Lecture 6

Alex Hassett
Applied Analysis

June 4, 2025

Definition 6.1. A binary operation/relation on a set X is a function from $X \times X$ into X. Binary operators are often written $+$, $\cdot$, or $*$, and the value of the function at the ordered pair (x, y) is usually written $x + y$, $x \cdot y$, or $x * y$. An equivalent (and somewhat simpler) definition is: given a set X, a *binary relation* on X is a subset $\mathfrak{R} \subset X \times X$, which consists of all ordered pairs where the relation is said to hold. Also note that instead of $(x, y) \in \mathfrak{R}$, we write $x \,\mathfrak{R}\, y$.

Remark 6.2. Intuitively, a binary operation (operator) on a set X is a rule which associates each ordered pair of elements of X with a unique element of X. For example, consider the operator $+$ (addition) on $\mathbb{R}$. Then we have that $1 + 2 = 3 \in \mathbb{R}$ (note that $1, 2 \in \mathbb{R}$). Therefore, the ordered pair $(1, 2)$ is in the set $+ \subset \mathbb{R} \times \mathbb{R}$.

Example 6.3. Let $A \coloneqq \{1, 2, 3\}$. Consider the relation "$<$". The corresponding set of pairs (the relation) is $\{(1, 2), (1, 3), (2, 3)\}$, i.e.

$$< \coloneqq \{(1, 2), (1, 3), (2, 3)\}.$$

So $1 < 2$ holds as $(1, 2)$ is in $<$, but $3 < 1$ does not hold as $(3, 1)$ is not in the set.

Definition 6.4. A relation $\mathfrak{R}$ on a set A is said to be

(*i*) *Reflexive* if $a \,\mathfrak{R}\, a$ for all $a \in A$.

(*ii*) *Symmetric* if $a \,\mathfrak{R}\, b$ implies $b \,\mathfrak{R}\, a$.

(*iii*) *Transitive* if $a \,\mathfrak{R}\, b$ and $b \,\mathfrak{R}\, c$ implies $a \,\mathfrak{R}\, c$.

If $\mathfrak{R}$ is reflexive, symmetric, and transitive, then it is said to be an *equivalence relation.*

Definition 6.5. Let A be a set and $\mathfrak{R}$ be an equivalence relation. An *equivalence class* of $a \in A$, often denoted by $[a]$, is the set

$$[a] \coloneqq \{\, x \in A \mid a \,\mathfrak{R}\, x \,\}.$$

Theorem 6.6. If $\mathfrak{R}$ is an equivalence relation on a set A, then every $a \in A$ is in exactly one equivalence class. Moreover, $a \,\mathfrak{R}\, b$ if and only if $[a] = [b]$.

Proof. Recall that for $a \in A$, the equivalence class of a is defined as

$$[a] = \{x \in A \mid a \,\mathfrak{R}\, x\}.$$

First, we show that every $a \in A$ belongs to at least one equivalence class. Indeed, $a \in [a]$ because $\mathfrak{R}$ is reflexive, so $a \,\mathfrak{R}\, a$. Next, we prove that any two equivalence classes are either equal or disjoint. Let $a, b \in A$. Suppose $[a] \cap [b] \neq \emptyset$. Then there exists some $c \in A$ such that $c \in [a]$ and $c \in [b]$, meaning

$$a \,\mathfrak{R}\, c \quad \text{and} \quad b \,\mathfrak{R}\, c.$$

Since $\mathfrak{R}$ is symmetric, $c \,\mathfrak{R}\, b$. By transitivity, we have

$$a \,\mathfrak{R}\, c \quad \text{and} \quad c \,\mathfrak{R}\, b \quad \Rightarrow \quad a \,\mathfrak{R}\, b.$$

