Topics in Algebra

David Cardozo

19 de diciembre de 2014

These are few notes and compilation of exercises of the book *Topics in Algebra.* by I. N. Herstein.

1. Preliminary notions

1.1. Set Theory

Given a set S we shall use the notation throughout $a \in S$ to read "*a is an element of S*". The set A will be said to be a *subset* of S if every element in A is an element of S, We shall write $A \subset S$. Two sets A and B are equal, if both $A \subset B$ and $B \subset A$. A set D will be called *proper subset* of S if $D \subset S$ but $D \neq S$. The null set is the set having no elements; it is a subset of every set. Given a set S we shall use the notation $A\{a \in S|P(a)\}$ to read " A is the set of all elements in S for which the property P holds.

Definition 1. *The* ***union*** *of the two sets A and B, written as $A \cup B$, is the set $\{x|x \in A \ or \ \in B\}$*

Remark when we say that x is in A or x is in B, we mean x is in at least one of A or B, and may be in both.

Definition 2. *The* ***intersection*** *of the two sets A and B, written as $A \cap B$, is the set $\{x|x \in A \ and \ x \in B\}$*

Two sets are said to be disjoint *if their intersection is empty.*

Proposition 1. *For any three sets, A, B, C we have*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Demostración. We will prove first $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. Observe $B \subset B \cup C$, so that $A \cap B \subset A \cap (B \cup C)$, in the same line of reasoning, $C \subset B \cap C$, so that $A \cap C \subset A \cap (B \cap C)$, and we conclude $(A \cap B) \cup (A \cap C) \subset (A \cap (B \cup C)) \cup (A \cap (B \cup C)) = A \cap (B \cup C)$. Now for the other direction, let $x \in A \cap (B \cup C)$, so that $x \in A$, and $x \in B \cup C$; suppose the former, and we have that $x \in (A \cap B)$. The second possibility, namely, $x \in C$, implies that $x \in A \cap C$. Thus in either case, $x \in (A \cap C) \cup (A \cap B)$, whence $A \cap (B \cup C) \subset (A \cap B)\,(A \cap C)$. Combining the two concluding assertions, they give us the equality of both sets □

Given a set T, we say that T serves as an *index set* for the family $F = \langle A_\alpha \}$ of sets if for every $\alpha \in T$, there exist a set of A_α in the family F. By the iunion of the set A_α, where α is in T, we mean the set $\{x | x \in A_\alpha \text{ for at least one } \alpha \in T\}$. We denote it by $\cup_{\alpha \in T} A_\alpha$. Similarly, we denote the intersection of the sets A_α by $\cap_{\alpha \in T} A_\alpha$. The sets A_α are mutually disjoint if for $\alpha \neq \beta$, $A_\alpha \cap A_\beta$ is the null set.

Definition 3. *Given the two sets A, B then the* ***difference set****, $A - B$, is the set $\{x \in A | x \notin N\}$*

Proposition 2. *For any set B, the set A satisfies*

$$A = (A \cap B) \cup (A - B).$$

Demostración. Again, using the same strategy used before, we will show first $(A \cap B) \cup (A - B) \subset A$, Observe that $A \cap B \subset A$, and $A - B \subset A$ so that $(A \cap B) \cup (A - B) \subset A$ Now, for the converse, we want to see $A \subset (A \cap B)$, first observe that if we suppose that $x \in A$, then either $x \in (A - B)$ or $x \in A \cap B$, so that in either case, eventually $x \in ((A \cap B) \cup (A - B))$, so we conclude $A \subset (A \cap B)$. Finally, combining the concluding assertions we have $A = (A \cap B)$ which proves our proposition. □

Observe $B \cap (A - B)$ is the null set. Observe than when $B \subset A$, we call $A - B$ the complement of B in A.

Definition 4. *The binary relation $\sim$ on A is said to be an* equivalence relation *on A if for all a, b, c in A*

- *$a \sim a$*
- *$a \sim b$ implies $b \sim a$*
- *$a \sim b$ and $b \sim c$ imply $a \sim c$*

The first of these properties is called reflexivity, the second, symmetry, and the third, transitivity

Definition 5. *If A is a set and if $\sim$ is an equivalence relation on A, then the equivalence class of $a \in A$ is the set $\{x \in A | a \sim x\}$. We write it as cl(a).*

Now it comes the first big result.

