MATH 3021: Algebra I

Joe Tran

Preface

These are the first edition of these lecture notes for MATH 3021 (Algebra I). Consequently, there may be several typographical errors. Not every result in these notes will be covered in class. For example, some results will be covered through assignments. However, these notes should be fairly self-contained. If you come across any typos, errors, omissions, or unclear explanations, please feel free to contact me so that I may continually improve these notes.

Contents

Week 1

September 4-8

LECTURE 1

September 6, 2023

- Meetings: MWF 9:30 AM R S174
- Student Hours: M 3:00 PM-4:00 PM via Zoom
- Text: Abstract Algebra, Judson
- Evaluation:
  - Assignments: 30%
  - Midterm: 30%
  - Final: 40%

What is algebra? Studies the 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 main subject of MATH 3021. This class is indeed a proof-based course, so MATH 1200 or equivalent is required to complete this course. It is important to be fluent in proof-writing and be familiar with proof methods (contradiction, induction, etc.).

We will be having a look at some review material from MATH 1200 first, before getting into the integers.

1. MATH 1200 Review

1.1. Set Notations.

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 natural numbers $\mathbb{N} = \{1, 2, 3, ...\}$
- Set of integers $\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$
- 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 $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$.
- $\mathcal{M}_n(\mathbb{R})$ denotes the set of all $n \times n$ matrices with real entries.
- $\mathbb{R}^{\mathbb{R}}$ denotes all functions $f : \mathbb{R} \to \mathbb{R}$.

NOTATION 1.1.3. Let A be a set, and let x be an object. We say that x is an element of A and write $x \in A$. If x is not an element of A, we write $x \notin A$.

NOTATION 1.1.4. Let A be a set. We denote the cardinality of the set A by $|A|$, which denotes the number of elements in the set A.

EXAMPLE 1.1.5. If $A = \emptyset$ and $B = \{1, 3, 5\}$, then $|A| = 0$, and $|B| = 3$.

NOTATION 1.1.6. For sets A and B, we say that A is a subset of B and write $A \subset B$, if every element in A is in B. We also say that A is a proper subset of B and write $A \subsetneq B$ if $A \subset B$ but $A \neq B$.

EXAMPLE 1.1.7. $\emptyset \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

NOTATION 1.1.8. For sets A and B, we have the following set operations

- $A \cup B$ for the union of two sets.
- $A \cap B$ for the intersection of 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.

1.2. Functions.

DEFINITION 1.2.1. Let X and Y be sets. A function $f : X \to Y$ is a rule that assigns to every $x \in X$ to a unique $f(x) \in Y$. We call X the domain and Y the codomain of f.

NOTATION 1.2.2. Let X and Y be sets and let $f : X \to Y$ be a function. The graph of f we denote it by

$$\mathrm{gr}(f) = \{(x, f(x)) : x \in X\} \subset X \times Y$$

EXAMPLE 1.2.3. Let X be a set. We denote the identity function by $id_X : X \to X$ and is a function such that for all $x \in X$, $id_X(x) = x$.

EXAMPLE 1.2.4. Let X and Y be sets, let $f : X \to Y$ be a function, and suppose $y_0 \in Y$ is arbitrary. Then $f(x) = y_0$ always.

DEFINITION 1.2.5. Let X and Y be nonempty sets, and let $f : X \to Y$ be a function.

- The function f is said to be *one-to-one* if for all $x_1, x_2 \in X$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$.
- The function f is said to be *onto* if for all $y \in Y$, there exists an $x \in X$ such that $f(x) = y$.
- The function f is said to be a *bijection* if it is both one-to-one and onto.

EXAMPLE 1.2.6. The following are examples that describes one-to-one, onto, and bijection:

- Let $f : \mathbb{R} \to \mathbb{R}$ be a function with $f(x) = e^x$. Then f is one-to-one, but it is not onto.

- Let $f : \mathbb{R} \to [0, \infty)$ be a function with $f(x) = x^2$. Then f is onto, but it is not one-to-one.
- Let $f : (0, \infty) \to \mathbb{R}$ be a function with $f(x) = \ln(x)$. Then f is both one-to-one and onto, therefore it is a bijection.

DEFINITION 1.2.7. Let X and Y be sets, let $f : X \to Y$ be a function, and let $A \subset X$. We define the *image of A under f* by

$$f(A) = \{y \in Y : \exists x \in A : f(x) = y\} = \{f(x) : x \in A\} \subset Y$$

In particular, $f(X)$ is called the range of f.

REMARK 1.2.8. The range and the codomain may not necessarily be the same.

EXAMPLE 1.2.9. Suppose we let $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2$. The codomain is $\mathbb{R}$ while the range is $f(\mathbb{R}) = [0, \infty)$.

NOTATION 1.2.10. Let X, Y and Z be sets, let $f : X \to Y$ and $g : Y \to Z$ be functions. We define the composition of $g \circ f$ as the function $g \circ f : X \to Z$.

EXAMPLE 1.2.11. Take $f : (0, \infty) \to \mathbb{R}$ with $f(x) = \sqrt{x} - x^2$ and $g : \mathbb{R} \to (0, \infty)$ given by $g(x) = e^x$. Then

$$g(f(x)) = e^{\sqrt{x} - x^2} : (0, \infty) \to (0, \infty)$$

REMARK 1.2.12. If X is a set and $f, g : X \to X$, then $g \circ f$ and $f \circ g$ exists, but are not necessarily the same.

