Abstract Algebra

Rohan Jain

Contents

Chapter 1 — **Page 2**

1.1 Introductory Notes — 2
Things to Remember — 2 • Set Review — 2 • Cartesian Products and Functions — 3 • Equivalence Relations — 4 • Complex Numbers and Matrices — 4 • Number Theory — 5

1.2 Group Theory — 6
Introduction to Groups — 6 • Properties of Groups — 7 • Subgroups — 9 • Permutations — 10 • Generators — 12 • Cosets — 13

1.3 Group Theory — 15
Isomorphisms — 15

1.4 Counting — 20

1.5 Rings — 21

Chapter 1

1.1 Introductory Notes

1.1.1 Things to Remember

Note:

- Definitions will usually be stated as "if" even though they mean "if and only if".
- Any form of proof is valid. Avoid proofs by contradiction because of disbelief in the law of excluded middle.
- When you define an object, you can *only* utilize its definition to prove anything about it.

1.1.2 Set Review

Definition 1.1.1: Set

In mathematics, a set is an undefined term. Basically, "everyone knows what it is." A few examples of sets are:

- The empty set is the set with no elements. It is denoted by ϕ or $\emptyset$.
- $\mathbb{N}$ is the set of natural numbers.
- $\mathbb{Z}$ is the set of integers.
- $\mathbb{Q}$ is the set of rational numbers.
- $\mathbb{R}$ is the set of real numbers.
- $\mathbb{C}$ is the set of complex numbers.

Note:

- A set is a well-defined collection of objects. The objects in a set are called elements of the set.
- A set is generally defined as a capital letter.
- $(A = B) \iff (\forall x : x \in A \iff x \in B)$
- $(A \subset B) \iff (\forall x \in A : x \in B)$
- A is a proper subset of B if $A \subset B$ and $A \neq B$.

Theorem 1.1.1

$A = B \iff A \subset B \wedge B \subset A$

Note:

- $A \cup B = x : x \in A \vee x \in B$
- $A \cap B = x : x \in A \wedge x \in B$
- $A \backslash B = x : x \in A \wedge x \notin B$
- $C \backslash (A \cup B) = (C \backslash A) \cap (C \backslash B)$

1.1.3 Cartesian Products and Functions

Note:

- $A \times B = \{(a, b) : a \in A \wedge b \in B\}$

Example 1.1.1 (Cartesian Product of two sets)

Let $A = \{1, 2, \Delta\}$ and $B = \{0, \pi\}$

- $(1, 0)$
- $(2, 0)$
- $(\Delta, 0)$
- $(1, \pi)$
- $(2, \pi)$
- (Δ, π)

Note:

Relations are subsets of Cartesian Products. For example, we can say that $<$ is a relation on the subset of $\mathbb{R} \times \mathbb{R}$ consisting of all ordered pairs of real numbers such that the first element is less than the second.

Definition 1.1.2: Function

A function f from a set A to a set B is a subset of $A \times B$ such that for every $a \in A$, there is exactly one $b \in B$ such that $(a, b) \in f$.

Note:

Let R be a relation from A to B.

- A is the domain
- B is the codomain
- $\{b : aRb\}$ is the image
- R is injective (one-to-one) if $a_1Rb \wedge a_2Rb \implies a_1 = a_2$
- R is surjective (onto) if $\forall b \in B : \exists a \in A : aRb$. Basically if the image is the entire codomain.
- R is bijective if it is injective and surjective

Note:

$A \xrightarrow{\text{R}} B$
$B \xrightarrow{\text{S}} C$
Define the composition as $S \circ R = \{(a, c) : \text{there is some } b \text{ such that } (a, b) \in R \text{ and } (b, c) \in S\}$

Theorem 1.1.2
Let $f : A \to B$, $g : B \to C$, and $h : C \to D$. Then

- $h \circ (g \circ f) = (h \circ g) \circ f$
- If f and g are injective, so is $g \circ f$
- If f and g are surjective, so is $g \circ f$
- If f and g are bijective, so is $g \circ f$

1.1.4 Equivalence Relations

Definition 1.1.3: Equivalence Relation

An equivalence relation is a relation that has the following special properties:

- Reflexivity: aRa for all $a \in A$
- Symmetry: $aRb \implies bRa$
- Transitivity: $aRb \wedge bRc \implies aRc$

Definition 1.1.4: Partition

Given a set S, a partition of S is a collection of subsets of S such that their union is S.

Note:
Equivalence relations go hand in hand with partitions.

Note:
If $\sim$ is an equivalence relation $a \sim b$, then $\sim$ partiations a set X into chunks. $X/\sim$ is the set of chunks.
Addition is *well-defined* as an operation on $\mathbb{Z}/x\mathbb{Z}$ for $x \in \mathbb{Z}$.

1.1.5 Complex Numbers and Matrices

Definition 1.1.5: Complex Number

A complex number is a number of the form $a + bi$, where a and b are real numbers and i is the imaginary unit. $i^2 = -1$.

Note:
Complex numbers generally take the from $z = a + bi$.
$\bar{z} = a - bi$ is the complex conjugate of z.
Divide complex numbers by multiplying by the complex conjugate of the denominator

Definition 1.1.6: Matrix

A matrix is a rectangular array of numbers. A $m \times n$ matrix is an array of m rows and n columns. Define the group of $m \times n$ matrices over a field $\mathbb{F}$ as $\mathbb{F}^{m \times n}$.

Note:
Multiplication by an $m \times n$ matrix is a function from $\mathbb{F}^n$ to $\mathbb{F}^m$. It is associative because all functions are associative.

Example 1.1.2 (2 × 2 matrix exercise)

Consider $\mathbb{Z}^{2\times 2}$. Define a relation $A \sim B$ if there is an integer matrix P whose determinant is one and $B = P^{-1}AP$. Note that if an integer matrix has a determinant 1 it is invertible and its inverse is also an integer matrix with determinant 1.

1. Show that this is an equivalence relation.
2. Show that two matrices with different determinants cannot be similar.
3. Determine whether $\begin{bmatrix} 6 & 0 \\ 0 & 1 \end{bmatrix}$ is similar to $\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$.
4. Determine whether $\begin{bmatrix} 6 & 0 \\ 0 & 1 \end{bmatrix}$ is similar to $\begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}$.

Solution:

1. Reflexive: $A = P^{-1}AP$ for $P = I_2$.
   Symmetric: $P^{-1}AP = P^{-1}BP$ for some P with determinant 1.
   Transitive: $B = P_1^{-1}AP_1 \wedge C = P_2^{-1}BP_2 \Rightarrow C = P_2^{-1}P_1^{-1}AP_1P_2$
2. Determinants are a multiplicative property. If $B = P^{-1}AP$ and $\det(B) \neq \det(A)$, then $\det(B) \neq 1 * \det(A) * 1$.
3. No, different JCF.
4. Yes, same JCF.

