Exercise Guide for *Algebra (2nd Edition)* by MacLane and Birkhoff

Muthu Chidambaram

Last Updated: June 16, 2019

Contents

About

> *"A modern mathematical proof is not very different from a modern machine, or a modern test setup: the simple fundamental principles are hidden and almost invisible under a mass of technical details."*
> - Hermann Weyl

What follows are short summaries of my solution ideas (most of them aren't really proofs) to exercises from the book *Algebra* (2nd Edition) by Saunders MacLane and Garrett Birkhoff. I used the 2nd Edition due to having access to a hard copy; the exercises/exposition through the majority of the 2nd and 3rd Editions are identical as far as I can tell.

1 Sets, Functions, and Integers

1.1 Sets

1.1.1 Exercise 5

When constructing a subset, each element in the set can either be in or out (2 choices). Hence, 2^n.

1.1.2 Exercise 6

There are n choices for the first element, $n-1$ choices for the second element, and so on up to $n-m$, hence dividing $n!$ by $(n-m)!$. The order of these m selected elements doesn't matter, hence the division by $m!$.

1.2 Functions

1.2.1 Exercise 2

$h_g \circ h_f$, where h corresponds to left-inverse.

1.2.2 Exercise 3

Let $f : A \to B$ and $g : B \to C$ be surjections. Then $g \circ f$ is surjective since $\exists x \in B$ such that $g(x) = y \quad \forall y \in C$, and $\exists x' \in A$ such that $f(x') = x \quad \forall x \in B$ (from the surjectivity of f and g). Proving injectivity follows similarly.

1.2.3 Exercise 4

The reverse direction follows from Exercise 3. If $f \circ g$ is injective and g is not, we could choose two elements from the domain of g that map to the same element in the domain of f (contradiction). Surjectivity is a similar argument.

1.2.4 Exercise 5

f has no right inverse since it is not surjective. There are infinitely many left inverses of f, two possibilities are mapping to square roots when possible and to 1 or 2 otherwise.

1.2.5 Exercise 6

Apply the left inverse of f.

1.2.6 Exercise 7

When surjective, use right inverse.

1.2.7 Exercise 8

Define h such that $h(y) = x$ if $\exists x \in S \mid f(x) = y$, and $h(y) = x'$ otherwise (axiom of choice necessary for choosing x). If f is injective, there will only be one choice of x, and if f is surjective, there will be some x for every y.

1.2.8 Exercise 9

Unique right inverse indicates that every element in the range has only one choice to map back to in the domain, implying injectivity.

1.2.9 Exercise 10

If g is a bijection, then we can define f such that $f(y) = x$ where $g(x) = y$. f is then a two-sided inverse. If f is a two-sided inverse of g, then every element of T maps to a unique element of S (from left inverse) and vice versa. Hence g is a bijection.

1.2.10 Exercise 11

Following the hint, we can see that $f : U \to \mathcal{F}$ is surjective since $S \in \mathcal{F} \implies S \neq \emptyset \implies \exists u \in S \implies u \in U \implies f(u) = S$. The existence of the right inverse then gives us the axiom of choice.

1.3 Relations and Binary Operations

1.3.1 Exercise 2

Symmetry + transitivity imply circularity. For the other direction, we have xRy, $yRy \implies yRx$, which gives both symmetry and transitivity.

1.3.2 Exercise 3

This only implies reflexivity for the elements $x, y \in X \mid (x, y) \in R$, not $\forall x \in X$.

1.3.3 Exercise 4

If R is transitive $T = R$. Otherwise, start with $T = R$ and add (x, z) to T whenever $(x, y), (y, z) \in R$. Repeat this process until there are no more pairs to add.