EXAMPLE 1.2.13. Let $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2 + 1$ and $g : \mathbb{R} \to \mathbb{R}$ with $g(x) = x + 1$. Then

$$f(g(x)) = (x + 1)^2 + 1 \quad g(f(x)) = x^2 + 2$$

DEFINITION 1.2.14. Let X and Y be sets and let $f : X \to Y$ be a function. We say that f is *invertible* if there exists a $g : Y \to X$ such that $f \circ g = id_Y(y)$ and $g \circ f = id_X$. If such a g exists, then denote it by f^{-1} and call it the inverse of f.

EXAMPLE 1.2.15. Take $f : \mathbb{R} \to (0, \infty)$ given by $f(x) = e^x$. Its inverse is the natural logarithm $g : (0, \infty) \to \mathbb{R}$ with $g(x) = \ln(x)$. Then $f(g(x)) = y$ and $g(f(x)) = x$.

PROPOSITION 1.3. *Let X and Y be sets. The function f is invertible if and only if it is a bijection.*

1.4. Equivalence Relations.

DEFINITION 1.4.1. Let X be a nonempty set. A binary relation "$\sim$" on X is called an *equivalence relation* if the following properties hold:

- (Reflexivity) For all $x \in X$, $x \sim x$.
- (Symmetry) For all $x, y \in X$, if $x \sim y$, then $y \sim x$.
- (Transitivity) For all $x, y, z \in X$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

EXAMPLE 1.4.2. Let $n \in \mathbb{N}$ and let $x, y \in \mathbb{Z}$. We say that x is congruent to y modulo n and write $x \equiv y \bmod n$ if $x - y$ is an integer multiple of n, i.e. $n \mid x - y$. We will show next time that congruence modulo is a relation.

LECTURE 2

September 8, 2023

1. Equivalence Relations

In the previous lecture, we started talking about the equivalence relations.

DEFINITION 1.1. Let X be a nonempty set. A binary relation "$\sim$" on X is called an *equivalence relation* if the following properties hold:

- (Reflexivity) For all $x \in X$, $x \sim x$.
- (Symmetry) For all $x, y \in X$, if $x \sim y$, then $y \sim x$.
- (Transitivity) For all $x, y, z \in X$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

EXAMPLE 1.2. Let $n \in \mathbb{N}$ and let $x, y \in \mathbb{Z}$. We say that x *is congruent to* y *modulo* n *and write* $x \equiv y$ *mod* n if $x - y$ is an integer multiple of n, i.e. $n \mid x - y$, or there exists an integer $k \in \mathbb{Z}$ such that $x - y = kn$.

For example, if we consider $7 \equiv 17 \mod 5$, then this congruence is true since $7 - 17 = -10 = (-2) \cdot 5$.

Using Definition 1.1, we will show that $x \equiv y \mod n$ is an equivalence relation.

First, showing reflexivity, let $x \in \mathbb{Z}$ be arbitrary. Then

$$x - x = 0 \cdot n \Rightarrow x \equiv x \mod n$$

Therefore, congruence modulo n is reflexive.

Next, showing symmetry, let $x, y \in \mathbb{Z}$ be arbitrary. Then there exists a $k \in \mathbb{Z}$ such that

$$x - y = kn \Rightarrow y - x = -k \cdot n \Rightarrow y \equiv x \mod n$$

Therefore, congruence modulo n is symmetric.

Finally, showing transitivity, since $x \equiv y \mod n$, there exists an integer $k_0 \in \mathbb{Z}$ such that $x - y = k_0 n$. Similarly, since $y \equiv z \mod n$, there exists an integer $k_1 \in \mathbb{Z}$ such that $y - z = k_1 n$. Now adding the two equations above, we have

$$x - z = k_0 n + k_1 n = (k_0 + k_1)n \Rightarrow x \equiv z \mod n$$

Therefore, congruence modulo n is transitive, and hence, congruence modulo n is an equivalence relation.

EXAMPLE 1.3. Consider the set $X = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Define "$\sim$" on X as follows: If $(p, q), (r, s) \in X$, then $(p, q) \sim (r, s)$ if $ps = qr$. This is an equivalence relation.

For example, consider $(3,2) \sim (9,6)$. Then these are equivalent since $3 \cdot 6 = 2 \cdot 9 = 18$.

As an exercise, show that $\sim$ is reflexive and symmetric. We will show that $\sim$ is transitive.

Consider three pairs $(p,q),(r,s),(u,v) \in X$ such that $(p,q) \sim (r,s)$ and $(r,s) \sim (u,v)$. Then this implies that $ps = qr$ and $rv = su$. We want to show that $(p,q) \sim (u,v)$, that is, $pv = qu$. Let us multiply the first equation by v. Then we would have that $pvs = qvr$. Here now, we can replace $rv = su$ and so $pvs = qsu$ and since $s \neq 0$, then we would obtain that $pv = qu$ and therefore, $(p,q) \sim (u,v)$.