1.1.6 Number Theory

Note:
Know induction, division algorithm, GCD and Bezout's lemma, and Primes and the Fundmental Theorem of Arithmetic.

Example 1.1.3 (Weak Induction)

Prove that $5|n^5 - n$ for all n.

Proof: Proof by induction.

1. $n = 1$ is true, $5|0$.
2. If it is true then $n = k$, show that it is true when $n = k + 1$.
   $(k+1)^5 - (k+1) = k^5 + 5k^4 + 10k^3 + 10k^3 + 5k + 1 - (k+1) = (k^5 - k) + (5k^4 + 10k^3 + 10k^2 + 5k)$.
   Both quantities are divisible by 5.

Therefore, $5|n^5 - n$ for all n. 😊

Example 1.1.4 (Strong Induction)

Prove that every integer n can be written as $n = d_1 1! + d_2 2! + \cdots + d_k k!$ for some $d_1, \ldots, d_k \leqslant k \in \mathbb{Z}$ and $k \geqslant 1$.

Proof: Strong induction.
Given n, chose s s.t. $s! \leqslant n < (s+1)!$. Then we can write $n = q \cdot s! + r$.

1. $q \leqslant s$ (if $q \geqslant s + 1$, then $n \geqslant (s+1)!$, which goes against our claim)

2. $r < s!$

Assume that this is true for any $k < n$. Then we can write $n = q \cdot s! + r$ for some $r < s!$. Then we can write r in the same format since it is true for all $k < n$. ☺

Example 1.1.5 (Well-ordering)
Prove that given $a, b, b \neq 0$, there exists unique q, r such that $a = qb + r$ and $0 \leqslant r < |b|$.

Proof: Well-ordering.
Consider all the integeres of the form $a - xb$ for $x \in \mathbb{Z}$. At least one of these is nonnegative. If $a > 0$, choose $x = 0$. If $a \leqslant 0$, then choose $x = -ab|b|$. So let the set of all negative $a - xb$ be nonempty. Let $q = x$ be the smallest. Define $r = a - qb$ so that $a = qb + r$ and $r < |b|$.
To prove uniqueness, consider two sets: qr and $q'r'$. Then $qb+r = q'b+r'$ and $r < |b|$. Or, $(q-q')b = r'-r$. The absolute value of the RHS has to be between $1 - |b|$ and $|b| - 1$. This has to be 0 since its the only multipe of b in that range. So $q - q' = 0$ and $q = q'$ and $r = r'$. ☺

Lemma 1.1.1 Bezout's Lemma
Given integers $a, b \neq 0$, their GCD can be written in the form $ra + sb$ for some r, s.

Definition 1.1.7

An integer is prime if it only has 1 and itself as positive divisors.

Note:
1 is not a prime.

Lemma 1.1.2
If p is prime and $p|ab$, then either $p|a$ or $p|b$.

Theorem 1.1.3 Fundamental Theorem of Arithmetic
Every integer greater than 1 is either a prime or can be written as a product of primes in a unique way.

1.2 Group Theory

1.2.1 Introduction to Groups

Definition 1.2.1: Binary Operation

Given a set S, a *binary operation* on S is a function $S \times S \longrightarrow S$.

Definition 1.2.2: Group

A *group* is a set G with a binary operation $*$ such that for all $a, b, c \in G$, the following hold:

1. $(a * b) * c = a * (b * c)$ (associativity)
2. $e * a = a * e = a$ (identity)
3. $a * a^{-1} = e$ (inverse)
4. $*$ is closed under G.

Note:

A set that only has associativity and identity is called a *monoid*.

Note:

Examples of groups

- $\mathbb{Z}, \mathbb{R}, \mathbb{R}^{3\times3}, \mathbb{C}, \mathbb{Q}$ with addition.
- $z \in \mathbb{C} : |z| = 1$ with multiplication.
- $GL(2, \mathbb{R})$ with matrix multiplication. However, this is not abelian.
- D_4 = symmetries of a square.
- D_2 = symmetries of a triangle.
- $U(n)$ with multiplication modulo n.

If we take a random group, say $U(5)$, then we can create a table for how the multiplication works:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

A table like this is called a *Cayley Table*. Notice that this table is actually symmetric. This means that the group is *commutative*, but more properly, *abelian*.

Definition 1.2.3: Abelian Group

An *abelian group*, G, is a group where $a * b = b * a$ for all $a, b \in G$.

1.2.2 Properties of Groups

Theorem 1.2.1

The identity element of a group is unique.

Proof: Let e_1 and e_2 be the identity elements. Then $e_1 * e_2 = e_2 * e_1 = e_1$. So $e_1 = e_2$. 😊

Theorem 1.2.2

Each element has a unique inverse.

Proof: Let a^{-1} and b both be inverses of a then consider the product baa^{-1}. Then $b = be = b(aa^{-1}) = (ba)a^{-1} = ea^{-1} = a^{-1}$. So $b = a^{-1}$. 😊

Corollary 1.2.1

$(ab)^{-1} = b^{-1}a^{-1}$

Proof: $abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$. 😊

Corollary 1.2.2

$(a_1a_2a_3 \dots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}a_{n-2}^{-1} \dots a_1$

Proof: Induction from 1.2.1. ☺

Corollary 1.2.3
$(a^{-1})^{-1} = a$

Proof: $(a^{-1})^{-1}a^{-1} = e = aa^{-1}$, so by uniqueness of inverses... ☺

Theorem 1.2.3
Given any $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solutions, though not necessary equal.

Proof: Let $x = a^{-1}b$ and $y = ba^{-1}$. Then $ax = a(a^{-1}b) = eb = b$ and $ya = ba^{-1}a = be = b$. To show uniqueness, consider $ax_1 = ax_2$ then left multiply by a^{-1}. ☺

Corollary 1.2.4 Cancellation Laws
In any group G, if $ac = bc$, then $a = b$. And if $ca = cb$, then $a = b$.

Proof: Right or left multiply by c^{-1} for appropriate equation. ☺

Note:
Proving that a group is associative from its Cayley digram takes too long. It is easier to show an isomorphism to a well-established group.