Now assume $a\,\mathfrak{R}\,b$. We claim that $[a]=[b]$. To show $[a]\subseteq[b]$, let $x\in[a]$. Then $a\,\mathfrak{R}\,x$. Since $a\,\mathfrak{R}\,b$ and $\mathfrak{R}$ is transitive, we obtain

$$b\,\mathfrak{R}\,a \quad \text{(by symmetry)} \quad \Rightarrow \quad b\,\mathfrak{R}\,x,$$

so $x\in[b]$. Hence $[a]\subseteq[b]$. A symmetric argument shows $[b]\subseteq[a]$. Thus, $[a]=[b]$. Conversely, suppose $[a]=[b]$. Then $b\in[b]=[a]$, so $a\,\mathfrak{R}\,b$. Finally, since equivalence classes are either equal or disjoint, and each $a\in A$ belongs to $[a]$, it follows that every element of A belongs to exactly one equivalence class. □

Theorem 6.7. Let f be a function X into Y. Let $\mathcal{A}$ be a collection of subsets of X, and let $\wp$ be a collection of subsets Y. Let $C\subset Y$. Then

(*i*) $f(\bigcup\mathcal{A})=\bigcup\{\,f(A)\mid A\in\mathcal{A}\,\}$,

(*ii*) $f^{-1}(\bigcup\wp)=\bigcup\{\,f^{-1}(C)\mid C\in\wp\,\}$,

(*iii*) $f^{-1}(\bigcap\wp)=\bigcap\{\,f^{-1}(C)\mid C\in\wp\,\}$,

(*iv*) $f^{-1}(C')=[f^{-1}(C)]'$.

Proof. To prove part (*i*), let $y\in f(\bigcup\mathcal{A})$. Then there exists $x\in\bigcup\mathcal{A}$ such that $f(x)=y$. Thus $x\in A_1$ for some $A_1\in\mathcal{A}$. Hence $y=f(x)\in f(A_1)$, and therefore $y\in\bigcup\{\,f(A)\mid A\in\mathcal{A}\,\}$. We have proved that

$$f\left(\bigcup\mathcal{A}\right)\subset\bigcup\{\,f(A)\mid A\in\mathcal{A}\,\}.$$

Now let $y\in\bigcup\{\,f(A)\mid A\in\mathcal{A}\,\}$, then $y\in f(A_1)$ for some $A_1\in\mathcal{A}$. Therefore, there exists $x\in A_1$ such that $f(x)=y$. Hence $x\in\bigcup\mathcal{A}$, and so $y=f(x)\in f(\bigcup\mathcal{A})$. We have proved that

$$\bigcup\{\,f(A)\mid A\in\mathcal{A}\,\}\subset f\left(\bigcup\mathcal{A}\right),$$

and part (*i*) now follows. To prove part (*ii*), let $x\in f^{-1}(\cup\wp)$. Then $f(x)\in\cup\wp$, and thus $f(x)\in C_1$ for some $C_1\in\wp$. Thus $x\in f^{-1}(C_1)$, and therefore $x\in\bigcup\{\,f^{-1}(C)\mid C\in\wp\,\}$. We proved that

$$f^{-1}(\cup\wp)\subset\bigcup\{\,f^{-1}(C)\mid C\in\wp\,\}.$$

Now let $x\in\bigcup\{\,f^{-1}(C)\mid C\in\wp\,\}$, then $x\in f^{-1}(C_1)$ for some $C_1\in\wp$. Therefore, $f(x)\in C_1$, and hence $f(x)\in\cup\wp$. It follows that $x\in f^{-1}(\cup\wp)$. We have proved that

$$\bigcup\{\,f^{-1}(C)\mid C\in\wp\,\}\subset f^{-1}(\cup\wp),$$

and part (*ii*) now follows. To prove part (*iii*), let $x\in f^{-1}(\cap\wp)$. Then $f(x)\in\cap\wp$, and thus $f(x)\in C_1$ for all $C_1\in\wp$. Thus $x\in f^{-1}(C_1)$ for all $C_1\in\wp$, and therefore $x\in\bigcap\{\,f^{-1}(C)\mid C\in\wp\,\}$. We have proved that

$$f^{-1}(\cap\wp)\subset\bigcap\{\,f^{-1}(C)\mid C\in\wp\,\}.$$

Now let $x\in\bigcap\{\,f^{-1}(C)\mid C\in\wp\,\}$, then $x\in f^{-1}(C_1)$ for all $C_1\in\wp$. Therefore, $f(x)\in C_1$ for all $C_1\in\wp$, and hence $f(x)\in\cap\wp$. It follows that $x\in f^{-1}(\cap\wp)$. We have proved that