2. Equivalence Classes

DEFINITION 2.1. Let X be a nonempty set, and let $\sim$ denote an equivalence relation on X. For $x \in X$, we define the *equivalence class* of x as follows:

$$[x] = \{y \in X : x \sim y\}$$

EXAMPLE 2.2. Take $\mathbb{Z}$ with congruence modulo 5. Say we take $3 \in \mathbb{Z}$, then

$$\begin{aligned}[3] &= \{3, 8, 13, 18, ..., -2, -7, ...\} \\ &= \{k \in \mathbb{Z} : 3 + 5k\}\end{aligned}$$

EXAMPLE 2.3. Take $X = \mathbb{Z} \setminus (\mathbb{Z} \setminus \{0\})$ with the defined $\sim$ in Example 1.3. Then say we take $(2,3)$. We have

$$\begin{aligned}[(2,3)] &= \{(2,3), (-2,-3), (4,6), (-4,-6), ...\} \\ &= \{k \in \mathbb{Z} : (2k, 3k)\} \\ &= \left\{\text{all pairs } (p,q) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \text{ such that } \frac{p}{q} = \frac{2}{3}\right\}\end{aligned}$$

THEOREM 2.4. *Let $\sim$ be an equivalence relation on a set X. Then the equivalence classes of $\sim$ form a partition of X. That is,*

1. *$X = \bigcup_{x \in X} [x]$, i.e. the collection of equivalence classes covers the set X.*
2. *If $x, y \in X$, then either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.*

PROOF. (i) Let $x, \in X$ be arbitrary. Then $[x] \subset X$ implies that $\bigcup_{x \in X} [x] \subset X$. We also show $X \subset \bigcup_{x \in X} [x]$. Let $x_0 \in X$ be arbitrary. Then $x_0 \sim x_0$ implies that $x_0 \in [x_0] \subset \bigcup_{x \in X} [x]$ implies that $X \subset \bigcup_{x \in X} [x]$, and hence $X = \bigcup_{x \in X} [x]$.

(ii) Let $x, y \in X$ be arbitrary. If $[x] \cap [y] = \emptyset$, there is nothing to prove. Otherwise, assume that there exists a point $z_0 \in [x] \cap [y]$. We will show that $[x] = [y]$, that is, $[x] \subset [y]$ and $[y] \subset [x]$. To see that $[x] \subset [y]$, let $w \in [x]$ be arbitrary. Then this implies that $x \sim w$. But $z_0 \in [x]$ as well, and so $x \sim z_0$. By these two relations, $w \sim z_0$ by transitivity. Furthermore, $z_0 \in [y]$ as well

and hence, $y \sim z_0$ and hence $w \sim y$ by transitivity once again, implying to $w \in [y]$, as desired. □

EXAMPLE 2.5. Let $X = \mathbb{Z}$ be equipped with the congruence modulo 5. Consider the following equivalence classes:

$$[0] = \{..., -10, -5, 0, 5, 10, ...\}$$
$$[1] = \{..., -9, -4, 1, 6, 11, ...\}$$
$$[2] = \{..., -8, -3, 2, 7, 12, ...\}$$
$$[3] = \{..., -7, -2, 3, 8, 13, ...\}$$
$$[4] = \{..., -6, -1, 4, 9, 14, ...\}$$

We can see that all of these sets are disjoint from each other.

3. The Integers: Mathematical Induction

Let $S(n)$ be a statement about some integers that is either True or False for each n.

EXAMPLE 3.1. For example,

- $S(n) := \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
- $S(n) := n$ is odd

THEOREM 3.2 (Principal of Mathematical Induction). *Let $S(n)$ be a statement about integers. Assume*

- *There exists an integer $k_0 \in \mathbb{Z}$ such that $S(k_0)$ is true.*
- *For any $k \geq k_0$ if $S(k)$ is true, then $S(k+1)$ must also be true.*

Then $S(n)$ must be true for all $n \geq k_0$.

Week 2

September 11-15

LECTURE 3

September 11, 2023

1. Mathematical Induction

Recall in the previous lecture, we started to introduce the concept of mathematical induction.

THEOREM 1.1 (Principal of Mathematical Induction). *Let $S(n)$ be a statement about integers. Assume*

- *There exists an integer $k_0 \in \mathbb{Z}$ such that $S(k_0)$ is true.*
- *For any $k \geq k_0$ if $S(k)$ is true, then $S(k+1)$ must also be true.*

Then $S(n)$ must be true for all $n \geq k_0$.

EXAMPLE 1.2. Prove that for all $n \in \mathbb{N}$, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

SOLUTION. We first show that for the base case $n = 1$, the statement is true. On the left side, we have $\sum_{k=1}^{1} k = 1$ and on the right side, we have $\frac{1\cdot(1+1)}{2} = \frac{2}{2} = 1$, so the base case is true. Now assume that for $n \in \mathbb{N}$, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ holds. Then we want to show that for $n+1 \in \mathbb{N}$, $\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$. On the left side, we have that

$$\begin{aligned}\sum_{k=1}^{n+1} k &= 1 + 2 + 3 + \cdots + n + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}\end{aligned}$$

as desired. Therefore, by mathematical induction, we have shown that $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

THEOREM 1.3 (Second Principal of Mathematical Induction (Strong Induction)). *Let $S(n)$ be a statement about integers and assume the following:*

- *There exists some integer $k_0 \in \mathbb{Z}$ such that $S(k_0)$ is true.*
- *If $k \geq k_0$ is an integer such that $S(k_0)$, $S(k_0+1)$, ..., $S(k)$ are all true, then $S(k+1)$ must also be true.*

Then for all $n \geq k_0$, $S(n)$ is true.

THEOREM 1.4 (Well-Ordering Principle). *Let A be a nonempty subset of $\mathbb{N} = \{1, 2, 3, ...\}$. Then A has a least element, i.e. there exists an $a_0 \in A$ such that for all $a \in A$, $a_0 \leq a$, or $a_0 = \min(A)$.*

REMARK 1.5. $\mathbb{Z}$ does not satisfy the Well-Ordering Principle (Theorem 1.4) since if we take $\mathbb{Z}$ as a subset of itself, it does not have a least element.