Theorem 1. *The distinct equivalence classes of an equivalence relation on A provide us with a decomposition of A as a union of mutually disjoint subsets. Conversely, given a decomposition of A as a union of mutually disjoint, nonempty subsets, we can define an equivalence relation on A for which these subsets are the distinct equivalence classes.*

Demostración. Let the equivalence relation on A denoted by $\sim$. Observe first that $a \sim s$, so that $a \in \text{cl}(a)$, whence the union of all cl(a)'s is all of A. We will now prove that two equivalence classes are either equal or disjoint, so suppose for the contrary that two distinct classes cl(a) and cl(b) their intersection is nonempty; then there exist an element $x \in$ cl(a) and $x \in$ cl(b), that is, $x \sim a$ and $x \sim b$, and by transitivity property of the equivalence relationship, we have $a \sim b$, now let $y \in$ cl(b); thus we have $b \sim y$. But, from $a \sim b$, and $b \sim y$, we have then $a \sim y$, so that, $y \in$ cl(a), and we conclude cl(b) $\subset$ cl(a), we observe also that the argument for $y \in$ cl(a) is symmetric, so that cl(a) $\subset$ cl(b), and we have the contradiction that we took two distinct classes, but cl(a) = cl(b). We conclude then that the distinct cl(a)'s are mutually disjoint and their union is A. Now for the other part of the theorem.

Suppose that $A = \cup A_\alpha$, where the a_α are mutually disjoint, nonempty sets. We define an equivalence relation $\sim$ as: given $a \in A$ (since a is in exactly one of the A_α), we define $a \sim b$ if and only if a and b are in the same A_α, we need to check if $\sim$ is an equivalence relation. First, observe $a \sim a$ since, again a is in exactly one of the A_α. Second, suppose $a \sim b$, that is $a, b \in A_\alpha$ for some unique α, which is the same as $b \sim a$. Finally, suppose $a \sim b$, and $b \sim c$ so that $a, b, c \in A\alpha$ for some unique α, and we can see that $a \sim c$.

Finally, let us observe that for any $a \in A$, cl(a) is a subset of A, so that cl(a) $\subset$ A, and $\bigcup_{\alpha \in A} cl(a) \subset A$; and let for $b \in A$, there exist a unique set cl(b) up to equivalence classes, so that $A \subset \bigcup_{\alpha \in A} cl(\alpha)$ □

1.2. Problems of Set Theory

5. For a finite set C let $|C|$ indicate the number of elements in C. If A and B are finite sets prove $|A \cup B| = |A| + |B| - |A \cap B|$

Solution Suppose A and B are finite sets, so that there exist $n, m \in \mathbb{N}$ for which $|A| = n$, and $|B| = m$. Let us remark that if D, C are finite set which are disjoint, $|D \cup C|$ is $|D| + |C|$. Given this two facts, observe $A \cup B = (A - (A \cap B)) \cup B$, and $A - (A \cap B) \cap B = \emptyset$, so that $|A \cup B| = |A| - |A \cap B| + |B|$.

6. If A is a finite set having n elements, prove that A has exactly 2^n distinct subsets.

Solution The proof is by induction. First, observe that if a set A has one element, the subset of A are $\{\emptyset, A\}$ which has 2^1 elements, so that the assertion is true for $n = 1$, now suppose that if a set A has n elements, then there are exactly 2^n distinct subsets. Now consider the set with $n + 1$ elements given by $\{a\} \cup A$, with $a \notin A$. So that the subsets of $\{a\} \cup A$ are given by first taking the subsets of A, which we know have 2^n elements, and then taking a copy of these subset and adding the element a, so that there exist:

$$2^n + 2^n = 2^n(1+1) = 2^n 2 = 2^{n+1}$$

so that for a set with $n+1$ element, there are exactly 2^{n+1} subsets. Then, by the principle of mathematical induction, we have shown that If A is a finite set having n elements, prove that A has exactly 2^n distinct subsets.

10 Let S be a set and let S^* be the set whose elements are the various subsets of S. In S^* we define an addition and multiplication as follows: If $A, B \in S^*$:

- $A + B = (A - B) \cup (B - A)$
- $A \cdot B = A \cap B$

Prove the following laws:

$$(A + B) + C = A + (B + C)$$

Proof Observe that $x \in A + B$ if and only if, $x \notin A \cap B$, so that $x \in ((A+B)+C)$ if and only if $x \notin (A+B) \cap C$, or in other words, $x \notin (A \cap B \cap C)$, which by the property that $\cap$ is associative, we have then $x \in (A + (B + C))$. So we conclude then $(A + B) + C = A + (B + C)$.

$$A \cdot (B + C) = A \cdot B + A \cdot C$$

Proof Observe:

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

$$A \cdot A = A$$

Proof By definition. $A \cdot A = A \cap A = A$

$$A + A = \emptyset$$

Proof By definition. $A + A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$

If $A + B = A + C$, then $B = C$ **Proof** Suppose is false that $B = C$, without loss of generalization, say that $x \in B$, but $x \notin C$. So two cases can happen:

i) if $x \in A + B$, observe that $x \notin A$. Note that $x \in A + B$ is equivalent to $x \in A + C$, so that $x \in C$. A contradiction.

ii) if $x \notin A+B$, we have that $x \notin A+C$, so that $x \in A \cap C$, which implies again $x \in C$. A contradiction.

We conclude then, if $A+B = A+C$, then $B = C$. (The system just described is an example of a *Boolean Algebra.*) **12.** Let S be the set of all integers an let $n > 1$ be a fixed integer. Define for $a, b \in S$, $a \sim b$ if $a - b$ is a multiple of n.

