

# Topics in Algebra, Chapter 1 Solutions

David Sillman

2022

# 1.1 - Set Theory

- (1a) If  $A \subset B$  and  $B \subset C$ , then every element  $a \in A$  is also  $a \in B$ . Likewise,  $B \subset C \Leftrightarrow (a \in B \Rightarrow a \in C)$ . Thus, every element  $a \in A$  is also in  $C$ . Therefore,  $A \subset C$ .
- (1b) If we presuppose that  $B \subset A$ , this means that  $x \in B \Rightarrow x \in A$ . In set-builder notation, we know that

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

Because every element of  $B$  is also in  $A$ , the set builder is reduced to

$$A \cup B = \{x \mid x \in A\} = A$$

Conversely, if we start by supposing that  $A \cup B = A$ , this implies, by logical necessity, that

$$(x \in A) \Leftrightarrow (x \in A \vee x \in B)$$

As alluded to above, this is logically transformable into the statement that  $x \in B \Rightarrow x \in A$ , and thus  $B \subset A$ .

## 1.1 - Set Theory

(1c) In the set  $B \cup C$ , every element satisfies  $x \in B \vee x \in C$ . Likewise, in  $A \cup C$ , every element satisfies  $x \in A \vee x \in C$ . In the case that  $x \in C$ , the right side of the disjunction is satisfied in both sets. If  $x \in B$ , then  $B \subset A$  implies that  $x \in A$ , and so both sets are satisfied again. This means that every element in  $B \cup C$  is in  $A \cup C$ , and so  $B \cup C \subset A \cup C$ .

Similarly, every element of  $B \cap C$  satisfies  $x \in B \wedge x \in C$  and every element of  $A \cap C$  satisfies  $x \in A \wedge x \in C$ . Because, again, due to  $B \subset A$ , we have that  $x \in B \Rightarrow x \in A$  and thus every element in  $B \cap C$  must also be in  $A \cap C$  and so  $B \cap C \subset A \cap C$ .

# 1.1 - Set Theory

- (2a) The commutativity of set intersection ( $\cap$ ) and set union ( $\cup$ ) follow from the analogous commutativity properties of logical operators  $\wedge$  and  $\vee$ , respectively. Because  $A \cap B$  consists of the elements which satisfy

$$x \in A \wedge x \in B \quad \equiv \quad x \in B \wedge x \in A$$

and thus it follows that  $A \cap B = B \cap A$ . The same argument follows for  $A \cup B = B \cup A$ .

- (2b) As with the last problem, the associativity of  $\cap$  follows from the associativity of logical  $\wedge$ . That is, the set  $(A \cap B) \cap C$  consists of elements which satisfy,

$$(x \in A \wedge x \in B) \wedge x \in C \quad \equiv \quad x \in A \wedge (x \in B \wedge x \in C)$$

And thus, exactly those same elements satisfy the necessary condition for being elements of  $A \cap (B \cap C)$ , giving the equality  $(A \cap B) \cap C = A \cap (B \cap C)$ .

## 1.1 - Set Theory

- (3) Logically speaking, the elements of  $A \cup (B \cap C)$  are those which satisfy  $x \in A \vee (x \in B \wedge x \in C)$ . By the distributivity of  $\vee$ , it follows that this logical condition is equivalent to the condition,

$$x \in A \vee (x \in B \wedge x \in C) \quad \equiv \quad (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$$

And thus, the elements in the former set must be exactly those elements in the latter set, giving the equality  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ .

- (4a) The elements of  $(A \cap B)'$  are those which satisfy  $\neg(x \in A \wedge x \in B)$ . Applying De Morgan's logical negation rules, we get that this is logically equivalent to  $x \notin A \vee x \notin B$ . The set whose elements all satisfy this condition is identically  $A' \cup B'$ .
- (4b) As in the last problem, we translate the set  $(A \cup B)'$  into the membership condition  $\neg(x \in A \vee x \in B)$ . De Morgan transforms this into the membership condition  $x \notin A \wedge x \notin B$ . This membership condition corresponds to the identical set,  $A' \cap B'$ .

## 1.1 - Set Theory

- (5) There are two cases: (i)  $A$  is disjoint from  $B$  ( $A \cap B = \emptyset$ ), or (ii)  $A$  is not disjoint from  $B$  ( $A \cap B \neq \emptyset$ ).

In case (i), we trivially have that  $o(A \cap B) = o(\emptyset) = 0$ . So, it is trivially the case that every element of  $A$  is represented in  $A \cup B$  and likewise for  $B$ , and all of these elements are distinct. Therefore,  $o(A \cup B) = o(A) + o(B)$ , which works for our hypothesis given that  $o(A \cap B) = 0$ .

In case (ii), let's suppose that there are  $k$  elements in common between  $A$  and  $B$ , such that  $o(A \cap B) = k$ . Because  $A \cup B$  will only contain one copy of each of the common elements, we must subtract  $o(A \cap B)$  from  $o(A) + o(B)$  to get the number of unique elements in  $A \cup B$ .

