Abstract AlgeBra Topic Notes

Textbook (TB) is:

Nicodemi, O., Sutherland, M. and Towsley, G. (2007). *An introduction to abstract algebra with notes to the future teacher*. Upper Saddle River, NJ: Pearson Prentice Hall.

Table of Contents

[(1) Induction and Divisibility (Summary) 3](#_Toc1413708)

[Numbers and Sets 3](#_Toc1413709)

[Arithmetic and Divisibility (1.2 of TB, pp. 9-15) 6](#_Toc1413710)

[Greatest Common Divisors and Euclid’s Algorithm 7](#_Toc1413711)

[(1) Induction and Divisibility 10](#_Toc1413712)

[Numbers and Sets 10](#_Toc1413713)

[Arithmetic and Divisibility (1.2 of TB, pp. 9-15) 16](#_Toc1413714)

[Greatest Common Divisors and Euclid’s Algorithm 23](#_Toc1413715)

[(2) Prime Numbers 33](#_Toc1413716)

[Chapter 1.4 Prime Numbers 33](#_Toc1413717)

[1.7 Theorems of Euler and Fermat 37](#_Toc1413718)

[(3) Relations and Congruence 40](#_Toc1413719)

[Euler-Phi Function Formulas 40](#_Toc1413720)

[Relations 40](#_Toc1413721)

[Congruence Modulo n 43](#_Toc1413722)

[The Ring [2.4] 45](#_Toc1413723)

[(4) Rings 46](#_Toc1413724)

[Linear Congruence Equations [2.1] 46](#_Toc1413725)

[Divisibility Tests [2.2] 52](#_Toc1413726)

[The Ring [2.4] 53](#_Toc1413727)

[Rings [2.5] 57](#_Toc1413728)

[(5) fields and Complex Numbers 59](#_Toc1413729)

[Rings [2.5] 59](#_Toc1413730)

[The Field of Complex Numbers [2.6] 63](#_Toc1413731)

[(6) Polynomials 66](#_Toc1413732)

[Polynomial over a Ring 66](#_Toc1413733)

[Rings 67](#_Toc1413734)

[Polynomial Arithmetic 67](#_Toc1413735)

[Polynomial as an Integral Domain 67](#_Toc1413736)

[Polynomial over a field 68](#_Toc1413737)

[Division Algorithm 68](#_Toc1413738)

[Remainder Theorem 68](#_Toc1413739)

[Root Theorem 69](#_Toc1413740)

[Maximum Roots 69](#_Toc1413741)

[Units 70](#_Toc1413742)

[Euclidean Algorithm 70](#_Toc1413743)

[Irreducible and Reucible Polynomials 71](#_Toc1413744)

[Fundamental Theorem of Arithmetic 71](#_Toc1413745)

[(7) Fundamental Theorem of Algebra 72](#_Toc1413746)

[The Fundamental Theorem of Algebra 72](#_Toc1413747)

[Rings 73](#_Toc1413748)

[Polynomial Arithmetic 73](#_Toc1413749)

[Polynomial as an Integral Domain 73](#_Toc1413750)

[Polynomial over a field 74](#_Toc1413751)

[Division Algorithm 74](#_Toc1413752)

[Remainder Theorem 74](#_Toc1413753)

[Root Theorem 75](#_Toc1413754)

[Maximum Roots 75](#_Toc1413755)

[Units 76](#_Toc1413756)

[Euclidean Algorithm 76](#_Toc1413757)

[Irreducible and Reucible Polynomials 77](#_Toc1413758)

[Fundamental Theorem of Arithmetic 77](#_Toc1413759)

[(8) Groups 77](#_Toc1413760)

[(9) Supgroups 77](#_Toc1413761)

[(10) Homomorphisms 77](#_Toc1413762)

[(11) RSA 77](#_Toc1413763)

# (1) Induction and Divisibility (Summary)

Week 1 Material | Due Tue. 6 March

## Numbers and Sets

Number theory mostly concerns the:

### Number Sets

Numbers can be categorised into various sets:

(Positive Integers) {1, 2, 3, 4, 5 …}

(Natural Numbers) {0, 1, 2, 3, 4, 5 …}

(Integers) {…, -3, -2, -1, 0, 1, 2, 3 …}

(Rational Numbers) {

(Real Numbers) {Any point on the Real Line}

(Complex Numbers) {Any point on the Complex Plane}

#### Subset Notation[[1]](#footnote-1)

Observe the following definitions:

|  |  |  |
| --- | --- | --- |
| ***Subset Symbol*** |  | A contains some elements of B |
| ***Proper Subset Symbol*** |  | P Contains some or all elements of Q |
| ***Subset, but not equal*** |  | M contains some elements of N, but not all elements |

Hence observe the relationship of the number sets:

### Set Orders

The Natural numbers have an intuitive order:

As do the real numbers:

However, the Complex Plane does not have any intuitive order because the numbers do not exist on a line where by mathematical operations can be seen as a symmetrical transformation of that line, but rather a plane, hence the order may become somewhat arbitrary[[2]](#footnote-2)

#### The Well-Ordering Principle (WOP)

The Well-Ordering Principle is an axiom that states:

*If,*

*a set contains only natural numbers, and*

*the set isn’t empty*

*then,*

*One of those elements is the smallest*

So, every set of natural numbers has a smallest member (except the empty-set).

While we can’t necessarily know what that smallest value is, we are guaranteed that it exists.

#### Sets of Integers

The *Well-Ordering Principle* doesn’t necessarily apply to other sets, e.g. integers, by negation, observe:

For any least element value:

There will exist

Thus the set of Integers does not have a least value and the *WOP* doesn’t apply.

Extra constraints applied would allow the *WOP* to apply, e.g. the *WOP* would apply to this set:

for

### Mathematical Induction

#### Summary

Mathematical Induction is a principle that provides:

A statement is true if:

1. The first statement is true,
2. Given one statement is true then so is the next

If these are both true, then all the statements are true.

#### Example

It is true that: all the dominoes fall down if:

1. It is true that: the first domino falls down
2. It is true that: one domino will always knock over the next

Thus, if the dominoes knock one another down and the first falls over, then all dominoes would fall over.

#### In Mathematical Terms

Let be a statement about an integer , this statement is true for all if:

1. is true, and:

## Arithmetic and Divisibility (1.2 of TB, pp. 9-15)

What’s important here, is the division algorithm, which states:

If an integer is divided by a natural number , the division algorithm guarantees there will be a remainder that lies between 0 and

Although this is a simple and somewhat obvious statement, it underlies all later proofs.

