Introduction to Abstract Algebra I: Optional Problems

Due on December 5, 2025 at 23:59

Victor Ostrik

Hashem A. Damrah
UO ID: 952102243

Exercise 0.17. Let A be a finite set, and let $|A|= s$. Based on the preceding exercise, make a conjecture about the value of $|\mathscr{P}(A)|$. Then try to prove your conjecture.

Solution. I conjecture that the cardinality of the power set of a finite set A with s elements is given by

$$|\mathscr{P}(A)|= 2^s.$$

We will prove this by induction on the number of elements in the set A. For the base case, let $|A|= 0$. Then $A = \emptyset$, and the only subset of A is the empty set itself. Thus, $|\mathscr{P}(A)|= 1 = 2^0$, which establishes the base case.

Now, assume that for some $k \geq 0$, the statement holds for all sets with k elements; that is, if $|A|= k$, then $|\mathscr{P}(A)|= 2^k$. We need to show that the statement holds for a set with $k + 1$ elements. Let A be a set with $k + 1$ elements, and let $a \in A$. We can express A as $A = B \cup \{a\}$, where B is a subset of A with k elements. By the induction hypothesis, we know that $|\mathscr{P}(B)|= 2^k$. The power set of A can be constructed by taking all subsets of B and adding the element a to each of those subsets. Therefore, the power set of A can be expressed as

$$\mathscr{P}(A) = \mathscr{P}(B) \cup \{S \cup \{a\} \mid S \in \mathscr{P}(B)\}.$$

The number of subsets in $\mathscr{P}(A)$ is thus twice the number of subsets in $\mathscr{P}(B)$, since for each subset S in $\mathscr{P}(B)$, there are two corresponding subsets in $\mathscr{P}(A)$: one that includes a and one that does not. Therefore,

$$|\mathscr{P}(A)|= 2 \cdot |\mathscr{P}(B)|= 2 \cdot 2^k = 2^{k+1}.$$

Therefore, by the principle of mathematical induction, the conjecture holds for all finite sets A with $|A|= s$.

Thus, we have shown that for any finite set A with s elements, the cardinality of its power set is given by $|\mathscr{P}(A)|= 2^s$. □

Exercise 0.18. For any set A, finite or infinite, let B^A be the set of all functions mapping A into the set $B = \{0, 1\}$. Show that the cardinality of B^A is the same as the cardinality of the set $\mathscr{P}(A)$. [Hint: Each element of B^A determines a subset of A in a natural way.]

Solution. To show that the cardinality of the set B^A is the same as the cardinality of the power set $\mathscr{P}(A)$, we will construct a bijection between these two sets.

Let $f \in B^A$ be a function that maps elements of A to either 0 or 1. We can associate each function f with a subset S_f of A defined as

$$S_f = \{a \in A \mid f(a) = 1\}.$$

In other words, S_f consists of all elements of A that are mapped to 1 by the function f. This defines a mapping $\Phi : B^A \to \mathscr{P}(A)$ given by $\Phi(f) = S_f$. Next, we need to show that this mapping Φ is both injective and surjective.

Suppose that $\Phi(f_1) = \Phi(f_2)$ for two functions $f_1, f_2 \in B^A$. This means that the subsets S_{f_1} and S_{f_2} are equal. Therefore, for every element $a \in A$, we have two cases. If $a \in S_{f_1}$, then $f_1(a) = 1$, and since $S_{f_1} = S_{f_2}$, it follows that $f_2(a) = 1$. Otherwise, then $f_1(a) = 0$, and since $S_{f_1} = S_{f_2}$, it follows that $f_2(a) = 0$. Thus, for all $a \in A$, we have $f_1(a) = f_2(a)$, which implies that $f_1 = f_2$. Therefore, Φ is injective.

Now, we need to show that Φ is surjective. Let $S \in \mathscr{P}(A)$ be any subset of A. We can define a function $f_S \in B^A$ as

$$f_S(a) = \begin{cases} 1 & \text{if } a \in S \\ 0 & \text{if } a \notin S \end{cases}.$$

By construction, we have $\Phi(f_S) = S$. Therefore, for every subset $S \in \mathscr{P}(A)$, there exists a function $f_S \in B^A$ such that $\Phi(f_S) = S$. This shows that Φ is surjective.

