PMATH347 Review Notes

University of Waterloo

The One And Only
Waterloo 76er
Bill Zhuo

Índice general

I Group Theory

1 Introduction to Groups 5
1.1 Basic Framework 5
1.2 Subgroups 6

2 Symmetric Groups & Dihedral Groups 9
2.1 Symmetric Groups 9
2.2 Dihedral Groups 11

3 Cosets & Quotient Groups 12
3.1 Cosets 12
3.2 Quotient Groups 13

4 Group Homomorphism 16
4.1 Group Homomorphism 16
4.2 First Isomorphism Theorem (76er) 18

5 Group Actions 20
5.1 Group Actions 20
5.2 Counting Applications 22
5.2.1 Class Equation 22
5.2.2 Burnside's Lemma 22
5.3 Finite Abelian Groups 23

II Ring Theory

6 Introduction to Rings 26
6.1 Rings 26
6.1.1 Subring 27
6.2 Integral Domain & Fields 28

7 Ring Homorphism 30
7.1 Ring Homorphism 30
7.2 Quotient Rings 31

8 Prime Ideal & Maximal Ideal 35
8.1 Prime Ideal & Maximal Ideal 35
8.2 Supportive Section: Set Theory 36

9 ED & PID & UFD 39
9.1 Euclidean Domain 39
9.2 Principal Ideal Domain 41
9.3 Unique Factorization Domain 43
9.5 PMATH347 Final Exam 46

III Assignment Section

10 Group Related Results 48

11 Ring Related Results 51

Group Theory

1 Introduction to Groups 5
1.1 Basic Framework
1.2 Subgroups

2 Symmetric Groups & Dihedral Groups . . 9
2.1 Symmetric Groups
2.2 Dihedral Groups

3 Cosets & Quotient Groups 12
3.1 Cosets
3.2 Quotient Groups

4 Group Homomorphism 16
4.1 Group Homomorphism
4.2 First Isomorphism Theorem (76er)

5 Group Actions 20
5.1 Group Actions
5.2 Counting Applications
5.3 Finite Abelian Groups

1. Introduction to Groups

1.1 Basic Framework

Definition 1.1.1 Group

A group is a set G equipped with a operation $\cdot$

$$\cdot : G \times G \to G$$

such that

1. **Associativity:** $\forall a,b,c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. **Identity:** $\exists e \in G$ such that $e \cdot g = g \cdot e, \forall g \in G$
3. **Inverses:** $\forall g \in G, \exists g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$, we call $g^{-1} \in G$ the inverse of g.

R If G is a group with $\cdot$, we write this as $(G, \cdot)$. If the operation is implicit, we will just write G.

■ **Example 1.1 Examples of Groups**

1. $(\mathbb{Q}, \cdot)$ is not a group since 0 is not invertible. But $(\mathbb{Q}^\times, \cdot), (\mathbb{R}^\times, \cdot), (\mathbb{C}^\times, \cdot), (\mathbb{Z}_p^\times, \cdot)$ are groups
2. $(\mathbb{Z}, +)$ is the integer additive group.
3. $(M_n(\mathbb{R}), +)$ is a group. But $(M_n(\mathbb{R}), \cdot)$ is not a group having inverse problems
4. $GL_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$. The general linear group $(GL_n(\mathbb{F}), \cdot)$ is a group, where $\mathbb{F}$ is any field.
5. $\mathscr{U}(n) = \{a \in \mathbb{Z}_n : \gcd(a,n) = 1\} = \{a \in \mathbb{Z}_n : \exists b \in \mathbb{Z}_n, ab = 1\}$, this is known as the group of units of $\mathbb{Z}$.

■

■ **Example 1.2** $C(\mathbb{R}) := \{f : \mathbb{R} \to \mathbb{R} : f \text{ is continuous}\}$

1. $(C(\mathbb{R}), +)$ ia group defined by

$$(f+g)(x) = f(x) + g(x)$$

2. $(C(\mathbb{R}),\circ)$ is not a group since $f(x)=x^2$ is not invertible defined by

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

3. $(C(\mathbb{R}),\cdot)$ is not a group since there exists $f(x)$ that has zero

$$(fg)(x)=f(x)g(x)$$

■

Proposition 1.1.1 Basic Properties of Group

1. The identity of G is unique
2. If $g\in G$, then $g^{-1}\in G$ is unique
3. If $g\in G$, then $(g^{-1})^{-1}=g$
4. If $a,b\in G$, then $(ab)^{-1}=b^{-1}a^{-1}$

Proposition 1.1.2 Left and Right Cancellation

Let G is a group and let $a,b,c\in G$, then

1. If $ab=ac$, then $b=c$
2. If $ba=ca$, then $b=c$

Definition 1.1.2 Special Groups

1. We say a group G is finite if $|G|<\infty$
2. We say a group G is abelian if $\forall a,b\in G$ that $ab=ba$
3. Let $(G,\cdot),(H,*)$ be two groups, we define the direct product by

$$G\times H:=\{(a,b):a\in G,b\in H\}$$

with the operation: $(a_1,b_1)\times(a_2,b_2)=(a_1\cdot a_2,b_1*b_2)$ This is a group.

■ **Example 1.3**

1. $GL_2(\mathbb{Z}_3)$ is finite and non-abelian
2. $G=\mathbb{R}^\times\times\mathbb{Z}_{12}$ with $e=(1,0)$ is a direct product of groups
3. $(V,+,\cdot)$ is a vector space and $(V,+)$ is an abelian group

■

R If $A_1,A_2,\ldots$ is a list of groups, we can define $A_1\times A_2\times\ldots$.

1.2 Subgroups

Definition 1.2.1 Subgroup

Let $(G,\cdot)$ be a group, we say $H\subseteq G$ is a subgroup of G if $(H,\cdot)$ forms a group. If H is a subgroup of G and we write $H\leq G$.

Theorem 1.2.1 Subgroup Test
Let G be a group, if $\emptyset \neq H \subseteq G$, then

$$H \leq G \iff \forall a,b \in H, ab^{-1} \in H$$

■ **Example 1.4 Examples of Subgroups**

1. For every group G, we have $\{e\}$ is the trivial subgroup and G is the largest subgroup
2. $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ where p, then the special linear group $SL_n(F) := \{A \in GL_n(F) : \det A = 1\}$. We know that
$$SL_n(F) \leq GL_n(F)$$
3. $G = \mathbb{Z}$ and $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ and $n\mathbb{Z} \leq \mathbb{Z}$.
4. $H_n := \{z \in \mathbb{C} : z^n = 1\}$ and $S^1 := \{z \in \mathbb{C} : |z| = 1\}$ and $H_n \leq \mathbb{C}^\times, S^1 \leq \mathbb{C}^\times$
5. G_1, G_2 are groups and $H_1 \leq G_1, H_2 \leq G_2$, then $H_1 \times H_2 \leq G_1 \times G_2$.
6. **Warning:** it is not true that every subgroup of $\mathbb{Z} \times \mathbb{Z}$ of the form $H_1 \times H_2$ where $H_1, H_2 \leq \mathbb{Z}$ since we have the counterexample
$$D = \{(a,a) : a \in \mathbb{Z}\} \neq \mathbb{Z} \times \mathbb{Z}$$
7. $H = \{-1, 0, 1\} \subseteq \mathbb{Z}$ but it is not a subgroup since $1 + 1 = 2 \notin H$.

■

Definition 1.2.2 Centre of A Group $Z(G)$
Let G be a group the centre of a group is defined as $Z(G) = \{g \in G : gx = xg, \forall x \in G\}$
We know that $Z(G) \leq G$ and in fact it is normal in G and always exists.

Definition 1.2.3 Order of A Group
Let G be a group, for $g \in G$, we define the order of g, $|g|$ to be the least $n \in \mathbb{N}$ such that $g^n = e$.
If no such n exists, we say g has infinite order $|g| = \infty$.

R

1. $(G, +)$ with $|g| = n$ means that $ng = 0$. In $\mathbb{Z}$, we have $|1| = \infty$ and in $\mathbb{Z}_n$, we have $|1| = n$. In $\mathbb{C}^\times$, we have $|i| = 4$.
2. $|g| = |g^{-1}|$
3. If G is finite, $g \in G$, we have $|g| < \infty$.

Definition 1.2.4 Cyclic Subgroup Generated By a
Let G be a group and $a \in G$, $\langle a \rangle := \{a^k : k \in \mathbb{Z}\}$ is thee cyclic subgroup of G generated by a.
We say a group G is cyclic if there exists $a \in G$ such that $\langle a \rangle = G$.

■ **Example 1.5 Cyclic Groups**

1. $\mathbb{Z} = \langle 1 \rangle$ and $\mathbb{Z}_n = \langle 1 \rangle$.
2. If a group is cyclic, then it is abelian. In particular, $|g| = |\langle g \rangle|$.
3. $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic. $|\mathbb{Z}_2 \times \mathbb{Z}_{\not=}| = 4$ but all elements at most have order $2 < 4$.

■

Proposition 1.2.2 GCD Result 1
Let G be a group, suppose $x \in G$, $m, n \in \mathbb{Z}$ (not both 0) such that $x^n = x^m = e$

1. If $d = \gcd(m,n)$, then $x^d = e$
2. If $k \in \mathbb{Z}$ such that $x^k = e$, then $|x|$ divides k

Proposition 1.2.3 GCD Result 2

Let G be a group. Suppose $x \in G$ and $m \in \mathbb{Z}\backslash\{0\}$.

