# Math 135 Notes

Thomas Liu

December 21, 2022

# Contents

# 1 Chapter 1 Introduction to the Language of Mathematics

## 1.1 Introducing Sets

Definition: a set is a well-defined unordered collection of distinct elements.
can write down a set by listing its member
Example:

- $\{\pi, *, 7, \&, \%\} = \{\&, \%, \pi, *, 7\}$
- $\{\pi, 7, \pi\}$ is not a set
- $\{\pi, \{*, \pi\}\}$ is a set with 2 elements
- $* \in \{\pi, *, 7\}$
- $135 \notin \{\pi, *, 7\}$
- $\{\} = \emptyset$
- $\emptyset \neq \{\emptyset\}$
- $\emptyset \notin \emptyset$
- $\{7\} \notin \{\pi, 7, *\}$

## 1.2 Familar Sets

$\mathbb{Z}$ is a set of integer
$\mathbb{N}$ is a set of natural number
$\mathbb{Q}$ is a set of rational number ($\frac{p}{q}$, $p$ and $q$ are integers and $q$ is not zero)
$\mathbb{R}$ is a set of real number

## 1.3 Statement

Definition: a statement is a sentence that is true or false
An open sentence is a sentence that becomes a statement if values are assigned to all variables in sentence

### 1.4 Negation

Suppose $P$ is statement
The negation of $P$ is statement $\neg P$ which is true when $P$ is false and false when $P$ is true. $P$ and $\neg(\neg P)$ always have the same truth value

### 1.5 Universally Quantified Statements

$\forall x \in \mathbb{N}$, $x^2 - x \geq 0$
$\forall$ is quantifier/for all, $x$ is variable, $\mathbb{N}$ is domain, $x^2 - x \geq 0$ is open sentence

### 1.6 Existential Statements

$\exists x \in S$, $P(x)$
Example: $\exists x \in \mathbb{Z}$, $\dfrac{x-7}{2x+4} = 5$
$\exists$ is there exists

- $\forall$ is true for all $x$
- $\forall$ is false at least one $x$
- $\exists$ is true at least one $x$
- $\exists$ is false for all $x$

### 1.7 Negating Quantifiers

$\neg(\forall x \in S, P(x)) = \exists x \in S, (\neg P(x))$
$\neg(\exists x \in S, P(x)) = \forall x \in S, (\neg P(x))$

## 2 Chapter 2 Logical Analysis of Mathematical Statements

### 2.1 Logic

Given a statement (variable), we can build more complex logical expressions using logical operators
The truth value of logical expression can be defined using truth table

| A | $\neg A$ |
|---|---|
| T | F |
| F | T |

## 2.2 And

The definition of $A$ and $B$, $A \wedge B$ is

| A | B | $A \wedge B$ |
|---|---|---|
| T | T | T |
| F | T | F |
| T | F | F |
| F | F | F |

$A \wedge B$ is only true when both $A$ and $B$ are true

## 2.3 Or

The definition of $A$ or $B$, $A \vee B$ is

| A | B | $A \vee B$ |
|---|---|---|
| T | T | T |
| F | T | T |
| T | F | T |
| F | F | F |

$A \vee B$ is only false when both $A$ and $B$ are false

## 2.4 Logical Equivalence

Two logical expression are logically equivalent if they have the same truth value of all choices of values for their opponent statement variables. Their truth value match in a truth table

## 2.5 De Morgan's Rule

$\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$
$\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$
$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$

## 2.6 Implication

An implication is a sentence of the form "If $H$ then $C$" or $H \Rightarrow C$

- logically equivalent to $(\neg H) \vee C$
- $H$ is hypothesis, $C$ is conclusion

| H | C | $H \Rightarrow C$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

## 2.7 Negation of Implication

The negation of $H \Rightarrow C$ is logically equivalent to $H \wedge (\neg C)$
$\neg(H \Rightarrow C) \equiv \neg((\neg H) \vee C) \equiv (\neg(\neg H)) \wedge (\neg C) \equiv H \wedge (\neg C)$

