MATH 3021: Algebra I

Joe Tran

August 29, 2023

Preface

Contents

Lecture 1

September 6, 2023

Your final grade for this class will be based on the following components.

1. 4 Homework Assignments on Crowdmark (30%)
2. Midterm (30%)
3. Final Exam (40%)

What is algebra? Studies operations between objects in sets such as

- Addition on numbers
- Multiplication between numbers
- Matrix multiplication
- Addition modulo n
- and others...

A set G is called a *group* if it is enclosed with an operation that satisfies certain properties. Groups are the subject of MATH 3021.

Prerequisites. A proof-based course (i.e. MATH 1200 or similar). It is very important to be fluent in proof methods (contradiction, induction, etc.)

Textbook. Undergraduate Algebra, by S. Lang

Before groups, we will review the properties of integers and functions.

1.1 Integers

Definition 1.1.1. A *set* is an unordered collection of objects.

Example 1.1.2. The following are examples of sets.

- Empty set: $\emptyset$
- Set of integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\}$
- Set of natural numbers $\mathbb{N} = \{1, 2, 3, ...\}$
- Set of rational numbers $\mathbb{Q} = \left\{\frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{N}\right\}$
- Set of real numbers $\mathbb{R}$
- Set of points in the plane $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$
- Set of complex numbers $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$

Notation 1.1.3. If A is a set and x is a member of A, we write $x \in A$. Otherwise, we write $x \notin A$.

Notation 1.1.4. For A, B we write $A \subseteq B$ if every element in A is also a element of B.

Example 1.1.5. $\emptyset \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Remark 1.1.6. It is possible that $A = B$, i.e. $A \subseteq A$

Notation 1.1.7. If $A \subseteq B$ and $A \neq B$, then we write $A \subsetneq B$.

Remark 1.1.8. For sets A and B, whenever $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Notation 1.1.9. For A and B, we write

- $A \cup B$ for the union of the two sets.
- $A \cap B$ for the intersection of the two sets.
- $A \setminus B$ for the difference of A from B
- $A \times B = \{(a, b) : a \in A, b \in B\}$ for the Cartesian product of the two sets.

Notation 1.1.10. For a finite set A we denote $|A|$ for the number of elements in A (or the cardinality of A). If A is infinite, then $|A| = \infty$.

1.2 Fundamental Properties of Integers

Definition 1.2.1. Let $A \subseteq \mathbb{R}$ be a nonempty set and $x \in \mathbb{R}$. We call x a *lower bound for A* if for all $y \in A$, $x \leq y$.

Definition 1.2.2. Let $A \subseteq \mathbb{R}$ and $x \in \mathbb{R}$. We call x a *minimum* of A and write $x = \min(A)$ if

- x is a lower bound of A
- $x \in A$.

Example 1.2.3. If $A = [0,1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$, then $\min(A) = 0$. If $B = (0,1)$, then B has no minimum.

Exercise. If $A \subseteq \mathbb{R}$ has a minimum, then it is unique.

Solution. To show the uniqueness of the minimum, suppose x and x' are minima of A. Then we have that $x, x' \in A$. Furthermore, for x, we have $x \leq x'$ and we also have that $x' \leq x$. As $\leq$ is antisymmetric, it follows that $x = x'$. That is, a minimum of A is unique if it exists.

Theorem 1.2.4 (The Well Ordering Principle)**.** *Every nonempty subset A of $\mathbb{N}$ has a minimum.*

Theorem 1.2.5 (Euclidean Algorithm)**.** *Let $n \in \mathbb{Z}$ and $m \in \mathbb{N}$. Then there exists a unique $q, r \in \mathbb{Z}$ with $0 \leq r < m$ and $n = qm + r$.*

Proof. For simplicity, we only treat the case for when $n > 0$. Define $S = \{k \in \mathbb{N} : km > n\}$. We show that $S \neq \emptyset$. Indeed, note that $k = n + 1 \in S$ because $km = (n+1)m > n$. By the Well Ordering Principle (Theorem 1.2.4), there exists a $k_0 = \min(S)$. Define $q = k_0 - 1$, and $r = n - qm$. Then $n = qm + r$. We need to show that $0 \leq r < m$.

Claim 1.2.6. $0 \leq r < m$.

Because $q = k_0 - 1 < k_0$, then $q \notin S$ and so $qm \leq n$ which implies that $r = n - qm \geq 0$.

