Then this is simply $\varphi(49000) = \varphi(2^3)\varphi(5^3)\varphi(7^2) = 4 \cdot 100 \cdot 42 = 16800$.

6. The first part of this exercise is trivial and incredibly tedious, so it is left as an exercise for the reader. The distinct subgroups are $\langle \overline{0} \rangle, \langle \overline{24} \rangle, \langle \overline{16} \rangle, \langle \overline{12} \rangle, \langle \overline{8} \rangle, \langle \overline{6} \rangle, \langle \overline{4} \rangle, \langle \overline{3} \rangle, \langle \overline{2} \rangle, \mathbb{Z}/48\mathbb{Z}$. They satisfy



7. The subgroups are $Z_1, Z_2, Z_3, Z_4, Z_6, Z_8, Z_{12}, Z_{16}, Z_{24}, Z_{48}$.

8. Note that $\mathbb{Z}/48\mathbb{Z} = \langle\overline{1} \mid 48 \cdot \overline{1} = \overline{0}\rangle$. So, φ_a extends to a homomorphism if $x^{48a} = 1$. Since $x^{48} = 1$, we find that φ_a is a homomorphism for all a. Since $|Z_{48}| = |\mathbb{Z}/48\mathbb{Z}|$, we need only prove that φ_a is surjective to prove that it is an isomorphism. Surjectivity requires $\langle x^a\rangle = Z_{48}$, which occurs iff $(a, 48) = 1$ by Proposition 6 of this section. Thus, if a is one of the following values $1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47$, then φ_a is an isomorphism.

9. Note that ψ_a extends to a well-defined homomorphism if $x^{48a} = 1$. Indeed, if $\overline{n} = \overline{m}$, then $n = m + 48k$ for some $k \in \mathbb{Z}$. Therefore, $\psi_a(\overline{n}) = x^{na} = x^{(m+48k)a} = x^{ma} = \psi_a(\overline{m})$, so ψ_a is well-defined. Given that $|x| = 36$, $x^{48a} = 1$ iff $36|48a$, which is equivalent to $3|4a$. Since $3 \nmid 4$, $x^{48a} = 1$ iff $3|a$. Thus, ψ_a extends to a well-defined homomorphism if $3|a$. For ψ_a to be a surjective homomorphism, we would require $\langle x^a\rangle = Z_{36}$. This occurs iff $(a, 36) = 1$. Since $3|a$, this is impossible. So ψ_a is never a surjective homomorphism.

10. The order of $\overline{30}$ is 9 by Proposition 5 of this section. The subgroup $\langle\overline{30}\rangle$ is

$$\langle\overline{30}\rangle = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}, \overline{42}, \overline{48}\}$$

Their orders are $|\overline{0}| = 1$, $|\overline{6}| = |\overline{12}| = |\overline{24}| = |\overline{30}| = |\overline{42}| = |\overline{48}| = 9$, and $|\overline{18}| = |\overline{36}| = 3$.

11. The cyclic subgroups of D_8 are

$$\langle 1\rangle = \{1\} \quad \langle r\rangle = \{1, r, r^2, r^3\} \quad \langle r^2\rangle = \{1, r^2\} \quad \langle r^3\rangle = \{1, r, r^2, r^3\}$$

$$\langle s\rangle = \{1, s\} \quad \langle sr\rangle = \{1, sr\} \quad \langle sr^2\rangle = \{1, sr^2\} \quad \langle sr^3\rangle = \{1, sr^3\}$$

The subgroup $\{1, s, r^2, sr^2\}$ is not a cyclic subgroup of D_8.

12. (a) Every element of $Z_2 \times Z_2$ is of order ≤ 2, which means that the cyclic subgroup generated by any element of $Z_2 \times Z_2$ is strictly smaller than $Z_2 \times Z_2$. It follows that $Z_2 \times Z_2$ is not a cyclic group.

12. (b) Let $Z_2 = \{1, x\}$. Note that any element of the form $(1, a)$ for any $a \in \mathbb{Z}$ cannot possibly generate an element of the form (x, b), since $(1, a)^n = (1^n, na) = (1, na)$ for all $n \in \mathbb{Z}$. In addition, any element of the form (x, a) for any $a \in \mathbb{Z}$ cannot possibly generate $(x, 2a)$, since $(x, a)^n = (x^n, na) = (x, 2a)$ requires $n = 2$, but $x^2 = 1 \neq x$. It follows that no element of $Z_2 \times \mathbb{Z}$ generates $Z_2 \times \mathbb{Z}$, so $Z_2 \times \mathbb{Z}$ is not cyclic.

12. (c) Suppose there exists an element $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ that generates $\mathbb{Z} \times \mathbb{Z}$. Let $p \in \mathbb{Z}$ be prime, and consider $(0, p), (p, 0) \in \mathbb{Z} \times \mathbb{Z}$. There must exist $n, m \in \mathbb{Z}$ such that $(a, b)^n = (0, p)$ and $(a, b)^m = (p, 0)$. If $(a, b)^n = (na, nb) = (0, p)$, we must have $a = 0$, since if $n = 0$, then $nb \neq p$. But then, $(a, b)^m = (ma, mb) = (0, mb) \neq (p, 0)$. This is a contradiction, so no such (a, b) exists and $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

13. (a) Suppose $\mathbb{Z} \times Z_2 \cong \mathbb{Z}$. Then there is an isomorphism $\varphi : \mathbb{Z} \times Z_2 \to \mathbb{Z}$. This implies that there exists an element $\varphi((0, x)) \in \mathbb{Z}$ such that $\varphi((0, x))^2 = \varphi((0, x)^2) = \varphi((0, x^2)) = \varphi((0, 1)) = 0$ (i.e., there exists an element of order 2 in $\mathbb{Z}$). But we know that no such element of $\mathbb{Z}$ exists! Thus, $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$ cannot be isomorphic.

13. (b) The proof is almost identical to the one in Exercise 13.(a).

14. We know that $|\sigma| = 12$. Since $13 \equiv 1 \pmod{12}$, $65 \equiv 5 \pmod{12}$, $626 \equiv 2 \pmod{12}$, $1195 \equiv 7 \pmod{12}$, $-6 \equiv 6 \pmod{12}$, $-81 \equiv 3 \pmod{12}$, $-570 \equiv 6 \pmod{12}$, and $-1211 \equiv 1 \pmod{12}$, we have

$$\sigma^{13} = \sigma^{-1211} = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12) \quad \sigma^{626} = (1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 6\ 8\ 10\ 12)$$

$$\sigma^{-81} = (1\ 4\ 7\ 10)(2\ 5\ 8\ 11)(3\ 6\ 9\ 12) \quad \sigma^{65} = (1\ 6\ 11\ 4\ 9\ 2\ 7\ 12\ 5\ 10\ 3\ 8)$$

$$\sigma^{-6} = \sigma^{-570} = (1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 11)(6\ 12) \quad \sigma^{1195} = (1\ 8\ 3\ 10\ 5\ 12\ 7\ 2\ 9\ 4\ 11\ 6)$$

15. Suppose $\mathbb{Q} \times \mathbb{Q}$ is cyclic. Then there exists $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ such that $\langle (a, b) \rangle = \mathbb{Q} \times \mathbb{Q}$. Let $p, q \in \mathbb{Z}$ be two distinct primes, and consider $\left(0, \frac{p}{q}\right), \left(\frac{p}{q}, 0\right) \in \mathbb{Q} \times \mathbb{Q}$. There exists, $n, m \in \mathbb{Z}$ such that $(a, b)^n = \left(0, \frac{p}{q}\right)$ and $(a, b)^m = \left(\frac{p}{q}, 0\right)$. If $(a, b)^n = (na, nb) = \left(0, \frac{p}{q}\right)$, then we must have $a = 0$. But then, $(a, b)^m = (ma, mb) = (0, mb) \neq \left(\frac{p}{q}, 0\right)$. This is a contradiction, so $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

16. Let $d = (n, m)$, $n = ad$, and $m = bd$. Let ℓ be the least common multiple of n and m. Then we have $\ell = \frac{nm}{d} = abd$. Observe that $(xy)^\ell = x^\ell y^\ell = x^{nb} y^{ma} = 1^b 1^a = 1$. Therefore, $|xy|$ divides ℓ. This is not necessarily true if x and y do not commute (indeed, if x and y do not commute, $|xy|$ could be ∞). Consider the elements r^2 and r^3 of D_{10}. All powers of r commute, and $|r^2| = |r^3| = 5$, but $|r^2 r^3| = |r^5| = |1| = 1$.