1. If $|x| = \infty$, then $|x^m| = \infty$
2. If $|x| = n$, then $|x^m| = \frac{n}{\gcd(m,n)}$

Proposition 1.2.4 GCD Result 3 (Cyclic)

Let $G = \langle x \rangle$ be a cyclic group

1. If $|x| = \infty$, then $G = \langle x^m \rangle$ if and only if $m = \pm 1$
2. If $|x| = n < \infty$, then $G = \langle x^m \rangle$ if and only if $\gcd(m,n) = 1$

■ **Example 1.6 Order and Generator**

1. In $G = \mathbb{Z}_{24}$, $|10| = \frac{24}{\gcd(24,10)} = 12$
2. In $G = \mathbb{Z}_7^\times$, the generators are $\{3,5\}$ since

$$3^m \Longrightarrow \gcd(m,6) = 1 \Longrightarrow m = 1,5$$

■

Proposition 1.2.5 Subgroups of A Cyclic Group

Let $G = \langle x \rangle$ be a cyclic group

1. Every subgroup of G is cyclic
2. If $|G| = n < \infty$, then for every positive $d|n$, there is a unique subgroup of order d. Moreover, these are all of the subgroups.

■ **Example 1.7** Given $\gcd(n,m) \neq 1$, then $\mathbb{Z}_n \times \mathbb{Z}_m$ is not cyclic.

Demostración. We can construct

$$H_1 \times \{0\}, \{0\} \times H_2 \leq \mathbb{Z}_n \times \mathbb{Z}_m$$

both can be subgroups of order $\gcd(m,n)$, thus, contradicts the proposition above. ■

■

2. Symmetric Groups & Dihedral Groups

2.1 Symmetric Groups

Definition 2.1.1 Symmetric Group
Let $X = \{1, 2, \ldots, n\}$, we write $S_X = S_n$ and it is called the symmetric group of degree n. Note that $|S_n| = n!$

Definition 2.1.2 m-cycle
A m-cycle is a string of m distinct numbers from $\{1, 2, \ldots, n\}$. The string $(a_1 a_2 \ldots a_m)$ denotes the permutation $a_i \mapsto a_{i+1}$ and $a_m \mapsto a_1$.

Theorem 2.1.1 Disjoint Cycle Form
Every $\sigma \in S_n$ can be written as a product of disjoint cycles. We call this the disjoint cycle form.

■ **Example 2.1 m-string Computation**

1. For S_5, $f = (13)(245), g = (1524)(3)$, then
$$\begin{aligned} f^2 g &= (13)(245)(13)(245)(1524)(3) \\ &(14)(2)(3)(5) = (14) \end{aligned}$$
2. For S_6, $f = (12)(45), g = (16532)$, then
$$\begin{aligned} fg &= (12)(45)(16532) \\ &= (16453) \end{aligned}$$

■

Theorem 2.1.2 Inverse of σ
Consider the m-cycle
$$\sigma = (a_1 a_2 \ldots a_m) \in S_n$$

then,

$$\sigma^{-1} = (a_m a_{m-1} \dots a_1)$$

In general, if $\sigma = \sigma_1 \sigma_2 \dots \sigma_l$ where σ_i's are m-cycles, then $\sigma^{-1} = \sigma_l^{-1} \sigma_{l-1}^{-1} \dots \sigma_1^{-1}$

Theorem 2.1.3 Order of σ
Given $\sigma = \sigma_1 \sigma_2 \dots \sigma_l \in S_n$ a disjoint cycle form. By A2, we have that

$$|\sigma| = \text{lcm}\,(|\sigma_1|, |\sigma_2|, \dots, |\sigma_l|)$$

also, for $\sigma_i = (a_{i1} a_{i2} \dots a_{ik})$, we have $|\sigma_i| = k$.

■ **Example 2.2 Order of σ**

$$f = (12)(345) \Longrightarrow |f| = \text{lcm}2, 3 = 6$$
$$g = (134)(25) \Longrightarrow |g| = \text{lcm}3, 2 = 6$$

but

$$fg = (14235) \Longrightarrow |fg| = 5$$

■

■ **Example 2.3** Find $f \in S_7$ such that $f^4 = (2143567)$.
Note that $|f^4| = 7 = \frac{|f|}{\gcd(|f|,4)}$. This means that $|f| = 7$. And $f^2 = (2516473)$, then $f = (2457136)$
general algorithm is given below:

So a square permutation is one that consists of a product of disjoint square cycles. Now when is a cycle square? If $c = (i_1 i_2 \dots i_k)$, then c^2 takes i_1 to i_3, i_2 to i_4, and so on. In other words:

If k is odd, c^2 is another k-cycle, which means that every k-cycle is a square.

If k is even, then $c^2 = (i_1 i_3 \dots i_{k-1})(i_2 i_4 \dots i_k)$.

Therefore: a permutation is a square if and only if the number of cycles of any even length in its disjoint cycle decomposition is even, and the algorithm you can use to find its root is as following:

1. Find the roots of all odd cycles, $\sqrt{c} = (i_1 i_{(k+3)/2} i_2 i_{(k+5)/2} \dots i_k i_{(k+1)/2})$.
2. Take pairs $c = (i_1 \dots i_k), d = (j_1 \dots j_k)$ of the even cycles of the same length and construct $\sqrt{c, d} = (i_1 j_1 \dots i_k j_k)$.

■

Definition 2.1.3 Transposition
A 2-cycle in S_n is called a transposition, $\sigma = (a_1 a_2)$.

Proposition 2.1.4 $S_n = \langle T \rangle$
Every $\sigma \in S_n$ can be written as a product of transpositions. That is if T is the set of transpositions in S_n, then $\langle T \rangle = S_n$.

2.2 Dihedral Groups

Definition 2.2.1 Dihedral Group
For $n > 1$, let D_{2n} denote the group of symmetries of the regular n-gon (under composition).

R We work with D_{2n} by realizing its elements as permutations in S_n. We do this by labelling the vertices with $\{1,2,\ldots,n\}$ by recording how the symmetry permute the vertices.

Definition 2.2.2 Elements of D_{2n}
Let $r = \frac{360}{n}$ and S =reflection over the line joining vertex 1 and the origin. Then, note that $|r| = n$ and $|s| = 2$. We have

$$D_{2n} = \{e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

we also note that $rs = sr^{-1} = sr^{n-1}$.

3. Cosets & Quotient Groups

3.1 Cosets

Definition 3.1.1 Coset

Let G be a group, $H \leq G$ and $g \in G$. We define the left coset of H in G to be

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

and the right coset to be

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

■ **Example 3.1 Cosets Examples**

1. $G = \mathbb{Z}, H = \langle 2 \rangle$, then

$$\begin{aligned} 0+H &= \{0+h : h \in H\} = H \\ 1+H &= \{1+h : h \in H\} = \{1+2k : k \in \mathbb{Z}\} \\ 3+H &= 1+H \end{aligned}$$

2. $G = S_4$ and $H = A_4$ (elements in A_4 can be written as even product of transpositions in S_4), then

$$(12)(14)(34)(23)(13)H = (12)H$$

since $(14)(34)(23)(13) \in H$.

■

Proposition 3.1.1 Cosets Properties

Let G be a group and $H \leq G$

1. $eH = He = H$
2. $gH = Hg = H \iff g \in H$
3. *a)* $aH = bH \iff b^{-1}a \in H$
   b) $Ha = Hb \iff ba^{-1} \in H$
4. $|gH| = |Hg| = |H|$

Proposition 3.1.2 Cosets Partitions the Group
Let G be a group and $H \leq G$
1. If $a, b \in G$, then $aH \cap bH = \emptyset$ or $aH = bH$
2. $\forall g \in G, g \in gH$, means that the distinct left cosets of H in G partitions G.

Theorem 3.1.3 Lagrange Theorem
If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$. Moreover, $\frac{|G|}{|H|}$ is the number of distinct left cosets of H in G.

Corollary 3.1.4 If G is a finite group and $g \in G$, then $|g|$ divides $|G|$.

Corollary 3.1.5 If $|G| = p$ is prime, then G is cyclic.

Corollary 3.1.6 Euler
If $\gcd(a,n) = 1$, then $a^{\phi(n)} = 1 \mod n$.

■ **Example 3.2 Converse of Lagrange is False**
$G = A_4$ with $|G| = 12$ and indeed $6|12$. But no subgroup of G has order 6. ■

Definition 3.1.2 Index
Let G be a group and $H \leq G$. We define the index of H in G to be $[G : H]$ to represent the number of distinct left (or right) cosets of H in G. We denote teh set of left cosets of H in G by G/H

R When G is finite we have $|G/H| = \frac{|G|}{|H|} = [G : H]$

■ **Example 3.3 Examples of Index**
1. $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\langle n \rangle$
2. $G = S_4$ and $H = S_4$, then $G/H = \{H, (12)H\}$ and $|G/H| = 2$.
3. $G_1 \times G_2 / G_1 \times \{e\} = \{(e,g)H : g \in G_2\}$

■

3.2 Quotient Groups

Definition 3.2.1 Normal Subgroup
Let G be a group and $H \leq G$, we say H is normal in G if for all $g \in G$, we have $gHg^{-1} = H$. Denote it as $H \trianglelefteq G$.

R
$$gHg^{-1} \iff gH = Hg$$

■ **Example 3.4 Examples of Normal Subgroups and Non-normal Subgroups**

1. $G = S_3$ and $H = \langle (12) \rangle$, then $H \not\trianglelefteq G$ since
$$(123)(12)(123)^{-1} = (123)(12)(321) = (23) \notin H$$

2. For any G, the centre $Z(G) \trianglelefteq G$. This is the go-to normal subgroup of G that we can consider for groups.

■

Theorem 3.2.1 Subgroup of Index 2 is Normal
Let G be a group and $H \leq G$. If $[G:H] = 2$, then $H \trianglelefteq G$.