1.3.4 Exercise 5

Let $R \subset X \times Y$, $S \subset Y \times Z$, $T \subset Z \times A$.

$$\begin{aligned} xR \circ (S \circ T)a &\implies \exists y \in Y \mid xRy, y(S \circ T)a \\ &\implies \exists z \in Z \mid ySz, zTa \\ &\implies x(R \circ S)z \\ &\implies x(R \circ S) \circ Ta \end{aligned}$$

1.3.5 Exercise 6

Let $R \subset X \times Y$, $S \subset Y \times Z$.

$$\begin{aligned} z(R \circ S)^{\smile}x &\implies x(R \circ S)z \\ &\implies \exists y \in Y \mid xRy, ySz \\ &\implies yR^{\smile}x,\ zS^{\smile}y \\ &\implies z(S^{\smile} \circ R^{\smile})x \end{aligned}$$

1.3.6 Exercise 7

$$\begin{aligned} (x, z) \in G(g \circ f) &\implies \exists y \in Y \mid g(y) = z,\ f(x) = y \\ &\implies (x, y) \in G(f),\ (y, z) \in G(g) \\ &\implies (x, z) \in G(f) \circ G(g) \end{aligned}$$

1.3.7 Exercise 9

$$\begin{aligned} (x, y) \in G(f) &\implies \forall x \in X,\ \exists y \in Y \mid f(x) = y \\ &\implies \forall x \in X,\ (x, x) \in G(f) \circ G^{\smile}(f) \\ \text{and} &\quad \forall y \in \mathrm{Im} f,\ (y, y) \in G^{\smile}(f) \circ G(f) \end{aligned}$$

1.3.8 Exercise 10

$$\begin{gathered} x\Box y = u\Box(x\Box y) = (u\Box y)\Box x = y\Box x \\ x\Box(y\Box z) = x\Box(z\Box y) = (x\Box y)\Box z \end{gathered}$$

1.4 The Natural Numbers

1.4.1 Exercise 1

$f^0 = 1_X$ is trivially an injection. Suppose f^n is an injection for some $n \in \mathbb{N}$. Then $f^{\sigma(n)} = f \circ f^n$ is a composition of injections and we are done.

1.4.2 Exercise 2

Same thing as Exercise 1.

1.4.3 Exercise 3

We have that $\sigma^0(0) = 0$. Now assuming $\sigma^n(0) = n$ for some $n \in \mathbb{N}$, we have $\sigma^{\sigma(n)}(0) = \sigma \circ \sigma^n(0) = \sigma(n) = n + 1$.

1.4.4 Exercise 6

We can take $\sigma^{-1}(n) = n - 1$ for $n > 0$ and $\sigma^{-1}(0) = 0, 1, 2$ to get 3 different left inverses.

1.4.5 Exercise 8

Let $n \in U$ if the elements in all sets of size n are equal. Since we can construct a set with two different elements, we have that $n = 1$ does not imply $\sigma(n) \in U$, and the induction axiom cannot be applied to U.

1.4.6 Exercise 9

(Property I, Property II): Take $X = \mathbb{N}$ and $\sigma(x) = x^2 + 1$.

(Property I, Property III): Let $X = \{0, 1\}$ and let $\sigma(0) = 1$, $\sigma(1) = 0$. Then σ is clearly injective, and any subset of X that contains 0 and $\sigma(0)$ is all of X.

(Property II, Property III): Again take $X = \{0, 1\}$, but this time let $\sigma(0) = \sigma(1) = 1$.

1.5 Addition and Multiplication

1.5.1 Exercise 1

$$\begin{aligned} n = 0: \; & (f^m)^0 = 1 = f^0 = f^{(\sigma^m)^0(0)} = f^{m0} \\ \text{Assume n}: \; & (f^m)^{(\sigma(n))} = f^m \circ f^{mn} = f^{m(n+1)} \end{aligned}$$

1.5.2 Exercise 2

(a) $mn = (\sigma^m)^n(0) = \sigma^{mn}(0) = \sigma^{nm}(0) = nm$.

(b) $\sigma(m)(n + n') = (\sigma^{\sigma(m)})^{n+n'}(0) = (\sigma^{\sigma(m)})^n(0) + (\sigma^{\sigma(m)})^{n'}(0)$.

1.5.3 Exercise 3

(a) To obtain a valid τ, simply permute the first few mappings of σ. For example, $\tau(0) = 2, \tau(1) = 3, \tau(2) = 1, n \geq 3: \; \tau(n) = n + 1$.

(b) Suppose τ satisfies Peano. Then we can let $\beta(0) = 0$ and $\beta(n) = \tau(\beta(n-1))\ \forall n > 0$. β is a bijection since τ is injective and maps to all of $\mathbb{N}/\{0\}$. Furthermore, $\beta\sigma(n) = \beta(n+1) = \tau\beta(n)$.