## 1.1 - Set Theory

- (6) First, we construct on  $A$  a bijective index  $i : A \rightarrow [n]$ . Every subset  $S \subset A$  is uniquely identified by an  $n$ -tuple of binary variables  $(b_1, \dots, b_n) \in B$ , with  $b_i \in \{0, 1\}$ . It's trivial to see that the set of all binary  $n$ -tuples  $B$  has  $2^n$  elements. From this set, we have a bijection which generates (and indexes) the set of all subsets of  $A$  (hereafter called the *power set* of  $A$ ,  $\mathcal{P}(A)$ ). That is, we define  $\sigma : B \rightarrow \mathcal{P}(A)$  via the map

$$\sigma : b \mapsto \bigcup_{b_j=1} i^{-1}(j)$$

In other words, if a particular subset had  $b_j = 1$ , this means the element  $a \in A$  with  $i(a) = j$  is included in the subset. Because there exists a bijective map between the finite sets  $B$  and  $\mathcal{P}(A)$ , we have that they are the same size. Therefore,  $\mathcal{P}(A)$  has  $2^n$  elements.

## 1.1 - Set Theory

- (7) Let  $S$  be the set of Americans. Let  $C$  be the set of Americans that like cheese, and  $A$  be the set of Americans that like apples. The proportions given suggest that  $|C|/|S| = 0.63$  and that  $|A|/|S| = 0.76$ . Because both  $C \subset S$  and  $A \subset S$ , we expect  $C \cup A \subset S$ . This necessitates that

$$\begin{aligned}|C \cup A| &\leq |S| \\ |C| + |A| - |C \cap A| &\leq |S|\end{aligned}$$

Rearranging terms and dividing through by  $|S|$ , we get a bound on the proportion of Americans which like both cheese and apples:

$$\begin{aligned}|C \cap A| &\geq \frac{|C|}{|S|} + \frac{|A|}{|S|} - 1.0 \\ |C \cap A| &\geq 0.63 + 0.76 - 1.0 \\ |C \cap A| &\geq 0.39\end{aligned}$$

In English, no fewer than 39% of Americans like both cheese and apples.



## 1.1 - Set Theory

- (8) Recall that set difference  $A - B$  entails the membership condition  $x \in A \wedge x \notin B$ . This means that the *symmetric difference*  $A * B$  entails the membership condition,

$$(x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)$$

By double-distributing the disjunction, we get to a CNF representation, and then set-difference:

$$\begin{aligned} & (x \in A \vee x \in B) \wedge (x \in A \vee x \notin A) \wedge \\ & (x \notin B \vee x \in B) \wedge (x \notin B \vee x \notin A) \\ & \quad \Downarrow \\ & (x \in A \vee x \in B) \wedge (x \notin B \vee x \notin A) \\ & \quad \Downarrow \\ & (x \in A \vee x \in B) \wedge \neg(x \in A \wedge x \in B) \end{aligned}$$

This shows logical equivalence in membership between  $A * B$  and  $(A \cup B) - (A \cap B)$ .

# 1.1 - Set Theory

(9a) For brevity, we argue non-symbolically. Every element of  $(A + B)$  is either unique to  $A$  or unique to  $B$ . Taking the symmetric difference, then,  $(A + B) + C$  must result in those elements which are either unique to  $A$ , unique to  $B$ , unique to  $C$ , or common to all three of them.

Likewise, the elements of  $(B + C)$  are those elements unique to  $B$  and unique to  $C$ . Taking the symmetric difference, we see that  $A + (B + C)$  is the set of elements which are unique to  $A$ , unique to  $B$ , unique to  $C$ , or common to all three. Therefore, the sets are equal and so  $(A + B) + C = A + (B + C)$ .

## 1.1 - Set Theory

- (9b) Reducing the symmetric differences and distributing the leftmost conjunction,

$$\begin{aligned} & A \cap ((B - C) \cup (C - B)) \\ & (A \cap (B - C)) \cup (A \cap (C - B)) \end{aligned}$$

We then use the fact that intersection distributes over set difference:

$$\begin{aligned} & ((A \cap B) - (A \cap C)) \cup ((A \cap C) - (A \cap B)) \\ & \quad \Downarrow \\ & A \cdot B + A \cdot C \end{aligned}$$

- (9c) It's trivially the case that  $A \cdot A = A \cap A = A$ .

## 1.1 - Set Theory

- (9d) Every element of  $A$  is also (identically) an element of  $A$ , so there are no elements unique to either set. Therefore,  $A + A = \emptyset$
- (9e) Taking the left-symmetric-difference from  $A$  of both sides of the equation and applying the associativity from part (a) with the cancellation property of part (d), we get:

$$\begin{aligned}A + (A + B) &= A + (A + C) \\(A + A) + B &= (A + A) + C \\ \emptyset + B &= \emptyset + C\end{aligned}$$

Trivially, the symmetric difference of any set with the empty set is simply the set itself, which gives us  $B = C$ .

