EITP20: Secure Systems Engineering — Reference Sheet
Lund University

Karl Hallsby

Last Edited: September 15, 2020

Contents

List of Theorems

1 Threat Analysis

To perform any kind of threat analysis, the system's specification must be considered. The state of the system (new or existing) must also be considered.

- The specification of the system to be analyzed
  - If a completely new system is about to be built, there might not even exist a system specification and it needs to be created.
  - If the analysis is to done on an existing system, the first task is to read existing system specifications, source code and/or make interviews with people familiar with the system.
- The specification must not necessarily be very detailed but can be a high-level description of the system.

Defn 1 (Attack Goal)**.** An *attack goal* is a technology, process, or thing that an attacker would like to gain access to. These are the things we are trying to protect against or mitigate.

1.1 Attack Trees

Defn 2 (Attack Tree)**.** The Schneider *attack tree* method is a straight-forward and step-by-step type of attack analysis. However, it is quite basic, so it might not be the best method to perform this analysis.

The steps involved are:

1. The starting point is a *good* system description.
2. Next, Attack Goals are identified.
3. Attack Goals are then broken down to specific attacks to form a so-called attack tree. Identify different attack vectors for the same Attack Goal with several iterations.
4. Identify dependencies in the Attack Goals.
5. Once the attack tree is created, it is transferred to a table where scores on risks/costs can be added as well as more details.

In a Single Sign-On system (SSO), there any many different points of failure. These will be illustrated with a basic Attack Tree. Some Attack Goals for this system are:

1. Get access to all services provided by all entities in the system
   (a) Get access to all services provided to all users at the ID Provider
   (b) Get access to all services offered through an OIDC Client
   (c) Get access to all services offered at the Hosting Server
2. Get access to all services provided to a single user provided by the ID Provider
3. Get access to all services provided to single user at the OIDC Client
4. Get access to all services provided to a single user at the Hosting Service
5. Get access to all services provided to an OIDC Client at the Hosting Service

Now, we identify dependencies in the various Attack Goals.

- Attack Goal 1 depends on goals 2, 3, 4, and 5 being completed.
- Goal 1.1 depends on goal 2 being completed.
- Goal 1.2 depends on goal 3 being completed.
- Goal 1.3 depends on goals 4 and 5 being completed.
- Goal 5 depends on goal 4 being completed.

We can now break each of the smaller goals down into concrete attack vectors.

1. Access to all services provided to all entities in the system.
   1.1. Access to all services offered by the ID Provider to all users.
      1.1.1. Get KeyCloak admin rights.
         1.1.1.1. Successful phishing attack.
         1.1.1.2. Break administrator authentication.
      1.1.2. Root access on the KeyCloak server.
         1.1.2.1. Utilize an OS vulnerability
         1.1.2.2. Break server isolation (For example, Docker or VMs)
2. Access to all services provided to a single user by the ID Provider
   2.1. Successful end-user password phishing attack.

2.2. Take over the end-user's client device.
   2.2.1. Place malware on the client device.
   2.2.2. Successful network attack on the end-user's client device.
2.3. Break the end-user authentication mechanism.
   2.3.1. Break authentication algorithm. (Difficult, if not impossible)
   2.3.2. Find flaw in authentication protocol.
   2.3.3. Find flaw in authentication algorithm implementation on the client or on the server.

As this "tree" shows, the when accounting for attack vectors, it can become quite large. You should start with the obvious cases, and move onto the les obvious as you go. The most important thing while doing this is you should think like an attacker.

Remark. Depending on the information of the system available, a very detailed attack break-down might be possible or not. The tree can later be complemented when more implementation information is available

Remark. The attack tree is a useful tool, but is not a final or complete solution to a security analysis problem.

1.2 Example Application of Attack Trees

1.3 Microsoft STRIDE Analysis

Defn 3 (STRIDE Analysis)**.** *STRIDE* is an acronym standing for

S Spoofing
T Tampering
R Repudiation
I Information Disclosure
D Denial of Service
E Elevation of Privilege

It is a model to identify computer security threats in software systems or components of a larger software system. It is general enough to analyze any part of a software system.

To perform a STRIDE analysis, it is commonly applied with these steps:

1. Identify the main entities in the system
2. Identify the interactions between/among the main entities.
3. For each entity, perform a STRIDE analysis on the following actions:
   - Processes
   - External Entities
   - Data Flows
   - Data Stores

Remark 3.1 (Incomplete Methodology). Like Attack Trees, STRIDE Analysis is not a complete methodology. It only helps identify typical attacks, but is not a "complete package".

1.3.1 Spoofing

Defn 4 (Spoofing)**.** *Spoofing* is pretending to be something or someone other than yourself. Table 1.1 gives one example, there are several others.

1. Spoofing the identity of an entity across a network. There is not mediating authority that takes reponisibility for telling that something is what it claims to be.
2. Spoofing the identity of an entity, even when there is a mediating authority. For example, a modified `.dll` file is mediated by the operating system to make sure it is the right one. If it's modified, th emediating authority might let it through, even when it has been modified.
3. Pretending to be a specific person, for example, Barack Obama.
4. Pretending to be in a specific role.

1.3.1.1 Spoofing a Process or File on the same Machine If an attacker creates a file before the real process, the process might interpret the file as being good data, and should be trusted. File permissions during a pipe operation, local procedure, etc. can create vulnerabilities.

Spoofing a process or file on a remote machine can work by creating the expected versions, or by pretending to be the expected machine.

Threat	Property Violated	Definition	Typical Victims	Example
Spoofing	Authentication	Pretending to be something or someone other than yourself	Processes, External Entities, People	Falsely claiming to be a police officer.
Tampering	Integrity	Modifying something on disk, on a network, or in memory	Data stores, data flows, processes	Changing spreadsheet, binary contents, database contents, modifying network packets, or the program running.
Repudiation	Non-Repudiation	Claiming that you didn't do something or were not responsible.	Process	Process: "I didn't hit the big red button".
Information Disclosure	Confidentiality	Providing information to someone not authorized to see it	Processes, data stores, data flows	Allow access to file contents/file metadata, network packets, contents of program memory.
Denial of Service	Availability	Deliberately absorbing more resources than needed to provide a service	Processes, data stores, data flows	Program uses all available memory, File fills up disk, too many network connections for real traffic.
Elevation of Privilege	Authorization	Allowing someone to do something they're not authorized to do.	Process	Allow normal user to execute code as administrator. Remote person can run code.

Table 1.1: STRIDE Acronym Definitions

Threat Examples	What the Attacker Does	Notes
Spoofing a process on the same machine	Creates a file before the real process	
	Renaming/Linking	Creating a trojan `su` and altering the `path`
	Renaming something	Naming your process `sshd`
Spoofing a file	Creates a file in the local directory	This can be a library, exeecutable, or config file
	Creates a link and changes it	Change should happen between link being checked and being accessed
	Creates many files in expected directory	Automate file creation to fill the space of files possible
Spoofing a machine	ARP Spoofing	
	IP Spoofing	
	DNS Spoofing	Forward or Reverse
	DNS Compromise	Compromise TLD, registrar, or DNS operator
	IP Redirection	At the switch or router level
Spoofing a person	Sets e-mail display name	
	Takes over a real account	
Spoofing a role	Declares themselves to be that role	Sometimes opening a special account with a relevant name

Table 1.2: Spoofing Threats

1.3.1.2 Spoofing a Machine Depending on what has been spoofed, ARP, DNS, IP, anything else in the networking stack, the attacks can vary. Once the attackers have this setup in place, then they can continue spoofing, or perform a man-in-the-middle attack. They could also steal cryptographic keys.

With a spoofed machine, they can perform phishing attacks to steal information using sites that appear to be valid.

1.3.1.3 Spoofing a Person

Typically, spoofing a person involves having access to the real person's digital account(s), then pretending to be the real person through another account.

1.3.2 Tampering

Defn 5 (Tampering)**.** *Tampering* is modifying something, typically on disk, on a network, or in memory. This can include changing the data in a spreadsheet, changing a binary or config file on dis, modifying a database, etc. On a network, packets can be added, modified, or removed.

Threat Examples	What the Attacker Does	Notes
Tampering with a File	Modifies a file they own and on which you rely	
	Modifies a file you own	
	Modifies a file on a file server you own	
	Modifies a file on their file server	Loads of fun when you include files from remote domains
	Modifies a file on their file server	XML schemas include remote schemas
	Modifies links or redirects	
Tampering with Memory	Modifies your code	Hard to defend against once attacker is running code as same user.
	Modifes data they've supplied to your API	Pass by value, not by reference when crossing a trust boundary
Tampering with a Network	Redirect flow of data to their machine	Often stage 1 of tampering
	Modifies data flowing over entwork	Even easier when the network is wireless (WiFi, 3G, LTE, etc.)
	Enhances spoofing attacks	

Table 1.3: Tampering Threats

1.3.2.1 Tampering with a File

Attackers can create/modify files if they have write permission. If the code you wrote relies on files other things (people or files) wrote, there's a possibility it was written maliciously.