17. A presentation for Z_n is $\langle x \mid x^n = 1 \rangle$.

18. Consider the map $\varphi : Z_n \to H$ defined by $\varphi(x^k) = h^k$ for any $k \in \mathbb{Z}$. This clearly maps x to h. Consider any two elements $x^i, x^j \in Z_n$ such that $x^i = x^j$. Then $n | i - j$ so that we may write $i = qn + j$ for some $q \in \mathbb{Z}$. Then $\varphi(x^i) = h^i = h^{qn+j} = (h^n)^q h^j = h^j = \varphi(x^j)$, so this map is well-defined. This map is also a homomorphism, since $\varphi(x^i)\varphi(x^j) = h^i h^j = h^{i+j} = \varphi(x^{i+j}) = \varphi(x^i x^j)$ for any two elements $x^i, x^j \in Z_n$. Finally, this homomorphism is unique. Let $\psi : Z_n \to H$ be another homomorphism satisfying $\psi(x) = h$. Then we have $\psi(x^k) = \psi(x)^k = h^k = \varphi(x^k)$ for all $x^k \in Z_n$, so necessarily, $\psi = \varphi$.

19. Consider the map $\varphi : \mathbb{Z} \to H$ defined by $\varphi(n) = h^n$. This map is well-defined, as there is no ambiguity in the representation of elements of $\mathbb{Z}$. In addition, this map is a homomorphism, since $\varphi(n)\varphi(m) = h^n h^m = h^{n+m} = \varphi(n + m)$ for all $n, m \in \mathbb{Z}$. Finally, let $\psi : \mathbb{Z} \to H$ be another homomorphism satisfying $\psi(1) = h$. Then because ψ is a homomorphism, we have $\psi(n) = \psi(1)^n = h^n = \varphi(n)$ for all $n \in \mathbb{Z}$. Thus, $\psi = \varphi$ and we conclude that φ is unique.

20. If $x^{p^n} = 1$, then x is of finite order, and $|x|$ divides p^n. Since p is prime, the only integers that divide p^n are of the form p^m, where $m \leq n$. Hence, $|x| = p^m$ for some $m \leq n$.

21. From the Binomial Theorem, we have

$$(1 + p)^{p^{n-1}} = \sum_{k=0}^{p^{n-1}} \binom{p^{n-1}}{k} p^k = \sum_{k=0}^{p^{n-1}} \frac{p^{n-1}!}{(p^{n-1} - k)!k!} p^k$$

We begin by proving that $p^{n-1} \geq n$, $\forall n \in \mathbb{Z}^+$. It is clearly true for $n = 1$, since $p^0 = 1$. Now, consider $n \geq 2$ and suppose it holds true for $n-1$. Then for n, we have $p^{n-1} = p \cdot p^{n-2} \geq p(n-1)$. Note that $p(n-1) \geq 3(n-1) \geq n$, from which it follows that $p^{n-1} \geq n$. Therefore, $p^{n-1} \geq n$ for all $n \in \mathbb{Z}^+$. It is clear that the k^{th} term is divisible by p^n for all $k \geq n$. So let us turn our attention to $1 \leq k < n$. We may write the k^{th} term of the sum as

$$\frac{p^{n-1}...(p^{n-1}-k+1)}{k!}p^k$$

Binomial coefficients are integers, so every factor of $k!$ is absorbed by the numerator. Note that for every factor of the form $mp^i < k$ in $k!$, there is a factor $p^{n-1} - mp^i$ in the numerator to absorb the p^i. Thus, we only need the factor p^{n-1} in the numerator to absorb powers of p originating from k itself. Since $k \leq p^{k-1}$, $\binom{p^{n-1}}{k}$ must be divisible by p^{n-k}. It follows that for $1 \leq k < n$, the k^{th} term of the sum is divisible by p^n. The only remaining term is the $k = 0$ term, which is simply 1. So, $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$

Next, we show that $p^{n-2} \geq n$, $\forall n \geq 3$. It holds for $n = 3$, since $p \geq 3$. Now, assume it holds for $n-1$, where $n > 3$. Then for n, we have $p^{n-2} = p \cdot p^{n-3} \geq p(n-1) \geq 3(n-1) \geq n$. Hence the claim. Note that the $k = 2$ term of the binomial expansion of $(1+p)^{p^{n-2}}$ is $\frac{p^{n-2}-1}{2}p^n$, which is divisible by p^n. Using similar reasoning to that used above, we find that $(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \pmod{p^n}$. Given $|1+p|$ divides p^{n-1}, we know that $|1+p|$ must be a power of p. However, because $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$, it follows that $|1+p| = p^{n-1}$.

21. (Alternate Solution) We prove that $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ for $n \in \mathbb{Z}^+$ by induction. Clearly, it holds for $n = 1$ since $1 + p \equiv 1 \pmod{p}$. So suppose it holds for $n-1$, where $n > 1$. It is easy to see that if $(1+p)^{p^{n-2}} \equiv 1 \pmod{p^{n-1}}$, then $(1+p)^{p^{n-2}} = 1 + qp^{n-1}$ for some $q \in \mathbb{Z}$. Thus, using the Binomial theorem, we have

$$(1+p)^{p^{n-1}} = ((1+p)^{p^{n-2}})^p = (1+qp^{n-1})^p = \sum_{i=0}^{p} \binom{p}{i} q^i p^{i(n-1)}$$

Obviously, for $i \geq 2$, the i^{th} term is divisible by p^n, because $n \geq 2$. The $i = 1$ term qp^n is also clearly divisible by p^n. We conclude that $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$, so the claim also holds for n and we are done.

Next, we prove that $(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \pmod{p^n}$ for $n \geq 2$ by induction. The claim holds for $n = 2$, since $1 + p \equiv 1 + p \pmod{p^2}$ trivially. So suppose it holds for $n-1$, where $n > 2$. Then we find that $(1+p)^{p^{n-3}} = 1 + p^{n-2} + qp^{n-1}$ for

some $q \in \mathbb{Z}$. Using the Binomial Theorem, we may write

$$(1+p)^{p^{n-2}} = ((1+p)^{p^{n-3}})^p = (1+(1+qp)p^{n-2})^p = \sum_{i=0}^{p} \binom{p}{i} (1+qp)^i p^{i(n-2)}$$

Since we are considering $n \geq 3$, it is easy to see that for $i \geq 3$, the i^{th} term is divisible by p^n. For $i = 2$, we have $\frac{p-1}{2}(1+qp)^2 p^{2n-3}$, which is also clearly divisible by p^n. The $i = 1$ term is $p^{n-1} + qp^n$. We are left with

$$(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \pmod{p^n}$$

Clearly, the claim holds for n as well, and we are done. Given $|1+p|$ divides p^{n-1}, we know that $|1+p|$ must be a power of p. However, because $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$, it follows that $|1+p| = p^{n-1}$.