Proposition 3. $\sim$ *is an equivalence relation*

Proof First, observe that $a \sim a$ since $a - a = 0$ ad $0 \cdot n = 0$, second, suppose $a \sim b$, or in other words, $kn = a - b$ for some integer k, observe $-kn = b - a$, and we have then $b \sim a$. Finally, suppose $a \sim b$ and $b \sim c$, more explicitly, $kn = a - b$ and $gn = b - c$ for some integers k and g, take note that $kn + gn = (k + g)n = a - c$, so that $a \sim c$.

Proposition 4. *There are exactly* n *distinct classes*

Proof Let cl(0), ...,cl(n-1), be the n different equivalence classes, defined by $\sim$ as above, observe that for an integer $x \geq n$, cl(x) is: $\{m \in \mathbb{Z} | x \sim m\}$, note that if $x \geq n$ is equivalent to say that, there exist integers $E = 0, 1, ...$ and $K = 0, ..., n - 1$ such that $x = En + K$. Since $x \sim m$, $En + K \sim m$, which by definition is: there exist an integer R for which $Rn = (En+K)-m$, or $(R - E)n = K - m$, so that $K \sim m$, and since $K = 0, ..., n - 1$, w have shown for $x \geq n$, x is in the any of the equivalence classes of cl(0), cl(1), $\ldots$cl$(n - 1)$.

1.3. Mappings

We introduce the concept of a mapping of one set into another. Informally, a mapping from one set, S, into another, T, is a ruler that associates with each element in S a *unique* element t in T.

Definition 6. *If S and T are nonempty sets, then a **mapping** from S to T is a subset, M, of $S \times T$ such that for every $s \in S$ there is a unique $t \in T$ such that the ordered pair (s, t) is in M.*

Alternatively and for pedagogical reasons, we think of a mapping as a rule that associates any element $s \in S$ some element $t \in T$. We shall say that t is the image of s under the mapping. **Notation Remarks** Let σ be a mapping from S to T; we denote this by writing $\sigma : S \to T$ or $S \xrightarrow{\sigma} T$, strangely enough, if t is the image of s under σ we shall represent this fact by $t = s\sigma$. Algebraists often write mappings on the right.

Given a mapping $\tau : S \to T$ we define for $t \in T$, the inverse image of t with respect to τ to be the set $\{s \in S | t = s\tau\}$

Definition 7. *The mapping τ of S into T is said to be* ***onto*** *T if given $t \in T$ there exits an element $s \in S$ such that $t = s\tau$*

Observe that we call the subset $S\tau = \{x \in T | x = s\tau$ for some $s \in S\}$ the **image** of S under τ, then τ is onto if the image of S under τ is all of T.

Definition 8. *The mapping τ of S into T is said to be a* ***one-to-one mapping*** *if whenever $s_1 \neq s_2$, then $s_1\tau = s_2\tau$.*

Remark Observe that the mapping τ is one-to-one if for any $t \in T$ the inverse image of t is either empty or is a set consisting of one element.

Definition 9. *The two mappings σ and τ of S into T are said to be* ***equal*** *if $s\sigma = s\tau$ for every $s \in S$.*

Definition 10. *If $\sigma : S \to T$ and $\tau : T \to U$ then the* ***composition*** *of σ and τ (also called their product) is the mapping $\sigma \circ \tau : S \to U$ defined by means of $s(\sigma \circ \tau) = (s\sigma)\tau$ for every $s \in S$*

Remark that it is read from left to right; that is, $\sigma \circ \tau$: first perform σ and then do τ.

For mappings of sets, provided the products make sense, the following holds:

Proposition 5 (Associative Law). *If $\sigma : S \to T$, $\tau : T \to U$, and $\mu : U \to V$, then $(\sigma \circ \tau) \circ \mu = \sigma \circ (\tau \circ \mu)$.*

Demostración. So, lt us see that the composition makes sense to be equal, observe that $\sigma \circ \tau$ takes an element of $s \in S$ to $t \in T$ so that $(\sigma \circ \tau) \circ \mu$ make sense and takes S into V. Similarly $\tau \circ \mu$ takes T into V and $\sigma \circ (\tau \circ \mu)$ takes also S into V, so we are rest to check if both functions are equal. So, we start with an element s in S and we want to see that $s((\sigma \circ \tau) \circ \mu) = s(\sigma \circ (\tau \circ \mu))$.

By definition of the composition of maps $s((\sigma \circ \tau) = (s(\sigma \circ \tau))\mu = ((s\sigma)\tau)\mu$, whereas $s(\sigma \circ (\tau \circ \mu)) = (s\sigma)(\tau \circ \mu) = (((s\sigma)\tau)\mu$. Thus, we conclude $(\sigma \circ \tau) \circ \mu = \sigma \circ (\tau \circ \mu)$. □

Proposition 6. *Let $\sigma : S \to T$ and $\tau : T \to U$; then*

- *$\sigma \circ \tau$ is* ***onto*** *if each of σ and τ is onto.*
- *$\sigma \circ \tau$ is* ***one-to-one*** *if each of σ and τ is one-to-one.*

Demostración.

