PMATH347: Groups & Rings

Felix Zhou[1]

Spring 2020
University of Waterloo

[1]from Professor William Slofstra's Lectures

Contents

Chapter 1

Introduction

1.1 What is Math?

1.1.1 Numbers

Generalizing numbers from natural numbers all the way to $\mathbb{C}$.

1.1.2 Algebra

Manipulating expressions? Solving equations?

Algebra is about operations.

1.1.3 Abstract Algebra

Study operations abstractly.

1.2 Binary Operations

Definition 1.2.1 (Binary Operation)
A binary operation on a set X is a function

$$b : X \times X \to X$$

We can use function notation or inline notation such as in addition or multiplication. If there is no chance of confusion, we can simply use concatentation to simply inline notation.

Definition 1.2.2 (*k*-nary Operation)
a k-nary operation on a set X is a function

$$X^k \to X$$

Definition 1.2.3 (Unary Operation)
1-ary operation.

Remark that the map $x \mapsto \frac{1}{x}$ is not a unary operation on $\mathbb{Q}$ but it is on

$$\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$$

1.3 Associativity & Commutativity

1.3.1 Associativity

Definition 1.3.1 (Associative)
A binary operation is associative if for all $a, b, c \in X$

$$a(bc) = (ab)c$$

Addition in $\mathbb{C}$, polynomial, and functions have this property. Some other examples matrix addition and multiplication, modular addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ and finally, function composition.

However, subtraction, equivalent to adding by additive inverse, is NOT associative.

Definition 1.3.2 (Bracketing)
A bracketing of a sequence $a_1, \ldots, a_n \in X$ is a way to indicate the order in which we evaluate some binary operation.

Proposition 1.3.1
A binary operation is associative if and only if for all finite sequences $a_1, \ldots, a_n \in X$, every bracketing of this sequence evaluates to the same element of X.

Proof ($\implies$)
By induction on n.

The base case is $n \leq 3$, which follow directly from the definition of associativity. Then consider the outer most bracket and notice that it separates the bracketing into two smaller sub-bracketings.

By induction re-order the sub-brackets into

$$((a_1 a_2) \dots a_k)(a_{k+1} \dots (a_{n-1} a_n))$$

Notice then we can "migrate" brackets from lhs to rhs to obtain

$$(a_1(a_2 \dots (a_{n-1} an)))$$

Since this is true for any bracketing, we are done.

1.3.2 Commutativity

Definition 1.3.3 (Commutative)
A binary operation is commutative (abelian) if

$$ab = ba$$

for all $a, b \in X$.

This Course

We will focus on groups associative but not necessarily commutative operations. For rings, we will focus on those with associative and commutative operations

1.4 Identities & Inverses

1.4.1 Identities

Definition 1.4.1 (Identity)
Let $\cdot$ be a binary operation on a set X.
$e \in X$ is an identity for $\cdot$ if

$$ex = xe = x$$

for all $x \in X$.

This is the ”zero” in addition or the ”one” in multiplication.

Lemma 1.4.1
Identities are unique.

Proof
$e = e \cdot e' = e'$.

1.4.2 Inverses

Definition 1.4.2 (Inverse)
Let $\cdot$ be a binary operation on X with an identity element e.
$y \in X$ is a left inverse for x if

$$yx = e$$

a right inverse for x if

$$xy = e$$

and an inverse if it is both a left and right inverse.

Lemma 1.4.2
Let $\cdot$ be an associative binary opearation with an identity e on X. If y_L, y_R are left, right identities respectively, then

$$y_L = y_R$$

Proof

$$\begin{aligned} y_L &= y_L e \\ &= y_L(xy_R) \\ &= (y_L x)y_R \\ &= ey_R \\ &= y_R \end{aligned}$$

Corollary 1.4.2.1
If x has both a right and left inverse, it has a unique inverse.

In general, left and right inverses are not unique. It is also possible to ONLY be left or ONLY be right invertible.

Definition 1.4.3 (Invertible)
An element $a \in X$ is invertible if it has an inverse, in which case the inverse is denoted by a^{-1}.

Properties of Inverses

Lemma 1.4.3

1. If $\cdot$ has identity e, e is invertible with $e^{-1} = e$
2. If a is invertible, then so is a^{-1}, with $(a^{-1})^{-1} = a$
3. If $\cdot$ is associative, and a, b are invertible, then so is ab with $(ab)^{-1} = b^{-1}a^{-1}$

Proposition 1.4.4
Let $\cdot$ be an associative binary operation on X with identity e. Let x, y be variables in X.
An element $a \in X$ is invertible $\iff$

$$ax = b, ya = b$$

have unique solutions.

1.4.3 Left & Right Cancellation Property

Proposition 1.4.5
Let $\cdot$ be an associative binary operation and $a \in x$.

1. If a has a left inverse and $au = av$, then $u = v$
2. If b has a right inverse and $ua = va$, then $u = v$.

Part I

Group Theory

Chapter 2

Groups

2.1 Definitions

Definition 2.1.1 (Group)
A group is a pair $(G, \cdot)$ where

(i) G is a set

(ii) $\cdot$ is an associative binary operation on G which has an identity e and every element of G is invertible

Definition 2.1.2 (Abelian Group)
A group is Abelian (commutative) if $\cdot$ is abelian.

Definition 2.1.3 (Finite Group)
A group is finite if G is a finite set.

Definition 2.1.4 (Order)
The order of G is the nunber of elements in G if G is finite and $+\infty$ if G is infinite.

We denote the order of G by $|G|$.

2.1.1 Some Terminology / Notation

We typically refer to $(G, \cdot)$ simply as G and assume the operation is given.

The identity of G is denoted by e or e_G to explicitly indicate it is the identity for the group G. $1, 1_G$ can also be used.

Since every element of a group is invertible, the map $g \mapsto g^{-1}$ is well-defined and is therefore an unary operation.

We will write exponentation to denote repeated multiplication. For example

$$(gh)^n = ghgh \dots gh$$

which is NOT necessarily the same as $g^n h^n$ if G is not Abelian!

2.2 Remarks & Immediate Results

Let $\iota : G \to G$ be the inverse map $g \mapsto g^{-1}$. Remark that it has an inverse. Namely

$$\iota \circ \iota = \mathrm{Id}_G$$

and thus ι is a bijection.

2.2.1 Examples

Definition 2.2.1 (Trivial Group)
Any singleton set forms a group with the single element being the identity.

Definition 2.2.2 (General Linear Group)
We write $\mathrm{GL}_n(\mathbb{K})$ to denote the invertible $n \times n$ matrices with entires in field $\mathbb{K}$.

$\mathrm{GL}_n(\mathbb{K})$ is a group and for $n \geq 2$, it is non-abelian.

2.2.2 Additive Notation

For groups like $(\mathbb{Z}, +)$, it is confusing to write mn instead of $m + n$.

For abelian groups G, we can write $+$ to denote the group operation. The identity is denoted by $0, 0_G$ and the inverse by $-g \in G$. Finally, we write

$$ng := \underbrace{g + g + \cdots + g}_{n}$$

For nonabelian groups, we always use multiplicative notation. For abelian groups, we must choose one of the two and be explicit about which one we choose!

2.2.3 Useful Tools

Definition 2.2.3 (Multiplication Table)
A table with rows and columns indexed by elements of G. The cells contain the product of indices.

This is defined for finite and infinite groups but only makes sense for (small) finite groups.

Definition 2.2.4 (Order)
If G is a group, the order of $g \in G$ is

$$|g| := \min\{k \geq 1 : g^k = e_G\} \cup \{\infty\}$$

Notice that $|g| = 1 \iff g = e_G$ and if $g^n = 1$ then $g^{-1} = g^{n-1}$!

Lemma 2.2.1
$g^n = e \iff g^{-n} = e$ so

$$|g| = |g^{-1}|$$

Proof
$g^n = e \iff (g^n)^{-1} = e^{-1} = e$.

But also $g^{-n} = (g^{-1})^n$.

2.3 Dihedral Groups

Definition 2.3.1 (n-gon)
A regular poly P_n with n vertices, for some $n \geq 3$, is an n-gon.

We can identify points of the (complex) unit circle with vertices and get the polygon and "connecting" adjacent points with straight lines.

Let

$$v_k := \left(\cos\frac{2\pi k}{n}, \sin\frac{2\pi k}{n}\right) = e^{\frac{2\pi k}{n}}$$

Then

$$P_n := \{\lambda v_k + (1-\lambda)v_{k+1} : 0 \leq k < n, \lambda \in [0,1]\}$$

where $v_n = v_0$.

Definition 2.3.2 (Symmetry)
A symmetry of the n-gon is some $T \in \mathrm{GL}_2(\mathbb{R})$ such that

$$TP_n = P_n$$

Definition 2.3.3 (Dihedral Group)
The set of symmetries of P_n denoted by D_{2n} or D_n.

Proposition 2.3.1
D_{2n} is a group under composition.

Proof
D_{2n} is a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

2.3.1 Results

Lemma 2.3.2

1. If $T \in D_{2n}$ then $T(v_0), T(v_1)$ are adjacent
2. If $S, T \in D_{2n}$ and $S(v_i) = T(v_i)$ for $i = 0, 1$ then $S = T$

Proof

1. $v_0, v1$ are adjacent and T is linear, thus the line between them are preserved
2. v_0, v_1 for a basis and uniquely determines linear maps.

Corollary 2.3.2.1
$|D_{2n}| \leq 2n$.

Proof
The injective map $D_{2n} \to A$ given by

$$T \mapsto (Tv_0, Tv_1)$$

has an image of cardinality $2n$.

Remark that if we show that there are $2n$ distinct elements of D_{2n}, then $|D_{2n}| = 2n$!

2.3.2 Rotations & Reflections

Let $s \in D_{2n}$ be the rotation by $\frac{2\pi}{n}$ radians so $|s| = n$. Notice $s^n = e$ and $s^k \neq e$ for all $1 \leq k < n$.

Consider r, the reflection through the $x - axis$. Clearly $|r| = 2$ as $r^2 = e$ while $r \neq e$.

$$r(v_0) = 0, r(v_1) = v_{n-1}$$

We see that

$$s^i(v_0) = v_i, s^i(v_1) = v_{i+1}$$

and

$$s^i r(v_0) = v_i, s^i r(v_1) = v_{i-1}$$

are all unique elements of D_{2n}.

Proposition 2.3.3
$D_{2n} = \{s^i r^j : 0 \leq i < n, 0 \leq j < 2\}$, so $|D|_{2n} = 2n$.

Now, consider what is rs?

$$rs(v_0) = v_{n-1}, rs(v_1) = v_{n-2}$$

so $rs = s^{n-1}r = s^{-1}r$.

Corollary 2.3.3.1
D_{2n} is a finite nonabelian group.

2.4 Permutation Groups

Let $\text{Fun}(X, X)$ be the set of functions $X \to X$ on a set X. Let S_X denote the subset of $\text{Fun}(X, X)$ which are bijections.

S_X form a group uner composition with idenity Id_X.

Definition 2.4.1 (Symmetric Groups)
The symmetric (permutation) group S_n is the group S_X with $X = [n]$.

Let π be a variable in S_X. There are n choices for $\pi(1)$, $n - 1$ for $\pi(2)$, and so on. So

$$|S_n| = n!$$

2.4.1 Permutations

The elements of S_n are called permutations.

Representations

Two-line

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

One-line $pi = \pi(1)\pi(2)\dots\pi(n)$

Disjoint cycle We can write (163) to indicate $\pi(1) = 6, \pi(6) = 3, \pi(3) = 1$. We can write π as the concatentation of all cycles of length 2 or more. The identity is empty under this notation so we use e

2.4.2 Multiplication

We can do multiplication (composition) in two-line or disjoint cycle notation

For the two-line representation, we can just follow composition through both permutations.

For cycle notation, it is more tricky. We also want to follow the composition through both permutations but start at 1 and proceed to "follow" the cycle until it is complete. Then we more on to the next smallest unchosen number.

We rarely use one-line notation as it is a bit of a pain.

2.4.3 Inverses

Inverses are equally as easy.

We can simply invert the rows of the two-line representation and sort the first row.

For the cycle notation, it is the same cycles but reversed. Simply start at the same initial element, then the last, the second last, etc.

2.4.4 Fixed Points & Support Sets

Let $\pi \in S_n$.

Definition 2.4.2 (Fixed Point)
A fixed point of π is $i \in [n]$ such that

$$\pi(i) = i$$

Definition 2.4.3 (Support Set)
the support set of π is

$$\text{supp}(\pi) = \{i \in [n] : \pi(i) \neq i\}$$

In general, the support set are numbers that appear in the disjoint cycle representation.

Definition 2.4.4 (Disjoint)
$\pi, \sigma \in S_n$ are disjoint if

$$\text{supp}(\pi) \cap \text{supp}(\sigma) = \varnothing$$

Remark that $\text{supp}(\pi) = \varnothing \iff \pi = e$. Also, $\text{supp}(\pi^{-1}) = \text{supp}(\pi)$. Finally, if $i \in \text{supp}(\pi)$ then $\pi(i) \in \text{supp}(\pi)$.

2.4.5 Commuting Elements

Definition 2.4.5
$g, h \in G$ commute if $gh = hg$.

Lemma 2.4.1
If $\pi, \sigma \in S_n$ are disjoint, then $\pi\sigma = \sigma\pi$.

Proof
For all $i \in [n]$, $i \in \text{supp}(\pi)$ or $i \in \text{supp}(\sigma)$ but not both.

2.4.6 Cycles

Definition 2.4.6 (k-Cycle)
A k-cycle is an element of S_n with disjoint cycle notation $(i_1 i_2 \cdots_k)$.

Let $c_i c_2 \ldots_\ell = \pi \in S_n$ be the cycles of π. We can regard c_i as an element of S_n and π as the product of cycles! Clearly c_i, c_j are disjoint for $i \neq j$ so $c_i c_j = c_j c_i$. In particular, the order of cycles in the disjoint cycle representation does not matter.

Since we can interpret $\pi = c_1 \cdot \cdots \cdot c_k$, we immediately get

$$\pi^{-1} = c_k^{-1} \cdot \cdots \cdot c_1^{-1} = c_1^{-1} \cdot \cdots \cdot c_k^{-1}$$

Note that if c, c' are NOT disjoint cycles, they do not necessarily commute.

However, for $\pi \in S_n$, π commutes with π^i for all i, but $\text{supp}(\pi), \text{supp}(\pi^i)$ are not necessarily (or even typically) disjoint.

Chapter 3

Subgroups & Homomorphisms

3.1 Subgroups

Definition 3.1.1 (Subgroup)
Let $(G, \cdot)$ be a group. $H \subseteq G$ is a subgroup if

(i) $g, h \in H \implies gh \in H$

(ii) $g \in H \implies g^{-1} \in H$

(iii) $e_G \in H$

We write $H \leq G$ to denote subgroup.

Example 3.1.1
For $G = D_{2n}$, $H := \{e, s, s^2, \ldots, s^{n-1}\}$ forms a group.

Definition 3.1.2 (Trivial Subgroup)
$\{e\}$

Notice that G is a subgroup of G, we say a subgroup H of G is proper if $H \neq G$. Furthermore, we say H is a proper nontrivial subgroup of G is $\{e\} \neq H < G$.

Proposition 3.1.2
If H is a subgroup of $(G, \cdot)$, then H is a group under the restriction $\cdot\big|_{H \times H}$.

We can do a faster check for subgroups.

Proposition 3.1.3
$H \leq G$ if and only if

(i) $H \neq \varnothing$

(ii) $gh^{-1} \in H$ for all $g, h \in H$.

For finite subgroups, there is an even simpler check.

Proposition 3.1.4
$H \subseteq G, |H| < \infty$ is a subgroup of G if and only if

(i) $H \neq \varnothing$

(ii) $gh \in H$ for all $g, h \in H$

3.1.1 Generated Subgroups

Proposition 3.1.5
If $\mathcal{F}$ is a non-empty collection of subgroups of G

$$K := \bigcap_{H \in \mathcal{F}} H$$

is a subgroup of G.

Definition 3.1.3
Let $S \subseteq G$. The subgroup generated by S in G is

$$\langle S \rangle := \bigcap_{S \subseteq H \leq G} H$$

Notice that $\langle S \rangle$ is the smallest subgroup of G containing S.

If $S = \{s_1, s_2, \ldots\}$, we often write

$$\langle S \rangle = \langle s_1, s_2, \ldots \rangle$$

Example 3.1.6
$s \in D_{2n}$ generates the subgroup

$$K := \{e, s, s^2, \ldots\}$$

For $S \subseteq G$, write

$$S^{-1} := \{s^{-1} : s \in S\}$$

Proposition 3.1.7
If $S \subseteq G$ and

$$K := \{e\} \cup \{s_1 \times s_2 \times \cdots \times s_k : k \geq 1, s_1, \ldots, s_k \in S \cup S_{-1}\}$$

then

$$\langle S \rangle = K$$

Proof
$K \subseteq \langle S \rangle$ This is obvious since $\langle S \rangle$ is closed under multiplication and inverses.

$\langle S \rangle \subseteq K$ This is by definition as K is a subgroup containing S and $\langle S \rangle$ is the smallest subgroup containing S.

Lattice of Subgroups

Subgroups of G are partialled ordered by inclusion.

Definition 3.1.4 (Lattice of Subgroups)
The collection of subgroups of G with order $\leq$.

3.2 Cyclic Groups

Definition 3.2.1 (Generator)
$S \subseteq G$ generates G if $\langle S \rangle = G$.

Definition 3.2.2 (Cyclic)
We say G is cyclic if $G = \langle a \rangle$ for some $a \in G$.

Notice that generators are not in general unique since a, a^{-1} are both generators.

Definition 3.2.3 (Cyclic Subgroup)
If G is a group with $a \in G$. Then $\langle a \rangle$ is a cyclic group for any $a \in G$.
We say this is the cyclic subgroup generated by a.

Lemma 3.2.1
If $a \in G$ then
$$\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$$

Lemma 3.2.2
If $|a| = n$ then
$$\langle a \rangle = \{a^i : 0 \leq i < n\}$$

Proposition 3.2.3
If $G = \langle a \rangle$, then
$$|G| = |a|$$

Proof
We know $|a| \leq |G|$.

Note this means if $|a| = \infty$, then there is nothing else to prove.

Suppose $|a| < \infty$. We know $\langle a \rangle = \{a^i : 0 \leq i < |a|\}$. So $|G| \leq |a|$.

3.2.1 $\mathbb{Z}/n\mathbb{Z}$

Lemma 3.2.4
Suppose $G = \langle S \rangle$.
$G = \langle T \rangle$ if and only if $S \subseteq \langle T \rangle$.

This shows that $\mathbb{Z}/n\mathbb{Z} = \langle a \rangle$ if and only if $1 \in \langle a \rangle$. In particular a has a multiplicative inverse mod n. So a, n must be relatively prime.

Order of Elements

Lemma 3.2.5
If G is a group with $g \in G, g^n = e$, then
$$|g| | n$$

Lemma 3.2.6
Suppose $a|n$, then
$$|a| = \frac{n}{a}$$

Proof
Clearly $|a| \leq \frac{n}{a}$.

But then $\ell a \neq n$ for all $1 \leq \ell < \frac{n}{a}$ so $|a| \geq \frac{n}{a}$ as well.

Lemma 3.2.7
Suppose $a \in \mathbb{Z}$ with $b = \gcd(a, n)$. Then
$$\langle a \rangle = \langle b \rangle$$

Proof
Clearly $a \in \langle b \rangle$ as $b|a$.

There is some $x, y \in \mathbb{Z}$ such that
$$xa + yn = b$$
so $b = xa$ and $b \in \langle a \rangle$ as desired.

Proposition 3.2.8
Suppose $a \in \mathbb{Z}$. Then
$$|a| = \frac{n}{\gcd(a, n)}$$

Proof
Define $b = \gcd(a, n)$. Our work prior says $\langle a \rangle = \langle b \rangle$.

Then
$$|a| = |\langle a \rangle| = |\langle b \rangle| = |b|$$

Finally
$$|b| = \frac{n}{b}$$

Corollary 3.2.8.1
The order d of any cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ divides n.
In addition, there is a unique cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d for every $d|n$. It is generated by $a = \frac{n}{d}$.

Proof
Set $|\langle a\rangle| = d$. We know $d = \frac{n}{\gcd(a,n)}$ by the lemma above so $d|n$.

Conversely, if $d|n, a := \frac{n}{d}$ then $|\langle a\rangle| = d$ as desired.

3.3 Homomorphisms

Definition 3.3.1 (Group Homomorphism)
Let G, H be groups. $\phi : G \to H$ is a homomorphism (morphism) if

$$\phi(gh) = \phi(g)\phi(h)$$

for all $g, h \in G$.

Lemma 3.3.1
Let $\phi : G \to H$ be a homomorphism

(a) $\phi(e_G) = e_H$

(b) $\phi(g^{-1}) = \phi(g)^{-1}$

(c) $\phi(g^n) = \phi(g)^n$

(d) $|\phi(g)|$ divides $|g|$ for all $g \in G$ (assuming $n|\infty$ for all $n \in \mathbb{N}$)

Lemma 3.3.2
If $H \leq G$ then the $i : H \to G$

$$x \mapsto s$$

is a homomorphism.

Lemma 3.3.3
If $\phi : G \to H, \varphi : H \to K$ are homomorphism, then $\varphi \circ \phi$ is a homomorphism.

Corollary 3.3.3.1
If $\phi : G \to H$ is a homomorphism, then for all $K \leq G$

$$\phi\Big|_K$$

is a homomorphism.

3.3.1 Images of Homomorphisms

Proposition 3.3.4
If $\phi : G \to H$ is a homomorphism with $K \leq G$

$$\phi(K) \leq H$$

Definition 3.3.2 (Image Subgroup)
Given $\phi : G \to H$ a homomorphism, the image of ϕ is the subgroup

$$\phi(G) \leq H$$

Lemma 3.3.5
If $\phi : G \to H$ is a homomorphism with

$$\phi(G) \leq K \leq H$$

then $\tilde{\phi} := G \to K$ given by

$$x \mapsto \phi(x)$$

is still a homomorphism with $\tilde{\phi}(G) \leq K$.

Lemma 3.3.6
A homomorphism $\phi : G \to H$ is surjective if and only if

$$\phi(G) = H$$

Corollary 3.3.6.1
ϕ induces a surjective homomorphism

$$\tilde{\phi} : G \to K$$

where $K = \phi(G)$.

Proposition 3.3.7
Let $\phi : G \to H$ be a homomorphism with $S \subseteq G$. Then

$$\phi\langle S\rangle = \langle \phi(S)\rangle$$

3.3.2 Pre-Images of Homomorphisms

Proposition 3.3.8
If $\phi : G \to H$ is a homomorphism and $K \leq H$. Then

$$\phi^{-1}(K) \leq G$$

Definition 3.3.3 (Kernel)
If $\phi : G \to H$ is a homomorphism, then the kernel of ϕ is

$$\phi^{-1}(\{e_H\})$$

Remark that the kernel is always a subgroup of G.

Proposition 3.3.9
A homomorphism $\phi : G \to H$ is injective if and only if $\ker \phi = \{e_G\}$.

Proposition 3.3.10
If H is a subgroup of a cyclic group G, then H is cyclic.

Proof
Since G is cyclic, there is a surjective homomorphism $\phi : \mathbb{Z} \to G$.

As all subgroups of $\mathbb{Z}$ are cyclic, there is $m \in \mathbb{Z}$ such that

$$\phi^{-1}(H) = \langle m \rangle$$

Let $\varphi : \mathbb{Z} \to \mathbb{Z}$ be a homomorphism with

$$\varphi(k) = mk$$

It follows that $\phi \circ \varphi : \mathbb{Z} \to G$ is a homomorphism.

We have

$$\begin{aligned} \phi \circ \varphi(\mathbb{Z}) &= \phi(m\mathbb{Z}) \\ &= \phi(\phi^{-1}(H)) \\ &= H \end{aligned}$$

So we can restrict $\phi \circ \varphi$ to get a surjective homomorphism

$$\mathbb{Z} \to H$$

We conclude H is cyclic.

3.4 Isomorphisms

Definition 3.4.1 (Isomorphism)
Bijective homomorphism.

Lemma 3.4.1
$\phi : G \to H$ is isomorphic if and only if $\ker\phi = \{e_G\}$ and

$$\phi(G) = H$$

Proposition 3.4.2
The inverse of an isomorphism is also an isomorphism.

Corollary 3.4.2.1
A homomorphism $\phi : G \to H$ is an isomorphism if and only if there is a homomorphism $\varphi : H \to G$ such that

$$\varphi \circ \phi = 1_G, \phi \circ \varphi = 1_H$$

Definition 3.4.2 (Isomorphic)
We say G, H are isomorphic if there exists an isomorphism $\phi : G \to H$.

We write $G \cong H$ in this case.