22. We follow a similar strategy to the alternate solution to Exercise 21 above. We start by proving $(1+2^2)^{2^{n-2}} \equiv 1 \pmod{2^n}$. For $n = 3$, we note that $(1+2^2)^2 = 1 + 2^3 + 2^4 \equiv 1 \pmod{2^3}$. Suppose it holds true for $n-1$, where $n > 3$. Then $(1+2^2)^{2^{n-3}} = 1 + 2^{n-1}q$ for some $q \in \mathbb{Z}$. It follows that

$$(1+2^2)^{2^{n-2}} = ((1+2^2)^{2^{n-3}})^2 = (1+2^{n-1}q)^2 = 1 + 2^n q + 2^{2n-2}q^2$$

Since we are considering $n > 3$, we find that $(1+2^2)^{2^{n-2}} \equiv 1 \pmod{2^n}$. So we have the claim.

Now we prove that $(1+2^2)^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$ for $n \geq 3$. For $n = 3$, the claim holds trivially, since we have $(1+2^2) \equiv 1 + 2^2 \pmod{2^3}$. Suppose it holds for $n-1$, where $n > 3$. Then we have $(1+2^2)^{2^{n-4}} = 1 + 2^{n-2} + 2^{n-1}q = 1 + 2^{n-2}(1+2q)$ for some $q \in \mathbb{Z}$. So, we may write

$$(1+2^2)^{2^{n-3}} = ((1+2^2)^{2^{n-4}})^2 = (1+2^{n-2}(1+2q))^2 = 1+2^{n-1}(1+2q)+2^{2n-2}(1+2q)^2$$

We are considering $n \geq 4$, so we find that $(1+2^2)^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$. Thus, the claim holds. Using identical reasoning to that used in Exercise 21, we are forced to conclude that 5 is an element of order 2^{n-2} in $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

23. Consider $2^n - 1$. Its square is $(2^n-1)^2 = 2^{2n} - 2^{n+1} + 1 \equiv 1 \pmod{2^n}$, so it is an element of order 2. Next, consider $2^{n-1} - 1$. Its square is $(2^{n-1}-1)^2 = 2^{2n-2} - 2^n + 1$. Since $n \geq 3$, $2n - 2 \geq n + 1$. Thus, $(2^{n-1}-1)^2 \equiv 1 \pmod{2^n}$. These elements generate two different subgroups of order 2, which is not possible in a cyclic group. Therefore, $(\mathbb{Z}/2^n\mathbb{Z})^\times$ cannot be a cyclic group for $n \geq 3$.

24. (a) Let $S = \langle x \rangle$. S, by definition, contains only integral powers of x. Therefore, if $g \in N_G(S)$ and $gxg^{-1} \neq x^a$ for any $a \in \mathbb{Z}$, then $gSg^{-1} \neq S$. This contradicts the membership of g in $N_G(S)$. So, $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

24. (b) Again, let $S = \langle x \rangle$. Consider the product gx^kg^{-1} for any $k \in \mathbb{Z}$. Note that we can stick the identity element $g^{-1}g$ anywhere we want to in this product without changing its value. So let us insert an identity element between every pair of x's (if $k \geq 0$) or x^{-1}'s (if $k < 0$) in the product. Then we obtain $gx^kg^{-1} = (gxg^{-1})^k$ or $gx^kg^{-1} = (gx^{-1}g^{-1})^{-k}$. If $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$, then necessarily, $gx^{-1}g^{-1} = x^{-a}$. So, we may write $gx^kg^{-1} = x^{ak}$, and conclude that $gSg^{-1} \leq S$.

In Exercise 17 of Section 1.7, we proved that for any subset A of G and any fixed element $g \in G$, $|gAg^{-1}| = |A|$. Since $gSg^{-1} \leq S$ and $|gSg^{-1}| = |S|$, we find that $gSg^{-1} = S$.

25. Let G be a cyclic group of order n, and let z be a generator of G. Then by Proposition 6, z^k is also a generator of G. Then for any element $z^a \in G$, there is an integer $\ell \in \mathbb{Z}$ such that $z^a = (z^k)^\ell = (z^\ell)^k$. Since for every $z^a \in G$, there exists $z^\ell \in G$ such that $(z^\ell)^k = z^a$, we conclude that the map $x \mapsto x^k$ is surjective.

Now let G be any finite group of order n. Pick any element $g \in G$ and consider the subgroup $H = \langle g \rangle$. By Lagrange's theorem, $|H|$ divides $|G|$. It follows that $(|H|, k) = 1$, since $(|G|, k) = 1$. Thus, the map $x \mapsto x^k$ must be surjective on every such cyclic subgroup H. This implies that for every element $g \in G$, there exists $h \in G$ such that $h^k = g$. So, the map $x \mapsto x^k$ is surjective on G.

26. (a) Let x be a generator of Z_n. It is obvious that σ_a is a homomorphism, since $\sigma_a(x^ix^j) = \sigma_a(x^{i+j}) = x^{a(i+j)} = x^{ai}x^{aj} = \sigma_a(x^i)\sigma_a(x^j)$ for any $x^i, x^j \in Z_n$. We already have from Exercise 25 that if $(a, n) = 1$, then σ_a is a surjection. Consider any two elements $x^i, x^j \in Z_n$ such that $\sigma_a(x^i) = \sigma_a(x^j)$. This means $x^{ia} = x^{ja}$ or $x^{a(i-j)} = 1$. It must be that $n|i - j$ since $(a, n) = 1$. It follows that $x^i = x^{j+qn} = x^jx^{qn} = x^j$ for some $q \in \mathbb{Z}$. So σ_a must also be an injection, making it an automorphism.

Next, consider the case $(a, n) \neq 1$. Let $d = (a, n)$, $bd = a$, and $cd = n$. Since $c < n$, $x \neq x^{c+1}$. However, $\sigma_a(x^{c+1}) = x^{ac+a} = x^{bn}x^a = x^a = \sigma_a(x)$. So σ_a cannot be an injection, and therefore, cannot be an automorphism.

26. (b) If $a \equiv b \pmod{n}$, then $a = b + qn$ for some $q \in \mathbb{Z}$. Consider any element $x \in Z_n$. It is an easy corollary of Lagrange's theorem that if G is a finite group and x is any element of G, then $x^{|G|} = 1$. We have $\sigma_a(x) = x^a = x^{b+qn} = x^b = \sigma_b(x)$. Thus, $\sigma_a = \sigma_b$.

Conversely, if $\sigma_a = \sigma_b$, then $\sigma_a(x) = x^a = x^b = \sigma_b(x)$, where x is a generator of Z_n. It follows that $x^{b-a} = 1$, which implies that $n|b - a$. Therefore, $a \equiv b \pmod{n}$.

26. (c) Let x be a generator of Z_n and consider any automorphism $\varphi : Z_n \to Z_n$. It is easy to see that φ is completely determined by its action on x. φ must map x to some element $x^a \in Z_n$. This fact allows us to see that for any element $x^i \in Z_n$, we have $\varphi(x^i) = \varphi(x)^i = (x^a)^i = x^{ai} = \sigma_a(x^i)$. Thus, $\varphi = \sigma_a$ for some $a \in \mathbb{Z}$.