This can commonly happen when a website has been compromised and is serving malicious JavaScript. They can also modify links that the website gives you to be compromised as well. This same link manipulation can happen on your local disk as well.

1.3.2.2 Tampering with Memory

Attacker can modify your code, if they are running at the same or higher privilege level. This is difficult to find and handle, since the bad code is running at the same privilege and under the same user as the good code, and it is near impossible to tell them apart.

If you handle data in a pass-by-reference fashion, the attacker can modify it after security checks have been performed.

1.3.2.3 Tampering with a Network

There are a variety of tricks for this. The attacker can forward some data that is intact and some that is modified.

Other tricks use the radio communication used for wireless data transmission. Software-Defined Radio has made this type of attack trivial.

1.3.3 Repudiation

Defn 6 (Repudiation)**.** *Repudiation* is claiming you didn't do something, or were not responsible for what happened. This can be done honestly or deceptively.

Typically, this is done above any technical layer, and is instead in the business logic of buying products, for example.

Repudiation often deals with logs and logging, which tracks everything that happened in order to find who/what was/is responsible.

Threat Examples	What the Attacker Does	Notes
Repudiating an action	Claims to have not clicked	Maybe they really did
	Claims to have received	Maybe they did, but didn't read. Maybe cached. Maybe pre-fetched.
	Claims to have been a fraud victim	
	Uses someone else's account	
	Uses someone else's payment instrument without authorization	
Attacking the logs	Notices you have no logs	
	Puts attacks in logs to confuse logs, log-reading code, or a person	

Table 1.4: Repudiation Threats

1.3.3.1 Attacking the Logs If there is no logging, we don't retain logs, cannot analyze them, repudiation actions are difficult to dispute. There needs to be log centralization and analysis capabilities. There needs to be a clear definition of what is logged.

1.3.3.2 Repudiating an Action More useful to talk about "someone" than "an attacker" in this context. Since many people who perform some action that may need to have repudiation are usually people that have been failed by technology or a process.

1.3.4 Information Disclosure

Defn 7 (Information Disclosure)**.** *Information disclosure* is about allowing people to see information they are not authorized to see.

1.3.4.1 Information Disclosure from a Process A process will disclose information that helps further attacks. This can be done by leaking memory addresses, extracting secrets from error messages, or extracting design details from errors messages.

1.3.4.2 Information Disclosure from a Data Store Since data stores store data, they can leak it multiple ways:

- Failure to properly use security mechanisms
- Not setting permisions
- Cryptographic keys being found/leaked
- Files read over the network are readable over the network
- Metadata (filenames, author, etc.) is also important
- OS-level leaks when swapping things out
- Data extracted from things using OS under attacker control.

1.3.4.3 Information Disclosure from a Data Flow Data flows are particularly susceptible. Data flows on a single machine that is shared among multiple mutually distrustful uses of a system is a main susceptibility. Attackers can redirect information to themselves. Attackers can gain information even when the traffic is encrypted.

1.3.5 Denial of Service

Defn 8 (Denial of Service)**.** *Denial-of-service* attacks consume a resource that is needed to provide a service.

These attacks can be split into attacks that work while the attacker is actively attacking, and ones that occur persistently. These can also be amplified or unamplified. Amplified attacks are relatively small attacks that have big effects.

1.3.6 Elevation of Privilege

Defn 9 (Elevation of Privilege)**.** *Elevation of privilege* is allowing someone to do something they are not authorized to to. For example, allowing a remote user to execute code as an administrator, or allowing a remote person without privileges to run code.

Threat Examples	What the Attacker Does	Notes
Information disclosure against a process	Extract secrets from error messages	
	Reads error messages from username/passwords to entire database tables	
	Extract machine secrets from error messages	Makes defense against memory corruption less useful
	Extract business/personal secrets from error cases	
Information disclosure against data stores	Takes advantage of inappropriate or missing ACLs	
	Takes advantage of bad database permissions	
	Finds files protected by obscurity	
	Finds cryptographic keys on disk or in memory	
	Sees interesting information in metadata	
	Reads files as they traverse the network	
	Gets data from logs or temp files	
	Gets data from swap or other temp storage	
	Extracts data by obtaining device, changing OS	
Information disclosure against data flows	Reads data on network	
	Redirects traffic to enable reading data on network	
	Learn secrets by analyzing traffic	
	Learn who's talking to whom by watching DNS	
	Learn who's talking to whom by social network info disclosure	

Table 1.5: Information Disclosure Threats

Threat Examples	What the Attacker Does	Notes
Denial of service against a process	Absorbs memory	
	Absorbs storage	
	Absorbs CPU cycles	
	Uses process as an amplifier	
Denial of service against a data store	Fills data store up	
	Makes enough requests to slow down the system	
Denial of service against a data flow	Consumes network resources	

Table 1.6: Denial of Service Threats

1.3.6.1 Elevate Privileges by Corrupting a Process

Corrupting a process can involve:

- Smashing the stack
- Exploiting information on the heap
- Other techniques

These attacks allow the attacker to gain influence or control over a program's control flow.

Threat Examples	What the Attacker Does	Notes
Elevation of privilege against a process by corrupting the process	Send inputs that the code doesn't handle properly	These are very common and are usually high impact
	Gains access to read/write memory inappropriately	Writing memory is bad, but reading memory allows further attacks.
Elevation through missed authorization checks		
Elevation through buggy authorization checks		Centralizing such checks makes bugs easier to manage
Elevation through data tampering	Modifies bits on disk to do things other than what the authorized user intends	

Table 1.7: Elevation of Privilege Threats

1.3.6.2 Elevate Privileges through Authorization Failures If we don't check authorization on every path through a program, this can be a problem. If there are buggy checks, the attacker can take advantage of them. If a program relies on other programs, configuration files, or datasets being trustworthy, those are possible targets as well.

1.3.7 STRIDE-per-Interaction

This variant of STRIDE Analysis involves applying the traditional STRIDE Analysis to interations between elements in a system, rather than considering the system as a whole.

1.4 MITRE TARA Analysis

A Complex Numbers

Defn A.0.1 (Complex Number)**.** A *complex number* is a hyper real number system. This means that two real numbers, $a, b \in \mathbb{R}$, are used to construct the set of complex numbers, denoted mathbbC.

A complex number is written, in Cartesian form, as shown in Equation (A.1) below.

$$z = a \pm ib \tag{A.1}$$

where

$$i = \sqrt{-1} \tag{A.2}$$

Remark (i vs. j for Imaginary Numbers)*.* Complex numbers are generally denoted with either i or j. Electrical engineering regularly makes use of j as the imaginary value. This is because alternating current i is already taken, so j is used as the imaginary value instad.

A.1 Parts of a Complex Number

A Complex Number is made of up 2 parts:

1. Real Part
2. Imaginary Part

Defn A.1.1 (Real Part)**.** The *real part* of an imaginary number, denoted with the Re operator, is the portion of the Complex Number with no part of the imaginary value i present.

If $z = x + iy$, then

$$\mathrm{Re}\{z\} = x \tag{A.3}$$

Remark A.1.1.1 (Alternative Notation)*.* The Real Part of a number sometimes uses a slightly different symbol for denoting the operation. It is:

$$\Re\mathfrak{e}$$

Defn A.1.2 (Imaginary Part)**.** The *imaginary part* of an imaginary number, denoted with the Im operator, is the portion of the Complex Number where the imaginary value i is present.