As a matter of fact most later proofs could be considered corollaries[[3]](#footnote-3) of the division algorithm.

### Properties of the Integers (p. 10)

The Integers satisfy 6 mathematical properties:

1. Addition and multiplication are **associative:**
2. Addition and multiplication are **commutative**
3. There always exists a unique **additive identity** 0
   1. there exists 0 :
4. There exists a unique **multiplicative identity 1**
   1. there exists 0 :
5. Every integer has an additive inverse:
   1. there exists :
6. Addition and multiplication satisfy the **distributive law**

### Divisibility Definition (p. 11)

Let and be integers with :

**divides** if there is another integer () such that :

When divides this is the same as:

* is **divisible** by
* is a **multiple** of

### Divisibility properties

### Division Algorithm

#### Definition

Let and be any integers with .

There are unique integers and such that , where

i.e.

## Greatest Common Divisors and Euclid’s Algorithm

### Definition

Suppose and are nonzero integers, the *greatest common divisor* of and is the largest integer that divides both of them and is denoted:

1. is undefined because it would be
2. ; because any number divides and the largest number that divides is itself
   1. unless , in which case it would be like #1 above.
3. ; because the divides both terms and is the largest possible divisor of .

#### Theorem 1 (p. 16)

If

Then is the smallest positive integer that can be expressed in the form:

##### Corollary

Observe further, that for , these two statement are wholly equivalent

i.e.

### Relatively Prime

#### Definition

Suppose and are non-zero integers, they are *relatively prime* (i.e. *coprime*) if

#### Proposition; Relatively prime by GCD

Suppose and are non-zero integers, and let ;

Then and are relatively prime.

### Theorem; Euclids Lemma[[4]](#footnote-4) (p. 18)

##### Definition

Suppose are integers such that and are coprime.

If is a multiple of ,

Then must be a multiple of

(because was prime)

### Theorem; gcd Becomes remainder and factor(proposition 6 - p. 18)

##### Definition

Suppose are all integers, such that:

Then,

### Euclid’s Algorithm (i.e. calculating gcd’s) (p. 19)

*Euclid’s Algorithm* allows for a method to find *greatest common denominators:*

For two positive natural numbers, such that

1. write in the form of , where with
2. If , then and hence
3. If , then
   1. Now repeat from step 1 over and over

Euclid’s Algorithm allows for a method to find greatest common denominators:

### Lowest Common Multiples

For two integers , the *Lowest Common Multiple*, is the smallest integer that is a multiple of both and

The *lcm* is a number that is the smallest possible multiple of other numbers

##### Finding the LCM

In order to find the lcm:

# (1) Induction and Divisibility

Week 1 Material | Due Tue. 6 March

## Numbers and Sets

Number theory mostly concerns the:

### Number Sets

Numbers can be categorised into various sets:

(Positive Integers) {1, 2, 3, 4, 5 …}

(Natural Numbers) {0, 1, 2, 3, 4, 5 …}

(Integers) {…, -3, -2, -1, 0, 1, 2, 3 …}

(Rational Numbers) {

(Real Numbers) {Any point on the Real Line}

(Complex Numbers) {Any point on the Complex Plane}

#### Subset Notation[[5]](#footnote-5)

Observe the following definitions:

|  |  |  |
| --- | --- | --- |
| ***Subset Symbol*** |  | A contains some elements of B |
| ***Proper Subset Symbol*** |  | P Contains some or all elements of Q |
| ***Subset, but not equal*** |  | M contains some elements of N, but not all elements |

Hence observe the relationship of the number sets:

### Set Orders

The Natural numbers have an intuitive order:

As do the real numbers:

However, the Complex Plane does not have any intuitive order because the numbers do not exist on a line where by mathematical operations can be seen as a symmetrical transformation of that line, but rather a plane, hence the order may become somewhat arbitrary[[6]](#footnote-6)

#### The Well-Ordering Principle (WOP)

The Well-Ordering Principle is an axiom that states:

*If,*

*a set contains only natural numbers, and*

*the set isn’t empty*

*then,*

*One of those elements is the smallest*

So, every set of natural numbers has a smallest member (except the empty-set).

While we can’t necessarily know what that smallest value is, we are guaranteed that it exists.

#### Sets of Integers

The *Well-Ordering Principle* doesn’t necessarily apply to other sets, e.g. integers, by negation, observe:

For any least element value:

There will exist

Thus the set of Integers does not have a least value and the *WOP* doesn’t apply.

Extra constraints applied would allow the *WOP* to apply,

e.g. the *WOP* would apply to this set:

### Mathematical Induction

#### Summary

Mathematical Induction is a principle that provides:

A statement is true if:

1. The first statement is true,
2. Given one statement is true then so is the next

If these are both true, then all the statements are true.

#### Example

It is true that: all the dominoes fall down if:

1. It is true that: the first domino falls down
2. It is true that: one domino will always knock over the next

Thus, if the dominoes knock one another down and the first falls over, then all dominoes would fall over.

#### In Mathematical Terms

Let be a statement about an integer , this statement is true for all if:

1. is true, and:

##### Logical If-Then Statement

When trying to utilise mathematical induction, it is necessary to prove the second statement to do this:

Assume that is true and then prove that is true

Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
￼
￼
￼
￼
￼￼￼￼￼
￼￼￼￼
￼￼￼￼
￼
If that is shown, the ‘if-then’ statement cannot be false:

#### Proof of Mathematical Induction

##### Pre-requisite Theory

We will prove this statement by way of contradiction, recall basic logical statements:

Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
Ink Drawings
￼
￼
￼
￼
￼
￼￼￼￼
￼￼
￼￼
￼￼
￼￼￼
￼￼
￼
￼￼￼
￼
￼￼￼
￼￼￼￼
￼￼￼￼
￼￼￼￼
￼
Ink Drawings


A Contradiction implies the negation of a tautology,[[7]](#footnote-7) a tautology is a statement which is always true.[[8]](#footnote-8)

###### Proof of Negation vs Proof by Contradiction[[9]](#footnote-9)

Proof by Negation is an inference rule which explains:

To prove assume and then derive absurdity

Proof by Contradiction is a different rule that explains

To prove assume and derive absurdity.