PROOF. We will take for granted that 1 is the least element of $\mathbb{N}$. Take $A \subset \mathbb{N}$ and assume that $A \neq \emptyset$. We will prove using cases.

Case 1: Assume that $1 \in A$, then obvious, $1 = \min(A)$.

Case 2: Assume that $1 \notin A$. Assume A has no least element, i.e. for every $a \in A$, there exists an $a_1 \in A$ such that $a_1 < a$. We will perform a clever strong induction (Theorem 1.3) to show that $A = \emptyset$. This would be absurd. The statement $S(n)$ will be "$n \notin A$". We verify the base case for when $n = 1$. Because we are in Case 2, $1 \notin A$, which is true. For the inductive hypothesis, let $k > 1$ such that $1 \notin A$, $2 \notin A$,..., $k \notin A$. Then we want to show that $k + 1 \notin A$. Assume that $k + 1 \in A$ (for contradiction). Since A has no least element, $k + 1$ is not the least element, therefore there is some $a \in A$ with $a < k + 1$, then $1 \leq a \leq k$, but by the inductive hypothesis, $a \notin A$, which is absurd, and therefore, we finished the induction and so $k + 1 \notin A$.

Therefore, by strong induction, for all $n \in \mathbb{N}$ with $n \notin A$, i.e. $A = \emptyset$. This is absurd. □

DEFINITION 1.6. Let $A \subset \mathbb{Z}$ be a nonempty set.

- An integer $k \in \mathbb{Z}$ is said to be a *lower bound* of A if for all $a \in A$, $k \leq a$.
- If there exists a $k \in \mathbb{Z}$ such that k is a lower bound for A, then we say that A is *bounded below*.

EXERCISE 1.7. Let $A \subset \mathbb{Z}$ be a nonempty subset and bounded below. Prove that A has a least element using strong induction.

EXERCISE 1.8. Formulate what it should mean that a subset of $\mathbb{Z}$ is bounded above.

EXERCISE 1.9. Prove that a nonempty subset $A \subset \mathbb{Z}$ and bounded above has a greatest element using strong element.

2. Division

NOTATION 2.1. For $a, b \in \mathbb{Z}$ with $a \neq 0$, we will say a *divides* b and write $a \mid b$ if b is an integer multiple of a, i.e. there exists some integer $k \in \mathbb{Z}$ such that $b = ka$.

EXAMPLE 2.2. For example, we can consider $2 \mid 4$ and $3 \mid 27$, but $3 \nmid 14$.

PROPOSITION 2.3. *If $a, b, c, x, y \in \mathbb{Z}$ with $a \neq 0$, and $a \mid b$ and $a \mid c$, then $a \mid xb + yc$. To see this,*

PROOF. Since $a \mid b$, there exists an integer $k \in \mathbb{Z}$ such that $b = ka$. Similarly, since $a \mid c$, there exists an integer $m \in \mathbb{Z}$ such that $c = ma$. Multiplying the first equation by x and multiplying the second equation by y we obtain $xb = xka$ and $yc = yma$ and so adding these two equations together, we obtain

$$xb + yc = xka + yma = (xk + ym)a$$

where $xk + ym \in \mathbb{Z}$ as well, and thus, by definition of divisibility, $a \mid xb + yc$ as desired. □

PROPOSITION 2.4. *If $a, b \in \mathbb{Z}$ with $a, b \neq 0$ such that $a \mid b$, then $|a| \leq |b|$.*

PROOF. Indeed, since $a \mid b$, we have some integer $k \in \mathbb{Z}$ such that $b = ka$ and so $|b| = |k||a|$. But since $b \neq 0$, then $k \neq 0$ and therefore, $|k| \geq 1$, implying that $|b| = |k||a| \geq 1 \cdot |a| = |a|$, as desired. □

THEOREM 2.5 (Division Algorithm). *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that $0 \leq r < b$ such that $a = qb + r$. We call q the quotient and r the remainder of the division a by b. By unique, we mean that there is exactly one q and one r that will make $a = qb + r$.*

REMARK 2.6. $a \equiv r \bmod b$ since $a - r = qb$.

LECTURE 4

September 13, 2023

1. The Division Algorithm

Recall in the previous lecture we started to have a look at divisibility and the Euclidean division algorithm.

NOTATION 1.1. For $a, b \in \mathbb{Z}$ with $a \neq 0$, we will say a *divides* b and write $a \mid b$ if b is an integer multiple of a, i.e. there exists some integer $k \in \mathbb{Z}$ such that $b = ka$.

THEOREM 1.2 (Division Algorithm). *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that $0 \leq r < b$ such that $a = qb + r$. We call q the quotient and r the remainder of the division a by b. By unique, we mean that there is exactly one q and one r that will make $a = qb + r$.*

REMARK 1.3. $a \equiv r \bmod b$ since $a - r = qb$.

PROOF. Define $S = \{a - kb : k \in \mathbb{Z} \text{ and } a - kb \geq 0\}$. Note that S is bounded below by 0 and S has to be nonempty, which we have to verify! We will take two cases, depending on the value of a.

(1) If $a \geq 0$, then $a = a - 0 \cdot b \in S$.
(2) If $a < 0$, then $(-a)(b - 1) = a - a \cdot b \geq 0$ and so $a - ab \in S$.

Thus, S cannot be empty.