■ **Example 3.5** 1.

$$A_n \trianglelefteq S_n$$

2. G abelian and $H \leq G$, then $H \trianglelefteq G$

■

Proposition 3.2.2 Normal Subgroup Test

1. Need to do the subgroup test first
2. If $H \leq G$, then

$$H \trianglelefteq G \iff \forall g \in G, gHg^{-1} \subseteq H$$

■ **Example 3.6** $SL_n(R) = GL_n(R)$ ■

Proposition 3.2.3 Normality is Necessary and Sufficient for Quotient Group
Let G be a group and $H \leq G$, then G/H is group via the operation $(aH)(bH) = abH$ if and only if $H \trianglelefteq G$.

■ **Example 3.7 Examples of Quotient Groups**

1. $\mathbb{Z}/n\mathbb{Z} := \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ is a quotient group since $\mathbb{Z}$ is abelian
2. $S_n/A_n := \{\overline{e}, \overline{(12)}\}$ is a quotient group since $[S_n : A_n] = 2$.
3. $\mathbf{Q}/\langle i \rangle = \{\overline{1}, \overline{j}\}$ is a quotient group.
4. $GL_2(\mathbb{R})/SL_2(\mathbb{R})$
5. $H \trianglelefteq G$ and $[G:H] = n < \infty$. Let $g \in G$ and $\overline{g} \in G/H$

$$\implies (\overline{g})^n = \overline{e} = \overline{g^n} \implies g^n \in H$$

■

Theorem 3.2.4 Cauchy's Theorem for Abelian Group (76er)
Let G be a finite abelian group, if p is prime such that $p \big| |G|$, then there exists $g \in G$ such that $|g| = p$.

Demostración. Suppose p is a prime such that $p \big| |G|$. We proceed with induction on $|G|$

1. If $G = |p|$, then $\forall e \neq g \in G$, $G = \langle g \rangle$ and so $|g| = |p| = |G|$
2. Assume the result for all smaller groups than G with order divisible by p.
   Take $e \neq x \in G$ and elt $N = \langle x \rangle$. If $G = N = \langle x \rangle$, then we are done since G is cyclic. So, we assume N is a proper subgroup of G.
   a) **Case 1:** if $p \big| |N|$, then there exists $g \in N$ such that $|g| = p$ by hypothesis.

b) **Case 2:** if $p \not| |N|$, then $p \Big| \left|{}^{G}/_{N}\right|$. ${}^{G}/_{N}$ is group since G is abelian and all subgroups are normal in G and $\left|{}^{G}/_{N}\right| < |G|$. By hypothesis ${}^{G}/_{N}$ has an element $\overline{y} = yN$ such that $|\overline{y}| = p$ in ${}^{G}/_{N}$. In particular, $\overline{y} \neq \overline{e}$ and $\overline{y}^p = \overline{e}$. This means that $y \notin N$ but $y^p \in N$. Let $m = |y|$, then

$$|y^p| = \frac{m}{\gcd(m,p)} \in \{\frac{m}{p}, m\}$$

but $\langle y^p \rangle \subseteq \langle y \rangle$ and $\langle y^p \rangle \neq \langle y \rangle$. In particular

$$|y^n| \neq |y| \Longrightarrow |y^p| \neq m \Longrightarrow |y^p| = \frac{m}{p}$$

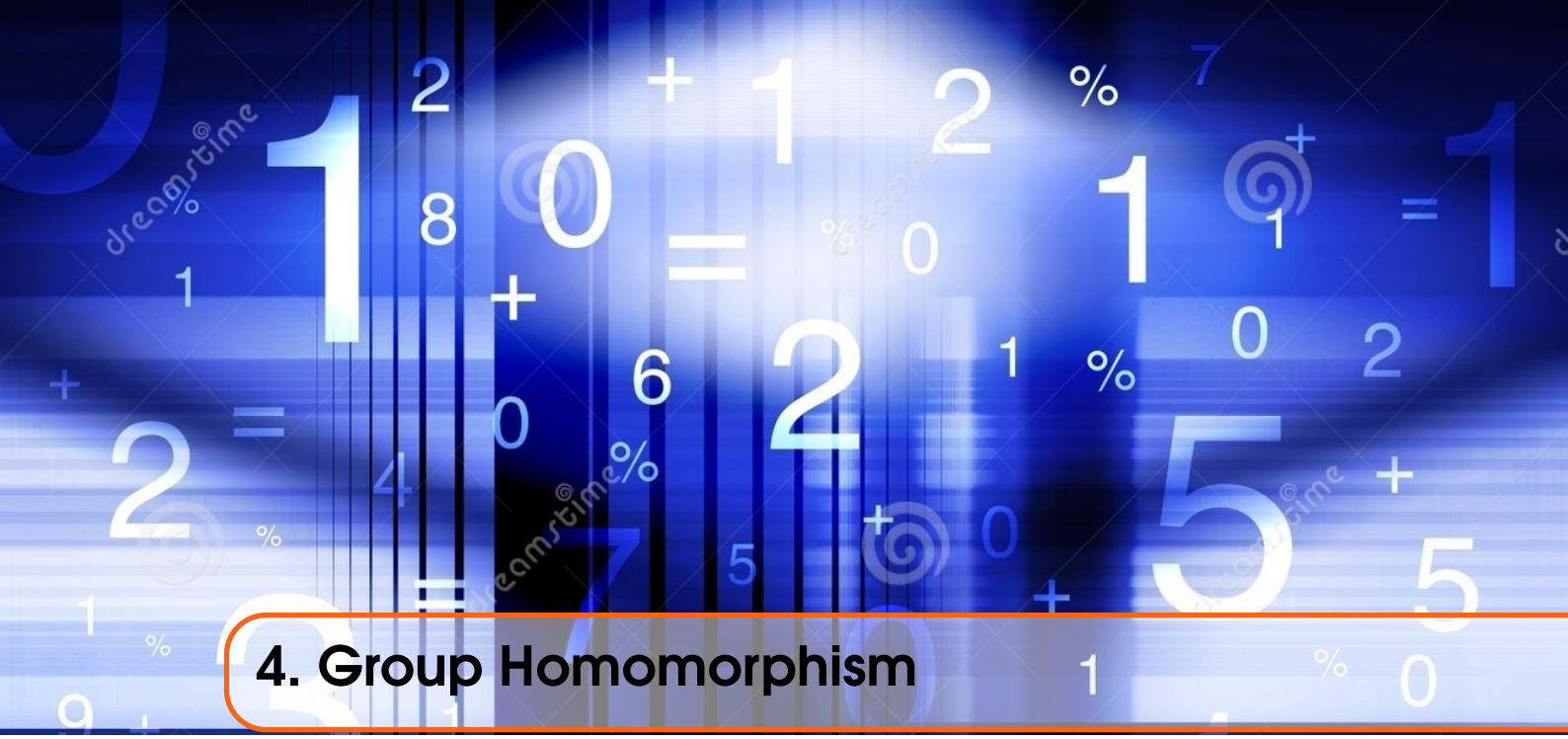
so p divides m. By **case 1**, we can repeat the process with $N = \langle y \rangle$.

■

■ **Example 3.8 Warning: Normality of Subgroups Are Not Transitive**
$G = S_4$, then note that

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V = \{(12)(34), (13)(24), (14)(23), e\} \leq G$$
$$H = \langle e, (12), (34) \rangle$$

Note that $H \trianglelefteq V$ and $V \trianglelefteq G$, but $H \not\trianglelefteq G$. ■



4. Group Homomorphism

4.1 Group Homomorphism

Definition 4.1.1 Group Homomorphism
Let A, B be groups. A function $\varphi : A \to B$ is called a homomorphism if

$$\forall x, y \in A, \varphi(xy) = \varphi(x)\varphi(y)$$

Definition 4.1.2 Embedding
Let $\varphi : A \to B$ be a homomorphism. If ρ is injective, we call φ an embedding of A into B.

Definition 4.1.3 Isomorphism
If φ is bijective, then we call φ an isomorphism. If there exists such a φ from A to B, then we say A and B are isomorphic, denoted by $A \cong B$.

■ **Example 4.1 Examples of Homomorphisms**

1. $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\varphi(a) = [a]$ is a homorphism
2. $\varphi : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ defined by
$$\varphi(A) = \det(A)$$
is a homomorphism
3. $\varphi : (M_2(\mathbb{R}), +) \to \mathbb{R}$ defined by the determinant is not a homomorphism; but the trace is a homomorphism.
4. $\varphi : S_n \to C_2 := (\{-1, 1\}, \cdot)$ defined by $\varphi(\sigma) = \operatorname{sgn}(\sigma)$ is a homomorphism
5. $\varphi : \mathbb{R}^\times \times \mathbb{R}^\times \to GL_2(\mathbb{R})$ defined by
$$\varphi(a, b) = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$
is an embedding. Moverover, let
$$D = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{R}^\times \right\}$$

which is a group, then $\varphi : \mathbb{R}^\times \times \mathbb{R}^\times \to D$ becomes an isomorphism.

6. $\varphi : \mathbb{Z}_2 \to C_2$ defined by
$$\varphi(x) = \begin{cases} 1 & x = 0 \\ -1 & x = 1 \end{cases}$$
is an isomorphism.
7. Let V be a real vector space with finite dimension n. Then,
$$GL(V) := \{T : V \to V | T \text{ is invertible and linear}\}$$
By previous linear algebra course, we know that $GL(V) \cong GL_n(\mathbb{R})$.

■

Proposition 4.1.1 Cyclic Groups of The Same Order are Isomorphic
Let A, B be cyclic groups such that $|A| = |B|$ and $A = \langle a \rangle$ and $B = \langle b \rangle$. Then $\varphi : A \to B$ given by $\varphi(a^l) = b^l$ is an isomorphism. Moreover,
$$A \cong B \cong \mathbb{Z}_n$$
with $n = |A| = |B|$.