Proposition 3.4.3
If G, H are cyclic groups, then $G \cong H$ if and only if

$$|G| = |H|$$

Corollary 3.4.3.1
Let G be a cylic group.
If $|G| = \infty$, then $G \cong \mathbb{Z}$. Else if $|G| = n < \infty$, then $G \cong \mathbb{Z}/n\mathbb{Z}$.

Corollary 3.4.3.2
Cyclic groups are abelian.

It may be useful to have multiplicative form of cylic groups. Let a be a formal indeterminate.

Write

$$C_\infty := \{a^i : i \in \mathbb{Z}\}$$
$$C_n := \{a^i : i \in \mathbb{Z}/n\mathbb{Z}\}$$

Chapter 4

Lagrange's Theorem

4.1 Cosets

4.1.1 Motivation

Let $T : V \to W$ be a linear map between two vector spaces. We are concerned with the solutions to

$$Tx = b$$

If $b \in \operatorname{Im} T$, then all solutions are in the form

$$x_0 + \ker T$$

Definition 4.1.1 (Affine Subspace)
$x_0 + \ker T$

This is like a linear subspace but does not necessarily contain 0.

4.1.2 Cosets

Let$S \subseteq G, g \in G$.

Definition 4.1.2 (Left Coset)
A left coset of H in G is a set of the form

$$gH := \{gh : h \in H\}$$

Definition 4.1.3 (Right Coset)
A right coset of H in G is a set of the form

$$Hg := \{hg : h \in H\}$$

Example 4.1.1
The right cosets of $\langle s \rangle \subseteq D_{2n}$ are $\langle s \rangle, \langle s \rangle r$.

The left cosets of $\langle s \rangle \subseteq D_{2n}$ are $\langle s \rangle, r\langle s \rangle = \langle s \rangle r$.

The left cosets of $\langle r \rangle \subseteq D_{2n}$ are $\langle r \rangle, s^i\langle r \rangle$ for $0 \leq i < n$.

The right cosets of $\langle r \rangle \subseteq D_{2n}$ are $\langle r \rangle, \langle r \rangle s^i$ for $0 \leq i < n$.

We write

$$G/H := \{gH : g \in G\}$$

and

$$H \setminus G := \{Hg : g \in G\}$$

to denote the set of left/right cosets of H in G.

4.1.3 Cosets of a Kernel

Suppose $\phi : G \to K$ is a homomorphism and $H := \ker \phi$.

Lemma 4.1.2
Suppose $\phi(x_0) = b$, the set of solutions

$$\phi^{-1}\{b\}$$

is

$$x_0 H = H x_0$$

Proof
If $\phi(x_1) = b$

$$\phi(x_0^{-1}x_1) = b^{-1}b = e$$

so $x_0^{-1}x_1 \in H$ and

$$x_1 = x_0(x_0^{-1}x_1) \in x_0 H$$

Conversely, if $x_1 = x_0 h$ for $h \in H$, then

$$\phi(x_1) = \phi(x_0)\phi(h) = b$$

so every element of $x_0 H$ is a solution.

The case for right cosets is idential.

Proposition 4.1.3
If $\phi : G \to K$ is a homomorphism, then there is a bijection between

$$G/\ker\phi, \operatorname{Im}\phi$$

Proof
Fix $\phi(g) \in \operatorname{Im} G$. Then $g \ker\phi$ is the set of solutions $\phi(x) = \phi(g)$. So

$$\phi(g\ker\phi) = \{\phi(g)\}$$

and we have surjectivity.

To see injectivity

$$g\ker\phi = \phi^{-1}\{\phi(g)\}$$

by the lemma.

Example 4.1.4
The map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by

$$a \mapsto [a]$$

has kernel of $n\mathbb{Z}$ with the image being $\mathbb{Z}/n\mathbb{Z}$.

Thus

$$a + n\mathbb{Z}$$

is the set of solutions to $[x] = [a]$.

4.2 Lagrange's Theorem

4.2.1 Group Index

Given $H \leq G$, how many left cosets does H have?

Definition 4.2.1 (Index)
The index of H in G is

$$[G : H] := \begin{cases} |G/H|, & |G/H| < \infty \\ \infty, & \text{else} \end{cases}$$

Why use the left cosets?

Proposition 4.2.1
The function $\phi : G/H \to H \setminus G$ given by

$$S \mapsto S^{-1}$$

is a bijection.

Proof
Suppose $S \in G/H$ so $S = gH$ for some $g \in G$.

$$\begin{aligned} S^{-1} &= \{h^{-1}g^{-1} : h \in H\} \\ &= \{hg^{-1} : h \in H\} && h \mapsto h^{-1} \text{ is bijection} \\ &= Hg^{-1} \end{aligned}$$

Thus we can actually use either the left or right coset to define the index.

4.2.2 Lagrange's Theorem

Proposition 4.2.2
Let $H \leq G$ and $g, k \in G$. The following are equivalent.

(a) $g^{-1}k \in H$

(b) $k \in gH$

(c) $gH = kH$

(d) $gH \cap kH \neq \varnothing$

Proof
$\underline{(a) \implies (b)}$ Trivial.

$\underline{(b) \implies (c)}$ Suppose $k = gh$ for some $h \in H$.

If $kh' \in kH$ then $kh' = g(hh') \in gH$. Thus $kH \subseteq gH$.

But for all $gh' \in gH$, we have $gh' = kh^{-1}h' \in kH$. So $gH \subseteq kH$ as well.

$\underline{(c) \implies (d)}$ Trivial.

$\underline{(d) \implies (e)}$ Pick $x \in gH \cap kH$ so $x = gh_1, = kh_2$. Thus

$$g^{-1}k = h_1h_2^{-1} \in H$$

Corollary 4.2.2.1
If $H \leq G$, then G/H is a partition of G.

Proof
$g \in gH$, thus every element belongs to some left coset in G/H.

Suppose $S \neq T \in G/H$ shares an element. Then $S = T$ by the previous proposition.

Lemma 4.2.3
If $S \subseteq G, g \in G$ then the map $S \to gS$

$$s \mapsto gs$$

is a bijection.

Proof
The inverse is given by $gS \to S$

$$gs \mapsto g^{-1}gs = s$$

So if H is finite and $g \in G$

$$|gH| = |H|$$

Theorem 4.2.4 (Lagrange)
If $H \leq G$ then

$$|G| = [G : H] \cdot |H|$$

Proof
If $|H| = \infty$ then $|G| = \infty$.

By the fact that cosets partition G

$$[G : H] = \infty \implies |G| = \infty$$

Now, suppose $|H|, [G : H] < \infty$. By the lemma

$$|gH| = |H|$$

for all $h \in G$.

Thus G is a disjoint union of equally sized cosets G/H and

$$|G| = [G : H] \cdot |H|$$

Fix $H \leq G$. Looking back we could have defined $\sim_H$ on G by

$$g \sim_H k \iff g^{-1}k \in H$$

This is an equivalence relation by our work earlier and thus partitions G precisely into the classes

$$[g] = gH$$

Consequences

Corollary 4.2.4.1
If $x \in G$ then $|x|$ divides $|G|$.

Proof
$|x| = |\langle x \rangle|$ and the latter divides G.

Corollary 4.2.4.2
If $|G|$ is prime, then G is cyclic.

Proof
Let $e \neq x \in G$. then $|x| \neq 1$ but divides $|G|$ so it is equal to $|G|$. Thus

$$|\langle x \rangle| = |G| \implies \langle x \rangle = |G|$$

Corollary 4.2.4.3
If $\phi : G \to K$ is a homomorphism, then

$$|\operatorname{Im} \phi| = [G : \ker \phi]$$

and hence divides $|G|$.

Notice how $|\operatorname{Im} \phi|$ is the cardinality of a subgroup of K and thus also divides $|K|$.

Proposition 4.2.5
If G, K have coprime order, then the only homomorphism $\phi : G \to K$ is the trivial homomorphism

$$g \mapsto e_K$$

Chapter 5

Normal Subgroups

5.1 Definitions

5.1.1 Motivation

Proposition 5.1.1
Suppose $H \leq G$ and $g, k \in G$. Then following are equivalent.

(a) $kg^{-1} \in H$

(b) $k \in Hg$

(c) $Hg = Hk$

(d) $Hg \cap Hk \neq \varnothing$

Proof
Symmetric to the proof of proposition earlier.

This begs the question of when a right coset a left coset.

Lemma 5.1.2
If $H \leq G$ and $Hg = hH$ for $g, h \in G$

$$gH = Hg, hH = Hh$$

Proof
$g \in Hg = hH$ so

$$gH = hH = Hg$$

Similarly, $h \in hH = Hg$ so

$$Hh = Hg = hH$$

5.1.2 Normal Subgroup

Definition 5.1.1 (Normal Subgroup)
$N \leq G$ is a normal subgroup if

$$gN = Ng$$

for all $g \in G$.

' We will write $N \trianglelefteq G$ to denote a normal subgroup of G.

Definition 5.1.2 (Conjugate)
If $g, h \in G$, the conjugate of h by g is

$$ghg^{-1}$$

Observe that

$$gSg^{-1} = \{ghg^{-1} : h \in S\}$$

and so

$$gN = Ng \iff gNg^{-1} = N$$

This gives us

$$S \subseteq T \iff gS \subseteq gT \iff Sg \subseteq Tg$$

5.1.3 Equivalent Characterizations

Proposition 5.1.3
Let $N \leq G$. The following are equivalent.

(1) $N \trianglelefteq G$

(2) $gNg^{-1} = N$ for all $g \in G$

(3) $gNg^{-1} \subseteq N$ for all $g \in G$

(4) $G/N = N\backslash G$

(5) $G/N \subseteq N\backslash G$

(6) $N/G \subseteq G/N$.

Proof

(1) $\iff$ (2) Done.

(2) $\implies$ (3) Trivial.

(3) $\implies$ (2) Suppose $gNg^{-1} \subseteq N$ for all $g \in G$. Then

$$g^{-1}Ng \subseteq N \implies N \subseteq gNg^{-1}$$

so we have equality.

(1) $\implies$ (4) $\implies$ (5), (6) Trivial.

(5) $\implies$ (1) Suppose $G/N \subseteq N\backslash G$. Then for all $g \in G$

$$gN = Nh$$

for some $h \in G$.

By the lemma $gN = Ng$.

(6) $\implies$ (1) Suppose $N\backslash G \subseteq G/N$. Then for all $g \in G$

$$Ng = hN$$

for some $h \in G$.

Thus by the lemma $Ng = gN$.

Remark that if G is abelian, all subgroups are of course normal.

If $\phi : G \to K$ is a homomorphism, then $\ker\phi$ is normal! Indeed

$$G/\ker\phi, \ker\phi\backslash G$$

are precisely the solution sets to the equations

$$\phi(x) = b, b \in \operatorname{Im}\phi$$

so they are equivalent.

A Warning

$\trianglelefteq$ is NOT transitive while $\leq$ is!

For example

$$\langle r, s^2 \rangle \trianglelefteq D_8$$

and

$$\langle r \rangle \trianglelefteq \langle r, s^2 \rangle$$

since $\langle r, s^2 \rangle$ is commutative. But

$$\langle r \rangle \not\trianglelefteq \langle r, s^2 \rangle$$

5.2 Normalizers & The Centre

5.2.1 The Normalizer

Definition 5.2.1 (Normalizer)
Let $S \subseteq G$. Then

$$N_G(S) := \{g \in G : gSg^{-1} = S\}$$

is the normalizer of S in G.

Lemma 5.2.1
$N_G(S) \leq G$.

Proof
$eSe = S$ so the identity lives in the normalizer.

If $g, h \in N_G(S)$, then

$$ghS(gh)^{-1} = g(hSh^{-1})g^{-1} = S$$

so $gh \in N_G(S)$.

Clearly, $N_G(S)$ is closed under taking inverses. So we are done.

Lemma 5.2.2
Suppose $H \leq G$. Then

$$H \trianglelefteq G$$

if and only if

$$N_G(H) = G$$

Proof
Trivial.

Corollary 5.2.2.1
If $G = \langle S \rangle$ and $H \leq G$, then $H \trianglelefteq G$ if and only if

$$gHg^{-1} = H$$

for all $g \in S$.

Proof
$H \trianglelefteq G$ if and only if

$$N_G(H) = G$$

But since $N_G(H)$ is a subgroup of G, this happens if and only if

$$S \subseteq N_G(H)$$

As a word of precaution, it is entirely possible that

$$gHg^{-1} \subsetneq H, g \notin N_G(H)$$

Lemma 5.2.3
If $|g| < \infty$ and $gHg^{-1} \subseteq H$, then

$$g \in N_G(H)$$

Proof
We can argue by induction

$$g(g^{i-1}Hg^{-i+1})g^{-1}$$

so

$$g^{-1}Hg = g^{n-1}Hg^{-n+1} \subseteq H \implies H \subseteq gHg^{-1}$$

Combined with our initial assumption

$$gHg^{-1} = H$$

Corollary 5.2.3.1
Let $G = \langle S \rangle$ be finite and $H \leq G$. If $gHg^{-1} \subseteq H$ for all $g \in S$ then

$$H \trianglelefteq G$$

5.2.2 The Centre

Definition 5.2.2 (Centre)
If G is a group, then centre of G is

$$Z(G) := \{g \in G : gh = hg, h \in G\}$$

Example 5.2.4
$Z(\mathrm{GL}_n \mathbb{C}) = \{\lambda I_n : \lambda \neq 0\}$

Proposition 5.2.5
$Z(G) \trianglelefteq G$

Proof
By definition.

Chapter 6

Product Groups

How can we create more groups from pre-existing ones?

6.1 Definitions

Proposition 6.1.1
Suppose $(G_1, \cdot_1), (G_2, \cdot_2)$ are groups. Then

$$G_1 \times G_2$$

is a group under the operation

$$(g_1, g_2) \cdot (h_1, g_2) = (g_1 \cdot_1 h_1, g_2 \cdot_2 h_2)$$

Definition 6.1.1 (Product)
If G_1, G_2 are groups

$$G_1 \times G_2$$

with the component-wise operation is the product of G_1, G_2

Proposition 6.1.2
Suppose $G = H \times K$. Consider

$$\tilde{H} := \{(h, e_K) : h \in H\}, \tilde{K} := \{(e_H, k) : k \in K\}$$

Then

(a) $\tilde{H}, \tilde{K} \leq G$

(b) $H \to \tilde{H}, K \to \tilde{K}$ given by

$$h \mapsto (h, e), k \mapsto (e, k)$$

are isomorphisms.

We can thus think of H, K as subgroups of $H \times K$.

Lemma 6.1.3
Let $h \in \tilde{H}, k \in \tilde{K}$, then

$$hk = kh$$

Keep in mind these are elements of $H \times K$.

Corollary 6.1.3.1
If $\phi : H \times K \to G$ is a homomorphism then

$$\phi(h)\phi(k) = \phi(k)\phi(h)$$

for all $h \in \tilde{H}, k \in \tilde{K}$.

6.2 Homomorphisms Between Products

Lemma 6.2.1
If $\alpha : H \to G, \beta : K \to G$ are homomorphisms, such that

$$\alpha(h)\beta(k) = \beta(k)\alpha(h)$$

for all $h \in H, k \in K$, then $\gamma : H \times K \to G$ given by

$$(h, k) \mapsto \alpha(h)\beta(k)$$

is a homomorphism.

Proof
Check definitions.

We call this homomorphism $\gamma = \alpha \cdot \beta$.

Corollary 6.2.1.1
If $\alpha : H \to H', \beta : K \to K'$ are homomorphisms, then $\gamma : H \times K \to H' \times K'$ given by

$$(h, k) \mapsto (\alpha(h), \beta(k))$$

is a homomorphism.

Proof
$\gamma = \tilde{\alpha} \cdot \tilde{\beta}$ where

$$\tilde{\alpha}(x) = (\alpha(x), e), \tilde{\beta}(h) = (e, \beta(y))$$

are homomorphisms as well.

We write $\gamma = \alpha \times \beta$ to denote this homomorphism.

Corollary 6.2.1.2
If $\alpha : H \to H', \beta : K \to K'$ are isomorphisms so is

$$\alpha \times \beta$$

Proof
Inverse given by $\alpha^{-1} \times \beta^{-1}$.

Proposition 6.2.2
$G \to G \times \{e\}$ given by

$$g \mapsto (g, e)$$

is an isomorphism.

Theorem 6.2.3 (Univeral Property of Products)
Let $\alpha : H \to G$ and $\beta : K \to G$ be homomorphisms, and let i_H, i_K be the inclusions of H, K in the product $H \times K$.
There is a homomorphism $\phi : H \times K \to G$ such that

$$\phi \circ i_H = \alpha, \phi \circ i_K = \beta$$

if and only if

$$\alpha(h)\beta(k) = \beta(k)\alpha(h)$$

for all $h \in H, k \in K$.

Proof
$(\implies)$ Suppose such a homomomorphism ϕ existed. Then for all $h \in H$, and $k \in K$

$$\begin{aligned} \alpha(h)\beta(k) &= \phi \circ i_H(h) \cdot \phi \circ i_K(k) \\ &= \phi \circ i_K(k) \cdot \phi \circ i_H(h) \\ &= \beta(k)\alpha(h) \end{aligned}$$

by our corollary above.

$(\impliedby)$ Suppose we have α, β which satisfies the desired properties. By our previous lemma, the map

$$\phi(h, k) := \alpha(h)\beta(k) = \beta(k)\alpha(h)$$

is a homomorphism.

Moreoever, it clearly satisfies

$$\phi \circ i_H(h) = \gamma(h, e) = \alpha(h)$$

and similarly for β thus γ is the desired homomorphism.

6.3 Identifing Product Groups

Proposition 6.3.1
Suppose p is prime and

$$|G| = p^2$$

then either G is cyclic or

$$G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$$

Proposition 6.3.2
Suppose $G = H \times K$ and let $\tilde{H}, \tilde{K}$ be as before.
Every element of G can be uniquely written as

$$g = \tilde{h}\tilde{k}$$

for some $\tilde{h} \in \tilde{H}, \tilde{k} \in \tilde{K}$.

6.3.1 Unique Factorization

Given $S, T \subseteq G$ let

$$ST := \{gh : g \in S, h \in T\}$$

Lemma 6.3.3
$G = ST$ if and only if every element $g \in G$ can be written as $g = hk$ for some $h \in S, k \in T$.

Proof
Trivial.

Observe that if $e \neq g \in H \cap K$ then

$$g = e \cdot g = g \cdot e$$

so the intersection being trivial is necessary to have unique factorization.

Lemma 6.3.4
Suppose $G = H, K$ for $H, K \leq G$. Then every elemnt $h \in G$ can be writte as

$$g = hk$$

for unique $h \in H, k \in K$ if and only if

$$H \cap K = \{e\}$$

Proof
$(\implies)$ Obvious.

$(\impliedby)$ Suppose $H \cap K = \{e\}$.

If $g = hk = h'k'$. Then

$$(h')^{-1}h = k'k^{-1} \in H \cap K$$

So

$$\begin{aligned}(h')^{-1}h &= k'k^{-1}\\ &= e\\ &\implies\\ h &= h'\\ k &= k'\end{aligned}$$

as inverses are unique.

6.3.2 Internal (Direct) Products

Definition 6.3.1 (Internal Direct Product)
We say G is the internal direct product of subgroups $H, K \leq G$ if

(a) $HK = G$

(b) $H \cap K = \{e\}$

(c) $hk = kh$ for all $h \in H, k \in K$

Theorem 6.3.5
Suppose G is the internal direct product of H, K. Then $\phi : H \times K \to G$ given by

$$(h, k) \mapsto hk$$

is an isomorphism.

Proof
Let $i_H : H \to G, I_K : K \to G$ be the identity functions.

By definition

$$i_H(h)i_K(k) = i_K(h)i_H(h)$$

for all $h \in H, k \in K$.

Thus $\phi = i_H \cdot i_K$ is a homomorphism by our work prior.

By the lemma, every $g \in G$ can be written as

$$g = hk$$

for unique $h \in H, k \in K$.

So ϕ is a bijection and therefore a homomorphism.

A Weaker Condition

Lemma 6.3.6
Suppose G is the internal direct product of H, K. Then

$$H, K \trianglelefteq G$$

Proof
Suppose $g \in G$ so

$$g = hk, h \in H, k \in K$$

Then

$$\begin{aligned} kHk^{-1} &= \{khk^{-1} : h \in H\} \\ &= \{kk^{-1}h : h \in H\} \\ &= H \end{aligned}$$

and $H \trianglelefteq G$.

But then

$$\begin{aligned} gHg^{-1} &= hkHhk^{-1}h^{-1} \\ &= hHh^{-1} \\ &\subseteq H \end{aligned}$$

and $H \trianglelefteq G$ by our characterizations earlier.

The proof for K is identical.

The Commutator

Definition 6.3.2
The commutator of $g, h \in G$ is

$$[g, h] := g \cdot h \cdot g^{-1} \cdot h^{-1}$$

Lemma 6.3.7
If $g, h \in G$, then
$$[g, h] = e$$
if and only if
$$gh = hg$$

Proposition 6.3.8
G is the internal direct product of $H, K \leq G$ is and only if

(a) $G = HK$

(b) $H \cap K = \{e\}$

(c) $H, K \trianglelefteq G$

Proof

$\underline{\implies}$ By lemma.

$\underline{\impliedby}$ If $h \in H, k \in K$ then
$$[h, k] = (hkh^{-1})k^{-1} \in K$$
since $K \trianglelefteq G$.

But $[h, k] = h(kh^{-1}k^{-1}) \in H$ as $H \trianglelefteq G$.

Thus
$$[h, k] \in H \cap K = \{e\} \implies [h, k] = e$$
and $hk = kh$ for all $h \in H, k \in K$ and we are done.

Chapter 7

Quotient Groups

Recall if $H \leq G$, then G/H partitions G into equally sized subsets.

for selective subgroups, such as $n\mathbb{Z} \leq \mathbb{Z}$

$$G/H = \mathbb{Z}/n\mathbb{Z}$$

is a group with operation

$$[a] + [b] = [a + b]$$

Can we generalize this?

7.1 Group Struct of G/H

Definition 7.1.1 (Relation)
A relation R between X, Y is a subset of $X \times Y$. We write

$$aRb \iff (a, b) \in R$$

Definition 7.1.2 (Function)
A relation R is a function $X \to Y$ if

(a) for all $x \in X$, there is $y \in Y$ such that xRy

(b) for all $x \in X$, if $y, z \in Y$ such that xRz, xRy then $y = z$.

Let us define a relation $G/H \times G/H \to G/H$ by

$$([g], [h]) \to [gh]$$

Is this relation a function? The first property holds but what about (b)?

Lemma 7.1.1
The relation $\to$ is a function if and only if H is normal.
Furthermore, if H is normal, then

$$ghH = gH \cdot hH$$

the setwise product.

Proof
$(\implies)$ Suppose $\to$ is a function. Let $g \in G, h \in H$. Then

$$([g], [g^{-1}]) \to [e]$$

But $[g] = [gh]$ thus

$$([gh], [g^{-1}]) \to [ghg^{-1}] = [e]$$

So $ghg^{-1} \in H$ and $H \trianglelefteq G$.

$(\impliedby)$ Fix $g, h \in H$ and observe that

$$gH \cdot hH = gh(h^{-1}Hh)H$$

Suppose now that H is normal. We have

$$h^{-1}Hh \subseteq H \implies (h^{-1}Hh) \cdot H \subseteq H$$

As $e \in h^{-1}Hh$ we actually have equality.

Thus

$$gh \cdot hH = ghH$$

Finally, suppose that $(S, T) \to R$ and $(S, T) \to R'$ for some $S, T, R, R' \in G/H$. Then

$$R = S \cdot T = R'$$

and $\to$ is a function by our work above.

7.2 Quotient Groups

Theorem 7.2.1
Let $N \trianglelefteq G$. Then the setwise product

$$gH \cdot hN = ghN$$

makes G/N into a group.
Furthermore, the function $q : G \to G/N$ given by

$$g \mapsto gN$$

is a surjective homomorphism with

$$\ker q = N$$

Definition 7.2.1 (Quotient Group)
G/N is called the quotient group of G by N.

Elements of G/N can be written as $gN, [g], \bar{g}$. Group operations can be stated as

$$gN \cdot hN = ghN, [g] \cdot [h] = [gh], \bar{g} \cdot \bar{g} = \overline{gh}$$

Definition 7.2.2 (Quotient Map/Homomorphism)
q.

Proof
Associativity This comes directly from the associativtity of $\cdot$ in G.

Identity $[e]$ is an identiy since e is an identity.

Inverse $[g^{-1}]$ is an inverse as it inherits the inverseness from G.

Surjectivity q is clearly surjective, and

$$q(gh) = [gh] = [g] \cdot [h] = q(g) \cdot q(h)$$

thus it is also a homomorphism.

Kernel We have

$$q(g) = [g] = [e]$$

if and only if $g \in N$ thus the result follows.

We previously showed that if $\phi : G \to K$ is a homomorphism, then $\ker \phi \trianglelefteq G$.