- Suppose σ, and τ both are onto functions, that is, $S\sigma = T$, and $T\tau = U$, so we establish that $(S\sigma)\tau = U$, or equivalently, $S(\sigma \circ \tau) = U$, and we have then $\sigma \circ \tau$ is onto.
- Suppose that s_1, s_2 ar elements of S, and that $s_1 \neq s_2$. By the one-to-one property of σ, $s_1\sigma \neq s_2\sigma$. Since τ is also one-to-one, and $s_1\sigma, s_2\sigma$ are distinct elements of T, $(s_1\sigma)\tau \neq (s_2\sigma)\tau$, therefore $s_1(\sigma \circ \tau) = (s_1\sigma)\tau \neq (s_2\sigma)\tau = s_2(\sigma \circ \tau)$, and we establish the lemma.

□

Now, let us suppose that σ is a one-to-one mapping of S *onto* T; we call σ a **one-to-one correspondence** between S and T. so observe that for any $t \in T$, there exist $s \in S$ such that $t = s\sigma$; and by the property of one-to-one, this s is unique. We define the mapping $\sigma^{-1} : T \to S$ by $s = t\sigma^{-1}$ if and only if $t = s\sigma$. This map, is called the **inverse** of σ. Observe $\sigma \circ \sigma^{-1}$ maps S to S, note that $s(\sigma \circ \sigma^{-1}) = (s\sigma)\sigma^{-1} = t\sigma^{-1} = s$. so that $\sigma \circ \sigma^{-1}$ is the identity operator on S, similarly $\sigma^{-1} \circ \sigma$ is again the identity mapping of T. Conversely, if $\sigma : S \to T$ is such that there exist $\mu : T \to S$ with the property that $\sigma \circ \mu$ and $\mu \circ \sigma$ are the identity mappings on S and T respectively, we claim that σ is a one-to-one correspondence between S and T. First, observe that σ is onto, this given by the fact that, let $t \in T$, so that $= t = tI_t = t(\mu \circ \sigma) = (t\mu)\sigma$, and we take note that $t\mu \in S$ so that we shown that there exist $s \in S$ such that $t = s\sigma$ for any t and we conclude, σ is onto. Second, suppose $s_1\sigma = s_2\sigma$; take note that $s_1 = s_1I_s = s_1(\sigma \circ \mu) = (s_1\sigma)\mu = (s_2\sigma)\mu = s_2(\sigma \circ \mu) = s_2I_s = s_2$ The preceding discussion proves then:

Proposition 7. *The mapping $\sigma : S \to T$ is a **one-to-one correspondence** between S and T if and only if there exist a mapping $\mu : T \to S$ such that $\sigma \circ \mu$ and $\mu \circ \sigma$ are the identity mappings on S and T respectively.*

Definition 11. *If S is a nonempty set then $A(S)$ is the **set of all one-to-one mappings** of S onto itself.*

$A(S)$ plays a universal type of role in groups. We state the following theorem as the recollection of th previous lemma and results:

Theorem 2. *If σ, τ, μ are elements of $A(S)$, then:*

- *$\sigma \circ \tau$ is in $A(S)$.*
- *$(\sigma \circ \tau) \circ \mu = \sigma \circ (\tau \circ \mu)$.*
- *There exist an element i (the identity map) in $A(S)$ such that $\sigma \circ i = i \circ \sigma = \sigma$.*
- *There exist an element $\sigma^{-1} \in A(S)$ such that $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = i$.*

Demostración.

- Given by Proposition 6
- Given by Proposition 5 *em Given by Proposition 7*
- *Given by Proposition 7*

□

Proposition 8. *If S has more than two elements we can find two elements σ, τ in $A(S)$ such that $\sigma \circ \tau \neq \tau \circ \sigma$.*

Demostración. Consider U subset of S, with S having more than three elements, let us also suppose that the cardinality of U is 3. Define T as the complement of U with respect to S, that is, $T = S - U$. Now consider F the set of all one-to-one mappings and onto functions on S that fix T, i.e if $f \in F$ then $f(t) = t$ for all $t \in T$. Observe then that all functions on F are uniquely determined by the values of $f|_U : S \to S$. Let us rename the elements of U with x_1, x_2, x_3, define the mapping $\sigma \in F$ by $\sigma : S \to S$ by $x_1\sigma = x_2$, $x_2\sigma = x_3$, $x_3\sigma = x_1$, and the rest is determined already since $\sigma \in F$. Define the mapping $\tau : S \to S$, and $\tau \in F$ by $x_2\tau = x_3$, $x_3\tau = x_2$ and $x_1\tau = x_1$. Take note, $x_1(\sigma \circ \tau) = x_3$ but that $x_1(\tau \circ \sigma) = x_2 \neq x_3$. Thus $\sigma \circ \tau \neq \tau \circ \sigma$ □