## 2.8 Contrapositive

- Contrapositive of $A \Rightarrow B$ is implication $\neg B \Rightarrow \neg A$
- They are logically equivalent

## 2.9 Converse

- Converse of $A \Rightarrow B$ is implication $B \Rightarrow A$
- not logically equivalent

## 2.10 If and Only If

$\Longleftrightarrow$ read as "if and only if" / iff

| A | B | $A \Longleftrightarrow B$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | T |

# 3 Chapter 3 Prove Mathematical Statements

## 3.1 Statement

Example: For all real $x, y \in \mathbb{R}$, $x^4 + x^2y + y^2 \geq 5x^2y - 3y^2$

## 3.2 Divisibility

Definition: an integer $m$ divides an integer $n$ if there exists an integer $k$ so that $n = km$, write $m \mid n$

## 3.3 Transitivity of Divisibility (TD)

For $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$

## 3.4 Divisibility of Integer Combinations (DIC)

For all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for all $x, y \in \mathbb{Z}$

## 3.5 Proposition 8

For $a, b, c \in \mathbb{Z}$, if $a \mid b$ or $a \mid c$, then $a \mid bc$

### 3.5.1 Proof by Contradiction

We prove that a statement $P$ is true by

- assume $\neg P$ is true, then based on assumption
- prove both $Q$ and $\neg Q$ to prove statement $B$

## 3.6 Uniqueness

Two approaches
we can prove that there is a unique value satisfying some property by showing such a value exists and then

- assume it is satisfied by $x$ and $y$ and showing $x = y$
- use by contradiction

# 4 Chapter 4 Mathematical Induction

## 4.1 Principle of Mathematical Induction (POMI)

Let $P(n)$ is a statement that depends on $n \in \mathbb{N}$
If statements 1 and 2 are both true

1. $P(1)$ is true
2. For all $k \in \mathbb{N}$, if $P(k)$, then $P(k+1)$
3. Then, for all $n \in \mathbb{N}$, $P(n)$

## 4.2 Binomial Coefficients

For non-negative integers $n$ and $m$, we define:

- $\binom{n}{m} = \dfrac{m!}{(n-m)!m!}$ when $m \leq n$
- $\binom{n}{m} = 0$ when $m > n$

## 4.3 Pascal's Identity (PI)

For all positive integers $n$ and $m$ with $m < n$, we have
$\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m}$

## 4.4 The Binomial Theorem

## 4.5 Binomial Theorem Version 1 (BT1)

For all integer $n \geq 0$ and $x \in \mathbb{R}$

$$(1+x)^n = \sum_{m=0}^{n} \binom{n}{m} x^m$$

## 4.6 Binomial Theorem Version 2 (BT2)

For all integer $n \geq 0$ and $a, b \in \mathbb{R}$

$$(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} a^{n-m} b^m$$

### 4.7 Principle of Strong Induction (POSI)

Let $P(n)$ be a statement that depends on $n \in \mathbb{N}$, if

1. $P(1)$ is true
2. $\forall k \in \mathbb{N}$, $[(P(1) \wedge P(2) \wedge \cdots P(k)) \Rightarrow P(k+1)]$
   then $P(n)$ is true for all $n \in \mathbb{N}$

## 5 Chapter 5 Set

$\{x \in U : P(x)\}$
$\{f(x) : P(x)\}$
$\{f(x) : x \in U, P(x)\}$

### 5.1 Set-difference

The set-difference of two sets $S$ and $T$, written $S - T$ or $S \setminus T$ is the set of all elements belonging to $S$ but not $T$

### 5.2 Set Complement

The complement of a $S$, written $\overline{S}$, is the set of all elements in $U$ but not in $S$, $\overline{S} = U - S$

### 5.3 Subset

If $S$ and $T$ are sets, we say $S$ is a subset of $T$, write $S \subseteq T$ if every element of $S$ is an element of $T$