##### Proof of Mathematical Induction

###### Abstract form of Mathematical Induction

The abstract form of mathematical induction provides that:

For any , if:

1. , and

then

###### Proof by Contradiction

To prove that our set is equal to the set of all natural numbers we will prove by contradiction, so we will define such that properties 1 and 2 apply and assume that and derive absurdity:

Suppose ,

If , there must exist some element such that

Let T be the set of all natural numbers that aren’t in S:

This would mean that T is non empty because there must be some element :

The *Well Ordered Principle* implies that there must be some smallest element in T, say .

However property 1 provides that 0 is in and hence it mustn’t be in :

Now because , it must be a non negative number and hence:

Given than is the least element of we also know that:

Thus we know that:

Also from Property 2 we know that if is in S, then + 1 must be in S:

However we know that when is defined as not containing elements of S.

Thus the only way, for to be true is if element is simultaneously in and not in , this is absurd, thus

***Q.E.D***

## Arithmetic and Divisibility (1.2 of TB, pp. 9-15)

What’s important here, is the division algorithm, which states:

If an integer is divided by a natural number , the division algorithm guarantees there will be a remainder that lies between 0 and

Although this is a simple and somewhat obvious statement, it underlies all later proofs.

As a matter of fact most later proofs could be considered corollaries[[10]](#footnote-10) of the division algorithm.

### Properties of the Integers (p. 10)

The Integers satisfy 6 mathematical properties:

1. Addition and multiplication are **associative:**
2. Addition and multiplication are **commutative**
3. There always exists a unique **additive identity** 0
   1. there exists 0 :
4. There exists a unique **multiplicative identity 1**
   1. there exists 0 :
5. Every integer has an additive inverse:
   1. there exists :
6. Addition and multiplication satisfy the **distributive law**

#### Example application of integer rules

**Prove**

To prove this we will manipulate only with the rules of integers and the principle that changing both sides of an equation in the same way preserves the equality relationship.

First start with the proposition:

Now multiply both sides by 0:

Property 3 provides that , so we will substitute that on the left hand side:

Property 2 allows the terms to be commutated

Property 6 allows the equation to be Distributed:

Property 5 provides that every value has an additive inverse, in this case we will take the additive inverse of and add it to both sides of our equation:

Property 1 allows the terms to be rearranged:

Property 5 allows us to replace the with its sum 0:

Property 5 allows us to replace with just :

Now we have the relationship that we want to prove,

Every integer, multiplied by zero, given the properties of integers, must be equal to .

Q.E.D

The whole point of this, is when we encounter other number systems or mathematical objects that share these properties the proofs will transfer directly, reflect on the 10 axioms of a vector and how this same proof could apply.

### Divisibility Definition (p. 11)

Let and be integers with :

**divides** if there is another integer () such that :

When divides this is the same as:

* is **divisible** by
* is a **multiple** of

### Divisibility properties

##### Proof

Observe that:

and

Now via substitution

Sub

##### Proof

Observe that:

and

|  |  |  |  |
| --- | --- | --- | --- |
| Let | | | Let |
|  | | | |
|  |  |  | |
| Let  By the division algorithm | | | |

### Division Algorithm

#### Definition

Let and be any integers with .

There are unique integers and such that , where

i.e.

#### Proof (p. 13)

There are two elements of this definition and hence proof:

1. actually exist such that
2. are unique (i.e. There is only one solution.

##### 1. Existence

Let be the set of positive remainders from and defined thusly:

Example:

For example, if and , various values of can be used to generate an infinite number of values:

So the set would be

Observe this set would look like this:

All the remainders are whole positive numbers thus:

and because 0 is allowed to be a remainder:

One of the remainder values must be the smallest value (this is the *Well-Ordering Principle),* let this smallest value be :

Because is in S, a corresponding a value can be solved:

Let and both values and have been proven to exist.

Now we need to show that :

Because every remainder value is a positive value:

Assume that :

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
|  |  | is an arbitrary natural number, thus |
| Because it must be:  However is the least element of …  cannot contain as it’s least element and also contain , therefore the initial assumption of must be false and thus: | | |

So we have:

Now that we have proven that and exist such that we must prove there uniqueness

##### 2. Uniqueness

###### Method

It must be shown that if:

|  |  |
| --- | --- |
| , and | , and |

Then:

and

###### Proof

Thus observe,

|  |  |
| --- | --- |
|  |  |

Hence and are multiples of .

|  |  |
| --- | --- |
| **If**  Observe that:  Also  Hence, | **If**  Observe that:  Also  Hence, |
| The only multiple of in this range is 0, thus:  Further observe that:  and  Means that | |

Thus,

If and be are integers with , then there must exist unique integers and such that , where .

Q.E.D.

## Greatest Common Divisors and Euclid’s Algorithm

### Definition

Suppose and are nonzero integers, the *greatest common divisor* of and is the largest integer that divides both of them and is denoted:

1. is undefined because it would be
2. ; because any number divides and the largest number that divides is itself
   1. unless , in which case it would be like #1 above.
3. ; because the divides both terms and is the largest possible divisor of .

#### Theorem 1 (p. 16)

If

Then is the smallest positive integer that can be expressed in the form:

##### Proof

Assume and

Thus we know that and

Hence (by the *Well-Ordered Principle*), has a least element, we will let that be .

*We are trying to prove that*

We know that , thus it must be such that:

for

###### Show and (i.e. it’s a common divisor)

Assume is false, then it must be such that:

where

By simplification:

Let and , observe that and substitute:

Observe that this would imply that and from before :

is not the least element of

So the assumption that being false leads to not being the least element of , which we defined it as, thus it must be such that is true.

This same reasoning provides that

###### Show is the greatest value

So now we know that is a common divisor of both and , observe that must be the largest common divisor:

Suppose is a common divisor of and , we know that for :

Observe that is the least value of the set of all such combinations, thus:

###### Conclusion

Given values of :

If is the smallest possible combination of:

Then:

1. is a common divisor of and
2. is the smallest common divisor

i.e.

##### Corollary

Observe further, that for , these two statement are wholly equivalent

i.e.

###### Proof

We know that:

Prove

Show that if statement 1 is true then statement 2 is true:

We know that and , thus:

Prove

Show that if statement 2 is true then statement 1 is true:

Let ;

Q.E.D.

Conclusion

if and only if can be expressed as a linear combination of and then is a multiple of the greatest common denominator of and

### Relatively Prime

#### Definition

Suppose and are non-zero integers, they are *relatively prime* (i.e. *coprime*) if

#### Proposition; Relatively prime by GCD

Suppose and are non-zero integers, and let ;

Then and are relatively prime.

##### Proof

We know that for some

Thus if , then

#### Theorem; Euclids Lemma[[11]](#footnote-11) (p. 18)

##### Definition

Suppose are integers such that and are coprime.