$$\bigcap\{\,f^{-1}(C)\mid C\in\wp\,\}\subset f^{-1}(\cap\wp),$$

and part (*iii*) now follows. To prove part (*iv*), let $x\in f^{-1}(C')$. Then $f(x)\in C'$, and thus $f(x)\notin C$. Therefore $x\notin f^{-1}(C)$, and hence $x\in[f^{-1}(C)]'$. We have proved that

$$f^{-1}(C')\subset[f^{-1}(C)]'.$$

Now let $x\in[f^{-1}(C)]'$, then $x\notin f^{-1}(C)$. Therefore $f(x)\notin C$, and hence $f(x)\in C'$. It follows that $x\in f^{-1}(C')$. We have proved that

$$[f^{-1}(C)]'\subset f^{-1}(C'),$$

and part (*iv*) now follows. □

Remark 6.8. Note that for Theorem 6.7, in the case $\mathcal{A} = \{A, B\}$ and $\wp = \{C, D\}$, the conclusions of the theorem may be written

(*i*) $f(A \cup B) = f(A) \cup f(B)$,

(*ii*) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$,

(*iii*) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

It is not true that in general one has $f(A \cap B) = f(A) \cap f(B)$.

Theorem 6.9. Let X and Y be sets and let $f : X \to Y$. Then f is a one-to-one function if and only if

$$f(A \cap B) = f(A) \cap f(B)$$

for all subsets A and B of X. We leave the proof of this theorem as an exercise to the reader as the writer finds the proof quite tedious.

Definition 6.10. A group is a non-empty set G together with a binary operation on G, here denoted "$\cdot$", that combines any two elements, a and b, of G to form an element of G (i.e. the operation must have closure), denoted $a \cdot b$, such that the following three requirements, known as the group axioms, are satisfied:

(*i*) Associativity: for all $a, b, c \in G$, one has $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

(*ii*) Identity element: there exists an element e in G such that, for every a in G, one has $e \cdot a = a$ and $a \cdot e = a$. Note that e is unique.

(*iii*) Inverse element: for each a in G, there exists an element b in G such that $a \cdot b = e$ and $b \cdot a = e$, where e is the identity element. Note that for each a, the element b is unique.

Formally, a group $(G, \cdot)$ is an ordered pair of a set (called the "underlying set") and a binary operation (called the "group law" or "group action") on this set that satisfies the group axioms. Note that for $(G, \cdot)$ the underlying set is G and the group law is $\cdot$.

Definition 6.11. An abelian (commutative) group $(G, \cdot)$ is an ordered pair such that the group axioms are satisfied and the following axiom is satisfied:

(*iv*) For all a, b in G, $a \cdot b = b \cdot a$.

Theorem 6.12. Let $S = \mathbb{Z}^+ \times \mathbb{Z}^+ = \{(a, b) \mid a, b \in \mathbb{Z}^+\}$. Define a binary relation $\sim$ on S by declaring that

$$(a, b) \sim (c, d) \quad \text{if and only if} \quad a + d = b + c.$$

Then $\sim$ is an equivalence relation on S.

Proof. We verify the three properties of an equivalence relation.

- *Reflexivity.* For any $(a, b) \in S$, we have $a + b = b + a$, so $(a, b) \sim (a, b)$.
- *Symmetry.* Suppose $(a, b) \sim (c, d)$. Then $a + d = b + c$, which implies $c + b = d + a$, so $(c, d) \sim (a, b)$.
- *Transitivity.* Suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $a + d = b + c$ and $c + f = d + e$. Adding these equations gives

  $$(a + d) + (c + f) = (b + c) + (d + e),$$

  which simplifies to $a + f = b + e$. Thus, $(a, b) \sim (e, f)$.