Since Φ is both injective and surjective, it is a bijection between the sets B^A and $\mathscr{P}(A)$. Therefore, the cardinality of B^A is the same as the cardinality of $\mathscr{P}(A)$, i.e., $|B^A|= |\mathscr{P}(A)|$. □

Exercise 0.19. Show that the power set of a set A, finite or infinite, has too many elements to be able to be put in a one-to-one correspondence with A. Explain why this intuitively means that there are an infinite number of infinite cardinal numbers. [Hint: Imagine a one-to-one function φ mapping A into $\mathscr{P}(A)$ to be given. Show that φ cannot be onto $\mathscr{P}(A)$ by considering, for each $x \in A$, whether $x \in \varphi(x)$ and using this idea to define a subset S of A that is not in the range of φ.] Is the set of everything a logically acceptable concept? Why or why not?

Solution. To show that the power set of a set A, denoted as $\mathscr{P}(A)$, has too many elements to be put in a one-to-one correspondence with A, we will use a proof by contradiction.

Assume that there exists a one-to-one function $\varphi : A \to \mathscr{P}(A)$ that is also onto, meaning that for every subset $S \in \mathscr{P}(A)$, there exists an element $x \in A$ such that $\varphi(x) = S$.

Consider the subset S of A defined as

$$S = \{x \in A \mid x \notin \varphi(x)\}.$$

In other words, S consists of all elements of A that are not contained in their corresponding subset under the function φ.

Now, since φ is assumed to be onto, there must exist an element $y \in A$ such that $\varphi(y) = S$. We now consider whether y is an element of the subset S.

If $y \in S$, then by the definition of S, it must be the case that $y \notin \varphi(y)$. However, since $\varphi(y) = S$, this implies that $y \notin S$, which is a contradiction. Otherwise, if $y \notin S$, then by the definition of S, it must be the case that $y \in \varphi(y)$. However, since $\varphi(y) = S$, this implies that $y \in S$, which is again a contradiction.

In both cases, we arrive at a contradiction. Therefore, the function φ cannot be onto $\mathscr{P}(A)$, which means that there is no one-to-one correspondence between A and $\mathscr{P}(A)$. This shows that the cardinality of $\mathscr{P}(A)$ is strictly greater than the cardinality of A, i.e., $|\mathscr{P}(A)| > |A|$.

This result intuitively means that there are an infinite number of infinite cardinal numbers because for any infinite set A, we can always find a larger set $\mathscr{P}(A)$ with a strictly greater cardinality. This process can be repeated indefinitely, leading to an infinite hierarchy of infinite cardinal numbers.

Regarding the question of whether the set of everything is a logically acceptable concept, it is not. The reason is that if we consider the "set of everything," it would include all sets, including itself. This leads to paradoxes such as Russell's paradox, which popup when we consider the set of all sets that do not contain themselves. Therefore, the concept of a "set of everything" is not well-defined, and it is not considered a logically acceptable concept. □

Exercise 1.44. Let S be a set and let $*$ be a binary operation on S satisfying the two laws

- $x * x = x$ for all $x \in S$
- $(x * y) * z = (y * z) * x$ for all $x, y, z \in S$.

Show that $*$ is associative and commutative. (This is problem B-1 on the 1971 Putnam Competition.)

Solution. We start with showing that for all $x, y \in S$, $x * y = y * x$. Using the second law, we have

$$(x * y) * z = (y * z) * x.$$

Now, let $z = x$. Then we have

$$(x * y) * x = (y * x) * x.$$

Using the first law, we know that $x * x = x$. Therefore, we can simplify both sides:

$$(x * y) * x = (y * x) * x \Rightarrow (x * y) = (y * x).$$

Thus, we have shown that $x * y = y * x$ for all $x, y \in S$, proving commutativity.

Lastly, we show that for all $x, y, z \in S$, $(x * y) * z = x * (y * z)$. Using the second law again, we have

$$(x * y) * z = (y * z) * x.$$

Now, let $z = y$. Then we have

$$(x * y) * y = (y * y) * x.$$

Using the first law, we know that $y * y = y$. Therefore, we can simplify both sides:

$$(x * y) * y = (y) * x \Rightarrow (x * y) = (y * x).$$

Since we have already established commutativity, we can rewrite this as

$$(x * y) = (x * y).$$

This shows that $(x * y) * z = x * (y * z)$ for all $x, y, z \in S$, proving associativity.