By the Well-Ordering Principle (Theorem 1.4), there exists an $r = \min(S)$, i.e. $r \in S$ and for all $m \in S$, $r \leq m$. Since $r \in S$, we know that $0 \leq r$ and there exists a $k \in \mathbb{Z}$ such that $r = a - kb$. Let us relabel k as q, so that $a = qb + r$.

We now need to show that $0 \leq r < b$. We know $0 \leq r$, so we check $r < b$. Towards contradiction, assume that $r \geq b$. Then this implies that $0 \leq r - b = a - qb - b = a - b(q + 1) \in S$ and $r - b < r = \min(S)$, which is absurd. Therefore, it must be the case that $r < b$.

Finally, we need to show that q and r are unique. Take $q', r' \in \mathbb{Z}$ such that $0 \leq r' < b$ and $a = q'b + r'$, we need to show that $q' = q$ and $r' = r$. Observe that $0 \leq r' = a - q'b \in S$ so $r' \geq \min(S) = r$. Now proceed by contradiction and assume that $r' \neq r$. Since $r' \geq r$ from, and $r' \neq r$, then $r' > r$. So now $0 < r' - r = a - q'b - (a - qb) = (q - q')b$ which implies that $b \mid r' - r$ therefore, by Proposition 2.4, $|b| \leq |r' - r|$ which implies that $b \leq r' - r \leq r'$. This is absurd since $r' < b$. Therefore, $r = r'$ and thus, it follows that $q = q'$ as well. □

2. Greatest Common Divisor

DEFINITION 2.1. Let $a, b \in \mathbb{Z} \setminus \{0\}$. The *greatest common divisor* of a and b is defined as

$$\gcd(a, b) = \max\{k \in \mathbb{N} : k \mid a \text{ and } k \mid b\}$$

REMARK 2.2. $\gcd(a, b)$ is well-defined and $1 \leq \gcd(a, b) \leq \min\{|a|, |b|\}$. We justify that We justify that $D = \{k \in \mathbb{N} : k \mid a \text{ and } k \mid b\}$ contains 1 and thus, nonempty. Second, if $k \in D$, then because $k \mid a$, then $|k| \leq |a|$ which implies that $k \leq |a|$. Similarly, since $k \mid b$, then $|k| \leq |b|$ which implies that $k \leq |b|$. Therefore, $\min\{|a|, |b|\}$ is an upper bound for D.

THEOREM 2.3 (Bezouts' Theorem). *For $a, b \in \mathbb{Z} \setminus \{0\}$, there exists integers $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = xa + yb$.*

PROOF. Define $S = \{xa + yb : x, y \in \mathbb{Z}, xa + yb \geq 1\}$. We need to observe that $S \neq \emptyset$. Indeed, take $1 \leq |a| = \frac{|a|}{a} \cdot a + 0 \cdot b \in S$ which implies that $|a| \in S$ and similarly, $|b| \in S$ as well. By the Well-Ordering Principle (Theorem 1.4), there exists a $d = \min(S)$ and $d \leq \min\{|a|, |b|\}$. Since $d \in S$, there exists $x, y \in \mathbb{Z}$ such that $d = xa + yb$ and $d \geq 1$.

We want to show that $xa + yb = \gcd(a, b)$. The first step is to show that d divides a. By the Division Algorithm (Theorem 1.2), there exists $q, r \in \mathbb{Z}$ such that $0 \leq r < d$ such that $a = qd + r$. We claim that $r = 0$ so that $d \mid a$. Assume otherwise that $r \neq 0$, and so in particular, $1 \leq r < d$, and so writing $1 \leq r = a - qd = a - q(xa + yb) = (1 - qx)a + (-qy)b$, and thus, $r \in S$ and $r < d = \min(S)$ which is absurd. The proof to show that $d \mid b$ is similar.

Finally, we need to show that d is a common divisor of a and b, and we need to show that it is the greatest. If we take $k \in \mathbb{N}$ such that $k \mid a$ and $k \mid b$, then we need to deduce that $k \leq d$. Since $k \mid a$ and $k \mid b$, then $k \mid xa + yb = d$ (by Proposition 2.3), which implies that $|k| \leq |d|$ (by Proposition 2.4) and therefore, $k \leq d$ as desired. □

REMARK 2.4. If $a, b \in \mathbb{Z} \setminus \{0\}$ such that $\gcd(a, b) = 1$, then a and b are called *relatively prime* or *coprime*. In this case, by Bezout's Theorem (Theorem 2.3), there exists integers $x, y \in \mathbb{Z}$ such that $xa + yb = 1$.

3. Prime Numbers

DEFINITION 3.1. A $p \in \mathbb{N}$ is called a prime number if

(1) $p \geq 2$
(2) the number $k \in \mathbb{N}$ such that $k \mid p$ are $k = 1$ and $k = p$.

REMARK 3.2. If $n \in \mathbb{N}$ with $n \geq 2$, always $1, n \in \{k \in \mathbb{N} : k \mid n\}$. A number $p \geq 2$ if this set is the smallest possible.

LECTURE 5

September 15, 2023

1. Prime Numbers

Recall in the previous lecture, we have defined and shown the following:

REMARK 1.1. If $a, b \in \mathbb{Z} \setminus \{0\}$ such that $\gcd(a, b) = 1$, then a and b are called *relatively prime* or *coprime*. In this case, by Bezout's Theorem (Theorem 2.3), there exists integers $x, y \in \mathbb{Z}$ such that $xa + yb = 1$.