Next, show that $r < m$. Towards contradiction, we assume that $r \geq m$. Then this implies that $m \leq n - qm = r$ and so $(1+q)m \leq n$, which implies that $k_0 m \leq n$ and so $k_0 \notin S$, which is a contradiction, and so $r < m$, as required. $\square$

Exercise. Prove that q and r are unique.

Solution. Suppose that q and r are not unique. Then let $q, q', r, r' \in \mathbb{Z}$ be such that $0 \leq r < m$ and $0 \leq r' \leq m$ and $n = qm + r$ and $n = q'm + r'$. Furthermore, assume that $0 \leq r \leq r' < m$. Then $0 < r - r' < b$ and the expressions for n implies that

$$0 \leq (q - q')m = r' - r < b$$

which is absurd. Therefore, $r = r'$ and $q = q'$ as required.

Lecture 2

September 8, 2023

2.1 Fundamental Properties of Integers

Recall the following definitions and theorems.

Definition 2.1.1. Let $A \subseteq \mathbb{R}$ be a nonempty set and $x \in \mathbb{R}$. We call x a lower bound for A if for all $y \in A$, $x \leq y$.

Definition 2.1.2. Let $A \subseteq \mathbb{R}$ be a nonempty set and $x \in \mathbb{R}$. We call x a minimum of A if both of the following conditions hold.

- x is a lower bound of A
- $x \in A$

We then write $x = \min(A)$.

Remark 2.1.3. Not all nonempty sets of $\mathbb{R}$ have a minimum.

Theorem 2.1.4 (Well Ordering Principle)**.** *Every nonempty subset of* $\mathbb{N}$ *admits a minimum.*

Definition 2.1.5. Let $A \subseteq \mathbb{R}$ and $x \in \mathbb{R}$. We call x an upper bound of A if for all $y \in A$, $y \leq x$.

Definition 2.1.6. Let $A \subseteq \mathbb{R}$ and $x \in \mathbb{R}$. We call x a maximum of A if

- x is an upper bound of A
- $x \in A$

We then write $x = \max(A)$

Example 2.1.7. If $A = \{n \in \mathbb{Z} : n < 0\}$, then $\max(A) = -1$.

Remark 2.1.8. Some subsets of $\mathbb{N}$ have m maxima.

Example 2.1.9. $A = \mathbb{N}$ or $A =$ positive even numbers have m maxima.

Theorem 2.1.10. *If $A \subseteq \mathbb{Z}$ and $A \neq \emptyset$*

(i) If A has an upper bound, then A has a maximum.

(ii) If A has a lower bound, then A has a minimum.

2.2 Greatest Common Divisor

Definition 2.2.1. Let $d, n \in \mathbb{Z} \setminus \{0\}$. We say that d *divides* n and write $d \mid n$ if there exists a $q \in \mathbb{Z}$ such that $n = qd$.

Example 2.2.2. $3 \mid 12$ since $12 = 4 \cdot 3$.

Exercise. If $n, d \in \mathbb{Z} \setminus \{0\}$ such that $d \mid n$, then $1 \leq |d| \leq |n|$.

Solution. Since $d \mid n$, there exists a $q \in \mathbb{Z}$ such that $n = qd$, and so since $n \neq 0$, then $q \neq 0$, and so $|n| = |qd| = |q||d|$, where $|q| \geq 1$, and so $|n| \geq 1 \cdot |d| = |d|$. Furthermore, since $|d| \geq 0$, we have that $|d| \geq 1$, and therefore, $1 \leq |d| \leq |n|$, as required.

Definition 2.2.3. Let $m, n \in \mathbb{Z} \setminus \{0\}$. We define the *greatest common divisor* of m and n to be

$$\gcd(m, n) = \max\{d \in \mathbb{N} : d \mid m \text{ and } d \mid n\}$$

Remark 2.2.4. Note that $1 \in \{d \in \mathbb{N} : d \mid m \text{ and } d \mid n\}$. It has an upper bound, i.e. $|m|$. Therefore, by Theorem 2.1.10, the maximum of it exists.

Definition 2.2.5. A subset $J \subseteq \mathbb{Z}$ is called an ideal if it satisfies all following conditions:

- $0 \in J$
- For all $n \in J$ and for all $m \in \mathbb{Z}$, $mn \in J$ (it contains all multiples of its elements).
- For all $m, n \in J$, $m + n \in J$ (it contains all sums of its elements).