## 6 Chapter 6 The Greatest Common Divisor

### 6.1 Bounds by Divisibility (BBD)

For all $a, b \in \mathbb{Z}$, if $b \mid a$ and $a \neq 0$, then $b \leq |a|$

## 6.2 Division Algorithm (DA)

For all $a \in \mathbb{Z}$ and for all $b \in \mathbb{N}$
There exists unique integers $q$ and $r$ such that $a = bq + r$ where $0 \leq r < b$

## 6.3 GCD Formal Definition

Let $a, b \in \mathbb{Z}$
When $a$ and $b$ are not both zero, we say an integer $d > 0$ is the Greatest Common Divisor of $a$ and $b$, and writes $\gcd(a, b)$ iff

- $d \mid a$, $d \mid b$, and
- for all integers $c$, if $c \mid a$ and $c \mid b$ then $c \leq d$

Fact:
For all $a, b \in \mathbb{Z}$, $\gcd(3a + b, a) = \gcd(a, b)$

## 6.4 GCD with Remainders (GCDWR)

For all $a, b, q, r \in \mathbb{Z}$, if $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$

## 6.5 Euclidean Algorithm (EA)

Process to compute $\gcd(a, b)$ for $a, b \in \mathbb{N}$

## 6.6 GCD Characterization Theorem (GCDCT)

For $a, b, d \in \mathbb{Z}$ where $d \geq 0$
If $d \mid a$ and $d \mid b$ and there exists $s, t \in \mathbb{Z}$ such that $as + bt = d$, then $d = \gcd(a, b)$

## 6.7 Bézout's Lemma (BL)

For all $a, b \in \mathbb{Z}$, there exists $s, t \in \mathbb{Z}$ such that $as + bt = \gcd(a, b)$

## 6.8 Extended Euclidean Algorithm (EEA)

## 6.9 Common Divisor Divides GCD (CDD GCD)

For all integers $a, b, c$, if $c \mid a$ and $c \mid b$, then $c \mid \gcd(a, b)$

## 6.10 Coprimeness Characterization Theorem (CCT)

For all integers $a$ and $b$, $\gcd(a, b) = 1$ if and only if there exist integers $s$ and $t$ such that $as + bt = 1$

## 6.11 Division by the GCD (DB GCD)

For all integers $a$ and $b$, not both zero, $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, where $d = \gcd(a, b)$

## 6.12 Coprimeness and Divisibility (CAD)

For all integers $a, b, c$, if $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$

## 6.13 Prime Factorization (PF)

Every integer greater than 1 can be written as the product of primes

## 6.14 Euclid Theorem (ET)

There are infinitely many primes

## 6.15 Euclid Lemma (EL)

For all $a, b \in \mathbb{Z}$ and prime $p$, if $p \mid ab$, then $p \mid a$ or $p \mid b$

## 6.16 Divisors From Prime Factorization (DFPF)

Let $n > 1$ be an integer and let $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$ where $p$ are prime and $\alpha$ are positive integers. A positive integer $c$ divides $n$ iff there exists integers $\beta_1, \beta_2, \cdots, \beta_k$ such that $c = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \cdots p_k^{\beta_k}$ and $0 \leq \beta_i \leq \alpha_i$ for $i = 1, 2, \cdots, k$

## 6.17 GCD From Prime Factorization (GCDPF)

If $a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \cdots p_k^{\beta_k}$ where $p_1, p_2, \cdots, p_k$ are prime, all exponents are integers greater than or equal to 0, then $\gcd(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} p_3^{\gamma_3} \cdots p_k^{\gamma_k}$ where $\gamma_i = min\{\alpha_i, \beta_i\}$ for $i = 1, 2, \cdots, k$

# 7 Chapter 7 Linear Diophantine Equations

Given $a, b, c \in \mathbb{Z}$, find $x, y \in \mathbb{Z}$ such that $ax + by = c$

- Is there a solution? (LDET1)
- If so, how can we find one? (EEA)
- And can we find all solutions? (LDET2)