REMARK 1.2. If $n \in \mathbb{N}$ with $n \geq 2$, always $1, n \in \{k \in \mathbb{N} : k \mid n\}$. A number $p \geq 2$ if this set is the smallest possible.

DEFINITION 1.3. A $p \in \mathbb{N}$ is called a prime number if

(1) $p \geq 2$
(2) the number $k \in \mathbb{N}$ such that $k \mid p$ are $k = 1$ and $k = p$.

EXAMPLE 1.4. $p = 7$ is a prime because its divisors are 1 and 7. But $n = 6$ is not prime because its divisors are 1, 2, 3, 6.

PROPOSITION 1.5. *Let $n \in \mathbb{N}$ with $n \geq 2$. If n is not prime, then there exists $a, b \in \mathbb{Z}$ such that $n = ab$ and $2 \leq a, b \leq n - 1$.*

PROOF. Since n is not prime, there exists an $a \in \mathbb{N}$ such that $a \mid n$ and furthermore, $a \neq 1$ and $a \neq n$. In particular, $2 \leq a \leq n - 1$. $a \mid n$ implies that there exists an integer $b \in \mathbb{Z}$ such that $n = ab$. We need to show that $2 \leq b \leq n - 1$. Indeed, $b > 0$ since $n = ab > 0$. Furthermore, $b \neq 1$ since if otherwise, then $n = a$, which is not true. Moreover, $b \neq n$ since that would imply that $a = 1$. Finally, if $b \leq n$, then $b \mid n$. Therefore, $2 \leq b \leq n - 1$ is the only possibility. □

EXERCISE 1.6. Let p, q be prime. If $p \mid q$, then $p = q$.

PROOF. Let p, q be arbitrary prime numbers. Since $p \mid q$, then there exists an integer $k \in \mathbb{Z}$ such that $q = kp$. Since q is prime, it cannot be a product of two other integers, except if $k = 1$. So $q = 1 \cdot p$, and therefore, $p = q$, as desired. □

PROPOSITION 1.7. *Let p be a prime number and $a, b \in \mathbb{Z}$, if $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

PROOF. Assume that $p \mid a$, then there is nothing to prove. If $p \nmid a$, then we will show that $p \mid b$. Since p is prime and $p \nmid a$, the $\gcd(a, p) = 1$ (the greatest common divisor of a and p is 1 since p does not divide a, and so

the only value left that is a common divisor is 1.) By Bezout's Theorem (Theorem 2.3), there exists $x, y \in \mathbb{Z}$ such that

$$xa + yp = 1 \tag{1}$$

Since $p \mid ab$, there exists an integer $k \in \mathbb{Z}$ such that

$$ab = kp \tag{2}$$

Take (1), and multiply both sides by b so that

$$xab + ypb = b \tag{1}$$

Now, using (2), we can substitute (1) to (2) so that

$$xkp + ypb = b$$

and therefore,

$$(xk + yb)p = b$$

and so $p \mid b$, as desired. □

Corollary 1.8. *Let p be a prime number and $a_1, a_2, ..., a_n \in \mathbb{Z}$ such that $p \mid a_1 a_2 \cdots a_n$. For some $1 \leq i \leq n$, $p \mid a_i$.*

Proof. We will prove the corollary using induction. For the base case when $n = 2$, we have $p \mid a_1 a_2$, and by Proposition 1.7, $p \mid a_1$ or $p \mid a_2$. Now assume that for $n = k \in \mathbb{N}$, $p \mid a_1 a_2 \cdots a_k$ such that for some $1 \leq i \leq k$, $p \mid a_i$. We want to show that for $n = k + 1$, $p \mid a_1 a_2 \cdots a_{k+1}$ such that $p \mid a_i$. We consider the following cases:

(1) $\gcd(p, a_{k+1}) = p$, if so, let $i = n + 1$ and so $p \mid a_i$.
(2) $\gcd(p, a_{k+1}) = 1$, if so, $p \not| a_{n+1}$ so p and a_{n+1} are relatively prime and p divides $(a_1 \cdots a_n)a_{n+1}$, and thus, $p \mid a_1 \cdots a_n$.

Therefore, we have shown that $p \mid a_i$, □

Proposition 1.9. *Let $a, b, c \in \mathbb{Z} \setminus \{0\}$ and assume that $\gcd(a, b) = 1$ and $a \mid bc$. Then $a \mid c$.*

Proof. Assume that $\gcd(a, b) = 1$. Then by using Bezout's Theorem (Theorem 2.3), there exists integers $x, y \in \mathbb{Z}$ such that

$$xa + yb = 1 \tag{1}$$

Since $a \mid bc$, there exists an integer $k \in \mathbb{Z}$ such that

$$bc = ka \tag{2}$$

Now multiplying both sides of (1) by c, we have

$$xac + ybc = c \tag{1}$$

and now substituting (2) to (1) we obtain

$$xac + yka = c \Rightarrow a(xc + yk) = c$$

and therefore, $xc + yk \in \mathbb{Z}$ and so $a \mid c$, as desired. □

THEOREM 1.10 (Fundamental Theorem of Arithmetic). *For every integer $n \in \mathbb{N}$ with $n \geq 2$, there exists perhaps repeating prime numbers $p_1 \leq p_2 \leq \cdots \leq p_\ell$, such that*

$$n = p_1 \cdot p_2 \cdots p_\ell$$

Furthermore, these are unique, if $q_1 \leq q_2 \leq \cdots \leq q_m$ are prime numbers such that

$$n = q_1 \cdot q_2 \cdots q_m$$

Then $\ell = m$ and for each $1 \leq i \leq \ell = m$, $p_i = q_i$.