If $z = x + iy$, then

$$\mathrm{Im}\{z\} = y \tag{A.4}$$

Remark A.1.2.1 (Alternative Notation)*.* The Imaginary Part of a number sometimes uses a slightly different symbol for denoting the operation. It is:

$$\Im\mathfrak{m}$$

A.2 Binary Operations

The question here is if we are given 2 complex numbers, how should these binary operations work such that we end up with just one resulting complex number. There are only 2 real operations that we need to worry about, and the other 3 can be defined in terms of these two:

1. Addition
2. Multiplication

For the sections below, assume:

$$\begin{aligned} z &= x_1 + iy_1 \\ w &= x_2 + iy_2 \end{aligned}$$

A.2.1 Addition

The addition operation, still denoted with the + symbol is done pairwise. You should treat i like a variable in regular algebra, and not move it around.

$$z + w \coloneqq (x_1 + x_2) + i(y_1 + y_2) \tag{A.5}$$

A.2.2 Multiplication

The multiplication operation, like in traditional algebra, usually lacks a multiplication symbol. You should treat i like a variable in regular algebra, and not move it around.

$$\begin{aligned} zw &:= (x_1 + iy_1)(x_2 + iy_2) \\ &= (x_1x_2) + (iy_1x_2) + (ix_1y_2) + (i^2y_1y_2) \\ &= (x_1x_2) + i(y_1x_2 + x_1y_2) + (-1y_1y_2) \\ &= (x_1x_2 - y_1y_2) + i(y_1x_2 + x_1y_2) \end{aligned} \tag{A.6}$$

A.3 Complex Conjugates

Defn A.3.1 (Complex Conjugate)**.** The conjugate of a complex number is called its *complex conjugate*. The complex conjugate of a complex number is the number with an equal real part and an imaginary part equal in magnitude but opposite in sign. If we have a complex number as shown below,

$$z = a \pm bi$$

then, the conjugate is denoted and calculated as shown below.

$$\overline{z} = a \mp bi \tag{A.7}$$

The Complex Conjugate can also be denoted with an asterisk ($*$). This is generally done for complex functions, rather than single variables.

$$z^* = \overline{z} \tag{A.8}$$

A.3.1 Notable Complex Conjugate Expressions

There are 2 interesting things that we can perform with *just* the concept of a Complex Number and a Complex Conjugate:

1. $z\overline{z}$
2. $\frac{z}{\overline{z}}$

The first is interesting because of this simplification:

$$\begin{aligned} z\overline{z} &= (x + iy)(x - iy) \\ &= x^2 - xyi + xyi - i^2y^2 \\ &= x^2 - (-1)y^2 \\ &= x^2 + y^2 \end{aligned}$$

Thus,

$$z\overline{z} = x^2 + y^2 \tag{A.9}$$

which is interesting because, in comparison to the input values, the output is completely real.

The other interesting Complex Conjugate is dividing a Complex Number by its conjugate.

$$\frac{z}{\overline{z}} = \frac{x + iy}{x - iy}$$

We want to have this end up in a form of $a + ib$, so we multiply the entire fraction by z, to cause the denominator to be completely real.

$$z\left(\frac{z}{\overline{z}}\right) = \frac{z^2}{z\overline{z}}$$

Using our solution from Equation (A.9):

$$\begin{aligned} &= \frac{(x + iy)^2}{x^2 + y^2} \\ &= \frac{x^2 + 2xyi + i^2y^2}{x^2 + y^2} \end{aligned}$$

By breaking up the fraction's numerator, we can more easily recognize this to be teh Cartesian form of the Complex Number.

$$\begin{aligned}
&= \frac{(x^2 - y^2) + 2xyi}{x^2 + y^2} \\
&= \frac{x^2 - y^2}{x^2 + y^2} + \frac{2xyi}{x^2 + y^2}
\end{aligned}$$

This is an interesting development because, unlike the multiplication of a Complex Number by its Complex Conjugate, the division of these two values does **not** yield a purely real number.

$$\frac{z}{\overline{z}} = \frac{x^2 - y^2}{x^2 + y^2} + \frac{2xyi}{x^2 + y^2} \tag{A.10}$$

A.3.2 Properties of Complex Conjugates

Conjugation follows some of the traditional algebraic properties that you are already familiar with, namely commutativity.

First, start by defining some expressions so that we can prove some of these properties:

$$\begin{aligned}
z &= x + iy \\
\overline{z} &= x - iy
\end{aligned}$$

(i) The conjugation operation is commutative.

(ii) The conjugation operation can be distributed over addition and multiplication.

$$\begin{aligned}
\overline{z + w} &= \overline{z} + \overline{w} \\
\overline{zw} &= \overline{z}\overline{w}
\end{aligned}$$

Property **(ii)** can be proven by just performing a simplification.

*Prove Property **(ii)**.* Let z and w be complex numbers ($z, w \in$ mathbbC) where $z = x_1 + iy_1$ and $w = x_2 + iy_2$. Prove that $\overline{z + w} = \overline{z} + \overline{w}$.

We start by simplifying the left-hand side of the equation ($\overline{z + w}$).

$$\begin{aligned}
\overline{z + w} &= \overline{(x_1 + iy_1) + (x_2 + iy_2)} \\
&= \overline{(x_1 + x_2) + i(y_1 + y_2)} \\
&= (x_1 + x_2) - i(y_1 + y_2)
\end{aligned}$$

Now, we simplify the other side ($\overline{z} + \overline{w}$).

$$\begin{aligned}
\overline{z} + \overline{w} &= \overline{(x_1 + iy_1)} + \overline{(x_2 + iy_2)} \\
&= (x_1 - iy_1) + (x_2 - iy_2) \\
&= (x_1 + x_2) - i(y_1 + y_2)
\end{aligned}$$

We can see that both sides are equivalent, thus the addition portion of Property **(ii)** is correct.

Remark. The proof of the multiplication portion of Property **(ii)** is left as an exercise to the reader. However, that proof is quite similar to this proof of addition.

■

A.4 Geometry of Complex Numbers

So far, we have viewed Complex Numbers only algebraically. However, we can also view them geometrically as points on a 2 dimensional Argand Plane.

Defn A.4.1 (Argand Plane)**.** An *Argane Plane* is a standard two dimensional plane whose points are all elements of the complex numbers, $z \in$ mathbbC. This is taken from Descarte's definition of a completely real plane.

The Argand plane contains 2 lines that form the axes, that indicate the real component and the imaginary component of the complex number specified.

A Complex Number can be viewed as a point in the Argand Plane, where the Real Part is the "x"-component and the Imaginary Part is the "y"-component.

By plotting this, you see that we form a right triangle, so we can find the hypotenuse of that triangle. This hypotenuse is the distance the point p is from the origin, refered to as the Modulus.

Remark. When working with Complex Numbers geometrically, we refer to the points, where they are defined like so:

$$z = x + iy = p(x, y)$$

Note that p is **not** a function of x and y. Those are the values that inform us **where** p is located on the Argand Plane.

A.4.1 Modulus of a Complex Number

Defn A.4.2 (Modulus)**.** The *modulus* of a Complex Number is the distance from the origin to the complex point p. This is based off the Pythagorean Theorem.

$$\begin{aligned} |z|^2 &= x^2 + y^2 = z\overline{z} \\ |z| &= \sqrt{x^2 + y^2} \end{aligned} \tag{A.11}$$

(i) The *Law of Moduli* states that $|zw| = |z||w|$..

We can prove Property **(i)** using an algebraic identity.

*Prove Property **(i)**.* Let z and w be complex numbers ($z, w \in$ mathbbC). We are asked to prove

$$|zw| = |z||w|$$

But, it is actually easier to prove

$$|zw|^2 = |z|^2|w|^2$$

We start by simplifying the $|zw|^2$ equation above.

$$|zw|^2 = |z|^2|w|^2$$

Using the definition of the Modulus of a Complex Number in Equation (A.11), we can expand the modulus.

$$= (zw)(\overline{zw})$$

Using Property **(ii)** for multiplication allows us to do the next step.

$$= (zw)(\overline{z}\overline{w})$$

Using Multiplicative Associativity and Multiplicative Commutativity, we can simplify this further.

$$\begin{aligned} &= (z\overline{z})(w\overline{w}) \\ &= |z|^2|w|^2 \end{aligned}$$

Note how we never needed to define z or w, so this is as general a result as possible. ∎

A.4.1.1 Algebraic Effects of the Modulus' Property (i)

For this section, let $z = x_1 + iy_1$ and $w = x_2 + iy_2$. Now,

$$\begin{aligned} zw &= (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1) \\ |zw|^2 &= (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2 \\ &= \left(x_1^2 + x_2^2\right)\left(x_2^2 + y_2^2\right) \\ &= |z|^2|w|^2 \end{aligned}$$

However, the Law of Moduli (Property **(i)**) does **not** hold for a hyper complex number system one that uses 2 or more imaginaries, i.e. $z = a + iy + jz$. But, the Law of Moduli (Property **(i)**) **does** hold for hyper complex number system that uses 3 imaginaries, $a = z + iy + jz + k\ell$.

A.4.1.2 Conceptual Effects of the Modulus' Property (i)

We are interested in seeing if $|zw| = (x_1^2 + y_1^2)(x_2^2 + y_2^2)$ can be extended to more complex terms (3 terms in the complex number).