1.4. Problems of Mappings

2 If S and T are nonempty sets, prove that there exists a correspondence between $S \times T$ and $T \times S$

Proof Let us define the following mappings:

$$\begin{aligned} \sigma : (S \times T) &\to (T \times S) \\ (s,t) &\longmapsto (t,s) \end{aligned}$$

and

$$\begin{aligned} \mu : (T \times S) &\to (S \times T) \\ (t,s) &\longmapsto (s,t) \end{aligned}$$

Observe first that, $\sigma \circ \mu = i_{(S\times T)}$, since $(s,t)(\sigma \circ \mu) = ((s,t)\sigma)\mu = (t,s)\mu = (s,t) = (s,t)i_{(S\times T)}$, similarly for $\mu \circ \sigma = i_{(T\times S)}$

4.a If there is a one-to-one correspondence between S and T, prove that there exist a one/to/one correspondence between T and S.

Proof Suppose $\sigma : S \to T$ is a one-to-one correspondence between S and T, so that, there exist a mapping $\mu : T \to S$ for which:

$$\begin{aligned} \sigma \circ \mu &= i_S \\ \mu \circ \sigma &= i_T \end{aligned}$$

Clearly, μ is a one-to-one correspondence between T and S.

4.b If there is a one-to-one correspondence between S and T and between T and U, prove that there is a one-to-one correspondence between S and U

Proof Suppose $\sigma : S \to T$ is a one-to-one correspondence between S and T, $\mu : T \to U$ is a one-to-one correspondence between T and U. Observe then, we have the following relations:

$$\begin{aligned} \sigma : S \to T &\qquad \mu : T \to U \\ \sigma^{-1} : T \to S &\qquad \mu^{-1} U \to T \end{aligned}$$

We want to see that $(\sigma \circ \mu)$ is a one-to-one correspondence between S and U.

First, we want to see that $(\sigma \circ \mu) \circ (\mu^{-1} \circ \sigma^{-1}) = i_s$, observe that it can be establish by the following chains of equalities, let $s \in S$, $s((\sigma \circ \mu) \circ (\mu^{-1} \circ \sigma^{-1})) = (s(\sigma \circ \mu))(\mu^{-1} \circ \sigma^{-1}) = ((s\sigma)\mu)(\mu^{-1} \circ \sigma^{-1}) = (((s\sigma)\mu)\mu^{-1})\sigma^{-1}$. And by the associative law for composition of functions $((s\sigma)(\mu\mu^{-1})\sigma^{-1}) = ((s\sigma)(i_t)\sigma^{-1}) = ((s\sigma)\sigma^{-1}) = si_s$, so we conclude then $(\sigma \circ \mu) \circ (\mu^{-1} \circ \sigma^{-1}) = i_s$. Similarly we take note that, $(\mu^{-1} \circ \sigma^{-1}) \circ (\sigma \circ \mu) = i_u$. and we have shown that, $(\sigma \circ \mu)$ is a one-to-one correspondence between S and U.

6. If S is any set, prove that it is *impossible* to find a mapping of S onto S^*.

Proof Recall that the definition of s^* is the set of subsets of S.

Consider any set S and any function f from S to s^*. We want to see that f is not onto S^*. So observe that for that purpose we will find some subset A of S that is not in the range f. Let us consider the set:

$$A = x \in S | x \notin f(x)$$

We remark then that A makes sense, and that, when x is in S, $f(x)$ will be a subset of S, and it might not contain x itself. So we have shown that $A \subset S$. we want to see that A is not in the range of f. Or equivalently, for each $x_0 \in S$, we have $f(x_0) \neq A$. We see that for the construction of the set A.

$$x_0 \in A \leftrightarrow x_0 \notin S$$

But this tell us that the two sets A and $f(x_0)$ differ in at least one way, explicitly one of the two contains x_0 and the other does not.

7. If the set S has n elements, prove that $A(S)$ has $n!$ elements.

Proof. Suppose S is a finite set, take note that we can enumerate all the elements of S as $x_1, x_2, ..., x_n$. Observe that if we want to construct a mapping f that is a one-to-one correspondence between S and itself, $f(x_1)$ can take up to n values, $f(x_2)$ up to $n-1$ values, ... and so on. So by the principle of counting, we conclude then, there are $n!$ mappings that are a one-to-one correspondence between S and itself.