## 1.1 - Set Theory

- (10a) The relation of having a common ancestor is reflexive, symmetric and transitive. Therefore, it is a valid equivalence relation.
- (10b) The relation of living within 100 miles of each other is reflexive and symmetric, but not transitive. Therefore, it is not a valid equivalence relation.
- (10c) The relation of having the same father is reflexive, symmetric and transitive. Therefore, it is a valid equivalence relation.
- (10d) The relation of having the same absolute value is reflexive, symmetric and transitive. Therefore, it is a valid equivalence relation.
- (10e) The relation of being strictly greater and strictly lesser than one another is impossible to satisfy. Therefore, it is not a valid equivalence relation.
- (10f) The relation of two lines having the same slope in the plane is reflexive, symmetric and transitive. Therefore, it is a valid equivalence relation.

# 1.1 - Set Theory

- (11a) Using only symmetry and transitivity, we do not have a guarantee that there exists a  $b$  for  $a$  such that  $a \sim b$ . Thus, this argument does not account for cases that each equivalence class  $[a]$  are each only individual elements.
- (11b) If we include a property known as *seriality*, which necessitates that every  $a$  has a  $b$  such that  $a \sim b$ . Under this assumption, both symmetry and transitivity imply reflexivity.

# 1.1 - Set Theory

- (12) Clearly,  $a \sim a$  because 0 is a multiple of  $n$ . Likewise, if  $a \sim b$ , then it means  $a - b = pn$  and so  $b - a = -pn$ , which is also a multiple of  $n$ , implying  $b \sim a$ . Finally,  $a \sim b$  and  $b \sim c$  mean that  $a - b = pn$  and  $b - c = qn$ . Adding the equations together gives us  $a - c = (p + q)n$ , so  $a \sim c$ . Therefore, differing by a multiple of  $n$  is a valid equivalence relation. Each of the equivalence classes are defined to be  $\text{cl}(i) = \{x \in \mathbb{Z} \mid x \equiv i \pmod{n}\}$ . Because every integer must have a remainder in  $[n]$  after division by  $n$ , we have that  $\text{cl} : [n] \rightarrow \mathbb{Z}$  is a surjection, and so there are at most  $n$  equivalence classes. Because each equivalence class  $\text{cl}(i)$  trivially contains  $i$  for  $0 \leq i < n$ , we have that there are at least  $n$  equivalence classes. Therefore, there are exactly  $n$  equivalence classes.

## 1.1 - Set Theory

- (13) It's clear that being in the same mutually disjoint subset  $A_\alpha$  is a valid equivalence relation. This follows from the demonstrable reflexivity, symmetry and transitivity. Moreover, the equivalence classes must be the distinct  $A_\alpha$ 's because that is how we defined our equivalence.



## 1.2 - Mappings

As a matter of notation, I invoke  $\sqrt{t}$  as meaning the *positive square root* of  $t$ , so  $\sqrt{t} \geq 0$ .

- (1a)  $\sigma$  is surjective, but not injective. Every  $t \in T$  has preimages  $\sigma^{-1}(t) = \{-\sqrt{t}, \sqrt{t}\}$ .
- (1b)  $\sigma$  is both injective and surjective. Every  $t \in T$  is mapped to its preimage  $\sigma^{-1}(t) = \sqrt{t}$ .
- (1c)  $\sigma$  is injective, but not surjective. Only the perfect squares  $t \in T$  have preimages of the form  $\sigma^{-1}(t) = \sqrt{t}$ .
- (1d)  $\sigma$  is injective, but not surjective. Only the even integers  $t \in T$  have preimages of the form  $\sigma^{-1}(t) = t/2$ .

## 1.2 - Mappings

- (2) I define the injection  $\alpha : S \times T \rightarrow T \times S$  as the “swap” map,  $\alpha : (s, t) \mapsto (t, s)$ . This map is provably an injection because

$$(t, s) = (t', s') \quad \Leftrightarrow \quad (s, t) = (s', t')$$

So, this injection,  $\alpha$ , is evidence of the one-to-one correspondence between the sets.

- (3a) As in problem (2), the injection  $\alpha : (S \times T) \times U \rightarrow S \times (T \times U)$  defined by  $\alpha : ((s, t), u) \mapsto (s, (t, u))$  evidences a one-to-one correspondence between the sets.
- (3b) We define the injection  $\alpha : (S \times T) \times U \rightarrow S \times T \times U$  via the map  $\alpha : ((s, t), u) \mapsto (s, t, u)$ , which evidences the one-to-one correspondence between the sets.

## 1.2 - Mappings

- (4a) If there's a one-to-one correspondence between  $S$  and  $T$ , then there exists an injection  $\sigma : S \rightarrow T$  satisfying  $\sigma(s) = \sigma(s') \Rightarrow s = s'$ . This injection induces an inverse injection,  $\sigma^{-1} : T \rightarrow S$  defined by  $\sigma^{-1}(t) = \{s \in S \mid \sigma(s) = t\}$ . The injection  $\sigma^{-1}$  evidences a one-to-one correspondence between  $T$  and  $S$ .
- (4b) Suppose that the injections  $\alpha : S \rightarrow T$  and  $\beta : T \rightarrow U$  evidence the one-to-one correspondences between  $S$  and  $T$ , and  $T$  and  $U$  respectively. Then we can define the composed injection  $\sigma : S \rightarrow U$  via the map  $\sigma : s \mapsto \beta(\alpha(s))$ . Because  $\beta(t) = \beta(t') \Rightarrow t = t'$  and  $\alpha(s) = \alpha(s') \Rightarrow s = s'$ , it follows that  $\sigma(s) = \sigma(s') \Rightarrow s = s'$  and thus  $\sigma$  is injective. This shows that there is a one-to-one correspondence between  $S$  and  $U$ .