## 7.1 LDET1

Let $a, b \in \mathbb{Z}$, both not zero and $d = \gcd(a, b)$. Then LDE $ax + by = c$ has a solution iff $d \mid c$

## 7.2 LDET2

Let $\gcd(a, b) = d$ where $a, b \neq 0$
If $(x, y) = (x_0, y_0)$ is one particular integer solution to the LDE $ax + by = c$, then the complete integer solution is

$$\{(x_0 + \frac{b}{d}n, y_0 - \frac{a}{d}n) : n \in \mathbb{Z}\}$$

# 8 Chapter 8 Congruence and Modular Arithmetic

Congruence: -1 is congruent to 7 modulo 8

## 8.1 Definition

Let $a, b \in \mathbb{Z}$, let $m \in \mathbb{N}$
We say a is congruent to b modulo m when $m \mid (a-b)$, write $a \equiv b \pmod{m}$.
Otherwise we write $a \not\equiv b \pmod{m}$
Note: let $a, b \in \mathbb{Z}$, let $m \in \mathbb{N}$

## 8.2 Congruence is an Equivalent Relations (CER)

For $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$

1. $a \equiv b \pmod{m}$
2. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
3. $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

## 8.3 Congruence Add and Multiply (CAM)

For $n \in \mathbb{Z}^+$, for all integers $a_1, a_2, ..., a_n$ and $b_1, b_2, ..., b_n$, if $a_i \equiv b_i \pmod{m}$ for all $1 \leq i \leq n$ then

1. $a_1 + ... + a_n \equiv b_1 + ... + b_n \pmod{m}$
2. $a_1 a_2 ... a_n \equiv b_1 b_2 ... b_n \pmod{m}$

## 8.4 Congruence Power (CP)

For all positive integer $n$ and $a, b, c \in \mathbb{Z}$
If $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$

## 8.5 Congruence Division (CD)

Let $a, b, c \in \mathbb{Z}$, let $m \in \mathbb{N}$
If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$

## 8.6 Congruent Iff Same Remainder (CISR) and Congruent To Remainder (CTR)

$\forall a, b \in \mathbb{Z}$, $m \in \mathbb{N}$
CISR: $a \equiv b \pmod{m}$ or $a$ and $b$ have the same remainder when divides $m$
CTR: $0 \leq b < m$, $a \equiv b \pmod{m}$ iff $a$ has remainder $b$ when divided by $m$

## 8.7 Linear Congruence

Let $m \in \mathbb{Z}$
Let $a, c \in \mathbb{Z}$ where $a \neq 0$
Find all $a \in \mathbb{Z}$ such that $ax \equiv c \pmod{m}$

- Is there a solution?
- If so, can we find one?
- If so, can we find all?

## 8.8 Linear Congruence Theorem (LCT)

For all integers $a$ and $c$ with $a$ non-zero, the linear congruence $ax \equiv c \pmod{m}$ has a solution iff $d \mid c$ where $\gcd(a, m) = d$
Moreover, if $x = x_0$ is a particular solution, then the complete solution is $\{x \in \mathbb{Z} : x \equiv x_0 \pmod{\frac{m}{d}}\}$
or equivalently: $\{x \in \mathbb{Z} : x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, ..., x_0 + (d-1)\frac{m}{d} \pmod{m}\}$
Informally, LCT tells us there is

- one solution modulo $\frac{m}{d}$
- $d$ solutions modulo $m$

## 8.9 Congruence Class Definition

Let $m \in \mathbb{N}$, let $a \in \mathbb{Z}$
The congruence class of $a$ modulo $m$ is $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}$ The congruence modulo $m$ is $\mathbb{Z}_m = \{[0], [1], [2], ..., [m-1]\}$ or $= \{[x] : x \in \mathbb{Z}\}$
$|\mathbb{Z}_m| = m$

