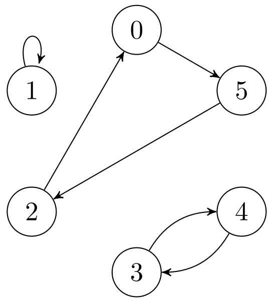
Exercise 5.1.

1. Here is a possible realization of G_f:



2. We can without loss of generality assume that $S = \underline{n}$ for some n. Since f is a function, every node in G_f has exactly one outgoing edge: if there is a node with no outgoing edge, then the function is not defined for the element of $\underline{n}$ belonging to this node which is impossible; if there are more than two outgoing edges, then the element corresponding to the node is mapped to at least two different elements, and hence f cannot be a function. Since f is surjective, each node v has an incoming edge, since there is an element mapped to the element corresponding to v by f. Finally, since f is injective, each node has exactly one incoming edge, since otherwise there are two elements of $\underline{n}$ mapped to the same element.

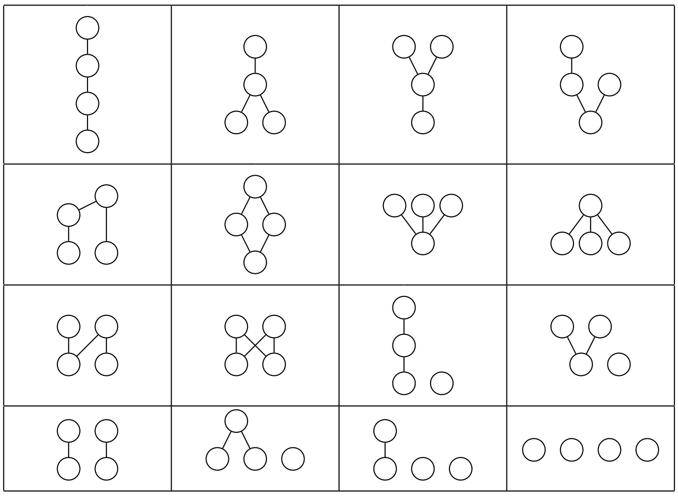
3. We proceed by induction on n: If $n = 1$, then G_f is a selfloop with one node, hence it is a disjoint union of cycles. Suppose now that $n > 1$. Let v_0 be an arbitrary node in G_f. Let v_1 be the node obtained by moving from v_0 along its outgoing edge; let v_2 be the node obtained by moving from v_1 along its outgoing edge; in general, let v_i, $i \geq 1$, be the node obtained by moving from v_{i-1} along its outgoing edge. Since the set $S = \underline{n}$ is finite, there are i and j, $i < j$, such that $v_i = v_j$. Let i be the smallest index with this property. Then $i = 0$, since otherwise there are two incoming edges into v_i, one from v_{i-1}, and one from v_{j-1}. It follows that $v_0 \to v_1 \to \cdots \to v_{j-1} \to v_0$ is a cycle. We remove it from G_f. The resulting graph is the graph of a bijective map on $S - \{v_0, \ldots, v_{j-1}\}$, and hence is a disjoint union of cycles by the induction hypothesis. It follows that G_f is a disjoint union of cycles.

4. If G_f is a cycle of length n, then $f^n = \mathrm{id}$: if $f(v_i) = v_{i+1}$ for $i = 0, \ldots, n-2$, and $f(v_{n-1}) = v_0$, then $f^2(v_i) = v_{(i+2) \bmod n}$, $f^3(v_i) = v_{(i+3) \bmod n}$, and in general $f^k(v_i) = v_{(i+k) \bmod n}$. Therefore, $f^n = \mathrm{id}$, and $f^j \neq \mathrm{id}$ for $1 \leq j < n$. Now let f be a general permutation on a set with n elements, say $\underline{n}$. By the previous part we know that G_f is a disjoint union of cycles. Hence, there is a partition $S_1 \sqcup S_2 \sqcup \cdots \sqcup S_t$ of $\underline{n}$ such that f restricted to S_i is a cycle, i.e., the elements of S_i, say $a_1, \ldots, a_\ell$, can be ordered in such a way that $f(a_j) = a_{(j+1) \bmod \ell}$. Let f_i denote the function f restricted in S_i. We can write f as $f(x) = \delta_1(x)f_1(x) + \cdots + \delta_t(x)f_t(x)$, where $\delta_i(x) = 1$ if $x \in S_i$, and $\delta_i(x) = 0$ otherwise. It follows that $f^k(x) = \delta_1(x)f_1^k(x) + \cdots + \delta_t(x)f_t^k(x)$, and hence $f^k = \mathrm{id}$ iff $f_i^k = \mathrm{id}$ for all k. If $n_1, n_2, \ldots, n_t$ denote the sizes of $S_1, S_2, \ldots, S_k$, respectively, then by the first part we proved above, we know that $f_i^{n_i} = \mathrm{id}$ and that n_i is the smallest positive integer with the property. It follows that for all n divisible by

$N := \mathrm{lcm}(n_1, n_2, \ldots, n_t)$ we have that $f^n = \mathrm{id}$, and N is the smallest positive integer with this property.