Note:
Groups of order n:

- 1: $\mathbb{Z}_1$
- 2: $\mathbb{Z}_2$
- 3: $\mathbb{Z}_3$
- 4: $\mathbb{Z}_4, V$
- 5: $\mathbb{Z}_5$
- 6: $D_3, \mathbb{Z}_6$
- 7: $\mathbb{Z}_7$
- 8: $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4, H$
- 9: $\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$

Note:
A note on notation:
$a \cdot a = a^2, a \cdot a \cdot a = a^3 \dots$

Definition 1.2.4: Direct Product

Given G_1, G_2 groups, then the direct proudct $G_1 \times G_2$ is the group of ordered pairs (g_1, g_2) where $g_1 \in G_1$ and $g_2 \in G_2$. The operation is $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2)$.

Example 1.2.1
$\{e\} \times G \cong G$

Example 1.2.2
$\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$

Example 1.2.3
$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong Z_6$

Theorem 1.2.4
Let $(G, \circ, e)$ be a set with the binary operation $\circ$ and left identity e. Then assume each $x \in G$ has a left inverse such that $x^{-1} \circ x = e$. Then G is a group.

Proof: what is $xe =$?
Let $y = xe$. Then $x^{-1}y = x^{-1}(xe) = (x^{-1}x)e = e$. So $x^{-1}y = e = x^{-1}x$. Multiply by $x^{-1^{-1}}$ to get $y = x$. Therefore, e is a two-sided identity.
To show that x^{-1}, consider $z = x \circ x^{-1}$. Left multiply by x^{-1} to get $x^{-1} \circ z = x^{-1} \circ (x \circ x^{-1}) = (x^{-1} \circ x) \circ x^{-1} = x^{-1}$. Left multiply both sides by $x^{-1^{-1}}$ to see that $e \circ z = z = e$. Therefore, x^{-1} is a left inverse and G is a group. 😊

1.2.3 Subgroups

Definition 1.2.5: Subgroups

Let $(G, \circ, e)$ be a group and let $H \subset G$. If H is a group under the same operation $\circ$, then H is a *subgroup* of G. This is denoted as $H < G$.

Note:
Having the same operation is critical. For example $GL(2) \subset \mathbb{R}^{2\times 2}$, but $GL(2)$ is not a subgroup of $\mathbb{R}^{2\times 2}$ because the operation is matrix multiplication, not addition.

Lenma 1.2.1
If $H \subset G$ and for any $h_1, h_2 \in H$, $h_1 h_2^{-1} \in H$, then H is a subgroup.

Proof: Following:

- Choose $h_2 = h_1$, then $H \supset h_1 h_1^{-1} = e$.
- Let $h_1 = e, h_2 = h$. Then $eh^{-1} = h^{-1} \in H$.
- $h_1 h_2 = h_1 (h_2^{-1})^{-1}$.

😊

Example 1.2.4 (Quarternion Units)
Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. These function such that $i^2 = j^2 = k^2 = ijk = -1$. All the two element subgroups are $\{\pm 1\}$.

Definition 1.2.6: Cyclic Subgroup

Given $a \in G$, the *cyclic subgroup generated by* a, denoted $\langle a \rangle$, is the set $\{a^n : n \in \mathbb{Z}\}$. The element a is called the *generator*.

Example 1.2.5 (Cylic Subgroups)

- $\mathbb{Z} = \langle 1 \rangle$
- $\mathbb{Z}_7 = \langle 1 \rangle, \langle 5 \rangle$
- $\mathbb{Z}_{10} = \langle 1 \rangle, \langle 7 \rangle$

Proposition 1.2.1

Every subgroup of $\mathbb{Z}$ is cyclic.

Addendum: Any subgroup of any cyclic subgroup is itself cyclic. 😊

Note:

Some $U(n)$ groups are cyclic while others are not. They are cyclic if n has primitive roots.

Lenma 1.2.2

Let $a \in G$, order of $a = n$. Then order of $a^k = \frac{n}{\gcd(a,k)}$

Proof: Let $b = a^k$. Order is the smallest number we can find such that $b^s = e$. Note that $b^s = a^{ks}$, so we need $n|ks$. Let $d = \gcd(n, k)$. Then $n = dn'$ and $k = dk'$. Then we need dn' to be a divisor of sdk'. So, $n'|sk'$. Since n' and k' are coprime, $n'|s$. Therefore, the smallest possible s is $n' = n/\gcd(a, k)$. 😊

Theorem 1.2.5

A group has no proper nontrivial subgroups is and only if it is a cyclic group of prime order.

Proof: Let $G = \langle a \rangle$ for any $a \in G$. What is the oder of a? If a isn't prime, $a = xy$ and $y \neq 1$. Then a^x has order y. 😊

1.2.4 Permutations

Definition 1.2.7: Permutation

A permutation is a bijection from a set S to itself.

Note:

All permutations of a set A forms a group called S_A. This can be called either "permutation on A" or "symmetric group of A".
$|S_n| = n!$.

Example 1.2.6 (Compositions and Cycles)

Given two permutations, it is not hard to multiply then. For example:

$$\begin{pmatrix}1&2&3&4&5&6\\2&4&3&6&5&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\4&3&5&1&6&2\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\4&5&3&2&6&1\end{pmatrix}$$

Note:

This notation can be seen as quite cumbersome and redundant given the fact that the first row is always the same. To simplify this, we can use the following *cycle* notation:

$$\begin{pmatrix}1&2&3&4&5&6\\4&5&3&2&6&1\end{pmatrix}=\begin{pmatrix}1&4&2&5&6\end{pmatrix}\begin{pmatrix}3\end{pmatrix}$$

This is read as the permutation that sends 1 to 4 to 2 to 5 to 6 and 3 to 3.
The identity permutation is $\begin{pmatrix}1&2&3&4&5&6\end{pmatrix}$, which is annoying so mathematicians just say e.

Lenma 1.2.3

Disjoint cycles commute.

Theorem 1.2.6

Every permutation can be written as a product of disjoint cycles.

Proof: Strong Induction:

Assume any permutation that moves $< n$ elements can be written. Consider σ which has n elements. Consider the set, which is called the orbit, of σ: $1, \sigma(1), \sigma^2(1) \ldots$. By the pigeonhole principle, this repeats. Cut off this set at the repeat of 1 and removed the curly braces and commas to get a cycle that 1 belongs to. 😄

Note:

The inverse of a cyclic is just the cycle backwards.

Definition 1.2.8: Transposition

A transposition is a permutation that swaps just two elements. Also known as a “swap” or “2-cycle”

Lenma 1.2.4

Any permutation may be written as a product of not disjoint transpositions.