## 8.10 Operations

Let $m \in \mathbb{N}$, let $a, b \in \mathbb{Z}$ We define

- $[a] + [b] = [a + b]$
- $[a][b] = [ab]$

## 8.11 Different ways of saying the same thing

Let $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$

- $a \equiv b \pmod{m}$
- $m \mid (a - b)$
- $\exists k \in \mathbb{Z}, a - b = km$
- $\exists k \in \mathbb{Z}, a = km + b$
- $a$ and $b$ have the same remainder when divided by $m$
- $[a] = [b]$ in $\mathbb{Z}_m$

## 8.12 Identities and Inverses in $\mathbb{Z}_m$

Let $[a] \in \mathbb{Z}_m$

- $[0]$ is the additive identity because $[a] + [0] = [a]$
- $[1]$ is the multiplicative identity because $[a][1] = [1][a] = [a]$
- $[-a]$ is the additive inverse of $[a]$ because $[a] + [-a] = 0$
- The multiplicative inverse of $[a]$ (if it exists) is an element $[b]$ such that $[a][b] = [b][a] = [1]$ and we write $[b] = [a]^{-1}$

## 8.13 Modular Arithmetic Theorem (MAT)

Let $\gcd(a, m) = d \neq 0$
The equation $[a][x] = [c]$ in $\mathbb{Z}_m$ has a solution iff $d \mid c$. Moreover, if $[x] = [x_0]$ is one particular solution, the complete solution is
$\{[x_0], [x_0 + \frac{m}{d}], [x_0 + 2\frac{m}{d}], ..., [x_0 + (d-1)\frac{m}{d}]\}$

## 8.14 Multiplicative Inverses

Inverses in $\mathbb{Z}_m$ (INV $\mathbb{Z}_m$)
Let $a \in \mathbb{Z}$ with $0 \leq a \leq m-1$. Then element $[a] \in \mathbb{Z}_m$ has a multiplicative inverse iff $\gcd(a, m) = 1$. Moreover, when $\gcd(a, m) = 1$, the multiplicative inverse is unique inverses in $\mathbb{Z}_q$ (INV $\mathbb{Z}_q$)
For all primes numbers $p$ and non-zero elements $[a] \in \mathbb{Z}_q$ has a unique multiplicative inverse

## 8.15 Fermat's Little Theorem (F$\ell$T)

Let $p$ be prime. Let $a \in \mathbb{Z}$. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$

## 8.16 Corollary to F$\ell$T

Let $p$ be prime, let $a \in \mathbb{Z}$
Then $a^p \equiv a \pmod p$

## 8.17 Chinese Remainder Theorem (CRT)

Suppose $\gcd(m_1, m_2) = 1$ and $a_1, a_2 \in \mathbb{Z}$
There is a unique solution modulo $m_1 m_2$ to the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

That is, once we have one solution $x = x_0$, CRT also tells us that the full solution is $x \equiv x_0 \pmod{m_1 m_2}$

## 8.18 General CRT (GCRT)

If $m_1, m_2, ..., m_k \in \mathbb{N}$ and $\gcd(m_i, m_j) = 1$ whenever $i \neq j$, then for any choice of integers $a_1, a_2, ..., a_k$, there exists solution to simultaneous congruences

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \\ &\cdots \\ n &\equiv a_k \pmod{m_k} \end{aligned}$$

Moreover, if $n = n_0$ is one integer solution, then the complete solution is $n \equiv n_0 \pmod{m_1 m_2 ... m_k}$

### 8.19 Splitting the Modulus Theorem (SMT)

Let $m_1, m_2$ be coprime positive integers, then for any two integers $x$ and $a$

$$x \equiv a \pmod{m_1 m_2} \Longleftrightarrow \begin{cases} x \equiv a \pmod{m_1} \\ x \equiv a \pmod{m_2} \end{cases}$$