If is a multiple of ,

Then must be a multiple of

(because was prime)

##### Proof

We know that, for some

To prove this we must assume that is a multiple of and show that this implies is a multiple of :

If , then, for some :

Now observe that for :

Let

#### Theorem; gcd of linear combination is gcd of remainder and factor(proposition 6 - p. 18)

##### Definition

Suppose are all integers, such that:

Then,

##### Proof

Let:

|  |  |
| --- | --- |
|  |  |

If we can show that ; the proof is complete.

Take some , thus:

So and , thus , therefore

Take some

So and , thus , therefore

Conclusion

Because:

Thus the

#### Euclid’s Algorithm (i.e. calculating gcd’s) (p. 19)

*Euclid’s Algorithm* allows for a method to find *greatest common denominators:*

For two positive natural numbers, such that

1. write in the form of , where with
2. If , then and hence
3. If , then
   1. Now repeat from step 1 over and over

##### Exercises

Find the *greatest common denominator* of 27 and 6:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | |  | |  | |
|  |  | |  | |  |  |  |
|  | |  | |  | |
|  |  | |  | |  |
|  | |  | |  | |

the *greatest common denominator* is 3.

#### Lowest Common Multiples

For two integers , the *Lowest Common Multiple*, is the smallest integer that is a multiple of both and

The *lcm* is a number that is the smallest possible multiple of other numbers

##### Example

Take and as a combination of prime values:

Such that:

Then

From this observe:

##### Finding the LCM

In order to find the lcm:

##### Proof

We are trying to prove that:

Let

For some :

Observe that:

Now let

If we show that now must equal the proof is complete:

Show that e is a **common multiple**

Observe that:

|  |  |
| --- | --- |
|  |  |

Thus is a common multiple

Show e is the **least** common multiple

Suppose that is any positive common multiple of and , if we can show that is always less than , then must be the least common multiple and the proof is complete.

Given that is a common multiple of and we know that (for some :

|  |  |
| --- | --- |
|  |  |

So now we know that and also , thus by *Euclid’s Lemma:*

Thus, for some ,

Now, given that:

We know that , hence:

Thus is the lowest common denominator Q.E.D

# (2) Prime Numbers

Week 2 Material | Due Tue. 13 March

## Chapter 1.4 Prime Numbers

### Definitions

A prime number is any number :

A composite number is any number :

* is not prime

Observe that 1 is neither prime nor composite, this is important for later.

### Infinite Primes (theorem 1) p. 27

#### Summary

There are infinite prime numbers

#### Proof

Suppose;

Is the set of the first prime numbers,

Let:

Observe that would not be a multiple of any value

*Although this does not mean q is necessarily prime (primes can be much more difficult to generate), is possibly a composite of primes not in , but regardless, is not divisible by any .*

Thus cannot contain all primes.

Observe likewise, no set could be constructed such that it contained all primes.

Therefore, the set of all prime numbers must not be finite (i.e. there are infinite primes).

### Primes of Multiples (Proposition 2) p. 28

If a prime number divides a composite, it must divide one of the factors of that composite number

#### Summary

is a prime number if and only if:

#### Proof

Suppose is a prime number:

Either divides or it does not:

|  |  |
| --- | --- |
| If divides | If does not divide |
| , thus  the proof is complete | , thus  Because and  Then by Euclids Lemma:  Thus,  The proof is complete |

Thus:

### Primes Factors (Proiposition 3) p. 28

#### Summary

Suppose is prime and divides

Then divides :

Moreover, if is prime, then

#### Proof

There is no need for a proof because it is reasonably self explanatory

### The Fundamental Theorem of Arithmetic (Theorem 4), p. 28

#### Summary

For any integer :

1. The above factorisation of is unique to the value of

#### Proof

The proof is provided on p. 28 of the TB,[[12]](#footnote-12) it’s a little dense though, I haven’t reproduced it.

It is somewhat obvious that a number can be broken up into factors and those factors broken further up into factors and so on until prime values are reached.

What is less clear to necessarily demonstrated is that the factorisation must be unique for every value.

### Rational Numbers, (Corollary 5), p. 29

Every rational number can be expressed in a lowest form of relatively prime integers

#### Summary

Every rational number can be expressed uniquely as ,

Where :

#### Proof

No proof is provided for this

### (Theorem 6) p. 29

The square root of 2 is an irrational number

#### Summary

#### Proof

Suppose and ,

We know that

Thus to prove by contradiction it must be shown that:

because then and are not relatively prime and hence

##### Show

Observe,

So

Thus

##### Show

##### Conclusion

Thus because a rational number ) that is assumed to be such that

Is found to be impossible to express as a ratio of two relatively prime integers,

must not be a rational number

Because all rational numbers can be expressed as the ratio of two relatively prime integers.

## 1.7 Theorems of Euler and Fermat

### Euler- Function

The *Euler phi-function* counts the number of integers relatively prime to that are less than ,

#### Definition

For ;

is the number of positive integers less than or equal to that are relatively prime to .

e.g.

2, 3, 7 are relatively prime to 10, thus,

### Powers of Euler-Phi Function (Proposition 1 p. 43

#### Summary

If is prime and ,

#### Proof

All the numbers between and are relatively prime to , thus .

All integers less than (for are relatively prime to except for multiples of

i.e. all values less than are relatively prime except for .

So there are exactly multiples of that are multiples and hence not relatively prime.

Thus there is a total of numbers between and that are relatively prime to .

### Multiplicative Functions (Definition 2) p. 44

Some function is multiplicative if:

### Euler-Phi Function is Multiplicative

#### Summary

For positive relatively prime integers and :

#### Proof

The Proof is on page 44.

### cOROLLARY (P. 31 OF lECTURE sLIDES)

For primes and ,

Given some value:

Then the Euler Phi function is:

Further it follows:

### Eulers Theorem (Theorem 3) p. 45

#### Summary

For relatively prime integers and :

#### Proof

The proof is on page 45 of the TB.

### Fermats Little Theorem (p. 46)

The special case of *Euler’s Theorem*, when is prime, is known as *Fermat’s Little Theorem*.

#### Summary

For some prime and integer :

#### Proof

|  |  |
| --- | --- |
| If  Then | If  Then and are relatively prime, thus, *Eulers Theorem* applies;  Then by *Eulers Theorem*: |
| Thus for a prime and integer : | |

# (3) Relations and Congruence

Week 3 Material | Due Tue. 20 March

## Euler-Phi Function Formulas

### Eulers Theorem (Theorem 3) p. 45

#### Summary

For relatively prime integers and :

#### Proof

The proof is on page 45 of the TB.