However, Langrange proved that the equation below **always** holds. Note that the z below has no relation to the z above.

$$(x_1 + y_1 + z_1) \neq X^2 + Y^2 + Z^2$$

A.5 Circles and Complex Numbers

We need to define both a center and a radius, just like with regular purely real values. Equation (A.12) defines the relation required for a circle using Complex Numbers.

$$|z - a| = r \tag{A.12}$$

Example A.1: Convert to Circle. Lecture 2, Example 1

Given the expression below, find the location of the center of the circle and the radius of the circle?

$$|5iz + 10| = 7$$

This is just a matter of simplification and moving terms around.

$$\begin{aligned}
|5iz + 10| &= 7 \\
|5i(z + \frac{10}{5i})| &= 7 \\
|5i(z + \frac{2}{i})| &= 7 \\
|5i(z + \frac{2}{i}\frac{-i}{-i})| &= 7 \\
|5i(z - 2i)| &= 7
\end{aligned}$$

Now using the Law of Moduli (Property **(i)**) $|ab| = |a||b|$, we can simplify out the extra imaginary term.

$$\begin{aligned}
|5i||z - 2i| &= 7 \\
5|z - 2i| &= 7 \\
|z - 2i| &= \frac{7}{5}
\end{aligned}$$

Thus, the circle formed by the equation $|5iz + 10| = 7$ is actually $|z - 2i| = \frac{7}{5}$, with a center at $a = 2i$ and a radius of $\frac{7}{5}$.

A.5.1 Annulus

Defn A.5.1 (Annulus)**.** An *annulus* is a region that is bounded by 2 concentric circles. This takes the form of Equation (A.13).

$$r_1 \leq |z - a| \leq r_2 \tag{A.13}$$

In Equation (A.13), each of the $\leq$ symbols could also be replaced with $<$. This leads to 3 different possibilities for the annulus:

1. If both inequality symbols are $\leq$, then it is a **Closed Annulus**.
2. If both inequality symbols are $<$, then it is an **Open Annulus**.
3. If **only one** inequality symbol $<$ and the other $\leq$, then it is not an **Open Annulus**.

The concept of an Annulus can be extended to angles and arguments of a Complex Number. A general example of this is shown below.

$$\theta_1 \leq \arg(z) \leq \theta_2$$

Angular Annuli follow all the same rules as regular annuli.

A.6 Polar Form

The polar form of a Complex Number is an alternative, but equally useful way to express a complex number. In polar form, we express the distance the complex number is from the origin and the angle it sits at from the real axis. This is seen in Equation (A.14).

$$z = r\big(\cos(\theta) + i\sin(\theta)\big) \tag{A.14}$$

Remark. Note that in the definition of polar form (Equation (A.14)), there is no allowance for the radius, r, to be negative. You must fix this by figuring out the angle change that is required for the radius to become positive.

Thus,

$$\begin{aligned}
r &= |z| \\
\theta &= \arg(z)
\end{aligned}$$

Example A.2: Find Polar Coordinates from Cartesian Coordinates. Lecture 2, Example 1

Find the complex number's $z = -\sqrt{3} + i$ polar coordinates?

We start by finding the radius of z (modulus of z).

$$\begin{aligned} r &= |z| \\ &= \sqrt{\mathrm{Re}\{z\}^2 + \mathrm{Im}\{z\}^2} \\ &= \sqrt{\left(-\sqrt{3}\right)^2 + 1^2} \\ &= \sqrt{3+1} \\ &= \sqrt{4} \\ &= 2 \end{aligned}$$

Thus, the point is 2 units away from the origin, the radius is 2 $r = 2$.
Now, we need to find the angle, the argument, of the Complex Number.

$$\begin{aligned} \cos(\theta) &= \frac{-\sqrt{3}}{2} \\ \theta &= \cos^{-1}\left(\frac{-\sqrt{3}}{2}\right) \\ &= \frac{5\pi}{6} \end{aligned}$$

Now that we have one angle for the point, we also need to consider the possibility that there have been an unknown amount of rotations around the entire plane, meaning there have been $2\pi k$, where $k = 0, 1, \ldots$.
We now have all the information required to reconstruct this point using polar coordinates:

$$\begin{aligned} r &= 2 \\ \theta &= \frac{5\pi}{6} \\ \arg(z) &= \frac{5\pi}{6} + 2\pi k \end{aligned}$$

A.6.1 Converting Between Cartesian and Polar Forms

Using Equation (A.14) and Equation (A.1), it is easy to see the relation between r, θ, x, and y.

Definition of a Complex Number in Cartesian form.

$$z = x + iy$$

Definition of a Complex Number in polar form.

$$\begin{aligned} z &= r\big(\cos(\theta) + i\sin(\theta)\big) \\ &= r\cos(\theta) + ir\sin(\theta) \end{aligned}$$

Thus,

$$\begin{aligned} x &= r\cos(\theta) \\ y &= r\sin(\theta) \end{aligned} \tag{A.15}$$

A.6.2 Benefits of Polar Form

Polar form is good for multiplication of Complex Numbers because of the way sin and cos multiply together. The Cartesian form is good for addition and subtraction. Take the examples below to show what I mean.

A.6.2.1 Multiplication For multiplication, the radii are multiplied together, and the angles are added.

$$\Big(r_1\big(\cos(\theta) + i\sin(\theta)\big)\Big)\Big(r_2\big(\cos(\phi) + i\sin(\phi)\big)\Big) = r_1 r_2\big(\cos(\theta+\phi) + i\sin(\theta+\phi)\big) \tag{A.16}$$

A.6.2.2 Division For division, the radii are divided by each other, and the angles are subtracted.

$$\frac{r_1\big(\cos(\theta) + i\sin(\theta)\big)}{r_2\big(\cos(\phi) + i\sin(\phi)\big)} = \frac{r_1}{r_2}\big(\cos(\theta-\phi) + i\sin(\theta-\phi)\big) \tag{A.17}$$

A.6.2.3 Exponentiation Because exponentiation is defined to be repeated multiplication, Paragraph A.6.2.1 applies. That this generalization is true was proven by de Moiver, and is called de Moiver's Law.

Defn A.6.1 (de Moiver's Law)**.** Given a complex number z, $z \in$ mathbbC and a rational number n, $n \in$ mathbbQ, the exponentiation of z^n is defined as Equation (A.18).

$$z^n = r^n\big(\cos(n\theta) + i\sin(n\theta)\big) \tag{A.18}$$

A.7 Roots of a Complex Number

de Moiver's Law also applies to finding **roots** of a Complex Number.

$$z^{\frac{1}{n}} = r^{\frac{1}{n}}\left(\cos\left(\frac{\arg z}{n}\right) + i\sin\left(\frac{\arg z}{n}\right)\right) \tag{A.19}$$

Remark. As the entire $\arg z$ term is being divided by n, the $2\pi k$ is **ALSO** divided by n.

Roots of a Complex Number satisfy Equation (A.20). To demonstrate that equation, $z = r\big(\cos(\theta) + i\sin(\theta)\big)$ and $w = \rho\big(\cos(\phi) + i\sin(\phi)\big)$.

$$w^n = z \tag{A.20}$$

A w that satisfies Equation (A.20) is an nth root of z.

Example A.3: Roots of a Complex Number. Lecture 2, Example 2

Find the cube roots of $z = -\sqrt{3} + i$?

From Example A.2, we know that the polar form of z is

$$z = 2\left(\cos\left(\frac{5\pi}{6} + 2\pi k\right) + i\sin\left(\frac{5\pi}{6} + 2\pi k\right)\right)$$

Because the question is asking for **cube** roots, that means there are 3 roots. Using Equation (A.19), we can find the general form of the roots.

$$\begin{aligned}
z &= 2\left(\cos\left(\frac{5\pi}{6} + 2\pi k\right) + i\sin\left(\frac{5\pi}{6} + 2\pi k\right)\right) \\
z^{\frac{1}{3}} &= \sqrt[3]{2}\left(\cos\left(\frac{1}{3}\left(\frac{5\pi}{6} + 2\pi k\right)\right) + i\sin\left(\frac{1}{3}\left(\frac{5\pi}{6} + 2\pi k\right)\right)\right) \\
&= \sqrt[3]{2}\left(\cos\left(\frac{\pi + 12\pi k}{18}\right) + i\sin\left(\frac{\pi + 12\pi k}{18}\right)\right)
\end{aligned}$$

Now that we have a general equation for **all** possible cube roots, we need to find all the unique ones. This is because after $k = n$ roots, the roots start to repeat themselves, because the $2\pi k$ part of the expression becomes effective, making the angle a full rotation. We simply enumerate $k \in \mathbb{Z}^+$, so $k = 0, 1, 2, \ldots$.