Proposition 4.1.2 Basic Properties of Homomorphisms
Let $\varphi : A \to B$ be a homomorphism,

1. $\varphi(e_A) = e_B$
2. $\forall g \in A$, $(\varphi(g))^{-1} = \varphi(g^{-1})$
3. If $H \leq A$, then $\varphi(H) \leq B$
4. If $H \leq B$, then $\varphi^{-1}(H) \leq A$
5. The kernel of φ,
$$\ker \varphi := \{x \in A : \varphi(x) = e\}$$
then, $\ker \varphi \trianglelefteq A$. This is always true, another go-to example of normal subgroup.
6. φ is an embedding, if and only if
$$\ker \varphi = \{e_A\} \subseteq A$$

Big Picture

1. $\varphi : A \to B$ is an embedding, then $A \cong \varphi(A) \leq B$
2. $\varphi : A \to B$ is an isomorphism, then we can say
A is the same group as B up to relabelling.
3. If $\varphi : A \to B$ is an embedding, then
$$a^n = e \iff \varphi(a^n) = e \iff (\varphi(a))^n = e$$

Exercise 4.1 Why are the following NOT isomorphic?

1. $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ are not isomorphic since $\mathbb{Z}$ is cyclic while the other is not **(Cyclicness)**
2. $\mathbb{R}^\times$ and $(0, \infty)$ are not isomorphic since $|-1| = 2$ in $\mathbb{C}^\times$ while it is not true in the other. **(Order problem)**
3. $\mathbb{R}^\times$ and $\mathbb{C}^\times$ are not isomorphic since $|-1| = 2$ and $|i| = 4$. Again, order problem.
4. We can also check for whether the order is Abelian or not. For example, there does not exist an embedding $\varphi : GL_2(\mathbb{R}) \to \mathbb{R}^\times$

5. $\varphi : \mathbb{Z}_3 \to \mathbb{Z}_6$ given by $\phi(a) = a$ is not a homomorphism since $\varphi(2+2) = \varphi(2) + \varphi(2)$ is **not well-defined!!** since $1 \neq 4$ in $\mathbb{Z}_6$.
6. **[Bonus]** $(\mathbb{R}, +) \cong (\mathbb{C}, +)$
7. Give an example of a group G with $H \leq G$ such that $H \cong G$ but $H \neq G$ (note that this cannot be done for finite groups)
   a) Let $G = \prod_{i=1}^{\infty} \mathbb{Z}$ and $H = \{0\} \times \prod_{i=1}^{\infty} \mathbb{Z}$
   b) $2\mathbb{Z} \leq \mathbb{Z}$
8. $G = \prod_{i=1}^{\infty} \mathbb{Z}$ and $H_1 = \mathbb{Z} \times \prod_{i=1}^{\infty} \{0\}$ and $H_2 = \mathbb{Z} \times \mathbb{Z} \times \prod_{i=1}^{\infty} \{0\}$. Even though

$$G/H_1 \cong G \cong G/H_2$$

but $H_1 \ncong H_2$ since $\mathbb{Z}$ is cyclic and $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

■

Proposition 4.1.3 Uniqueness of Kernel
Let G be a group, then $H \trianglelefteq G$ if and only if there exists a homomorphism $\varphi : G \to G'$ such that $H = \ker \varphi$.

R If you are normal, then you are some kernel of a homomorphism.

4.2 First Isomorphism Theorem (76er)

Theorem 4.2.1 First Isomorphism Theorem
Let $\varphi : G \to G'$ be a homomorphism. Then,

$$G/\ker \varphi \cong \varphi(G)$$

via the isomorphism $\overline{g} \mapsto \varphi(g)$.

R If φ is surjective, then $G/\ker \varphi \cong \varphi(G) = G'$

■ Example 4.2 Examples of FIT

1. $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times$ under the $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ which is a surjective homomorphism and $\ker \det = SL_n(\mathbb{R})$.
2. $S_n/A_n \cong C_2 = \{-1, 1\}$ and $sgn : S_n \to C_2$ is a surjective homomorphism, then $\ker sgn = A_n$.
3. $G = \mathbb{C}[x]$, $H = \{f(x) \in G : f(0) = 0\}$. $G/H \cong \mathbb{C}$ and $\varphi : G \to \mathbb{C}$ given by $\varphi(f(x)) = f(0)$.
4. $\mathbb{R}/\mathbb{Z} \cong S^1$ where $S^1 = \{z \in \mathbb{Z} : |z| = 1\}$. The isomorphism is $\varphi(\overline{t}) = e^{i2\pi t}$

■

Definition 4.2.1 Automorphism
$\varphi : G \to G$ is called an automorphism. Then,

$$\mathbf{Aut}(G) := \{\varphi : \varphi \text{ is an automorphism of } G\}$$

Definition 4.2.2 Inner Automorphism of G
For $g \in G$, $\varphi_g : G \to G$ given by

$$\varphi_g(x) = gxg^{-1}$$

is an automorphism. Then, the inner automorphism of G is

$$\mathbf{Inn}(G) := \{\varphi_g : g \in G\} \leq \mathbf{Aut}(G)$$

Theorem 4.2.2 Fact

$$\mathbf{Inn}(G) \trianglelefteq \mathbf{Aut}(G)$$

Corollary 4.2.3

$$G \Big/ Z(G) \cong \mathbf{Inn}(G)$$

5. Group Actions

5.1 Group Actions

Definition 5.1.1 Group Action

Let G be a group and let X be a set. A group action of G on X is a map

$$\cdot : G \times X \longrightarrow X$$

1. $e \cdot x = x, \forall x \in X$
2. $\forall g, h \in G, x \in X$, $(gh) \cdot x = g(h \cdot x)$

Definition 5.1.2 Stabilizer and Orbit of X

Let G acts on X, if $x \in X$, then the stabilizer of x is

$$\mathbf{stab}(x) = \{g \in G : g \cdot x = x\}$$

the orbit of x is

$$\mathbf{orb}(x) = \{g \cdot x : g \in G\}$$

Definition 5.1.3 Faithful and Transitive

Let G acts on X,

1. We say the action is faithful if $\forall e \neq g \in G, \exists x \in X$ such that $gx \neq x$.
2. We say the action is transitive if $\forall x, y \in X, \exists g \in G$ such that $gx = y$.

R Let G acts on X, for $x \in X$, then

$$\mathbf{stab}(x) \leq G$$

and

$$\mathbf{orb}(x) \subseteq X$$

■ **Example 5.1 Examples of Group Actions**

1. Let $G = X$ be group, then the group action "left multiplication"
$$g \cdot x = gx$$
fix $x \in X = G$, $\mathbf{stab}(x) = \{e\}$ and $\mathbf{orb}(x) = G$. This implies that this group action is transitive.
2. Let $G = X$ be group and define $g \cdot x = gxg^{-1}$. Then, for $x \in X$, $\mathbf{stab}(x) = \{g \in G : gxg^{-1}\} = \{g \in G : gx = xg\}$.

■

Definition 5.1.4 Centralizer
Let G be a group and $x \in G$. The centralizer of x in G is

$$C(x) = \{g \in G : gx = xg\}$$

■ **Example 5.2 Continuing from Above**

1. $G = S_n$, $X = \{1,2,\ldots,n\}$, then $\sigma \cdot i = \sigma(i)$ is a transitive group action
2. $H \leq S_n$, then H acts on $\{1,2,\ldots,n\}$ in the same way. Then, we might get something different. Note that $H = \langle(12)\rangle \leq S_3$ and H acts on $X = \{1,2,3\}$. But it is not transitive since there does not exist a $\sigma \in H$ such that $\sigma(1) = 3$.
3. $G = S_n$ for $n > 2$ and $X = \{\Delta, -\Delta\}$, then for all $\sigma \in A_n$, $\sigma(\Delta) = \Delta$ and $\sigma(-\Delta) = -\Delta$. Thus, not faithful!
4. Let G be a group and $X = \{H \subseteq G : H \leq G\}$, then consider the conjugation action defined by $g \cdot H = gHg^{-1}$. Fix $H \in X$, then $\mathbf{stab}(H) = \{g \in G : gHg^{-1} = H\} = N_G(H)$ is the normalizer of H.

■

Theorem 5.1.1 Cayley's Theorem (76er)
Every finite group G is isomorphic to a subgroup of S_n where $n = |G|$.

Demostración. Say $G = \{g_1, g_2, \ldots, g_n\}$ and $g_i \neq g_j$ for $i \neq j$. Take $g \in G$, note that $gg_i = gg_j \iff g_i = g_j \iff i = j$. Thus,

$$(gg_1, gg_2, \ldots, gg_n) = (g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(n)})$$

for some $\sigma \in S_n$. Define $\psi : G \to S_n$ by $\psi(g) = \sigma$ as above.

1. **Claim 1:** ψ is a homomorphism
Let $a, b \in G$ such that $\psi(a) = \alpha$ and $\psi(b) = \beta$. Then,
$$(abg_1, \ldots, abg_n) = (ag_{\beta(1)}, \ldots, ag_{\beta(n)}) = (g_{\alpha(\beta(1))}, \ldots, g_{\alpha(\beta(n))})$$
Thus, $\psi(ab) = \alpha \cdot \beta = \psi(a)\psi(b)$. Thus ψ is a homomorphism.
2. **Claim 2:** ψ is an embeding
Note that
$$g \in \ker \varphi \iff gg_i = g_i \iff g = e$$
Thus, ψ is injective. There exists an embedding $\psi : G \to S_n$ and G is isomorphic to a subgroup of S_n.