26. (d) Consider any two maps $\sigma_a, \sigma_b \in \mathrm{Aut}(Z_n)$ and any element $z \in Z_n$. We have $\sigma_a \circ \sigma_b(z) = \sigma_a(z^b) = z^{ab} = \sigma_{ab}(z)$. It follows that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Let us define the map $\varphi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(Z_n)$ by $\varphi(\bar{a}) = \sigma_a$. It is easy to see that this map is well-defined using the results of Exercise 26.(b), and it must be a homomorphism, since $\varphi(\bar{a}) \circ \varphi(\bar{b}) = \sigma_a \circ \sigma_b = \sigma_{ab} = \varphi(\overline{ab})$.

Since the codomain is $\mathrm{Aut}(Z_n)$, it contains only maps σ_a such that $(a, n) = 1$. Thus, by Proposition 4 of Section 0.3, we find that for every element $\sigma_a \in \mathrm{Aut}(Z_n)$, there exists $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\varphi(\bar{a}) = \sigma_a$. φ is therefore a surjection.

Finally, if $\varphi(\bar{a}) = \sigma_a = \sigma_b = \varphi(\bar{b})$, then it must be that $a \equiv b \pmod{n}$. This implies that $\bar{a} = \bar{b}$, so φ is also an injection and therefore, an isomorphism.

2.4 Subgroups Generated by Subsets of a Group

1. Everything in H must be in $\langle H \rangle$, since $\langle H \rangle$ is the intersection of all subgroups of G containing H. H is one of the subgroups of G containing H, so anything not in H would not be an element of $\langle H \rangle$. Therefore, everything in $\langle H \rangle$ is also in H, and $H = \langle H \rangle$.

2. Consider any element $a \in \langle A \rangle$. Every subgroup containing A must contain a. Since $A \subseteq B$, every subgroup containing B also contains A and therefore, contains a. It follows that $a \in \langle B \rangle$ and $\langle A \rangle \leq \langle B \rangle$.

Consider the group $\mathbb{Z}/4\mathbb{Z}$ and let $A = \{\bar{2}\}$ and $B = \{\bar{0}, \bar{2}\}$. Clearly, $A \subsetneq B$, but $\langle A \rangle = \langle B \rangle$.

3. Every element of $\langle H, Z(G) \rangle$ is a finite product of elements of H and/or $Z(G)$. From the definition of $Z(G)$ and the fact that H is an abelian subgroup, we know that all elements of H and $Z(G)$ commute with each other. Consider any two elements $a, b \in \langle H, Z(G) \rangle$ and write $a = a_1^{\epsilon_1} ... a_n^{\epsilon_n}$ and $b = b_1^{\delta_1} ... b_m^{\delta_m}$, where the $a_i, b_j \in H \cup Z(G)$. We can commute the a_i's and b_j's in the product ab to see that $ab = a_1^{\epsilon_1} ... a_n^{\epsilon_n} b_1^{\delta_1} ... b_m^{\delta_m} = b_1^{\delta_1} ... b_m^{\delta_m} a_1^{\epsilon_1} ... a_n^{\epsilon_n} = ba$. So $\langle H, Z(G) \rangle$ must be abelian.

Let A be a finite abelian group and $G = A \times D_6$. Let $H = \{(a, 1) | a \in A\}$. Then for any $b, c \in A$, we know that $(b, r), (c, s) \in C_G(H)$. But $(b, r)(c, s) = (bc, rs) \neq (bc, sr) = (c, s)(b, r)$, so $\langle H, C_G(H) \rangle$ cannot be abelian.

4. Consider any element $h \in \langle H - \{1\} \rangle$. It must be true that $h \in H$ or it would contradict the fact that H is closed under the group operation, so $\langle H - \{1\} \rangle \subseteq H$. Note that $\langle H - \{1\} \rangle$ contains the identity because it is a subgroup of G. So every element of H is also in $\langle H - \{1\} \rangle$. It follows that $H = \langle H - \{1\} \rangle$.

5. No two distinct 2-cycles of S_3 are disjoint, so let $(a\ b), (b\ c) \in S_3$ be any two distinct 2-cycles. Since $(a\ b)(b\ c) = (a\ b\ c)$, $(b\ c)(a\ b) = (a\ c\ b)$, and $(b\ c)(a\ b\ c) = (a\ c)$, we find that $\langle (a\ b), (b\ c) \rangle = S_3$.

6. Notice that $(1\ 2)$ and $(1\ 2)(3\ 4)$ generate distinct subgroups of order 2, so the subgroup generated by both elements cannot be cyclic. Furthermore, these elements commute, and their product $(1\ 2)(1\ 2)(3\ 4) = (3\ 4)$ is an element of order 2. Thus, $\langle (1\ 2), (1\ 2)(3\ 4) \rangle$ is a noncyclic subgroup of order 4.

7. Observe that $(1\ 2)(1\ 3)(2\ 4) = (1\ 3\ 2\ 4)$. Clearly, the subgroup of S_4 generated by $(1\ 2)$ and $(1\ 3)(2\ 4)$ is identical to the subgroup generated by $(1\ 2)$ and $(1\ 3\ 2\ 4)$.

Call this subgroup G. Observe that $(1\ 2)(1\ 3\ 2\ 4) = (1\ 3\ 2\ 4)^3(1\ 2)$. With this relation, we can deduce that $|G| \leq 8$. Given that $|\langle(1\ 3\ 2\ 4)\rangle| = 4$ and $(1\ 2) \notin \langle(1\ 3\ 2\ 4)\rangle$, we can apply Lagrange's Theorem to conclude that $|G| = 8$. Now, define the map $\varphi : D_8 \to G$ by $\varphi(r) = (1\ 3\ 2\ 4)$ and $\varphi(s) = (1\ 2)$. D_8 has the presentation $D_8 = \langle r, s \mid r^4 = s^2 = 1, sr = rs^{-1}\rangle$. It is clear that $\varphi(s)^2 = \text{id}$, $\varphi(r)^4 = \text{id}$, and $\varphi(s)\varphi(r) = (1\ 2)(1\ 3\ 2\ 4) = (1\ 3)(2\ 4) = (1\ 4\ 2\ 3)(1\ 2) = \varphi(r)^{-1}\varphi(s)$. Thus, φ extends uniquely to a homomorphism from D_8 to G. Furthermore, since $\varphi(s), \varphi(r)$ generate G, and $|D_8| = |G|$, φ is an isomorphism. So $D_8 \cong G$.

8. Note that $(1\ 2\ 3\ 4)^2(1\ 2\ 4\ 3) = (1\ 4)$ and that $(1\ 2\ 4\ 3)(1\ 4) = (1\ 4)(1\ 2\ 4\ 3)^3$. Thus, the subgroup $\langle(1\ 4), (1\ 2\ 4\ 3)\rangle$ is of order at most 8. Since $|\langle(1\ 2\ 4\ 3)\rangle| = 4$ and $(1\ 4) \notin \langle(1\ 2\ 4\ 3)\rangle$ we can apply Lagrange's Theorem to conclude that $|\langle(1\ 4), (1\ 2\ 4\ 3)\rangle| = 8$. In addition, $(1\ 2\ 3\ 4)(1\ 2\ 4\ 3) = (1\ 3\ 2)$, which generates a subgroup of order 3. By Lagrange's Theorem, 3 and 8 divide the order of $G = \langle(1\ 2\ 3\ 4), (1\ 2\ 4\ 3)\rangle$, so $|G| \geq 24$. Since $|S_4| = 24$, G must be all of S_4.