Example 2.2.6. The following are examples are ideals.

- $J = \mathbb{Z}$ is an ideal.
- $J = \{0\}$ is an ideal.
- $J = \{n, k \in \mathbb{Z} : n = 2k\}$

Example 2.2.7. Suppose $m_1, m_2, ..., m_r \in \mathbb{Z}$. Consider the set given by

$$J = \left\{ \sum_{i=1}^{r} x_i m_i : x_i \in \mathbb{Z}, 1 \leq i \leq r \right\}$$

Then J is an ideal and we say that it is *generated* by $m_1, m_2, ..., m_r$. To see that J is an ideal, first note that if we consider for each $1 \leq i \leq r$, $x_i = 0$, then $0 \in J$.

Next, take $n \in J$ and $m \in \mathbb{Z}$. We need to show that $mn \in J$. Since $n \in J$, for each $1 \leq i \leq r$, there exists $x_i \in \mathbb{Z}$ such that

$$n = \sum_{i=1}^{r} x_i m_i$$

So

$$mn = m \sum_{i=1}^{r} x_i m_i = \sum_{i=1}^{r} x_i m_i m \in J$$

Finally, take $m = \sum_{i=1}^{r} x_i m_i \in J$ and $n = \sum_{i=1}^{r} y_i m_i \in J$. Then

$$m + n = \sum_{i=1}^{r} x_i m_i + \sum_{i=1}^{r} y_i m_i = \left(\sum_{i=1}^{n} m_i (x_i + y_i) \right) \in J$$

Therefore, J is an ideal.

Theorem 2.2.8. *Let J be a nonzero ideal (i.e. $J \neq \{0\}$). Then there exists an $m_0 \in \mathbb{Z}$ that generates J, i.e. $J = \{x m_0 : x \in \mathbb{Z}\}$. In fact, we may take $m_0 = \min\{n \in J : n > 0\}$.*

Proof. We need to show that $\{n \in J : n > 0\}$ is

(i) Bounded below (1 is a lower bound)

(ii) It is nonempty. We assumed there exists an $n \in J \setminus \{0\}$.

  - If $n > 0$ then we are done.
  - If $n < 0$, then $-1 \cdot n > 0$ and $-1 \cdot n \in J$.

Take $m_0 = \min\{n \in J : n > 0\}$ (which exists). Take an arbitrary $n \in J$. We will use the Euclidean algorithm to write $n = qm_0 + r$, where $0 \leq r < m_0$.

Claim 2.2.9. $r = 0$. *If the claim is true, then* $n = qm_0$, *and so* $n = \{x \cdot m_0 : x \in \mathbb{Z}\}$, *which implies that* $J \subseteq \{x \cdot m_0 : x \in \mathbb{Z}\}$.

To show that the claim is true, assume that $r \neq 0$. Then $0 < r < m_0$. Since $m_0 \in J$, then $-q \cdot m_0 \in J$. Since $n \in J$, then $n + (-q) \cdot m_0 \in J$ which implies that $r \in J$. This is absurd since m_0 has to be the smallest positive number of J and r is even smaller. □

Theorem 2.2.10. *Let* $m_1, m_2 \in \mathbb{Z} \setminus \{0\}$ *and* J *be the ideal generated by then, i.e.* $J = \{x_1 m_1 + x_2 m_2 : x_1, x_2 \in \mathbb{Z}\}$. *Then* $\gcd(m_1, m_2)$ *generates* J.

Proof. From Theorem 2.2.8, if we set $m_0 = \min\{n \in J : n > 0\}$, then m_0 generates J. We will show that $m_0 = \gcd(m_1, m_2)$. Since m_0 generates J, there exists x_1, x_2 such that

$$m_1 = x_1 \cdot m_0 \Rightarrow m_0 \mid m_1$$

and

$$m_2 = x_2 \cdot m_0 \Rightarrow m_0 \mid m_2$$

Since $m_0 \in \mathbb{N}$, $1 \leq m_0 \leq \gcd(m_1, m_2)$. We will now show that $\gcd(m_1, m_2) \mid m_0$. We have that

$$1 \leq |\gcd(m_1, m_2)| \leq |m_0| \Rightarrow 1 \leq \gcd(m_1, m_2) \leq m_0$$