Therefore, $\sim$ is an equivalence relation on S. □

Definition 6.13. The set of integers $\mathbb{Z}$ is defined to be the set of equivalence classes of $S = \mathbb{Z}^+ \times \mathbb{Z}^+$ under the relation $\sim$. That is,

$$\mathbb{Z} := \{[(a, b)] \mid (a, b) \in S\}.$$

Each element of $\mathbb{Z}$ is an equivalence class $[(a, b)]$, where $(a, b) \in S$.

Remark 6.14. The equivalence class $[(a, b)]$ is interpreted as representing the integer $a - b$. Specifically:

- If $a > b$, then $[(a, b)]$ corresponds to the positive integer $a - b$.
- If $a = b$, then $[(a, b)]$ corresponds to 0.
- If $a < b$, then $[(a, b)]$ corresponds to the negative integer $-(b - a)$.

Thus, the set $\mathbb{Z}$ represents the integers as ”formal differences” of positive integers.

Definition 6.15. An *algebraic structure* is a set G equipped with one or more operations. An *operation* on G is a function of the form

$$\star : G \times G \to G,$$

that is, a rule that assigns to each pair $(g_1, g_2) \in G \times G$ an element $g_1 \star g_2 \in G$. More generally, an algebraic structure may consist of:

- a set G,
- one or more operations on G (binary, unary, or nullary),
- and possibly one or more distinguished elements (such as an identity element).

Example 6.16. Examples of algebraic structures include:

- Groups $(G, +)$
- Rings $(R, +, \cdot)$
- Fields $(F, +, \cdot)$
- Monoids, Semigroups, Modules, Vector Spaces, etc.

Definition 6.17. Let $(G, \star)$ and $(H, \circ)$ be algebraic structures (such as groups or rings). A function $\varphi : G \to H$ is called an *isomorphism* if:

- φ is a *bijection*, and
- φ *preserves the operation*, i.e. for all $g_1, g_2 \in G$,

$$\varphi(g_1 \star g_2) = \varphi(g_1) \circ \varphi(g_2).$$

If such an isomorphism exists, we say that G and H are *isomorphic*, written $G \cong H$.

Theorem 6.18. Let $\mathbb{Z}$ be the set of equivalence classes $[(a, b)]$ defined in Definition 6.13. Define a function $\varphi : \mathbb{Z} \to \{\dots, -2, -1, 0, 1, 2, \dots\}$ by

$$\varphi([(a, b)]) = a - b.$$

We will show that φ is an isomorphism from the constructed $\mathbb{Z}$ (with the usual addition) to the traditional set of integers.

Proof. First, we show that φ is *well-defined.* Suppose $(a, b) \sim (c, d)$, i.e. $a + d = b + c$. Then

$$(a - b) = (c - d).$$

Hence $\varphi([(a, b)]) = \varphi([(c, d)])$. Thus φ is well-defined on equivalence classes. Next, we show that φ is a *bijection.*

- *Injectivity:* Suppose $\varphi([(a, b)]) = \varphi([(c, d)])$. Then $a - b = c - d$, so $a + d = b + c$, i.e. $(a, b) \sim (c, d)$, so $[(a, b)] = [(c, d)]$.

- *Surjectivity:* Given any $n \in \{\dots, -2, -1, 0, 1, 2, \dots\}$, define:

$$\begin{cases} [(n+1, 1)] & \text{if } n \geq 0, \\ [(1, 1-n)] & \text{if } n < 0. \end{cases}$$

  Then $\varphi([(n+1,1)]) = n$ or $\varphi([(1,1-n)]) = n$, so every integer is attained.

Finally, we show that φ *preserves addition.* Recall that addition in $\mathbb{Z}$ is defined by

$$[(a,b)] + [(c,d)] = [(a+c, b+d)].$$

Then,

$$\varphi\left([(a,b)] + [(c,d)]\right) = \varphi([(a+c, b+d)]) = (a+c) - (b+d) = (a-b) + (c-d).$$

On the other hand,

$$\varphi([(a,b)]) + \varphi([(c,d)]) = (a-b) + (c-d).$$

Thus,

$$\varphi\left([(a,b)] + [(c,d)]\right) = \varphi([(a,b)]) + \varphi([(c,d)]).$$

Hence φ preserves addition. Therefore, φ is an isomorphism of the constructed $\mathbb{Z}$ onto the traditional set of integers with usual addition. □

