The Search for a Title

A Profound Subtitle

Dr. John Smith

PUBLISHED BY PUBLISHER

BOOK-WEBSITE.COM

First printing, March 2019

Contents

I Part One

1 Text Chapter 9
1.1 Paragraphs of Text 9
1.2 Citation 10
1.3 Lists 10
1.3.1 Numbered List 10
1.3.2 Bullet Points 10
1.3.3 Descriptions and Definitions 10

2 In-text Elements 11
2.1 Theorems 11
2.1.1 Several equations 11
2.1.2 Single Line 11
2.2 Definitions 11
2.3 Notations 12
2.4 Remarks 12
2.5 Corollaries 12
2.6 Propositions 12
2.6.1 Several equations 12
2.6.2 Single Line 12
2.7 Examples 12
2.7.1 Equation and Text 12
2.7.2 Paragraph of Text 13

2.8 Exercises 13
2.9 Problems 13
2.10 Vocabulary 13

II Part Two

3 Presenting Information 17
3.1 Table 17
3.2 Figure 17

III Tor Specification

4 Preliminaries 21
4.1 Ciphers 21
4.1.1 Stream Cipher 21
4.2 Citation 23
4.3 Lists 23
4.3.1 Numbered List 23
4.3.2 Bullet Points 23
4.3.3 Descriptions and Definitions 23

5 In-text Elements 25
5.1 Theorems 25
5.1.1 Several equations 25
5.1.2 Single Line 25
5.2 Definitions 25
5.3 Notations 26
5.4 Remarks 26
5.5 Corollaries 26
5.6 Propositions 26
5.6.1 Several equations 26
5.6.2 Single Line 26
5.7 Examples 26
5.7.1 Equation and Text 26
5.7.2 Paragraph of Text 27
5.8 Exercises 27
5.9 Problems 27
5.10 Vocabulary 27

Bibliography 29
Articles 29
Books 29

Index 31

Part One

1 **Text Chapter** 9
1.1 Paragraphs of Text
1.2 Citation
1.3 Lists

2 **In-text Elements** 11
2.1 Theorems
2.2 Definitions
2.3 Notations
2.4 Remarks
2.5 Corollaries
2.6 Propositions
2.7 Examples
2.8 Exercises
2.9 Problems
2.10 Vocabulary

1. Text Chapter

1.1 Paragraphs of Text

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim.

Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

1.2 Citation

This statement requires citation [1]; this one is more specific [2, page 162].

1.3 Lists

Lists are useful to present information in a concise and/or ordered way[1].

1.3.1 Numbered List

1. The first item
2. The second item
3. The third item

1.3.2 Bullet Points

- The first item
- The second item
- The third item

1.3.3 Descriptions and Definitions

Name Description
Word Definition
Comment Elaboration

[1] Footnote example...

2. In-text Elements

2.1 Theorems

This is an example of theorems.

2.1.1 Several equations

This is a theorem consisting of several equations.

Theorem 2.1.1 — Name of the theorem. In $E = \mathbb{R}^n$ all norms are equivalent. It has the properties:

$$\big|\,||\mathbf{x}|| - ||\mathbf{y}||\,\big| \leq ||\mathbf{x}-\mathbf{y}|| \tag{2.1}$$

$$||\sum_{i=1}^{n} \mathbf{x}_i|| \leq \sum_{i=1}^{n} ||\mathbf{x}_i|| \quad \text{where } n \text{ is a finite integer} \tag{2.2}$$

2.1.2 Single Line

This is a theorem consisting of just one line.

Theorem 2.1.2 A set $\mathscr{D}(G)$ in dense in $L^2(G)$, $|\cdot|_0$.

2.2 Definitions

This is an example of a definition. A definition could be mathematical or it could define a concept.

Definition 2.2.1 — Definition name. Given a vector space E, a norm on E is an application, denoted $||\cdot||$, E in $\mathbb{R}^+ = [0, +\infty[$ such that:

$$||\mathbf{x}|| = 0 \;\Rightarrow\; \mathbf{x} = \mathbf{0} \tag{2.3}$$

$$||\lambda \mathbf{x}|| = |\lambda| \cdot ||\mathbf{x}|| \tag{2.4}$$

$$||\mathbf{x}+\mathbf{y}|| \leq ||\mathbf{x}|| + ||\mathbf{y}|| \tag{2.5}$$

2.3 Notations

Notation 2.1. *Given an open subset G of $\mathbb{R}^n$, the set of functions φ are:*

1. *Bounded support G;*
2. *Infinitely differentiable;*

a vector space is denoted by $\mathscr{D}(G)$.

2.4 Remarks

This is an example of a remark.