9. It is clear that $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$ is a subgroup of order 3. The products $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ generate a subgroup $\left\langle \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \right\rangle$ of order 8. Therefore, by Lagrange's Theorem, the subgroup $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$ is of order at least 24. Since $|SL_2(\mathbb{F}_3)| = 24$, it follows that $SL_2(\mathbb{F}_3) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$.

10. Let $G = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right\rangle$. Define the map $\varphi : Q_8 \to G$ by $\varphi(i) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\varphi(j) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. It is easy to verify that $\varphi(i)^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\varphi(i)^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \varphi(j)^2$, and $\varphi(i)\varphi(j) = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} = -\varphi(j)\varphi(i)$. Thus, φ extends uniquely to a homomorphism from Q_8 to G. Furthermore, since $\varphi(i), \varphi(j)$ generate G and $|G| = |Q_8|$, φ is an isomorphism. So $Q_8 \cong G$.

11. $SL_2(\mathbb{F}_3)$ cannot be isomorphic to S_4, as $SL_2(\mathbb{F}_3)$ contains $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, an element of order 6, whereas S_4 has no such element.

12. The diagonal elements of an upper triangular matrix in $GL_3(\mathbb{F}_2)$ must be 1, so there are only three free elements in such a matrix. From this, we can conclude that the order of this subgroup is 2^3. Call this subgroup G. Define the map $\varphi : D_8 \to G$

by $\varphi(s) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $\varphi(r) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. We see that $\varphi(r)^4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\varphi(s)^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, and $\varphi(r)\varphi(s) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \varphi(s)\varphi(r)^{-1}$. Thus, φ extends uniquely to a homomorphism from D_8 to G. It is easy to verify that $\varphi(s), \varphi(r)$ generate G. Since $\varphi(s), \varphi(r)$ generate G and $|G| = |D_8|$, φ is an isomorphism. So $D_8 \cong G$.

13. Notice that the subgroup G generated by $\left\{ \frac{1}{p} \;\middle|\; p \text{ is prime} \right\}$ must contain all primes p, since groups are closed under inverses. Now consider any positive rational number $\frac{m}{n}$, where $m, n \in \mathbb{Z}$. m and n each have unique prime factorizations $m = p_1^{k_1} p_2^{k_2} ... p_i^{x_i}$, $n = q_1^{\ell_1} q_2^{\ell_2} ... q_j^{\ell_j}$. Then we find that $\frac{m}{n} = p_1^{k_1} p_2^{k_2} ... p_i^{x_i} \frac{1}{q_1^{\ell_1}} \frac{1}{q_2^{\ell_2}} ... \frac{1}{q_j^{\ell_j}}$, so any positive rational may be written as a product of known elements of G. Therefore, the set $\left\{ \frac{1}{p} \;\middle|\; p \text{ is prime} \right\}$ generates the multiplicative group of positive rationals.

14. (a) Any finite group can be generated by the set of all its elements, so every finite group is finitely generated.

14. (b) The cyclic group $\langle 1 \rangle = \{1 \cdot n \mid n \in \mathbb{Z}\}$ contains all elements of $\mathbb{Z}$. Hence, $\mathbb{Z}$ is finitely generated.

14. (c) Consider any finitely generated subgroup H of $\mathbb{Q}$, and let k be the product of all the denominators that show up in a set of generators for H. Note that every element in that set of generators may be written as a multiple of $\frac{1}{k}$. It follows that $H \leq \langle \frac{1}{k} \rangle$. Recall that every subgroup of a cyclic group is also cyclic. Thus, any finitely generated subgroup of $\mathbb{Q}$ is cyclic.

14. (d) Suppose for contradiction that there is a finite set A that generates $\mathbb{Q}$. Then $\langle A \rangle$ must be cyclic, so there is some element $x \in A$ such that $\langle x \rangle = \mathbb{Q}$. But $\frac{1}{2}x \notin \langle x \rangle$ is an element of $\mathbb{Q}$. We have a contradiction, so $\mathbb{Q}$ cannot be finitely generated.

15. The subgroup generated by $\left\{ \frac{1}{2^n} \;\middle|\; n \in \mathbb{Z}^+ \right\}$ is a proper subgroup of $\mathbb{Q}$ that is not finitely generated.

16. (a) Suppose for contradiction that H is a proper subgroup of G and there is no maximal subgroup of G containing H. If there were no proper subgroups of G containing H, then H itself would be a maximal subgroup, so there must be at least

one proper subgroup of G containing H. Furthermore, there can only be finitely many proper subgroups of G containing H since G is finite. Hence there must be some subgroup $M < G$ of largest order containing H. But notice that this M is a maximal subgroup! We have reached a contradiction. So if H is a proper subgroup of the finite group G, then there is a maximal subgroup of G containing H.

16. (b) Let R be the subgroup of all rotations in D_{2n}. The elements of $D_{2n} \setminus R$ are of the form sr^i where $0 \leq i < n$. Notice that for any i, $\langle R \cup \{sr^i\} \rangle$ will contain the generators s and r of D_{2n}, so that $\langle R \cup \{sr^i\} \rangle = D_{2n}$. It follows that R is a maximal subgroup of D_{2n}.

16. (c) Let $G = \langle x \rangle$ be a cyclic group of order $n \geq 1$. Let $H = \langle x^p \rangle$ for some prime p dividing n. Suppose that there is a proper subgroup $K = \langle x^d \rangle$ of G such that $H < K$ and $K \neq G$. Since $|H|p = |K|d$ and $|H| < |K|$, it follows that $d < p$. Furthermore, if $x^p \in K$, then p must be a multiple of d. This contradicts the primality of p, so no such K can exist. Therefore, H is a maximal subgroup.

Now, consider a proper subgroup $H = \langle x^d \rangle$ of G, where d is not prime. Then there exist $a, b \in \mathbb{Z}^+$ with $1 < a < d$ and $1 < b < d$ such that $d = ab$. Notice that $K = \langle x^a \rangle$ is also a proper subgroup of G with $H \leq K$. Since $|H|d = |K|a$ and $a < d$, it follows that $|H| < |K|$. Then $H < K$ and H cannot be a maximal subgroup. So, we may conclude that H is a maximal subgroup iff $H = \langle x^p \rangle$ for some p dividing n.

17. (a) Every proper subgroup of G must contain the identity, so $H \neq \emptyset$. Now, consider any two elements $h_1, h_2 \in H$. There must be subgroups $H_1, H_2 \in \mathcal{C}$ such that $h_1 \in H_1$ and $h_2 \in H_2$. Since $\mathcal{C}$ is a chain, either $H_1 \leq H_2$ or vice versa. Assume WLOG that $H_1 \leq H_2$. Then $h_1, h_2 \in H_2$ and therefore, so is $h_1 h_2^{-1}$. Since $h_1 h_2^{-1} \in H_2$, it must also be in H. So, H is a subgroup of G.

17. (b) Suppose that H is not a proper subgroup of G. Then H contains every generator of G. So for each generator g_i, there must be some $H_i \in \mathcal{C}$ such that $g_i \in H_i$. Since $\mathcal{C}$ is a chain, one of these subgroups must contain all the others. Call this subgroup H_m. H_m cannot be a proper subgroup of G, yet it is an element of $\mathcal{S}$. We have a contradiction, so H must be a proper subgroup of G.

17. (c) Note that for every chain $\mathcal{C}$ in $\mathcal{S}$, there is an upper bound $H \in \mathcal{S}$: the union of all elements of $\mathcal{C}$. So, by Zorn's Lemma, $\mathcal{S}$ must have a maximal element.