### Fermats Little Theorem (p. 46)

The special case of *Euler’s Theorem*, when is prime, is known as *Fermat’s Little Theorem*.

#### Summary

For some prime and integer :

## Relations

A relation on a set is a subset of the cartesian product:

If we write that .

### Example

If we had the Relation < on the set

The cartesian product would be:

The set corresponding to the relation < would be:

And we would write each that satisfies the relation:

### Relation Properties

* **Reflexive** relations are relations where
* **Symmetric** relations are such that
* **Transitive** relations are such that

An equivalence relation is a relation that is relflexive, symmetric and transitive

#### Example 1

Let

We will define a relation as satisfied it those people share the same parents.

Define a relation:

if has the same parents as

Observe the following properties:

* **Reflexivity;** any person will be related to themselves because they share the same parents
* **Symmetry;** if Percy is related to Fred, then they share parents and hence then Fred must be related to Percy
* **Transitivity;** if Percy is related to Fred and Fred is Related to Ron, Ron and Percy must share parents, thus Ron and Percy are Related.

This is thus an **equivalence** relation.

#### Example 2

Let be all real numbers.

Define a relation:

if

Observe the following properties:

* **Non-Reflexive;** any number is not less than its own value.
* **Non-Symmetry:** take 5 and 7, if then
* **Transitive;** It is true that if, say, and then
  + This property is why we ordinarily write ,
    - Be careful, you can make transcription errors using greater than symbols.

Because the relation is not reflexive and not symmetrical this is not an equivalence relation.

### Equivalence class

Given a relation on some set ,

If , is the set of all elements of that satisfy the relation for :

This is called the *equivalence class of with respect to*

#### Example

Let be all real numbers.

Define a relation:

if

Let’s find the equivalence class of

#### Proposition

Let R be an equivalence relation on A:

If , then either,

* , OR

So if and are both elements of , then their equivalence classes are identical or absolutely different.

## Congruence Modulo n

Let and

We say that:

and are *congruent modulo n*  if

And it is expressed:

Or in other words:

Further Notation;

Generally, the notation:

Refers to the remainder after has been divided by (i.e. the residue of modulo )

So be careful:

|  |  |
| --- | --- |
| ***A number*** | ***A statement about divisibility*** |
|  |  |

### Division Algorithm

If then

Recall from the *Euclids Algorithm*

If , then

This translates to:

If then

### Eulers Theorem and Fermats Theorem

These can now be restated:

### Eulers Theorem (Theorem 3) p. 45

#### Summary

For relatively prime integers and :

#### Proof

The proof is on page 45 of the TB.

### Fermats Little Theorem (p. 46)

The special case of *Euler’s Theorem*, when is prime, is known as *Fermat’s Little Theorem*.

#### Summary

For some prime and integer :

### Residue of modulo (i.e. remainder of division algorithm)

If and

Then if and only if and have the same remainder when divided by .

If the remainder is then:

(i.e. )

This value is known as the *residue of modulo* and can always be found to exist.

### Mod laws

Let and and



### Congruence Class

Let and

The congruence class of modulo is expressed as

It is the equivalence class of whereby the relation is a congruence in modulo

So in mathematical terms, the congruence class of is :

e.g.

Observe here that

Observe:

Here the residue modulo n is 1, i.e.

The between and any element of the congruence class is divisible by .

## The Ring [2.4]

A ring is the set of all congruence classes less than such that:

### Example

We could list all the congruence classes of :

Where:

Hence, could be expressed equivalently as:

### Operations on Congruence Classes

The elements of can be manipulated algebraically, they have an algebraic structure.:

For :

#### Addition

Addition is commutative and associative:

#### Multiplication

Multiplication is commutative and associative:

#### Linear Combination

Addition and multiplication can be combined:

# (4) Rings

Week 4 Material | Due Tue. 27 March

## Linear Congruence Equations [2.1]

A linear congruence equation is of the form:

Where and are fixed numbers and is a variable.

So an example could be:

The solution to this equation is the set of all values for which the expression is true.

#### Congruence Class

If some is a solution of a linear congruence equation, then all members of the congruence class ( are also solutions as well.

The complete set of solutions is the congruence class .

#### Testing Whether a Solution exists

A linear congruence equation only has a solution, if and only if:

##### Example

has **no** solution because

has a solution because

has a solution **only if**

#### Quick Solution for Multiples

If then,

##### Example

Solve,

thus

Thus we know that the difference between x and 1 is always divisible by 3, so:

So our solutions, is the congruence class:

Test the Solution

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

### General Method for Solving Linear Congruence Equation

Consider the equation , where

* Is there a solution for
  + There is because
* A solution can thus be found using the Euclidean Algorithm
* If is a solution to the equation, then the complete set of solutions is
  + This is proven on p. 64 of the TB
  + Although all elements of are solutions, the set may not contain all the solutions.

#### Example 1 (Euclidean Algorithm)

Give the complete set of solutions to

First observe that , thus there is a solution for .

If is an integer solution, then:

The values of and can be solved via the *Euclidean Algorithm* by using back substitution.

##### Euclidean Algorithm

We are concerned with , because that’s what our variables are multiplied by:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **(1)**  **(2)**  **(3)**  **n/a** |

Now recall that we are trying to find the values of and :

We will solve for in terms of 34 and 60, because we will be able to multiply by a factor of afterwards and have all integer solutions.

##### Backward Substitution

**State (3)**

**Sub (2)**

**Sub (1)**

**Multiply by**

##### Solve for and

Thus,

Hence,

And,

##### Conclusion

Thus a solution is

The set of all solutions is:

Where:

* is the modulo
* is the solution to

Thus the solution set for is the congruence class:

#### Example 2 (Multiplicative Inverse)

Solve

In this case because , we can solve this using a multiplicative inverse as an alternate method.[[13]](#footnote-13)

The multiplicataive inverse cannot be solved for when

What we are looking for, is a multiplicative inverse, we will call it , such that:

When we find , we expect that:

Now, if:

Then:

##### Euclidean algorithm

Now use Euclids Algorithm on 17 and 29:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **(1)**  **(2)**  **(3)**  **(4)**  **n/a** |

##### Backwards Substitution

So our goal is to find :

State (4)

Sub (3)

Sub (2)

Sub (1)

Now;

Thus we have shown that:

##### Solve for

The original question is:

Thus is a solution, hence the residue is a solution:

##### Conclusion; Solve for the Set of Solutions

The complete set of solutions is the congruence class:

Where is the modulo and :

## Divisibility Tests [2.2]

It is possible to test for divisibility by 9 or 3 by summing the components, e.g.:

This can be generalised into a theorem:

An integer (in decimal notation) is divisible by 9 if and only if is divisible by 9.