Corollary 7.2.1.1
Let $N \trianglelefteq G$. Then there is a group K and homomorphism $\phi : G \to K$ such that

$$N = \ker \phi$$

Proof
Take $K = G/N$ and $q : G \to G/N$. We have

$$\ker q = N$$

as desired.

Example 7.2.2 (Projective General Linear Group)
$\mathrm{GL}_n \mathbb{K}/Z(GL_n\mathbb{K})$ is the invertible transformations of lines through the origin in $\mathbb{K}^n$.

Chapter 8

Isomorphism Theorems

8.1 The Universal Property of Quotients

Definition 8.1.1 (Hom)
If G, K are groups
$$\text{Hom}(G, K) := \{\text{morphisms } G \to K\}$$

Lemma 8.1.1
If $\alpha : G \to H$ is surjective and $\psi_1, \psi_2 : H \to K$ are such that
$$\psi_1 \circ \alpha = \psi_2 \circ \alpha$$
then $\psi_1 = \psi_2$.

Proof
If $h \in H$, then there is $g \in G$ with
$$\alpha(g) = h$$

So
$$\begin{aligned}\psi_1(h) &= \psi_1(\alpha(g)) \\ &= \psi_2(\alpha(g)) \\ &= \psi_2(h)\end{aligned}$$

and we conclude $\psi_1 = \psi_2$.

Theorem 8.1.2 (Universal Property of Quotients)
Suppose $\phi : G \to K$ is a homomorphism, and $N \trianglelefteq G$. Let $q : G \to G/N$ be the quotient homomorphism.
There is a homomorphism $\psi : G/N \to K$ such that $\psi \circ q = \phi$ if and only if $N \subseteq \ker \phi$.
Furthermore, if ψ exists, it is unique.

Proof
<u>$(\implies)$</u> Suppose ψ exists. Pick $n \in N$. We have

$$\phi(n) = \psi(q(n)) = \psi(e) = e$$

and $N \subseteq \ker \phi$.

<u>$(\impliedby)$</u> Now suppose $N \subseteq \ker \phi$. Define $\psi : G/N \to K$ given by

$$[g] \mapsto \phi(g)$$

This is well-defined since the kernel contains N. Suppose $[g] = [h]$,

$$g^{-1}H \in N \subseteq \ker \phi$$

so

$$\phi(g)^{-1}\phi(h) = \phi(g^{-1}h) = e$$

and

$$\phi(g) = \phi(h)$$

as desired.

We have

$$\psi \circ q(g) = \psi([g]) = \phi(g)$$

for all $g \in G$ so $\psi \circ q = \phi$.

If $\phi' : G/N \to K$ is another homomorphism with $\phi' \circ q = \phi$, then it must be equal to ψ by the lemma, and uniquenss holds.

An equivalent way to define ψ is the following:

$$\phi(gN) = \phi(g)\phi(N) = \phi(g)\{e\} = \{\phi(g)\}$$

So if $S \in G/N$ then $\phi(S) = \{b\}$, a singleton set.

We can define $\psi(S) := b$ for $b \in K$ such that $\phi(s) = \{b\}$.

Corollary 8.1.2.1
For any groups G, K and $N \trianglelefteq G$, the function

$$q^* : \text{Hom}(G/N, K) \to \{\phi \in \text{Hom}(G, K) : N \subseteq \ker \phi\}$$

given by

$$\psi \mapsto \psi \circ q$$

is a bijection.

Compare this with the universal property of products.

Proposition 8.1.3
There is a bijection between $\text{Hom}(H \times K, G)$ and

$$\{(\alpha, \beta) \in \text{Hom}(H, G)^2 : \alpha(h)\beta(k) = \beta(k)\alpha(h)\}$$

8.2 First Isomorphism Theorem

Theorem 8.2.1 (First Isomorphism Theorem)
Suppose that $\phi : G \to K$ is a homomorphism. There is an isomorphism

$$\psi : G/\ker \phi \to \text{Im}\,\phi$$

such that $\phi = \psi \circ q$, where $q : G \to G/\ker \phi$ is the quotient homomorphism.

Proof
$\ker \phi \subseteq \ker \phi$ so by the universal property there is a homomorphism

$$\psi : G/\ker \phi \to K$$

such that $\psi \circ q = \phi$.

We can regard ψ as a surjective homomorphism $G/\ker \phi \to \text{Im}\,\phi$.

Suppose now that $\phi([g]) = e$. Then $\phi(g) = e$ and $g \in \ker \phi$. Thus $[g] = [e]$. This shows that ψ is injective and finally, an isomorphism.

8.2.1 Applications

The first isomorphism theorem is the best way to determine G/N for some $N \trianglelefteq G$.

We find a homomorphism $\phi : G \to K$ such that $\ker\phi = N$. Then we can conclude

$$G/N \cong \operatorname{Im}\phi$$

8.3 The Correspondance Theorem

We wish to understand subgroups of G/N using the quotient map.

8.3.1 Set Operations

Lemma 8.3.1
If $\phi : G \to H$ is a homomorphism

(a) If $K_1 \leq K_2 \leq G$ then $f(K_1) \leq f(K_2)$

(b) If $K_1 \leq K_2 \leq H$ then $f^{-1}(K_1) \leq f^{-1}(K_2)$.

Lemma 8.3.2
If $\phi : G \to H$ is a homomorphism, and $K_1, K_2 \leq H$, then

$$\phi^{-1}(K_1 \cap K_2) = \phi^{-1}(K_1) \cap \phi^{-1}(K_2)$$

Lemma 8.3.3
If $\phi : G \to H$ is a surjective homomorphism and $K \leq H$, then

$$\phi(\phi^{-1}(K)) = K$$

8.3.2 Subgroup Correspondance

Definition 8.3.1 (Sub)
For a group G

$$\operatorname{Sub}(G) := \{H \leq G\}$$

Lemma 8.3.4
Let $\phi : G \to H$ be a homomorphism

(a) If $K \leq H$ then $\ker\phi \leq \phi^{-1}(K)$

(b) If $\ker\phi \leq K \leq G$ then $\phi^{-1}(\phi(K)) = K$

Proof
(a) We have

$$\ker\phi = \phi^{-1}\{e\} \subseteq \phi^{-1}(K)$$

(b) We know $K \leq \phi^{-1}(\phi(K))$. It suffices to prove the reverse inclusion.

Suppose $y \in \phi^{-1}(\phi(K))$. Then $\phi(y) \in \phi(K)$, so $\phi(y) = \phi(k)$ for some $k \in K$.

Since $\phi(k^{-1}y) = e$

$$k^{-1}y \in \ker\phi \subseteq K \implies y \in K$$

We conclude that $\phi^{-1}(\phi(K)) = K$.

The conclusion is that

$$K = \phi^{-1}(K') \iff \ker\phi \leq K$$

8.3.3 The Correspondance Theorem

Theorem 8.3.5
Let $\phi : G \to H$ be a surjective homomorphism. There is a bijection

$$\{K \in \mathrm{Sub}(G) : \ker\phi \leq K\} \to \mathrm{Sub}(H)$$

given by

$$K \mapsto \phi(K)$$

Furthermore, if $\ker\phi \leq K, K_1, K_2 \leq G$

(a) $K_1 \leq K_2 \iff \phi(K_1) \leq \phi(K_2)$

(b) $\phi(K_1 \cap K_2) = \phi(K_1) \cap \phi(K_2)$

(c) $K \trianglelefteq G \iff \phi(K) \trianglelefteq H$

Proof
Since ϕ is surjective

$$\phi(\phi^{-1}(K')) = K'$$

for all $K' \leq H$.

Conversely if $\ker \phi \leq K \leq G$, then $\phi^{-1}(\phi(K)) = K$.

So ϕ, ϕ^{-1} are inverses when considered as set (subgroup) functions.

(a) This follows from the fact that ϕ, ϕ^{-1} are inverses and preserve $\leq$

(b)

$$\begin{aligned}\phi^{-1}(\phi(K_1) \cap \phi(K_2)) &= \phi^{-1}(\phi(K_1)) \cap \phi^{-1}(\phi(K_2)) \\ &= K_1 \cap K_2\end{aligned}$$

since $\phi(\phi^{-1}(K)) = K$, we have

$$\phi(K_1 \cap K_2) = \phi(K_1) \cap \phi(K_2)$$

(c) Exercise.

Quotient Groups

Theorem 8.3.6 (Correspondance Theorem for Quotient Groups)
Let $N \trianglelefteq G$. There is a bijection

$$\{K \in \mathrm{Sub}(G) : N \trianglelefteq K\} \to \mathrm{Sub}(G/N)$$

given by

$$K \mapsto q(K)$$

Furthermore, if $N \leq K, K_1, K_2, \leq G$

(a) $K_1 \leq K_2 \iff q(K_1) \leq q(K_2)$

(b) $q(K_1 \cap K_2) = q(K_1) \cap q(K_2)$

(c) $K \trianglelefteq G \iff q(K) \trianglelefteq G/N$

Remarks

Recall from the First Isomorphism Theorem that if $\phi : G \to H$ is a surjective homomorphism, then

$$G/\ker \phi \cong H$$

So there is a bijection

$$\mathrm{Sub}(H) \mapsto \mathrm{Sub}(G/\ker \phi)$$

We can check that the First Isomorphism theorem, the subgroup correspondance for isomorphisms, and correspondance theorem for quotient groups gives the correspondance theorem for surjective homomorphisms.

Proposition 8.3.7
Suppose $N \leq G$ and $N \leq K \leq G$ and let $q : G \to G/N$ be the quotient map.
Then the function

$$K/N \to q(K) \leq G/N$$

given by

$$kN \mapsto kN$$

is an isomorphism.

Definition 8.3.2
If $N \trianglelefteq G$ and $N \leq K \leq G$, then the subgroup $q(K)$ corresponding to K in G/N is denoted by

$$K/N$$

8.4 Second Isomorphism Theorem

8.4.1 Motivation

Recall the definition of the internal direct product of subgroups. We can uniquely factor $G = HK$ if and only if $H \cap K = \{e\}$.

Observe that for such H, K

$$|HK| = |H| \cdot |K|$$

But what if $H \cap K \neq \{e\}$?

$$HK = \bigcup_{h \in H} hK$$

which is a union of cosets of K.

Define

$$X := \{hK : h \in H\} \subseteq G/K$$

so that X partitions HK and

$$|HK| = |X| \cdot |K|$$

Lemma 8.4.1
Let $H, K \leq G$. If $h_1, h_2 \in H$ then

$$h_1K = h_2K$$

if and only if

$$h_1(H \cap K) = h_2(H \cap K)$$

Proof
We have

$$h_kK = h_2K \iff h_1^{-1}h_2 \in K \iff h_1^{-1}h_2 \in H \cap K$$

But

$$h_1^{-1}h_2 \in H \cap K \iff h_1H \cap K = h_2H \cap K$$

We may reprase this as considering the equivalence relation $\sim_K$ on G, $\sim_{H\cap K}$ on H. If $h_1, h_2 \in H$ then

$$h_1 \sim_K h_2 \iff h_1 \sim_{H\cap K} h_2$$

Corollary 8.4.1.1
The function

$$H/H \cap K \to X$$

given by

$$hH \cap K \mapsto hK$$

is a bijection.

Proof
The lemma shows well-defined and injectivity. Surjectivity is obvious.

Proposition 8.4.2
If $H, K \leq G$ then

$$|HK||H \cap K| = |H||K|$$

Proof
We have

$$|HK| = |X||K| = [H : H \cap K]|K|$$

By Lagrange's theorem

$$|HK||H \cap K| = |H||K|$$

Proposition 8.4.3
Let $H, K \leq G$. Then $HK \leq G$ if and only if

$$HK = KH$$

if and only if

$$KH \subseteq HK$$

Proof
$(\implies)$ Suppose $HK \leq G$.

Pick $h \in H, k \in K$ so that $h, k \in HK$. This gives

$$kh \in HK$$

Also $k^{-1}h^{-1} \in HK$ thus there is some h_0, k_0 such that

$$k^{-1}h^{-1} = h_0k_0$$

Hence

$$hk = (k^{-1}h^{-1})^{-1} = k_0^{-1}h_0^{-1} \in KH$$

So $KH \subseteq HK$ and $HK \subseteq KH$ which means equality.

$(\impliedby)$ Suppose $KH \subseteq HK$. We always have $e \in HK$.

If $x, y \in HK$, then $x = h_0k_0$ and $y = h_1k_1$ for some $h_0, h_1 \in H, k_0, k_1 \in K$.

Since $KH \subseteq HK$

$$k_0^{-1}h_0^{-1}h_1 = h_2k_2$$

for some $h_2 \in H, k_2 \in K$.

It follows that

$$x^{-1}y = k_0^{-1}h_0^{-1}h_1k_1 = h_2k_2k_1 \in HK$$

and thus $HK \leq G$.

Corollary 8.4.3.1
If $KH \subseteq HK$ then

$$[H : H \cap K] = [HK : K]$$

But when is $HK \subseteq KH$? It is sufficient but not necessary to have

$$\forall h \in H, \exists h' \in H, Kh = h'K$$

but then $h'K = hK$.

Rephrasing the condition gives us

$$hKh^{-1} = K$$

for all $h \in H$.

Corollary 8.4.3.2
If $H \subseteq N_G(K)$, then $HK \leq G$, and hence

$$[H : H \cap K] = [HK : K]$$

8.4.2 Second Isomorphism Theorem

Theorem 8.4.4
Suppose $H \subseteq N_G(K)$. Then

$$HK \leq G, K \trianglelefteq HK, H \cap K \trianglelefteq H$$

Furthermore, if $i_H : H \to HK$ is the inclusion, $q_1 : H \to H/H \cap K$, and $q_2 : HK \to HK/K$ are the quotient maps, there is an isomorphism

$$\psi : H/H \cap K \to HK/K$$

such that

$$\psi \circ q_1 = q_2 \circ i_H$$

Proof
If $H \subseteq N_G(K)$, then we know

$$hKh^{-1} = K, kKk^{-1} = K$$

so

$$H, K \subseteq N_{HK}(K) \implies N_{HK}(K) = HK \implies K \trianglelefteq HK$$

If $k \in H \cap K$ and $h \in H$, then

$$hkh^{-1} \in H \cap K$$

since it belongs to H by definition and it belongs to K by the assumption of the normalizer. So

$$H \cap K \trianglelefteq H$$

We have already shown that $HK \leq G, K \trianglelefteq HK, H \cap K \trianglelefteq H$.

If $h \in H, k \in K$ then

$$hkK = hK$$

so

$$HK/K = \{gK : g \in HK\} = \{hK : h \in H\}$$

but then

$$\operatorname{Im} q_2 \circ i_H = \{hK : h \in H\} = HK/K$$

It follows that

$$\ker q_2 \circ i_H = i_H^{-1}(q_2^{-1}\{e\}) = i_H^{-1}(K) = H \cap K$$

By the first isomorphism theorem, there is an isomorphism ψ as desired.

8.5 Third Isomorphism Theorem

Suppose $N \trianglelefteq G$ and $N \leq K \leq G$. Check that

$$K \trianglelefteq G \iff K/N \trianglelefteq G/N$$

Suppose that is the case. What is

$$(G/N)/(K/N)$$

Theorem 8.5.1 (Third Isomorphism)
Let $N \trianglelefteq G$ and $N \leq K \trianglelefteq G$. Let the following be quotient maps

$$\begin{aligned} q_1 &: G \to G/n \\ q_2 &: G/N \to (G/N)(K/N) \\ q_3 &: G \to G/K \end{aligned}$$

Then there is an isomorphism

$$\psi : G/K \to (G/N)(K/N)$$

such that

$$\psi \circ q_3 = q_2 \circ q_1$$

Proof
Notice that

$$\begin{aligned} \ker q_2 \circ q_1 &= (q_2 \circ q_1)^{-1}\{e\} \\ &= q_1^{-1}(q_2^{-1}\{e\}) \\ &= q_1^{-1}(K/N) \\ &= K \end{aligned}$$

and

$$\operatorname{Im} q_2 \circ q_1 = (G/N)(K/N)$$

By the First Isomorphism Theorem, there is an isomorphism

$$\psi : G/K \to (G/N)(K/N)$$

such that

$$\psi \circ q_3 = q_2 \circ q_1$$

8.5.1 Non-Normal Subgroups

If K is not normal then G/K is not a group. However, we can still talke about $[G : K]$, $[G/N : K/N]$.

Proposition 8.5.2
If $N \trianglelefteq G$ and $N \leq K \leq G$, then

$$[G : K] = [G/N : K/N]$$

In fact, there is not reason to use quotient spaces. This holds for surjective homomorphisms.

Proposition 8.5.3
Let $\phi : G \to H$ be a surjective homomorphism, and suppose $\ker \phi \leq K \leq G$. Then

$$[G : K] = [H : \phi(K)]$$

Proof
Define a function

$$f : G/K \to H/\phi(K)$$

given by

$$gK \mapsto \phi(g)\phi(K)$$

To see it is well-defined, suppose $gK = hK$

$$\begin{aligned} h^{-1}g \in K \implies \phi(h^{-1})\phi(g) \\ = \phi(h^{-1}g) \\ \in \phi(K) \end{aligned}$$

so $\phi(g)\phi(K) = \phi(h)\phi(K)$.

Since ϕ is surjective, f is also surjective.

Suppose $f(gK) = f(hK)$, so

$$\phi(g)\phi(K) = \phi(h)\phi(K)$$

Then

$$\begin{aligned} \phi(h^{-1}g) &= \phi(h)^{-1}\phi(g) \\ &\in \phi(K) \\ \implies & \\ h^{-1}g &\in \phi^{-1}(\phi(K)) \\ &= K \end{aligned}$$

thus $gK = hK$, and f is injective.

We conclude that f is a bijection.

Chapter 9

Group Actions

Observe that for matrices, we can view them as a group but also as linear maps on vectors.

9.1 Group Actions

Definition 9.1.1 (Left Action)
A left action of G on a set X is a function

$$G \times X \to X$$

such that

(a) $e \cdot x = x$ for all $x \in X$

(b) $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G, x \in X$

Proposition 9.1.1
Let X be a set. The group S_X (invertible functions under composition) acts on X via

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

Lemma 9.1.2
If G acts on X, and $H \leq G$, then H acts on G by the restricted action $H \times X \to X$ given by

$$(h, x) \mapsto h \cdot x$$

9.2 About Actions

9.2.1 Invariant Subsets

Definition 9.2.1 (Invariant Under Action)
If G acts on X, a subset $Y \subseteq X$ is invariant under the action of G if

$$g \cdot y \in Y$$

for all $g \in G, y \in Y$.

Lemma 9.2.1
If G acts on X and Y is an invariant subset, then G acts on Y via $G \times Y \to Y$ given by

$$(g, y) \mapsto g \cdot y$$

9.2.2 Action on Functions

Proposition 9.2.2
Suppose G acts on X and Y, and let $\mathrm{Fun}(X, Y)$ denote the set of functions from $X \to Y$. If $g \in G, f \in \mathrm{Fun}(X, Y)$, let $g \cdot f$ be the function $X \to Y$ given by

$$x \mapsto g \cdot f(g^{-1}x)$$

Then $G \times \mathrm{Fun}(X, Y) \to \mathrm{Fun}(X, Y)$ given by

$$(g, f) \mapsto g \cdot f$$

is a left action of G on $\mathrm{Fun}(X, Y)$.

We often apply this function with the trivial action on Y so

$$g \cdot f(x) = f(g^{-1}x)$$

9.2.3 Action on Subsets

Proposition 9.2.3
Suppose G acts on X. Let 2^X denote the set of subsets of X.
Then

$$g \cdot S := \{g \cdot s : s \in S\}$$

defines an action of G on 2^X.

Proof
Check the definitions.

$$e \cdot S = S$$

For all $g, h \in G$ and $S \in 2^X$

$$\begin{aligned} g \cdot (h \cdot S) &= g \cdot \{h \cdot s : s \in S\} \\ &= \{g \cdot (g \cdot s) : s \in S\} \\ &= \{gh \cdot s : s \in S\} \\ &=: gh \cdot S \end{aligned}$$

9.2.4 Left Regular Action

Does every group act on some set?

Lemma 9.2.4
If G is a group the multiplication map

$$G \times G \to G$$

is a left action of G on G.

This called the left regular action of G on G.

Lemma 9.2.5
If $H \leq G$, then G acts on G/H by

$$g \cdot (kH) = gkH$$

Sine $G/\{e\} = G$, this generalizes the left regular action.

9.2.5 Right Multiplication

Unfortunately, right multiplication does not define a left action in general unless our group is commutative.

Definition 9.2.2 (Right Action)
Let G be a group. A right action of G on a set X is a function $X \times G \to X$ such that

(a) $x \cdot e = x$ for all $x \in X$

(b) $(x \cdot g) \cdot h = x \cdot (gh)$ for all $g, h \in G$ and $x \in X$

There is a right regular action on G itself similar to the left regular action. The same applies to $H \backslash G$.

There is again a trivial right action.

If there is a right action of G on X and Y is any set

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

defines a left action of G on $\mathrm{Fun}(X, Y)$.

Proposition 9.2.6
If $\cdot$ is a right action of G on X, then

$$g \cdot x := x \cdot g^{-1}$$

defines a left action of G on X.

Proof
Clearly $x \cdot x = c\dot{e} = x$.

Let $g, h \in G$ and $x \in X$.

$$\begin{aligned} g \cdot (h \cdot x) &= g(x \cdot h^{-1}) \\ &= (x \cdot h^{-1})g^{-1} \\ &= x \cdot h^{-1} \cdot g^{-1} \\ &= x \cdot (gh)^{-1} \\ &= gh \cdot x \end{aligned}$$

Combined with the last example, this proposition explains why, if $\cdot$ is a left action of G on X, we define the left action of G on $\mathrm{Fun}(X, Y)$ by setting

$$(g \cdot f)(x) := f(g^{-1}x)$$

Essentially, $x \cdot g := f(g \cdot x)$ is a right action on G. So when we take the inverse, it becomes a left action.

9.3 Permutation Representations

Lemma 9.3.1
If G has a left action on a set X, and $g \in G$, let $\ell_g : X \to X$ be defined by

$$\ell_g(x) := g \cdot x$$

Then

(a) $\ell_g \circ \ell_h = \ell_{gh}$ for all $g, h \in G$

(b) $\ell_e = 1$

(c) ℓ_g is a bijection for all $g \in G$

Proof
The first two follow from the definition.

The last property

$$\begin{aligned} \ell_g \circ \ell_{g^{-1}} &= \ell_e \\ &= 1 \\ &= \ell_{g^{-1}} \circ \ell_g \end{aligned}$$

comes from the fact that ℓ_g is invertible.

Corollary 9.3.1.1
Every left action of G on X gives a homomorphism $\phi : G \to S_X$ given by

$$g \mapsto \ell_g$$

with

$$\phi(g)(x) = g \cdot x$$

Definition 9.3.1 (Permutation Representation)
If X is a set, a permutation representation of G on X is a homomorphism

$$\phi : G \to S_X$$

If $|X| = n$ then

$$S_X \cong S_n$$

thus actions on finite sets X with $|X| = n$ gives homomorphisms to S_n.

Theorem 9.3.2
If G acts on X, then there is a homomorphism $\phi : G \to S_X$ defined by

$$\phi(g)(x) = g \cdot x$$

Moreoever, if $\phi : G \to S_X$ is a homomorphism, then

$$g \cdot x = \phi(g)(x)$$

defines a group action of G on X.

Proof
We have already shown the first statement.

To see the second statement, first note that

$$e \cdot x = \phi(e)(x) = 1(x) = x$$

for all $x \in X$.

Now, if $g, h \in G$ and $x \in X$ then

$$\begin{aligned} g \cdot (h \cdot x) &= \phi(g)(\phi(h)x) \\ &= (\phi(g) \circ \phi(h))(x) \\ &= \phi(gh)(x) \end{aligned}$$

This shows that group actions are essentially equivalent to permutation representations. We can treat the two interchangeably.

9.4 Cayley's Theorem

9.4.1 Faithful Actions

Definition 9.4.1 (Faithful)
Let G act on a set X, and let $\phi : G \to S_X$ be the corresponding permutation representation.
The kernel of the action is $\ker\phi$, and the action is faithful if

$$\ker\phi = \{e\}$$

Lemma 9.4.1
An action of G on X is faithful if and only if for every $g \in G$ such that $g \neq e$, there is $x \in X$ such that $g \cdot x \neq x$.

Proof
We know $\ell_g \neq 1$ if and only if there is $x \in X$ such that

$$g \cdot x = \phi(g)(x) \neq x$$

9.4.2 Cayley's Theorem

Theorem 9.4.2 (Cayley)
The left regular action of G on G is faithful.
Consequently, G is isomorphic to a subgroup of S_G. In particular, if $|G| = n < \infty$, then G is isomorphic to a subgroup of S_n.

Proof
For any $e \neq g \in G$

$$g \cdot e = g \neq e$$

so the left regular action is faithful.

Hence the permutation representation $\phi : G \to S_G$ is injective. So G is isomorphic to $\operatorname{Im}\phi \leq S_G$.