which implies that $\gcd(m_1, m_2) = m_0$. Since $m_0 \in J$, there exists $y_1, y_2 \in \mathbb{Z}$ such that

$$m_0 = y_1 m_1 + y_2 m_2 \tag{1}$$

Since $\gcd(m_1, m_2) \mid m_1$ and $\gcd(m_1, m_2) \mid m_2$, there exists $z_1, z_2 \in \mathbb{Z}$ such that

$$m_1 = z_1 \gcd(m_1, m_2) \quad m_2 = z_2 \gcd(m_1, m_2) \tag{2}$$

Substituting (2) to (1) gives us

$$\begin{aligned} m_0 &= y_1 z_1 \gcd(m_1, m_2) + y_2 z_2 \gcd(m_1, m_2) \\ &= (y_1 z_1 + y_2 z_2) \gcd(m_1, m_2) \end{aligned}$$

which implies that $\gcd(m_1, m_2) \mid m_0$, as required. □

Corollary 2.2.11 (Bezout's Theorem)**.** *If* $m_1, m_2 \in \mathbb{Z} \setminus \{0\}$*, then there exists* $x_1, x_2 \in \mathbb{Z}$ *such that* $\gcd(m_1, m_2) = x_1 m_1 + x_2 m_2$.

Proof. If J is an ideal generated by m_1 and m_2, then $\gcd(m_1, m_2) \in J$ by the previous theorem. $\square$

Lecture 3

September 11, 2023

Recall that in the previous lecture, we mentioned the following:

Definition 3.0.1. For $m, n \in \mathbb{Z} \setminus \{0\}$,

$$\gcd(m, n) = \max\{d \in \mathbb{N} : d \mid m \text{ and } d \mid n\}$$

Theorem 3.0.2 (Bezout's Theorem)**.** *Let $m_1, m_2 \in \mathbb{Z} \setminus \{0\}$. Then there exists $x_1, x_2 \in \mathbb{Z}$ such that $\gcd(m_1, m_2) = x_1 m_1 + x_2 m_2$.*

Remark 3.0.3. A similar proof yields that for $m_1, m_2, ..., m_r \in \mathbb{Z} \setminus \{0\}$, there exists $x_1, x_2, ..., x_r \in \mathbb{Z}$ such that

$$\gcd(m_1, m_2, ..., m_r) = x_1 m_1 + x_2 m_2 + \cdots + x_r m_r$$

Here,

$$\gcd(m_1, m_2, ..., m_r) = \max\{d \in \mathbb{N} : d \mid m_1, d \mid m_2, ..., d \mid m_r\}$$

Theorem 3.0.4 (Well Ordering Principle)**.** *Let $A \subseteq \mathbb{N}$ be a nonempty set. Then A has a minimum.*

3.1 Mathematical Induction

Theorem 3.1.1 (Principle of Mathematical Induction)**.** *For all $n \in \mathbb{N}$, let $A(n)$ be an assertion (i.e. a statement that is either true or false). Assume that we can prove the following*

(i) $A(1)$ is true.

(ii) *Whenever $n \in \mathbb{N}$ is such that $A(n)$ is true, then $A(n+1)$ must be true as well.*

Then $A(n)$ is true for all $n \in \mathbb{N}$.

Example 3.1.2. Suppose $A(n)$ is the assertion that "$n \leq 2^n$" for all $n \in \mathbb{N}$. We could see that $A(1)$, $A(2)$, $A(3)$ is true, and may also be true for higher n.

Proof. Define $S = \{n \in \mathbb{N} : A(n) \text{ is true}\}$. We want to show $S = \mathbb{N}$. From (i), $1 \in S$. Define $B = \mathbb{N} \setminus S$. We will show that $B = \emptyset$, which then implies $S = \mathbb{N}$. For contradiction, let us assume that $B \neq \emptyset$. By the Well Ordering Principle (Theorem 3.0.4), there exists an $m_0 = \min(B)$ since

- $1 \in S$ which implies $m_0 \neq 1$ and so $m_0 > 1$ or $m_0 \geq 2$.
- $m_0 - 1 < m_0 = \min(B)$ which implies that $m_0 - 1 \geq 1$ and $m_0 - 1 \notin B$ which implies that $m_0 - 1 \in S$ and so $A(m_0 - 1)$ is true.