Proof: The cycle $\begin{pmatrix}A&B&C&\ldots&Y&Z\end{pmatrix}=(AZ)(AY)\ldots(AC)(AB)$. 😄

Lenma 1.2.5

The following are true:

1. $(AB) = (BA)$.
2. $(AB)(AC) = (A\ B\ C)$
3. $(AB)(CD) = (CD)(AB)$
4. $(\ldots X\ Y\ Z \ldots)(AY) = (\ldots X\ Y\ A\ Z)$
5. $(AY)(\ldots X\ Y\ Z \ldots) = (\ldots X\ A\ Y\ Z)$
6. $(\ldots P\ Q\ R \ldots X\ Y\ Z)(QY) = (\ldots P\ Q\ Z \ldots)(\ R \ldots X\ Y)$
7. $\begin{pmatrix}A&B&C&\ldots&Y&Z\end{pmatrix}=(AZ)(AY)\ldots(AC)(AB)$

Theorem 1.2.7

Let σ be a permutation. Then σ can be written as a product of transpositions. Say $\sigma = \tau_n\tau_{n-1}\ldots\tau_1$. This permutation is not unique, but if we say that $\sigma = \tau_k\tau_{k-1}\ldots\tau_1$, then $k = n \pmod 2$.

Definition 1.2.9: Parity

Parity of σ is even or odd as k is.

Theorem 1.2.8

There are $n!/2$ odd permutations and $n!/2$ even permutations.

Theorem 1.2.9

The even permutations form a subgroup of S_n, called the *alternating group*, denoted A_n.

Note:

An *alternating polynomial* is one that flips sign when you switch two of its elements. For example, $x^2 - y^2$ is alternating while $xy+yz+xz$ is not. The alternating group is the group of permutations that leave alternating polynomials invariant.

1.2.5 Generators

Example 1.2.7 (Motivating Example)

The dihedral group, D_4, can be generated by two elements: r_{90} and f_v. All rotations are certainly powers of r_{90} and the other flips can be constructure by f_v and r_{90}. Therefore, r_{90} and f_v are the *generators* of D_4.

Definition 1.2.10: Generator

A generator of a group is an element that generates the group.

Lenma 1.2.6

The transpositions $\{(1\ 2), (2\ 3), \ldots, (n-1\ n)\}$ generate S_n.

Theorem 1.2.10

The transposition $\tau = (1\ 2)$ and the cycle $\sigma = (1\ 2\ \ldots\ n)$ generate S_n.

Definition 1.2.11: Group Presentation

A group presentation, $\langle g_1, g_2 \ldots, g_j | r_1, r_2, \ldots, r_k\rangle$ is a set of generators and relations. Each relation, r_i is meant to simplify to e.

Example 1.2.8 (Group Presentations)

- $\mathbb{Z}_6 = \langle a | a^6\rangle$
- $D_4 = \langle r_{90}, f_v | r_{90}^4, f_v^2, r_{90}f_vr_{90}f_v\rangle$

1.2.6 Cosets

Definition 1.2.12: Cosets

Let $H < G$ and $g \in G$. The *left coset* of H with representative g is the set $gH = \{gh : h \in H\}$. The *right coset* of H with representative g is the set $Hg = \{hg : h \in H\}$.

Example 1.2.9 (Cosets)

Let $G = D_4$ and $H = \{e, f_1\}$. Then there are eight left cosets and eight right cosets of H, according to the eight elements of D_4, that could be the representative. They are listed out below:

Representative	Left coset	Right coset
e	$\{e, f_1\}$	$\{e, f_1\}$
r_{90}	$\{r_{90}, f_v\}$	$\{r_{90}, f_h\}$
r_{180}	$\{r_{180}, f_{-1}\}$	$\{r_{180}, f_{-1}\}$
r_{270}	$\{r_{270}, f_h\}$	$\{r_{270}, f_v\}$
f_1	$\{f_1, e\}$	$\{f_1, e\}$
f_v	$\{f_v, r_{90}\}$	$\{f_v, r_{270}\}$
f_{-1}	$\{f_{-1}, r_{180}\}$	$\{f_{-1}, r_{180}\}$
f_h	$\{f_h, r_{270}\}$	$\{f_h, r_{90}\}$

Lenma 1.2.7

Let $H < G$, then H is a subgroup of G and let g_1, g_2 be arbitrary elements of G. Then the following are equivalent:

1. $g_1H = g_2H$
2. $Hg_1^{-1} = Hg_2^{-1}$
3. $g_1H \subset g_2H$
4. $g_1 \in g_2H$
5. $g_1^{-1}g_2 \in H$

Proof: We will prove that $1 \implies 2 \implies 3 \implies 4 \implies 5 \implies 1$ so that the statements prove each other in a circular manner, so if any is true the rest become true.

($1 \implies 2$) Consider a typical element hg_1^{-1} of Hg_1^{-1}. Its inverse is g_1h^{-1}. Since $h \in H$ and H is a subgroup, $h^{-1} \in H$, so $g_1h^{-1} \in g_1H$. Thus it is also in g_2H, so can be written in the form g_2h'. So we have $\left(hg_1^{-1}\right)^{-1} = g_2h'$. Take the inverse on both sides, to find $hg_1^{-1} = h^{-1}g_2^{-1}$. Since $h' \in H$ we also have $h'^{-1} \in H$, so this is a member of Hg_2^{-1}. In other words, any member of Hg_1^{-1} is in Hg_2^{-1}. The reverse inclusion is proven the same way, so the two sets must be equal to each other.

($2 \implies 3$) Consider a typical element g_1h of g_1H. Its inverse is $h^{-1}g_1^{-1} \in Hg_1^{-1} = Hg_2^{-1}$. So the inverse can be written as $h'g_2^{-1}$. Then, reinverting both of these, $g_1h = g_2h'^{-1} \in g_2H$.

($3 \implies 4$) Since H is a subgroup, $e \in H$, so $g_1e = g_1 \in g_1H$. By subsets, it must be in g_2H.

($4 \implies 5$) Since $g_1 \in g_2H$ we know that we can write $g_1 = g_2h$. Rearranging this gives $g_1^{-1}g_2h = e$ or $g_1^{-1}g_2 = h^{-1}$. Since H is a subgroups and $h \in H$, of course $h^{-1} \in H$.

($5 \implies 1$) Let $g_2h \in g_2H$ be a typical element. Since $g_1^{-1}g_2 \in H$ we can choose $k \in H$ so that $g_1^{-1}g_2 = k$. Then $g_1^{-1}g_2h = kh$, or $g_2h = g_1(kh)$.H is a subgroup so contains product of its elements, and thus $g_1(kh) \in g_1H$. Thus any element of g_2H is in g_1H, or $g_2H \subset g_1H$. Since $g_1^{-1}g_2$ is in H, so is its inverse $g_2^{-1}g_1$ so the argument of the previous paragraph may be repeated to show $g_1H \subset g_2H$. ☺

Theorem 1.2.11
Left cosets g_1H and g_2H are either identical or disjoint. Also true for right cosets.

