Exercise Guide for *Algebra* by MacLane and Birkhoff

Muthu Chidambaram

Last Updated: June 8, 2019

Contents

1 Sets, Functions, and Integers **4**
1.1 Sets . . . 4
1.1.1 Exercise 5 . . . 4
1.1.2 Exercise 6 . . . 4
1.2 Functions . . . 4
1.2.1 Exercise 2 . . . 4
1.2.2 Exercise 3 . . . 4
1.2.3 Exercise 4 . . . 4
1.2.4 Exercise 5 . . . 4
1.2.5 Exercise 6 . . . 4
1.2.6 Exercise 7 . . . 4
1.2.7 Exercise 8 . . . 5
1.2.8 Exercise 9 . . . 5
1.2.9 Exercise 10 . . . 5
1.2.10 Exercise 11 . . . 5
1.3 Relations and Binary Operations . . . 5
1.3.1 Exercise 2 . . . 5
1.3.2 Exercise 3 . . . 5
1.3.3 Exercise 4 . . . 5
1.3.4 Exercise 5 . . . 6
1.3.5 Exercise 6 . . . 6
1.3.6 Exercise 7 . . . 6
1.3.7 Exercise 9 . . . 6
1.3.8 Exercise 10 . . . 6
1.4 The Natural Numbers . . . 6
1.4.1 Exercise 1 . . . 6
1.4.2 Exercise 2 . . . 7
1.4.3 Exercise 3 . . . 7
1.4.4 Exercise 6 . . . 7
1.4.5 Exercise 8 . . . 7

1.4.6 Exercise 9 . . . 7
1.5 Addition and Multiplication . . . 7
1.5.1 Exercise 1 . . . 7
1.5.2 Exercise 2 . . . 7
1.5.3 Exercise 3 . . . 7
1.5.4 Exercise 4 . . . 8
1.5.5 Exercise 6 . . . 8
1.6 Inequalities . . . 8
1.6.1 Exercise 1 . . . 8
1.6.2 Exercise 2 . . . 8
1.6.3 Exercise 3 . . . 8
1.6.4 Exercise 4 . . . 8
1.6.5 Exercise 6 . . . 9
1.7 The Integers . . . 9
1.7.1 Exercise 1 . . . 9
1.7.2 Exercise 3 . . . 9
1.7.3 Exercise 4 . . . 9
1.7.4 Exercise 5 . . . 9
1.8 The Integers Modulo n . . . 9
1.8.1 Exercise 3 . . . 9
1.8.2 Exercise 4 . . . 9
1.8.3 Exercise 5 . . . 9
1.8.4 Exercise 6 . . . 10
1.9 Equivalence Relations and Quotient Sets . . . 10
1.9.1 Exercise 1 . . . 10
1.9.2 Exercise 2 . . . 10
1.9.3 Exercise 3 . . . 10
1.10 Morphisms . . . 10
1.10.1 Exercise 1 . . . 10
1.10.2 Exercise 2 . . . 10
1.10.3 Exercise 3 . . . 10
1.10.4 Exercise 4 . . . 10
1.10.5 Exercise 5 . . . 11
1.10.6 Exercise 7 . . . 11
1.11 Semigroups and Monoids . . . 11
1.11.1 Exercise 1 . . . 11
1.11.2 Exercise 2 . . . 11
1.11.3 Exercise 3 . . . 11
1.11.4 Exercise 4 . . . 11
1.11.5 Exercise 5 . . . 11

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

These notes contain short summaries of (my) proof ideas for a decent chunk of the exercises from the book *Algebra* (2nd Edition) by Saunders MacLane and Garrett Birkhoff. I have tried to make the summaries as brief as possible; sometimes only one direction of proof, one line, or even one equation. My goal was to include enough information in the summaries so that someone reading would be able to reconstruct a full proof with all the details if necessary. However, these summaries are tuned to my own personal context, and as such I'm sure mileage will vary. I would greatly appreciate any feedback/fixes.

Also, I like when people include (what they presume to be) relevant quotes in their notes, so I have to ask you to forgive my haughtiness in starting these notes with a quote from Hermann Weyl.

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

$$\begin{aligned} x\square y = u\square(x\square y) = (u\square y)\square x = y\square x \\ x\square(y\square z) = x\square(z\square y) = (x\square y)\square z \end{aligned}$$

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

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

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 $0, ..., 7 \bmod 8$ 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

$$f(1 * 1) = f(1) + f(1) \implies f(1) = 0$$
$$f(0 * 0) = f(0) + f(0) \implies f(0) = 0$$

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 $u \square u' = u' = u$.

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.