The homomorphism $G \to S_G$ given by this theorem is called left regular representation of G.

Chapter 10

Orbits & Stabilizers

10.1 Orbits

Definition 10.1.1 (G-Orbit)
Let G act on X. The G-orbit of x is

$$\mathcal{O}_x := \{g \cdot x : g \in G\}$$

Definition 10.1.2 (Orbit)
A subset $\mathcal{O} \subseteq X$ is an orbit of

$$\mathcal{O} = \mathcal{O}_x$$

for some $x \in X$.

Definition 10.1.3 (Transitive)
A group action is transitive if

$$\mathcal{O}_x = X$$

for some $x \in X$.

10.1.1 An Equivalence Relation

If G acts on X, let us say

$$x \sim_G y$$

if there is $g \in G$ such that

$$g \cdot x = y$$

Lemma 10.1.1
If G acts on X, then $\sim_G$ is an equivalence relation on X.

Proof
Since $e \cdot x = x$, we have reflexivity.

If $g \cdot x = y$, then $g^{-1} \cdot y = x$, thus

$$x \sim_G y \implies y \sim_G x$$

Finally, if $g \cdot x = y$, and $h \cdot y = z$, then $hg \cdot x = z$, so we actually have $x \sim_G y$ and

$$y \sim_G z \implies x \sim_G z$$

Observe that if $x \in X$, then the equivalence classes $[x]_{\sim_G}$ of x is

$$\{y \in X : x \sim_G y\} = \{y \in X : y = g \cdot x, g \in G\} = \mathcal{O}_x$$

so the orbits of G form a partition of X. So the action is transitive if and only if there is one orbit.

Proposition 10.1.2
If G acts on X, then orbits of G form a partition of X. In particular, the action is transitive if and onl if there is one orbit.

Definition 10.1.4 (Set of Representatives)
Let $\sim$ be an equivalence relation on a set X. $S \subseteq X$ is said to be a set of representatives for $\sim$ if each equivalence class of $\sim$ contains exactly one element of S.

This requires the Axiom of Choice.

Corollary 10.1.2.1
Suppose G acts on a set X and S is a set of representatives for $\sim_G$.
Then

$$|X| = \sum_{x \in S} |\mathcal{O}_x|$$

10.2 Stabilizers

To determin $|\mathcal{O}_x|$, we can use the function

$$g \mapsto g \cdot x$$

but need to deal with non-injectiveness.

Definition 10.2.1 (Stabilizer)
If G acts on X, and $x \in X$, the stabilizer of x is

$$G_x := \{g \in G : g \cdot x = x\}$$

Proposition 10.2.1
If G acts on X and $x \in X$, then G_x is a subgroup of G.

Proof
First observe that $e \in G_x$.

Second, if $g, h \in G_x$, then

$$\begin{aligned} gh \cdot x &= g \cdot (h \cdot x) \\ &= g \cdot x \\ &= x \end{aligned}$$

and G_x is closed under group operation.

Finally, if $g \in G_x$ then

$$\begin{aligned} g^{-1} \cdot x &= g^{-1} \cdot (g \cdot x) \\ &= e \cdot x \\ &= x \end{aligned}$$

and $g^{-1} \in G_x$.

10.2.1 Orbit-Stabilizer Theorem

Theorem 10.2.2 (Orbit-Stabilizer)
If G acts on X and $x \in X$, then there is a bijection $G/G_x \to \mathcal{O}_x$ given by

$$gG_x \mapsto g \cdot x$$

Proof
If $gG_x = hG_x$, then $g^{-1}h \in G_x$. So

$$g^{-1}h \cdot x = x \implies h \cdot x = g \cdot x$$

To see injectivity, suppose that $g \cdot x = h \cdot x$. Then

$$g^{-1}h \cdot x = x$$

and $g^{-1}h \in G_x$ means $gG_x = hG_x$, by our prior work with cosets.

Finally we show surjectivity. If $y \in \mathcal{O}_x$, then

$$y = g \cdot x$$

for some g by definition.

Corollary 10.2.2.1
If G acts on X and $x \in X$, then

$$|\mathcal{O}_x| = [G : G_x]$$

Example 10.2.3
The stabilizer of $i \in [n]$ with respect to S_n acting on $[n]$ is

$$G_i = \{\pi \in S_n : \pi(i) = i\}$$

Proposition 10.2.4
Let $H \leq G$. Then the left multiplication action of G on G/H is transitive, and

$$G_{eH} = H$$

Proof
If $gH \in G/H$, then

$$gH = g \cdot eH$$

so $\mathcal{O}_{eH} = G/H$.

But

$$g \cdot eH = eH \iff gH = H \iff g \in H$$

and

$$H = G_{eH}$$

Observe all that the orbit-stabilizer theorem says is

$$G/H = \mathcal{O}_{eH} \cong G/G_{eH} = G/H$$

10.2.2 Kernel & Stabilizer

If G acts on X, the kernel of action is

$$\{g \in G : g \cdot x = x\}$$

for all $x \in X$.

Whereas

$$G_x := \{g \in G : g \cdot x = x\}$$

for a fixed x.

Consequently, if H is the kernel of action, then $H \leq G_x$ for all $x \in X$.

Proposition 10.2.5
If G acts on X, then the kernel of the action is

$$\bigcap_{x \in X} G_x$$

the intersection of the stabilizers.

Proof
By definition, g is in the kernel if and only if

$$\forall x \in X, g \in G_x$$

Application

Theorem 10.2.6
If G is finite and $H \leq G$ has index

$$[G : H] = p$$

where p is the smallest prime divisor of $|G|$, then

$$H \trianglelefteq G$$

Proof
Let K be the kernel of action of G on G/H. Notice K is normal.

By our previous proposition

$$K \leq H = G_{eH}$$

Let

$$k := [H : K] = \frac{|H|}{|K|}$$

Now

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = p \cdot k$$

By the first isomorphism theorem, G/K is isomorphic to a subgroup of S_p. So

$$\begin{aligned} |G/K| = kp &| |S_p| \\ &= p! \end{aligned}$$

gives

$$k | (p-1)!$$

But we also have $k||G|$. Since p is smallest prime dividing $|G|$, we must have $k = 1$ thus

$$|H| = |K| \implies H = K$$

Chapter 11

Conjugation

11.1 Conjugation

Recall that left multiplication defines a left action of G on G. It turns on that there is another natural left action.

Lemma 11.1.1
$G \times G \to G$ given by

$$(g, k) \mapsto gkg^{-1}$$

defines an action of G on G.

This action is called the conjugation action of G on G. We will write

$$g \bullet k = gkg^{-1}$$

Proof
If $k \in G$, then

$$e \bullet k = eke = k$$

If $g, h \in G$ and $k \in G$, then

$$\begin{aligned} g \bullet (h \bullet k) &= g \bullet hkh^{-1} \\ &= ghkh^{-1}g^{-1} \\ &= (gh)k(gh)^{-1} \\ &= gh \bullet k \end{aligned}$$

Definition 11.1.1 (Conjugacy Class)
The orbit of $k \in G$ under the conjugation action is called the conjugacy class of k.

We will write

$$\mathrm{Conj}_G(k) := \{gkg^{-1} : g \in G\}$$

for the orbit of $k \in G$ to avoid confusion.

Definition 11.1.2 (Centralizer)
The stabilizer of $k \in G$ is called the centralizer of k in G.

We will write

$$C_G(k) = \{g \in G : gkg^{-1} = k\} = \{g \in G : gk = kg\}$$

By the orbit-stabilizer theorem

$$|\mathrm{Conj}_G(k)| = [G : C_G(k)]$$

11.2 Conjugation & Normalizers

The conjugation action of G on G induces an action of G on 2^G.

If $g \in G, S \subseteq G$

$$\begin{aligned} g \bullet S &= \{g \bullet h : h \in S\} \\ &= \{ghg^{-1} : h \in S\} \\ &= gSg^{-1} \end{aligned}$$

Thus the stabilizer of S is

$$\{g \in G : gSg^{-1} = S\} =: N_G(S)$$

where $N_G(S)$ denotes the normalizer of S in G.

11.3 Class Equation

Using standard facts about orbits

$$|G| = \sum_{g \in S} |\mathrm{Conj}(g)| = \sum_{g \in S} [G : C_G(g)]$$

where S is the set of representativecs for conjugacy classes.

Lemma 11.3.1
$|\text{Conj}(k)| = 1 \iff C_G(k) = G \iff k \in Z(G)$.

Proof
$\text{Conj}(k)$ has size one if and only if $gkg^{-1} = k$ for all $g \in G$. This happens if and only if $C_G(k) = G$ and finally if and only if $k \in Z(G)$.

Theorem 11.3.2 (Class Equation)
If G is a finite group, then

$$|G| = |Z(G)| + \sum_{g \in T} |\text{Conj}(g)|$$

where T is a set of representatives for conjugacy classes not contained in the center.

Cauchy's Theorem

Theorem 11.3.3 (Cauchy)
If G is a finite group and p is a prime dividing $|G|$, then G contains an element of order p

Proof
Let $|G| = pm$.

Case I : G is abelian We argue by induction on m. If $m = 1$ G is cyclic and we are done.

Inductively pick $e \neq a \in G$ where

$$|a| < |G|$$

If p divides $|a|$, then apply induction to get element $b \in \langle a \rangle$ with

$$|b| = p$$

Otherwise G is abelian gives

$$N = \langle a \rangle \trianglelefteq G$$

Now

$$|G/N| = \frac{|G|}{|N|} < |G|$$

Since

$$p||G|, p \not| |N|, p||G/N|$$

G/N must have an element gN of order p.

Let $n = |g|$. Since $g^n = 1$ we know

$$q(g)^n = 1$$

where q is the quotient map. Thus $p|n$.

If $G = \langle g \rangle$, then we are done. Otherwise we can apply induction to $\langle g \rangle$.

Case II g is not abelian We will argue by induction on $|G|$ again.

By the class equation

$$|G| = |Z(G)| + \sum_{g \in T} |\text{Conj}(g)|$$

If $p \not| |\text{Conj}(g)| = \frac{|G|}{C_G(g)}$ for some $g \in T$, then

$$p||C_G(g)|$$

Since $g \notin Z(G)$, we know

$$|\text{Conj}(g)| > 1 \implies |C_G(g)| < |G|$$

By induction, $C_G(g)$ contains an element of order p. If $p||\text{Conj}(g)|$ for all $g \in T$, then

$$p||Z(G)|$$

Now, $Z(G)$ is an abelian group, so by the abelian case, $Z(G)$ contains an element of order p.

11.4 Center of p-Groups

Definition 11.4.1 (p-Group)
Let p be prime. A group G is a p-group if

$$|G| = p^k$$

for some $k \geq 1$.

Theorem 11.4.1
If G is a p-group, then

$$Z(G) \neq \{e\}$$

Proof
We have

$$|G| = |Z(G)| + \sum_{g \in T} [G : C_G(g)]$$

Moreover

$$[G : C_G(g)] \,|\, |G|$$

If $g \notin Z(G)$ then

$$[G : C_G(g)] > 1 \implies p | [G : C_G(g)]$$

So $p|Z(G)$. Since the other terms in the summation all have a common denominator of p.

11.5 Conjugation in Permutation Groups

Suppose $\pi, \sigma \in S_n$, we want to find out what is

$$\pi\sigma\pi^{-1}$$

Lemma 11.5.1
If $\sigma(i) = j$ then

$$(\pi\sigma\pi^{-1})(\pi(i)) = \pi(j) = \pi(\sigma(i))$$

so $\pi\sigma\pi^{-1}$ sends the "successor" of i under π, to the successor of $\sigma(i)$ under π.

Corollary 11.5.1.1
If

$$\sigma = (i_{11} \dots i_{1k_1}) \dots (i_{m1} \dots i_{mk_m})$$

then

$$\pi\sigma\pi^{-1}(\pi(i_{11}) \dots \pi(i_{1k_1})) \dots (\pi(i_{1m_1}) \dots \pi(i_{mk_m}))$$

11.5.1 Conjugacy Classes

Definition 11.5.1 (Cycle Type)
For $n \geq 1$, if $\sigma \in S_n$, the cycle type of σ is the function $\lambda : [n] \to \mathbb{N}$ such that $\lambda(i)$ is the number of cycles in the disjoint cycle representation of σ of length i.

Remark that

$$\sum_{i=1}^{n} i\lambda(i) = n$$

Proposition 11.5.2
If $\sigma \in S_n$ has cycle type λ

$$\operatorname{Conj}(\sigma) = \{\tau \in S_n : \tau \text{ has cycle type } \lambda\} =: \operatorname{Conj}(\lambda)$$

Proof
$\subseteq$ This is clear by the previous proposition.

$\supseteq$ Suppose τ has the same cycle type as

$$\sigma = (i_{11} \dots i_{1k_1}) \dots (i_{m1} \dots i_{mk_m})$$

We can rearrange the disjoint cycle notation of τ so that the i-th disjoint cycle has length k_i (matching σ).

$$\sigma = (j_{11} \dots j_{1k_1}) \dots (j_{m1} \dots j_{mk_m})$$

Let π be the permutation sending

$$\pi(i_{ab}) := j_{ab}$$

then

$$\pi\sigma\pi^{-1} = \tau$$

and we are done.

11.5.2 Counting Conjugacy Classes

Definition 11.5.2 (Partition of n)
A tuple λ of natural numbers
$$(\lambda_1, \dots, \lambda_k)$$
such that
$$\lambda_i \geq \lambda_{i+1}$$
and
$$\sum_{i=1}^{k} \lambda_i = n$$

To avoid repetition, we can use exponent notation

$$(2,1,1) = (2,1^2)$$

as a partition of 4.

Lemma 11.5.3
There is a bijection between partitions of n, and functions $\lambda : [n] \to \mathbb{N}$ such that

$$\sum_{i=1}^{n} i\lambda(i) = n$$

Proof
Consider the invertible map
$$\lambda \mapsto (n^{\lambda(n)}, \dots, 1^{\lambda(1)})$$

Write

$$p(n) := \text{number of partitions of } n \approx e^{\pi\sqrt{\frac{2}{3}}} << n! \approx n^n$$

Corollary 11.5.3.1
The number of conjugacy classes in S_n is $p(n)$.

Proof
$\lambda : [n] \to \mathbb{N}$ is the cycle type of some permutation if and only if

$$\sum_{i=1} i\lambda(i) = n$$

11.5.3 Stabilizers

We wish to appeal to the Orbit-Stabilizer theorem. This requires us to determine the stabilizers/centralizers of elements.

$$C_{S_n}(\sigma)$$

Proposition 11.5.4
Let

$$\sigma = (i_{11} \dots i_{1k_1}) \dots (i_{m1} \dots i_{mk_m})$$

be a permutation of cycle type λ.
If $\pi \in C_{S_n}(\lambda)$, then π is completely determined by

$$\pi(i_{11}), \dots, \pi(i_{m1})$$

Consequently

$$|C_{S_n}(\sigma)| = \prod_{i=1}^{n} i^{\lambda_i} \lambda_i!$$

Proof
For the first claim, once we know $\pi(i_{11}) = i_{ab}$, since $\pi = \sigma$, we must have

$$\pi(i_{12}) = \pi(i_{ab})$$

and the entire disjoint cycle is determined.

For the enumeration claim, note that $\pi(i_{a1})$ must go to a cycle of length $k = k_a$, so π permutes the cycles of length k, of which there are $\lambda_k!$ such choices.

Once we fix which cycle i_{a1} maps to, there are k choices for where in the cycle it can go. λ_i independent choices give an extra factor of k^{λ_i}.

Corollary 11.5.4.1
If $\lambda : [n] \to \mathbb{N}$ with $\sum_{i=1}^n i\lambda(i) = n$, then

$$|\mathrm{Conj}(\lambda)| = \frac{n!}{\prod_{i=1}^n i^{\lambda_i} \lambda_i!}$$

by the Orbit-Stabilizer theorem and Lagrange's theorem.

Since the orbits partition S_n, we get the nice combinatorial identity

$$n! = \sum_{\lambda} \frac{n!}{\prod_{i=1}^n i^{\lambda_i} \lambda_i!}$$

Chapter 12

Classification of Groups

One of the big questions in modern mathematics is to classify all groups up to isomorphism.

12.1 Toy Examples

For example, we solved have the following result.

Proposition 12.1.1
If p is prime and $|G| = p^2$.
Then G is either cyclic or

$$G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$$

Lemma 12.1.2
Suppose $H, K \trianglelefteq G$, where $\gcd(H, K) = 1$ and $|H| \cdot |K| = |G|$
Then

$$G \cong H \times K$$

Proof
Since $|H \cap K|$ divides both $|H|, |K|$, it must be 1. Thus

$$H \cap K = \{e\}$$

Moreoever

$$|HK| = |H| \cdot \frac{|K|}{|H \cap K|} = |G|$$

and so $HK = G$.

The characterization of products then applies.

12.1.1 Difficulties

Notice in the lemma above, we require H, K to be normal subgroups. We can have $G = HK$ without H, K both being normal.

However, this concern does not arrive with finite abelian groups.

12.2 Abelian Groups

Lemma 12.2.1
Suppose G is abelian. Define

$$G^{(m)} := \{g \in G : g^m = e\}$$

Then $G^{(m)} \leq G$ for all $m \geq 1$.

Proof
$e \in G^{(m)}$ for all $m \geq 1$.

If $g, h \in G^{(m)}$ then

$$(g^{-1}h)^m = g^{-m}h^m = e$$

by commutativity.

Definition 12.2.1 (m-Torsion Subgroup)
$G^{(m)}$ from above.

Proposition 12.2.2
Suppose $|G| = mn$ for coprime m, n. Then $\phi : G \to G^m \times G^n$ given by

$$g \mapsto (g^n, g^m)$$

is an isomorphism.
Moreoever, $|G^{(m)}| = m$ and $|G^{(n)}| = n$.

Proof
Part I: If $g \in G$, then $g^{mn} = e$ so

$$g^n \in G^{(m)}, g^m \in G^{(n)}$$

This shows that ϕ is well-defined.

By Bezout's lemma, there are some $a, b \in \mathbb{Z}$ such that

$$an + bm = 1$$

Suppose now that $\phi(g) = e$. Then

$$g^n = g^m = e \implies g = g^{an+bm} = e$$

and so ϕ is injective.

Choose $g \in G^{(m)}, h \in G^{(n)}$. We have

$$g^{an} = g^{an+bm} = g$$

and

$$h^{bm} = h^{an+bm} = h$$

Thus

$$\phi(g^a h^b)(g^{an} h^{bn}, g^{am} h^{bm}) = (g, h)$$

which shows that ϕ is surjective.

It remains to show that ϕ is a homomorphism. We have

$$\begin{aligned}\phi(gh) &= ((gh)^n, (gh)^m) \\ &= (g^n h^n, g^m h^m) \\ &= (g^n, g^m)(h^n, h^m) \\ &= \phi(g)\phi(h)\end{aligned}$$

as required.

<u>Part II:</u> We now know that

$$|G| = |G^{(m)}| \cdot |G^{(n)}|$$

Suppose

$$|G| = \prod_{i=1}^{k} p_i^{a_i}$$

is the prime factorization of $|G|$.

We must have

$$|G^{(m)}| = \prod_{i=1}^{k} p_i^{b_i}$$

$$|G^{(n)}| = \prod_{i=1}^{k} p_i^{c_i}$$

where $a_i = b_i + c_i$ and only one of b_i, c_i is non-zero by coprimality.

Suppose that $b_i > 0$. If $p_i || G^{(n)}|$, then by Cauchy's theorem $G^{(n)}$ contains an element of order p_i. But then a is also in $G^{(n)}$ and thus by our work in part 1,

$$a = e$$

which is a contradiction.

Repeating this argument for all p_i then for $G^{(n)}$ yields

$$m||G^{(m)}|, n||G^{(n)}|$$

Thus

$$|G^{(m)}| = m, |G^{(n)}| = n$$

as desired.

Proposition 12.2.3 (Chinese Remainder Theorem)
Suppose $\gcd(m, n) = 1$.
Then

$$G := \mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

Proof
Consider $G^{(m)}$. By definition

$$G^{(m)} := \{x \in G : mx = 0\}$$

But $mx = 0$ if and only if

$$mn|mx \iff n|x$$

Thus

$$G^{(m)} = n\mathbb{Z}/mn\mathbb{Z}$$

Since the map $\mathbb{Z} \to n\mathbb{Z}$ given by

$$x \mapsto nx$$

is an isomorphism. We see that is it is also an isomorphism $m\mathbb{Z} \to mn\mathbb{Z}$. Therefore

$$n\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$$

When we consider the map acting on cosets.

Similarly

$$G^{(n)} \cong m\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$$

In conclusion

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

Corollary 12.2.3.1
Let G be a finite abelian group, and

$$|G| = \prod_{i=1}^{k} p_i^{a_i}$$

be the prime factorization of $|G|$.
Then

$$G \cong \times_{i=1}^{k} G_i$$

where $|G_i| = p_i^{a_i}$.

Proof
We know that

$$G \cong G^{(p_1^{a_1})} \times G^{(\prod_{i=2}^{k} p_i^{a_i})}$$

The rest follows by induction.

Proposition 12.2.4
If G is a finite abelian group, then

$$G \cong \times_{i=1}^{k} C_{a_i}$$

for some sequence $a_1, \ldots, a_k$ where every a_i is a prime power.
Where C_n is the multiplicative form of $\mathbb{Z}/n\mathbb{Z}$.

Proof
By the previous corollary, it suffices to consider the case when G is a p-group.

Write

$$|G| = p^n$$

We will argue by induction on n.

The base case is $n = 0$, which trivially holds as G is the trivial (cyclic) group.

Choose an element $x \in G$ of maximal order, and let

$$|x| = p^r$$

Since G is abelian

$$N := \langle x \rangle \trianglelefteq G$$

Bu then by induction

$$G/N \cong \times_{j=1}^{\ell} C_{b_j}$$

for some sequence b_j of prime powers. Notice that by Lagrange's theorem,

$$b_j = p^{s_j}$$

since the order of C_{b_j} necessarily divides $|G| = p^r$.

For each $1 \leq j \leq \ell$, let

$$\tilde{y_j}$$

be a generator of C_{b_j}.

Now let

$$y_j N \in G/N$$

be the element of G/N corresponding to

$$(e, \dots, e, \tilde{y_j}, e, \dots, e)$$

(j-th position).

We know that

$$|y_j| = p^{t_j}$$

for some $r \geq t_j \geq s_j$ by the choice of $\tilde{y_j}$.

Since $C_{b_j} = \langle \tilde{y_j} \rangle$, we also know that

$$(y_j N)^{b_j} = N \implies y_j^{b_j} \in N$$

Thus we can write

$$y_j^{b_j} = x^{c_j}$$

Now $b_j = p^{s_j}$, so we have taken it p^{s_j} of the way to its order. Thus

$$|y_j^{b_j}| = \frac{p^{t_j}}{p^{s_j}} = p^{t_j - s_j}$$

But $|x| = p^r$. Seeing how

$$(y_j^{b_j})^{p^{t_j - s_j}} = (x^{c_j})^{p^{t_j - s_j}} = e$$

It must be that

$$c_j p^{(t_j - s_j)} | p^r$$

and we can conclude that

$$c_j = d_j p^{r - (t_j - s_j)} = d_j p^{r - t_j + s_j}$$

Define

$$z_j := y_j x^{-d_j p^{r - t_j}}$$

Since powers of x live in N, we know that

$$z_j N = y_j N$$

Moreoever

$$z_j^{b_j} = y_j^{b_j} x^{-d_j p^{r-t_j+s_j}} = y_j^{b_j} y_j^{-b_j} = e$$

So $|z_j| | b_j$. Let $q : G \to G/N$ be the quotient map and remark that if $|z_j| < b_j$ then

$$q(y_j) = q(z_j) \implies eN = q(z_j^{|z_j|}) = q(z_j)^{|z_j|} = q(y_j)^{|z_j|}$$

But $\tilde{y_j}^{|z_j|} \in \langle \tilde{y_j} \rangle \setminus \{e\}$ and so $(y_j N)^{|z_j|} \neq eN$, which is a contradiction. So $b_j \leq |z_j|$. Putting the two observation together give us

$$|z_j| = b_j$$

Let

$$H := \langle z_1, \dots, z_\ell \rangle \leq G$$

and suppose $w \in H \cap N$.