Proof: Let $x \in g_1H \cap g_2H$. Then $x \in g_1H$ so therefore $xH = g_1H$. Same argument for $xH = g_2H$. 😊

Lenma 1.2.8
There is a one-to-one correspondence between left and right cosets.

Proof: Consider the map $gH \to Hg^{-1}$. It is a well-defined map by statements 1 and 2 of the lemma which also show why this map is one-to-one and onto. 😊

Note:
$xH = yH \Leftrightarrow Hx = Hy$

Definition 1.2.13: Index

The number of cosets of H in G (right or left, since these numbers are the same by the lemma) is called the index of H in G and is denoted by $[G : H]$.

Lenma 1.2.9
The function $f_g : H \to gH$ given by $f_g(x) = gx$ is a bijection between the elements of H and the elements of gH.

Theorem 1.2.12 Lagrange's Theorem
If G is a finite group and H is a subgroup of G, then the following equation is satisfied:

$$|G| = [G : H]|H|.$$

Proof: Cosets are equinumerous with H and either identical or disjoint, we're done! 😊

Corollary 1.2.5
$|H|$ divides $|G|$.

Corollary 1.2.6
Groups of prime order are necessarily cyclic, and each non-identity elements are the generators.

Theorem 1.2.13
Let $K < H < G$. Then $K < G$, and $[G : K] = [G : H][H : K]$.

Theorem 1.2.14
If you have an abelian group G whose order is the product mn where m and n are relativity prime, then G is cyclic. Its generator is ab where a is an element with order m and b is an element with order n.

Theorem 1.2.15 Euler
If a is relatively prime to n, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof: $|U(n)| = \phi(n)$ so the order of every element is a divisor of $\phi(n)$. 😄

Theorem 1.2.16 Fermat's Little Theorem

If p is a prime number, then $a^p \equiv a \pmod{p}$.

Proof: If p is a divisor of a then both sides are congruent to zero modulo p. Otherwise $\phi(p) = p - 1$ and the result obtains by multiplying both sides of the result of Euler's Theorem by a. 😄

Note:

While Lagrange eliminates subgroups of certain orders (order that is relatively prime to the order of the parent group), it does not guarantee the existence of any order.

Example 1.2.10 (A_4)

A_4 has 12 elements, but does not have any subgroups of size six. For assume there were such a subgroup H. Now H would have only two left cosets-itself and gH for some g not in H. But it also only has two right cosets. Since cosets are either disjoint or identical, the right coset of H other then H itself must also be the left coset. That is, $gH = Hg$. So for any $h \in H$, there is an h' so that $gh = h'g$. Another way of saying this is that $ghg^{-1} = h' \in H$ for any $h \in H$ and any $g \in G$.
Now consider the three-cycles in A_4. There are eight of them. So by the pigeonhole principle, there must be a three-cycle in H. Without loss of generality assume $(123) \in H$. By the result of the previous paragraph, $(124)(123)(142) = (243) \in H$. Also, $(234)\ (123)(243) = (134) \in H$. In fact, all three-cycles must be in H. But then H has more than just six elements!

Theorem 1.2.17

If $\sigma \in S_n$ is a cycle of length k, then $\tau \in S_n$ is also a cycle of length k iff $\tau = g\sigma g^{-1}$ for some $g \in S_n$.

Corollary 1.2.7

Two permutations have the same cycle structure if and only if they are conjugates.

1.3 Group Theory

1.3.1 Isomorphisms

Definition 1.3.1: Isomorphic

Let $(G, \cdot)$ and $(H, \circ)$ be groups. We say that G and H are isomorphic if there is a bijection $f : G \to H$ such that $f(g_1 \cdot g_2) = f(g_1) \circ f(g_2)$ for all $g_1, g_2 \in G$.

Example 1.3.1

$\phi : \mathbb{Z}_4 \to \{i, -1, -i, 1\}$ defined by $\phi(n) = i^n$. This is obviously a one-to-one and onto mapping, and trades addition in $\mathbb{Z}_4$ for multiplication in $\mathbb{C}$.

Theorem 1.3.1

If ϕ is an isomorphism, then so is ϕ^{-1}.

Corollary 1.3.1
If $\phi : G \to H$ is an isomorphism, then:

- $\phi(e_G) = e_H$
- $\phi(g^{-1}) = \phi(g)^{-1}$
- $\phi(g^k) = (\phi(g))^k$

Theorem 1.3.2 Cayley's Theorem
Every group is isomorphic to a permutation group.

Definition 1.3.2: Direct Product

Let $(G, \cdot, e)$ and $(H, \circ, i)$ be groups. The *direct product* of G and H, denoted as $G \times H$, is the group whose elements take the form (g, h) for $g \in G$ and $h \in H$. The operation is defined as $(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2)$. The identity element is (e, i).

Lenma 1.3.1
If g has order m in G and h has order n in H, then (g, h) has order $\operatorname{lcm}(m, n)$ in $G \times H$.

Corollary 1.3.2
If m and n are relatively prime, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$.

Definition 1.3.3: Internal Direct Product

Let G be a group with subgroups H and K that fit together as follows:

- $H \cap K = \{e\}$
- $G = HK = \{hk : h \in H, k \in K\}$
- $hk = kh$ for any $h \in H$ and $k \in K$

Then G is called the *internal direct product* of H and K, and is isomorphic to $H \times K$.

Definition 1.3.4: Normal Subgroup

A subgroup H of G is called *normal* if $gH = Hg$ for all $g \in G$.

Theorem 1.3.3
Let H be a subgroup of G. Then the following assertions are equivalent:

1. H is normal in G.
2. For any $g \in G$, $gHg^{-1} \subset H$.
3. For any $g \in G$, $gHg^{-1} = H$.

Theorem 1.3.4
Let N be a normal subgroup of G. Then the cosets of N form a group denoted G/N.

Example 1.3.2 (D_5/R)

The quotient group $D_5/R = \{\text{rotations}, \text{reflections}\}$.

Example 1.3.3 ($\mathbb{Z}/8\mathbb{Z}$)

$\mathbb{Z}/8\mathbb{Z} = \mathbb{Z}_8$

Example 1.3.4 (D_6 with the 120 degree rotations)

If we have $N = \{e, r_{120}, r_{240}\}$, then N is normal so we can analyze D_6/N, which we see is the same as V.

Theorem 1.3.5

If N is normal in G and $H < G$, then $H \cap N$ is normal in H.