■

5.2 Counting Applications

5.2.1 Class Equation

Theorem 5.2.1 Orbit-Stabilizer Theorem
Let G be a finite group and G acts on X. Then

$$\forall x \in X, |G| = |\mathbf{stab}(x)| \cdot |\mathbf{orb}(x)|$$

R **Orb(x) Partitions X**
For $x, y \in X$, we either have $\mathbf{orb}(x) = \mathbf{orb}(y)$ or $\mathbf{orb}(x) \cap \mathbf{orb}(y) = \emptyset$

Theorem 5.2.2 Class Equation
Let G acts on $X = G$ by conjugation. Then

$$|G| = |Z(G) + \sum [G : C(b_i)]$$

where b_i are the none-central orbit representatives.

Proposition 5.2.3 Examples of Class Equation Application
For p prime and $|G| = p^n$, then $Z(G) \neq \{e\}$

Theorem 5.2.4 Cauchy's Theorem (76er)
If G is a finite group and p is a prime such that $p \big| |G|$, then G has an element of order p.

Demostración. We know that by Class Equation,

$$|G| = |Z(G)| + \sum \frac{|G|}{|C(b_i)|}$$

1. **Case 1:** If $p \big| |Z(G)|$, we are done by Cauchy's theorem for a Abelian group
2. **Case 2:** Suppose $p \not| |z(G)|$, then there exists i such that

$$p \not| \frac{|G|}{|C(b_i)|} \Longrightarrow p \not| |C(b_i) < G$$

The result follows by induction.

■

5.2.2 Burnside's Lemma

Theorem 5.2.5 Burnside's Lemma
Let G be a finite group acts on finite X. For $g \in G$, define the fix to be

$$\mathbf{Fix}(g) := \{x \in X : gx = x\}$$

and $X/G = \{\text{orbits of this action}\}$. Then,

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|\mathbf{Fix}(g)|$$

■ **Example 5.3 Applications of Burnside's Lemma**

1. **Floor Tiles:** Given n colours, how many floor tiles can we make? (at the four corner)

   Demostración. Let X be the set of all configurations of all possible tiles. Note two $x, y \in X$ are same tile if and only if $\exists g \in \{e, r, r^2, r^3\}$ such that $gx = y$ if and only if $\mathbf{orb}(x) = \mathbf{orb}(y)$. Let $G = \{e, r, r^2, r^3\}$, then $|\mathbf{Fix}(e)| = n^4$, $|\mathbf{Fix}(r)| = n$, $|\mathbf{Fix}(r^3)| = n$, $|\mathbf{Fix}(r^2)| = n^2$. Thus, by Burnside's Lemma, the number of tiles is $\frac{1}{4}(n^4 + n^2 + 2n)$. ■

2. **Round Table Seating:** given n people, how many ways can we arrange their seating around a table?

   Demostración. Let X be the set of all configurations of all such seating. Let $G = C_n = \langle r \rangle$. Note that $|\mathbf{Fix}(e)| = n!$ but $|\mathbf{Fix}(g)| = 0|$ for all $e \neq g \in C_n$. Thus, by Burnsides lemma, the answer is $\frac{1}{n}n! = (n-1)!$. ■

3. **Ugly Necklace:** Given n colours, how many different necklaces can be made?

   Demostración. Let X be the set of all configurations of possible necklaces. Let $G = D_6$. Then, $|\mathbf{Fix}(e)| = n^3$, $|\mathbf{Fix}(r)| = n$, $|\mathbf{Fix}(r^2)| = n$, $|\mathbf{Fix}(s)| = n^2$, $|\mathbf{Fix}(rs)| = n^2$, $|\mathbf{Fix}(r^2 s)| = n^2$. Then, by Burnside's lemma, the answer is $\frac{1}{6}(n^3 + 3n^2 + 2n)$ ■

■

5.3 Finite Abelian Groups

Proposition 5.3.1 Isomorphism Between Internal Product and External Product
Let G be a group, $H \trianglelefteq G$ and $K \trianglelefteq G$ with $H \cap K = \{e\}$, then

$$HK \cong H \times K$$

In particular, $|HK| = |H| \cdot |K|$.

Theorem 5.3.2 Sylow's First Theorem For Abelian Groups
Let p be a prime and let G be a prime group such that $|G| = p^n m$ with $n, m \in \mathbb{N}$ and $p \nmid m$, then G has a subgroup of order p^n.

Proposition 5.3.3 Extension
Let G be a group, $H_1, \ldots, H_k \trianglelefteq G$ and $\forall i, H_i \cap H_1 H_2 \ldots H_i \ldots H_k = \{e\}$. Then,

$$H_1 H_2 \ldots H_k \leq G$$

and

$$H_1 H_2 \ldots H_k \cong H_1 \times H_2 \times \cdots \times H_k$$

Definition 5.3.1 p-Group
Let p be a prime, a group G is called a p-group is $|G| - p^n$ for some $n \in \mathbb{N}$.

Lemma 5.4 Unique Subgroup in p-group
Let G be a finite abelian p-group. If G has a unique subgroup of order p, then G is cyclic.

Theorem 5.4.1 Fundamental Theorem of Finite Abelian Groups
Every finite abelian group is isomorphic to a external direct product of cyclic groups.

■ **Example 5.4 Application of the theorem**

1. Find a complete, irredundant list of abelian groups of order 1176 up to isomorphism.

   Demostración. Note that $1176 = 2^3 \times 3 \times 7^2$. Using the proposition $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{mn}$ if $\gcd(m,n) = 1$ and swaping is an isomorphism, we have
   a) $\mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_{7^2}$
   b) $\mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_{7^2}$
   c) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{7^2}$
   d) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7$
   e) $\mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7$
   f) $\mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7$

   ■

2. Find all abelian groups of order $108 = 2^2 \times 3^3$ that have exactly one subgroup of order 3.

   Demostración. By lemma **Unique Subgroup in p-group**, we know that our result cannot be a non-cyclic group. Thus, the only options are

   $$\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^3} \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^3}$$

   ■

■

II Ring Theory

6 Introduction to Rings 26
6.1 Rings
6.2 Integral Domain & Fields

7 Ring Homorphism 30
7.1 Ring Homorphism
7.2 Quotient Rings

8 Prime Ideal & Maximal Ideal 35
8.1 Prime Ideal & Maximal Ideal
8.2 Supportive Section: Set Theory

9 ED & PID & UFD 39
9.1 Euclidean Domain
9.2 Principal Ideal Domain
9.3 Unique Factorization Domain
9.5 PMATH347 Final Exam

6. Introduction to Rings

6.1 Rings

Definition 6.1.1 Ring

A ring is an abelian group $(R,+)$ equipped with an operation $\cdot : R \times R \to R$ called multiplication such that

1. **Associativity of Multiplication:** $\forall a,b,c \in R, (ab)c = a(bc)$
2. **Distributivity:** $\forall a,b,c \in R, a(b+c) = ab+bc$ and $(b+c)a = ba+ca$

R

1. $(R,+)$ is abelian additive group. We denote the identity of $(R,+)$ by the symbol 0 as the additive identity
2. We do not assume there exists $1 \in R$ such that $1x = x1 = x, \forall x \in R$. When R does admit such an element $1 \in R$, we say R is **unital** and call 1 the unity of R.
3. If R is unital and $a \in R$ such that $\exists b \in R$ with $ab = ba = 1$, then we say a is a unit and call b the multiplicative inverse of a and write $b = a^{-1}$. Denote the collection of units of R to be $R^{\times}$.
4. If R is a ring such that $ab = ba, \forall a,b \in R$, we say that R is commutative.

Example 6.1 Examples of Rings

1. Given R is a ring, then $M_n(R), R[x]$ are rings.
2. **Non-commutative ring:** $M_n(\mathbb{R})$
3. **Non-unital ring:** $2\mathbb{Z}$
4. **Finite non-commutative ring:** $M_3(\mathbb{Z}_5)$
5. **Finite non-unital ring:** $\{0,2,4,6\} \subseteq \mathbb{Z}_8$ is non-unital
6. R, S are rings, then we define the direct sum

$$R \oplus S = \{(a,b) : a \in R, b \in S\}$$

by $(a,b)+(c,d) = (a+c, b+d)$ and $(a,b)\cdot(c,d) = (ac,bd)$ is a ring.

7. $R = \mathscr{R}\{f : \mathbb{R} \to \mathbb{R} \text{ continuous}\}$ with the operation

$$(f+g)(x) = f(x)+g(x)$$
$$(fg)(x) = f(x)g(x)$$

is a ring. **Warning!** $(\mathscr{C}(\mathbb{R}), +, \circ)$ with function composition is not a ring.
8. Let V be a vector space, then $(\mathscr{L}(V), +, \circ)$ is a ring.

■

Proposition 6.1.1 Basic Properties of Ring
$\forall a, b, c \in R$,

1. $a0 = 0a = 0$
2. $a(-b) = (-a)b$
3. $a(b-c) = ab - ac$
4. $(b-c)a = ba - ca$

6.1.1 Subring

Definition 6.1.2 Subring Let R be a ring and $\emptyset \neq S \subseteq R$ is a subring of R is and only if for all $a, b \in S$,

1. $a - b \in S$
2. $ab \in S$

denote by $S \leq R$.

■ **Example 6.2 Examples of Subrings**

1. Let R be a ring, the center of R

$$Z(R) = \{a \in R : ab = ba, \forall b \in R\}$$

$Z(R) \leq R$.
2. Let $d \in \mathbb{Z}$ be square-free ($\nexists p, p^2 | d$). The ring of quadratic integers, $\mathbb{Z}[\sqrt{d}] \leq \mathbb{C}$.
3. Ring of Gaussian Integers: $\mathbb{Z}[i] \leq \mathbb{C}$.

■

Definition 6.1.3 Nilpotent
We say $r \in R$ is nilpotent if there exists $n \in \mathbb{N}$ such that $r^n = 0$.

$$\mathbf{Nil}(R) := \{r \in R : r \text{ is nilpotent}\}$$

R

If R is commutative, $\mathbf{Nil}(R) \leq R$.
When R is not commutative, this is not guaranteed, consider $R = M_2(\mathbb{R})$ and

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

then, $A^2 = B^2 = 0 \in \mathbf{Nil}(R)$ but $A + B = A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \notin \mathbf{Nil}(R)$.