## 1.2 - Mappings

- (5) Because the identity automorphism  $\iota : s \mapsto s$ , it's clear that  $\sigma \circ \iota : s \mapsto \sigma(s)$ , which is identical to the map  $\sigma : s \mapsto \sigma(s)$ . An identical argument holds for  $\iota \circ \sigma$ , and so it holds that  $\sigma = \sigma \circ \iota = \iota \circ \sigma$ .
- (6) Because we know that  $|S^*| > |S|$  for any set, it is impossible for any mapping of the  $|S|$  elements of  $S$  to cover the  $|S^*|$  elements of  $S^*$ . Therefore, no mapping  $S \rightarrow S^*$  will ever be surjective.
- (7) We can consider constructing an element  $\sigma \in A(S)$  as a sequence of choosing unique images  $\sigma(s_i)$  for each  $s_i \in S$ ,  $1 \leq i \leq n$ .  $s_1$  could have any one of the  $n$  elements of  $S$  as its image. Each subsequent  $s_i$  will have one fewer option for its image. This generates a set of  $n!$  distinct automorphisms, and this set is  $A(S)$ .

## 1.2 - Mappings

- (8a) Suppose for the sake of argument that  $\sigma : S \rightarrow S$  is surjective, but not injective. Specifically, suppose that there exists an  $s^* \in S$  with more than one preimage,  $\gamma = \sigma^{-1}(s^*)$ . Then, it follows that  $\sigma$  is still surjective if its restriction  $\bar{\sigma} : S - \gamma \rightarrow S - s^*$  is surjective (note that we must remove  $\gamma$  from our domain in order to enforce the constraint that an element of the domain cannot have two different images). However, the domain of  $\bar{\sigma}$  is smaller than its codomain, which means that  $\bar{\sigma}$  cannot be surjective because no element of the domain can map to two different images. Therefore, neither  $\bar{\sigma}$  nor  $\sigma$  itself can be surjective without also being injective.

## 1.2 - Mappings

- (8b) Using the reverse argument from problem (8a), we suppose for the sake of contradiction that  $\sigma$  is not surjective. Because it *is* injective, we have that every element  $s \in S$  in the domain is mapped to a unique image  $\sigma(s) \in S$ . Because we assume it is not surjective, we assume that there is an  $s^* \in S$  which does not have a preimage. So,  $\sigma$  maps the  $|S|$  elements of  $S$  to the  $|S| - 1$  elements of  $S - \{s^*\}$ . By the pigeonhole principle,  $\sigma$  must map two distinct inputs to the same image, and so  $\sigma$  cannot be injective. We have a contradiction, so we prove the result

$$\sigma \text{ is injective} \quad \Leftrightarrow \quad \sigma \text{ is surjective}$$

## 1.2 - Mappings

(8c) Consider the mapping  $\sigma : \mathbb{Z} \rightarrow \mathbb{Z}$  via the assignment  $n \mapsto \lfloor n/2 \rfloor$ . Clearly,  $\sigma$  is surjective because every integer can be doubled to result in one of its preimages. However, it is not injective because  $n$  has the multiple preimages  $\{2n, 2n + 1\}$ . So,  $\sigma$  is an infinite counter-example to (8a).

On the other hand, the mapping  $\sigma : \mathbb{Z} \rightarrow \mathbb{Z}$  via the assignment  $n \mapsto 2n$  is clearly injective because every integer can be doubled to result in a unique image. However, it is not surjective because the odd integers have no preimages (they are not the result of any integer being doubled). This evidences an infinite counter-example to (8b).

## 1.2 - Mappings

(9a) Consider the maps

$$\begin{array}{ll} \sigma : [2] \rightarrow [2] & \sigma : i \mapsto 1 \\ \tau : [2] \rightarrow [1] & \tau : 1 \mapsto 1 \end{array}$$

Clearly,  $\sigma$  is not surjective because 2 has no preimage. However,  $\sigma \circ \tau$  is surjective because 1 does have a preimage. So, the converse of the lemma is false.

(9b) Consider the maps

$$\begin{array}{ll} \sigma : [1] \rightarrow [2] & \sigma : 1 \mapsto 1 \\ \tau : [2] \rightarrow [2] & \tau : i \mapsto 1 \end{array}$$

Clearly,  $\tau$  is not injective because both 1 and 2 are mapped to the same image, 1. However,  $\sigma \circ \tau$  is injective because 1 has only one preimage. So, the converse of the lemma is false.



## 1.2 - Mappings

- (10) We define the map  $\kappa : \mathbb{Z} \rightarrow \mathbb{Q}$  via the assignment based on prime factorization of each integer:

$$p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} \mapsto \frac{p_1^{r_1}}{p_2^{r_2} \cdots p_n^{r_n}}$$

It's clear that the numerator and denominator are coprime, and so the image of each integer is a valid rational. Moreover, every rational has at most one preimage. If two images  $(p/q)$  and  $(p'/q')$  are equal, then it means that their components  $p = p'$  and  $q = q'$ , and so their preimages are equal,  $pq = p'q'$ . This shows that  $\kappa$  is an injection and so there is a one-to-one correspondence between the integers and the rationals.