Proof: Need to show that for all $hinH, hK = Kh$ if we call $K = H \cap N$. Or $hKh^{-1} \subset K$. First we claim that $hkh^{-1} \in H$ because all the elements are in H and groups are closed. Then we claim that $hkh^{-1} \in K$ because $k \in N$, so $hkh^{-1} \in N$ because N is normal in G. So, $hkh^{-1} \in H \cap N$. 😊

Definition 1.3.5: Simple

A group with no proper normal subgroups is called *simple*.

Lenma 1.3.2

All even permutations can be written as a product of 3-cycles ($n \geqslant 4$).

Proof: Even permutations are generated by products of even numbers of transpostions. Two transpositions overlap at either 0, 1 or both places. In any case, you can factor it into a product of 3-cycles. 😊

Lenma 1.3.3

If a normal subgroup of A_n, $n \geqslant 3$, contains even one 3-cycle, then it contains all of A_n.

Proof: If you have $(a\ b\ c)$ and you conjugate it with $(a\ b\ d)$, then you get $(a;\ c\ d)$. In other words, the conjugate of any 3-cycle forms all 3-cycles, which generate A_n. 😊

Theorem 1.3.6

For $n \geqslant 5$, A_n is simple.

Proof: Let N be a nontrivial normal subgroup of A_n. We will show that N contains a three-cycle $\Rightarrow$ is all of A_n. Now we check the five cases:

1. If N contains a three-cycle, then we're done by previous lemmas.

2. N contains a permutation σ that can be written in cycle notation as $\mu\rho$ where ρ is a cycle whose length is greater than three, say $\rho = (a_1 a_2 a_3 a_4 \ldots a_k)$. Then by normality, N also contains the permutation $(a_1 a_2 a_3)\,\sigma\,(a_3 a_2 a_1)$. Since none of the cycles in μ contain a_1, a_2, or a_3, we get that $(a_1 a_2 a_3)\,\sigma\,(a_3 a_2 a_1) = (a_1 a_2 a_3)\,\mu\rho\,(a_3 a_2 a_1) = \mu\,(a_1 a_2 a_3)\,\rho\,(a_3 a_2 a_1) = \mu\,(a_2 a_3 a_1 a_4 \ldots a_k)$. Since this is in N and σ^{-1} must be in N, we can multiply the two to find that $(a_k \ldots a_3 a_2 a_1)\,\mu^{-1}\mu\,(a_2 a_3 a_1 a_4 \ldots a_k) = (a_k \ldots a_3 a_2 a_1)\,(a_2 a_3 a_1 a_4 \ldots a_k) = (a_1 a_3 a_k)$ is in $N-$ so N contains a three-cycle!

3. N contains a permutation which has all transpositions and three-cycles, containing at least two three-cycles. So N contains an element like $\sigma = \mu(a_1a_2a_3)\begin{pmatrix} a_4 & a_5 & a_6 \end{pmatrix}$ (note that $n \geqslant 6$ in this case). N contains σ conjugated by $(a_1a_2a_4)$, which is $\mu(a_1a_5a_6)(a_2a_4a_3)$. Multiply this on the left by σ^{-1} to find that N also contains $\begin{pmatrix} a_6 & a_5 & a_4 \end{pmatrix}(a_3a_2a_1)(a_1a_5a_6)\begin{pmatrix} a_2 & a_4 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_4 & a_2 & a_6 & a_3 \end{pmatrix}$ which is a 5-cycle, and we are complete under Case 2.

4. N contains a permutation which has all transpotions and just one three cycle: $\mu(a_1a_2a_3)$. Then N also contains the square of this element, which is $(a_1a_3a_2)$, a three-cycle, so we're done once again.

5. N contains an element that is a product of an even number of transpositions and no other cycles. So N contains an element like $\mu(a_1a_2)(a_3a_4)$. Conjugate by $(a_1a_2a_3)$ to obtain $\mu(a_1a_4)(a_2a_3)$. Now multiply this by σ^{-1} to obtain $(a_1a_2)(a_3a_4)(a_1a_4)(a_2a_3) = (a_1a_3)(a_2a_4)$. We finally use the fact that $n \geqslant 5$ to conjugate this by $(a_1a_2a_5)$ yielding $(a_2a_3)(a_4a_5)$ is also in N. Then N contains the product of these last two elements, which is $(a_1a_3a_4a_5a_2)$. Since this is a 5 -cycle, we are done by Case 2.

😊

Definition 1.3.6: Homomorphism

Let $(G, \cdot)$ and $(H, *)$ be groups. A *homomorphism* from G to H is a map $\phi : G \to H$ that satisfies $\phi(g \cdot h) = \phi(g) * \phi(h)$ for all $g, h \in G$.

Example 1.3.5 (Determinants)

The function $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ is a homomorphism because of the multiplicative property of determinants.

Example 1.3.6 (Projection Homomorphisms)

Let G, H be any two groups. Then there are two *projection homormorphisms*. Namely, they are $\pi_1(g, h) = g$ and $\pi_2(g, h) = h$ for all $g, h \in G \times H$.

Example 1.3.7 (Inclusion Homomorphism)

We say that D_4 is included in S_4 because any symmetry of a square is definitely a permutation of its vertices.

Example 1.3.8 (Canonical Map)

Let $N \trianglelefteq G$. Then, the *natural map*(or *canonical map*) is the homomorphism $\phi : G \to G/N$ given by $\phi(g) = gN$.

Note:

- An onto map is called a *surjection*.
- A one-to-one map is called an *injection*.
- A surjective homomorphism is called a *epimorphism*.
- An injective homomorphism is called a *monomorphism*.

Theorem 1.3.7

Let $\phi : G_1 \to G_2$ be a homomorphism.

1. $\phi(e_1) = e_2$.
2. For $g \in G_1$, $\phi(g^{-1}) = (\phi(g))^{-1}$.

3. If $H < G$, then $\phi(H) < G_2$. If $H \trianglelefteq G_1$, then $\phi(H)$ is normal in $\phi(G_1)$.
4. If $H_2 < G_2$, then $\phi^{-1}(H_2) < G_1$. If $H_2 \trianglelefteq G_2$, then $\phi^{-1}(H_2)$ is normal in $\phi^{-1}(G_1)$.

Definition 1.3.7: Kernel

Given a homomorphism $\phi : G_1 \to G_2$. Then, $\{e_2\}$ is normal in G_2. By the previous theorem, $\phi^{-1}(\{e_2\})$ is normal in G_1. The inverse image is called the *kernel* of ϕ.

Theorem 1.3.8 First Isomorphism Theorem

Let $\varphi : G \to H$ be a homomorphism of G onto H. Let K be the kernel of φ and let $\phi : G \to G/K$ be the natural homomorphism. Then there is a unique isomorphism $\psi : G/K \to H$ such that $\psi \circ \phi = \varphi$.