1.5.4 Exercise 4

(a)

$$\begin{aligned} \phi(n) = m &\implies \sigma(\phi(n)) = m+1 \\ &\implies \phi(\sigma(n)) = \phi(n+1) = m+1 \end{aligned}$$

Thus, once we fix $\phi(0)$, we fix the rest of ϕ.

(b) There is only one choice of τ which satisfies Peano's Postulates: $\tau(0) = 1$ with τ satisfying the relation indicated in (a). This is exactly the successor function σ.

1.5.5 Exercise 6

$k + n = \sigma^n(k) = \sigma^n(m) \implies k = m$ since a composition of injections is an injection.

1.6 Inequalities

1.6.1 Exercise 1

Since $x = x$ we have reflexivity of $\leq$. Since $x \leq y \implies x + a = y$ and $y \leq z \implies y + b = z$, we have $x + a + b = z$ giving transitivity.

1.6.2 Exercise 2

$$\begin{aligned} m < n &\implies m + x = n \\ &\implies m + x + k = n + k \\ &\implies m + k < n + k \end{aligned}$$

Multiplication is also isotonic since it's just iterated addition.

1.6.3 Exercise 3

Suppose $0 \in U$, $n \in U \implies \sigma(n) \in U$ and $U \neq \mathbb{N}$. Then from well-ordering, we have that $\mathbb{N}/U$ has a first element f such that $m < f \implies m \in U$. However, this gives us that $\exists m \in U \mid \sigma(m) = f$ which leads to a contradiction.

1.6.4 Exercise 4

Suppose S is well-ordered with first element f but $U \subset S$ is not. Then $V \subset U \mid V \neq \emptyset$ and V has no first element. However, since $V \subset S$, we have a contradiction, since well-ordering implies that every subset of S has a first element.

1.6.5 Exercise 6

The subset consisting of that infinite descending sequence would contain no first element.

1.7 The Integers

1.7.1 Exercise 1

Let $u = sdu + u_0$ and let $v = sdv + v_0$.

$$\begin{aligned} uv &= (sdu)(sdv) + (sdu)(v_0) + (u_0)(sdv) + u_0v_0 \\ d(uv) &= d((sdu)(sdv)) + 0 + 0 + 0 \\ &= (du)(dv) \end{aligned}$$

1.7.2 Exercise 3

Follows from the steps of lemma, since we have that $du \oplus' dv = d(u+v) = d(sdu + sdv) = du \oplus dv$.

1.7.3 Exercise 4

Suppose $a \oplus x_1 = a \oplus x_2$. Then $a' \oplus (a \oplus x_1) = a' \oplus (a \oplus x_2)$, which gives $x_1 = x_2$.

1.7.4 Exercise 5

Same logic as Exercise 3, except using the result of Exercise 1.

1.8 The Integers Modulo N

1.8.1 Exercise 3

$$\begin{aligned} h-k \in n\mathbb{Z},\ r-s \in n\mathbb{Z} &\implies (h-k)+(r-s) \in n\mathbb{Z} \\ &\implies (h+r)-(k+s) \in n\mathbb{Z} \\ h(r-s) \in n\mathbb{Z},\ s(h-k) \in n\mathbb{Z} &\implies h(r-s)+s(h-k) \in n\mathbb{Z} \\ &\implies hr-ks \in n\mathbb{Z} \end{aligned}$$

1.8.2 Exercise 4

Just check the squares of $0, ..., 7$ mod 8 to get the desired result.

1.8.3 Exercise 5

7 cannot be decomposed into a sum of 3 integers from the set $\{0, 1, 4\}$.

1.8.4 Exercise 6

One of the three consecutive integers must be divisible by 3; let the remainder of this integer mod 9 be k. Then, WLOG, we can let the other two integers be $k-1$ and $k+1$ mod 9. We then have that $(k-1)^3 + k^3 + (k+1)^3 = 3k^3 + 6k$, which is divisible by 9 since k is divisible by 3.