EXAMPLE 1.11. $6 = 2 \cdot 3$, $21 = 3 \cdot 7$, $28 = 2 \cdot 2 \cdot 7$.

REMARK 1.12. By grouping repeating numbers, for $n \geq 2$, $n \in \mathbb{N}$, there exists prime numbers $p_1 < p_2 < \cdots < p_\ell$ and $k_1, k_2, ..., k_\ell \in \mathbb{N}$ such that

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_\ell^{k_\ell}$$

EXAMPLE 1.13. Take $28 = 2 \cdot 2 \cdot 7$ from above. Then $28 = 2^2 \cdot 7$. Take $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$. Then $360 = 2^3 \cdot 3^2 \cdot 5$.

PROOF. We will prove the theorem for $n \in \mathbb{N}$ with $n \geq 2$ by strong induction, starting with $n = 2$. Take $p_1 = 2$, i.e. $n = p_1$. Next, assume

$$2 = q_1 \cdot q_2 \cdots q_m$$

where $q_1, q_2, ..., q_m$ are prime. Take $1 \leq i \leq m$, then $q_i \mid 2$ implies that $q_i = 2$, and therefore, $2 = 2^m$ and so $m = 1$.

Let $k \in \mathbb{N}$ with $k \geq 2$ such that for all $2 \leq n \leq k$, the conclusion holds. Take $n = k + 1$, and we want to show that the conclusion also holds. We will take two cases.

(1) Assume that $k + 1$ is prime, then we are done...same argument as the base case.
(2) Assume that $k + 1$ is not prime, i.e. $k + 1$ is composite. By the Proposition 1.7, there exists $a, b \in \mathbb{Z}$ such that $k + 1 = ab$ and $2 \leq a, b \leq k$, by the inductive hypothesis, there exists $p_1^{(a)}, p_2^{(a)}, ..., p_s^{(a)}$ and $q_1^{(b)}, q_2^{(b)}, ..., q_t^{(b)}$ such that $a = p_1^{(a)} \cdots p_s^{(a)}$ and $b = q_1^{(b)} \cdots q_t^{(b)}$ (and they are all prime), therefore $k + 1 = ab = p_1^{(a)} \cdots p_s^{(a)} \cdot q_1^{(b)} \cdots q_t^{(b)}$. By relabelling, there are prime numbers $p_1 \leq \cdots \leq p_\ell$ such that $k + 1 = p_1 \cdots p_\ell$.

To prove the uniqueness, take prime numbers $q_1 \leq q_2 \leq \cdots \leq q_m$ such that $k + 1 = q_1 \cdots q_m$. We prove that $\ell = m$ and for each $1 \leq i \leq \ell = m$, $p_i = q_i$. Since $q_1 \mid k + 1 = p_1 \cdots p_\ell$, there exists $1 \leq i \leq \ell$ such that $q_1 \mid p_i$ and therefore $q_1 = p_i$. So now, we have $p_1 = q_j \geq q_1 = p_i \geq p_1$, i.e. they are equal or $p_1 = q_1$. Now, $k + 1 = p_1 \cdots p_\ell = q_1 \cdots q_m$, and therefore, by left cancellation,

$$p_2 \cdots p_\ell = q_2 \cdots q_m$$

Now take $c = p_2 \cdots p_\ell$, then $2 \leq c < k+1$, and so $c = p_2 \cdots p_\ell = q_2 \cdots q_m$. By the inductive hypothesis, both ways are equivalent, i.e. length is the same $\ell = m$, and $p_2 = q_2$,..., $p_\ell = q_\ell$, as desired.

□

Week 3

September 18-23

LECTURE 6

September 18, 2023

1. Groups: Binary Operations on a Set

DEFINITION 1.1. Let X be a set. A binary operation on X is a function $* : X \times X \to X$. Informally, it is a rule that assigns to every pair $(a, b) \in X \times X$ another member of X, usually denoted $a * b$.

EXAMPLE 1.2. On $\mathbb{Z}$, "$+$" and "$\cdot$" are binary operations.

EXAMPLE 1.3. For $\mathbb{N}$, denote $\mathcal{M}_n(\mathbb{R})$ to be the set of all $n \times n$ matrices with real entries. Then "$+$" and "$\cdot$" (matrix multiplication) are binary operations on $\mathcal{M}_n(\mathbb{R})$. If $A, B \in \mathcal{M}_n(\mathbb{R})$, then sometimes $A \cdot B \neq B \cdot A$, hence why the order matters.

EXAMPLE 1.4. On $\mathbb{R}^n$, with $n \geq 2$, then "$+$" is a binary operation on $\mathbb{R}^n$.

EXAMPLE 1.5. However, "$\langle \cdot, \cdot \rangle$" is not a binary operation on $\mathbb{R}^n$ because for $x, y \in \mathbb{R}^n$, $\langle x, y \rangle \notin \mathbb{R}^n$.

EXAMPLE 1.6. On $\mathbb{N}$, define $m * n = \frac{m}{n}$ is not a binary operation on $\mathbb{N}$ since sometimes $\frac{m}{n} \notin \mathbb{N}$.

EXAMPLE 1.7. On $\mathbb{Q}$, $a * b = \frac{a}{b}$, is also not a binary operation on $\mathbb{Q}$ since sometimes it is not defined.