Theorem 1.3.9 Second Isomorphism Theorem

Let G be a group, H a subgroup, and N a normal subgroup. Then $H \cap N$ is normal in H, HN is normal in N, and $H/(H \cap N)$ is isomorphic to HN/N.

Theorem 1.3.10 Third Isomorphism Theorem

Let G be a group with normal subgroups H and N with $N \subset H$. Then $G/H \cong \dfrac{G/N}{H/N}$.

Theorem 1.3.11 Correspondence Theorem

If H_1 and H_2 are subgroups of G that contain N, then

1. $A \subset B$ iff $A/N \subset B/N$.
2. If $A \subset B$, then $[B : A] = [B/N : A/N]$.
3. $\langle A, B\rangle/N = \langle A/N, B/N\rangle$.
4. $(A \cap B)/N = (A/N) \cap (B/N)$.

Theorem 1.3.12 Fundmental Theorem of Finite Abelian Groups

Every finite abelian group G is isomorphic to a direct product of cyclic groups $\mathbb{Z}_a$ where a is a prime power.

Theorem 1.3.13

Given a non-trivial abelian group, the following two conditions are equivalent for a subset X of G.

1. Every non-zero element $x \in G$ can be expressed as a linear combination of x_i.
2. X generates G and no linear combination equals 0 for nonzero coefficients.

Definition 1.3.8: Free Abelian Group

A group G that has a subset that generates G where the only relation is $ab = ba$ is called a *free abelian group*.

Theorem 1.3.14

If G is a free abelian group with finite bases, then all bases for G are finite with the same number of elements.

1.4 Counting

Definition 1.4.1: Rank

The *rank* of a free abelian group with a finite basis is the number of elements in a basis.

Definition 1.4.2: G-equivalent

$x \sim_G y$ if $y = gx$ for some $g \in G$ and $x, y \in X$.

Definition 1.4.3: Orbit

The *orbit*, O_x is all y such that $x \sim_G y$.

Definition 1.4.4: Fixed-point set

Let G act on X. Choose a particular element $g \in G$. The set $X_g = \{x \in X : gx = x\}$ is called the *fixed-point set* of g.

Definition 1.4.5: Stabilizer

Let G act on X. Choose a particular element $x \in X$. The set $G_x = \{g \in G : gx = x\}$ is called the *stabilizer* of x.

Lenma 1.4.1

The stabilizer of any element of X is a subgroup of G.

Proof: The proof is by direct computation. The stabilizer is also called the stabilizer subgroup, or sometimes the *isotropy* group. 😃

Theorem 1.4.1

For any finite group G and finite G-set X, given $x \in X$, then $|O_x| = [G : G_x]$.

Definition 1.4.6: X_G

$X_G = \{x \in X : gx = x \forall g \in G\}$

Note:

If $x \in X_G$, then $|O_x| = 1$. Thie yields us a simple equation for the order of X:

$$|X| = |X_G| + \sum_{i=1}^{k} |O_{x_i}|$$

Definition 1.4.7: Class Equation

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C(x_i)]$$

Corollary 1.4.1
The order of any conjugacy class must divide the order of the group.

Corollary 1.4.2
A group of order p^n where p is prime has a nontrivial center.

Theorem 1.4.2 Cauchy's Theorem
If p is prime and divides $|G|$, then G has a subgroup of order p.

Lenma 1.4.2
Let X be a G-set and $x \sim_G y$. Then G_x and G_y are isomorphic.

Theorem 1.4.3 Burnside's Theorem
Let G be a finite group and X a finite G-set. If k is the number of orbits of G, then

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

Proof: First we have to understand that the following equation:

$$\sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|$$

Both of these go through all the elements of X and count each one a number of times equal to the number of elements of G that fix it, so these sums must be equal.

Now, within any orbit, all the $|G_y|$ for y in that orbit are equal (all such stabilizers are isomorphic, so trivially they are equinumerous). So for each orbit $\mathcal{O}_x$, the portion of the sum relating to it is given as follows:

$$\sum_{y \in \mathcal{O}_x} |G_y| = |\mathcal{O}_x||G_x|.$$

Now we know that $|\mathcal{O}_x| = [G : G_x] = |G|/|G_x|$. So each orbit contributes $|G|$ to the sum of $\sum_{x \in X} |G_x|$. Since there are k orbits, the final sum must be $k|G|$, and the theorem follows. ☺

1.5 Rings

Definition 1.5.1: Ring

A *ring* is a set R with two binary operations and is denoted as $(R, +, \cdot)$, that satisfies the following conditions:

- $(R, +)$ is an abelian group.
- $(R, \cdot)$ is associative.
- $\cdot$ distributes over $+$.

Lenma 1.5.1

If R is a ring, then

- $0x = x0 = 0$ for all $x \in R$
- $(x)(-y) = (-a)(b) = -(ab)$ for all $a, b \in R$
- $(-a)(-b) = ab$ for all $a, b \in R$

Proof: Note that $a0 = a(0+0) = a0 + a0$ and the result is obtained by additive cancellation.

The same works for $0a = (0+0)a = 0a + 0a$.

Then $0 = a0 = a(b + (-b)) = ab + a(-b)$. Adding the opposite $-(ab)$ to both sides yields $a(-b) = -(ab)$. The other half is similar using $0b = (a + (-a))b$.

The third bullet comes from the second and the fact that the inverse of the inverse is the original element by uniqueness of inverses. 😄

Definition 1.5.2: Ring with unity

If a ring has a multiplicative identity (which will usually be notated 1, though note that matrices often use I for the identity), it is called a *ring with unity*.

Definition 1.5.3: Unit

In a ring with unity, any element with an inverse is called an *unit*.

Definition 1.5.4: Division Ring

A ring with unity in which each non-zero element is a unit is called a *division ring* (or a *skew field*).

Definition 1.5.5: Field

A commutative division ring is called a *field*.

Definition 1.5.6: Zero Divisor

In any ring, non-zero elements a and b are called *zero divisors* if $ab = 0$. a is the left zero divisor while b is the right zero divisor.

Lenma 1.5.2 Left Cancellation

If a is not a left zero divisor and $ab = ac$, then $b = c$.

Lenma 1.5.3 Right Cancellation

If a is not a right zero divisor and $ba = ca$, then $b = c$.

Definition 1.5.7: Integral Domain

A commutative ring with no zero divisors is called an integral domain.

Theorem 1.5.1 Wedderburn

Every finite division ring is a field.

Definition 1.5.8: Characteristic

The *characteristic* of a ring is the smallest positive integer n such that $n1 = 0$. If no such n exists, the characteristic is 0. This is denoted $char(R)$.

Lenma 1.5.4

Let R be a ring with unity and a unity element of 1. Then, the characteristic of R is the order of 1.