8. If the set S has a finite number of elements, prove the following:

a. If σ maps S onto S, then σ is one-to-one

Proof. Suppose $\sigma : S \to S$ is onto S, observe that this condition is saying also that $S = \sigma S$ and the cardinality of $S, \sigma S$ is n since S is a finite set. Suppose for the sake of contradiction that σ is onto, but is not a one-to-one mapping, i.e, there exist $s_1 \neq s_2$ elements of S such that $\sigma(s_1) = \sigma(s_2)$, now consider the set $f(S) = \{\sigma(s_1), \sigma(s_2), \dots, \sigma(s_n)\}$, observe that the cardinality of $\sigma(S)$ is $n-1$, and this contradicts the fact that the cardinality of $\sigma(S)$ is n.

b. If σ is a one-to-one mapping of S onto itself, then σ is onto. **Proof.**

Suppose $\sigma : S \to S$ is a one-to-one mapping onto S. Also, suppose for the sake of contradiction that there exist a $s_x \in S$ such that for all $s \in S$ it happens that $s_s \neq s\sigma$. Since S is a finite set, enumerate the elements of the set $\{p_1, p_2, p_3, \ldots, p_{n-1}, s_x\}$, where $p_i = s_i\sigma$ for $1 \leq i \leq n-1$, observe that every p_i has a inverse image consisting of only element, observe that since σ is a one-to-one mapping, the set $s_1, \ldots, s_{n-1}$ has $n-1$ elements, so now consider the element σs_n, by the property of σ, it is forced that $s_x = \sigma s_n$, but this contradict our assumption that s_x is not the image of any of the $s \in S$.

8.c Prove, by example, that both part (a) and part (b) are false if S does not have a finite number of elements.

Onto does not implies one-to-one Let us consider the function $g : \mathbb{N} \to \mathbb{N}$, defined by:

$$g(0) = 0$$
$$g(x+1) = x$$

Observe then that $N = g\mathbb{N}$ so that is an onto function, but $g(0) = g(0+1)$ which implies is not a one-to-one function.

One-to-One function does not implies onto Consider the mapping $f : N \to N$, defined by $f(n) = 2n$, observe then that f is a one-to-one mapping but there are elements of $\mathbb{N}$, specifically natural numbers of the form $2k+1$, for which $2n = 2k+1$.

10 Prove that there is a one-to-one correspondence between the set of integers and the set of rational numbers.

Proof. to be completed

13. A set S is said to be infinite if there is a one-to-one correspondence between S and a proper subset of S. Prove

(a) The set of integers is infinite.

Proof To be added

(b) The set of real numbers is infinite.

Proof To be added

(c) If a set S has a subset A which is infinite, then S must be infinite.

Proof To be added

14 If S is infinite and can be brought into one-to-one correspondence with the set of integers, prove that there is one-to-one correspondence between S and $S \times S$

Proof. to be added

1.5. The Integers

Given a and b, with $b \neq 0$, we can divide a by b to get a nonnegative remainder r which is smaller in size than b; that is, we can find m and r

such that $a = mb + r$ where $0 \leq r < |b|$. This is commonly known as the Euclidean Algorithm. We say that $b \neq 0$ *divides* a of $a = mb$ for some m. We denote this fact as $a|b$ a divides b and $a \nmid b$ if it does not. Observe that of $a \mid 1$ then $a = \pm 1$, and also we have that if $a \mid b$ and $b \mid a$ we have $a = \pm b$, and that any b divides 0.

Definition 12. *The positive integer c is said to ne the greatest common divisor of a and b if*

- *c is a divisor of a and of b*
- *Any divisor of a and b is a divisor of c*

We shall use the notation (a, b) for the greatest common divisor of a and b. Observe that since we are forcing that the greatest common divisor be positive, the following properties holds: $(a, b) = (-a, b), (a, -b), (-a, -b)$.

Proposition 9. *if (a,b) exists then it is unique.*

Demostración. Let c_1 and c_2 be such that the condition on the previous definition holds. Observe then that $c_1 \mid c_2$ and $c_2 \mid c_1$ so that $c_1 = \pm c_2$, and since we insist on the greatest common divisor to be positive, we have then $c_1 = c_2$ □

Proposition 10. *If a and b are integers, not both* 0*, then* (a, b) *exist; moreover, we can find integers* $m_0 and n_0$ *such that* $(a, b) = m_0 a + n_0 b$

Demostración. Let M be the set defined by $M = \{ma + nb \in \mathbb{Z} | m, n \in \mathbb{Z}\}$, let us observe first that $m \neq \emptyset$, since at least one of them is not zero, either $1 \cdot a$ or $1 \cdot b$ is a nonzero integer in M. Now, let $x \in M$, i.e, $x = ma + nb$, take note that $-x = -ma + -nb$ is also in M, we conclude then that M has some positive integers. With this observation at hand, we take the smallest positive integer, $c \in M$, and we claim that $c = (a, b)$.Observe first, if $d \mid a$ and $d \mid b$, we have that $d \mid m_0 a + n_0 b$ so that $d \mid c$, and we have that c complies with the first condition of the definition. Now, given $x = ma + nb \in M$, we have by the Euclidean algorithm, $x = tc + r$, where $0 \leq r < c$, writing this explicitly, $ma + nb = t(m_0 a + n_0 b) + r$, or equivalently, $r = (m - tm_0)a + (n - tn_0)b$ and we see then, $r \in M$. Since $0 \leq r$ and $r < c$, by the choice of minimality of c, we have then $r = 0$. Thus, $x = tc$, and we have seen that for any $x \in M$ $c \mid x$ and since $a = 1a + 0b \in M$ and $b = 0a + 1b \in M$ we conclude $c \mid a$ and $c \mid b$, which is the last condition of the previous definition. □

Observe then that the previous proposition proves the existence of (a, b), and at the same time that c must be of a particular form.