R The concepts presented here are now in conventional employment in mathematics. Vector spaces are taken over the field $\mathbb{K} = \mathbb{R}$, however, established properties are easily extended to $\mathbb{K} = \mathbb{C}$.

2.5 Corollaries

This is an example of a corollary.

Corollary 2.5.1 — Corollary name. The concepts presented here are now in conventional employment in mathematics. Vector spaces are taken over the field $\mathbb{K} = \mathbb{R}$, however, established properties are easily extended to $\mathbb{K} = \mathbb{C}$.

2.6 Propositions

This is an example of propositions.

2.6.1 Several equations

Proposition 2.6.1 — Proposition name. It has the properties:

$$\big|\,||\mathbf{x}|| - ||\mathbf{y}||\,\big| \leq ||\mathbf{x}-\mathbf{y}|| \tag{2.6}$$

$$||\sum_{i=1}^{n}\mathbf{x}_i|| \leq \sum_{i=1}^{n}||\mathbf{x}_i|| \quad \text{where } n \text{ is a finite integer} \tag{2.7}$$

2.6.2 Single Line

Proposition 2.6.2 Let $f, g \in L^2(G)$; if $\forall \varphi \in \mathscr{D}(G)$, $(f,\varphi)_0 = (g,\varphi)_0$ then $f = g$.

2.7 Examples

This is an example of examples.

2.7.1 Equation and Text

■ **Example 2.1** Let $G = \{x \in \mathbb{R}^2 : |x| < 3\}$ and denoted by: $x^0 = (1,1)$; consider the function:

$$f(x) = \begin{cases} \mathrm{e}^{|x|} & \text{si } |x-x^0| \leq 1/2 \\ 0 & \text{si } |x-x^0| > 1/2 \end{cases} \tag{2.8}$$

The function f has bounded support, we can take $A = \{x \in \mathbb{R}^2 : |x-x^0| \leq 1/2+\varepsilon\}$ for all $\varepsilon \in]0;5/2-\sqrt{2}[$. ■

2.7.2 Paragraph of Text

■ **Example 2.2 — Example name.** Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

■

2.8 Exercises

This is an example of an exercise.

Exercise 2.1 This is a good place to ask a question to test learning progress or further cement ideas into students' minds. ■

2.9 Problems

Problem 2.1 What is the average airspeed velocity of an unladen swallow?

2.10 Vocabulary

Define a word to improve a students' vocabulary.
Vocabulary 2.1 — Word. Definition of word.

Part Two

3 Presenting Information 17
3.1 Table
3.2 Figure

3. Presenting Information

3.1 Table

Treatments	Response 1	Response 2
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296

Table 3.1: Table caption

Referencing Table 3.1 in-text automatically.

3.2 Figure

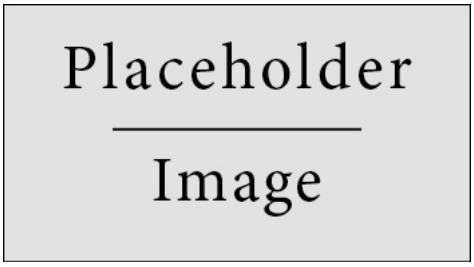

Figure 3.1: Figure caption

Referencing Figure 3.1 in-text automatically.

Tor Specification

4 Preliminaries 21
4.1 Ciphers
4.2 Citation
4.3 Lists

5 In-text Elements 25
5.1 Theorems
5.2 Definitions
5.3 Notations
5.4 Remarks
5.5 Corollaries
5.6 Propositions
5.7 Examples
5.8 Exercises
5.9 Problems
5.10 Vocabulary

Bibliography 29
Articles
Books

Index 31

4. Preliminaries

4.1 Ciphers

4.1.1 Stream Cipher

For stream ciphers Tor uses 128-bit AES in counter mode, with an IV of all 0 bytes.
Here we provide some notes about AES counter mode:

AES

AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware.

High-level description of the algorithm:

1. KeyExpantion: round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial round key addition:
   (a) AddRoundKey: each byte of the state is combined with a block of the round key using bitwise xor.
3. For 9, 11 or 13 rounds:
   (a) SubBytes: a non-linear substitution step where each byte is replaced with another according to a lookup table.
   (b) ShiftRows: a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
   (c) MixColumns: a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
   (d) AddRoundKey
4. Final round (making 10, 12 or 14 rounds in total):
   (a) SubBytes
   (b) ShiftRows
   (c) AddRoundKey

In cryptography, a block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block. A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block.

Counter mode encryption

The figure 4.1 will show a block cipher encryption with counter mode operation.