Therefore, we have shown that the binary operation $*$ is both associative and commutative. □

Exercise 2.38. Let G be a group and let $a, b \in G$. Show that $(a * b)' = a' * b'$ if and only if $a * b = b * a$.

Solution. Assume that $(a * b)' = a' * b'$. We want to show that this implies $a * b = b * a$. Taking the inverse of both sides, we have

$$(a' * b')' = (a * b).$$

Using the property of inverses in groups, we know that $(x * y)' = y' * x'$ for any elements $x, y \in G$. Applying this property to the left side, we get

$$(a' * b')' = b'' * a'' = b * a.$$

Therefore, we have $a * b = b * a$.

Conversely, assume that $a * b = b * a$. We want to show that this implies $(a * b)' = a' * b'$. Taking the inverse of both sides, we have

$$(a * b)' = (b * a)'.$$

Using the property of inverses in groups, we know that $(x * y)' = y' * x'$ for any elements $x, y \in G$. Applying this property to the right side, we get

$$(b * a)' = a' * b'.$$

Therefore, we have $(a * b)' = a' * b'$.

Thus, we have shown that $(a * b)' = a' * b'$ if and only if $a * b = b * a$. □

Exercise 2.40. Prove that a set G, together with a binary operation $*$ on G satisfying the left axioms 1, 2, and 3 given after Corollary 2.19, is a group.

Solution. Assume G is a set with a binary operation $*$ satisfying the left axioms, i.e., $*$ is associative, there exists a left identity, and every element has a left inverse. We first show that the left identity is also a right identity. Let e be the left identity, so for all $a \in G$, we have $e * a = a$. We need to show that $a * e = a$ for all $a \in G$. Let $a \in G$ and let a' be the left inverse of a, so that $a' * a = e$. Then,

$$a * e = a * (a' * a) = (a * a') * a = e * a = a.$$

Thus, e is also a right identity.

Next, we show that every element has a right inverse. Let $a \in G$ and let a' be the left inverse of a, so that $a' * a = e$. We need to find an element $b \in G$ such that $a * b = e$. We can take $b = a'$. Then,

$$a * b = a * a' = e.$$

Thus, every element has a right inverse, namely its left inverse.

Therefore, we have shown that G satisfies all the group axioms: associativity, the existence of an identity element, and the existence of inverses for every element. Hence, G is a group. □

Exercise 2.41. Prove that a nonempty set G, together with an associative binary operation $*$ on G such that

$$a * x = b \text{ and } y * a = b \text{ have solutions in } G \text{ for all } a, b \in G,$$

is a group. [Hint: Use Exercise 40.]

Solution. Since $a*x = b$ has a solution in G for all $a, b \in G$, there exists an element $e \in G$ such that $a*e = a$ for all $a \in G$. This shows that e is a right identity. It holds similarly for the second equation with $e' \in G$. Subbing $y * a = b$ into the first equation, we have

$$a * x = y * a.$$

From here, we can deduce that $x = y$ for all $a, b \in G$. Thus, we have shown that the left and right identities are equal, i.e., $e = e'$.

Next, we need to show that every element has an inverse. For the first equation, $a * x = b$, if we let $a \in G$ be arbitrary, and $b = e$ (identity element), then there exists an element $a' \in G$ such that $a * a' = e$. Similarly, for the second equation, $y * a = b$, if we let $a \in G$ be arbitrary, and $b = e$, then there exists an element $a'' \in G$ such that $a'' * a = e$. Now, we show that $a' = a''$. We have

$$a * a' = e \Rightarrow a'' * (a * a') = a'' * e \Rightarrow (a'' * a) * a' = a'' \Rightarrow e * a' = a'' \Rightarrow a' = a''.$$

Thus, every element has a two-sided inverse.

Hence, G is a group. □

Exercise 4.34. (See the warning following Theorem 4.8.) Let G be a group with binary operation $*$. Let G' be the same set as G, and define a binary operation $*'$ on G' by $x *' y = y * x$ for all $x, y \in G'$.

(i) (Intuitive argument that G' under $*'$ is a group.) Suppose the front wall of your classroom were made of transparent glass, and that all possible products $a*b = c$ and all possible instances $a*(b*c) = (a*b)*c$ of the associative property for G under $*$ were written on the wall with a magic marker. What would a person see when looking at the other side of the wall from the next room in front of yours?