k = 0

$$\sqrt[3]{2}\left(\cos\left(\frac{\pi + 12\pi(0)}{18}\right) + i\sin\left(\frac{\pi + 12\pi(0)}{18}\right)\right) = \sqrt[3]{2}\left(\cos\left(\frac{\pi}{18}\right) + i\sin\left(\frac{\pi}{18}\right)\right)$$

k = 1

$$\sqrt[3]{2}\left(\cos\left(\frac{\pi + 12\pi(1)}{18}\right) + i\sin\left(\frac{\pi + 12\pi(1)}{18}\right)\right) = \sqrt[3]{2}\left(\cos\left(\frac{13\pi}{18}\right) + i\sin\left(\frac{13\pi}{18}\right)\right)$$

k = 2

$$\sqrt[3]{2}\left(\cos\left(\frac{\pi+12\pi(2)}{18}\right)+i\sin\left(\frac{\pi+12\pi(2)}{18}\right)\right)=\sqrt[3]{2}\left(\cos\left(\frac{25\pi}{18}\right)+i\sin\left(\frac{25\pi}{18}\right)\right)$$

k = 3

$$\begin{aligned}\sqrt[3]{2}\left(\cos\left(\frac{\pi+12\pi(3)}{18}\right)+i\sin\left(\frac{\pi+12\pi(3)}{18}\right)\right)&=\sqrt[3]{2}\left(\cos\left(\frac{\pi}{18}+\frac{36\pi}{18}\right)+i\sin\left(\frac{\pi}{18}+\frac{36\pi}{18}\right)\right)\\&=\sqrt[3]{2}\left(\cos\left(\frac{\pi}{18}+2\pi\right)+i\sin\left(\frac{\pi}{18}+2\pi\right)\right)\\&=\sqrt[3]{2}\left(\cos\left(\frac{\pi}{18}\right)+i\sin\left(\frac{\pi}{18}\right)\right)\end{aligned}$$

Thus, the 3 cube roots of z are:

$$\begin{aligned}z_1^{\frac{1}{3}}&=\sqrt[3]{2}\left(\cos\left(\frac{\pi}{18}\right)+i\sin\left(\frac{\pi}{18}\right)\right)\\z_2^{\frac{1}{3}}&=\sqrt[3]{2}\left(\cos\left(\frac{13\pi}{18}\right)+i\sin\left(\frac{13\pi}{18}\right)\right)\\z_3^{\frac{1}{3}}&=\sqrt[3]{2}\left(\cos\left(\frac{25\pi}{18}\right)+i\sin\left(\frac{25\pi}{18}\right)\right)\end{aligned}$$

A.8 Arguments

There are 2 types of arguments that we can talk about for a Complex Number.

1. The Argument
2. The Principal Argument

Defn A.8.1 (Argument)**.** The *argument* of a Complex Number refers to **all** possible angles that can satisfy the angle requirement of a Complex Number.

Example A.4: Argument of Complex Number. Lecture 3, Example 1

If $z=-1-i$, then what is its **Argument**?

You can plot this value on the Argand Plane and find the angle graphically/geometrically, or you can "cheat" and use $\tan^{-1}$ (so long as you correct for the proper quadrant). I will "cheat", as I cannot plot easily.

$$\begin{aligned}z&=-1-i\\\arg(z)=\tan(\theta)&=\frac{-i}{-1}\\&=\frac{\pi}{4}\end{aligned}$$

Remember to correct for the proper quadrant. We are in quadrant IV.

$$=\frac{5\pi}{4}$$

Now, we have to account for **all** possible angles that form this angle.

$$\arg(z)=\frac{5\pi}{4}+2\pi k$$

Thus, the argument of $z=-1-i$ is $\arg(z)=\frac{5\pi}{4}+2\pi k$.

Defn A.8.2 (Principal Argument)**.** The *principal argument* is the exact or reference angle of the Complex Number. By convention, the principal Argument of a complex number z is defined to be bounded like so: $-\pi<\text{Arg}(z)\leq\pi$.

Example A.5: Principal Argument of Complex Number. Lecture 3, Example 1

If $z = -1 - i$, then what is its **Principal Argument**?

You can plot this value on the Argand Plane and find the angle graphically/geometrically, or you can "cheat" and use $\tan^{-1}$ (so long as you correct for the proper quadrant). I will "cheat", as I cannot plot easily.

$$\begin{aligned} z &= -1 - i \\ \arg(z) = \tan(\theta) &= \frac{-i}{-1} \\ &= \frac{\pi}{4} \end{aligned}$$

Remember to correct for the proper quadrant. We are in quadrant IV.

$$= \frac{5\pi}{4}$$

Thus, the Principal Argument of $z = -1 - i$ is $\operatorname{Arg}(z) = \frac{5\pi}{4}$.

A.9 Complex Exponentials

The definition of an exponential with a Complex Number as its exponent is defined in Equation (A.21).

$$e^z = e^{x+iy} = e^x\big(\cos(y) + i\sin(y)\big) \tag{A.21}$$

If instead of e as the base, we have some value a, then we have Equation (A.22).

$$\begin{aligned} a^z &= e^{z\ln(a)} \\ &= e^{\mathrm{Re}\{z\ln(a)\}}\Big(\cos\big(\mathrm{Im}\{z\ln(a)\}\big) + i\sin\big(\mathrm{Im}\{z\ln(a)\}\big)\Big) \end{aligned} \tag{A.22}$$

In the case of Equation (A.21), z can be presented in either Cartesian or polar form, they are equivalent.

Example A.6: Simplify Simple Complex Exponential. Lecture 3

Simplify the expression below, then find its Modulus, Argument, and its Principal Argument?

$$e^{-1+i\sqrt{3}}$$

If we look at the exponent on the exponential, we see

$$z = -1 + i\sqrt{3}$$

which means

$$\begin{aligned} x &= -1 \\ y &= \sqrt{3} \end{aligned}$$

With this information, we can simplify the expression **just** by observation, with no calculations required.

$$e^{-1+i\sqrt{3}} = e^{-1}\big(\cos(\sqrt{3}) + i\sin(\sqrt{3})\big)$$

Now, we can solve the other 3 parts of this example **by observation**.

$$\begin{aligned} |e^{-1+i\sqrt{3}}| &= |e^{-1}\big(\cos(\sqrt{3}) + i\sin(\sqrt{3})\big)| \\ &= e^{-1} \\ \arg\left(e^{-1+i\sqrt{3}}\right) &= \arg\left(e^{-1}\big(\cos(\sqrt{3}) + i\sin(\sqrt{3})\big)\right) \\ &= \sqrt{3} + 2\pi k \\ \operatorname{Arg}\left(e^{-1+i\sqrt{3}}\right) &= \operatorname{Arg}\left(e^{-1}\big(\cos(\sqrt{3}) + i\sin(\sqrt{3})\big)\right) \\ &= \sqrt{3} \end{aligned}$$

Example A.7: Simplify Complex Exponential Exponent. Lecture 3

Given $z = e^{-e^{-i}}$, what is this expression in polar form, what is its Modulus, its Argument, and its Principal Argument?

We start by simplifying the exponent of the base exponential, i.e. e^{-i}.

$$\begin{aligned} e^{-i} &= e^{0-i} \\ &= e^{0}\big(\cos(-1) + i\sin(-1)\big) \\ &= 1\big(\cos(-1) + i\sin(-1)\big) \end{aligned}$$

Now, with that exponent simplified, we can solve the main question.

$$\begin{aligned} e^{-e^{-i}} &= e^{-1\big(\cos(-1)+i\sin(-1)\big)} \\ &= e^{-1\big(\cos(1)-i\sin(1)\big)} \\ &= e^{-\cos(1)+i\sin(1)} \end{aligned}$$

If we refer back to Equation (A.21), then it becomes obvious what x and y are.

$$\begin{aligned} x &= -\cos(1) \\ y &= \sin(1) \\ e^{-e^{-i}} &= e^{-\cos(1)}\Big(\cos\big(\sin(1)\big) + i\sin\big(\sin(1)\big)\Big) \end{aligned}$$

Now that we have "simplified" this exponential, we can solve the other 3 questions by **observation**.

$$\begin{aligned} |e^{-e^{-i}}| &= |e^{-\cos(1)}\Big(\cos\big(\sin(1)\big) + i\sin\big(\sin(1)\big)\Big)| \\ &= e^{-\cos(1)} \\ \arg\left(e^{-e^{-i}}\right) &= \arg\left(e^{-\cos(1)}\Big(\cos\big(\sin(1)\big) + i\sin\big(\sin(1)\big)\Big)\right) \\ &= \sin(1) + 2\pi k \\ \operatorname{Arg}\left(e^{-e^{-i}}\right) &= \operatorname{Arg}\left(e^{-\cos(1)}\Big(\cos\big(\sin(1)\big) + i\sin\big(\sin(1)\big)\Big)\right) \\ &= \sin(1) \end{aligned}$$

Example A.8: Non-e Complex Exponential. Lecture 3

Find all values of $z = 1^{i}$?