Remark 6.19. It is important to understand that the set $\mathbb{Z}$, as constructed in Definition 6.13, does not literally contain the familiar symbols $\dots, -2, -1, 0, 1, 2, \dots$. Rather, $\mathbb{Z}$ is formally defined as a set of equivalence classes $[(a,b)]$ of ordered pairs of positive integers under the equivalence relation $\sim$. The *traditional set of integers*, written as $\{\dots, -2, -1, 0, 1, 2, \dots\}$, is an intuitive and well-known representation. However, strictly speaking, this traditional set is a different set from $\mathbb{Z}$ as constructed. What connects these two sets is the *isomorphism* defined in Theorem 6.18, which establishes a precise correspondence between the equivalence classes $[(a,b)]$ and the familiar integers $n \in \mathbb{Z}$. In particular, the integers we typically write and manipulate in practice (such as -3, 0, 5) are *not* the actual elements of the set $\mathbb{Z}$ as constructed. Rather, they are shorthand for the images of equivalence classes under this isomorphism:

$$[(a,b)] \mapsto a - b.$$

Because this isomorphism is *bijective* and *preserves addition*, there is no loss of mathematical rigor in "abusing notation" and writing $n \in \mathbb{Z}$ as if the set $\mathbb{Z}$ *were* the traditional set of integers. This is a common and useful practice in mathematics. The reason we work with the integers themselves, rather than equivalence classes, is for clarity, simplicity, and intuition. The isomorphism guarantees that all algebraic properties proven in the equivalence class construction hold equally for the traditional integers, so it is both safe and convenient to adopt the familiar notation in most contexts.

Definition 6.20. The set of *negative integers* ($\mathbb{Z}^-$) is defined as

$$\mathbb{Z}^- = \{z \in \mathbb{Z} \mid z < 0\}.$$

Equivalently, in terms of the equivalence classes of Definition 6.13, we may write

$$\mathbb{Z}^- = \{[(a,b)] \in \mathbb{Z} \mid a < b\}.$$

That is, the set of negative integers consists of all equivalence classes $[(a,b)]$ where $a - b < 0$.

Remark 6.21. Note that Definition 4.22 is the formal definition for the set of all positive integers. However, this definition is not often taught and many students are told the definition of the set of all positive integers ($\mathbb{Z}^+$) is

$$\mathbb{Z}^+ = \{1, 2, 3, \dots\}.$$

However, this is not the formal definition of $\mathbb{Z}^+$ as it is an informal description of the elements of $\mathbb{Z}^+$. The "..." are an informal symbol and any attempt to formally define the ellipses (the infinite pattern) would result in Definition 4.22 (or something equivalent to Definition 4.22). Another common, incorrect, definition of $\mathbb{Z}^+$ given by students is

$$\mathbb{Z}^+ = \{\, n \in \mathbb{Z} \mid n \geq 1 \,\}.$$

However, this is too is not a formal definition because the set of all integers ($\mathbb{Z}$) is constructed from the set of all positive integers, as shown in Definition 4.13. Attempting to define $\mathbb{Z}^+$ in this way results in a circular definition.

Definition 6.22. Let $x \in \mathbb{Z}$ such that $x \geq 0$. Then $x!$, read "x factorial", is defined as

$$x! = x(x-1)(x-2)\cdots(2)(1).$$

Note that $0! = 1$. Clearly, if $x > 0$, then $x! = x \cdot (x-1)!$.

Theorem 6.23. Pascal's identity is stated as follows: If n and k and are positive integers and $n \geq k$, then

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Note that $\binom{n}{k}$ is read "n choose k".

Proof. By direct computation, we have

$$\begin{aligned}
\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\
&= (n-1)!\left[\frac{n-k}{k!(n-k)!} + \frac{k}{k!(n-k)!}\right] \\
&= (n-1)!\left(\frac{n}{k!(n-k)!}\right) \\
&= \frac{n!}{k!(n-k)!} \\
\binom{n-1}{k} + \binom{n-1}{k-1} &= \binom{n}{k},
\end{aligned}$$

as desired. □

Remark 6.24. Note that an equivalent definition for Pascal's identity is

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

where $n, k \in \mathbb{Z}^+$ and $n \geq k$.

