UMA205: Introduction to Algebraic Structures

Naman Mishra

January 2024

Contents

Lecture 01: Wed 03 Jan '24

0 The course

Instructor: Prof. Arvind Ayyer
Office: X-15
Office hours: TBD
Lecture hours: MWF 11:00–11:50
Tutorial hours: Tue 9:00–9:50

80% attendance is mandatory.

Prerequisites: UMA101 and UMA102 **Texts:** Several

- *Analysis I*, Terence Tao.

Grading

(20%) Quizzes on alternate Tuesdays, worst dropped. No makeup quizzes, but if a quiz is missed for a medical reason (with certificate), that quiz will be dropped.

(30%) Midterm

(50%) Final

Homeworks after every class, ungraded. Exams are closed book and closed notes, with no electronic devices allowed.

Aims of the Course

- Deal with formal mathematical structures.
- Learning the axiomatic method.
- See how more complicated structures arise from simpler ones.

1 Peano's Axioms

We try to formulate two fundamental quantities: 0 and the successor function $n \mapsto n_{++}$.

(P1) 0 is a natural number.

(P2) If n is a natural number, so is n_{++}.

(P3) 0 is not the successor of any natural number.

(P4) Different natural numbers have different successors.

(P5) (Principle of mathematical induction) Let $P(n)$ be any "property" for a natural number n. Suppose that $P(0)$ is true, and that $P(n_{++})$ is true whenever $P(n)$ is true. Then P is true for all natural numbers.

Denote *the* set of natural numbers by $\mathbb{N}$. (Any two sets satisfying the Peano axioms are isomorphic.) Note that $\mathbb{N}$ is itself infinite, but all of its elements are finite.

Proof. 0 is finite. If n is finite, then n_{++} is finite. Thus, by induction, all natural numbers are finite. (But wtf is a finite number?) □

Remarks.

- There exist number systems which admit infinite numbers. For example, cardinals, ordinals, etc.
- This way of thinking is *axiomatic*, but not constructive.

Lecture 02: Mon 08 Jan '24

Definition 1.1 (Addition)**.** Suppose $m, n \in \mathbb{N}$. We define the binary operation $+$ by setting $0 + m = m$. Suppose we have defined $n + m$. Then we inductively define $n_{++} + m = (n + m)_{++}$.

For example, note that $1 + m = (0 + m)_{++} = m_{++}$.

Lemma 1.2. For $n \in \mathbb{N}$, we have $n + 0 = n$.

Proof. $0 + 0 = 0$. If $n + 0 = n$, then $n_{++} + 0 = (n + 0)_{++} = n_{++}$. $\square$

Lemma 1.3. For $m, n \in \mathbb{N}$, we have $n + m_{++} = (n + m)_{++}$.

Proof. Fix m and induct on n. For $n = 0$, we have $0 + m_{++} = m_{++} = (0 + m)_{++}$. Suppose $n + m_{++} = (n + m)_{++}$. Then

$$\begin{aligned} n_{++} + m_{++} &= (n + m_{++})_{++} && \text{(definition)} \\ &= ((n + m)_{++})_{++} && \text{(hypothesis)} \\ &= (n_{++} + m)_{++} && \text{(definition)} \end{aligned}$$

as desired. $\square$

Problem 0.1. (Commutativity) For $m, n \in \mathbb{N}$, we have $n + m = m + n$.

Proof. Fix m and induct on n. For $n = 0$, we have $0 + m = m = m + 0$. Suppose $n + m = m + n$. Then

$$\begin{aligned} n_{++} + m &= (n + m)_{++} && \text{(definition)} \\ &= (m + n)_{++} && \text{(hypothesis)} \\ &= m + n_{++} \end{aligned}$$

by the previous lemma. $\square$

Problem 0.2. (Associativity) For $m, n, p \in \mathbb{N}$, we have $(m + n) + p = m + (n + p)$.