Use Equation (A.22) to simplify this to a base of e, where we can use the usual Equation (A.21) to solve this.

$$\begin{aligned} a^{z} &= e^{z\ln(a)} \\ 1^{i} &= e^{i\ln(1)} \end{aligned}$$

Simplify the logarithm in the exponent first, $\ln(1)$.

$$\begin{aligned} \ln(1) &= \log_e|1| + i\arg(1) \\ &= \log_e(1) + i(0 + 2\pi k) \\ &= 0 + 2\pi k i \\ &= 2\pi k i \end{aligned}$$

Now, plug $\ln(1)$ back into the exponent, and solve the exponential.

$$\begin{aligned} e^{i(2\pi k i)} &= e^{2\pi k i^{2}} \\ &= e^{2\pi k(-1)} \\ z &= e^{-2\pi k} \end{aligned}$$

Thus, all values of $z = e^{-2\pi k}$ where $k = 0, 1, \ldots$.

A.9.1 Complex Conjugates of Exponentials

$$\overline{e^z} = e^{\overline{z}} \tag{A.23}$$

A.10 Complex Logarithms

There are some denotational changes that need to be made for this to work. The traditional real-number natural logarithm ln needs to be redefined to its defining form $\log_e$.

With that denotational change, we can now use ln for the Complex Logarithm.

Defn A.10.1 (Complex Logarithm)**.** The *complex logarithm* is defined in Equation (A.24). The only requirement for this equation to hold true is that $w \neq 0$.

$$\begin{aligned} e^z &= w \\ z &= \ln(w) \\ &= \log_e|w| + i\arg(w) \end{aligned} \tag{A.24}$$

Remark A.10.1.1. The Complex Logarithm is different than it's purely-real cousin because we allow negative numbers to be input. This means it is more general, but we must lose the precision of the purely-real logarithm. This means that each nonzero number has infinitely many logarithms.

Example A.9: All Complex Logarithms of Simple Expression. Lecture 3

What are **all** Complex Logarithms of $z = -1$?

We can apply the definition of a Complex Logarithm (Equation (A.24)) directly.

$$\begin{aligned} \ln(z) &= \log_e|z| + i\arg(z) \\ &= \log_e|-1| + i\arg(-1) \\ &= \log_e(1) + i(\pi + 2\pi k) \\ &= 0 + i(\pi + 2\pi k) \\ &= i(\pi + 2\pi k) \end{aligned}$$

Thus, all logarithms of $z = -1$ are defined by the expression $i(\pi + 2\pi k)$, $k = 0, 1, \ldots$.

Remark. You can see the loss of specificity in the Complex Logarithm because the variable k is still present in the final answer.

Example A.10: All Complex Logarithms of Complex Logarithm. Lecture 3

What are **all** the Complex Logarithms of $z = \ln(1)$?

We start by simplifying z, before finding $\ln(z)$. We can make use of Equation (A.24), to simplify this value.

$$\begin{aligned} \ln(w) &= \log_e|w| + i\arg(w) \\ \ln(1) &= \log_e|1| + i\arg(1) \\ &= \log_e 1 + i(0 + 2\pi k) \\ &= 0 + 2\pi k i \\ &= 2\pi k i \end{aligned}$$

Now that we have simplified z, we can solve for $\ln(z)$.

$$\begin{aligned} \ln(z) &= \ln(2\pi k i) \\ &= \log_e|2\pi k i| + i\arg(2\pi k i) \\ &= \log_e(2\pi|k|) + \left(i \begin{cases} \frac{\pi}{2} + 2\pi m & k > 0 \\ \frac{-\pi}{2} + 2\pi m & k < 0 \end{cases} \right) \end{aligned}$$

The $|k|$ is the **absolute value** of k, because k is an integer.

Thus, our solution of $\ln\big(\ln(1)\big) = \log_e(2\pi|k|) + \left(i \begin{cases} \frac{\pi}{2} + 2\pi m & k > 0 \\ \frac{-\pi}{2} + 2\pi m & k < 0 \end{cases} \right)$.

A.10.1 Complex Conjugates of Logarithms

$$\overline{\log(z)} = \log(\overline{z}) \tag{A.25}$$

A.11 Complex Trigonometry

For the equations below, $z \in$ mathbbC. These equations are based on Euler's relationship, Appendix B.2

$$\cos(z) = \frac{e^{iz} + e^{-iz}}{2} \tag{A.26}$$

$$\sin(z) = \frac{e^{iz} - e^{-iz}}{2i} \tag{A.27}$$

Example A.11: Simplify Complex Sinusoid. Lecture 3

Solve for z in the equation $\cos(z) = 5$?

We start by using the defintion of complex cosine Equation (A.26).

$$\begin{aligned} \cos(z) &= 5 \\ \frac{e^{iz} + e^{-iz}}{2} &= 5 \\ e^{iz} + e^{-iz} &= 10 \\ e^{iz}\left(e^{iz} + e^{-iz}\right) &= e^{iz}(10) \\ {e^{iz}}^2 + 1 &= 10e^{iz} \\ {e^{iz}}^2 - 10e^{iz} + 1 = 0 \end{aligned}$$

Solve this quadratic equation by using the Quadratic Equation.

$$\begin{aligned} e^{iz} &= \frac{-(-10) \pm \sqrt{(-10)^2 - 4(1)(1)}}{2(1)} \\ &= \frac{10 \pm \sqrt{100 - 4}}{2} \\ &= \frac{10 \pm \sqrt{96}}{2} \\ &= \frac{10 \pm 4\sqrt{6}}{2} \\ &= 5 \pm 2\sqrt{6} \end{aligned}$$

Use the definition of complex logarithms to simplify the exponential.

$$\begin{aligned} iz &= \ln(5 \pm 2\sqrt{6}) \\ &= \log_e|5 \pm 2\sqrt{6}| + i\arg(5 \pm 2\sqrt{6}) \\ &= \log_e|5 \pm 2\sqrt{6}| + i(0 + 2\pi k) \\ &= \log_e|5 \pm 2\sqrt{6}| + 2\pi k i \\ z &= \frac{1}{i}\left(\log_e|5 \pm 2\sqrt{6}| + 2\pi k i\right) \\ &= \frac{-i}{-i}\frac{1}{i}\left(\log_e|5 \pm 2\sqrt{6}|\right) + 2\pi k \\ &= 2\pi k - i\log_e|5 \pm 2\sqrt{6}| \end{aligned}$$

Thus, $z = 2\pi k - i\log_e|5 \pm 2\sqrt{6}|$.

A.11.1 Complex Angle Sum and Difference Identities

Because the definitions of sine and cosine are unsatisfactory in their Euler definitions, we can use angle sum and difference formulas and their Euler definitions to yield a set of Cartesian equations.

$$\cos(x+iy) = \big(\cos(x)\cosh(y)\big) - i\big(\sin(x)\sinh(y)\big) \tag{A.28}$$

$$\sin(x+iy) = \big(\sin(x)\cosh(y)\big) + i\big(\cos(x)\sinh(y)\big) \tag{A.29}$$

Example A.12: Simplify Trigonometric Exponential. Lecture 3

Simpify $z = e^{\cos(2+3i)}$, and find z's Modulus, Argument, and Principal Argument?