# 9 Chapter 9 The RSA Public-Key Encryption Scheme

For all integers $p, q, n, e, d, M, CandR$, if

1. $p$ and $q$ are distinct primes
2. $n = pq$
3. $e$ and $d$ are positive integers such that $ed \equiv 1 \pmod{(p-1)(q-1)}$ and $1 < e,\, d < (p-1)(q-1)$
4. $0 \leq M < n$
5. $M^e \equiv C \pmod{n}$ where $0 \leq C < n$
6. $C^d \equiv R \pmod{n}$ where $0 \leq R < n$

then $R = M$

# 10 Chapter 10 Complex Numbers

A complex number in standard form is an expression of form $x + yi$ where $x, y \in \mathbb{R}$. $\mathbb{C} = \{x + yi : x, y\mathbb{R}\}$

## 10.1 Arithmetic

- $(a+bi)+(c+di)=(a+c)+(b+d)i$
- $(a+bi)(c+di)=(ac-bd)+(ad+bc)i$

Informally, we can treat elements of $\mathbb{C}$ as "normal" algebraic expressions where $i^2=-1$ and "everything works"

- 0 is the additive identity and in $\mathbb{C}$
- $-z$ is the additive inverse of $z$ in $\mathbb{C}$
- 1 is the multiplicative identity in $\mathbb{C}$
- $\dfrac{a-bi}{a^2+b^2}$ is the unique multiplicative inverse $a+bi\neq 0$

## 10.2 Properties of Complex Arithmetic (PCA)

Let $u,v,z\in\mathbb{C}$ with $z=x+yi$

1. $(u+v)+z=u+(v+z)$
2. $u+v=v+u$
3. $z+0=z$ where $0+0i=0$
4. $z+(-z)=0$ where $-z=-x-yi$
5. $(uv)w=u(vw)$
6. $uv=vu$
7. $z\cdot 1=z$ where $1=1+0i$
8. $z\neq 0\Rightarrow zz^{-1}=1$ where $z^{-1}=\dfrac{x-yi}{x^2+y^2}$
9. $z(u+v)=zu+zv$

## 10.3 More about Complex Numbers

- For $z \in \mathbb{C}$, we define $z^0 = 1$, $z^1 = z$, and $z^{k+1} = zz^k$ for $k \in \mathbb{N}$
- For $z \in \mathbb{C}$, we define $z^{-k} = (z^k)^{-1}$ for $k \in \mathbb{N}$
- Exponent laws with integer exponents hold for complex numbers
- The Binomial Theorem (BT) is true when $a, b \in \mathbb{C}$
- The complex numbers connot be put ”in order”
  - $z < w$ and $z \leq w$ do not mean anything for $z, w \in \mathbb{C}$
- Let $r \in \mathbb{R}$ where $r > 0$
  - $(\sqrt{r}i)^2 = (0 + \sqrt{r}i) \cdot (0 + \sqrt{r}i) = -r$

## 10.4 Complex Conjugate

Let $z = a + bi$ be a complex number in standard form
The complex conjugate of $z$ is $\overline{z} = a - bi$

## 10.5 Properties of Complex Conjugates (PCJ)

Let $z, w \in \mathbb{C}$. Then

1. $\overline{(\overline{z})} = z$
2. $\overline{z + w} = \overline{z} + \overline{w}$
3. $z + \overline{z} = 2Re(z)$ and $z - \overline{z} = 2Im(z)i$
4. $\overline{zw} = \overline{z}\,\overline{w}$
5. $z \neq 0 \Rightarrow \overline{z^{-1}} = (\overline{z})^{-1}$

## 10.6 Modulus

Let $z = x + yi \in \mathbb{C}$. The modulus of $z$ is $|x + yi| = \sqrt{x^2 + y^2}$

## 10.7 Properties Modulus (PM)

1. $|z| = 0$ iff $z = 0$
2. $|\overline{z}| = |z|$
3. $z\overline{z} = |z|^2$
4. $|zw| = |z||w|$
5. If $z \neq 0$, then $|z^{-1}| = |z|^{-1}$

## 10.8 Corollary 6

For all positive integers $n$ and complex number $z_1, z_2, \cdots, z_n$, we have