## 1.2 - Mappings

- (11a) Trivially, because  $\sigma$  is a mapping into  $T$ , and  $\sigma(A) = \sigma_A(A)$ ,  $\sigma_A$  is thus a mapping  $A \rightarrow T$ .
- (11b) If we assume that  $\sigma$  is injective, then we know that every element of  $\sigma(S)$  is the image of exactly one  $s \in S$ . Because  $\sigma(A) \subset \sigma(S)$ , we have that every element of  $\sigma(A)$  is the image of exactly one  $a \in A$ . Because  $\sigma(A) = \sigma_A(A)$ , the same property is true of  $\sigma_A$ 's domain. Therefore,  $\sigma_A$  is injective.
- (11c) If the set of elements,  $\bar{T} \subset T$ , in  $T$  which have more than one preimage is disjoint from  $\sigma(A)$  such that  $\sigma(A) \cap \bar{T} = \emptyset$ , then  $\sigma$  will still have the property of mapping each  $a \in A$  to a unique image  $\sigma(a) \in \sigma(A)$ . Therefore,  $\sigma_A$  can still be injective, even if  $\sigma$  as a whole is not.

## 1.2 - Mappings

- (12) First, we recognize that  $\sigma(A) \subset A$ , so  $\sigma \circ \sigma(A) \subset A$ . On the other hand,  $\sigma_A(A) = \sigma(A) \subset A$ , and likewise for  $\sigma_A \circ \sigma_A(A)$ . Because of this equality, we have that  $\sigma \circ \sigma(A) = \sigma_A \circ \sigma_A(A)$ , and so the domain of both  $(\sigma \circ \sigma)_A$  and  $\sigma_A \circ \sigma_A$  are mapped to the same images, and so the functions are the same.
- (13a) Consider the proper subset  $5\mathbb{Z} \subset \mathbb{Z}$ . The injection  $\sigma : x \mapsto 5x$  evidences a one-to-one correspondence between the sets, and so  $\mathbb{Z}$  is infinite.
- (13b) Consider the proper subset  $\mathbb{R}_{>0} \subset \mathbb{R}$ . The injection  $\sigma : x \mapsto e^x$  evidences a one-to-one correspondence between the sets, and so  $\mathbb{R}$  is infinite.
- (13c) Because  $A$  is infinite, it has a subset  $\bar{A} \subset A \subset S$  with which it has a one-to-one correspondence. This means that  $S$  also has the same one-to-one correspondence with  $\bar{A}$  and so  $S$  is also infinite.

## 1.2 - Mappings

- (14) Let “ $S \rightarrow \mathbb{Z}$ ” denote that there is a one-to-one correspondence, called  $\alpha$ , between  $S$  and  $\mathbb{Z}$ . Because  $\mathbb{Z} \rightarrow \mathbb{Q}$  via the mapping  $\kappa$  from problem (10) and the transitivity proved in problem (4b), we have  $S \rightarrow \mathbb{Q}$ . Moreover, via the injection  $f : \mathbb{Q} \rightarrow \mathbb{Z} \times \mathbb{Z}$  with map  $p/q \mapsto (p, q)$ , we establish  $\mathbb{Q} \rightarrow \mathbb{Z} \times \mathbb{Z}$ . Finally, by inverting and pairing  $\alpha$ , we can inject  $A^{-1} : \mathbb{Z} \times \mathbb{Z} \rightarrow S \times S$  via the assignment  $A^{-1} : (p, q) \mapsto (\alpha^{-1}(p), \alpha^{-1}(q))$ . This injection completes our transitive chain by implying  $S \rightarrow S \times S$ , as desired.

## 1.2 - Mappings

- (15) First, we show that there exists a surjective map  $\sigma : U \rightarrow S$ . This follows from the existence of surjective maps  $\alpha : U \rightarrow T$  and  $\beta : T \rightarrow S$ , which compose to give  $\sigma = \alpha \circ \beta$ .

Second, we consider a hypothetical surjective map  $\gamma : S \rightarrow U$ . If such a map existed, its inputs could first be mapped into  $T$ , then mapped surjectively onto  $U$ . This violates our assumption that there does not exist a surjective map between  $T$  and  $U$ . So, there cannot exist a surjective map from  $S \rightarrow U$ . Therefore,  $S < U$ .

## 1.2 - Mappings

- (16) If we start by supposing that  $m < n$ , then we can easily find a surjective map  $\sigma : T \rightarrow S$  by the pigeonhole principle. Moreover, we cannot form a surjective map  $\gamma : S \rightarrow T$ . If we assign every  $s \in S$  in the domain to a unique image  $t \in T$ , then there will always be at least one element  $t^* \in T$  with no preimage in  $S$ . Therefore, there can be no surjective map from  $S \rightarrow T$ . So,  $S < T$ .