Proof. Induct on m. $(0 + n) + p = n + p = 0 + (n + p)$.
Suppose $(m + n) + p = m + (n + p)$. Then

$$\begin{aligned} (m_{++} + n) + p &= (m + n)_{++} + p && \text{(definition)} \\ &= ((m + n) + p)_{++} && \text{(definition)} \\ &= (m + (n + p))_{++} && \text{(hypothesis)} \\ &= m_{++} + (n + p). && \text{(definition)} \end{aligned}$$

This closes the induction. $\square$

Problem 0.3. (Cancellation) For $m, n, p \in \mathbb{N}$, if $m + n = m + p$, then $n = p$.

Proof. Induct on m. $0 + n = 0 + p$ implies $n = p$.

Suppose $m + n = m + p$ implies $n = p$. Then $m_{++} + n = m_{++} + p$ implies $(m + n)_{++} = (m + p)_{++}$ and so $m + n = m + p$ by (P4). By the inductive hypothesis, $n = p$. $\square$

Definition 1.4 (Positive)**.** A natural number is positive if it is not 0.

Proposition 1.5. If a is positive and $b \in \mathbb{N}$, then $a + b$ is positive.

Proof. Induct on b. $a + 0 = a$ is positive. $a + b_{++} = (a + b)_{++}$ is positive since 0 is not the successor of any natural number. $\square$

Problem 0.4. If m, n in $\mathbb{N}$ with $m + n = 0$, then $m = n = 0$.

Proof. Contrapositive of the previous proposition, with commutativity. $\square$

Problem 0.5. Let a be positive. Then there exists a unique $b \in \mathbb{N}$ such that $a = b_{++}$.

Proof. Let $P(n)$ be that n is zero or there exists a unique $b \in \mathbb{N}$ such that $n = b_{++}$. $P(0)$ is true.

Suppose $P(n)$ is true. n_{++} is non-zero, successor of n and only n, by (P3) and (P4). Thus $P(n_{++})$ is true. $\square$

Definition 1.6 (Order)**.** Let $m, n \in \mathbb{N}$. We say that n is greater than or equal to m, written $n \geq m$ or $m \leq n$, if $n = m + a$ for some $a \in \mathbb{N}$.

Similarly, we say that n is (strictly) greater than m, written $n > m$ or $m < n$, if $n \geq m$ and $n \neq m$.

Note that $n_{++} > n$, so there is no largest natural number.

Proposition 1.7. Let $a, b, c \in \mathbb{N}$. Then

1) $a \geq a$ (reflexivity),
2) $a \geq b$ and $b \geq a$ implies $a = b$ (antisymmetry),
3) $a \geq b$ and $b \geq c$ implies $a \geq c$ (transitivity),
4) $a \geq b \iff a + c \geq b + c$,
5) $a > b \iff a \geq b_{++}$,
6) $a > b \iff a = b + c$ for some positive c.

Proof.

1) $a = a + 0$.
2) $a = b + c$ and $b = a + d$ implies $a = a + (c + d)$. By cancellation, $c + d = 0$ and so $c = d = 0$.
3) $a = b + m$ and $b = c + n$ implies $a = c + (m + n)$.
4) $a = b + m \iff (a + c) = (b + c) + m$.
5) From 6), $a > b \iff a = b + c$ for some positive c, iff $a = b + d_{++} = b_{++} + d$.
6) $a > b \iff a = b + c$ but $a \neq b$. Since $a \neq b$, c cannot be zero. Conversely, if c is positive, $a \neq b$. □

Proposition 1.8 (Trichotomy)**.** Let $a, b \in \mathbb{N}$. Then exactly one of the following holds: $a > b$, $a = b$, or $a < b$.

Proof. We first prove that no more than one of the three holds. $a = b$ cannot hold simultaneously with $a > b$ or $a < b$ by their definitions. Suppose $a > b$ and $a < b$. Then $a = b + c$ and $b = a + d$ for some positive c and d. Thus $a = a + (c + d)$ and so $c + d = 0$, a contradiction.