1.9 Equivalence Relations and Quotient Sets

1.9.1 Exercise 1

The quotient T/S consists of the set of all possible equivalence classes of triangles based on the relation of triangle similarity. Thus, each element of T/S corresponds to a different kind of triangle similarity, or “shape”.

1.9.2 Exercise 2

$p \times p$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}$. Furthermore, $(p \times p)(x, y) = (p \times p)(x', y') \implies p(x + y) = p(x' + y')$. Then by Theorem 19, we can define addition of cosets of two integers as the function that commutes with the coset of the sum of the integers.

1.9.3 Exercise 3

Reflexivity and symmetry are clear; transitivity follows from the fact that if $(x_1, y_1)E(x_2, y_2)$, $(x_2, y_2)E(x_3, y_3)$, then $x_3 - x_1 = x_3 - x_2 + x_2 - x_1$ which is the sum of two integers and therefore an integer.

1.10 Morphisms

1.10.1 Exercise 1

The additive endomorphisms of $\mathbb{Z}$ are completely determined by the value they map 1 to. Thus, they are all functions of the form $f(z) = cz$ for some constant $c \in \mathbb{Z}$.

1.10.2 Exercise 2

Every additive morphism from $\mathbb{Z}_n$ to $\mathbb{Z}_m$ is of the form $f(z) = p_m(cz)$ where $p_m : \mathbb{Z} \to \mathbb{Z}_m$ maps elements of $\mathbb{Z}$ to their remainders mod m and $c \in \mathbb{Z}_m$.

1.10.3 Exercise 3

Follows the structure indicated in Exercise 2.

1.10.4 Exercise 4

Each rotation of the square can be decomposed into clockwise rotations. If we label the vertices of the square as $0, 1, 2, 3$, then a clockwise rotation can be thought of as adding 1 mod 4. Thus, the isomorphisms between $(\mathbb{Z}_4, +)$ and $(Q, \circ)$ are exactly the additive isomorphisms between $\mathbb{Z}_4$ and itself. There are only 2 such isomorphisms: $f(1) = 1$ and $f(1) = 3$.

1.10.5 Exercise 5

Follows from left inverse for injectivity and right inverse for surjectivity.

1.10.6 Exercise 7

Any morphism $f : (\mathbb{R}, \times) \to (\mathbb{R}, +)$ satisfies

$$\begin{aligned} f(1 * 1) = f(1) + f(1) &\implies f(1) = 0 \\ f(0 * 0) = f(0) + f(0) &\implies f(0) = 0 \end{aligned}$$

Which means f cannot be an isomorphism.

1.11 Semigroups and Monoids

1.11.1 Exercise 1

If u and u' are both units, then $u \Box u' = u' = u$.

1.11.2 Exercise 2

The terms $a_1, ..., a_m$ and $a_{m+1}, ..., a_{m+n}$ together give $a_1, ..., a_{m+n}$.

1.11.3 Exercise 3

As stated in the text, follows from induction on n (the proofs can be found in previous sections).

1.11.4 Exercise 4

Due to commutativity, we can rearrange the terms in the double sum as we like, thereby allowing us to swap sums.

1.11.5 Exercise 5

Let $f : (\mathbb{N}, +) \to (\mathbb{N}, \times)$ be such that $f(n) = 0 \, \forall n \in \mathbb{N}$. Then f is a morphism that does not map the additive unit 0 to the multiplicative unit 1.

2 Groups

2.1 Groups and Symmetry

2.1.1 Exercise 2

Map each element $x \in \mathbb{Z}_6$ to the pair $(p_2(x), p_3(x))$. This is an isomorphism, since the projections $\mathbb{Z}_6 \to \mathbb{Z}_3$ and $\mathbb{Z}_6 \to \mathbb{Z}_3$ are both group morphisms, and the mapping itself is a bijection.

2.1.2 Exercise 3

To see that there is no isomorphism $f : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$, consider $f(1)$ and $f(3)$. We have that $f(0) = f(1+3) = f(1) + f(3)$ which is not possible since $f(0) = (0,0)$ (has to be the case since $f(x) = f(0) + f(x)$).

Rotations do not preserve symmetry for rectangles, since distances between adjacent vertices change. The only transformations that preserve symmetry are reflections across the vertical and horizontal axes, giving 4 possible transformations. We can then map $(0,0)$ to the identity, $(0,1)$ to a vertical reflection, $(1,0)$ to a horizontal reflection, and $(1,1)$ to a vertical + horizontal reflection.