18. (a) Suppose $H_k \leq H_m$ for some $k, m \in \mathbb{Z}^+$. Then $|H_k| \leq |H_m|$, or $p^k \leq p^m$. It follows that $k \leq m$.

Now suppose that $k \leq m$. Consider any element $z \in H_k$. It is easy to see that $z^{p^m} = \left(z^{p^k}\right)^{p^{m-k}} = 1^{p^{m-k}} = 1$. Since every element of H_k is also an element of H_m, $H_k \leq H_m$. Thus, $H_k \leq H_m$ iff $k \leq m$.

18. (b) Consider any $k \in \mathbb{Z}^+$. Notice that the elements of H_k are simply integer powers of $\exp(2\pi i/p^k)$. So, we may write $H_k = \langle \exp(2\pi i/p^k) \rangle$.

18. (c) Consider any proper subgroup G of Z. There is at least one $z \in Z$ such that $z \notin G$. Let $|z| = p^n$. It is clear that for all $k \geq n$, none of the generators of H_k are in G; otherwise, G would contain z. Therefore, G is finite and contains elements of order at most p^{n-1}.

Now, let g be the element of largest order in G, and let $|g| = p^m$, where $m < n$. Note that g generates H_m, so that $H_m \leq G$. H_m, in turn, contains all elements of order at most p^m. Hence, every element of G is in H_m and $G \leq H_m$. It follows that $G = H_m$, so we have the claim.

18. (d) Suppose that Z is finitely generated. Then there are generators $z_1, z_2, ..., z_m$ such that $Z = \langle z_1, z_2, ..., z_m \rangle$. Denote by z_k the generator of largest order, and let $|z_k| = p^n$. Then $Z = \langle z_1, z_2, ..., z_m \rangle = \langle z_k \rangle = H_n$. But this implies that $H_{n+1} \leq H_n$, which is absurd! So, Z cannot be finitely generated.

19. (a) Consider any $q \in \mathbb{Q}$. Note that for any $k \in \mathbb{Z} \setminus \{0\}$, $\frac{q}{k} \in \mathbb{Q}$.

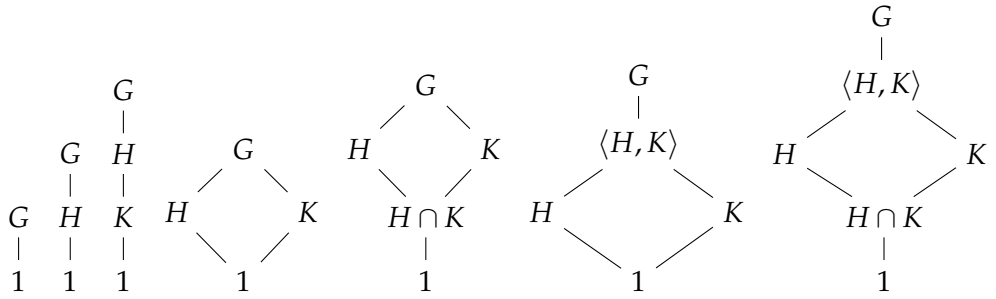
19. (b) Suppose that there is a finite divisible abelian group A. Let $|A| = n$ and consider any non-identity element $a \in A$. Since A is divisible, there must be distinct elements $x_1, ..., x_{n+1}$ such that x_i is the i^{th} root of a. This is impossible, as $|A| = n$. So, a finite divisible abelian group cannot exist.

20. Let A, B be two divisible groups, and consider any element $(a, b) \in A \times B$. Since A, B are divisible, for each $k \in \mathbb{Z} \setminus \{0\}$, there exists $x \in A$, $y \in B$ such that $x^k = a$ and $y^k = b$. Therefore, for each $k \in \mathbb{Z} \setminus \{0\}$, there exists $(x, y) \in A \times B$ such that $(x, y)^k = (x^k, y^k) = (a, b)$. So, $A \times B$ is divisible.

Now, let $A \times B$ be a divisible group. Consider any $a \in A$, any $b \in B$, and any $k \in \mathbb{Z} \setminus \{0\}$. Since $(a, b) \in A \times B$, $\exists (x, y) \in A \times B$ such that $(x, y)^k = (x^k, y^k) = (a, b)$. So, there exists $x \in A$ and $y \in B$ such that $x^k = a$ and $y^k = b$. It follows that A, B are divisible.

2.5 The Lattice of Subgroups of a Group

1. The following are possible sublattice structures. Any subgroups not explicitly represented in a sublattice are assumed to be equal to one of the subgroups that are. Other sublattices may be obtained by swapping/substituting subgroups.



2. (a) $\langle sr^6\rangle, \langle sr^2\rangle, \langle r^4\rangle, 1$

2. (b) $\langle sr^7\rangle, \langle sr^3\rangle, \langle r^4\rangle, 1$

2. (c) $\langle r\rangle, \langle r^2\rangle, \langle sr^2, r^4\rangle, \langle s, r^4\rangle, \langle sr^3, r^4\rangle, \langle sr^5, r^4\rangle, \langle s, r^2\rangle, \langle sr, r^2\rangle, D_{16}$

2. (d) $\langle s, r^4\rangle, \langle s, r^2\rangle, D_{16}$

3. The following is a presentation for V_4: $\langle a, b \mid a^2 = b^2 = 1, ab = ba\rangle$. Define the map $\varphi : V_4 \to \langle s, r^2\rangle$ by $\varphi(a) = s$ and $\varphi(b) = r^2$. It is clear that $\varphi(a)^2 = \varphi(b)^2 = 1$, and that $\varphi(a)\varphi(b) = sr^2 = r^{-2}s = r^2s = \varphi(b)\varphi(a)$. So φ extends to a unique homomorphism. Since s, r^2 obviously generate $\langle s, r^2\rangle$ and $|V_4| = |\langle s, r^2\rangle|$, we find that φ is an isomorphism. Thus, $V_4 \cong \langle s, r^2\rangle$.

4. $D_8 = \langle r, s\rangle = \langle r^2s, r\rangle = \langle rs, r\rangle = \langle r^3s, r\rangle = \langle s, rs\rangle = \langle s, r^3s\rangle = \langle r^2s, rs\rangle = \langle r^2s, r^3s\rangle = \langle r^3, s\rangle = \langle r^2s, r^3\rangle = \langle rs, r^3\rangle = \langle r^3s, r^3\rangle$.

5. x could be $r, r^3, r^5, r^7, sr, sr^3, sr^5$, or sr^7.

6. (a) $C_{D_8}(1) = C_{D_8}(r^2) = D_8$, $C_{D_8}(r) = C_{D_8}(r^3) = \langle r\rangle$, $C_{D_8}(s) = C_{D_8}(r^2s) = \langle s, r^2\rangle$, $C_{D_8}(rs) = C_{D_8}(r^3s) = \langle rs, r^2\rangle$.

6. (b) $C_{Q_8}(1) = C_{Q_8}(-1) = Q_8$, $C_{Q_8}(i) = C_{Q_8}(-i) = \langle i\rangle$, $C_{Q_8}(j) = C_{Q_8}(-j) = \langle j\rangle$, $C_{Q_8}(k) = C_{Q_8}(-k) = \langle k\rangle$.

6. (c) $C_{S_3}(1) = S_3$, $C_{S_3}((1\,2)) = \langle(1\,2)\rangle$, $C_{S_3}((1\,3)) = \langle(1\,3)\rangle$, $C_{S_3}((2\,3)) = \langle(2\,3)\rangle$, $C_{S_3}((1\,2\,3)) = C_{S_3}((1\,3\,2)) = \langle(1\,2\,3)\rangle$.