We now prove that at least one of the three holds by induction on a. Since $b = 0 + b$, either $0 = b$ or $b > 0$. Suppose at least one of $a \geq b$ and $a < b$ holds. If $a = b + c$, then $a_{++} = b + (c_{++})$ and so $a_{++} > b$. If $a < b$, then by proposition 1.7(5), $a_{++} \leq b$. This completes the induction. □

Proposition 1.9 (Strong induction)**.** Let $m_0 \in \mathbb{N}$ and let $P(m)$ be a property for all $m \in \mathbb{N}$. Suppose for all $m \geq m_0$, we have the following: if $P(m')$ holds for all $m_0 \leq m' < m$, then $P(m)$ holds. Then $P(m)$ holds for all $m \geq m_0$.

Note that the inductive step is vacuously true for $m = m_0$.

Proof. Define $Q(m)$ to be "$P(m')$ holds for all $m_0 \leq m' < m$". $Q(0)$ holds vacuously, since there are no $m' < 0$.

Suppose $Q(m)$ holds. If $m < m_0$, then $Q(m_{++})$ holds vacuously, since $m_{++} \leq m_0$ and so no m' satisfies $m_0 \leq m' < m_{++} \leq m_0$.

Now if $m \geq m_0$, then $Q(m)$ and the proposition imply $P(m)$. Thus $P(m')$ holds for all $m_0 \leq m' \leq m \iff m_0 \leq m' < m_{++}$. Thus $Q(m_{++})$ holds. □

Problem 0.6 (Backwards induction)**.** Let $m_0 \in \mathbb{N}$, and let $P(m)$ be a property pertaining to the natural numbers such that whenever $P(m_{++})$ is true, then $P(m)$ is true. Suppose that $P(m_0)$ is also true. Prove that $P(m)$ is true for all natural numbers $m \leq m_0$.

Proof. Define $Q(m)$ to be "if $P(m)$ is true, then $P(m')$ is true for all $m' \leq m$". $Q(0)$ holds vacuously, since $m' \leq 0$ implies $m' = 0$.

Suppose $Q(m)$ holds. Then if $P(m_{++})$ is true, so is $P(m)$, and by the inductive hypothesis, $P(m')$ is true for all $m' \leq m$. Thus $Q(m_{++})$ holds. Thus $Q(m)$ holds for all $m \in \mathbb{N}$.

In particular, $Q(m_0)$ holds, and so $P(m')$ is true for all $m' \leq m_0$. □

From now on, we will assume the usual laws of addition.

Definition 1.10 (Multiplication)**.** Let $m \in \mathbb{N}$. The binary operation multiplication, denoted by $*$, is defined as follows. Set $0 * m = 0$. Then define it inductively as follows. If we know $n * m$, set $n_{++} * m = (n * m) + m$.

Lemma 1.11. Let $m, n \in \mathbb{N}$, Then $m * n = n * m$.

Proof. First note that $m*0 = 0$, since $0*0 = 0$ and $m_{++}*0 = m*0+0 = m*0$.

Next note that $n * m_{++} = (n * m) + n$, since $0 * m_{++} = 0 = (0 * m) + 0$, and $n_{++} * m_{++} = (n * m_{++}) + m_{++}$ which is equal to $(n * m) + n + m_{++} = (n * m) + m + n_{++} = (n_{++} * m) + n_{++}$ by the inductive hypothesis.

Finally, $0 * n = n * 0$, and $m_{++} * n = n * m_{++}$ gives $m * n = n * m$ by induction on m. $\square$

We use the notation mn for $m * n$ and also employ the usual convention for precedence, so that $mn + p$ means $(m * n) + p$ and not $m * (n + p)$.

Lemma 1.12. Let $m, n \in \mathbb{N}$. Then $mn = 0$ iff at least one of m and n is 0.