Definition 13. *The integers a and b are* ***relatively prime*** *if* $(a, b) = 1$

As an immediate consequence of previous proposition, we have

Proposition 11. *If a and b are relatively prime, we can find integers m and n such that $ma + nb = 1$*

Demostración. Since $(a, b) = 1$, replace c with 1 in the previous proposition □

For the proceeding discussion we choose not to let 1 to be a prime number. By this we shall mean an integer which has no nontrivial factorization.

Definition 14. *The integer $p > 1$ is a **prime number** if its only divisors are ± 1, and $\pm p$*

Observe that this characterization is identically to say that, an integer p (larger than 1) is a prime number if and only if given any other integer n then either $(p, n) = 1$ or $p \mid n$.

Proposition 12. *If a is relatively prime to b but $a \mid bc$, then $a \mid c$*

Demostración. Suppose $a \mid bc$, and a is relatively prime to b, i.e, $(a, b) = 1$, by Bezout's identity we have then, that there exits $m, n \in \mathbb{Z}$ such that $1 = ma + nb$, observe then $c = cma + cnb$, and take note that $a \mid cma$ and $a \mid cnb$, so that $a \mid cma + cnb$, and finally since $cma + cnb = c$ we have then $a \mid c$. □

Proposition 13. *If a prime number divides the product of certain integers it must divide at least one of these integers.*

Demostración. The following proof will be done via induction.
Base case Suppose p is a prime and $p \mid a_1 a_2$, and suppose without loss of generalization $p \not| a_1$, we then must show that $p \mid a_2$. Take note $(p, a_1) \mid p$, and p is prime, so $(p, a_1) = 1$ or $(p, a_1) = p$. Observe that for the first case, the previous proposition give us the desired result. If $(p, a_1) = p$, observe then $p \mid a_1$ but that contradicts our assumption. This establish the result for $n = 2$.
Induction case Assume $n > 2$ and presume the result is true when p divides a product with less than n factors. Suppose that $p \mid a_1 a_2 a_3 \ldots a_n$. Grouping the terms, we have:

$$p \mid (a_1 \ldots a_{n-1}) a_n$$

Given by the base case, either $p \mid a_1 \ldots a_{n-1}$ or $p \mid a_n$. Observe then, if $p \mid a_n$ we are done. Otherwise, if $p \mid a_1 \ldots a_{n-1}$, then p divides one of the $a_1, \ldots, a_n n - 1$ by the hypothesis of induction. In any case, we have just shown that p divides one of the a_i so that gives us the desired result. □

Now, here comes the big theorem of this section:

Theorem 3. *Any positive integer $a > 1$ can be factored in a unique way as $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$, where $p_1 > p_2 > p_3 > \dots > p_t$ are prime numbers and where each $\alpha_i > 0$*

Demostración. Let's observe that the theorem has two important results in the back. First, the theorem is telling us that given a positive integer we can factor this integer as a product of primes. Secondly, that this factorization is unique. Let us then prove the two assertions.
Remark, the following proof will use induction, more specifically, we will use the assertion that if given a proposition P and if the proposition $P(m_0)$ is true and if the truth of $P(r)$ for all r such that $m_0 \leq r < k$ implies the truth of $P(k)$, then $P(n)$ is true for all $n \geq m_0$.
First, we will prove that every integer $a > 1$ can be factored as a product of prime powers.
Base case Certainly, for $m_0 = 2$, being a prime number, it can be factored as a product of prime numbers.
Induction case Suppose that for any integer r, $2 \leq r < k$ can be factored as a product of primes. If k itself is a prime number, then it is a product of prime powers. Suppose now, that k is not a prime number, then $k = uv$, for which $1 < u < k$ and $1 < v < k$. By the induction hypothesis, since both u and v are less than k, they can be factored as a product of prime powers. Thus $k = uv$ is such product. By the Principle of mathematical induction, we have just shown that any integer $a \geq 2$ can be factored as a product of prime powers.
Finally, we prove uniqueness. Suppose that:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$$

where $p_1 > p_2 > \dots > p_r$, $q_1 > \dots > q_s$ are prime numbers, and where each $\alpha_i > 0$ and each $\beta_i > 0$ Our objective is to prove:

- $r = s$
- $p_1 = q_1, p_2 = q_2, \dots p_r = q_r$
- $\alpha_1 = \beta_1, \dots, \alpha_r = \beta_r$