Definition 6.1.4 Characteristic
Let R be a unital ring, the characteristic of R is defined to be $n = |1|$ in the group $(R,+)$. If $|1| = \infty$, then we say R has characteristic 0. (Note that this is a definition exclusively for unital rings)

6.2 Integral Domain & Fields

Definition 6.2.1 Left/Right Zero Divisors
Let R be a ring, we say $0 \neq a \in R$ is a left zero divisor if there exists $0 \neq b \in R$ such that $ab = 0$; we say $0 \neq a \in R$ is a right zero divisor is there exists $0 \neq b \in R$ such that $ba = 0$.

Definition 6.2.2 Integral Domain (ID)
We say a ring R is an integral domain if it is
1. commutative
2. unital
3. no zero divisors

Definition 6.2.3 Field We say a ring R is an field if it is
1. commutative
2. unital
3. every nonzero element in R is a unit

1. We say $a \in R$ is a zero divisor if a is a left or zero divisor
2. For a unital ring, we insist $1 \neq 0$.

■ **Example 6.3 Examples of ID and Fields**

1. $\{0\}$ is the trivial ring and it is by convention not a unital ring
2. $\mathbf{Char}(\mathbb{Z}_n) = n$, $\mathbf{Char}(\mathbb{Z}) = 0$, and similar to the group result

$$\mathbf{Char}(\mathbb{Z}_n \oplus \mathbb{Z}_m) = \operatorname{lcm}(m,n)$$

3. Usual ID: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[\sqrt{d}]$ with d square-free
4. **If R is ID, then $R[x]$ is ID!!!**
5. Usual Fields: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ with p prim, and $\mathbb{Q}(\sqrt{d})$
6. If F is a field, then the rational function field is a field

$$\mathscr{F}(x) = \left\{ \frac{f(x)}{g(x)} : f,g \in F[x], g \neq 0 \right\}$$

7. **ID, but not Field:** $F[x]$ even if F is a field and $\mathbb{Z}$
8. Let R be an ID, but $R \oplus R$ is never an ID since $(1,0)\cdot(0,1) = 0$ as zero divisors.

■

Proposition 6.2.1 Characteristics
Let R be unital,

1. If $\mathbf{Char}(R) = 0$, then there does not exists a positive integer n such that $nr = 0, \forall r \in R$
2. If $\mathbf{Char}(R) = n > 0$, then $nr = 0, \forall r \in R$.

Proposition 6.2.2 Cancellation
Let R be a ring and $a, b, c, d \in R$ such that $a \neq 0, ab = ac$ and a is not a left zero divisor, then $b = c$.

Theorem 6.2.3 Every field is an ID
Every field is an integral domain.

Theorem 6.2.4 Every Finite ID is A Field (76er)
Every fintie integral domain is a field.

Demostración. Let R be a finite ID, so it is commutative and unital already. Let $0 \neq a \in R$. We know that $R = \{a_1, a_2, \ldots, a_n\}$ is finite so

$$aa_i = aa_j \iff a_i = a_j$$

so $R = \{aa_1, aa_2, \ldots, aa_n\}$, thus there must exist some i such that $aa_i = 1$. ■

Proposition 6.2.5 ID Has Prime Characteristics or 0 (76er)
Let R be an ID, then $\mathbf{Char}(R) = 0$ or p a prime.

Demostración. If $\mathbf{Char}(R) = 0$, we are done. Suppose $\mathbf{Char}(R) = n > 0$, where n is not a prime. Then, $n = ab$ for some $1 < a, b < n$ then $0 = n = ab$ in R (where interpret a to be the sum of a many of $1 \in R$), note that $a = 0$ or $b \neq 0$ since this is an ID. But by the minimality of $\mathbf{Char}(R) = n$, we have a contradiction. ■

7. Ring Homorphism

7.1 Ring Homorphism

Definition 7.1.1 Ring Homomorphism

Let R, S be rings. A function $\varphi : R \to S$ is a homomorphism if $\forall x, y \in R$ such that

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$
2. $\varphi(ab) = \varphi(a)\varphi(b)$

R Note that if $\varphi : R \to S$ is ring homomorphism, then $\varphi : (R,+) \to (S,+)$ is the underlying group homomorphism.

■ **Example 7.1 Examples of Ring Homomorphism**

1. $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\varphi(x) = [x]$ is a homomorphism
2. **Group homomorphisms that are not ring homomorphisms:** $\varphi : M_n(\mathbb{R}) \to \mathbb{R}$ given by $\varphi(x) = \det(x)$ or $Tr(x)$. The first one breaks down under addition and the second one breaks down under multiplication.
3. Let R be a commutative ring. Then, for $a \in R$, $\varphi : R[x] \to R$ given by $\varphi(f(x)) = f(a)$ is a homomorphism.
4. Let R be a commutative and unital ring, $\mathbf{Char}(R) = p$ be a prime, then $\varphi(x) = x^p$ is a homomorphism from R to R. (See Assignment Section)

■

Exercise 7.1 Find all homomorphisms $\varphi : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}$ ■

Demostración. Let φ be such a homomorphism and say $\varphi(1,0) = n$ and $\varphi(0,1) = m$. Then, for $(a,b) \in \mathbb{Z} \oplus \mathbb{Z}$, note that

$$\varphi(a,b) = \varphi[a(1,0) + b(0,1)] = a\varphi(1,0) + b\varphi(0,1) = an + bm$$

We only need to determine m, n. Note that $\varphi(1,0)\varphi(1,0) = \varphi((1,0)(1,0)) = \varphi(1,0)$, so $n^2 = n$. Thus, $n \in \{0,1\}$ and $m \in \{0,1\}$. We have several cases to do:

1. $n=0, m=0$, we have the trivial zero homomorphism
2. $n=1, m=0$, $\varphi(a,b)=a$ a homomorphism
3. $n=0, m=1$, $\varphi(a,b)=b$ a homomorphism
4. $n=1, m=1$, $\varphi(a,b)=a+b$ is not a homomorphism

■

Definition 7.1.2 Ring Embedding & Isomorphism
Let R, S be rings, $\varphi : R \to S$ be a homomorphism
1. If φ is injective, we say φ is an embedding
2. If φ is bijective, we say φ is an isomorphism, denoted by $R \cong S$.

7.2 Quotient Rings

Definition 7.2.1 Quotient Ring
Let R be a ring and $S \leq R$, then $(S,+) \leq (R,+)$. Moreover, since $(R,+)$ is abelian and so $(S,+) \trianglelefteq (R,+)$. Let R/S denote the set of cosets of $(S,+)$ in $(R,+)$, i.e.

$$R/S = \{a+S : a \in R\}$$

since $(S,+) \trianglelefteq (R,+)$, we have $(R/S,+)$ as an abelian group, where

$$(a+S)+(b+S) = (a+b)+S$$

Further more, to make it a ring, we need $S \trianglelefteq R$ to be an ideal (defined later), equipped with the multiplication

$$(a+S)(b+S) = ab+S$$

Then, $(R/S,+,\cdot)$ is a quotient group of R.

■ Example 7.2 Well-defineness
$\mathbb{R} \leq \mathbb{C}$ and $(1+i)+\mathbb{R} = i+\mathbb{R}$, $(1+2i)+\mathbb{R} = 2i+\mathbb{R}$ in $\mathbb{C}/\mathbb{R}$. However,

$$(1+i+\mathbb{R})(1+2i+\mathbb{R}) = 3i+\mathbb{R}$$

$$(i+\mathbb{R})(2i+\mathbb{R}) = 0+\mathbb{R}$$

But $3i+\mathbb{R} \neq 0+\mathbb{R}$ since $3i \notin \mathbb{R}$. ■

Definition 7.2.2 Ideal
Let $S \leq R$, we say S is a left ideal if for all $a \in S$ and $r \in R$, we have $ra \in S$; we say S is a right ideal if for all $a \in S, r \in R$, we have $ar \in S$. We say S is an ideal of R, if it is left and right ideal of R. Denote by $S \trianglelefteq R$.

Proposition 7.2.1 Ideal Test
Let $\emptyset \neq I \subseteq R$, then $I \trianglelefteq R$ if and only if
1. $\forall a, b \in I, a-b \in I$
2. $\forall a \in I, b \in S, ab \in S$ and $ba \in S$

Definition 7.2.3 Generated Ideals by a
Let R be a ring and $a \in R$,
1. the left ideal of R generated by a is

$$Ra = \{ra : r \in R\}$$

2. the right ideal of R generated by a is

$$aR = ar : r \in R$$

3. the **principal ideal of R generated by a** is

$$RaR = \langle a \rangle = \{r_1 a r_1' + \cdots + r_n a r_n' : r_i, r_i' \in R, n \in \mathbb{N}\}$$

1. If R is not unital, it is not true that $a \in RaR$.
2. The collection $\{rar' : r, r' \in R\}$ might not be a subring of R since addition might not be closed
3. Our definition of principal ideal does not have such a problem.

■ **Example 7.3 Distinct Left and Right Ideals** Let $R = M_2(\mathbb{R})$

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & a \\ 0 & c \end{bmatrix}$$

so

$$RA := \left\{ \begin{bmatrix} 0 & x \\ 0 & y \end{bmatrix} : x, y \in \mathbb{R} \right\}$$

Then,

$$AR = \left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} : x, y \in \mathbb{R} \right\}$$

but

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \notin AR$$

thus, AR is not a left ideal. ■

When R is commutative, left ideal, right ideal, and ideal are equivalent. If R also unital, we have $a \in \langle a \rangle$ as well.