Proof: The characteristic can't be smaller than n since that's the minimum number of 1s that need to be added to get 0. If it's larger, $nx = (x + x + \cdots + x) = x(1 + 1 + \cdots + 1) = x(0) = 0$. 😊

Corollary 1.5.1

The characteristic of any integral domain is either zero or a prime.

Proof: Assume the characteristic is composite and equal to ab. Then $a1 \neq 0$ and $b1 \neq 0$, but $(a1)(b1) = 0$. Then, the ring has zero divisors and is therefore not an integral domain. 😊

Corollary 1.5.2

The additive group structure underlying any finite field is isomorphic to $\mathbb{Z}_p^k$.

Definition 1.5.9: Ring Homomorphism

Let R and S be rings with a map $\phi : R \longrightarrow S$. Then, ϕ is a *ring homormophism* if

$$\phi(ab) = \phi(a)\phi(b)$$
$$\phi(a + b) = \phi(a) + \phi(b)$$

for all $a, b \in R$. Additionally, if ϕ is a bijection, it is a *ring isomorphism*.

Example 1.5.1 (Evaluation Homomorphism)

$\phi_x : \mathbb{R}^x \longrightarrow \mathbb{R}$ where $\phi_x(p(y)) = p(x)$ is called the *evaluation homomorphism* and it is not hard to check that this is indeed a homomorphism.

Definition 1.5.10: Ideal

Let R be a ring. An *ideal* of R is a subring I of R such that for $r \in R$ and $i \in I$, we have that $ri \in I$ and $ir \in I$. We often write this as $Ia \subseteq I$ and $aI \subseteq I$.

Definition 1.5.11: Principal Ideal

A *principal ideal* generated by a in a commutative ring R with unity is the set given by $\langle a \rangle = \{ar : r \in R\}$.

Definition 1.5.12: Maximum Ideal

An ideal M of R is called a *maximum ideal* if it is a proper ideal but there are no proper ideals of R containing it. That is, any ideal of R strictly containing M must be R itself.

Theorem 1.5.2
An ideal M of commutative ring with unity R is maximal if and only if R/M is a field.

Definition 1.5.13: Prime Ideal

An ideal P in a commutative ring with unity is a *prime* ideal if and only if whenever $ab \in P$ for elements a and b or R, then at least one of a or b is already in P.

Theorem 1.5.3
If P is an ideal of commutative ring R with unity, then R/P is an integral domain iff P is a prime ideal.

Theorem 1.5.4
$R[x]$ is a ring. If R is commutative, then so is $R[x]$. If R has unity, then so does $R[x]$. If R has no zero divisors, then neither does $R[x]$.

Theorem 1.5.5
Let R be a commutative ring with $\alpha \in R$ and $R[x]$ its ring of polynomials in the indeterminate x. There is an evaluation homomorphism $\phi_\alpha : R[x] \to R$ such that all x are replaced by α. That is, $\phi_\alpha(p(x)) = p(\alpha)$.

Note:
Here are the major steps to prove the Fundmental Theorem of Artihmetic:

1. Either n is prime or $n = ab$ is a factorization such that $a, b < n$.
2. If n is not prime, its smallest factor other than 1 is prime.
3. By strong induction, n can be factored into primes.
4. If $p|ab$ then $p|a$ or $p|b$.
5. Factorization is unique.

Theorem 1.5.6
Let $f(x), g(x) \in F[x]$ where F is a field and $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ such that

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

and either $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x)$.

Definition 1.5.14: Root

Define $\alpha \in F[x]$ to be a root of $f(x)$ if $\phi_\alpha(f(x)) = 0$.

Corollary 1.5.3
In $F[x]$, α is a root of $f(x)$ iff $(x - \alpha)$ is a factor of $f(x)$.

Corollary 1.5.4
A polynomial of degree n in $F[x]$ can have at most n roots.

Theorem 1.5.7

Given any two polynomials $a(x)$ and $b(x)$, not both zero, in $F[x]$, their gcd exists, is unique, and and can be written as a combination $s(x)a(x) + t(x)b(x)$ for some polynomials s and t in $F[x]$.

Definition 1.5.15: Irreducible

In a ring R, an element a is *irreducible* if its only divisors are units and associates. (x and y are associates if $x = uy$ for some unit u.)

Example 1.5.2

$2x^3 + 2x + 1 = (x + 1)(2x^2 + x + 1)$ in $\mathbb{Z}_3[x]$. However, if we look at $\mathbb{Z}_{11}[x]$, this does not remain true; the polynomial is irreducible.

Theorem 1.5.8 Gauss' Lemma

The product of two primitive polynomials is primitive. A primitive polynomial is irreducible over the integers if and only if it is irreducible over the rational numbers. In particular, if $p(x)$ is a monic polynomial with integer coefficients that factors into two polynomials $\alpha(x)\beta(x)$ with rational coefficients, then it factors into the product of two integer monic polynomials $a(x)b(x)$ with the degrees of a and b equalling thoseof α and β respectively.

Corollary 1.5.5

Let $p(x)$ be a monic polynomial with integer coefficients, and a nonzero constant term. Then any rational root of $p(x)$ must be an integer. Such root divides the constant term.

Note:

The above is a baby version of the rational root theorem.

Corollary 1.5.6 Einsenstein's Criterion

Let $f(x)$ be a polynomial and let p be prime. Assume that $p \nmid a_n$ (the leading coefficient) but that p divides every other coefficient. Also assume that $p^2 \nmid a_0$. Then $f(x)$ is irreducible over $\mathbb{Q}$.

Definition 1.5.16: Unique Factorization Domain

An integral domain is an *unique factorization domain* or *UFD* if:

1. Every element other than zero or a unit can be written as a product of irreducible elements of the integral domain.
2. If $a = p_1p_2 \ldots p_n = q_1q_2 \ldots q_m$ are two factorizations of a into irreducibles, then $n = m$ and there is a permutation π of the q's so that p_i and $q_{\pi(i)}$ are associates.

Definition 1.5.17: Principal Ideal Domain

An integral domain is a *principal ideal domain* or *PID* if every ideal is principal.

Theorem 1.5.9

In a PID, an element a is irreducible iff $\langle a \rangle$ is maximal; a is prime $\langle a \rangle$ is a prime ideal.

Corollary 1.5.7

In a principal ideal domain all irreducibles are prime.

Definition 1.5.18: Noetherian

A ring satisfies the ascending chain condition (ACC) if, given a chain of ideals $I_1 \subset I_2 \subset \cdots$ the chain eventually becomes stable. That is, there is some positive integer such that $I_n = I_N$ for all $n > N$. Such rings are called *Noetherian*.