For $a = 2$ this is trivially true. Proceeding by induction we suppose that the assertion is true for all integers u, whence $2 \leq u < a$. Now, since:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$$

and since $a_i > 0$, $p_1 \mid a$, hence $p_1 \mid q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$. Take note that p_1 is a prime number and by the preceding Proposition we have $p_1 = q_i$ for some i. Thus, we have then $q_1 \geq q_i = p_1$. In the same fashion, since $q_1 \mid a$ we get $q_1 = p_j$ for some j, whence $p_1 \geq p_j = q_1$. Which combined give us the desired conclusion that $q_1 = p_1$. We have then:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = p_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$$

But observe then, that if $\alpha_1 > \beta_1$, we have then:

$$a = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = q_2^{\beta_2} \dots q_s^{\beta_s}$$

But then, p_1 divides the right hand side, but not the left hand side, which is a contradiction. Similarly for $\beta_1 > \alpha_1$, and we conclude then $\alpha_1 = \beta_1$. Now let us define:

$$b = \frac{a}{p^{\alpha_1}} = p_2^{\alpha_2} \dots p_r^{\alpha_r} = q_2^{\beta_2} \dots q_s^{\beta_s}$$

If $b = 1$, then $a_2 = 0 \dots = \alpha_r = 0$ and $\beta_2 = \dots = \beta_s = 0$; that is, $r = s = 1$, and we are done. If $b > 1$, then since $b < a$ we can apply our induction hypothesis to b to get:

- The number of distinct prime power (in b) on both sides is equal, i.e, $r - 1 = s - 1$, which implies $r = s$
- $\alpha_2 = \beta_2, \dots, \alpha_r = \beta_r$.
- $p_2 = q_2, \dots p_r = q_r$

Together and with the fact that $p_1 = q_1$ and $\alpha_1 = \beta_1$, we have then shown that the assumption that the factorization of integers less than a implies the factorization of a, which by Principle of mathematical induction, makes the proposition holds for all integers $a > 2$. □

Definition 15. *Let $n > 0$ be a fixed integer. We define $a \equiv b \mod n$ if $n \mid (a - b)$*

The congruence relation enjoy the following properties

Proposition 14. *The relation* congruence modulo n *defines an equivalence relation on the set of integers.*

Demostración. We first verify the condition of symmetric. We take note that since $n \mid 0$, we have then $n \mid (a-a)$ so that $a \equiv a \mod n$ for every a. Second, we observe then the if $a \equiv b \mod n$ we have $n \mid (a - b)$, and $n \mid -(b - a)$ so that $b \equiv a \mod n$. Finally suppose $a \equiv b \mod n$ and $b \equiv c \mod n$ so that $n \mid (a - b)$ and $n \mid (b + c)$ whence $n \mid \{(a - b) + (b - c)\}$, equivalently, $n \mid (a - c)$, which implies $a \equiv c \mod n$ □

Proposition 15. *The relation congruence modulo n has n distinct equivalence classes.*

Demostración. Let us denote the equivalence class of this relation via $[a]$, more briefly the *congruence class* of a. Given any integer a, by the Euclidean algorithm, $a = kn + r$ where $0 \leq r < n$. But observe $a - r = kn$ so that $r \in [a]$, so there are at most n congruence classes, however these classes are distinct, for if $[i] = [j]$, with $0 \leq i < j < n$, it would mean, $n \mid (j - i)$. where $j - i$ is a positive integer less than n, so that is impossible (see that $4 \not| 2$). As a consequence there are exactly n distinct congruence classes, $[0], [1], \ldots, [n-1]$ □

Proposition 16. *If $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$ and $ac \equiv bd \mod n$.*

Demostración. Suppose $a \equiv b \mod n$ and $c \equiv d \mod n$; therefore, $n \mid (a - b)$ and $n \mid (c - d)$ whence $n \mid \{(a - d) + (c - d)\}$ or equivalently $n \mid \{(a + c) - (b + d)\}$ so that $a + c \equiv b + d \mod n$. Take note that also we have, $n \mid \{(a - b)c - (c - d)d\} = ac - bd$ so that $ac \equiv bd \mod n$. □

Proposition 17. *If $ab \equiv ac \mod n$ and a is relatively prime to n, then $b \equiv c \mod n$*

Demostración. Suppose that $ab \equiv ac \mod n$, or in other words, $n \mid a(b-c)$, and since $(a, n) = 1$ by a preceding lemma above, we have then $n \mid b - c$ or more explicitly, $b \equiv c \mod n$ □

Now, let us define J_n to be the set of the congruences classes $\mod n$; i.e, $J_n = \{[0], [1], \ldots, [n-1]\}$. Let us over this set define two operations, so that given two elements, $[i]$ and $[j]$ in J_n we have:

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

Proposition 18. *The previous definitions of .^{a}ddition.^{a}nd ”multiplicationïn J_n are well defined.*

Demostración. Suppose $[i] = [i']$ and $[j] = [j']$ are elements of J_n. That is $i \equiv$ □