### Proof

First observe that any integer can be expressed as a sum of its unit values (e.g.

Now utilise the fact that :

Now we know that , thus

### In terms of 3

Observe that ; hence the same rules apply for the value of 3, and a similar proof.

## The Ring [2.4]

For , it is defined:

### Example

Recall that:

Hence,

### Algebra in

In order to do algebra in we need to manipulate elements of

Take

#### Addition

We define:

Because:

##### Addition in is Commutative

This has the consequence that addition in is commutative:

#### Multiplication

We define:

Because:

##### Multiplication in is Commutative

This has the consequence that addition in is commutative:

#### Multiplicative Inverses

Any value is a multiplicative inverse in if it is such that:

Any will have a multiplicative inverse if and only if:

##### Example

Take

All the possible element multiplication that could be done in :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  | 3 |
|  |  |  |  | 0 |
|  | 1 |  | 3 | 3 |
|  |  |  |  | 2 |
|  |  |  |  | 1 |

In this case observe that, in

### Solving the Multiplicative Inverse in

Solve the multiplicative Inverse of 19 in .

First, a multiplicative inverse exists if and only if :

So we want to find some value :

So now we have a linear congruence equation, use the method above to solve for and you have the multiplicative inverse.

## Rings [2.5]

### Definition and Axioms

A ring is a set R that has two operations:

* Addition (+)
* Multiplication (

And satisfies the axioms of a ring:

1. Associativity of Addition
2. Commutativity of Addition
3. Additive Elements Exists
4. Additive Inverse Exists
   1. (
   2. This can be equivalently written:
5. Associativity of Multiplication
6. Distributivity of Multiplication over Addition
   1. AND,

### Further Axioms

The following axioms are not necessarily exhibited by rings, but if they are the rings are given special names.

1. Commutativity of Multiplication
   * 1. A ring that satisfies this property is called a **commutative ring**
2. Existence of a Multiplicative identity Element (A ring with Unity)
   * 1. A ring that satisfies this property is called a **ring with identity** or equivalently a **ring with unity**
        1. The multiplicative identity element () is called the **unity** of the ring.

A ring that satisfies 7 and 8 is called a **commutative ring with identity/unity**.

#### Examples of Rings

* is not a ring, because there is no additive inverse
* are all commutative rings with identity/unity
* The set of all even integers () is a ring because
  + It is closed under addition and multiplication
  + It satisfies all other axioms
  + It is a commutative ring
  + Because 1 is not even there is no multiplicative identity, hence it is NOT a ring with unity/identity.
* Square matrices are rings with unity/identity
  + They are not commutative because the order of multiplication is important.

### Properties of Rings

Proofs for these properties are provided in the lecture notes and textbook:

#### Unique Identities

* The additive identity of a ring is always unique
* The additive inverse of a ring is always unique
* The multiplicative identity of a ring is always unique (i.e. if the ring has a multiplicative inverse).

#### Algebraic Rules

The following rules hold for rings:

Let

* 1. Assuming a multiplicative identity exists for the ring .

# (5) fields and Complex Numbers

Week 5 Material | Due Tue. 3 April 2018

## Rings [2.5]

### Zero Divisors

An element of some ring R is a **zero divisor** if:

OR

#### Examples

Take

in

Hence, 2 and 3 are both **zero divisors**

### Units

An element , of some ring is a **unit** if:

The element always has a multiplicative inverse, i.e.

* 1 is a unit of all rings
* Any ring with unity/identity is such that -1 is a unit
  + Because

#### Examples

|  |  |
| --- | --- |
| * in is a unit * is a unit * In :   + is a unit   + is a unit   + is a unit   + is a unit | In any is a unit because: |

#### Application

If is a unit, then the equation:

Can be solved by multiplying both sides by

##### Example

For there exists an inverse:

3 is a unit because there exists 5 such that:

Hence,

### Unit or Zero Divisor not Both

An element cannot be both a zero divisor and a unit,

Because the prior multiplies to give zero and the latter multiplies to give 1

### Integral Domain

An integral domain is a ring that:

1. Is commutative
2. Is with unity/identity
3. Has no zero divisors

#### Property of Integral Domain

In an integral domain we can cancel, i.e.:

##### Proof

But:

#### Example

So for example is an integral domain because:

1. The elements of are commutative
2. , hence it is with unity
3. There are no non-zero values in that multiply to give 0

Further,

Take :

All are Integral Domains

### Fields

A field is:

1. An Integral Domain
2. In which every non-zero element is a unit.

So for clarity a field is a set F that is:

1. A Ring
2. A commutative Ring
3. A Ring with unity/identity
4. All elements are units
   1. This necessitates that no elements can be zero-divisors, for they are mutually exclusive.

i.e. in a mathematical language the following statements are equivilant:

#### Examples

is not a Ring because it does not contain an additive identity 0

is an integral domain because it is commutative, with unity and has no non-zero value that multiply to give 0; It is NOT a field because not all values have an inverse (e.g.

are all fields because every element has a multiplicative identity and are hence units

## The Field of Complex Numbers [2.6]

The field of complex numbers is:

Addition is defined by:

Multiplication is defined by:

More over we represent the real and imaginary parts of a complex number thusly:

### The Set of Complex Numbers is a Field

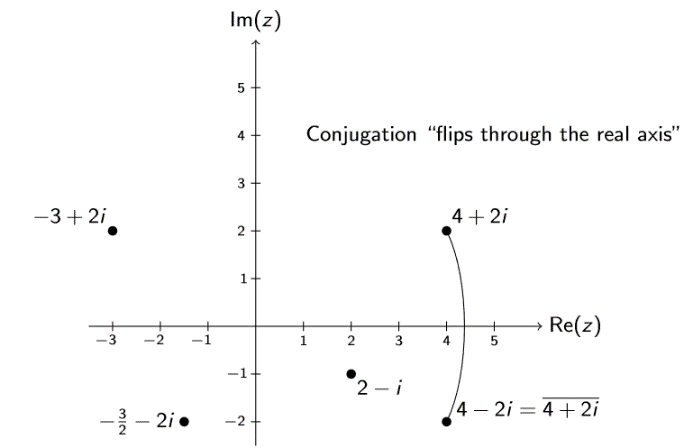
Remember that a field is:

1. A Ring
2. A commutative Ring
3. A Ring with unity/identity
4. All elements are units
   1. This necessitates that no elements can be zero-divisors, for they are mutually exclusive.

