“Sparknotes” for *Algebra* by MacLane and Birkhoff

Muthu Chidambaram

Last Updated: May 21, 2019

Contents

Preface

> "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 exercises and some theorems from the book *Algebra* by MacLane and Birkhoff. I have tried to make the summaries as brief as possible, sometimes only one line or one equation. My hope is that the summaries will give enough information to reconstruct a full proof without bogging the reader down with details. In many cases, I am sure that I inadvertently sacrificed clarity in an attempt to obtain brevity, and would greatly appreciate any feedback.

Also, I like when people include (what they presume to be) relevant quotes from mathematicians of past generations 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

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

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

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

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.