Conversely, if we start by supposing that  $S < T$ , then it is evident that there cannot exist a surjective map  $S \rightarrow T$ . If  $m \geq n$ , then we can easily find a surjective map onto  $T$  by the pigeonhole principle. Therefore, this enforces that  $m < n$ .

Both directions prove that  $S < T$  for finite sets  $S, T$  equivalently means  $m < n$ .

## 1.3 - The Integers

- (1)  $a \mid b$  implies that  $b = pa$ , while  $b \mid a$  implies that  $a = qb$ . This system is solved with  $p = q \in \{-1, 1\}$ , and so  $a = \pm b$ .
- (2)  $b$  being a divisor of  $g$  and  $h$  means we can express  $g = \alpha b$  and  $h = \beta b$ . This means that  $mg + nh = m\alpha b + n\beta b = (m\alpha + n\beta)b$ , which clearly has  $b$  as a divisor.
- (3) Clearly,  $[a, b]$  exists because it can always be at most  $ab$ , which always exists. If  $a$  and  $b$  share a common divisor,  $k$ , then  $ab/k$  satisfies condition (a), but not necessarily condition (b). This is because, unless  $k$  is the greatest common divisor of  $a$  and  $b$ , then there will be a lesser common multiple  $ab/k$  which ultimately satisfies condition (b). Therefore,  $[a, b]$  exists and is of the form  $ab/(a, b)$ .

## 1.3 - The Integers

- (4) Suppose that the prime decomposition of  $a$  and  $b$  are  $a = \alpha_1^{p_1} \cdots \alpha_n^{p_n}$  and  $b = \beta_1^{q_1} \cdots \beta_m^{p_m}$ , respectively, where each  $\alpha_i^{p_i}$  and  $\beta_i^{q_i}$  are distinct powers of primes. Because  $(a, b) = 1$ , it means that  $a$  and  $b$  have no prime factors in common. So, the set of prime powers  $A = \{\alpha^p\}_i$  and  $B = \{\beta^q\}_i$  are disjoint. However, if  $a \mid x$  and  $b \mid x$ , this means that the set of prime powers of  $x$ , denoted  $X$ , contains both  $A$  and  $B$  as (disjoint) subsets. Thus,  $A \cup B \subset X$  with  $A \cup B$  being the set of prime powers of  $ab$ . This implies that  $(ab) \mid x$ , as desired.



## 1.3 - The Integers

(5a) First, we show that  $p_1^{\delta_1} \cdots p_k^{\delta_k}$  is a common divisor of  $a$  and  $b$ . Because  $\delta_i = \min\{\alpha_i, \beta_i\}$ , it's clear that  $p_i^{\delta_i} \mid p_i^{\alpha_i}$  because  $\delta_i \leq \alpha_i$  and, likewise,  $p_i^{\delta_i} \mid p_i^{\beta_i}$  because  $\delta_i \leq \beta_i$ . Therefore,  $p_1^{\delta_1} \cdots p_k^{\delta_k}$  as a whole must at least be a common divisor of both  $a$  and  $b$ .

Second, we show that there cannot be a greater common divisor. Clearly, the prime factorization of  $(a, b)$  cannot contain any prime  $q_i$  which isn't in  $\{p\}_i$ , because then it wouldn't divide  $a$  or  $b$ . So, a greater common divisor would need to have that any  $\delta_i > \alpha_i$  or  $\delta_i > \beta_i$  for one or more  $i$ . However, it's trivial that  $p_i^{\delta_i} \nmid p_i^{\alpha_i}$  or  $p_i^{\delta_i} \nmid p_i^{\beta_i}$  for those  $i$ , implying then that such a number could not divide both  $a$  and  $b$  under these conditions. Therefore, the *greatest* common divisor must be  $(a, b) = p_1^{\delta_1} \cdots p_k^{\delta_k}$ .

## 1.3 - The Integers

(5b) As in the last problem, we begin by confirming that  $p_1^{\gamma_1} \cdots p_k^{\gamma_k}$  is a common multiple of  $a$  and  $b$ . Sure enough, because  $\gamma_i = \max\{\alpha_i, \beta_i\}$ , it follows that  $p_i^{\alpha_i} \mid p_i^{\gamma_i}$  because  $\gamma_i \geq \alpha_i$  and  $p_i^{\beta_i} \mid p_i^{\gamma_i}$  because  $\gamma_i \geq \beta_i$ . This implies that  $p_1^{\gamma_1} \cdots p_k^{\gamma_k}$  is a multiple of both  $a$  and  $b$ .

Now, we show that there cannot be a lesser common multiple. As in the last problem, it's clear that no foreign prime power  $q_i$  can appear in the prime factorization of  $[a, b]$ . If we could set any  $\gamma_i < \alpha_i$  or  $\gamma_i < \beta_i$ , then either  $p_i^{\alpha_i} \nmid p_i^{\gamma_i}$  or  $p_i^{\beta_i} \nmid p_i^{\gamma_i}$ , making it impossible for either  $a$  or  $b$  to divide  $[a, b]$ , which is a contradiction. Therefore, the *least* common multiple is  $[a, b] = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ .

## 1.3 - The Integers

- (6) The last line of the Euclidean algorithm will state that  $r_{n-1} = q_n r_n$ , which is equivalent to stating that  $r_n \mid r_{n-1}$ . The second-to-last line will read  $r_{n-2} = q_{n-1} r_{n-1} + r_n$ , which can be restated as  $r_{n-2} = q_{n-1} q_n r_n + r_n$ , which emphasizes that  $r_n \mid r_{n-2}$ . We continue this substitutive process up the chain until we reach the second-to-top line, which will read  $b = q_1 r_1 + r_2$ . Because  $r_n \mid r_1$  and  $r_n \mid r_2$ , our divisibility chain reaches  $r_n \mid b$ , which substitutes into the first line with  $a = q_0 b + r_1$ , which finally shows  $r_n \mid a$ . So, we've shown  $r_n$  is a common divisor of both  $a$  and  $b$ .

As we've shown, if there existed a larger common divisor  $r^* > r_n$ , such a common divisor would divide  $a$ ,  $b$ , and  $r_1$ . If it divided  $b$  and  $r_1$ , then it would necessarily divide  $r_2$  and upward until  $r_i = 0$ . Therefore,  $r_n = r^*$  by definition (being the last remainder until  $r_i = 0$ ). So,  $r_n = (a, b)$ .

## 1.3 - The Integers

(7a) Executing the Euclidean algorithm,

$$1128 = 34 \cdot 33 + 6$$

$$33 = 5 \cdot 6 + 3$$

$$6 = 2 \cdot 3 + 0$$

Which tells us that  $(1128, 33) = 3$ .

(7a) Executing the Euclidean algorithm,

$$6540 = 5 \cdot 1206 + 510$$

$$1206 = 2 \cdot 510 + 86$$

$$510 = 5 \cdot 86 + 80$$

$$86 = 1 \cdot 80 + 6$$

$$80 = 13 \cdot 6 + 2$$

$$6 = 3 \cdot 2 + 0$$

Which tells us that  $(6540, 1206) = 2$ .

## 1.3 - The Integers

- (8) If we suppose that no prime  $p \leq \sqrt{n}$  divides  $n$ , then it means that the prime factorization of  $n = p_1^{r_1} \cdots p_k^{r_k}$  does not contain any primes  $1 < p_i \leq \sqrt{n}$ . If the factorization contains multiple primes  $p_i, p_j > \sqrt{n}$ , then their product will be  $p_i p_j > n$ , which violates our assumption that  $n = p_1^{r_1} \cdots p_k^{r_k}$ . Therefore, such an  $n$  can have a prime factorization which consists of only one prime with power less than 2. So,  $n = p$  and thus  $n$  is prime.

## 1.3 - The Integers

- (9) We begin by supposing  $n$  is prime. By definition,  $n$ 's only divisors are  $\pm 1$  and  $\pm n$ . So, if  $1 < a = kn$ , then clearly  $n \mid a$ . Otherwise,  $a$  will share no common divisor with  $n$  and thus  $(a, n) = 1$ .

Conversely, we start by supposing either  $n \mid a$  or  $(a, n) = 1$ . The former implies  $a = kn$ . The latter implies that  $a$  and  $n$  share no common divisors. These two facts necessitate that  $n$  has no common divisors with any  $a$  which is not a multiple of  $n$ . This is equivalent to claiming that the divisors of  $n$  are only  $\pm n$  and  $\pm 1$ . Therefore, by definition,  $n$  must be prime.

## 1.3 - The Integers

- (10a) Suppose for the sake of contradiction that, despite presuppositions (1) and (2), there exists an  $n^* \geq m_0$  such that  $P(n^*)$  is false. Clearly, by presupposition (1),  $n^* \neq m_0$ . However, by recursively applying presupposition (2), we build the chain of implications:

$$P(m_0) \Rightarrow P(m_0 + 1) \Rightarrow \cdots \Rightarrow P(n^*)$$

Because we've assumed that  $P(m_0)$  is true and true cannot imply false, this chain propagates truth all the way through to  $P(n^*)$ , which necessitates that  $P(n^*)$  is true. This contradicts our assumption that  $P(n^*)$  is false, and so any and all  $n \geq m_0$  must satisfy  $P(n) = \text{true}$ .

## 1.3 - The Integers

- (10b) In presupposition (2), we substitute  $m = m_0 + 1$ . This means that, because  $P(a) = P(m_0)$  is presupposed to be true by (1), then  $P(m) = P(m_0 + 1)$  is true. Repeating this process  $k$  times allows us to show that the truth of  $P(m_0)$  alone implies the truth of  $P(m_0 + k)$ . Because every  $n \geq m_0$  is of the form  $n = m_0 + k$  for  $k \geq 0$ , this shows that every  $n \geq m_0$  can be proven to be true by repeating the above process an arbitrary number of times.



## 1.3 - The Integers

- (11) Every element of  $[i]$  is of the form  $a = \alpha n + i$  and every element of  $[j]$  is of the form  $b = \beta n + j$ . Adding these two arbitrary elements together, we get the sum

$$a + b = \alpha n + \beta n + i + j = (\alpha + \beta)n + (i + j)$$

Which is of the form  $kn + (i + j)$ , and so  $a + b \in [i + j]$ . This shows that addition is well defined under  $[i] + [j] = [i + j]$ .