6. (d) $C_{D_{16}}(1) = C_{D_{16}}(r^4) = D_{16}$, $C_{D_{16}}(r) = C_{D_{16}}(r^2) = C_{D_{16}}(r^3) = C_{D_{16}}(r^5) = C_{D_{16}}(r^6) = C_{D_{16}}(r^7) = \langle r \rangle$, $C_{D_{16}}(s) = C_{D_{16}}(sr^4) = \langle s, r^4 \rangle$, $C_{D_{16}}(sr^6) = C_{D_{16}}(sr^2) = \langle sr^2, r^4 \rangle$, $C_{D_{16}}(sr^3) = C_{D_{16}}(sr^7) = \langle sr^3, r^4 \rangle$, $C_{D_{16}}(sr^5) = C_{D_{16}}(sr) = \langle sr^5, r^4 \rangle$.

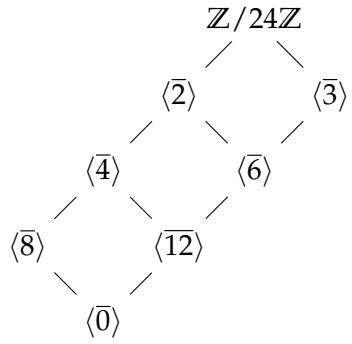
7. From the previous exercise, it is clear that $Z(D_{16}) = \langle r^4 \rangle$.

8. (a) $N_{S_3}(1) = N_{S_3}(\langle (1\ 2\ 3) \rangle) = S_3$, $N_{S_3}(\langle (1\ 2) \rangle) = \langle (1\ 2) \rangle$, $N_{S_3}(\langle (1\ 3) \rangle) = \langle (1\ 3) \rangle$, $N_{S_3}(\langle (2\ 3) \rangle) = \langle (2\ 3) \rangle$.

8. (b) $N_{Q_8}(1) = N_{Q_8}(\langle -1 \rangle) = N_{Q_8}(\langle i \rangle) = N_{Q_8}(\langle j \rangle) = N_{Q_8}(\langle k \rangle) = Q_8$.

9. (a) The lattice of subgroups is shown below:

9. (b) The lattice of subgroups is shown below:



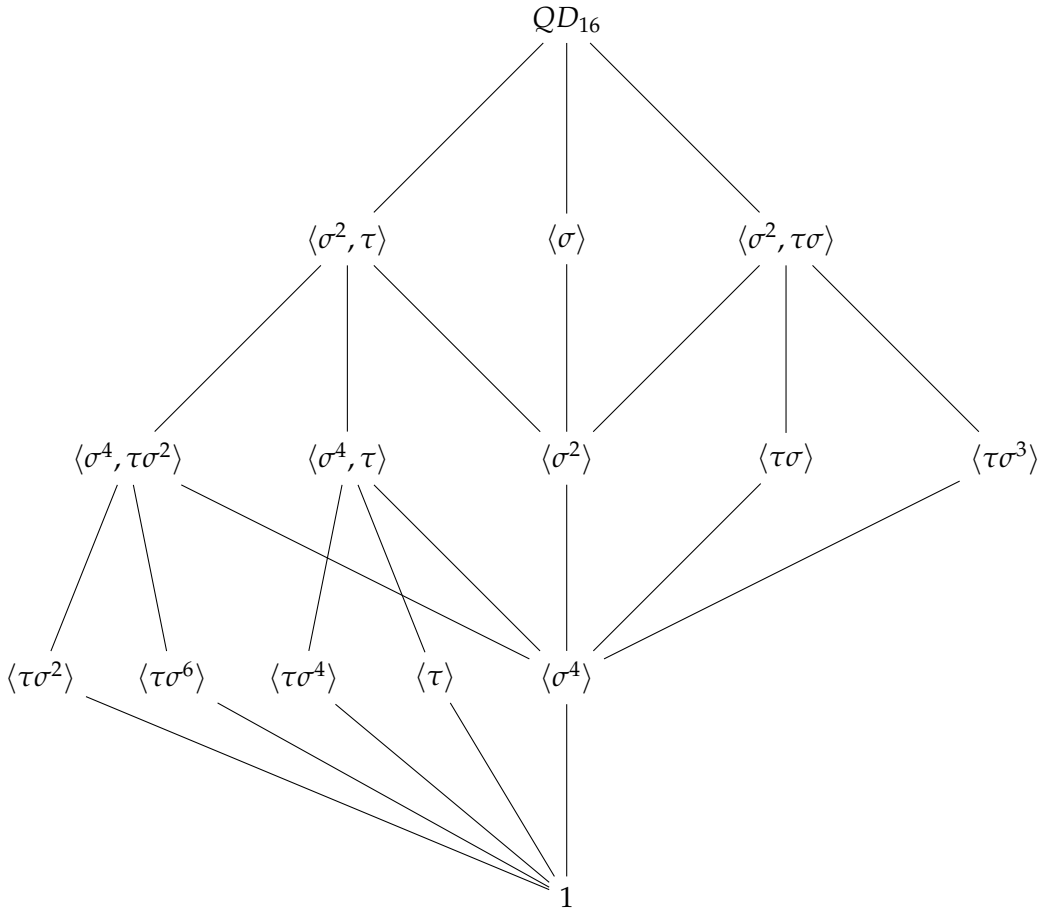
9. (c) This was done in Exercise 6 of Chapter 2 Section 3.

10. Consider any group G of order 4. We first note that G must be abelian. If it were not, there would be two distinct non-identity elements $g, h \in G$ that do not commute. This would imply that $1, g, h, gh, hg$ are all distinct elements of G, contradicting the fact that $|G| = 4$.

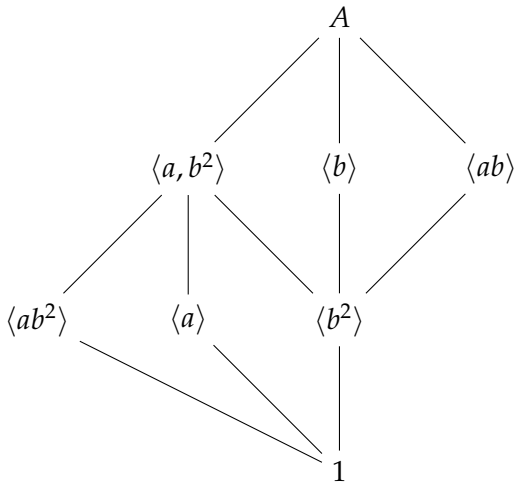
If G has an element of order 4, then G must be cyclic. Since $|G| = |Z_4|$, Theorem 4 of Chapter 2 Section 3 allows us to conclude that $G \cong Z_4$.

If G has no elements of order 4, then it cannot have elements of order 3 either. Suppose there were such an element $r \in G$. Then there must also be a non-identity element $g \in G$ such that $g \notin \langle r \rangle$. But this element must be of order at least 2, and Lagrange's theorem would then imply that $|G| \geq 6$. This is absurd. Hence, all non-identity elements of G must be of order 2. From here, an argument identical to the one used in Exercise 3 of this section may be used to prove that $G \cong V_4$.