We start by simplifying the cos using Equation (A.28).

$$\begin{aligned}\cos(x+iy) &= \big(\cos(x)\cosh(y)\big) - i\big(\sin(x)\sinh(y)\big)\\ \cos(2+3i) &= \big(\cos(2)\cosh(3)\big) - i\big(\sin(2)\sinh(3)\big)\end{aligned}$$

Now that we have put the cos into a Cartesian form, one that is usable with Equation (A.21), we can solve this.

$$\begin{aligned}e^z &= e^{x+iy} = e^x\big(\cos(y) + i\sin(y)\big)\\ x &= \cos(2)\cosh(3)\\ y &= -\sin(2)\sinh(3)\\ e^{\cos(2)\cosh(3) - i\sin(2)\sinh(3)} &= e^{\cos(2)\cosh(3)}\Big(\cos\big(-\sin(2)\sinh(3)\big) + i\sin\big(-\sin(2)\sinh(3)\big)\Big)\end{aligned}$$

Now that we have simplified z, we can solve for the modulus, argument, and principal argument **by observation**.

$$\begin{aligned}|z| &= |e^{\cos(2)\cosh(3)}\Big(\cos\big(-\sin(2)\sinh(3)\big) + i\sin\big(-\sin(2)\sinh(3)\big)\Big)|\\ &= e^{\cos(2)\cosh(3)}\\ \arg(z) &= \arg(e^{\cos(2)\cosh(3)}\Big(\cos\big(-\sin(2)\sinh(3)\big) + i\sin\big(-\sin(2)\sinh(3)\big)\Big))\\ &= -\sin(2)\sinh(3) + 2\pi k\\ \operatorname{Arg}(z) &= \operatorname{Arg}(e^{\cos(2)\cosh(3)}\Big(\cos\big(-\sin(2)\sinh(3)\big) + i\sin\big(-\sin(2)\sinh(3)\big)\Big))\\ &= -\sin(2)\sinh(3)\end{aligned}$$

A.11.2 Complex Conjugates of Sinusoids

Since sinusoids can be represented by complex exponentials, as shown in Appendix B.2, we could calculate their complex conjugate.

$$\begin{aligned}\overline{\cos(x)} &= \cos(x)\\ &= \frac{1}{2}\left(e^{ix} + e^{-ix}\right)\end{aligned} \tag{A.30}$$

$$\begin{aligned}\overline{\sin(x)} &= \sin(x)\\ &= \frac{1}{2i}\left(e^{ix} - e^{-ix}\right)\end{aligned} \tag{A.31}$$

B Trigonometry

B.1 Trigonometric Formulas

$$\sin(\alpha) \pm \sin(\beta) = 2\sin\left(\frac{\alpha \pm \beta}{2}\right)\cos\left(\frac{\alpha \mp \beta}{2}\right) \tag{B.1}$$

$$\cos(\theta)\sin(\theta) = \frac{1}{2}\sin(2\theta) \tag{B.2}$$

B.2 Euler Equivalents of Trigonometric Functions

$$e^{\pm j\alpha} = \cos(\alpha) \pm j\sin(\alpha) \tag{B.3}$$

$$\cos(x) = \frac{e^{jx} + e^{-jx}}{2} \tag{B.4}$$

$$\sin(x) = \frac{e^{jx} - e^{-jx}}{2j} \tag{B.5}$$

$$\sinh(x) = \frac{e^{x} - e^{-x}}{2} \tag{B.6}$$

$$\cosh(x) = \frac{e^{x} + e^{-x}}{2} \tag{B.7}$$

B.3 Angle Sum and Difference Identities

$$\sin(\alpha \pm \beta) = \sin(\alpha)\cos(\beta) \pm \cos(\alpha)\sin(\beta) \tag{B.8}$$

$$\cos(\alpha \pm \beta) = \cos(\alpha)\cos(\beta) \mp \sin(\alpha)\sin(\beta) \tag{B.9}$$

B.4 Double-Angle Formulae

$$\sin(2\alpha) = 2\sin(\alpha)\cos(\alpha) \tag{B.10}$$

$$\cos(2\alpha) = \cos^2(\alpha) - \sin^2(\alpha) \tag{B.11}$$

B.5 Half-Angle Formulae

$$\sin\left(\frac{\alpha}{2}\right) = \sqrt{\frac{1-\cos(\alpha)}{2}} \tag{B.12}$$

$$\cos\left(\frac{\alpha}{2}\right) = \sqrt{\frac{1+\cos(\alpha)}{2}} \tag{B.13}$$

B.6 Exponent Reduction Formulae

$$\sin^2(\alpha) = \big(\sin(\alpha)\big) = \frac{1-\cos(2\alpha)}{2} \tag{B.14}$$

$$\cos^2(\alpha) = \big(\cos(\alpha)\big) = \frac{1+\cos(2\alpha)}{2} \tag{B.15}$$

B.7 Product-to-Sum Identities

$$2\cos(\alpha)\cos(\beta) = \cos(\alpha-\beta) + \cos(\alpha+\beta) \tag{B.16}$$

$$2\sin(\alpha)\sin(\beta) = \cos(\alpha-\beta) - \cos(\alpha+\beta) \tag{B.17}$$

$$2\sin(\alpha)\cos(\beta) = \sin(\alpha+\beta) + \sin(\alpha-\beta) \tag{B.18}$$

$$2\cos(\alpha)\sin(\beta) = \sin(\alpha+\beta) - \sin(\alpha-\beta) \tag{B.19}$$

B.8 Sum-to-Product Identities

$$\sin(\alpha) \pm \sin(\beta) = 2\sin\left(\frac{\alpha \pm \beta}{2}\right)\cos\left(\frac{\alpha \mp \beta}{2}\right) \tag{B.20}$$

$$\cos(\alpha) + \cos(\beta) = 2\cos\left(\frac{\alpha + \beta}{2}\right)\cos\left(\frac{\alpha - \beta}{2}\right) \tag{B.21}$$

$$\cos(\alpha) - \cos(\beta) = -2\sin\left(\frac{\alpha + \beta}{2}\right)\sin\left(\frac{\alpha - \beta}{2}\right) \tag{B.22}$$

B.9 Pythagorean Theorem for Trig

$$\cos^2(\alpha) + \sin^2(\alpha) = 1^2 \tag{B.23}$$

$$\cosh^2(\alpha) - \sinh^2(\alpha) = 1^2 \tag{B.24}$$

B.10 Rectangular to Polar

$$a + jb = \sqrt{a^2 + b^2}e^{j\theta} = re^{j\theta} \tag{B.25}$$

$$\theta = \begin{cases} \arctan\left(\frac{b}{a}\right) & a > 0 \\ \pi - \arctan\left(\frac{b}{a}\right) & a < 0 \end{cases} \tag{B.26}$$

B.11 Polar to Rectangular

$$re^{j\theta} = r\cos(\theta) + jr\sin(\theta) \tag{B.27}$$

C Calculus

C.1 L'Hopital's Rule

L'Hopital's Rule can be used to simplify and solve expressions regarding limits that yield irreconcialable results.

Lemma C.0.1 (L'Hopital's Rule)**.** *If the equation*

$$\lim_{x \to a} \frac{f(x)}{g(x)} = \begin{cases} \frac{0}{0} \\ \frac{\infty}{\infty} \end{cases}$$

then Equation (C.1) *holds.*

$$\lim_{x \to a} \frac{f(x)}{g(x)} = \lim_{x \to a} \frac{f'(x)}{g'(x)} \tag{C.1}$$

C.2 Fundamental Theorems of Calculus

Defn C.2.1 (First Fundamental Theorem of Calculus)**.** The *first fundamental theorem of calculus* states that, if f is continuous on the closed interval $[a, b]$ and F is the indefinite integral of f on $[a, b]$, then

$$\int_a^b f(x)\, dx = F(b) - F(a) \tag{C.2}$$

Defn C.2.2 (Second Fundamental Theorem of Calculus)**.** The *second fundamental theorem of calculus* holds for f a continuous function on an open interval I and a any point in I, and states that if F is defined by

$$F(x) = \int_a^x f(t)\, dt,$$

then

$$\begin{aligned} \frac{d}{dx} \int_a^x f(t)\, dt &= f(x) \\ F'(x) &= f(x) \end{aligned} \tag{C.3}$$

Defn C.2.3 (argmax)**.** The arguments to the *argmax* function are to be maximized by using their derivatives. You must take the derivative of the function, find critical points, then determine if that critical point is a global maxima. This is denoted as

$$\underset{x}{\operatorname{argmax}}$$

C.3 Rules of Calculus

C.3.1 Chain Rule

Defn C.3.1 (Chain Rule)**.** The *chain rule* is a way to differentiate a function that has 2 functions multiplied together.