Then

$$w = z_1^{n_1} \dots z_\ell^{n_\ell}$$

for some $0 \leq n_j < b_j$ as we as in the finite abelian setting. We have

$$\begin{aligned} q(w) &= \prod_{j=1}^{\ell} q(z_j)^{n_j} \\ &= \prod_{j=1}^{\ell} (z_j N)^{n_j} \\ &= \prod_{j=1}^{\ell} (y_j)^{n_j} \\ &\cong (\tilde{y_j}^{n_j}) \end{aligned}$$

But $w \in N$ so $q(w) = e$ and $n_j = 0$. This shows that

$$H \cap N = \{e\}$$

Suppose $g \in G$. Then

$$gN \cong (\tilde{y_j}^{m_\ell})$$

This implies that

$$gN = \prod_{j=1}^{\ell} (z_j N)^{m_j} = \left(\prod_{j=1}^{\ell} z_j^{m_j} \right) N$$

Notice then that

$$gN := \{gn : n \in N\} = \left(\prod_{j=1}^{\ell} z_j^{m_j} \right) N = \left\{ \left(\prod_{j=1}^{\ell} z_j^{m_j} \right) n : n \in N \right\}$$

and G is the union of all such cosets. In particular we have

$$g \in HN$$

Since G is abelian, $H, N \trianglelefteq G$. Thus

$$G = N \times H$$

We know that $N \cong C_{p_r}$ and $|H| < |G|$. So by induction, H is also a product of cyclic p-groups.

12.2.1 The Classification

Theorem 12.2.5
If G is a finite abelian group, then

$$G \cong \times_{i=1}^{k} C_{a_i}$$

where $a_i \leq a_{i+1}$ is a sequence of prime powers.
Furthermore, this decomposition is unique.

Notice that

$$C_2 \times C_3 \cong C_6$$

so if we do not require prime powers, the decomposition is not unique.

Proof
It suffices to prove uniqueness.

Suppose that

$$G \cong \times_{j=1}^{\ell} C_{b_\ell}$$

By observation

$$G^{(m)} \cong \times_{j=1}^{\ell} C_{b_j}^{(m)}$$

If $p \neq q$ are primes, then

$$C_{p^r}^{(q^s)} = \{e\}$$

Otherwise

$$|C_{p_r}^{(p^s)}| = p^{\min(r,s)}$$

By our work before for the case where $r \leq s$ and $s \geq r$ is the entire group as the order of any element divides the order of G.

So

$$\begin{aligned}|G^{(p^r)}| &= \prod_{s=1} \prod_{j:b_j=p^s} |C_{b_j}^{(p^r)}| \\ &= \prod_{s=1} \prod_{j:b_j=p^s} p^{\min(r,s)}\end{aligned}$$

For $1 \leq s < r$ the formular for $|C_{b_j}^{(p^r)}|$ is identical. It only changes when we have $s \geq r$. Thus

$$\frac{|G^{(p^r)}|}{G^{(p^{r-1})}} = \prod_{s \geq r} \prod_{j:b_j=p^s} \frac{p^r}{p^{r-1}}$$

It follows that by taking $\log_p$ of both sides

$$\log_p |G^{(p^r)}| - \log_p |G^{(p^{r-1})}| = |\{j : b_j = p^s, s \geq r\}|$$

Notice that the LHS does not depend on the decomposition at all. Given the RHS however, we can easily recover the b_j's by querying all prime power divisors of G in decreasing size and subtracting off powers we have already seen. This means that there is only one single decomposition, since we can use the same formulat to extract the a_i's.

Chapter 13

Finitely Presented Groups

How can we get more groups?

The idea is to take some generators and define some relations between them.

13.1 Free Groups

What if we did not have any relations?

Definition 13.1.1 (Word)
A (group) word over a set S is a formal expression

$$s_1^{a_1} \dots s_k^{a_k}$$

where $k \geq 0$ and $s_1, \dots, s_k$ is a sequence in S and $a_1, \dots, a_k \in \mathbb{Z}$.
When $k = 0$, we get the empty word

$$\epsilon$$

(also denoted e).

Definition 13.1.2 (Concatenation)
The concatenation of two words w_1, w_2 is the sequence

$$w_1 w_2$$

Definition 13.1.3 (Reduced)
A word

$$s_1^{a_1} \dots s_k^{a_k}$$

is reduced if

$$s_i \neq s_{i+1}$$

for all $1 \leq i \leq k-1$ and

$$a_i \neq 0$$

for $1 \leq i \leq n$.

Definition 13.1.4 (Equivalent)
Two words w_1, w_2 are equivalent if w_1 can be changed to w_2 by inserting or deleting s^0, replacing by s^{a+b} with $s^a s^b$ for $a, b \in \mathbb{Z}$ or the inverse.

Lemma 13.1.1
Every word is equivalent to a unique reduced word.

Definition 13.1.5 (Free Group)
Let S be a set.
The free group

$$\mathcal{F}(S)$$

generated by S is the set of reduced words over S.
The group operation is concatenation.
The identity is ϵ, the empty word.

13.1.1 Universal Property

Proposition 13.1.2 (Universal Property of Free Groups)
If $\phi : G \to S$ is a function, there is a unique group homomorphism $\tilde{\phi} : \mathcal{F}(S) \to G$ with

$$\tilde{\phi}(s) = \phi(s)$$

for all $s \in S$.

13.2 Group Presentations

Definition 13.2.1 (Generated Normal Subgroup)
Let G be a group, and let $S \subseteq G$.
The normal subgroup generated by S is

$$\bigcap_{S \subseteq N \trianglelefteq G} N$$

Remark that this is a normal subgroup.

Definition 13.2.2 (Group Presentation)
Let S be a set and $R \subseteq \mathcal{F}(S)$.
The group presentation

$$\langle S : R \rangle$$

denotes the group

$$\mathcal{F}(S)/K$$

where K is the normal subgroup of $\mathcal{F}(S)$ generated by R.

Definition 13.2.3 (Presentation)
If

$$G \cong \langle S : R \rangle$$

then $\langle S : R \rangle$ is called a presentation of G.

Presentations in general are not unique. Moreover every group has a presentation whose generators are simply the members of G.

13.2.1 Finitely Presented Groups

Definition 13.2.4 (Finitely Presentable)
A presentation $\langle S : R \rangle$ is finite if both S, R are finite.
A group G is fintiely presentable if

$$G \cong \langle S : R \rangle$$

for some finite presentation $\langle S : R \rangle$.

Theorem 13.2.1 (Universal Property of Finitely Presented Groups)
Let $G = \langle S : R \rangle$ and let H be a group.
If $\phi : S \to H$ is a function such that

$$\phi(s_1)^{a_1} \dots \phi(s_k)^{a_k} = e$$

for all words in R, then there is a unique homomorphism $\tilde{\phi} : G \to H$ such that

$$\tilde{\phi}(s) = \phi(s)$$

for all $s \in S$.

13.2.2 Word Problem

Given $S, R \subseteq \mathcal{F}(S)$, and $w \in \mathcal{F}(S)$, determine if

$$[w] = e$$

in $\langle S : R \rangle$.

Often we fix S, R, in which case this is called the word problem is $\langle S : R \rangle$.

Theorem 13.2.2
There is a finite presentation $\langle S : R \rangle$ for which the word problem is undecidable.

Now consider another problem:

Given finite $S, R \subseteq \mathcal{F}(S)$, determin if $\langle S : R \rangle$ is the trivial group.

This is a special case of the isomorphism problem. Given a finite S_1, S_2 and $R_1 \subseteq \mathcal{F}(S_1)$ and $R_2 \subseteq \mathcal{F}(S_2)$, determine if $\langle S_1 : R_1 \rangle$ and $\langle S_2 : R_2 \rangle$ are isomorphic.

Theorem 13.2.3
The problem of determining whether

$$\langle S : R \rangle$$

is trivial for finite S and R is undecidable.

13.3 Optional Group Material

13.3.1 Simple Groups

Definition 13.3.1
A group is simple if it has no non-trivial proper normal subgroups.

Simple groups can be thought of as building blocks for other groups.

13.3.2 Semidirect Products

Definition 13.3.2 (Automorphism)
An isomorphism $\phi : G \to G$.

We write $\mathrm{Aut}(G)$ to denote the collection of all automorphisms of G.

Lemma 13.3.1
$\mathrm{Aut}(G)$ is a group under composition.

Definition 13.3.3 (Semidirect Product)
Let G, H be groups and let $\phi : G \to \mathrm{Aut}(H)$ be a homomorphism.
The semidirect product of G, H is the set $G \times H$ with binary operation

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, \phi(g_1)(h_1)h_2)$$

The semidirect product is denoted by $G \ltimes H$.

Theorem 13.3.2
Suppose G is a groups and $H \leq G, N \trianglelefteq G$ such that G is the internal direct product of H, N.
Then $\phi : H \to \mathrm{Aut}(N)$ given by

$$h \mapsto C_h$$

is a homomorphism, and

$$G \cong H \ltimes_\phi N$$

Here C_h refers to the conjugation automorphism of h on G.

Part II

Rings

Chapter 14

Rings & Fields

14.1 Rings

Definition 14.1.1 (Ring)
A tuple $(R, +, \cdot)$ where $(R, +)$ is an abelian group and $\cdot$ is an associative binary operation which is also distributive.

Definition 14.1.2 (Commutative Ring)
We say a ring is commutative if multiplication is commutative.

We write $-a$ to indicate the additive inverse of a in R.

14.1.1 Basic Properties

Proposition 14.1.1
If R is a ring

(a) $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$

(b) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ for all $a, b \in R$

(c) $(-a) \cdot (-b) = a \cdot b$ for all $a, b \in R$

Proof
(a)

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \implies 0 \cdot a = 0$$

since it acts as the unique additive identity. The other case is analogous.

(b)

$$0 = 0 \cdot b = (a + (-a)) \cdot b = ab + (-a)b \implies -(ab) = (-a)b$$

and similarly $-(ab) = a(-b)$ so they are the same by the uniqueness of the inverse.

(c)

$$(-a)(-b) = -(a \cdot (-b)) = -(-(ab)) = ab$$

By the previous case.

14.1.2 Multiplicative Identities

Recall that an identity exists for a binary operation if there is an element 1 such that

$$1x = x1 = x$$

for all elements x.

Definition 14.1.3 (Ring with Identity)
A ring with identity is a ring where the multiplication operation has an identity.

In general, we use rings to indicate rings with identities.

We will specifically indicate a ring may not have a multiplicative identity. The term rng is sometimes used.

Another term for rings with identities is unital rings. Non-unital rings indicate rings without an identity.

Proposition 14.1.2
If R is a ring, then

$$-a = (-1) \cdot a$$

for all $a \in R$.

Proof
We have

$$\begin{aligned} 0 &= 0 \cdot a \\ &= (1 + (-1))a \\ &= 1 \cdot a + (-1) \cdot a \\ &= a + (-1) \cdot a \end{aligned}$$

So we must have

$$(-1) \cdot a = -a$$

by the uniqueness of the additive inverse.

14.2 Fields & Division Rings

Definition 14.2.1 (Unit)
Let R be a ring. An element $x \in R$ is called a unit if x has an inverse with respect to $\cdot$.

The set of all units is denoted by

$$R^{\times}$$

The set of units $R^{\times}$ forms a group under multiplication. Thus it is referred to as the group of units of R.

14.2.1 Trivial Ring

The smallest possible ring is $R = \{0\}$. This is a ring with identity $1 = 0$.

We call this the trivial or zero ring.

Unfortunately, the trivial ring is often an annoyance.

Lemma 14.2.1
Let R be a ring,

$$1 = 0$$

if and only if R is trivial.

Proof
If $1 = 0$, then

$$\begin{aligned} x &= 1 \cdot x \\ &= 0 \cdot x \\ &= 0 \end{aligned}$$

for all $x \in R$.

The converse is obvious.

14.2.2 Fields & Division Rings

If R is a ring with $1 \neq 0$, then

$$0 \cdot y = 0 \neq 1$$

for all $y \in R$ which implies $0 \notin R^\times$.

Definition 14.2.2 (Division Ring)
A ring R with $1 \neq 0$ such that

$$R^\times = R \setminus \{0\}$$

Definition 14.2.3 (Field)
A commutative division ring.

$\mathbb{Z}/n\mathbb{Z}$

Lemma 14.2.2
x is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(x, n) = 1$.

Proof
If $\gcd(x, n) = 1$, Bezout's lemma gives us the inverse for all non-zero elements.

Conversely, if $ax = 1$, then

$$ax + bn = 1$$

for some $b \in \mathbb{Z}$.

Thus $\gcd(x, n) = 1$ since $\gcd(x, n) | ax + bn$.

Corollary 14.2.2.1
$\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.

14.2.3 Division Rings

Theorem 14.2.3 (Wedderburn)
Any finite division ring is a field.

Definition 14.2.4 (Quaternions)
The ring of quaternions is the ring

$$Q = (\mathbb{R}^4, + \cdot)$$

The standard basis vectors are

$$1, i, j, k$$

with multiplication defined by

$$\begin{aligned} i^2 &= -1 \\ j^2 &= -1 \\ k^2 &= -1 \\ ijk &= -1 \end{aligned}$$

Notice that $ij = k$ and $i = jk$ which implies

$$ji = -k$$

and we actually have anti-commutativity.

14.3 Subrings

Definition 14.3.1 (Subring)
A subset $S \subseteq R$ is a subring if

1. $(S, +)$ is a group
2. $a, b \in S$ means $ab \in S$
3. $1 \in S$

Lemma 14.3.1
If S is a subring of R, then S is a ring.

If we are working with non-unital rings, we can leave out the last condition. If then in addition the third condition holds, then S is a unital subring.

We will use the terms subring and unital subrings interchangeably.

$x\mathbb{R}[x]$ and compactly supported functions are both examples of non-unital subrings.

14.3.1 Unital Subrings

Lemma 14.3.2
If R is a ring, $x \in R$, and $n, m \in \mathbb{Z}$, then

(i) $n1 \cdot x = x \cdot n1 = nx$

(ii) n(mx) = (nm)x

Proof
Distributivity.

Prime Subring

Lemma 14.3.3
Let R be a ring.

$$R_0 := \{n1 : n \in \mathbb{Z}\}$$

is a subring of R and is contained in every other subring.
As a group

$$R_0 \cong \mathbb{Z}/k\mathbb{Z}$$

where $k := \min\{m \in \mathbb{N} : m1 = 0\}$ and 0 if the set is empty.

Proof
R_0 is the cyclic subgroup of $(R, +)$ generated by 1. As a cyclic group,

$$R_0 \cong \mathbb{Z}/k\mathbb{Z}$$

If $n, m \in \mathbb{Z}$ then

$$n1 \cdot m1 = nm1 \in R_0$$

so R_0 is a unital subring.

If S is a unital subring of R, then $1 \in S$, so S contains the cyclic subgroup R_0 generated by 1.

Definition 14.3.2 (Prime Subring)
R_0

Definition 14.3.3 (Field Characteristic)
$\min\{m \in \mathbb{N} : m1 = 0\}$ and 0 if the set is empty.

14.4 Centre of a Ring

Definition 14.4.1 (Centre)
If R is a ring, its center is

$$Z(R) := \{x \in R : \forall y \in R, xy = yx\}$$

Lemma 14.4.1
$Z(R)$ is a subring of R.

Corollary 14.4.1.1
If R is a non-zero ring, then $Z(R)$ is non-trivial.

Proof
$Z(R)$ contains the prime subring R_0.

14.5 Homomorphisms

Definition 14.5.1 (Ring Homomorphism)
Let R, S be rings. A function $\phi : R \to S$ is a (unital) homomorphism if

(1) $\phi : (R, +) \to (S, +)$ is a group homomorphism

(2) $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$

(3) $\phi(1_R) = 1_S$

If the last condition is not satisfied, ϕ is a non-unital homomorphism.

Definition 14.5.2 (Ring Isomorphism)
A bijective homomorphism.

Proposition 14.5.1
Let $R_0 := \mathbb{Z}1_R$ be the prime subring of a ring R and $n := \text{char}(R)$.
Then $\phi : \mathbb{Z}/n\mathbb{Z} \to R_0$ given by

$$a \mapsto a1$$

is a ring isomorphism.

Proof
We already know that ϕ is a group isomorphism. We need to check that it satisfies the additional constraints to be a ring homomorphism.

If $a, b \in \mathbb{Z}/n\mathbb{Z}$, then

$$\begin{aligned} \phi(ab) &= ab1 \\ &= a(b1) \\ &= (a1)(b1) \\ &= \phi(a)\phi(b) \end{aligned}$$

Moreoever $\phi(1) = 1_R$, so ϕ is a ring isomorphism by our prior remarks.

14.5.1 Basic Properties

Proposition 14.5.2
Let $R \to S$ be a homomorphism

(a) If $a \in R$ and $n \geq 0$ then $\phi(a^n) = \phi(a)^n$

(b) If $u \in R^\times$, then $\phi(u) \in S^\times$, and $\phi(u^n) = \phi(u)^n$ for all $n \in \mathbb{Z}$

(c) If ϕ is an isomorphism, then ϕ^{-1} is a ring homomorphism.

Proof
The only non-trivial statement is (c).

We already know that ϕ^{-1} is a group homomorphism. Moreover

$$\phi(1_R) = 1_S \implies \phi^{-1}(1_S) = 1_R$$

If $a, b \in S$, then $a = \phi(\phi^{-1}(a))$ and likewise for b. Thus

$$\begin{aligned} ab &= \phi(\phi^{-1}(a))\phi(\phi^{-b}(b)) \\ &= \phi(\phi^{-1}(a)\phi^{-1}(b)) \\ &\implies \\ \phi^{-1}(ab) &= \phi^{-1}(a)\phi^{-1}(b) \end{aligned}$$

and so ϕ^{-1} is indeed a homomorphism.

Proposition 14.5.3
Let $\phi : R \to S$ be a homomorphism, where S is not zero.

(a) $\operatorname{Im}\phi$ is a subring of S

(b) $\ker\phi$ is a non-unital subring of R

Proof
(a): We already know that $\operatorname{Im}\phi$ is a subgroup of $(S, +)$.

Since $\phi(1_R) = 1_S$, we have $1_S \in \operatorname{Im}\phi$.

Finally, if $a, b \in \operatorname{Im}\phi$, then $a = \phi(x), b \in \phi(y)$ for some $x, y \in R$. Thus

$$ab = \phi(x)\phi(y) = \phi(xy) \in \operatorname{Im}\phi$$

(b): We delay the proof until we learn about ideals.

Observe that if $1 \in \ker\phi$ and ϕ is unital, then $1_S = \phi(1_R) = 0_S$, so S MUST be the zero ring.

14.6 Polynomials

Definition 14.6.1 (Polynomial)
Given a ring R, define

$$R[x] := \{(a_i)_{i\geq 0} \subseteq R : \exists n, \forall i \geq n, a_i = 0\}$$

We define the binary operation $+$ component-wise and the binary operation $\cdot$ as expected.

Lemma 14.6.1
$(R[x], +, \cdot)$ forms a ring.

$R[x]$ is called the ring of polynomials in variable x with coefficients in R.

Definition 14.6.2 (Degree)
The degree of $(a_i)_{i\geq 0} \in R[x]$ is the largest integer such that $a_i \neq 0$ and $-\infty$ is no such n exists.

By definition

$$\deg(0) = -\infty$$

Definition 14.6.3 (Coefficient)
The coefficient of x^i in $(a_i)_{i\geq 0}$ is a_i.

Definition 14.6.4 (Monomial)
A polynomial of the form

$$x^i$$

for some $i \geq 0$.

Definition 14.6.5 (Term)
A polynomial of the form

$$a_i x^i$$

If

$$p(x) = \sum_{i=0}^{n} a_i x^i$$

is a polynomial of degree n, then the monomials $a_i x^i$ are the terms of p.

$a_n x^n$ is the leading term, and a_n is the leading coefficient.

14.6.1 Constant Polynomials

Definition 14.6.6 (Constant Polynomials)
Polynomials of degree at most 0 are called constant polynomials

Lemma 14.6.2
Let R be a ring. Then set of constant polynomiasl in $R[x]$ is a subring. Moreoever, it is isomorphic to R.

We can think of R as a subring of $R[x]$.

14.6.2 Commutativity

Lemma 14.6.3
If R is commutative, then $R[x]$ is commutative.

Proof
Pick $p, q \in R[x]$.

$$\begin{aligned} pq &= \sum_{i=0}^{n} a_i x^i \sum_{j=0}^{m} b_j x^j \\ &= \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j} \\ &= \sum_{i=0}^{n} \sum_{j=0}^{m} b_j a_i x^{i+j} \\ &= \sum_{j=0}^{m} b_j x^j \sum_{i=0}^{n} a_i x^i \\ &= qp \end{aligned}$$

While $R[x]$ makes sense even if R is not commutative. However, since $x \in Z(R[x])$, it is not the most "natural".

14.6.3 Evaluation

Definition 14.6.7 (Evaluation)
If

$$p(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$$

and $c \in R$, then the evaluation of $p(x)$ at c is

$$p(c) := \sum_{i=0}^{n} a_i c^i.$$

Proposition 14.6.4
If R is commutative and $c \in R$, then $R[x] \to R$ given by

$$p(x) \mapsto p(c)$$

is a homomorphism.

This homomorphism is called evaluation at c or substitution at c. When necessary we denote it by

$$\mathrm{ev}_c$$

14.6.4 Polynomials over Fields

The most common type of polynomial rings are $\mathbb{K}[x]$ where $\mathbb{K}$ is some field.

Proposition 14.6.5
Let $\mathbb{K}$ be some field.

(a) $\deg(fg) = \deg(f) + \deg(g)$ for all $f, g \in \mathbb{K}[x]$

(b) $\mathbb{K}[x]^\times = \mathbb{K}^\times$

Remark that

$$\deg(0 \cdot f) = -\infty = -\infty + \deg(f)$$

which explains why we defined things this way.

14.6.5 Multivariable Polynomials

Definition 14.6.8 (Multivariable Polynomial)
For any sequence of variables

$$x_1, \ldots, x_n$$

and a ring R, we define recursively define

$$R[x_1, \ldots, x_n] := R[x_1, \ldots, x_{n-1}][x_n]$$

Elements of $R[x_1, \ldots, x_n]$ are technically of the form

$$\sum_i a_i(x_1, \ldots, x_{n-1}) x_n^i$$

where $a_i \in R[x_1, \ldots, x_{n-1}]$ is an $n-1$-variate polynomial. However we usually just write

$$\sum_{i=(i_1,\ldots,i_n)} a_i x^i$$

where

$$x^i := x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$$

What if we reorder $x_1, \dots, x_n$?

Lemma 14.6.6
Let R be a ring, $x_1, \dots, x_n$ a sequence of variables, and $\sigma \in S_n$.
Then there is an isomorphism $R[x_{\sigma(1)}, \dots, x_{\sigma(n)}] \to R[x_1, \dots, x_n]$ where

$$\sum_{i_1, i_2, \dots, i_n} a_i x_{\sigma(1)}^{i_1} \dots x_{\sigma(n)}^{i_n} \mapsto \sum_{i_1, \dots, i_n} a_i x_1^{i_{\sigma^{-1}(1)}} \dots x_n^{i_{\sigma^{-1}(n)}}$$

The isomorphism in the lemma should not be confused with the isomorphism $\mathbb{Z}[y, x] \to \mathbb{Z}[x, y]$ given by

$$p(y, x) \mapsto p(x, y)$$

Definition 14.6.9 (Evaluation)
If $p = \sum_i a_i x^i \in R[x_1, \dots, x_n]$ and $c \in R^n$ then we define

$$p(c) := \sum_i a_i c_1^{i_1} \dots c_n^{i_n}$$

Lemma 14.6.7
Let $c \in R^n$.
Then funtion $\mathrm{ev}_c : R[x_1, \dots, x_n] \to R$ given by

$$p \mapsto p(c)$$

is precisely the composition

$$\begin{aligned} \mathrm{ev}_{c_1} \circ \dots \circ \mathrm{ev}_{c_n} : R[x_1, \dots, x_{n-1}][x_n] &\to R[x_1, \dots, x_{n-1}] \\ &= R[x_1, \dots, x_{n-2}][x_{n-1}] \\ &\to \dots \\ &\to R[x_1] \\ &\to R \end{aligned}$$

and hence is a homomorphism given that R is commutative.

14.7 Group Rings

Definition 14.7.1 (Group Ring)
Let G be a group and R a ring.
The group ring RG of G with coefficients in R is the set of formal sums

$$\left\{\sum_{g\in G} c_g \cdot g : \exists X \subseteq G, |X| < \infty, \forall g \notin X, c_g = 0\right\}$$

The group ring RG is equiped with operations

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g$$

and

$$\begin{aligned}\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) &= \sum_{g,h\in G} a_g b_h gh \\ &= \sum_{k\in G}\left(\sum_{g\in G} a_g b_{g^{-1}k}\right) k\end{aligned}$$

A formal sum with coefficients in R is a finitely supported function $G \to R$ given by

$$g \mapsto a_g$$

Definition 14.7.2 (Finitely Supported)
0 except at finitely many points of G.

The group elements $g \in G$ are "placeholders" in this formal sum.

14.7.1 Commutativity

Proposition 14.7.1
Let R be a ring and G a group.
RG is a ring with identity $\underline{e}$.
Moreoever, if G is commutative, then RG is commutative.

Since we will be focusing on commutative rings, we omit the proof.

14.7.2 Homomorphisms

Proposition 14.7.2
Let R be a ring and $\phi : G \to H$ a group homomorphism.
Then $\psi : RG \to RH$ defined by

$$\psi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \phi(g)$$

is a ring homomorphism.