Likewise, multiplying the arbitrary elements  $a \in [i]$ ,  $b \in [j]$  yield the product

$$ab = \alpha\beta n^2 + \alpha jn + \beta in + ij = (\alpha\beta n + \alpha j + \beta i)n + ij$$

Which is of the form  $kn + ij$ , and so  $ab \in [ij]$ . This shows that multiplication is well defined under  $[i][j] = [ij]$ .

## 1.3 - The Integers

(12a) Because  $i, j \in \mathbb{Z}$  and addition is commutative in that context, we use

$$[i] + [j] = [i + j] = [j + i] = [j] + [i]$$

(12b) As in (12a), we inherit the commutativity of multiplication in  $\mathbb{Z}$ , we use

$$[i][j] = [ij] = [ji] = [j][i]$$

(12c) Because  $i, j, k \in \mathbb{Z}$  and addition is associative in that context, we use

$$\begin{aligned} ([i] + [j]) + [k] &= [i + j] + [k] = [(i + j) + k] \\ &= [i + (j + k)] = [i] + [j + k] \\ &= [i] + ([j] + [k]) \end{aligned}$$

## 1.3 - The Integers

- (12d) As in (12c), we inherit the associativity of multiplication in  $\mathbb{Z}$ , we use

$$([i][j])[k] = [ij][k] = [(ij)k] = [i(jk)] = [i][jk] = [i]([j][k])$$

- (12e) Because  $i, j, k \in \mathbb{Z}$  and multiplication distributes over addition in that context, we use

$$\begin{aligned}[i]([j] + [k]) &= [i][j + k] = [i(j + k)] \\ &= [ij + ik] = [ij] + [ik]\end{aligned}$$

- (12f) Because the integers have a 0 element, we use

$$[0] + [i] = [0 + i] = [i]$$

- (12g) Because the integers have a 1 element, we use

$$[1][i] = [1i] = [i]$$

## 1.3 - The Integers

- (13) If  $(a, n) = 1$ , then equivalently there exist  $b, q$  such that  $ab + nq = 1$ . This means that  $[ab] = [1]$ , and thus  $[a][b] = [1]$ , so there exists an equivalence class,  $[b] \in J_n$  such that  $[a][b] = [1]$ .
- (14) Consider the first  $p - 1$  multiples of  $a$ ,  $\{a, 2a, \dots, (p - 1)a\}$ . Each of these must be in a unique equivalence class,  $[ia] \in J_p$ . This gives us a system of  $(p - 1)$  congruences,  $ia \in [ia] = [\alpha_i]$  where  $0 \leq \alpha_i \leq p - 1$ . Multiplying all of these congruences together gives us the congruence,

$$(p - 1)!a^{(p-1)} \equiv (p - 1)! \pmod{p}$$

When we divide both sides of the expression by  $(p - 1)!$ , we are left with the congruence

$$a^{(p-1)} \equiv 1 \pmod{p}$$

Which equivalently tells us that  $a^p \equiv a \pmod{p}$ .

## 1.3 - The Integers

- (15) We are essentially asking if there exists integers  $p, q$  such that we can equate  $mp + a = nq + b$ . Moreover, because the greatest common divisor is  $(m, n) = 1$ , we can write  $um + vn = 1$ . Multiplying this expression by  $(a - b)$  gives us an equation,  $(a - b)um + (a - b)vnb = a - b$ , which rearranges to,

$$(b - a)um + a = (a - b)vn + b$$

This shows that our solutions are  $p = (b - a)u$  and  $q = (a - b)v$ , which each give the solution, so such a system of equations is always solvable.

## 1.3 - The Integers

- (16) Let's call our product  $\chi = x_1 \cdots x_n$ . Suppose for the sake of contradiction that a prime  $p \mid \chi$ , despite  $p \nmid x_i$  for any  $i$ . If we expand each  $x_i$  into its prime factorization, then none of the primes can equal  $p$  to enforce the non-divisibility. However, the product of all of the prime factorizations must equal  $\chi$ , which is supposed to satisfy  $p \mid \chi$ . This implies that, for some prime or product of primes  $q$ ,  $p \mid q$ , which is absurd. Therefore,  $p$  must divide at least one  $x_i$  in the product,  $\chi$ .

## 1.3 - The Integers

(17) We start by supposing that  $n$  is prime. Then, if  $[a][b] = [0]$ , then  $[ab] = [0]$ , and thus we can express  $ab = kn$ . Clearly, such an equality can only hold if  $n \mid b$  or  $n \mid a$ , which is equivalent to stating that either  $[a] = [0]$  or  $[b] = [0]$ .

Conversely, we can start from  $[a][b] = [0]$  implying  $[a] = [b] = [0]$ . If we suppose that  $n$  has a nontrivial divisor,  $1 < q < n$ , then we can define  $a = q$  and  $b = n/q$ , giving  $ab = n \in [0]$ , despite  $a, b \notin [0]$ . This violates our assumption, so we prove by contradiction that such an implication can only hold if  $n$  is prime.