By (ii), $A(m_0 - 1)$ being true implies $A(m_0 - 1 + 1) = A(m_0)$ is true and so $m_0 \in S$. But this is absurd, and so $B = \emptyset$. $\square$

Exercise. Prove that for all $n \in \mathbb{N}$,

$$\left(1 + \frac{1}{1}\right)^1 \left(1 + \frac{1}{2}\right)^2 \cdots \left(1 + \frac{1}{n}\right)^n = \frac{(n+1)^n}{n!}$$

Solution. For the base case $n = 1$, we have

$$\left(1 + \frac{1}{1}\right)^1 = 2$$

and

$$\frac{(1+1)^1}{1!} = 2$$

So the base case is true. Now assume that for all $n \in \mathbb{N}$,

$$\left(1 + \frac{1}{1}\right)^1 \left(1 + \frac{1}{2}\right)^2 \cdots \left(1 + \frac{1}{n}\right)^n = \frac{(n+1)^n}{n!}$$

Then for $n + 1 \in \mathbb{N}$, we have

$$\begin{aligned}
\left(1 + \frac{1}{1}\right)^1 \left(1 + \frac{1}{2}\right)^2 \cdots \left(1 + \frac{1}{n+1}\right)^{n+1} &= \frac{(n+1)^n}{n!} \cdot \left(1 + \frac{1}{n+1}\right)^{n+1} \\
&= \frac{(n+1)^n}{n!} \left(\frac{n+2}{n+1}\right)^{n+1} \\
&= \frac{(n+2)^{n+1}}{(n+1)n!} = \frac{(n+2)^{n+1}}{(n+1)!}
\end{aligned}$$

as desired.

Theorem 3.1.3 (Strong Mathematical Induction)**.** *For $n \in \mathbb{N}$, let $A(n)$ be an assertion and assume that we can prove the following:*

(i) *$A(1)$ is true*

(ii) *If $n \in \mathbb{N}$ is such that $A(1), A(2), ..., A(n)$ are all true, then $A(n+1)$ must also be true as well.*

Then for all $n \in \mathbb{N}$, $A(n)$ is true.

Proof. The proof is similar as Theorem 3.1.1. □

3.2 Unique Factorization

Recall that if $p \in \mathbb{N}$ is such that $p \geq 2$, then p is called a *prime number* if its only divisors in $\mathbb{N}$ are 1 and p.

Example 3.2.1. 2, 3, 5, 7, 11,... are all prime numbers

Theorem 3.2.2 (Prime Factorization)**.** *Let $n \in \mathbb{N}$ with $n \geq 2$. Then n can be written as a product of prime numbers*

$$n = p_1 \cdot p_2 \cdots p_r$$

Remark 3.2.3. (i) If $n = p_1 \cdot p_2 \cdots p_r$, then some of the primes may be repeated. For example, $12 = 2 \cdot 2 \cdot 3$.

(ii) If $n = p$ is already prime, we consider this a trivial product of primes.

Proof by Strong Induction. For the base case $n = 2$ is prime, so it is trivially a product of primes. Let $n \in \mathbb{N}$ for $n \geq 2$ be such that 2, 3, 4,..., n can all be written as a product of primes. We want to show that $n+1$ is a product of primes.

Case 1: $n+1$ is already prime, so there is nothing that needs to be shown.

Case 2: $n+1$ is not prime, then there exists a $d \in \mathbb{N}$ such that $d \neq 1$ and $d \neq n+1$ such that $d \mid n+1$. Since $1 \leq d \leq n+1$, we have

$$1 < d < n+1 \tag{1}$$

Then there exists a $q \in \mathbb{Z}$ such that $n+1 = qd$. Then $q \in \mathbb{N}$ and $q \mid n+1$ which implies that $1 \leq q \leq n+1$. From (1), we have

$$1 < q < n+1 \tag{2}$$

and so we have $2 \leq d \leq n$ and $2 \leq q \leq n$. By the inductive hypothesis, d and q may be written as products of primes. Because $n+1 = qd$ is a product of primes. $\square$

Remark 3.2.4. In $n = p_1 \cdot p_2 \cdots p_r$ there may be repetitions. We may avoid these and write

$$n = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$$

where $p_1 < p_2 < \cdots < p_s$ are prime numbers and $m_1, m_2, ..., m_s \in \mathbb{N}$.

Example 3.2.5. $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3^1$