Proof
Clearly the formal sum $\sum_{g\in G} a_g\phi(g)$ is finitely supported.

We have

$$\psi(\underline{e_G}) = \underline{\phi(e)} = \underline{e_H}$$

so ψ is unital.

Pick

$$x := \sum_{g\in G} a_g \underline{g}, y := \sum_{h\in G} b_h \underline{h}$$

We have

$$\begin{aligned}\psi(x+y) &= \sum_{g\in G}(a_g + b_g)\phi(g) \\ &= \sum_{g\in G} \vec{a}_g \underline{\phi(g)} + \sum_{g\in G} b_g \underline{\phi(g)} \\ &= \psi(x) + \psi(y)\end{aligned}$$

Moreoever

$$\begin{aligned}\psi(xy) &= \sum_{g,h} a_g b_h \underline{\phi(gh)} \\ &= \sum_{g,h} a_g b_h \underline{\phi(g)\phi(h)} \\ &= \left(\sum_{g\in G} a_g \underline{\phi(g)}\right)\left(\sum_{h\in G} b_h \underline{\phi(h)}\right) \\ &= \psi(x)\psi(y)\end{aligned}$$

So ψ is a homomorphism by definition.

Chapter 15

Ideals & Quotients

15.1 Ideals

Definition 15.1.1 (Ideal)
An ideal of a ring R is a subgroup $\mathcal{I}$ of $(R,+)$ such that $m \in \mathcal{I}, r \in R$ implies

$$rm, mr \in \mathcal{I}$$

Lemma 15.1.1
If $\phi : R \to S$ is a homomorphism and $m \in \ker\phi$, then rm, mr are in $\ker\phi$ for all $r \in R$.

Proof
We have

$$\phi(rm)\phi(r)\phi(m) = \phi(r) \cdot 0_S = 0$$

and similary for mr.

This completes the statement and proof of our earlier proposition

Proposition 15.1.2
Let $\phi : R \to S$ be a homomorphism, where S is not zero.
Then $\operatorname{Im}\phi$ is a subring of S.
Moreoever $\ker\phi$ is an ideal of R.

15.1.1 Equivalence Characterizations

Lemma 15.1.3
Let R be a ring and $\mathcal{I} \subseteq R$. $\mathcal{I}$ is an ideal if and only if

(a) $\mathcal{I}$ is non-empty

(b) if $r \in R$ and $f, g \in \mathcal{I}$, then $rf + g, fr + g \in \mathcal{I}$

15.1.2 Examples

Lemma 15.1.4
$m\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for every $m \in \mathbb{Z}$.

Lemma 15.1.5
If $f(x) \in R[x]$ has degree at most n, and $c \in R$, then there are

$$a_0, \ldots, a_n \in R$$

such that

$$f(x) = \sum_{i=0}^{n} a_i (x - c)^i$$

where $(x - c)^0$ is understood to be 1.

Proof
Induction on n.

The base case of $n = 0$ holds trivially.

If the coefficient of x^n in $f(x)$ is a_n, then

$$\deg\left(f(x) - a_n (x - c)^n\right) \leq n - 1$$

By induction we are done.

Since ev_c is a homomorphism

$$\mathrm{ev}_c (x - c)^i = \begin{cases} 0, & i > 0 \\ 1, & i = 0 \end{cases}$$

So if $f(x) = \sum_{i=0}^{n} a_i(x-c)^i$ then

$$f(c) = a_0$$

Specifically $f(c) = 0$ if and only if $a_0 = 0$ and

$$f(x) = \sum_{i=1}^{n} a_i(x-c)^i = (x-c)\sum_{i=1}^{n} a_i(x-c)^{i-1}$$

Hence

$$\ker \mathrm{ev}_c = (x-c)R[x]$$

15.1.3 Proper Ideals

Lemma 15.1.6
If $\mathcal{I}$ is an ideal of R and $1 \in \mathcal{I}$, then $\mathcal{I} \in R$.

Thus we typically want to look at $\mathcal{I} \neq R$.

Definition 15.1.2 (Proper Ideal)
$\mathcal{I} \subseteq R$ but $I \neq R$.

15.1.4 Ideals in Fields

Proposition 15.1.7
The only ideals in a field $\mathbb{K}$ are (0) and $\mathbb{K}$.

Proof
Suppose $\mathcal{I} \subseteq \mathbb{K}$ is an ideal. If $x \in \mathcal{I}$ where $x \neq 0$ then

$$x^{-1}x = 1 \in \mathcal{I}$$

Thus $\mathcal{I} = \mathbb{K}$.

More specifically, having ANY invertible element in $\mathcal{I}$ means $\mathcal{I}$ is NOT proper.

Corollary 15.1.7.1
Let $\phi : \mathbb{K} \to R \neq (0)$ be a ring homomorphism where $\mathbb{K}$ is a field.
Then ϕ is an injection.

Proof
$\ker\phi$ is an ideal of $\mathbb{K}$, so $\ker\phi$ is either (0) or $\mathbb{K}$.

If $\ker\phi = (0)$, then

$$0 = \phi(1_{\mathbb{K}}) = 1_R$$

so R was zero.

This cannot be so

$$\ker\phi = (0)$$

This suffices to show that ϕ is injective.

Notice that this means there are no homomorphisms from an infinite field to a finite field, as all such homomorphisms are non-injective.

A concrete example is that any function $\mathbb{R} \to \mathbb{Q}$ is NOT a homomorphism.

15.2 Quotient Rings

Recall that kernels of homomorphisms are normal subgroups and vice versa. Are ideals the kernel of some homomorphism?

Let R be a ring and $\mathcal{I}$ an ideal of R. Since $(R,+)$ is abelian, $\mathcal{I} \trianglelefteq R$. Why not put a ring struture on

$$R/\mathcal{I}$$

Theorem 15.2.1
Let $\mathcal{I}$ be an ideal of R. Let addition and multiplication be defined as

$$[x] + [y] = [x + y], [x][y] = [xy]$$

Then $(R/\mathcal{I}, +, \cdot)$ is a ring. Moreoever, the quotient map $q : R \to R/\mathcal{I}$ given by

$$x \mapsto [x]$$

is a surjective ring homomorphism with

$$\ker q = \mathcal{I}$$

Proof
We already know that $(R/\mathcal{I}, +)$ is an abelian group.

Well-definedness, associativity, existence of a multiplicative identity, and distributivity follows literally from definition. So $R/\mathcal{I}$ is a ring.

We know that q is a group homomorphism. Checking the definition for ring homomorphisms shows that it is indeed a ring homomorphism.

Definition 15.2.1 (Quotient Ring)
$R/\mathcal{I}$ is called the quotient of R by the ideal $\mathcal{I}$, or just a quotient ring.

Corollary 15.2.1.1
Every ideal is the kernel of some homomorphism.

15.3 Generated Ideals

Proposition 15.3.1
Let $\mathcal{F}$ be an arbitrary family of ideals in R. Then

$$\bigcap_{\mathcal{I}\in\mathcal{F}} \mathcal{I}$$

is an ideal of R.

Definition 15.3.1 (Generated Ideal)
Let $X \subseteq R$, the ideal generated by X is

$$(X) := \bigcap_{\mathcal{I}\in\mathcal{F}} \mathcal{I}$$

where $\mathcal{F}$ is the family of ideals containing X.

Observe that for $X \subseteq \mathcal{I}$ where $\mathcal{I}$ is an ideal

$$X \subseteq (X) \subseteq \mathcal{I}.$$

We say that (X) is the smallest ideal containing X.

Proposition 15.3.2
If R is a ring with $X \subseteq R$, then

$$(X) = \left\{ \sum_{i=1}^{k} s_i x_i t_i : k \geq 0, s_i, t_i \in R, x_i \in X, 1 \leq i \leq k \right\} =: \mathcal{I}.$$

Proof
$(X) \subseteq \mathcal{I}$ Use the ideal test to see that $\mathcal{I}$ is an ideal. The result follows from definition.

$(X) \supseteq \mathcal{I}$ Each individual term of the sum is a member of (X), thus their sum is also in (X).

Corollary 15.3.2.1
If R is commutative and $X \subseteq R$

$$(X) = \left\{ \sum_{i=1}^{k} s_i x_i : k \geq 0, s_i, x_i \in R, x_i \in X, 1 \leq i \leq k \right\}.$$

15.3.1 Sum of Ideals

Definition 15.3.2 (Sum fo Ideals)
If $\mathcal{I}, \mathcal{J}$ are ideals

$$\mathcal{I} + \mathcal{J} := \{x + y : x \in \mathcal{I}, y \in \mathcal{J}\}.$$

Corollary 15.3.2.2
$(\mathcal{I} \cup \mathcal{J}) = \mathcal{I} + \mathcal{J}$.

Proof
It is clear that

$$\mathcal{I} + \mathcal{J} \subseteq (\mathcal{I} \cup \mathcal{J}).$$

since any ideal containing $\mathcal{I}, \mathcal{J}$ must contain both $\mathcal{I} + \mathcal{J}$.

To see the reverse inclusion, split a finite summation into terms of $(\mathcal{I})$ and terms of $(\mathcal{J})$. The sum can then be expressed as some $i + j \in \mathcal{I} + \mathcal{J}$ as desired.

15.3.2 Lattic of Ideals

The ideals of R are partialled ordered by set inclusion.

Definition 15.3.3 (Lattice of Ideals)
The ideals of R with order $\subseteq$.

The biggest subgroup below both $\mathcal{I}_1, \mathcal{I}_2$ is

$$\mathcal{I}_1 \cap \mathcal{I}_2.$$

The smallest subgroup above both $\mathcal{I}_1, \mathcal{I}_2$ is

$$\mathcal{I}_1 + \mathcal{I}_2.$$

15.4 Quotients by a Subset

For any $X \subseteq R$, we can get a new ring by considering

$$R/(X).$$

We know that $R/(X)$ is a unital ring, but when it is non-zero?

From group theory, we know that

$$R/\mathcal{I} = \{0\}$$

if and only if $\mathcal{I} = R$. We have shown that this happens if and only if $1 \in \mathcal{I}$.

Proposition 15.4.1
Let R be a ring and $X \subseteq R$. Then

$$R/(X) = \{0\}$$

if and only if there are $s_i, t_i \in R$ and $x_i \in X$ such that

$$\sum_{i=1}^{k} x_i x_i t_i = 1.$$

If R is commutative, we can ignore the t_i's.

15.5 Finitely Generated Ideals

Proposition 15.5.1
If R is commutative and $X = \{x_i\}_{1=1}^{n} \subseteq R$, then

$$(X) = \left\{ \sum_{i=1}^{n} r_i x_i : r_i \in R, 1 \leq i \leq n \right\}.$$

15.5.1 Principal Ideals

Definition 15.5.1 (Principal Ideal)
An ideal generated by a single element is called a Principal Ideal.

If $R = \mathbb{Z}$ and $m \in \mathbb{Z}$, then

$$(m) = m\mathbb{Z}$$

is a principle ideal.

Noncommutative Rings

If R is noncommutative, it is clear that (x) is not necessarily equal to

$$\{rx : r \in R\}$$

since $xr \in (x)$ for all $r \in R$.

In general, there is no nice formula and we have to use the general one.

Non-Principal Ideals

In $\mathbb{Z}[x, y]$

$$(x, y) = \{p(x, y)x + q(x, y)y : p, q \in \mathbb{Z}[x, y]\}.$$

This ideal is proper since it does not contain the constant polynomials.

Proposition 15.5.2
If there are polynomials $f, p, q \in \mathbb{Z}[x, y]$ such that

$$pf = x, qf = y$$

then $f \in \{\pm 1\}$.

Thus the only principal ideal containing (x, y) is $\mathbb{Z}[x, y]$ and (x, y) is not principal.

How about $(2, x)$ in $\mathbb{Z}[x]$? These are the polynomials for which the constant term is even.

Proposition 15.5.3
If $p, f \in \mathbb{Z}[x]$ are such that

$$pf = 2$$

then

$$f \in \{\pm 1, \pm 2\}.$$

This means that the only principal ideal containing $(2, x)$ is $\mathbb{Z}[x]$.

Chapter 16

Isomorphism Theorems

Most of these results follow directly from our work with group isomorphisms.

16.1 Universal Property of Quotient Rings

Let $\phi : G \to K$ be a group homomorphism, $N \trianglelefteq G$, and $q : G \to G/N$ the quotient homomorphism. Recall the universal property of quotient groups says that there is a homomorphism $\psi : G/N \to K$ such that

$$\psi \circ q = \phi$$

if and only if $N \subseteq \ker \phi$. Furthermore, if ψ exists, then it is unique.

Lemma 16.1.1
Let R, S, T be rings. Suppose that $\psi_1 : R \to T$ is a ring homomorphism and $\psi_2 : T \to S$ is a group homomorphism such that

$$\psi_2 \circ \psi_1$$

is a ring homomomorphism.
If ψ_1 is surjective, then ψ_2 is a ring homomorphism.

Proof
Follow the definitions.

Theorem 16.1.2 (Universal Property of Quotient Rings)
Suppose $\phi : R \to S$ is a ring homomorphism, and $\mathcal{I}$ is an ideal of R. Let $q : R \to R/\mathcal{I}$ be the quotient homomorphism.
There is a ring homomorphism $\psi : R/\mathcal{I} \to S$ such that

$$\psi \circ q = \phi$$

if and only if $\mathcal{I} \subseteq \ker \phi$. Furthermore, if ψ exists, then it is unique.

Proof
Existence: If $\mathcal{I} \subseteq \ker \phi$, then ψ exists as a group homomorphism.

Apply the previous lemma to see that ψ is a ring homomorphism.

Uniqueness: Leverage the uniqueness of quotient group homomorphism.

$\mathcal{I} \subseteq \ker \phi$: If ψ exists, it is also a group homomorphism. Apply the universal property of quotient groups.

16.2 First Isomorphism Theorem

Theorem 16.2.1 (First Isomorphism)
If $\phi : R \to S$ is a ring homomorphism then there is a ring isomorphism $\psi : R/\ker \phi \to \operatorname{Im} \phi$ such that

$$\phi = \psi \circ q$$

where $q : R \to R/\ker \phi$ is the quotient homomorphism.

Proof
By the universal property, there is a ring homomorphism $\psi : R/\ker \phi \to \operatorname{Im} \phi$ such that

$$\psi \circ q = \phi.$$

From the first isomorphism theorem for groups, there is a group isomorphism $\psi' : R/\ker \phi \to \operatorname{Im} \phi$ such that

$$\psi' \circ q = \phi$$

Now ψ is also a group homomorphism so by the uniqueness of ψ'

$$\psi = \psi'$$

is a bijection.

Proposition 16.2.2
Let R be a commmutative ring and $c \in R$.
Then
$$R[x]/(x-c)R[x] \cong R.$$

Proof
$(x-c)R[x] = \ker \operatorname{ev}_c$ where $\operatorname{ev}_c : R[x] \to R$ is the evaluation map.

If $r \in R$, then $\operatorname{ev}_c(r) = r$, so
$$\operatorname{Im} \operatorname{ev}_c = R.$$

By the first isomorphism theorem
$$R[x]/(x-c)R[x] \cong R.$$

16.3 Correspondance Theorem

Proposition 16.3.1
Let $\phi : R \to S$ be a ring homomorphism.

(a) If $\mathcal{I}$ is an ideal of S, then $\phi^{-1}(\mathcal{I})$ is an ideal of R

(b) If $\mathcal{I}$ is an ideal of R, and ϕ is surjective, then $\phi(\mathcal{I})$ is an ideal of S

Recall from group theory that if $\phi : G \to H$ is a group homomorphism, then there is a bijection
$$\{K \in \operatorname{Sub}(G) : \ker \phi \leq K\} \rightleftharpoons \operatorname{Sub}(H).$$

given by
$$K \mapsto \phi(K)$$

and
$$K' \mapsto \phi^{-1}(K').$$

Furthermore, if $\ker \phi \leq K, K_1, K_2 \leq G$

(a) $K_1 \leq K_2 \iff \phi(K_1) \leq \phi(K_2)$

(b) $\phi(K_1 \cap K_2) = \phi(K_1) \cap \phi(K_2)$

(c) K is normal if and only if $\phi(K)$ is normal

Theorem 16.3.2 (Correspondance Theorem for Rings)
Let $\phi : R \to S$ be a surjective group homomorphism.
There is a bijection

$$\{K \in \mathrm{Sub}(R^+) : \ker\phi \le K\} \rightleftharpoons \mathrm{Sub}(S^+).$$

Moreoever, if $\ker\phi \le K \le R^+$, then K is an ideal if and only if

$$\phi(K)$$

is an ideal.

Proof
Apply the previous proposition and use the fact that surjectiveness gives

$$K = \phi^{-1}(\phi(K)).$$

The special case of the quotient map $q : R \to R/\mathcal{I}$ is that if $\mathcal{I} \subseteq \mathcal{K} \le R^+$, then $\mathcal{K}$ is an ideal of R if and only if

$$\mathcal{K}/\mathcal{I}$$

is an ideal of $R/\mathcal{I}$.

Let R be a commutative ring. What are the ideal of $R[x]$ containing (x)?

We know that (x) is the kernel of the surjective homomorphism $\mathrm{ev}_0 : R[x] \to R$. Thus the ideals of $R[x]$ containing x correspond to ideals $\mathcal{I}$ of R.

If $\mathcal{I}$ is an ideal of R, the corresponding ideal of $R[x]$ is

$$\mathrm{ev}_0^{-1}(\mathcal{I}) = \{f \in R[x] : f(0) \in \mathcal{I}\} = \left\{\sum_{i=0}^{n} a_i x^i : n \ge 0, a_i \in R, 0 \le i \le n, a_0 \in \mathcal{I}\right\}.$$

16.4 Second Isomorphism Theorem

Recall from group theoy that if G is abelian and $H, K \le G$, then $H + K \le G$.

Furthermore, suppose that $i_H : H \to H + K$ is the inclusion, and $q_1 : H \to H/H \cap K$ and $q_2 : H + K \to (H + K)/K$ are the quotient maps.

Then there is an isomorphism

$$\psi : H/H \cap K \to (H + K)/K$$

such that $\psi \circ q_1 = q_2 \circ i_H$.

Let us extend this for rings.

Theorem 16.4.1 (Second Isomorphism Theorem for Rings)
Let S be a subring of R and $\mathcal{I}$ an ideal.
Then $S + \mathcal{I}$ is a subring of R and $S \cap \mathcal{I}$ is an ideal of S.
Moreoever, let $i_S : S \to S + \mathcal{I}$ be the inclusion with $q_1 : S \to S/S \cap \mathcal{I}$ and $q_2 : S \to (S + \mathcal{I})/\mathcal{I}$ being the quotient maps.
There is an isomorphism

$$\psi : S/S \cap \mathcal{I} \to (S + \mathcal{I})/\mathcal{I}$$

such that $\psi \circ q_1 = q_2 \circ i_s$.

Proof
$S + \mathcal{I}$ is a subring

$S \cap \mathcal{I}$ is an ideal of S

By the second isomorphism theorem for groups, there is group isomorphism ψ.

Apply the lemma from the Universal Property of Quotient Rings to see that it is a ring homomorphism as well.

Let $\mathcal{J}$ be an ideal of a commutative ring R. Define

$$\mathcal{I} := \{f \in R[x] : f(0) \in \mathcal{J}\} =: \mathrm{ev}_0^{-1}(\mathcal{J}).$$

Then R is a subring of $R[x]$, $R + \mathcal{I} = R[x]$ and $R \cap \mathcal{I} = \mathcal{J}$.

So

$$R/\mathcal{J} \cong R[x]/\mathcal{I}$$

by the second isomorphism theorem.

16.5 Third Isomorphism Theorem

Recall from group theory that if $N \trianglelefteq G$ and $N \leq K \trianglelefteq G$, with $q_1 : G \to G/N$, $q_2 : G/N \to (G/N)/(K/N)$, and $q_3 : G \to G/K$ being quotient maps, then there is an isomorphism

$$\psi : G/K \to (G/N)/(K/N)$$

such that $\psi \circ q_3 = q_2 \circ q_1$.

Theorem 16.5.1 (Third Isomorphism Theorem for Rings)
Suppose $\mathcal{I} \subseteq \mathcal{K}$ are ideals of a ring R.
Let $q_1 : R \to G/\mathcal{I}$, $q_2 : R/\mathcal{I} \to (R/\mathcal{I})/(\mathcal{K}/\mathcal{I})$, and $q_3 : R \to R/\mathcal{K}$ be quotient maps.
Then there is an isomorphism

$$\psi : R/\mathcal{K} \to (R/\mathcal{I})/(\mathcal{K}/\mathcal{I})$$

such that $\psi \circ q_3 = q_2 \circ q_1$.

Proof
Simply apply the lemma from the Universal Property of Quotient Rings again.

Chapter 17

More Ideals

17.1 Complex Numbers

Suppose we did not know about $\mathbb{C}$ but wanted a square root of -1. Take $\mathbb{R}[x]$ and mod it by x^2+1. The motivation is that

$$x^2+1=0 \iff x^2=-1.$$

Lemma 17.1.1
Every element of $\mathbb{R}[x]/(x^2+1)$ can be written uniquely in the form

$$a+b\bar{x}$$

for some $a, b \in \mathbb{R}$.

Theorem 17.1.2
$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Proof
Since $\mathbb{R}$ is a subring of $\mathbb{C}$, we can consider $\mathbb{R}[x]$ as a subring of $\mathbb{C}[x]$.

Consider the homomorphism $\phi : \mathbb{R}[x] \to \mathbb{C}$ given by

$$p(x) \mapsto p(i).$$

Since $i^2+1=0$, $(x^2+1) \subseteq \ker\phi$.

By the universal property of quotient rings, there is a homomorphism

$$\psi : \mathbb{R}[x]/(x^2+1) \to \mathbb{C}$$

such that $\psi \circ q = \phi$.

Thus

$$\psi(a + b\bar{x}) = a + bi.$$

By the lemma, ψ is a bijection.

Generalization

We constructed $\mathbb{C}$ by asking for an element x satisfying some polynomial equation(s).

In general we can construct rings this way but if we ask for too much, the ring might be zero.

17.2 Maximal Ideals

Let $\mathcal{I}$ be an ideal of a commutative ring R.

Definition 17.2.1
An ideal $\mathcal{I}$ of a ring R is maximal if the only ideals containing $\mathcal{I}$ are

$$\mathcal{I}, R.$$

A maximal ideal is a proper ideal which is maximal with respect to $\subseteq$.

Lemma 17.2.1
If $R/\mathcal{I}$ is a field, then $\mathcal{I}$ is maximal.

Proof
We know the only ideals in a field $\mathbb{K}$ are (0) and $\mathbb{K}$. Suppose that $\mathbb{K} = R/\mathcal{I}$ and $q : R \to \mathbb{K}$ is the quotient map. By the correspondence theorem, the only ideals of R containing $\mathcal{I}$ are

$$q^{-1}(\langle 0 \rangle) = \ker q = \mathcal{I}, q^{-1}(\mathbb{K}) = R.$$

Proposition 17.2.2
A commutative ring R is a field if and only if $1 \neq 0$ and the only ideals in R are $(0), R$.

Proof
$\underline{\implies}$ We know that any $0 \neq x \in \mathcal{I}$ has an inverse, thus $x^{-1}x = 1 \in \mathcal{I}$ and $\mathcal{I} = R$.

$\underline{\Longleftarrow}$ Suppose that $0 \neq x \in R$, then $(x) = R$, so there is some $y \in R$ such that

$$xy = 1.$$

By definition R is a field.

Theorem 17.2.3
Let $\mathcal{I}$ be an ideal in a commutative ring R.
Then $R/\mathcal{I}$ is a field if and only if $\mathcal{I}$ is maximal.

Proof
By the correspondence theorem, the only ideals of $R/\mathcal{I}$ are (0) and $R/\mathcal{I}$ if and only if the only ideals of R containing $\mathcal{I}$ are $\mathcal{I}, R$.

Thus by the proposition, $R/\mathcal{I}$ is a field if and only if $\mathcal{I}$ is maximal.

17.2.1 Zorn's Lemma

Lemma 17.2.4
Let R be a commutative ring and $\mathcal{F}$ a chain of ideals.
Then

$$\bigcup_{\mathcal{I} \in \mathcal{F}} \mathcal{I}$$

is an ideal of R.

Corollary 17.2.4.1
If $\mathcal{F}$ is a chain of proper ideals of R, there is a proper ideal which is an upper bound for $\mathcal{F}$.

Proof
$1 \notin F$ for all $F \in \mathcal{F}$.

Proposition 17.2.5
Suppose $\mathcal{J}$ is a proper ideal in a commutative ring R. There is a maximal ideal $\mathcal{K}$ of R containing $\mathcal{J}$.

Proof
Let $\mathcal{P}$ be the poset of proper ideals of R containing $\mathcal{J}$ and $\mathcal{F}$ a chain in $\mathcal{P}$.

By the lemma

$$\mathcal{I}' := \bigcup_{\mathcal{I} \in \mathcal{F}} \mathcal{I}$$

is an ideal of R.