1. $\overline{z_1 + z_2 + \cdots + z_n} = \overline{z_1} + \overline{z_2} + \cdots + \overline{z_n}$
2. $\overline{z_1 z_2 \cdots z_n} = \overline{z_1 z_2} \cdots \overline{z_n}$
3. $|z_1 z_2 \cdots z_n| = |z_1||z_2| \cdots |z_n|$

## 10.9 Triangle Inequality (TIQ)

For all $z, w \in \mathbb{C}$, we have $|z + w| \leq |z| + |w|$

## 10.10 Complex Plane

$\overline{z}$ is the reflection of $z$ in the real axis
$|z|$ is the distance from $z$ to the origin
$z + w$ is connected to vector addition
Definition:
The polar form of a complex number $z$ is $z = r(\cos\theta + i\sin\theta)$
$r = |z|$ and $\theta$ is an angle measured counter-clockwise from the positive real axis

## 10.11 Polar Multiplication of Complex Number (PM$\mathbb{C}$)

For all complex number $z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$, $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$

$$z_1 z_2 = r_1 r_2(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2))$$

### 10.12 De Moivre's Theorem (DMT)

For all $n \in \mathbb{Z}$, and $\theta \in \mathbb{R}$

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

### 10.13 Collary to DMT

For all $n \in \mathbb{Z}$, complex number $z = r(\cos\theta + \sin\theta) \neq 0$

$$z^n = r^n(\cos(n\theta) + i\sin(n\theta))$$

### 10.14 Complex n-th Roots Theorem (CNRT)

Let $n \in \mathbb{N}$, if $r(\cos\theta + i\sin\theta)$ is the polar form of a complex number $a$, then the solutions to $z^n = a$ are

$$\sqrt[n]{r}(\cos(\frac{\theta + 2k\pi}{n}) + i\sin(\frac{\theta + 2k\pi}{n}))\text{for}k = 0, 1, 2, \cdots, n-1$$

## 11 Chapter 11 Polynomials

For all $a, b, c \in \mathbb{C}$ with $a \neq 0$, the solution to $ax^2 + bx + c = 0$ are $\dfrac{-b \pm w}{2a}$ where $w^2 = b^2 - 4ac$

### 11.1 Field

Definition:
In this course, the only examples of a field we will encounter are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ (and in notes noly, $\mathbb{Z}_p$ where $p$ is prime)

- all non-zero numbers have a multiplicative inverse
- $ab = 0$ iff $a = 0$ or $b = 0$

## 11.2 Polynomial Definition

Let $n \in \mathbb{Z}$, $n \geq 0$ and $a_n, a_{n-1}, \cdots, a_1, a_0 \in \mathbb{F}$ where $\mathbb{F}$ is a field An expression of form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

is a polynomial in $x$ over $\mathbb{F}$
$iz^3 + (2+3i)z + \pi$

- $(2+3i)$ - coefficients
- $iz^3$ - term
- $z$ - indeterminate
- complex polynomial
- degree is 3
- cubic polynomial
- in $\mathbb{C}[z]$

## 11.3 Arithmetic with Polynomials

Let $f(x) = \sum_{i=0}^{m} a_i x^i$ and $g(x) = \sum_{j=0}^{n} b_j x^j$ be the polynomials in $\mathbb{F}[x]$

- **Addition** of $f(x)$ and $g(x)$ is defined as

  $$f(x) + g(x) = \sum_{k=0}^{max\{m,n\}} (a_k + b_k)x^k$$

  where $a_k = 0$ for $k > m$, and $b_k = 0$ for $k > n$

- **Multiplication** of $f(x)$ and $g(x)$ is defined as

  $$f(x)g(x) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j x^{i+j} = \sum_{\ell=0}^{m+n} c_\ell x^\ell$$

where

$$c_\ell = a_0 b_\ell + a_1 b_{\ell-1} + \cdots + a_{\ell-1} b_1 + a_\ell b_0 = \sum_{i=0}^{\ell} a_i b_{\ell-i}$$

for $\ell = 0, 1, \cdots, m+n$ and where again $a_k = 0$ for $k > m$, and $b_k = 0$ for $k > n$