2.1.3 Exercise 4

2.1.4 Exercise 5

2.1.5 Exercise 6

2.1.6 Exercise 10

The set of these permutations has identity $(1,0)$, and any permutation (a,b) has inverse $(\frac{1}{a}, -\frac{b}{a})$. Furthermore, $(a_2, b_2) \circ (a_1, b_1) = (a_1 a_2, a_2 b_1 + b_2)$, which is associative since multiplication and addition are both associative.

2.1.7 Exercise 11

(a) To show that the given function is a permutation on $\mathbb{R} \cup \infty$, we need to show that it is a bijection from $\mathbb{R} \cup \infty \to \mathbb{R} \cup \infty$. Suppose $f(x_1) = f(x_2)$. Then

$$\frac{ax_1 + b}{cx_1 + d} = \frac{ax_2 + b}{cx_2 + d}$$
$$(ad - bc)x_1 = (ad - bc)x_2 \implies x_1 = x_2$$

So f is an injection from $\mathbb{R} \cup \infty \to \mathbb{R} \cup \infty$. Furthermore, if we set $f(x) = y$, we can solve for x, which gives us that f is also a surjection.

(b) I'm sure an inverse can be found, but it's tedious... Associativity then follows again from associativity of multiplication and addition.

2.1.8 Exercise 12

2.1.9 Exercise 13

(a) Any automorphism of $\mathbb{Z}_3$ has to fix 0. Thus, the only two automorphisms are the identity and the automorphism that swaps 1 and 2.

(b) Fixing $(0, 0)$, we see that we can permute the remaining three elements as we want, giving the isomorphism to S_3.

(c)

2.2 Rules of Calculation

2.2.1 Exercise 1

(a) Multiply by inverse and use associativity.

(b) Associativity.

(c) Associativity and then inverse of product.

2.2.2 Exercise 2

Multiply by a^{-1}.

2.2.3 Exercise 3

Since the unit is its own inverse, we're left with $2n-1$ elements that need to be paired with one another. Since $2n-1$ is odd, we have that one of the elements must be its own inverse.

2.2.4 Exercise 4

Any group with 3 elements must be of the form $1, a, a^{-1}$. Thus, each of these groups is clearly isomorphic to the others.

2.2.5 Exercise 5

I struggled to untie the ideas of cancellation and inverse, so I ended up looking up a hint for this one. To see that an infinite set with cancellation does not need to be a group, consider $(\mathbb{N}, +)$. This is a monoid that was proven to have cancellation in chapter 1, but does not contain inverses.

For the case of a finite set G, we can use the fact that $f(x) = ax$ is an injection for any $a \in G$, since $ax = ay \implies x = y$ by cancellation. Since G is finite, f is also a surjection. Therefore, $\exists a \mid ax = 1$ which gives us that there is a left inverse. Applying the same logic using $f(x) = xa$ gives a right inverse, which completes the proof since these inverses must be equal.

2.2.6 Exercise 6

Left cancellation is possible due to left inverse and left unit. Furthermore, $uu = u \implies (a'a)u = a'a \implies au = a$ by left cancellation, indicating that u is also a right unit. Then we have that $ua' = a'u \implies a'aa' = a'u \implies aa' = u$, and a' is also a right inverse. This proves that X is a group.

2.2.7 Exercise 7

We proceed as directed in the hint. Since the equation $ua = a$ has solution u, and any b can be written as $b = ay$, we have $ub = u(ay) = ay = b$. Thus, u is a left unit. Since the equation $a'a = u$ also has a solution a', we are done by Exercise 6.

2.2.8 Exercise 10

Since each element of G has a unique inverse, $f(a) = a^{-1}$ is a bijection. Additionally, $f(ab) = (ab)^{-1} = b^{-1}a^{-1} = f(b)f(a) = f(a)\square^{\mathrm{op}}f(b)$.

2.2.9 Exercise 11

Associativity of $\square$ immediately follows from the associativity of G 's binary operation and the fact that p is a morphism. Additionally, since p is an epimorphism, $\forall x$, $\exists g \mid x = p(g)$. Since $ug = gu$, $p(u)$ is then the unit for X. Similarly, $p(g')$ is the inverse of x, thus making X a group.