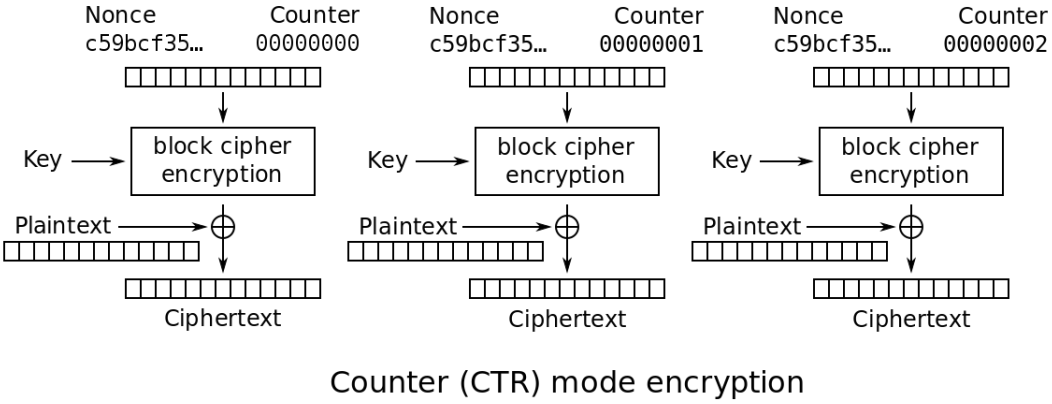

Figure 4.1: AES counter mode

Note that the nonce in this diagram is equivalent to the initialization vector (IV) in the other diagrams. However, if the offset/location information is corrupt, it will be impossible to partially recover such data due to the dependence on byte offset.

You can see details of counter mode in figure 4.2.

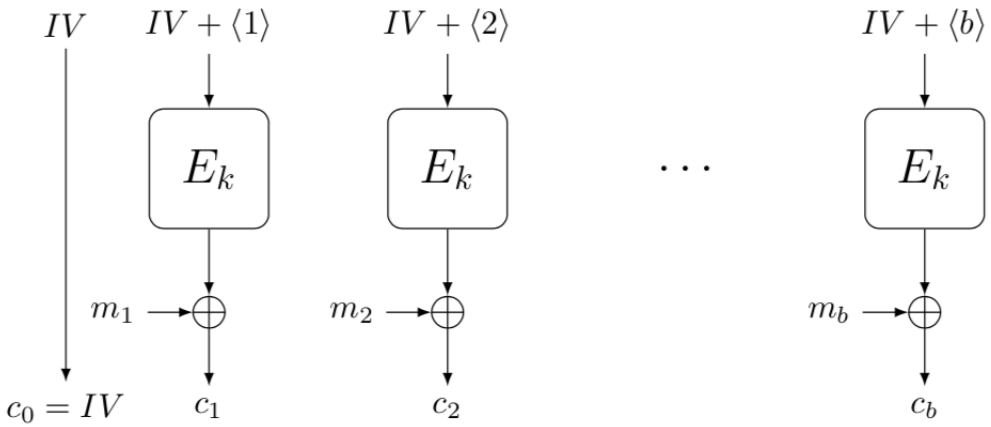

Figure 4.2: AES counter mode

At first, should choose an IV randomly from $\{0,1\}^n$ then the purpose is finding every c in this way:

$$c_i = m_i \oplus E(IV + < i >),\ i = 1,2,...,b$$

In the above equation $< i >$ will illustrate binary format for number i, also $IV + < i >$ is modular summation with the base of 2^n.
One of the advantages for CTR operation mode is that we can pararellize the encryption and decryption procedure in this mode.

4.2 Citation

This statement requires citation [1]; this one is more specific [2, page 162].

4.3 Lists

Lists are useful to present information in a concise and/or ordered way[1].

4.3.1 Numbered List

1. The first item
2. The second item
3. The third item

4.3.2 Bullet Points

- The first item
- The second item
- The third item

4.3.3 Descriptions and Definitions

Name Description
Word Definition
Comment Elaboration

[1] Footnote example...

5. In-text Elements

5.1 Theorems

This is an example of theorems.

5.1.1 Several equations

This is a theorem consisting of several equations.

Theorem 5.1.1 — Name of the theorem. In $E = \mathbb{R}^n$ all norms are equivalent. It has the properties:

$$\big|\,||\mathbf{x}|| - ||\mathbf{y}||\,\big| \leq ||\mathbf{x}-\mathbf{y}|| \tag{5.1}$$

$$||\sum_{i=1}^{n} \mathbf{x}_i|| \leq \sum_{i=1}^{n} ||\mathbf{x}_i|| \quad \text{where } n \text{ is a finite integer} \tag{5.2}$$

5.1.2 Single Line

This is a theorem consisting of just one line.