## 11.4 Degree of a Product (DP)

For all fields $\mathbb{F}$, and all non-zero polynomials $f(x)$ and $g(x)$ in $\mathbb{F}[x]$, we have

$$\deg f(x)g(x) = \deg f(x) + \deg g(x)$$

## 11.5 Division Algorithm for Polynomials (DAP)

For all fields $\mathbb{F}$, and all polynomials $f(x)$ and $g(x)$ in $\mathbb{F}[x]$ with $g(x)$ not the zero polynomial, there exist unique polynomial $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

where $r(x)$ is the zero polynomial, or deg $r(x) <$ deg $g(x)$

## 11.6 Remainder Theorem (RT)

Suppose $f(x) \in \mathbb{F}[x]$ and $c \in \mathbb{F}$. The remainder when $f(x)$ is divided by $x-c$ is the constant polynomial $f(c)$

## 11.7 Factor Theorem (FT)

Suppose $f(x)$ and $x-c$ are in $\mathbb{F}[x]$ and $c \in \mathbb{F}$
Then $x-c$ is a factor of $f(x)$ if and only if $f(c) = 0$
Equivalently, $x-c$ is a factor $f(x)$ iff c is a root of $f(x)$

## 11.8 Fundamental Theorem of Algebra (FTA)

Every complex polynomial of positive degree has a complex root

## 11.9 Complex Polynomials of Degree n Have n Roots (CPN)

If $f(x)$ is a complex polynomial of degree $n \geq 1$, then there exist complex numbers $c_1, c_2, \cdots, c_n$ and $c \neq 0$ such that

$$f(z) = c(z - c_1)(z - c_2) \cdots (z - c_n)$$

Moreover, the roots of $f(z)$ are $c_1, c_2, \cdots, c_n$

## 11.10 Proposition 7

Let $f(x) \in \mathbb{F}[x]$ where $\mathbb{F}$ is a field
Let $n$ be the degree of $f(x)$
The number of roots of $f(x)$ is at most $n$

## 11.11 Multiplicity

The multiplicity of a root of $c$ of a polynomial $f(x)$ is the largest positive integer $k$ such that $(x - c)^k$ is a factor of $f(x)$

## 11.12 Reducible and Irreducible Polynomial

A polynomial in $\mathbb{F}[x]$ of positive degree is a reducible polynomial in $\mathbb{F}[x]$ when it can be written as the product of two polynomials in $\mathbb{F}[x]$ of positive degree. Otherwise, we say that the polynomial is an irreducible polynomial in $\mathbb{F}[x]$

## 11.13 Conjugate Roots Theorem (CJRT)

Let $f(x)$ be a polynomial with real coefficients. If $z \in \mathbb{C}$ and $f(z) = 0$, then $f(\overline{z}) = 0$

## 11.14 Real Quadratic Factors (RQF)

Let $f(x) \in \mathbb{R}[x]$. If $f(c) = 0$ for some $c \in \mathbb{C}$ with $lm(c) \neq 0$, then there exists a real quadratic irreducible polynomial $g(x)$ and a real polynomial $q(x)$ such that $f(x) = g(x)q(x)$

## 11.15 Real Factors of Real Polynomials

Every non-constant polynomial with real coefficients can be written as a product of real linear and real quadratic factors.

$$(x - r_1)(x - r_2)\cdots(x - r_k)(x - c_1)(x - \overline{c_1})(x - c_2)(x - \overline{c_2})\cdots(x - c_\ell)(x - \overline{c_\ell})$$

$$\begin{aligned}(x - c_1)(x - \overline{c_1}) &= x^2 - (c_1 + \overline{c_1})x + c_1\overline{c_1} \\ &= x^2 - 2Re(c_1)x + |c_1|^2 \\ &\in \mathbb{R}[x]\end{aligned}$$