In this case the complex numbers:

1. Are indeed a ring
2. Complex Numbers are commutative
3. There exists a multiplicative Identity
4. Every element has an inverse

### Polar Notation

A complex Number, can be represented on the complex plane

And any complex number can be represented also in polar notation:

And the combination is equivilant because:

Flowing from power series for exponential, cosine and sine functions we have also:

### Multiplying Complex Numbers

Polar notation makes it far easier to multiply numbers.

Remember that multiplying a number on the complex plane involves scaling and rotating the plane from the point 1 (the multiplicative identity) to the point of the multiplier.

Hence it stands to reason that the distance from the origin of the new point will be larger by a factor of the scaling and the rotation on the plane will simply be added.[[14]](#footnote-15)

For:

### Powers of Complex Numbers De Moivre’s Theorem

It follows algebraically that raising complex numbers to the power of some :

### Roots of Complex Numbers

Multiple Complex Numbers, when raised to a power, may equal the same end result, hence solutions for given are:

There are always roots.

# (6) Polynomials

Week 6 Material | Due Tue. 10 April 2018

## Polynomial over a Ring

Take some polynomial function:

But, for the sake of clarity use :

If we imaged that we were dealing in a ring:

|  |  |
| --- | --- |
|  |  |
|  |  |

### Definitions

Take the polynomial:

In this case:

* The **Coefficients** are:
  + - The **Leading Coefficient** of is:
      * + If , is **monic**
    - The **Leading Term** of is:
* The **Leading Coefficient** is:
* The **Degree** of the polynomial is:
  + - If , the degree is said to be infinite
* The **root** of a polynomial is the value :

## Rings

Remember that a ring is any set that satisfies the ring axioms[[15]](#footnote-16) the following are all commutative: (an example of a ring that is not commutative could be .

A unit in a ring is an element of a ring that always has a multiplicative identity.

## Polynomial Arithmetic

A polynomial with coefficients in a commutative ring is of the form:

Where:

* is a variable

If the coefficients of a polynomial are sourced from some ring , then the set of all polynomials with coefficients in that ring is .

If the coefficients are sourced from some ring, , then the set of all polynomials with coefficients in that ring is .

Notes on Polynomials

* If there exists a unit in then there also exists a unit in .
* Remember that is just a placeholder, it is not assumed to stand for any element of the ring .
* The polynomial is only defined if the coefficients are sourced from a ***commutative*** *ring.*

### Equal Polynomials

Two polynomials in are equal *if and only if* all their coefficients are identical.

### Polynomials as symbols and functions

A polynomial can be treated like an algebraic symbol or as a function .

## Polynomial as an Integral Domain

If is a ring with 1 then:

is an **integral domain** *if and only if* is an integral domain.

The proof of this is, because, there are no zero divisors in there are no zero divisors in , hence is a commutative ring with unity with no zero divisors (which is an integral domain.

### Degree of Polynomial

If a polynomial is an integral domain:

## Polynomial over a field

Recall that a field is a commutative ring for which every element has an inverse (except zero, which is special because it is the additive identity).

If the coefficients of a polynomial are all in some field , then the set of all polynomials with coefficients in that ring is .

## Division Algorithm

The division algorithm is the precursor to Euclid’s Algorithm.

### For Integers

Let and be any integers with .

There are unique integers and such that , where

i.e.

### For Polynomials

Let be a field, (i.e. a commutative ring for which all non-zero elements are invertible)

Let and be two polynomials in .

There hence exist unique polynomials such that:

#### Polynomial Long Division

and can be found using ***polynomial long division***.

## Remainder Theorem

Let and be polynomials where all coefficients are in a some ring,

i.e. for some ring ;

If

Where

Then

### Proof

## Root Theorem

Let be a polynomial where all coefficients are in a field,

i.e.

for any ,

*if and only if* is a factor of .

### Proof

If , then for some value , So

***Prove that factor implies root***

***Prove that root implies factor***

By the division algorithm:

For some and some

By the Remainder Theorem,

So,

Which implies

## Maximum Roots

A polynomial of degree , can have at most roots.

## Units

A unit is an element in some ring that has an inverse in that ring.

e.g. in the set of all real numbers, all elements are units and in 3 and 2 are units because

### Polynomial Units

So you need to be careful here, it’s not inversible functions that are units per se, it’s polynomials that satisfy the following property:

Take some commutative ring R, any polynomials are units if and only if:

If R is a ring with unity, then is with unity

#### Units in polynomial fields

If is some field, then the units of are all the polynomials:

##### Proof

So for some unit , that unit must have a degree of 0 (essentially be a constant value)

## Euclidean Algorithm

The greatest common divisor of two polynomials , is a polynomial of greatest possible degree that divides both and , it is written:

This might seem useless, but a practical application is provided on p. 127 of the TB.

### Algorithm for Polynomials

It’s pretty much the same, just different:

Write:

Such that

Then:

By a process of repetition, the smallest value will represent the GCD.

## Irreducible and Reucible Polynomials

Reducible and irreducible polynomials are like prime and composite integers.

Some polynomial is reducible if

For non-units

Where R is a commutative integral domain.

Page 123 of TB.

## Fundamental Theorem of Arithmetic

So the fundamental theorem of arithmetic states that any number is either a prime or can be written as a unique product of prime numbers.

In terms of polynomials:

For some field , the set of polynomials with coefficients from that field ( ) is either irreducible or can be written as a product of irreducible polynomials.

This is unique, up to:

* Reordering polynomials
* Multiplying through by units

# (7) Fundamental Theorem of Algebra

Week 7 Material | Due Tue. 17 April 2018

## The Fundamental Theorem of Algebra

|  |  |
| --- | --- |
|  |  |

The fundamental theorem of algebra says:

Every polynomial has a

Every polynomial has c

### finitions

Take the polynomial:

In this case:

* The **Coefficients** are:
  + - The **Leading Coefficient** of is:
      * + If , is **monic**
    - The **Leading Term** of is:
* The **Leading Coefficient** is:
* The **Degree** of the polynomial is:
  + - If , the degree is said to be infinite
* The **root** of a polynomial is the value :

## Rings

Remember that a ring is any set that satisfies the ring axioms[[16]](#footnote-17) the following are all commutative: (an example of a ring that is not commutative could be .