Clearly $\mathcal{J} \subseteq \mathcal{I}'$ and $1 \notin \mathcal{I}'$ so $\mathcal{I}' \in \mathcal{P}$. Thus $\mathcal{I}'$ is an upper bound for $\mathcal{F}$ in $\mathcal{P}$.

By Zorn's lemma, $\mathcal{P}$ has a maximal element.

Corollary 17.2.5.1
For every non-zero commutative ring R, there is a field $\mathcal{K}$ such that there is a homomorphism

$$\phi : R \to \mathbb{K}.$$

Proof
Let $\mathcal{I}$ be any maximal ideal of R and let $\phi : R \to R/\mathcal{I}$ be the quotient map.

17.3 Integral Domains

17.3.1 Zero Divisors

Definition 17.3.1
Let R be a ring.
A non-zero element x is a zero divisor if there exists $0 \neq y \in R$ such that

$$xy = 0$$

or

$$yx = 0.$$

Lemma 17.3.1
Let u be a unit in a ring R. Then u is not a zero divisor.

Proof
Suppose for a contradiction that u is a zero divisor.

$$\begin{aligned} uv &= 0 \\ v &= u^{-1}uv = 0 \\ vu &= 0 \\ v &= vuu^{-1} = 0 \end{aligned}$$

Proposition 17.3.2
Suppose a non-zero element $x \in R$ is not a zero divisor.
If $xa = xb$ or $ax = bx$ for $a, b \in R$ then

$$a = b.$$

Proof
If $xa = xb$ then $x(a - b) = 0$. We must have $a - b = 0$.

A symmetric argument holds for $ax = bx$.

Corollary 17.3.2.1
Let R be a finite ring.
If $0 \neq x \in R$ is not a zero divisor, then x is a unit.

Proof
The function $\ell_x : R \to R$ given by

$$y \mapsto xy$$

is injective.

But since R is finite, ℓ_x is also surjective. Thus there is $y \in R$ such that

$$xy = 1.$$

The same argument holds to find a left inverse for x. Thus x is invertible.

17.3.2 Integral Domains

Definition 17.3.2 (Integral Domain)
A commutative ring R such that $1 \neq 0$ and R has no zero divisors.

Proposition 17.3.3
All finite integral domains are fields.

Proposition 17.3.4
If R is an integral domain

(a) If $f, g \in R[x]$ then $\deg fg = \deg f + \deg g$

(b) $R[x]$ is an integral domain

Proof
(a) No largest coefficients do not cancel.

(b) If $\deg fg = -\infty$ then by the previous formula either $\deg f = -\infty$ or $\deg g = -\infty$.

Proposition 17.3.5
If R is a subring of a field $\mathbb{K}$ then R is an (integral) domain.

Proof
Suppose that $x \neq 0$.

If $xy = 0$ for some $0 \neq y \in R$ then

$$y = x^{-1}xy = 0 \in \mathbb{K}$$

but then $y = 0 \in R$ as well.

So R has no zero divisors.

An nice example is $\mathbb{Z}$ being a subring of $\mathbb{Q}$ and hence a domain.

Proposition 17.3.6
If $\alpha \in \mathbb{C}$ satisfies $\alpha^2 \in \mathbb{Z}$ then

$$\mathbb{Z}[\alpha] := \{a + b\alpha : a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$.

This leads to interesting domains like the Gaussian Integers

$$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}.$$

17.4 Prime Ideals

Definition 17.4.1
Let R be a commutative ring.
A proper idea $\mathcal{I}$ of R is prime if for all $a, b \in \mathcal{R}$

$$ab \in \mathcal{I} \implies a \in \mathcal{I} \vee b \in \mathcal{I}.$$

Theorem 17.4.1
Let $\mathcal{I}$ be an ideal in a commutative ring R.
Then

$$R/\mathcal{I}$$

is an integral domain if and only if $\mathcal{I}$ is a prime ideal.

Proof
Since R is commutative and the quotient map q is surjective, $R/\mathcal{I}$ is commutative for any ideal $\mathcal{I}$. Moreover $R/\mathcal{I}$ is zero if and only if $\mathcal{I} = R$.

By the surjectivity of q, $R/\mathcal{I}$ has no zero divisors if and only if for all $a, b \in R$

$$(\bar{a} \cdot \bar{b} = 0 \implies \bar{a} = 0 \vee \bar{b} = 0) \iff (ab \in \mathcal{I} \implies a \in \mathcal{I} \vee b \in \mathcal{I}).$$

Thus $R/\mathcal{I}$ is an integral domain if and only if $\mathcal{I}$ is prime.

17.4.1 Primality & Factoring

Lemma 17.4.2
If R is an integral domain and $f, g \in R[x]$ have degree at least 1, then

$$fgR[x]$$

is not prime (ie $R/fgR[x]$ is not an integral domain).

Proof
We know that

$$\deg fgh \geq \deg fg = \deg f + \deg g > \deg f, \deg g$$

for all non-zero $h \in R[x]$.

So $fg \in fgR[x]$ but

$$f, g \notin fgR[x].$$

Proposition 17.4.3
Suppose R is a subring of a domain S and $x \in S$ is such that

$$x^2 = t^2$$

for some $t \in R$.
Then

$$x = t \vee x = -t.$$

Proof
If $x^2 = t^2$, then $x^2 - t^2 = 0$ so

$$(x-t)(x+t) = 0.$$

Since S is a domain, one of $x - t, x + t$ must be zero.

Chapter 18

Fields of Fractions

18.1 Subrings & Subfields

Proposition 18.1.1
If R is a subring of a field $\mathbb{K}$, then R is a domain.

Lemma 18.1.2
Let $\mathbb{K}$ be a field containing $\mathbb{Z}$ as a subring. Then $\mathbb{K}$ contains $\mathbb{Q}$ as a subfield.

Proof
Let $\phi : \mathbb{Z} \to \mathbb{K}$ be the subgroup inclusion map. Define $\psi : \mathbb{Q} \to \mathbb{K}$ by

$$\frac{a}{b} \mapsto \phi(a)\phi(b)^{-1}.$$

This map is well defined since if $\frac{a}{b} = \frac{c}{d}$

$$\begin{aligned} \phi(a)\phi(d) &= \phi(ad) \\ &= \phi(bc) \\ &= \phi(b)\phi(c). \end{aligned}$$

Thus

$$\phi(a)\phi(b)^{-c} = \phi(c)\phi(d)^{-1}$$

as required.

ψ is also a ring homomorphism. Moreover, any map from a field is injective, so ψ is an injective homomorphism.

18.2 Localization

Our goal is to take a commutative ring R and make a ring of fractions $\frac{a}{b}$ with $a, b \in R$.

Definition 18.2.1 (Multiplicatively Closed)
We say a subset of a ring $S \subseteq R$ is multiplicatively closed if and only if

$$1 \in S$$

and

$$b, d \in S \implies bd \in S.$$

The idea is to restrict the denominator to a multiplicatively closed subset of R.

Theorem 18.2.1
Let R be a commutative ring and S a multiplicatively closed subset which does not include 0 or zero divisors.
There is a commutative ring Q and an injective homomorphism $\phi : R \to Q$ such that

$$\forall a \in S, \phi(a) \in Q^{\times}$$

and every element of Q is of the form

$$\phi(a)\phi(b)^{-1}$$

for some $a \in R, b \in S$.
Moreover, if $\psi : R \to T$ is a homomorphism such that

$$\forall x \in S, \psi(x) \in T^{\times}$$

then there is a homomorphism $\tilde{\psi} : Q \to T$ such that

$$\tilde{\psi} \circ \phi = \psi.$$

Proof
Let $Q_0 := \{(a, b) : a \in R, b \in S\}$. Say

$$(a, b) \sim (c, d) \iff ad = bc$$

Show $\sim$ is an Equivalence Relation

Define $Q := Q/\sim$ as the set of equivalence classes of $\sim$.

Furthermore define addition and multiplication

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$$

and

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Addition & Multiplication are Well-Defined

$(Q,+)$ is a an Abelian Group

Take $\frac{0}{1}$ to be the zero of Q.

$(Q,+,\cdot)$ is a Commutative Ring

Define $\phi : R \to Q$ given by

$$a \mapsto \frac{a}{1}.$$

ϕ is a Homomorphism

Elements of Q They are all in the form $\frac{a}{b}$ for $a \in R, b \in S$, with $\phi(a) = \frac{a}{1}$.

Suppose $\psi : R \to T$ is a homomorphism such that

$$\psi(a) \in T^\times$$

for all $a \in S$.

We might as well assume T is commutative since $\operatorname{Im}\psi \cong R/\ker\phi$ is commutative.

Define $\tilde{\psi} : Q \to T$ with

$$\frac{a}{b} \mapsto \psi(a)\psi(b)^{-1}.$$

$\tilde{\psi}$ is Well-Defined

$\tilde{\psi}$ is a Homomorphism

Corollary 18.2.1.1 (Uniqueness of Localization)
Let S be a multiplicatively closed subset of a ring R which does not contain 0 or zero divisors.
If $Q_i, \phi_i, i = 1, 2$ are commutative rings and injective homomorphisms satisfying localization, then there is an isomorphism $\alpha : Q_1 \to Q_2$ such that

$$\alpha \circ \phi_1 = \phi_2.$$

Proof
Observe that Q_2, ϕ_2 satisfies the second statement of localization, thus we can get $\alpha : Q_1 \to Q_2$ with

$$\alpha \circ \phi_1 = \phi_2.$$

Similarly, get $\beta Q_2 \to Q_1$ such that

$$\beta \circ \phi_2 = \phi_1.$$

They are inverses of each other and thus isomorphisms.

18.2.1 Uniqueness of Localization

Definition 18.2.2 (Localization)
The ring Q from the theorem is referred to as the localization of R at S and is denoted

$$S^{-1}R.$$

If we leave out the requirement that every element of Q is of the form

$$\phi(a)\phi(b)^{-1}$$

then we no longer have uniqueness.

Consider $Q, Q[x]$.

18.3 Fields of Fractions

Definition 18.3.1 (Field of Fractions)
Let R be an integral domain and $S = R \setminus \{0\}$.
Then $S^{-1}R$ is the field of fractions of R.

Theorem 18.3.1
A ring R is an integral domain if and only if it is isomorphic to a subring of a field.

Proof
We know every subring of a field is an integral domain.

Conversely, every domain is a subring of its field of fractions.

18.3.1 Examples of Fields of Fractions

Lemma 18.3.2
The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$.

Rational Functions

Definition 18.3.2 (Rational Functions)
Let R be a domain.
The field of fractions of $R[x]$ is denoted by $R(x)$ and is called the field of rational functions over R.

Lemma 18.3.3
Let Q be the field of fractions of a domain R.
Then

$$Q(x) = R(x).$$

Proof
$R[x]$ is a subring of $Q[x]$. There is a homomorphism $\phi : R[x] \to Q[x]$.

Consider the inclusion homomorphism $R(x) \to Q(x)$. Since $R(x)$ is a field, this homomorphism is injective.

But $R(x)$ contains $\frac{a}{b}$ for any $a, b \in R, b \neq 0$. So the homomorphism is actually onto.

Thus for rational functions, we can assume the coefficients form a field.

let $\mathbb{K}$ be a field. Why do we call fractions of polynomials rational functions?

Definition 18.3.3
The domain $D(F)$ of $F \in \mathbb{K}(x)$ is the set of points $c \in \mathbb{K}$ such that

$$F = \frac{f(x)}{g(x)}$$

for some $f, g \in \mathbb{K}[x]$ where $g(c) \neq 0$.

We can actually $g(c) = 0$ but

$$c \in D(f/g).$$

Lemma 18.3.4
$F \in \mathbb{K}[x]$ defines a function $D(F) \to \mathbb{K}$ given by

$$c \mapsto \frac{f(c)}{g(c)}$$

where $f, g \in \mathbb{K}[x]$ are chosen so that $F = \frac{f}{g}$ and $g(c) \neq 0$.

Lemma 18.3.5
Let $\mathbb{K}$ be a field and $c \in \mathbb{K}$.
Then

$$R(c) = \{F \in \mathbb{K}(x) : c \in D(F)\}$$

is a subring of $\mathbb{K}(x)$.

18.3.2 Localization at a Prime Ideal

If R is a domain, then $R \setminus \{0\}$ is multiplicatively closed.

Lemma 18.3.6
Let $\mathcal{P}$ be an ideal of a commutative ring.
Then $R \setminus \mathcal{P}$ is multiplicatively closed if and only if $\mathcal{P}$ is prime.

Definition 18.3.4
Let $\mathcal{P}$ be a prime ideal of a domain R.
The localization of R at $\mathcal{P}$ is the ring

$$R_{\mathcal{P}} := S^{-1}R$$

where $S = R \setminus \mathcal{P}$.

Chapter 19

Chinese Remainder Theorem

19.1 Product Ideals

Definition 19.1.1 (Product Ideal)
Let $\mathcal{I}, \mathcal{J}$ be ideals in a ring R.
The product ideal is

$$\mathcal{I}\mathcal{J} := (ab : a \in \mathcal{I}, b \in \mathcal{J})$$

the ideal generated by products of elements from $\mathcal{I}, \mathcal{J}$.

19.1.1 Basic Properties

Lemma 19.1.1
Let $\mathcal{I}, \mathcal{J}$ be ideals in a ring R.
Then

$$\mathcal{I}\mathcal{J} = \left\{ \sum_{i=1}^{k} a_i b_i : k \geq 0, a_i \in \mathcal{I}, b_i \in \mathcal{J} \right\} =: K.$$

Moreover, if R is commutative and $\mathcal{I} = (S), \mathcal{J} = (T)$, then

$$\mathcal{I}\mathcal{J} = (ab : a \in S, b \in T) =: L.$$

Proof
If $x \in K$ then $-x \in K$ and K is closed under addition, so K is a subgroup.

If $r, s \in R$ and

$$x = \sum_{i=1}^{k} a_i b_i \in K$$

for $a_i \in \mathcal{I}, b_i \in \mathcal{J}$, then

$$rxs = \sum_{i=1}^{k} (ra_i)(b_i s) \in K$$

since $ra_i \in \mathcal{I}, b_i s \in \mathcal{J}$.

So K is an ideal containing the generating set for $\mathcal{I}, \mathcal{J}$ and is contained in $\mathcal{I}\mathcal{J}$, so we have

$$\mathcal{I}\mathcal{J} = K.$$

To see the second statement, note that $L \subseteq \mathcal{I}\mathcal{J}$ so we only need to show the reverse inclusion.

Suppose $x \in \mathcal{I}, y \in \mathcal{J}$. Then

$$x = \sum a_i s_i$$

for $a_i \in R, s_i \in S$ and

$$y = \sum b_i t_i$$

where $b_i \in R, t_i \in T$.

Thus

$$xy = \sum_{i,j} a_i b_j s_i t_j \in L.$$

Since L contains the generators of $\mathcal{I}\mathcal{J}$, it contains $\mathcal{I}, \mathcal{J}$.

19.1.2 Products & Intersections

Lemma 19.1.2
Let $\mathcal{I}, \mathcal{J}$ be ideals of the ring R. Then

$$\mathcal{I}\mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J}.$$

Proof
If $a \in \mathcal{I}, b \in \mathcal{J}$, then $ab \in \mathcal{I} \cap \mathcal{J}$.

Thus $\mathcal{I} \cap \mathcal{J}$ contains a generating set for $\mathcal{I}\mathcal{J}$. But $\mathcal{I}\mathcal{J}$ is an ideal. This shows the claim.

Note that the inclusion need not be strict.

19.2 Chinese Remainder Theorem

Recall from group theory that

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

This is the algebraic statement of the Chinese Remainder Theorem.

Recall that for $m, n \in \mathbb{Z}$

$$\gcd(m, n) = 1 \iff \operatorname{lcm}(m, n) = mn.$$

Lemma 19.2.1
Suppose $\operatorname{lcm}(m, n) = k$ for $k \geq 0$. Then

$$(m) \cap (n) = (k).$$

Let $\mathcal{I}, \mathcal{J}$ be ideals in R. Do we get a map $R/\mathcal{I}\mathcal{J} \to R/\mathcal{I} \times R/\mathcal{J}$ given by

$$\bar{r} \mapsto (\bar{r}, \bar{r})?$$

Lemma 19.2.2
If $\mathcal{I}, \mathcal{J}$ are ideals in a ring R and

$$\phi = q_1 \times q_2 : R \to R/\mathcal{I} \times R/\mathcal{J}$$

where q_1, q_2 are the quotient maps, then

$$\ker \phi = \mathcal{I} \cap \mathcal{J}.$$

Consequently, there is a homomorphism $\psi : R/\mathcal{I}\mathcal{J} \to R/\mathcal{I} \times R/\mathcal{J}$ such that

$$\psi(\bar{x}) = (q_1(x), q_2(x))$$

and

$$\ker \psi = \mathcal{I} \cap \mathcal{J}/\mathcal{I}\mathcal{J}.$$

Proof
Since $\mathcal{I}\mathcal{J} \subseteq \mathcal{I} \cap \mathcal{J} = \ker \phi$, the universal property of quotient rings apply.

19.3 Comaximal Ideals

Lemma 19.3.1
$\gcd(m, n) = 1$ if and only if
$$(m) + (n) = \mathbb{Z}.$$

Definition 19.3.1 (Comaximal)
Two ideals $\mathcal{I}, \mathcal{J}$ of ring R are comaximal (coprime) if
$$\mathcal{I} + \mathcal{J} = R$$
or
$$1 \in \mathcal{I} + \mathcal{J}.$$

19.4 Generalized Chinese Remainder Theorem

Theorem 19.4.1 (Generalized Chinese Remainder)
If $\mathcal{I}, \mathcal{J}$ are comaximal in a commutative ring R, then
$$\phi : R/\mathcal{I}\mathcal{J} \to R/\mathcal{I} \times R\mathcal{J}$$
given by
$$\bar{r} \mapsto (\bar{r}, \bar{r})$$
is an isomorphism.

Proof
Suppose $a \in \mathcal{I}, b \in \mathcal{J}$ such that
$$a + b = 1.$$

ϕ is Surjective

ϕ is Injective

Lemma 19.4.2
If $\mathcal{I}, \mathcal{J}, \mathcal{K}$ are ideals of R such that $\mathcal{I}, \mathcal{J}$ and $\mathcal{I}, \mathcal{K}$ are comaximal.
Then $\mathcal{I}$ and $\mathcal{J}\mathcal{K}$ are comaximal.

Theorem 19.4.3 (Extended Generalized Chinese Remainder)
Suppose

$$\mathcal{I}_1, \ldots, \mathcal{I}_k, k \geq 2$$

are ideals of a commutative ring R such that they are pairwise comaximal. There is an isomorphism

$$\phi : R/\mathcal{I}_1 \ldots \mathcal{I}_k \to R/\mathcal{I}_1 \times \cdots \times R/\mathcal{I}_k$$

defined by

$$\phi(\bar{r}) = (\bar{r}, \ldots, \bar{r}).$$

Proof
Induction on k.

Chapter 20

Domains

20.1 Principle Ideal Domains

20.1.1 Greatest Common Divisors

Divisors

Definition 20.1.1 (Divide)
Let R be a commutative ring.
An element $x \in R$ divides $y \in R$ if

$$y = xr$$

for some $r \in R$.

Observe the equivalent definition that $y \in Rx$. We write

$$x|y$$

to denote x divides y.

Proposition 20.1.1

(i) If $x|y$ then $x|yz$ for all $z \in R$

(ii) Every $x \in R$ divides 0 by definition

(iii) $u|1$ if and only if $u \in R^\times$

(iv) If $u \in R^\times$, then $x = u(u^{-1}x)$ for all $x \in R$

(v) $x = x \cdot 1$ thus $x|x$ for all $x \in R$

Proposition 20.1.2
Suppose $x, y \in R$ and $u \in R^\times$.
If $y = rx$ then

$$y = ru^{-1}(ux)$$

so $ux|y$.
In particular, $ux|x$ and

$$x = u^{-1}(ux)|ux$$

for all units $u \in R^\times$.

Associates

Definition 20.1.2 (Associates)
Two elements x, y of a commutative ring R are associates if $y = ux$ for some $u \in R^\times$.

We write

$$x \sim y$$

if x, y are associates.

Lemma 20.1.3
Let R be a commutative ring.

(a) $\sim$ is an equivalence relation

(b) If $x_1 \sim x_2$ and $y_2 \sim y_2$ then $x_1|y_2 \iff x_2|y_2$

(c) If $x \sim y$ then $x|y$ and $y|x$

Lemma 20.1.4
If R is a commutative ring, then

$$x|y \wedge y|x \iff (x) = (y).$$

Proof
We have

$$x|y \iff y \in (x) \iff (y) \subseteq (x)$$

and similarly for $y|x$.

Lemma 20.1.5
If R is a domain, then for all $x, y \in R$

$$x \sim y \iff x|y, y|x.$$

Proof
We know that if $x \sim y$, then $x|y, y|x$.

Conversely, suppose

$$y = xr, x = yt$$

for $r, t \in R$.

If $y = 0$, then $x = 0$ and $x \sim y$. Thus we may suppose $y \neq 0$.

Since

$$y = xr = yrt$$

then $(1 - rt)y = 0$.

Since $y \neq 0$ and R is a domain

$$1 - rt = 0 \implies r, t \in R^\times.$$

Greatest Common Divisor

Definition 20.1.3 (Common Divisor)
Let R be a commutative ring and $a, b \in R$.
$d \in R$ is a common divisor of a, b if

$$d|a, d|b.$$

Lemma 20.1.6
Let $d, a, b \in R$, where R is a commutative ring.
The following are equivalent.

(a) $d \mid a, d \mid b$

(b) $d \mid xa + yb$ for all $x, y \in R$

(c) $(a, b) \subseteq (d)$

Proof
<u>(1) $\iff$ (2)</u> If $a = dr, b = dt$ then

$$xa + yb = (xr + yt)d.$$

Conversely set $x = 1, y = 0$ and $x = 0, y = 1$.

<u>(2) $\iff$ (3)</u> Every element of (a, b) is for the form

$$xa + yb$$

for some $x, y \in R$ and

$$d \mid xa + yb \iff xa + yb \in (d).$$

Definition 20.1.4 (Greatest Common Divisor)
A common divisor d is a greatest common divisor if $d' \in R$ is a common divisor of a, b implies

$$d'|d.$$

We write

$$d = \gcd(x, y)$$

to mean that d is a greatest common divisor of x, y.

Proposition 20.1.7
If a, b have 0 as a common divisor, then

$$a = b = 0.$$

It follows that

$$\gcd(a, b) = 0 \iff a = b = 0.$$

Proposition 20.1.8
Every common divisor of $x \in R, u \in R^\times$ is a unit. Since units divide every element

$$v = \gcd(x, y)$$

for all $v \in R\times$.

Proposition 20.1.9
If d, d' are both gcd's of $x, y \in R$, then

$$d \mid d', d' \mid d.$$

Hence if R is a domain, then

$$d \sim d'$$

By a previous lemma.

Remark that if $d = \gcd(x, y)$ and $d \sim d'$ then

$$d' = \gcd(x, y).$$

The above shows that the gcd in integral domains is unique up to units.

Proposition 20.1.10
Let a, b be elements of a commutative ring R. Then a, b have a greatest common divisor if and only if there is a principle ideal $\mathcal{I}$ such that

$$(a, b) \subseteq \mathcal{I}$$

and for all principle ideals $\mathcal{J}$

$$(a, b) \subseteq \mathcal{J} \implies \mathcal{I} \subseteq \mathcal{J}.$$

Moreover, if $\mathcal{I}$ exists, it is unique with

$$\mathcal{I} = (d) \iff d = \gcd(a, b).$$

Proof
We already know that $d' = \gcd(a, b)$ if and only if $(a, b) \subseteq (d')$. Thus

$$d = \gcd(a, b) \iff \mathcal{I} := (d)$$

satisfies conditions (a), (b).

If $\mathcal{I}, \mathcal{I}'$ both satisfy conditions (a), (b), they contain each other and are thus equal. Combining uniqueness with our work above

$$\mathcal{I} = (d) \iff d = \gcd(a, b).$$

Corollary 20.1.10.1
Let $a, b \in R$ commutative ring. If (a, b) is a principle ideal, then a gcd of a, b exists. Consequently, if d is a common divisor of a, b such that

$$d = xa + yb$$

for some $x, y \in R$ then

$$d = \gcd(a, b).$$

Proof
If $(a, b) = (d)$ then

$$\mathcal{I} = (d)$$

satisfies (a), (b).

If d is a common divisor of a, b, then

$$(a, b) \subseteq (d)$$

and if

$$d = xa + yb$$

then

$$d \in (a, b).$$

It follows that

$$(d) = (a, b).$$

Corollary 20.1.10.2
Let $a, b \in R$ commutative ring and suppose that

$$(a), (b)$$

are comaximal.
then

$$1 = \gcd(a, b).$$

Proof
$(a) + (b) = (a)$.

For example, every ideal is principle in $\mathbb{Z}$, thus gcd's always exist.