2.2.10 Exercise 12

$bb_R = u \implies b_Lbb_R = b_L \implies b_Rb = b_Lb = u$.

2.3 Cyclic Groups

We first show that $\mathbb{Z}_n$ is generated only by those c that are coprime to n. If c is coprime to n, then $ac = 0$ only when $a = n$ since c and n share no prime factors. Thus, the subgroup generated by c has order n and is therefore all of $\mathbb{Z}_n$. Similarly, if c is a generator of $\mathbb{Z}_n$, then c has order n and must therefore be coprime to n.

2.3.1 Exercise 1

The only possible generators are 1 and 5, since those are the only elements of $\mathbb{Z}_6$ that are coprime to 6.

2.3.2 Exercise 2

The endomorphisms of $\mathbb{Z}_n$ are completely determined by the mapping of 1, so there are only n such endomorphisms.

2.3.3 Exercise 3

5 is prime, so all elements of $\mathbb{Z}_5$ other than 0 are coprime to it.

2.3.4 Exercise 4

14 has 6 positive integers less than it that are coprime to it (3, 5, 7, 9, 11, 13).

2.3.5 Exercise 5

The two generators of $\mathbb{Z}$ are 1 and -1, as elements of $\mathbb{Z}$ can be written as $-m$ or m.

2.3.6 Exercise 7

If G is abelian, then $(g_1 g_2)^m$ can be rearranged to $g_1^m g_2^m$. If $(g_1 g_2)^m = g_1^m g_2^m$. The reverse direction follows from the $m = 2$ case, $g_1 g_2 g_1 g_2 = g_1^2 g_2^2$.

2.3.7 Exercise 8

$(g_1 g_2)(g_1 g_2) = 1 \implies g_1 g_2 = g_2 g_1$.

2.3.8 Exercise 9

The automorphisms are all determined by the mappings of the generators; the isomorphisms follow from the number of generators of each group.

2.3.9 Exercise 10

2.4 Subgroups

2.4.1 Exercise 1

The subgroup mapping a given diagonal to itself consists of $\{1, R^3, D, D'\}$, where R^3 is 3 clockwise rotations, D is reflection across the given diagonal, and D' is reflection across the diagonal perpendicular to the given. Mapping those elements to $\{(0,0),(1,1),(0,1),(1,0)\}$ (in order) is an isomorphism.

2.4.2 Exercise 4

If S is closed under product and inverse, then it contains the identity and is thus a subgroup.

2.4.3 Exercise 5

We have that $(s,t)(t,s) = st^{-1}ts^{-1}$, so S contains the identity. Then $(1,s) = s^{-1}$ and $(s,t^{-1}) = st$, so S is closed under products and inverses as well, thus making it a subgroup.

2.4.4 Exercise 6

(a) The identity has order 1. Additionally, if a has finite order, so does a^{-1}. Finally, $a^n = 1,\ b^k = 1 \implies (ab)^{nk} = a^{nk}b^{nk} = 1$.

(b) If non-abelian, we do not necessarily have $(ab)^{nk} = a^{nk}b^{nk}$.

2.4.5 Exercise 7

If G has no proper subgroups, then it is generated by all of its non-identity elements. This is only possible if G has order 1 (vacuously true), or if G is a cyclic group of prime order (as was shown in the beginning of the previous section).

2.4.6 Exercise 8

(a) If a has order n, so does a^{-1}. Additionally, $(ab)^n = a^n b^n = 1$, making all elements that satisfy $a^n = 1$ a subgroup of A. To see that this is not true for non-abelian groups, consider S_3. The elements (12) and (23) are both of order 2, but (12)(23) = (123) is of order 3.

(b) That the n^{th} powers form a subgroup follows from $a^n a^{-n} = 1$ and $a^n b^n = (ab)^n$.

2.4.7 Exercise 9

If T is a submonoid of S, then $i : T \to S$ is a morphism of monoids, so T must necessarily be closed under products and identity. For the reverse direction, if T is closed under products and identity, then the insertion i is a morphism of monoids and T is a submonoid of S.