Definition 6.25. Here we define integer exponents of real numbers. Let $x \in \mathbb{R}$. We define

(i) $x^1 = x$

(ii) $x^{n+1} = x \cdot x^n$

for $n \in \mathbb{Z}^+$. If $x \neq 0$, we define

(iii) $x^0 = 1$

(iv) $x^{-n} = \frac{1}{x^n}$

for $n \in \mathbb{Z}^+$.

Theorem 6.26. Here we list the laws of integer exponents for real numbers:

(i) $x^{m+n} = x^m x^n$ for $x \in \mathbb{R}$, $x \neq 0$, and $m, n \in \mathbb{Z}$,

(ii) $x^n = \frac{1}{x^{-n}}$ for $x \in \mathbb{R}$, $x \neq 0$, and $n \in \mathbb{Z}$,

(iii) $(xy)^n = x^n y^n$ for $x, y \in \mathbb{R}$, $x \neq 0 \neq y$, and $n \in \mathbb{Z}$,

(iv) $(x^m)^n = x^{m \cdot n}$ for $x \in \mathbb{R}$, $x \neq 0$, and $m, n \in \mathbb{Z}$,

(v) $\left(\frac{x}{y}\right)^n = \frac{x^n}{y^n}$ for $x, y \in \mathbb{R}$, $x \neq 0 \neq y$, and $n \in \mathbb{Z}$,

(vi) if $0 < x < y$, then $x^n < y^n$ for $x, y \in \mathbb{R}$ and $n \in \mathbb{Z}^+$,

(vii) if $n < m$ and $x > 1$, then $x^n < x^m$ for $x \in \mathbb{R}$ and $n, m \in \mathbb{Z}$.

We leave the proof of this theorem as an exercise to the reader.

Remark 6.27. If the reader is unfamiliar with summations, then we advise that the reader review Lecture 7 before attempting or reading the proof of Theorem 6.28.

Theorem 6.28. The Binomial Theorem is stated as follows: If a and b are real numbers and n is a positive integer, then

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Proof. Let $S(n)$ be the statement of the theorem. If $n = 1$, then we have $(a+b)^1 = a + b$. The right side is

$$\sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a + b.$$

Thus $S(1)$ is true. Suppose $S(n)$ is true. Then using Definition 6.11, we have

$$(a+b)^{n+1} = (a+b)^n (a+b).$$

Using the hypothesis, we have

$$= \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \right) (a+b)$$
$$= \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1}.$$

Let $j = k + 1$, then

$$= \sum_{k=0}^{n} \binom{n}{k} a^{(n+1)-k} b^k + \sum_{j=1}^{n+1} \binom{n}{j-1} a^{(n+1)-j} b^j$$
$$= \binom{n}{0} a^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} a^{(n+1)-k} b^k \right] + \sum_{j=1}^{n} \left[\binom{n}{j-1} a^{(n+1)-j} b^j \right] + \binom{n}{n} b^{n+1}.$$

Combining the sums in the above equation, we have

$$= \binom{n}{0} a^{n+1} + \sum_{k=1}^{n} \left(\left[\binom{n}{k} + \binom{n}{k-1} \right] a^{(n+1)-k} b^k \right) + \binom{n}{n} b^{n+1}.$$

Using Theorem 6.9 (Remark 6.10), we have

$$\begin{aligned} &= \binom{n}{0}a^{n+1} + \sum_{k=1}^{n}\left[\binom{n+1}{k}a^{(n+1)-k}b^{k}\right] + \binom{n}{n}b^{n+1} \\ (a+b)^{n+1} &= \sum_{k=0}^{n+1}\binom{n+1}{k}a^{(n+1)-k}b^{k}, \end{aligned}$$

which proves that $S(n+1)$ is true. Therefore, by Theorem 4.24 we have proven that $S(n)$ is true for all $n \in \mathbb{Z}^{+}$. □