Exercise 5.2. Let A be the matrix representation of S and B be that of R, as suggested in the exercise. By definition, $S \circ R = \{(i,j) \mid \exists \ell \colon (i,\ell) \in S \wedge (\ell,j) \in R\}$. Therefore, $(i,j) \in S \circ R$ iff there exists ℓ such that $A_{i\ell} \wedge B_{\ell j}$ is one, which is the case iff $\vee_{\ell=1}^{n} A_{i\ell} \wedge B_{\ell j}$ is one.

Exercise 5.3. Here is a list in terms of their Hasse diagrams:



Exercise 5.4.

1. We have the following:

   (a) Reflexivity: since $(a,a) \in R$ for $a \in A$, and $(b,b) \in B$ for $b \in B$, we have $((a,b),(a,b)) \in S \times R$, by definition of $S \times R$.

   (b) Antisymmetry: suppose that $((a,b),(a',b')) \in R \times S$ and $((a',b'),(a,b)) \in R \times S$. It follows by the definition of $R \times S$ that $(a,a'),(a',a) \in R$, so $a = a'$ by the antisymmetry of R. In the same way, we prove that $b = b'$.

   (c) Transitivity: suppose that $((a,b),(a',b')),((a',b'),(a'',b'')) \in R \times S$. By the definition of $R \times S$, we deduce that $(a,a'),(a',a'') \in R$, and hence $(a,a'') \in R$ by the transitivity of R. In the same way, $(b,b'') \in S$. Hence, by definition, $((a,b),(a'',b'')) \in R \times S$.

   To show that the product of two lattices is again a lattice, let $(a_1,b_1),(a_2,b_2)$ be two elements of $A \times B$. Let $a_3 := a_1 \wedge a_2$ and $b_3 = b_1 \wedge b_2$. Then $(a_3,b_3) = (a_1,b_1) \wedge (a_2,b_2)$: by definition, $a_3 \leq a_1$ and $a_3 \leq a_2$, and the same for the b's. On the other hand, if $(a_4,b_4) \leq (a_1,b_1)$ and $(a_4,b_4) \leq (a_2,b_2)$, then, since $a_4 \leq a_1$ and $a_4 \leq a_2$, we know that $a_4 \leq a_3$, and in the same way $b_4 \leq b_3$. Hence, (a_3,b_3) is the infimum of (a_1,b_1) and (a_2,b_2). The existence and uniqueness of the supremum is proved analogously.

2. Suppose that $\gcd(n, m) = 1$. Then for every $d \mid nm$ there are uniquely determined $d_1 \mid n$ and $d_2 \mid m$ such that $d = d_1 d_2$. Consider the map $f\colon \mathrm{Div}(n) \times \mathrm{Div}(m) \to \mathrm{Div}(nm)$, mapping (d_1, d_2) to $d_1 d_2$. The aforementioned fact shows that this map is a bijection. Moreover, $((d_1, d_2), (m_1, m_2)) \in (\mathrm{Div}(n), |) \times (\mathrm{Div}(m), |)$ iff $d_1 \mid m_1$ and $d_2 \mid m_2$, which in this case means that $d_1 d_2 \mid m_1 m_2$. This shows that the mapping f is a bijection between $(\mathrm{Div}(n), |) \times (\mathrm{Div}(m), |)$ and $\mathrm{Div}(nm)$.

   We will now show that if $\gcd(n, m) \neq 1$, then $|\mathrm{Div}(n) \times \mathrm{Div}(m)| \neq |\mathrm{Div}(nm)|$. This shows that the structures of the lattices given are not the same. Let $\sigma(n) := |\mathrm{Div}(n)|$. We saw above that $\sigma(mn) = \sigma(m)\sigma(n)$ if m and n are coprime. Hence, $\sigma(\prod_{i=1}^{t} p_i^{a_i}) = \prod_{i=1}^{t} \sigma(p_i^{a_i})$, wherein the p_i are distinct primes, and the a_i are positive integers. It is easily seen that $\sigma(p_i^{a_i}) = (a_i + 1)$, so that $\sigma(\prod_{i=1}^{t} p_i^{a_i}) = \prod_{i=1}^{t}(a_i + 1)$. So, if $n = p^a n'$ and $m = p^b m'$ where p is a prime not dividing $m'n'$, then $\sigma(mn) = (a+b+1)\sigma(m'n') \neq (a+1)\sigma(n')(b+1)\sigma(m')$, if both a and b are larger than one. This shows the assertion.