Proof. The 'if' direction is clear. Suppose m, n are positive. Then $m = \tilde{m}_{++}$ for some $\tilde{m} \in \mathbb{N}$.

$$\begin{aligned} mn &= (\tilde{m}_{++})n \\ &= (\tilde{m}n) + n \end{aligned}$$

which is positive since n is positive. $\square$

Proposition 1.13 (Distributivity)**.** For $a, b, c \in \mathbb{N}$, we have $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

Proof. Prove the first by induction on a. $0(b + c) = 0 = 0 + 0 = 0b + 0c$.

Suppose $a(b + c) = ab + ac$. Then

$$\begin{aligned} a_{++}(b + c) &= a(b + c) + (b + c) && \text{(definition)} \\ &= (ab + ac) + (b + c) && \text{(hypothesis)} \\ &= (ab + b) + (ac + c) \\ &= a_{++}b + a_{++}c. && \text{(definition)} \end{aligned}$$

The second equality follows from the first by commutativity. $\square$

Problem 0.7. (Associativity) For $a, b, c \in \mathbb{N}$, we have $(ab)c = a(bc)$.

Proof. Induct on a. $(0b)c = 0c = 0 = 0(bc)$.

Suppose $(ab)c = a(bc)$. Then

$$\begin{aligned}
(a_{++}b)c &= (ab+b)c && \text{(definition)}\\
&= (ab)c + bc && \text{(distributivity)}\\
&= a(bc) + bc && \text{(hypothesis)}\\
&= a_{++}(bc)
\end{aligned}$$

by definition. □

Problem 0.8. (Order preservation) For $a, b, c \in \mathbb{N}$ with $a < b$ and $c \neq 0$, we have $ac < bc$.

Proof. Induct on c with base case $c = 1$. If $ac < bc$, then $ac + a < bc + a$ but $bc + a < bc + b$, both by order preservation under addition. By transitivity, $ac + a < bc + b$ and so $ac_{++} < bc_{++}$. □

Problem 0.9. (Cancellation) For $a, b, c \in \mathbb{N}$ with $ac = bc$ and $c \neq 0$, we have $a = b$.

Proof. From trichotomy and order preservation. □

Proposition 1.14 (Euclidean algorithm)**.** Let $n \in \mathbb{N}$ and m be positive. Then there exist unique $q, r \in \mathbb{N}$ such that $n = qm + r$ and $r < m$. We call q the quotient and r the remainder.

Proof. We first prove uniqueness. Suppose $n = qm + r = q'm + r'$. If $q < q' \iff q_{++} \leq q'$, then $qm + r < qm + m = q_{++}m \leq q'm \leq q'm + r'$, a contradiction. Similarly, $q' < q$ is impossible. This leaves $q = q'$. Then $qm + r = q'm + r'$ gives $r = r'$ by cancellation.

For existence, we induct on n. $0 = 0m + 0$. Suppose $n = qm + r$. Then $n_{++} = qm + r_{++}$. If $r_{++} < m$, we are done. Otherwise, $r_{++} = m$ (since $r < m \iff r_{++} \leq m$) and so $n_{++} = (q_{++})m + 0$. □

This proposition allows us to divide.

Definition 1.15 (Exponentiation)**.** Let m be positive. The binary operation exponentiation can be defined inductively as $m^0 = 1$ and $m^{n_{++}} = m^n m$. We further define $0^k = 0$ for all positive k.

Lecture 03: Mon 08 Jan '24

2 Axioms of Set Theory (ZFC)

Definition 2.1 (Set)**.** A set is a well-defined collection of objects, which we call elements. We will write $x \in A$ to say that x is an element of A.

Well-defined means that given any object, we can state without ambiguity whether it is an element of the set or not.

Axiom 2.1. Sets are themselves objects. If A and B are sets, it is meaningful to ask whether A is an element of B.