2. Integers Modulo n

NOTATION 2.1. For $n \in \mathbb{N}$, denote $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$. Therefore, if $a \in \mathbb{Z}_n$, then $a \in \mathbb{Z}$ and $0 \leq a < n$.

REMARK 2.2. Usual addition and multiplication are *not* binary operations on $\mathbb{Z}_n$. For example, define $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Then take $3, 4 \in \mathbb{Z}_5$ and define the operation "$+$". Then $3+4 = 7$, so it is not a binary operation since $7 \notin \mathbb{Z}_5$.

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then there exists a unique $r \in \mathbb{Z}_n$ such that $a \equiv r \pmod{n}$. In particular, r is the remainder of a divided by n.

DEFINITION 2.3. Let $n \in \mathbb{N}$. For $a, b \in \mathbb{Z}_n$, define the following:

(1) $a +_n b$ as the unique $r \in \mathbb{Z}_n$ such that $a + b \equiv r \pmod{n}$. This means $a +_n b \in \mathbb{Z}_n$ and $a + b \equiv a +_n b \pmod{n}$.

(2) $a \cdot_n b$ as the unique $s \in \mathbb{Z}_n$ such that $a \cdot b \equiv s \pmod{n}$. This means $a \cdot_n b \in \mathbb{Z}_n$ and $a \cdot b \equiv a \cdot_n b \pmod{n}$.

EXAMPLE 2.4. Take $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Take $3, 4 \in \mathbb{Z}_5$, $3 +_5 4 = 2$ because $3 + 4 = 7 \equiv 2 \pmod{5}$ and $2 \in \mathbb{Z}_5$. Similarly, take $2, 3 \in \mathbb{Z}_5$, then $2 \cdot_5 3 = 1$ since $2 \cdot 3 = 6 \equiv 1 \pmod{5}$ and $1 \in \mathbb{Z}_5$.

PROPOSITION 2.5. *Let $n \in \mathbb{N}$. Then the following hold for $a, b \in \mathbb{Z}_n$:*

(1) *$a +_n b = b +_n a$ and $a \cdot_n b = b \cdot_n a$ (commutativity of "$+_n$" and "$\cdot_n$")*
(2) *$(a +_n b) +_n c = a +_n (b +_n c)$ and $(a \cdot_n b) \cdot_n c = a \cdot_n (b \cdot_n c)$. (associativity of $+_n$ and $\cdot_n$)*
(3) *There exists an additive identity and multiplicative identity $0 \in \mathbb{Z}_n$ and $1 \in \mathbb{Z}_n$, respectively, such that $a +_n 0 = a$ and $a \cdot_n 1 = a$, respectively.*
(4) *$a \cdot_n (b +_n c) = a \cdot_n b + a \cdot_n c$ (distributive property)*
(5) *There exists $a\ b \in \mathbb{Z}_n$ such that $a +_n b = 0$*
(6) *For $b \in \mathbb{Z}_n$, the following are equivalent:*
    (a) *There exists $k \in \mathbb{Z}_n$ such that $b \cdot_n k = 1$*
    (b) $\gcd(n, b) = 1$.

PROOF. We will prove (2) and (6). Let $a, b, c \in \mathbb{Z}_n$ be arbitrary and write $a+b \equiv a+_n b \pmod{n}$ (this is a defining property) Write $a+b+c \equiv (a+_n b)+c \pmod{n}$. Similarly, $b + c \equiv b +_n c \pmod{n}$ and add a to both sides of this equation so that $a + b + c \equiv a + (b +_n c) \pmod{n}$. Thus, $(a +_n b) + c \equiv (a+_n b)+_n c \equiv a+b+c \pmod{n}$. Similarly,$a+(b+_n c) \equiv a+_n(b+_n c) \equiv a+b+c \pmod{n}$, and therefore, $(a +_n b) +_n c \equiv a +_n (b +_n c) \pmod{n}$. Since both sides are in $\mathbb{Z}_n$, they are equal.

To show that (6) is true, we show that (a) $\Rightarrow$ (b). Let $b, k \in \mathbb{Z}_b$ such that $b \cdot_n k = 1$. We will show that $\gcd(n, b) = 1$. Indeed, $1 = b_n k \equiv bk \pmod{n}$, which meas that $bk \equiv 1 \pmod{n}$. By definition $n \mid bk - 1$. Then by definition, there exists a $m \in \mathbb{N}$ such that $bk - 1 = mn$ and so $bk - mn = 1$. Since $d = \gcd(n, b)$ divides both n and b, it will also divide any linear combination of n and b, i.e. $bk - mn = 1$. But then, $d = \gcd(n, b) = 1$. Now show that (b) $\Rightarrow$ (a). Assume that $\gcd(n, b) = 1$. By Bezout's Theorem, there exists $x, y \in \mathbb{Z}$ such that $xb + yn = 1$. In other words, $xb - 1 = -yn$, which implies that $x \cdot b \equiv 1 \pmod{n}$. Take $k \in \mathbb{Z}_n$ such that $x \equiv k \pmod{n}$. Then we claim that $b \cdot_n k = 1$. Indeed, $b \cdot_n k \equiv b \cdot k \equiv b \cdot x \equiv 1 \pmod{n}$ and so $b \cdot_n k = 1$, as desired. □

3. Multiplication and Addition Tables of $\mathbb{Z}_4$

Let us consider $\mathbb{Z}_4$ given below for operations $+_n$ and $\cdot_n$.

$\cdot_n$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$+_n$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2