20.1.2 Principle Ideal Domains

Definition 20.1.5 (Principle Ideal Domain)
A integral domain R is a principle ideal domain if every ideal of R is principle.

Proposition 20.1.11
If R is a PID, every pair of elements $a, b \in R$ has a gcd.
Moreover

$$d = \gcd(amb) \iff d \mid a, b, d = xa + yb.$$

Proposition 20.1.12
If R is a PID, then every non-zero prime ideal of R is maximal.

Proof
All ideals are of the form (a). Suppose (a) is a prime ideal satisfying $(a) \subsetneq (b)$ so that

$$a = br \in (a)$$

Since (a) is prime either $b \in (a)$, in which case $(b) \subsetneq (a)$ which is what we want or

$$r \in (a).$$

In particular, $(r) \subsetneq (a)$. Coupled with $a = br \subsetneq (r)$, we have equality.

But R is a domain, thus $a \sim r$ and

$$a = ur$$

for some $r \in R^\times$.

We can write

$$br = a = ur \implies (b - u)r = 0.$$

Since (a) is non-zero, $r \neq 0$ and the absence of zero divisors imply

$$b = u.$$

This implies $(b) = (a)$.

Having considered both cases, (a) is maximal by definition.

Corollary 20.1.12.1
If R is a commutative ring such that

$$R[x]$$

is PID, then R MUST be a field.

Proof
If $R[x]$ is a PID, the it is a domain.

As a subring of $R[x]$, R must also be a domain.

Since

$$R \cong R[x]/(x),$$

(x) is prime. But then (x) is maximal by the proposition and R is a field.

20.2 Euclidean Domains

Definition 20.2.1 (Euclidean Domain)
A domain R is Euclidean if there is a function $N : R \to \mathbb{N} \cup \{0\}$ such that $N(0) = 0$ and for all $x, y \in R$ with $x \neq 0$, there is $q, r \in R$ such that

$$y = qx + r.$$

Moreover, either

$$r = 0 \vee N(r) < N(x).$$

It is possible to have norms with $N(x) = 0$ but $x \neq 0$. However, if $N(x) = 0$ then

$$1 = qx + r$$

with r necessarily being 0. So $x \mid 1$ and x is a unit.

Proposition 20.2.1
A Euclidean domain R is a PID.

Proof
Suppose $\mathcal{I}$ is an ideal of R. If $\mathcal{I}$ is zero, then it is certainly principle. Thus suppose $\mathcal{I} \neq (0)$.

Define

$$k := \min\{N(x) : x \in \mathcal{I}, x \neq 0\}$$

and choose $x \in \mathcal{I}$ such that

$$N(x) = k.$$

Suppose $y \in \mathcal{I}$. We have

$$y = qx + r$$

for $q, r \in R$.

Since

$$r = y - qx \in \mathcal{I}$$

we cannot have $N(r) < N(x)$. So $r = 0$.

It follows that

$$\mathcal{I} \subseteq (x).$$

But $x \in \mathcal{I}$ so

$$\mathcal{I} = (x).$$

Proposition 20.2.2
Let $\mathbb{K}$ be a field. Then

$$\mathbb{K}[x]$$

is a Euclidean domain.

Proof
Define

$$N : \mathbb{K}[x] \to \mathbb{N} \cup \{0\}$$

by

$$N(p) = \deg(p)$$

for $p \neq 0$ and $N(0) = 0$.

Suppose $y, p \in \mathbb{K}[x]$ with $p \neq 0$. If $\deg(p) = 0$, then p is a unit and

$$y = qp + 0$$

for some $q \in \mathbb{K}[x]$.

If $\deg(p) > 0$, we can divide by y by p to get

$$y = qp + r$$

for $q, r \in \mathbb{K}[x]$ with $\deg(r) < \deg(p)$.

In both cases

$$y = qp + r$$

with $q, r \in \mathbb{K}[x]$ and

$$r = 0 \vee N(r) < N(p).$$

Corollary 20.2.2.1
$\mathbb{K}[x]$ is a PID.

There are PIDs which are not Euclidean, for example

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right].$$

In PIDs, gcd's always exist. In Euclidean domains, there is an efficient algorithm to compute it.

20.3 Unique Factorization Domains

20.3.1 Primes & Irreducibles

Can we generalize prime numbers to arbitrary domains?

Let R be a domain and $p \in R$.

Definition 20.3.1 (Prime)
p is prime if $p \neq 0$ and for all $a, b \in R$

$$p \mid ab \implies p \mid a \vee p \mid b.$$

Definition 20.3.2 (Irreducible)
p is irreducible if p is not zero or a unit and for all $a, b \in R$

$$p = ab \implies a \in R^\times \vee b \in R^\times.$$

Let R be a domain.

Proposition 20.3.1
$p \in R$ is prime if and only if $p \neq 0$ and

$$(p)$$

is a prime ideal.

Proof
Use the fact that

$$p \mid m \iff m \in (p).$$

Proposition 20.3.2
If p, p' are associates, then p is prime/irreducible if and only if p' is prime/irreducible.

Proposition 20.3.3
If p is prime, then p is irreducible.

Proof
Suppose p is prime and $p = ab$

Then $p \mid ab$ thus $p \mid a$ or $p \mid b$.

Suppose $p \mid a$, then $a = up$ and

$$0 = p - ab = p(1 - ub).$$

Since R is a domain and $p \neq 0$

$$ub = 1$$

thus $b \in R^\times$.

The case for $p \mid b$ is analogous.

Proposition 20.3.4
Let p be an irreducible in a PID R.
Then p is prime.

Proof
Suppose $\mathcal{I}$ is an ideal of R containing (p). Since R is a PID,

$$\mathcal{I} = (q)$$

for some $q \in R$.

Since $p \in \mathcal{I}$, we can write

$$p = kq$$

for some $k \in R$.

Since p is irreducible, either k or q is a unit. If q is a unit, then

$$\mathcal{I} = R.$$

If k is a unit, then p, q are associates and

$$(p) = (q).$$

Thus (p) is maximal and hence a prime ideal. Since $p \neq 0$ by definition, p is prime.

20.3.2 Complete Factorizations

Let R be a domain.

Definition 20.3.3 (Complete Factorization)
We say $r \in R$ has a complete factorization into irreducibles if and only if

$$r = r_1 \dots r_k$$

for some $k \geq 1$ and each r_i is irreducible.

Definition 20.3.4 (Complete Factorization)
We say that R has complete factorizations (into irreducibles) if and only if every $r \in R \setminus R^\times \cup \{0\}$ has a complete factorization into irreducibles.

Lemma 20.3.5
If $r \in R$ is irreducible and a product of primes, then r is prime.

Proof
Suppose r is irreducible with

$$r = p_1 \dots p_k$$

for primes p_i.

If r is irreducible and $k \geq 2$, then either $(p_1 \dots p_{k-1})$ or p_k is a unit.

The latter cannot be a unit since it is prime. If the former is a unit with inverse q, then

$$p_1(p_2 \dots p_{k-1} q) = 1$$

so p_1 divides 1 and is a unit. Since primes cannot be units, we get a contradiction.

Thus $k = 1$ and r is prime.

Corollary 20.3.5.1
If R has complete factorizations into irreducibles, then R has complete factorizations into primes if and only if every irreducible in R is prime.

We know primes are irreducibles thus we can define complete factorization into primes similarly. Notice since primes are irreducibles, we get a strictly stronger definition. However, we do not know whether irreducibles are always prime, so we stick with the current condition.

Lemma 20.3.6
Let
$$r = r_1 r_2 \in R$$
where R is a domain so
$$(r) \subseteq (r_2).$$
If $r \neq 0$, then $(r) = (r_2)$ if and only if r_1 is a unit.

Proof
We know $(r) = (r_2)$ if and only if they are associates.

If r_1 is a unit then $(r) = (r_2)$.

Conversely if $(r) = (r_2)$, then $r = ur_2$ for a unit u. So
$$(r_1 - u)r_2 = 0.$$
Since $r, r_2 \neq 0$ it must be that
$$r_1 = u$$
is a unit.

Thus if r is reducible, then $r = r_1 r_2$ where
$$(r) \subsetneq (r_1), (r_2).$$
Repeatedly factoring does not terminate only if there is an infinite strictly increasing sequence of principle ideals
$$(r) \subsetneq (r_1) \subsetneq \dots.$$

Ascending Chain Condition

Definition 20.3.5 (Ascending Chain Condition for Principle Ideals)
We say R satisfies the ascending chain condition for principal ideals if there is no infinite strictly increasing sequence
$$\mathcal{I}_1 \subsetneq \mathcal{I}_2 \subsetneq \dots$$
of principal ideals in R.

Proposition 20.3.7
If R satisfies the ascending chain condition for principle ideals, then R has complete factorizations into irreducibles.

Proposition 20.3.8
If R is a PID, then R satisfies the ascending chain condition for principle ideals.

Proof
Suppose

$$\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \dots$$

is an increasing sequence of ideals.

Then

$$\mathcal{I} := \cup \mathcal{I}_i$$

is an ideal. Since R is a PID, $\mathcal{I} = (x)$ for some $x \in R$.

But $x \in \mathcal{I}$ so $x \in \mathcal{I}_k$ for some k. Thus

$$\mathcal{I}_k \subseteq \mathcal{I}_n = (x) \subseteq \mathcal{I}_k$$

for all $n \geq k$ and

$$\mathcal{I}_n = \mathcal{I}_k$$

for $n \geq k$.

20.3.3 Unique Factorizations

Definition 20.3.6 (Unique Factorization)
Let R be a domain. We say that complete factorizations are unique when they exist if for every two sequences of irreducibles

$$f_1 \dots f_n = g_1 \dots g_m$$

implies $n = m$ and there is a permutation σ such that

$$f_i \sim g_{\sigma(i)}$$

for all $1 \leq i \leq n$ (ie differ by a unit).

Lemma 20.3.9
If $f_1, \dots, f_n$ are irreducibles in a domain R for $n \geq 1$, then

$$f_1 \dots f_n \notin R^\times.$$

Proof
By contradiction. Show that one of f_i's are a unit otherwise.

Proposition 20.3.10
Let R be a domain such that every irreducible in R is prime. Then complete factorizations are unique when they exist.

Proof
Same as that for $\mathbb{Z}$.

20.3.4 Unique Factorization Domain

Definition 20.3.7 (Unique Factorization Domain)
A domain R is a unique factorization domain if R has complete factorizations into irreducibles and complete factorizations are unique when they exist.

Thus R is a UFD if every $r \in R \setminus R^\times \cup \{0\}$ is a product of irreducibles in R. In addition, if f_i, g_j are irreducibles such that

$$f_1 \dots f_n = g_1 \dots g_m$$

then $n = m$ and there is a permutation $\sigma \in S_n$ such that

$$f_i \sim g_{\sigma(i)}.$$

Proposition 20.3.11
PIDs are UFDs. In particular, Euclidean domains are UFDs.

If R is a UFD and

$$x \notin R^\times \cup \{0\}$$

we refer to the factorization of x into irreducibles as the prime factorization of x.

Lemma 20.3.12
Suppose R is a UFD and $a, b \in R$ are non-zero non-units. If $a \mid b$, then the number of factors in the prime factorization of a is at most the number of factors in the prime factorization of b. Moreover, equality holds if and only if

$$(a) = (b).$$

Theorem 20.3.13
Let R be a domain. R is a UFD if and only if R satisfies the ascending chain condition for principle ideals and every irreducible in R is prime.

Proof
We have already shown that the ascending chain condition for principle ideals implies the existence of a complete factorization. Moreover, the equivalence of irreducibles and primes shows that the factorization is unique.

Now suppose R is a UFD.

Irreducibles in R are Prime

R Satisfies the Ascending Chain Condition for Principle Ideals

Theorem 20.3.14
Let R be a UFD. Then $R[x]$ is a UFD.

20.3.5 Greatest Common Denominators in Unique Factorization Domains

Let R be a UFD.

Proposition 20.3.15
If $0 \neq x \in R$, there is $u \in R^\times$ and irreducibles $g_1, \dots, g_n, n \geq 0$ such that $g_i \not\sim g_j$ for $i \neq j$ where

$$x = u \prod_{i=1}^{n} g_i^{a_i}$$

for $a_i \in \mathbb{Z}^+$.

Proposition 20.3.16
Suppose $u, v \in R^\times$, and the irreducibles $g_1, \dots, g_n, n \geq 0$ are such that $g_i \not\sim g_j$ for $i \neq j$ where

$$u \prod_{i=1}^{n} g_i^{a_i} = v \prod_{i=1}^{n} g_i^{b_i}$$

for $a_i, b_j \in \mathbb{Z}^+$.
Then

$$u = v, a_i = b_i, i \in [n]$$

Proposition 20.3.17
Suppose

$$x = u \prod_{i=1}^{n} g_i^{a_i}$$

for $a_i \in \mathbb{Z}^+, u \in R^\times$ and irreducibles $g_1, \ldots, g_n, n \geq 0$ such that $g_i \not\sim g_j$ for $i \neq j$. Then $y \mid x$ if and only if

$$y = v \prod_{i=1}^{n} g_i^{b_i}$$

for $v \in R^\times$ and $0 \leq b_i \leq a_i, i \in [n]$.

Proposition 20.3.18
If $0 \neq x, y \in R$, there is $u, v \in R^\times$ and irreducibles $g_1, \ldots, g_n, n \geq 0$ such that $g_i \not\sim g_j$ for $i \neq j$ where

$$x = u \prod_{i=1}^{n} g_i^{a_i}$$

$$y = u \prod_{i=1}^{n} g_i^{b_i}$$

for $a_i \geq 0, b_i \geq 0$.

Note the importance here where we relax the conditions for powers of g_i.

Definition 20.3.8 (Division in a Domain)
If R is a domain with

$$a = kb = k'b$$

then

$$(k - k')b = 0 \implies k = k'.$$

Thus we can let

$$\frac{a}{b}$$

denote the unique element such that $a = bk$.

Proposition 20.3.19
Suppose R is a UFD, $u, v \in R^\times$, and $g_1, \dots, g_n$ are primes in R such that $g_i \not\sim g_j$ for $i \neq j$, and $a_1, \dots a_n, b_1, \dots, b_m \geq 0$.
Put $c_i := \min(a_i, b_i)$. We have

$$\prod_{i=1}^n g_i^{c_i} = \gcd\left(u \prod_{i=1}^n g_i^{a_i}, v \prod_{i=1}^n g_i^{b_i}\right).$$

20.4 Summary of Greatest Common Denominators

20.4.1 Euclidean Domains

The GCD always exists. It is computable from prime factorization as well as the Euclidean algorithm. There are $x, y \in R$ such that

$$\gcd(a, b) = xa + yb.$$

20.4.2 Principal Ideal Domain

The GCD always exists. It is computable from prime factorization. There are $x, y \in R$ such that

$$\gcd(a, b) = xa + yb.$$

20.4.3 Unique Factorization Domain

The GCD always exists. It is computable from prime factorization.

20.5 Unique Factorization in Polynomial Rings

Our goal is to show that $R[x]$ is a UFD given that R is a UFD.

20.5.1 Irreducibles

Recall that

$$\mathbb{K}[x]^\times = \mathbb{K}^\times.$$

Lemma 20.5.1
Let $\mathbb{K}$ be a field.
$f \in \mathbb{K}[x]$ is irreducible if and only if $\deg f \geq 1$ and

$$f \neq gh$$

for $\deg g, \deg h < \deg f$.

Proof
f is a non-unit if and only if $\deg f \geq 1$. If

$$0 \neq f = gh, \deg g = \deg f$$

then $\deg h = 0$ so $h \in \mathbb{K}^\times$.

If $\deg f \geq 1$, then f is reducible if and only if $f = gh$ with

$$\deg g, \deg h < \deg f.$$

Roots & Reducibility

Let R be a domain and suppose $c \in R$. We know

$$\ker \mathrm{ev}_c = (x - c) \subseteq R[x].$$

Equivalently

$$(x - c) \mid f(x) \in R[x] \iff f(c) = 0.$$

Lemma 20.5.2
Let $f \in R[x]$ and $\deg f \geq 2$.
If f has a root in R, then f is reducible.

Proof
If $f(c) = 0$, then

$$f = (x - c)g(x)$$

for some $g(x)$.

Since $\deg f \geq 2$

$$\deg g = \deg f - 1 \geq 1.$$

Thus $x - c, g \notin R[x]^\times$ and f is reducible.

Theorem 20.5.3 (Fundamental Theorem of Algebra)
Every non-constant polynomial in $\mathbb{C}[x]$ has a root.

Corollary 20.5.3.1
The irreducibles in $\mathbb{C}[x]$ are polynomials of the form

$$ax + b$$

for $a, b \in \mathbb{C}$ with $a \neq 0$.

Corollary 20.5.3.2
$f \in \mathbb{R}[x]$ is irreducible if and only if

$$\deg f \in \{1, 2\}$$

and f does not have a root in $\mathbb{R}$.

Proof
If $\deg f = 1$ we are done.

If $\deg f = 2$ then f is a product of two lower degree polynomials if and only $f(c) = 0$ for some $c \in \mathbb{R}$.

Suppose $\deg f \geq 3$. If f has a root in $\mathbb{R}$, then f is reducible. Otherwise, suppose f has no root in $\mathbb{R}$.

By the FTA, f has root $c \in \mathbb{C} \setminus \mathbb{R}$. Since $f \in \mathbb{R}[x]$ and $f(c) = 0$

$$f(\bar{c}) = \overline{f(c)} = 0.$$

Thus

$$(x - c), (x - \bar{c}) \mid f$$

and

$$(x^2 - 2\operatorname{Re} c + |c|^2) \mid f$$

so f is reducible.

20.5.2 Gauss' Lemma

Recall that if R is a domain

$$R[x]^\times = R^\times.$$

Lemma 20.5.4
Let R be a domain.
Then $p \in R$ is irreducible in R if and only if p is irreducible in $R[x]$.

Proof
Clearly
$$p \notin R \setminus R^\times \cup \{0\} \iff p \notin R[x] \setminus R[x]^\times \cup \{0\}.$$

Suppose p is irreducible in $R[x]$, and
$$p = ab$$
for $a, b \in R$.

Then one of a, b must belong to $R[x]^\times = R[x]$. Thus p is irreducible in R.

Suppose p is irreducible in R, and
$$p = f(x)g(x).$$
Then either f or g is in $R^\times = R[x]^\times$.

Lemma 20.5.5
Let $p \in R$ where R is a domain. p is prime in R if and only if p is prime in $R[x]$.

Proof
It can be shown that if $\mathcal{I}$ is an ideal of R, and
$$\mathcal{J} := (\mathcal{I})$$
in $R[x]$, then
$$R[x]/\mathcal{J} \cong (R/\mathcal{I})[x].$$

Thus
$$\begin{aligned}\mathcal{I} \subseteq R \text{ is prime} &\iff R/\mathcal{I} \text{ is a domain}\\ &\iff (R/\mathcal{I})[x] \text{ is a domain}\\ &\iff \mathcal{J} \text{ is prime in } R[x]\end{aligned}$$

$$\begin{aligned}p \in R \text{ is prime} &\iff (p) \text{ is prime in } R\\ &\iff (p) \text{ is prime in } R[x]\\ &\iff p \text{ is prime in } R[x].\end{aligned}$$

Higher Degree Irreducibles

Lemma 20.5.6
$ax + b$ is irreducible if and only if

$$\gcd(a, b) = 1.$$

If

$$ax + b = f(x)g(x)$$

then one of f, g must be in R. Hence if $ax + b$ is reducible, there must be $d \in R$ such that

$$0 \neq d \notin R^\times, d \mid a, b.$$

Proof
$ax + b$ is irreducible if and only if the only common divisors of a, b are units.

Primitive Polynomials

Definition 20.5.1 (Primitive Polynomial)
Let R be a UFD. A non-zero polynomial

$$f \in R[x]$$

is primitive if there is no irreducible $r \in R$ such that

$$r \mid f.$$

If we extend GCD to more than two elements, another way to say this is $\sum_{i=1}^{n} a_i x^i$ is primitive if

$$1 = \gcd(a_0, \dots, a_n).$$

Lemma 20.5.7
Let R be a UFD and $0 \neq f \in R[x]$.
There is $d \in R$ such that

$$d \mid f$$

and $\frac{f}{d}$ is primitive.

Proof
Put $f = \sum_{i=0}^n a_i x^i$. We can take

$$d = \gcd(a_0, \ldots, a_n).$$

Lemma 20.5.8
Let R be a UFD. If $f \in R[x]$ is irreducible and $\deg f \geq 1$, then f is primitive.

Proof
Suppose $p \mid f$ where $p \in R$ is prime. Then

$$f = p \cdot \frac{f}{p}$$

where $p, \frac{f}{p}$ are not units, hence f is reducible.

Since non-primitive polynomials are reducible, irreducible polynomials are primitive.

Lemma 20.5.9
If R is a UFD and $f \in R[x]$ is primitive with $\deg f \geq 1$, then f is reducible if and only if

$$f = gh$$

for $g, h \in R[x]$ with

$$\deg g, \deg h < \deg f.$$

Proof
$(\implies)$ Suppose $f = gh$ with g, h being non-units.

If $\deg g = \deg f$, then $h \in R$. Since R is a UFD, there must be a prime $p \mid h$.

So $p \mid f$, contradicting the primitivity of f.

Thus $\deg g < \deg f$ and similarly for $\deg h$.

$(\impliedby)$ This is clear.

Gauss' Lemma

Lemma 20.5.10 (Gauss)
Let R be a UFD with its field of fraction $\mathbb{K}$. If $f \in R[x]$ and $f = gh$ for $g, h \in \mathbb{K}[x]$, then there is $u \in \mathbb{K}^\times$ such that

$$ug, u^{-1}h \in R[x].$$

Proof
We can "clear denominators" and pick $d_1, d_2 \in R$ such that

$$d_1 g, d_2 h \in R[x].$$

Let $d := d_1 d_2$ so

$$df = (d_1 g)(d_2 h).$$

If $d \in R^\times$, then we are done. Suppose otherwise.

Let

$$d = p_1 \dots p_n$$

be its prime factorization in R.

Since p_1 is prime in $R[x]$ and

$$p_1 \mid (d_1 g)(d_2 h)$$

we must have

$$p_1 \mid d_1 g \vee p_1 \mid d_2 h.$$

Without loss of generality, the first case occurs and

$$\frac{d_1}{p_1} g \in R[x].$$

We can repeat this argument to get

$$p_2 \mid \frac{d_1}{p_1} g \vee p_2 \mid d_2 h.$$

Repeating this argument for all $p_1, \dots, p_n$, we eventually arrive at

$$f = \left(\frac{d_1}{p_{i_1} \dots p_{i_k}} g \right) \left(\frac{d_2}{p_{j_1} \dots p_{j_m}} h \right)$$

where both factors are in $R[x]$.

Proposition 20.5.11
Let R be a UFD and $\mathbb{K}$ its field of fraction.
Suppose $f \in R[x]$ has $\deg f \geq 1$. Then f is irreducible in $R[x]$ if and only if f is primitive and f is irreducible in $\mathbb{K}[x]$.

Proof
($\implies$) If $f \in R[x]$ is reducible, then either f is not primitive or $f = gh$ with $g, h \in R[x]$ and

$$\deg g, \deg h < \deg f$$

implying that f is reducible in $\mathbb{K}[x]$.

($\impliedby$) If f is not primitive, then f is reducible.

Moreover, if f is reducible in $\mathbb{K}[x]$, then $f = gh$ for $g, h \in \mathbb{K}[x]$ with

$$\deg g, \deg h < \deg f.$$

By Gauss' lemma, we can find $u \in \mathbb{K}^\times$ such that

$$ug, u^{-1}h \in R[x].$$

Since $f = (ug)(u^{-1}h)$ and $\deg ug, \deg u^{-1}h < \deg f$, f is thus reducible.

20.5.3 Polynomial Rings

Lemma 20.5.12
Suppose R is a UFD with field of fractions $\mathbb{K}$ and $f \in R[x]$ is primitive.
If $u \in \mathbb{K}$ such that $uf \in R[x]$, then

$$u \in R.$$

Proof
Let $f = \sum_{i=0}^n a_i x^i$ and

$$u = \frac{c}{d}$$

for $c, d \in R$.

Then $\frac{a_i c}{d} \in R$ for all i, thus there is $b_i \in R$ such that

$$b_i d = a_i c.$$

It follows that $d \mid a_i$ for all i. If $d \notin R^\times$, then there is a prime in R dividing f, thus f is not primitive.

This is the desired contradiction. Thus

$$d \in R^\times \implies u = \frac{cd^{-1}}{1} \in R.$$

Theorem 20.5.13
If R is a UFD, then $R[x]$ is a UFD.

Proof
Suppose R is a UFD and let $\mathbb{K}$ be the field of fractions of R.

Irreducibles in $R[x]$ are prime

$R[x]$ has has the ascending chain condition for ideals

Proposition 20.5.14
$R[x]$ is a UFD if and only if R is a UFD.