■ **Example 7.4 Implications of Ideals**

1. Let R be a unital ring and $u \in R^\times$ and $uR = R$, for $r \in R$, $r = uu^{-1}r \in uR$. **Unital ring makes ideal containing unit(s) to explode to the whole ring**
2. Let F be a field, then the only ideals F has are F and $\{0\}$.
3. Let R be a unital and non-commutative real. Note that $1 \in Z(R)$ and $Z(R) \neq R$ (otherwise, commutative). But $Z(G)$ is not a left or right ideal.
4. Let $R = \mathbb{Z} \oplus \mathbb{Z}$, the diagonal subring

$$S = \{(a,a) : a \in \mathbb{Z}\} \leq R$$

but it is not an ideal since $(1,1)(1,2) = (1,2) \notin S$.

5. $I = \{f(x) \in \mathbb{Z}[x] : f(0) = 0\} \trianglelefteq \mathbb{Z}[x]$

$$\mathbb{Z}[x] / I \cong \mathbb{Z}$$

6. $R = M_2(\mathbb{Z}), I = M_2(2\mathbb{Z}) \trianglelefteq R$

$$R/I \cong M_2(\mathbb{Z}_2)$$

■

Theorem 7.2.2 Division Algorithm
Let F be a field, let $R = F[x]$, for all $f, g \in R$ $g \neq 0$, there exists $q, r \in R$ such that

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

where $r(x) = 0$ or $\deg r(x) < \deg g(x)$. Moveover, $q(x)$ and $r(x)$ are unique.

■ **Example 7.5 How to Construct a Principal Ideal?** Let F be a field, $a \in F$, then

$$I = \{f(x) \in F[x] : f(a) = 0\} \trianglelefteq F[x]$$

Note that $f(x) = x - a \in I$. We claim $I = \langle x - a \rangle$. ■

R $\mathbb{Z}$ has a division algorithm, by the same argument, every ideal of $\mathbb{Z}$ is of the form $\langle n \rangle = n\mathbb{Z}$.

Theorem 7.2.3 First Isomorphism Theorem (76er)
Let R, S be rings and let $\varphi : R \to S$ be a ring homomorphism, then

$$R/\ker\varphi \cong \varphi(R) \leq S$$

via the isomorphism $\overline{a} \mapsto \varphi(a)$.

Demostración. **Exercise for the reader.** ■

Exercise 7.2 Let $\mathbb{Z}_3[x]/\langle x^2+2 \rangle = R$

1. Describe the elements of R
2. Find a well-known ring isomorphic to this ring

Demostración. Let $\overline{f(x)} \in R$, by division algorithm, $\exists q, r \in \mathbb{Z}_3[x]$ such that

$$f(x) = q(x)(x^2+2) + r(x)$$

where $\deg r(x) < 2$ or $r(x) = 0$. Moveover, in R, $\overline{f(x)} = \overline{0} + \overline{r(x)} \implies \overline{f(x)} = \overline{r(x)}$. Thus, $R = \{\overline{ax+b} : a, b \in \mathbb{Z}_3\}$. Note that

$$\overline{ax+b} = \overline{cx+d} \implies (a-c)x + (b-d) \in \langle x^2+2 \rangle \implies (a-c)x + (b-d) = 0$$

by degrees. Thus, each element in R is uniquely represented by $a, b \in \mathbb{Z}_3$. (This can be generalized to higher degrees). In particular, $|R| = 3^2$.

For the second part, we cliam $R \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$. Define $\varphi : \mathbb{Z}_3[x] \to \mathbb{Z}_3 \oplus \mathbb{Z}_3$ by $\varphi(f(x)) = (f(1), f(2))$. It is left as an exercise to check that this is a ring homomorphism with $\ker\varphi = \langle x^2+2 \rangle$. And φ is surjective (hard). Then, by FIT, we have

$$R \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

■

■

R In general, for field F and $f(x) \in F[x]$ with $\deg f(x) = n$, then

$$F[x] \Big/ \langle f(x) \rangle = \{\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : a_i \in F}\}$$

still has unique representation. Moveover, if $|F| = m < \infty$, then $\left|F[x] \Big/ \langle f(x) \rangle\right| = m^n$.

8. Prime Ideal & Maximal Ideal

8.1 Prime Ideal & Maximal Ideal

Definition 8.1.1 Prime Ideal & Maximal Ideal

Let $I \trianglelefteq R$ and proper $I \neq R$

1. We say I is prime if whenever $a,b \in R$ such that $aRa = \{arb : r \in R\} \subseteq I$, then $a \in I$ or $b \in I$
2. We say I is maximal if whenever $J \trianglelefteq R$ such that $I \subseteq J \subseteq R$, then $I = J$ or $J = R$.

R When R is commutative and unital $I \trianglelefteq R$ proper, then I is a prime if and only if whenever $a,b \in R$ such that $ab \in I$ then $a \in I$ or $b \in I$.

■ **Example 8.1 Examples of Prime Ideals**

1. $\langle n \rangle \trianglelefteq \mathbb{Z}, n > 1$ suppose n is prime. Let $a,b \in \mathbb{Z}$ such that $ab \in \langle n \rangle \implies n \mid ab \implies n \mid a$ or $n \mid b$ by Euclid's Lemma $\implies a \in \langle n \rangle$ or $b \in \langle n \rangle$. Thus, $\langle n \rangle$ is prime.
2. $I = \{a+bi : a,b \in 2\mathbb{Z}\} \trianglelefteq \mathbb{Z}[i]$ is not a prime ideal. Since $(1+i)(1+i) = 2i \in I$ but $1+i \notin I$.
3. Let $R = \mathbb{R}[x]$ and $I = \{f(x) : f(\pi) = 0\} \trianglelefteq R$. Since we can see that

$$R/I \cong \mathbb{R}$$

which is a field, so I must be maximal. But we give a proof as an exercise. Since $f(x) = x \notin I$ so $I \neq R$. Let $J \trianglelefteq R$ such that $I \subset J \subseteq R$, we show $J = R$. Let $0 \neq f(x) \in J$ such that $f(x) \neq I$. Thus, $f(\pi) \neq 0$, then let $g(x) = f(x) - f(\pi)$, then $g(\pi) = 0$, so $g(x) \in I$. Thus, $f(x) - g(x) \in J$ but $f(x) - g(x) = f(\pi) \in J$ but since $f(\pi) \neq 0 \implies f(\pi) \in R^\times$. Then, $J = R$. Thus, I is maximal.

■

R Let R be a commutative and unital ring. Let $a_1, a_2, \ldots, a_n \in R$, then

$$\langle a_1, a_2, \ldots, a_n \rangle = \cap \{I : I \trianglelefteq R, a_i \in I\}$$

see assignment section.

■ **Example 8.2 Prime but not maximal**
Let $R = \mathbb{Z}[x]$ and $I = \langle x \rangle$.

1. **Claim 1:** I is prime.
   Since $1 \notin I$ so $I \neq R$ and proper. Now, suppose $f, g \in R$ such that $fg \in I$, which means $f(0)g(0) = 0$, since $\mathbb{Z}$ is an ID, so either $f(0) = 0$ or $g(0) = 0$. Thus, either $f(x) \in I$ or $g(x) \in I$. Thus, I is prime.
2. **Claim 2:** I is not maximal.
   We give a larger ideal $\langle x \rangle \subset \langle x, 2 \rangle$ since $2 \notin \langle x \rangle$, the containment is proper. Suppose $\langle x, 2 \rangle = R$, then there exists $f, g \in R$ such that $1 = f(x)x + g(x)2 \implies 1 = 0 + g(0)2$, so 1 is even, which is a contradiction. Thus, I is not maximal.

In fact, for any p prime, $\langle x, p \rangle \trianglelefteq \mathbb{Z}[x]$ is a maximal ideal since

$$\mathbb{Z}[x] \Big/ \langle x, p \rangle \cong \mathbb{Z}_p$$

which is a field. ■

Theorem 8.1.1 The connection between quotients of prime ideals and ID (76er)
Let R be a commutative and unital ring. Let $I \trianglelefteq R$, then I is prime if and only if R/I is an ID

Demostración. 1. Suppose I is prime, then
   a) **Commutativity:** since R is commutative, R/I is commutative
   b) **Unital:** since $I \neq R$, so R/I is still unital (did not turn 1 into 0)
   c) **No zero divisors:** let $\overline{a}, \overline{b} \in R/I$ such that

$$\overline{a} \cdot \overline{b} = \overline{0} \implies \overline{ab} = \overline{0} \implies ab \in I \implies a \in I \text{ or } b \in I \implies \overline{a} = 0 \text{ or } \overline{b} = 0$$

   Thus, no zero divisors.
   Thus, R/I is an ID
2. Suppose R/I is an ID. Since unital and $I \neq R$. We have the proper containment already. Let $a, b \in R$ such that $ab \in I$, then

$$\overline{ab} = \overline{0} \implies \overline{a} \cdot \overline{b} = \overline{0} \implies \overline{a} = 0 \text{ or } \overline{b} = 0 \implies a \in I \text{ or } b \in I$$

   Thus, I is prime.

■

■ **Example 8.3** 1. $\mathbb{Z}[x] \Big/ \langle x \rangle \cong \mathbb{Z}$, since $\mathbb{Z}$ is ID, we have $\langle x \rangle$ is prime
2. $\mathbb{Z}[x] \Big/ \langle x, 4 \rangle \cong \mathbb{Z}_4$, since $\mathbb{Z}_4$ is not ID, we have $\langle x, 4 \rangle$ not prime
3. $\mathbb{Z}[x] \Big/ \langle x, p \rangle \cong \mathbb{Z}_p$ for any prime p. We have $\mathbb{Z}_p$ a field and $\langle x, p \rangle$ is a maximal ideal in $\mathbb{Z}[x]$.