Theorem 5.1.2 A set $\mathscr{D}(G)$ in dense in $L^2(G)$, $|\cdot|_0$.

5.2 Definitions

This is an example of a definition. A definition could be mathematical or it could define a concept.

Definition 5.2.1 — Definition name. Given a vector space E, a norm on E is an application, denoted $||\cdot||$, E in $\mathbb{R}^+ = [0, +\infty[$ such that:

$$||\mathbf{x}|| = 0 \;\Rightarrow\; \mathbf{x} = \mathbf{0} \tag{5.3}$$

$$||\lambda \mathbf{x}|| = |\lambda| \cdot ||\mathbf{x}|| \tag{5.4}$$

$$||\mathbf{x}+\mathbf{y}|| \leq ||\mathbf{x}|| + ||\mathbf{y}|| \tag{5.5}$$

5.3 Notations

Notation 5.1. *Given an open subset G of $\mathbb{R}^n$, the set of functions φ are:*

1. *Bounded support G;*
2. *Infinitely differentiable;*

a vector space is denoted by $\mathscr{D}(G)$.

5.4 Remarks

This is an example of a remark.

R The concepts presented here are now in conventional employment in mathematics. Vector spaces are taken over the field $\mathbb{K} = \mathbb{R}$, however, established properties are easily extended to $\mathbb{K} = \mathbb{C}$.

5.5 Corollaries

This is an example of a corollary.

Corollary 5.5.1 — Corollary name. The concepts presented here are now in conventional employment in mathematics. Vector spaces are taken over the field $\mathbb{K} = \mathbb{R}$, however, established properties are easily extended to $\mathbb{K} = \mathbb{C}$.

5.6 Propositions

This is an example of propositions.

5.6.1 Several equations

Proposition 5.6.1 — Proposition name. It has the properties:

$$\big|\,||\mathbf{x}|| - ||\mathbf{y}||\,\big| \leq ||\mathbf{x}-\mathbf{y}|| \tag{5.6}$$

$$||\sum_{i=1}^{n}\mathbf{x}_i|| \leq \sum_{i=1}^{n}||\mathbf{x}_i|| \quad \text{where } n \text{ is a finite integer} \tag{5.7}$$

5.6.2 Single Line

Proposition 5.6.2 Let $f, g \in L^2(G)$; if $\forall \varphi \in \mathscr{D}(G)$, $(f,\varphi)_0 = (g,\varphi)_0$ then $f = g$.

5.7 Examples

This is an example of examples.

5.7.1 Equation and Text

■ **Example 5.1** Let $G = \{x \in \mathbb{R}^2 : |x| < 3\}$ and denoted by: $x^0 = (1,1)$; consider the function:

$$f(x) = \begin{cases} \mathrm{e}^{|x|} & \text{si } |x-x^0| \leq 1/2 \\ 0 & \text{si } |x-x^0| > 1/2 \end{cases} \tag{5.8}$$

The function f has bounded support, we can take $A = \{x \in \mathbb{R}^2 : |x-x^0| \leq 1/2+\varepsilon\}$ for all $\varepsilon \in]0;5/2-\sqrt{2}[$. ■

5.7.2 Paragraph of Text

■ **Example 5.2 — Example name.** Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris. ■

5.8 Exercises

This is an example of an exercise.

Exercise 5.1 This is a good place to ask a question to test learning progress or further cement ideas into students' minds. ■

5.9 Problems

Problem 5.1 What is the average airspeed velocity of an unladen swallow?

5.10 Vocabulary

Define a word to improve a students' vocabulary.
Vocabulary 5.1 — Word. Definition of word.

Bibliography

Articles

[1] James Smith. “Article title”. In: 14.6 (Mar. 2013), pages 1–8 (cited on pages 10, 23).

Books

[2] John Smith. *Book title*. 1st edition. Volume 3. 2. City: Publisher, Jan. 2012, pages 123–200 (cited on pages 10, 23).

Index

Citation, 10, 23
Corollaries, 12, 26

Definitions, 11, 25

Examples, 12, 26
    Equation and Text, 12, 26
    Paragraph of Text, 13, 27
Exercises, 13, 27

Figure, 17

Lists, 10, 23
    Bullet Points, 10, 23
    Descriptions and Definitions, 10, 23
    Numbered List, 10, 23

Notations, 12, 26

Paragraphs of Text, 9
Problems, 13, 27
Propositions, 12, 26
    Several Equations, 12, 26
    Single Line, 12, 26

Remarks, 12, 26

Table, 17
Theorems, 11, 25
    Several Equations, 11, 25
    Single Line, 11, 25

Vocabulary, 13, 27