If

$$f(x) = g(x) \cdot h(x)$$

then,

$$\begin{aligned} f'(x) &= g'(x) \cdot h(x) + g(x) \cdot h'(x) \\ \frac{df(x)}{dx} &= \frac{dg(x)}{dx} \cdot g(x) + g(x) \cdot \frac{dh(x)}{dx} \end{aligned} \tag{C.4}$$

C.4 Useful Integrals

$$\int \cos(x)\, dx = \sin(x) \tag{C.5}$$

$$\int \sin(x)\, dx = -\cos(x) \tag{C.6}$$

$$\int x \cos(x)\, dx = \cos(x) + x \sin(x) \tag{C.7}$$

Equation (C.7) simplified with Integration by Parts.

$$\int x\sin(x)\;dx = \sin(x) - x\cos(x) \tag{C.8}$$

Equation (C.8) simplified with Integration by Parts.

$$\int x^2\cos(x)\;dx = 2x\cos(x) + (x^2-2)\sin(x) \tag{C.9}$$

Equation (C.9) simplified by using Integration by Parts twice.

$$\int x^2\sin(x)\;dx = 2x\sin(x) - (x^2-2)\cos(x) \tag{C.10}$$

Equation (C.10) simplified by using Integration by Parts twice.

$$\int e^{\alpha x}\cos(\beta x)\;dx = \frac{e^{\alpha x}\big(\alpha\cos(\beta x) + \beta\sin(\beta x)\big)}{\alpha^2+\beta^2} + C \tag{C.11}$$

$$\int e^{\alpha x}\sin(\beta x)\;dx = \frac{e^{\alpha x}\big(\alpha\sin(\beta x) - \beta\cos(\beta x)\big)}{\alpha^2+\beta^2} + C \tag{C.12}$$

$$\int e^{\alpha x}\;dx = \frac{e^{\alpha x}}{\alpha} \tag{C.13}$$

$$\int xe^{\alpha x}\;dx = e^{\alpha x}\left(\frac{x}{\alpha} - \frac{1}{\alpha^2}\right) \tag{C.14}$$

Equation (C.14) simplified with Integration by Parts.

$$\int \frac{dx}{\alpha+\beta x} = \int \frac{1}{\alpha+\beta x}\;dx = \frac{1}{\beta}\ln(\alpha+\beta x) \tag{C.15}$$

$$\int \frac{dx}{\alpha^2+\beta^2x^2} = \int \frac{1}{\alpha^2+\beta^2x^2}\;dx = \frac{1}{\alpha\beta}\arctan\left(\frac{\beta x}{\alpha}\right) \tag{C.16}$$

$$\int \alpha^x\;dx = \frac{\alpha^x}{\ln(\alpha)} \tag{C.17}$$

$$\frac{d}{dx}\alpha^x = \frac{d\alpha^x}{dx} = \alpha^x\ln(x) \tag{C.18}$$

C.5 Leibnitz's Rule

Lemma C.0.2 (Leibnitz's Rule)**.** *Given*

$$g(t) = \int_{a(t)}^{b(t)} f(x,t)\,dx$$

with $a(t)$ and $b(t)$ differentiable in t and $\frac{\partial f(x,t)}{\partial t}$ continuous in both t and x, then

$$\frac{d}{dt}g(t) = \frac{dg(t)}{dt} = \int_{a(t)}^{b(t)} \frac{\partial f(x,t)}{\partial t}\,dx + f\big[b(t),t\big]\,\frac{db(t)}{dt} - f\big[a(t),t\big]\,\frac{da(t)}{dt} \tag{C.19}$$

D Laplace Transform

D.1 Laplace Transform

Defn D.1.1 (Laplace Transform). The *Laplace transformation* operation is denoted as $\mathcal{L}\{x(t)\}$ and is defined as

$$X(s) = \int_{-\infty}^{\infty} x(t)e^{-st}dt \tag{D.1}$$

D.2 Inverse Laplace Transform

Defn D.2.1 (Inverse Laplace Transform). The *inverse Laplace transformation* operation is denoted as $\mathcal{L}^{-1}\{X(s)\}$ and is defined as

$$x(t) = \frac{1}{2j\pi}\int_{\sigma-\infty}^{\sigma+\infty} X(s)e^{st}\,ds \tag{D.2}$$

D.3 Properties of the Laplace Transform

D.3.1 Linearity

The Laplace Transform is a linear operation, meaning it obeys the laws of linearity. This means Equation (D.3) must hold.

$$x(t) = \alpha_1 x_1(t) + \alpha_2 x_2(t) \tag{D.3a}$$

$$X(s) = \alpha_1 X_1(s) + \alpha_2 X_2(s) \tag{D.3b}$$

D.3.2 Time Scaling

Scaling in the time domain (expanding or contracting) yields a slightly different transform. However, this only makes sense for $\alpha > 0$ in this case. This is seen in Equation (D.4).

$$\mathcal{L}\big\{x(\alpha t)\big\} = \frac{1}{\alpha}X\left(\frac{s}{\alpha}\right) \tag{D.4}$$

D.3.3 Time Shift

Shifting in the time domain means to change the point at which we consider $t = 0$. Equation (D.5) below holds for shifting both forward in time and backward.

$$\mathcal{L}\big\{x(t-a)\big\} = X(s)e^{-as} \tag{D.5}$$

D.3.4 Frequency Shift

Shifting in the frequency domain means to change the complex exponential in the time domain.

$$\mathcal{L}^{-1}\big\{X(s-a)\big\} = x(t)e^{at} \tag{D.6}$$

D.3.5 Integration in Time

Integrating in time is equivalent to scaling in the frequency domain.

$$\mathcal{L}\left\{\int_0^t x(\lambda)\,d\lambda\right\} = \frac{1}{s}X(s) \tag{D.7}$$

D.3.6 Frequency Multiplication

Multiplication of two signals in the frequency domain is equivalent to a convolution of the signals in the time domain.

$$\mathcal{L}\big\{x(t) * v(t)\big\} = X(s)V(s) \tag{D.8}$$

D.3.7 Relation to Fourier Transform

The Fourier transform looks and behaves very similarly to the Laplace transform. In fact, if $X(\omega)$ exists, then Equation (D.9) holds.

$$X(s) = X(\omega)|_{\omega=\frac{s}{j}} \tag{D.9}$$

D.4 Theorems

There are 2 theorems that are most useful here:

1. Intial Value Theorem
2. Final Value Theorem

Theorem D.1 (Intial Value Theorem)**.** *The Initial Value Theorem states that when the signal is treated at its starting time, i.e. $t = 0^+$, it is the same as taking the limit of the signal in the frequency domain.*

$$x(0^+) = \lim_{s \to \infty} sX(s)$$

Theorem D.2 (Final Value Theorem)**.** *The Final Value Theorem states that when taking a signal in time to infinity, it is equivalent to taking the signal in frequency to zero.*

$$\lim_{t \to \infty} x(t) = \lim_{s \to 0} sX(s)$$

D.5 Laplace Transform Pairs

Time Domain	Frequency Domain
$x(t)$	$X(s)$
$\delta(t)$	1
$\delta(t - T_0)$	e^{-sT_0}
$\mathcal{U}(t)$	$\frac{1}{s}$
$t^n \mathcal{U}(t)$	$\frac{n!}{s^{n+1}}$
$\mathcal{U}(t - T_0)$	$\frac{e^{-sT_0}}{s}$
$e^{at} \mathcal{U}(t)$	$\frac{1}{s-a}$
$t^n e^{at} \mathcal{U}(t)$	$\frac{n!}{(s-a)^{n+1}}$
$\cos(bt) \mathcal{U}(t)$	$\frac{s}{s^2+b^2}$
$\sin(bt) \mathcal{U}(t)$	$\frac{b}{s^2+b^2}$
$e^{-at} \cos(bt) \mathcal{U}(t)$	$\frac{s+a}{(s+a)^2+b^2}$
$e^{-at} \sin(bt) \mathcal{U}(t)$	$\frac{b}{(s+a)^2+b^2}$
$re^{-at} \cos(bt + \theta) \mathcal{U}(t)$	$\begin{cases} a: & \frac{sr\cos(\theta)+ar\cos(\theta)-br\sin(\theta)}{s^2+2as+(a^2+b^2)} \\ b: & \frac{1}{2}\left(\frac{re^{j\theta}}{s+a-jb} + \frac{re^{-j\theta}}{s+a+jb}\right) \\ c: & \frac{As+B}{s^2+2as+c} \begin{cases} r & = \sqrt{\frac{A^2c+B^2-2ABa}{c-a^2}} \\ \theta & = \arctan\left(\frac{Aa-B}{A\sqrt{c-a^2}}\right) \end{cases} \end{cases}$
$e^{-at}\left(A\cos(\sqrt{c-a^2}t) + \frac{B-Aa}{\sqrt{c-a^2}}\sin(\sqrt{c-a^2}t)\right)\mathcal{U}(t)$	$\frac{As+B}{s^2+2as+c}$

D.6 Higher-Order Transforms

Time Domain	Frequency Domain
$x(t)$	$X(s)$
$x(t)\sin(\omega_0 t)$	$\frac{j}{2}\left(X(s + j\omega_0) - X(s - j\omega_0)\right)$
$x(t)\cos(\omega_0 t)$	$\frac{1}{2}\left(X(s + j\omega_0) + X(s - j\omega_0)\right)$
$t^n x(t)$	$(-1)^n \frac{d^n}{ds^n} X(s)\; n \in \mathbb{N}$
$\frac{d^n}{dt^n} x(t)$	$s^n X(s) - \sum_{0}^{n-1} s^{n-1-i} \frac{d^i}{dt^i} x(t)\rvert_{t=0^-}\; n \in \mathbb{N}$