A unit in a ring is an element of a ring that always has a multiplicative identity.

## Polynomial Arithmetic

A polynomial with coefficients in a commutative ring is of the form:

Where:

* is a variable

If the coefficients of a polynomial are sourced from some ring , then the set of all polynomials with coefficients in that ring is .

If the coefficients are sourced from some ring, , then the set of all polynomials with coefficients in that ring is .

Notes on Polynomials

* If there exists a unit in then there also exists a unit in .
* Remember that is just a placeholder, it is not assumed to stand for any element of the ring .
* The polynomial is only defined if the coefficients are sourced from a ***commutative*** *ring.*

### Equal Polynomials

Two polynomials in are equal *if and only if* all their coefficients are identical.

### Polynomials as symbols and functions

A polynomial can be treated like an algebraic symbol or as a function .

## Polynomial as an Integral Domain

If is a ring with 1 then:

is an **integral domain** *if and only if* is an integral domain.

The proof of this is, because, there are no zero divisors in there are no zero divisors in , hence is a commutative ring with unity with no zero divisors (which is an integral domain.

### Degree of Polynomial

If a polynomial is an integral domain:

## Polynomial over a field

Recall that a field is a commutative ring for which every element has an inverse (except zero, which is special because it is the additive identity).

If the coefficients of a polynomial are all in some field , then the set of all polynomials with coefficients in that ring is .

## Division Algorithm

The division algorithm is the precursor to Euclid’s Algorithm.

### For Integers

Let and be any integers with .

There are unique integers and such that , where

i.e.

### For Polynomials

Let be a field, (i.e. a commutative ring for which all non-zero elements are invertible)

Let and be two polynomials in .

There hence exist unique polynomials such that:

#### Polynomial Long Division

and can be found using ***polynomial long division***.

## Remainder Theorem

Let and be polynomials where all coefficients are in a some ring,

i.e. for some ring ;

If

Where

Then

### Proof

## Root Theorem

Let be a polynomial where all coefficients are in a field,

i.e.

for any ,

*if and only if* is a factor of .

### Proof

If , then for some value , So

***Prove that factor implies root***

***Prove that root implies factor***

By the division algorithm:

For some and some

By the Remainder Theorem,

So,

Which implies

## Maximum Roots

A polynomial of degree , can have at most roots.

## Units

A unit is an element in some ring that has an inverse in that ring.

e.g. in the set of all real numbers, all elements are units and in 3 and 2 are units because

### Polynomial Units

So you need to be careful here, it’s not inversible functions that are units per se, it’s polynomials that satisfy the following property:

Take some commutative ring R, any polynomials are units if and only if:

If R is a ring with unity, then is with unity

#### Units in polynomial fields

If is some field, then the units of are all the polynomials:

##### Proof

So for some unit , that unit must have a degree of 0 (essentially be a constant value)

## Euclidean Algorithm

The greatest common divisor of two polynomials , is a polynomial of greatest possible degree that divides both and , it is written:

This might seem useless, but a practical application is provided on p. 127 of the TB.

### Algorithm for Polynomials

It’s pretty much the same, just different:

Write:

Such that

Then:

By a process of repetition, the smallest value will represent the GCD.

## Irreducible and Reucible Polynomials

Reducible and irreducible polynomials are like prime and composite integers.

Some polynomial is reducible if

For non-units

Where R is a commutative integral domain.

Page 123 of TB.

## Fundamental Theorem of Arithmetic

So the fundamental theorem of arithmetic states that any number is either a prime or can be written as a unique product of prime numbers.

In terms of polynomials:

For some field , the set of polynomials with coefficients from that field ( ) is either irreducible or can be written as a product of irreducible polynomials.

This is unique, up to:

* Reordering polynomials
* Multiplying through by units

# (8) Groups

***Yeah I fell behind and missed everything hereafter***

# (9) Supgroups

# (10) Homomorphisms

# (11) RSA

1. Mathsisfun.com. (2018). *Set Symbols*. [online] Available at: https://www.mathsisfun.com/sets/symbols.html [Accessed 7 Mar. 2018]. [↑](#footnote-ref-1)
2. *Euler's formula with introductory group theory*. (2017). [video] 3Blue1Brown. [online] Available at: <https://www.youtube.com/watch?v=mvmuCPvRoWQ>. [Accessed 7 Mar. 2018] [↑](#footnote-ref-2)
3. A corollary is a proposition that follows from one already proved. [↑](#footnote-ref-3)
4. A lemma is an intermediate theorem in a proof [↑](#footnote-ref-4)
5. Mathsisfun.com. (2018). *Set Symbols*. [online] Available at: https://www.mathsisfun.com/sets/symbols.html [Accessed 7 Mar. 2018]. [↑](#footnote-ref-5)
6. *Euler's formula with introductory group theory*. (2017). [video] 3Blue1Brown. [online] Available at: <https://www.youtube.com/watch?v=mvmuCPvRoWQ>. [Accessed 7 Mar. 2018] [↑](#footnote-ref-6)
7. <[*https://proofwiki.org/wiki/Contradiction\_is\_Negation\_of\_Tautology*](https://proofwiki.org/wiki/Contradiction_is_Negation_of_Tautology)> [↑](#footnote-ref-7)
8. <https://proofwiki.org/wiki/Definition:Tautology>> [↑](#footnote-ref-8)
9. [*http://math.andrej.com/2010/03/29/proof-of-negation-and-proof-by-contradiction/comment-page-1/*](http://math.andrej.com/2010/03/29/proof-of-negation-and-proof-by-contradiction/comment-page-1/)> [↑](#footnote-ref-9)
10. A corollary is a proposition that follows from one already proved. [↑](#footnote-ref-10)
11. A lemma is an intermediate theorem in a proof [↑](#footnote-ref-11)
12. Nicodemi, O., Sutherland, M. and Towsley, G. (2007). *An introduction to abstract algebra with notes to the future teacher*. Upper Saddle River, NJ: Pearson Prentice Hall. [↑](#footnote-ref-12)
13. P. 66 of TB [↑](#footnote-ref-13)
14. <https://www.youtube.com/watch?v=xbFCJO5fugQ> or with more detail https://www.youtube.com/watch?v=mvmuCPvRoWQ [↑](#footnote-ref-15)
15. Page 83 of TB [2.5] [↑](#footnote-ref-16)
16. Page 83 of TB [2.5] [↑](#footnote-ref-17)