(ii) Show from the mathematical definition of $*'$ that G' is a group under $*'$.

Solution to (i). A person looking at the other side of the wall from the next room would see all the products and associative properties reversed. Specifically, for every product $a * b = c$ written on the wall, they would see $b * a = c$ when looking from the other side. Similarly, for every instance of the associative property $a * (b * c) = (a * b) * c$, they would see $(c * b) * a = c * (b * a)$.

This reversal of products and associative properties corresponds to the definition of the new binary operation $*'$ on G', where $x *' y = y * x$. Therefore, the person would observe that the structure of the group is preserved, but with the order of multiplication reversed. □

Solution to (ii). To show that G' is a group under the binary operation $*'$, we need to verify the group axioms: closure, associativity, identity element, and inverses.

For any $x, y \in G'$, we have $x *' y = y * x$. Since G is a group under $*$, the product $y * x$ is also in G. Therefore, $x *' y \in G'$, satisfying closure.

For any $x, y, z \in G'$, we have

$$(x *' y) *' z = (y * x) *' z = z * (y * x),$$

and

$$x *' (y *' z) = x *' (z * y) = (z * y) * x.$$

Since G is associative under $*$, we have

$$z * (y * x) = (z * y) * x.$$

Thus, $(x *' y) *' z = x *' (y *' z)$, satisfying associativity.

Let e be the identity element in G under $*$. For any $x \in G'$, we have

$$x *' e = e * x = x \quad \text{and} \quad e *' x = x * e = x.$$

Thus, e is the identity element in G' under $*'$.

For any $x \in G'$, let x^{-1} be the inverse of x in G under $*$. Then, we have

$$x *' x^{-1} = x^{-1} * x = e \quad \text{and} \quad x^{-1} *' x = x * x^{-1} = e.$$

Thus, every element in G' has an inverse under $*'$.

Therefore, we have verified all the group axioms for G' under the binary operation $*'$. Hence, G' is a group under $*'$. □

Exercise 5.58. Let G be a group and let a be one fixed element of G. Show that

$$H_a = \{x \in G \mid xa = ax\},$$

is a subgroup of G.

Solution. Clearly, the identity element e of G is in H_a since $ea = ae$. Thus, H_a is non-empty.

Let $x, y \in H_a$. Then, by definition of H_a, we have $xa = ax$ and $ya = ay$. We need to show that the product $x * y$ is also in H_a. We have

$$(x * y)a = x(ya) = x(ay) = (xa)y = (ax)y = a(x * y),$$

since G is a group and the operation $*$ is associative. Thus, $x * y \in H_a$.

Next, we need to show that the inverse of any element in H_a is also in H_a. Let $x \in H_a$. Then, by definition of H_a, we have $xa = ax$. We need to show that x^{-1} is also in H_a. We have

$$x^{-1}a = x^{-1}(xa)x^{-1} = (x^{-1}x)ax^{-1} = eax^{-1} = ax^{-1}.$$

Thus, $x^{-1} \in H_a$.

Hence, H_a is a subgroup of G. □

Exercise 5.60. Let H be a subgroup of a group G. For $a, b \in G$, let $a \sim b$ if and only if $ab^{-1} \in H$. Show that $\sim$ is an equivalence relation on G.

Solution. To show that $\sim$ is an equivalence relation on G, we need to verify that it satisfies the three properties of an equivalence relation: reflexivity, symmetry, and transitivity.

For any $a \in G$, we have

$$aa^{-1} = e \in H,$$

where e is the identity element of G. Therefore, $a \sim a$ for all $a \in G$.

Suppose $a, b \in G$ such that $a \sim b$. This means that

$$ab^{-1} \in H.$$

Taking the inverse of both sides, we have

$$(ab^{-1})^{-1} = ba^{-1} \in H.$$

Therefore, $b \sim a$.

Suppose $a, b, c \in G$ such that $a \sim b$ and $b \sim c$. This means that

$$ab^{-1} \in H \quad \text{and} \quad bc^{-1} \in H.$$

Since H is a subgroup of G, it is closed under the group operation. Therefore, we have

$$(ab^{-1})(bc^{-1}) = ac^{-1} \in H.$$

Thus, $a \sim c$.

Since $\sim$ satisfies reflexivity, symmetry, and transitivity, it is an equivalence relation on G. □