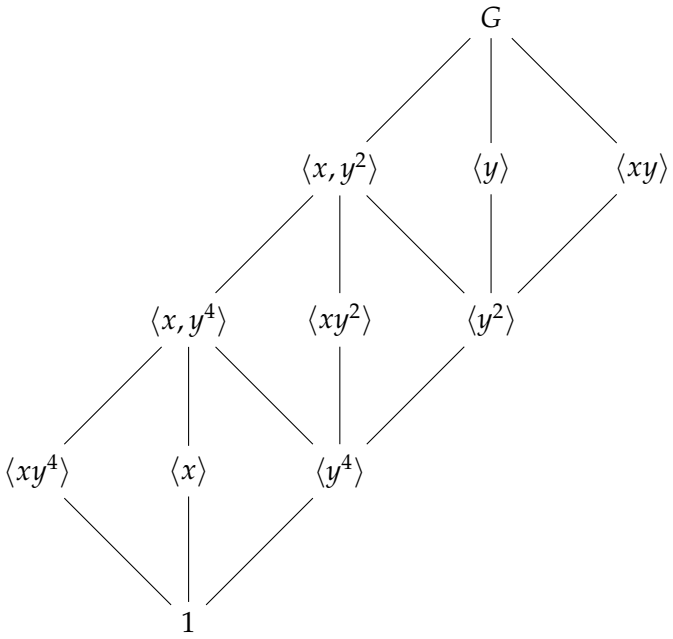
11. The following is the subgroup lattice of QD_{16}:



12. The following is the subgroup lattice of A:



13. The following is the subgroup lattice of G:

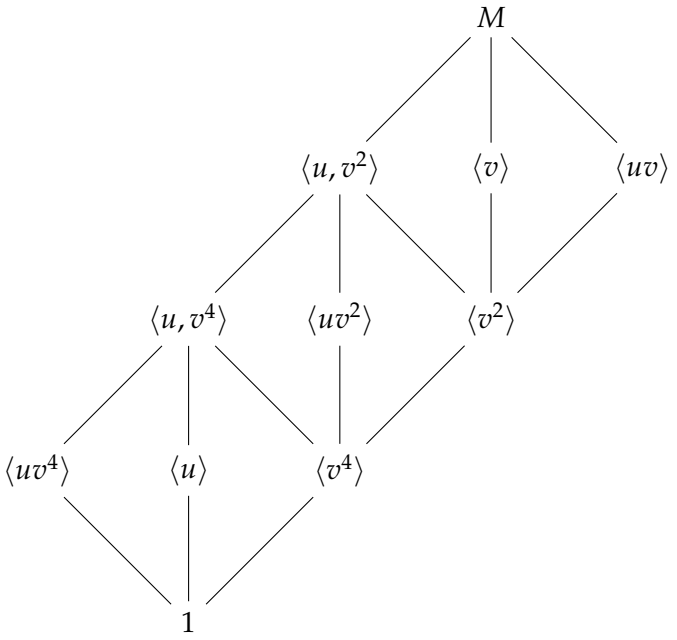


14. We begin by noting that $\langle v \rangle$ is a cyclic group of order 8, so by Theorem 4 of Chapter 2 Section 3, $\langle v \rangle \cong Z_8$.

Next, note that $\langle uv \rangle$ contains the elements $(uv)^0 = (uv)^8 = 1$, $(uv)^1 = uv$, $(uv)^2 = v^6$, $(uv)^3 = uv^7$, $(uv)^4 = v^4$, $(uv)^5 = uv^5$, $(uv)^6 = v^2$, $(uv)^7 = uv^3$. Thus, $\langle uv \rangle$ is a cyclic group of order 8, and $\langle uv \rangle \cong Z_8$.

Finally, we examine $\langle u, v^2 \rangle$. Define the map $\varphi : Z_2 \times Z_4 \to \langle u, v^2 \rangle$ by $\varphi(a) = u$ and $\varphi(b) = v^2$. Clearly, $\varphi(a)^2 = \varphi(b)^4 = 1$ and $\varphi(a)\varphi(b) = uv^2 = uv^{10} = v^2u = \varphi(b)\varphi(a)$, so φ extends to a unique homomorphism. It is not hard to see that $\langle u, v^2 \rangle$ is a group of order 8, and $\langle u, v^2 \rangle$ is obviously generated by $\varphi(a), \varphi(b)$. It follows that φ is an isomorphism and $\langle u, v^2 \rangle \cong Z_2 \times Z_4$.

The following is the subgroup lattice of M:



It is identical to the subgroup lattice of the abelian group $Z_2 \times Z_8$. Suppose that $M \cong Z_2 \times Z_8$, and let $\varphi : Z_2 \times Z_8 \to M$ be an isomorphism. Then there must be elements $z_1, z_2 \in Z_2 \times Z_8$ such that $\varphi(z_1) = u$ and $\varphi(z_2) = v$. Since φ is an isomorphism, we must have $\varphi(z_1)\varphi(z_2) = \varphi(z_1z_2) = \varphi(z_2z_1) = \varphi(z_2)\varphi(z_1)$. But we know from the presentation of M that $uv \neq vu$! Therefore, there can be no such isomorphism φ, and M is not isomorphic to $Z_2 \times Z_8$.

15. Obviously, $\langle r \rangle$ is a cyclic group of order 8, so we must have $\langle r \rangle \cong Z_8$.

The subgroups $\langle s, r^2 \rangle$ and $\langle sr, r^2 \rangle$ are isomorphic to D_8. This can be easily proven by using a presentation of D_8 to construct an isomorphism for each of these subgroups. In the case of $\langle s, r^2 \rangle$, the isomorphism maps $s \to s$ and $r \to r^2$. In the case of $\langle sr, r^2 \rangle$, the isomorphism maps $s \to sr$ and $r \to r^2$.

16. By inspection, we can see that the elements of order 2 in QD_{16} are $\tau\sigma^2$, $\tau\sigma^4$, $\tau\sigma^6$, τ, and σ^4. The join of their respective cyclic subgroups is obviously $\langle \sigma^2, \tau \rangle$.

17. By inspection, we can see that the elements of order 2 in M are uv^4, v^4, and u. Their join is $\langle u, v^4 \rangle$, a subgroup of order 4 containing exactly the elements of order ≤ 2 in M. In Exercise 10 of this section, we proved that if a group of order 4 has no elements of order 4, then it must be isomorphic to V_4. Hence, $\langle u, v^4 \rangle \cong V_4$.

18. $C_{QD_{16}}(1) = C_{QD_{16}}(\sigma^4) = QD16$, $C_{QD_{16}}(\sigma) = C_{QD_{16}}(\sigma^2) = C_{QD_{16}}(\sigma^3) = C_{QD_{16}}(\sigma^5) = C_{QD_{16}}(\sigma^6) = C_{QD_{16}}(\sigma^7) = \langle \sigma \rangle$, $C_{QD_{16}}(\tau) = C_{QD_{16}}(\tau\sigma^4) = \langle \sigma^4, \tau \rangle$, $C_{QD_{16}}(\tau\sigma^2) = C_{QD_{16}}(\tau\sigma^6) = \langle \sigma^4, \tau\sigma^2 \rangle$, $C_{QD_{16}}(\tau\sigma) = C_{QD_{16}}(\tau\sigma^5) = \langle \tau\sigma \rangle$, $C_{QD_{16}}(\tau\sigma^3) = C_{QD_{16}}(\tau\sigma^7) = \langle \tau\sigma^3 \rangle$.

19. $N_{D_{16}}(\langle s, r^4 \rangle) = \langle s, r^2 \rangle$.

20. (a) $N_{QD_{16}}(\langle \tau\sigma \rangle) = \langle \sigma^2, \tau\sigma \rangle$.

20. (b) $N_{QD_{16}}(\langle \tau, \sigma^4 \rangle) = \langle \sigma^2, \tau \rangle$