Axiom 2.2 (Extensionality)**.** Two sets A and B are equal, written $A = B$, if every element of A is a member of B and vice versa.

Axiom 2.3 (Existence)**.** There exists a set, denoted by $\varnothing$ or $\{\}$, known as the empty set, which does not contain any elements, *i.e.*, $x \notin \varnothing$ for all objects x.

Problem 0.10. $\varnothing$ is unique.

Proof. Suppose $\varnothing$ and $\varnothing'$ are both empty sets. Then $x \in \varnothing \iff x \in \varnothing'$ since both are always false. $\square$

Lemma 2.2 (Single choice)**.** Let A be a non-empty set. Then there exists an object x such that $x \in A$.

Proof. If not, then $x \notin A$ for all objects x and so $A = \varnothing$. $\square$

Thus, we can choose an element of A to certify its non-emptiness.

Axiom 2.4 (Pairing)**.** If a is an object, there exists a set, denoted $\{a\}$, whose only element is a. Similarly, if a and b are objects, there exists a set, denoted $\{a, b\}$, whose only elements are a and b.

For example, we can now construct $\varnothing$, $\{\varnothing\}$, $\{\{\varnothing\}\}$, $\{\varnothing, \{\varnothing\}\}$, etc, all of which are distinct.

Axiom 2.5 (Unions)**.** Given sets A and B, there exists a set, denoted $A \cup B$, called the union of A and B, which consists of exactly the elements in A, B, or both.

Problem 0.11. $A \cup B = B \cup A$.

Proof. By commutativity of $\vee$. $\square$

Problem 0.12. $(A \cup B) \cup C = A \cup (B \cup C)$.

Proof. By associativity of $\vee$. $\square$

Definition 2.3 (Subset)**.** A is a subset of B if every element of A is alaso an element of B, denoted $A \subseteq B$.

Axiom 2.6 (Specification)**.** (also called Separation). Let A be a set and let $P(x)$ be a property for every $x \in A$. Then there exists a set $S = \{x \in A \mid P(x)\}$ where $x \in S$ iff $x \in A$ and $P(x)$ is true.

We can now define the intersection, $A \cap B$, and difference, $A \setminus B$, of sets A and B.

Definition 2.4. Let A and B be sets. we define the intersection $A \cap B = \{x \in A \mid x \in B\}$ and the difference $A \setminus B = \{x \in A \mid x \notin B\}$.

A and B are said to be disjoint if $A \cap B = \varnothing$.

Recall that sets form a Boolean algebra under the operations $\cup$, $\cap$, and $\setminus$. For example, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, de Morgan's laws, etc.

Axiom 2.7 (Replacement)**.** Let A be a set and let $P(x, y)$ be a property for every $x \in A$ and every object y, such that for every $x \in A$ there is at most one y for which $P(x, y)$ is true. Then there exists a set $S = \{y \mid P(x, y) \text{ is true for some } x \in A\}$. That is, $y \in S$ iff $P(x, y)$ is true for some $x \in A$.

Examples.

- Let $A = \{7, 9, 22\}$ and $P(x, y) \equiv y = x_{++}$. Then $S = \{8, 10, 23\}$.

- Let $A = \{7, 9, 22\}$ and $P(x, y) \equiv y = 1$. Then $S = \{1\}$.

Axiom 2.8 (Infinity)**.** There exists a set, denoted $\mathbb{N}$, whose objects are called natural numbers, *i.e.*, an object $0 \in \mathbb{N}$, and n_{++} for every $n \in \mathbb{N}$, such that the Peano axioms hold.

Axiom 2.9 (Foundation)**.** (also called Regularity). If A is a non-empty set, then there exists at least one $x \in A$ which is either not a set or is disjoint from A.

For example, if $A = \{\{1, 2\}, \{1, 2, \{1, 2\}\}\}$, then $\{1, 2\}$ is an element of A which is disjoint from A.