■

8.2 Supportive Section: Set Theory

Definition 8.2.1 Partial Order
A relation $\leq$ is a partial order on X if

1. $\forall x \in X, x \leq x$
2. If $x \leq y, y \leq x$, then $y = x$ for all $x, y \in X$
3. If $x \leq y, y \leq z$, then $x \leq z$ for all $x, y, z \in X$

If $\leq$ is a partial order on X, we call $(X,\leq)$ is a poet.

Example 8.4 Examples of Posets

1. $X=\mathscr{P}(\mathbb{N})$ and $(X,\leq)$ is a poset
2. $X=\mathbb{R}$ and $(X,\leq)$ is poset
3. $X=\{(a_n)_n : a_i\in\mathbb{R}\}$ with the lexicagraphic ordering which means

$$(a_n)\leq(b_n)\iff \exists N\in\mathbb{N} \text{ such that } a_n=b_n \text{ for } n<N \text{ and } a_N<b_N$$

R $(X,\leq)$ be a poset, we do not insist that $\forall x,y\in X, x\leq y$ or $y\leq x$. If such $\leq$ does have this property, we call $\leq$ a **total order**.

4. $(\mathscr{P}(\mathbb{R}),\subseteq)$ is not a totally ordered poset.

■

Definition 8.2.2 Toset
$(X,\leq)$ is a poset. If $A\subseteq X$ and $(A,\leq)$ is a totally ordered poset, we call A a toset (chain)

Definition 8.2.3 Upper Bound
Let $(X,\leq)$ be a poset, $A\subseteq X$. An upper bound for A is an element $x\in X$ such that $a\leq X, \forall a\in A$ (upper bound is not necessarily in A)

Definition 8.2.4 Maximal
Let $(X,\leq)$ be a poset, we say $x\in X$ is maximal if there does not exist $y\in X$ such that $x\neq y$ and $x\leq y$.

Theorem 8.2.1 Zorn's Lemma
Let $(X,\leq)$ be an non-empty set (this is important). If every totally ordered subset of X has an upper bound in X, then X has a maximal element.

Theorem 8.2.2 Every proper ideal of a unital ring is contained in a maximal ideal (76er)
Let R be a unital ring. Every proper ideal I of R is contained in a maximal ideal. In particular, taking $J=\langle 0\rangle$, R has a maixmal ideal.

Demostración. Let $I\trianglelefteq R$ and $I\neq R$. Consider $X=\{J\trianglelefteq R : I\subset J, J\neq R\}$ Then $(X,\subseteq)$ is a poset by inclusion. Since $I\in X, X\neq\emptyset$, Y be a totally ordered subset of X. Let $J=\cup_{A\in Y}A$, so $I\subseteq J$.
Claim: $J\trianglelefteq R, J\neq R$.
Let $a,b\in J$ and $r\in R$, then $a\in A, b\in B$ for some $A,B\subset Y$. Since Y is totally ordered, we may assume $A\subseteq B$. Since $B\trianglelefteq R$, $a-b, ra, ar\in B$. Hence $a-b, ra, ar\in J$, thus $J\trianglelefteq R$.
Suppose $J=R$, then $1\in J$ and $1\in A$ for some $A\in Y$ but $A\in X$ means it cannot contain a unit. Contradiction. Thus, $J\neq R$ and $J\in X$.
Moreover, for $A\in Y, A\leq J$ and so J is an upper bound for $Y\in X$. By Zorn's Lemma, X has a maximal element. ■

R If $I,J\trianglelefteq R$, then $I+J=\{a+b : a\in I, b\in J\}\trianglelefteq R$

Theorem 8.2.3 The connection between quotients of maximal ideals and fields (76er)
Let R be a commutative and unital ring. Let $I \trianglelefteq R$, then R/I is a field if and only if I is maximal.

Demostración.

1. Suppose R/I is a field. Since it is unital and $I \neq R$. Let $J \trianglelefteq R$ such that $I \subset J \subseteq R$ and let $a \in J$ such that $a \notin I$. Then $\overline{0} \neq \overline{a} \in R/I$ and there exists $\overline{b} \in R/I$ such that $\overline{a} \cdot \overline{b} = \overline{1}$, so $\overline{ab-1} = \overline{0} \Longrightarrow ab-1 \in I \subset J$. But since $a \in J$, we know $ab \in J$, then $1 \in J$, Thus, $J = R$. Therefore, I is maximal.
2. Suppose I is a maximal ideal in R. Then, $I \neq R$ and R/I is commutative and unital by inheritance. We only need to check the inverses. Let $\overline{0} \neq \overline{a} \in R/I$, then $a \notin I$, so let $J = I + \langle a \rangle = R$ since I is maximal. Then,

$$\exists x \in I, b \in R, s.t, 1 = x + ab \Longrightarrow \overline{1} = \overline{a}\overline{b}$$

Thus, $\overline{a}$ is invertible with $\overline{0} \neq \overline{b} \in R/I$. Thus, R/I is a field.

■

Corollary 8.2.4 Every maximal ideal of R is prime (Commutative Version)
Let R be a commutative and unital ring. Every maximal ideal of R is prime. (This is extended to only unital rings in assignment section)

Exercise 8.1 Let $1 \neq d \in \mathbb{Z}$ be square-free. Then, $\{0\} \neq P \trianglelefteq \mathbb{Z}[\sqrt{d}]$ be a prime ideal, then P is maximal. ■

Demostración. Let $0 \neq a + b\sqrt{d} \in P$. Note that

$$(a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \neq 0$$

and let $N = a^2 - db^2 \in P$. Since P is a prime ideal, we know that R/P is an ID and

$$R/P \subseteq \{\overline{a} + \overline{b}\sqrt{\overline{d}} : 0 \leq a, b < N\}$$

which is a finite ID. This implies that R/P is a field. Then, we know that P must be maximal. ■

9. ED & PID & UFD

9.1 Euclidean Domain

Definition 9.1.1 gcd

Let R be a commutative and unital ring

1. We say d divides a, $d|a$ if there exists $x \in R$ such that $a = dx$
2. We say d is a common divisor of a and b, if $d|a$ and $d|b$
3. We say d is **a** greatest common divisor of a, b and whenever c is a common divisor of a, b, then $c|d$. Denote such a gcd as $d = \gcd(a,b)$

Definition 9.1.2 Euclidean Domain (ED)

Let R be an ID. A norm on R is a function $N : R \to \mathbb{N} \cup \{0\}$ such that $N(0) = 0$. We say R is an Euclidean Domain if there exists a norm N on R such that for all $a, b \in R, b \neq 0$, there exists $q, r \in R$ such that

$$a = bq + r$$

with $r = 0$ or $N(r) < N(b)$.

R **Z is an ED**

Let $R = \mathbb{Z}$ and $a, b \in R, b \neq 0$, we have

$$a = bq + r, 0 \leq r < |b|$$

Take $N(x) = |x|$

■ **Example 9.1 Examples of ED**

1. If F is a field, then $F[x]$ is an ED with $N(f(x)) = \deg f(x)$
2. If F is a field, then F is an ED with $N(x) = 0$

■

Exercise 9.1 $\mathbb{Z}[i]$ **is an Euclidean domain**

Demostración. Let $R=\mathbb{Z}[i]$. The norm is $N(a+bi)=a^{+}b^{2}$. Let $x=a+bi$ and $y=c+di\in R$, $y\neq 0$. Note taht $\mathbb{Q}(i)$ is a field. Then, $xy^{-1}=\alpha+\beta i\in\mathbb{Q}(i)$. Let $x+yi\in R$ such that $|p-\alpha|\leq\frac{1}{2}$ and $|q-\beta|\leq\frac{1}{2}$. Thus,

$$x=y(p+qi)-y(p+qi)+x$$

say $r=x-y(p+qi)=y(\alpha_{\beta}i)-y(p+qi)=y((\alpha-p)+(\beta-q)i)$. Suppose $r\neq 0$, otherwise, we are done. Then

$$N(r)=N(y)N((\alpha-p)+(\beta-q)i)=N(y)[(\alpha-p)^2+(\beta-q)^2]<\frac{1}{2}N(y)<N(y)$$

Thus, R is an ED. ■

■

Theorem 9.1.1 **ED$\Longrightarrow$PID (76er)**
If R is an ED, then R is an PID.

Demostración. Let $I\trianglelefteq R$, if $I=\langle 0\rangle$, we are done. Otherwise, take $0\neq x\in I$ of the smallest norm. We claim that $I=\langle x\rangle$. Clearly, $\langle x\rangle\subseteq I$. Take $y\in I$, then there exists $q,r\in R$ such that

$$y=xq+r$$

with $r=0$ or $N(r)<N(x)$. But x is of minimum norm, so $r=0$. Thus, $y\in\langle x\rangle$ and $I=\langle x\rangle$ as a principal ideal. ■

Proposition 9.1.2 **Principal Ideal Generator**
Let R be a commutative and unital ring. Let $a,b\in R$ be nonzero. If $I=\langle a,b\rangle$ is principal, then $I=\langle d\rangle$ for any $d=\gcd(a,b)$.

Definition 9.1.3 **Associates**
Let R be a commutative and unital ring. We $a,b\in R$ are associates if $a=ub$ for some $u\in R^{\times}$.

Proposition 9.1.3 **Associates and Principal Ideals**
Let R be an ID, and $a,b\in R$. a,b are associates if and only if $\langle a\rangle=\langle b\rangle$. Moreover, if a,b are nonzero, and d,d' are gcds of a,b, then d,d' are associates. (Ask prof: why R needs to be an ID?)

R **Bezout's Lemma**
Let R be a commutative and unital ring, and $\langle a,b\rangle=\langle d\rangle$ with $a,b\neq 0$, then $d=ax+by,x,y\in R$.

Theorem 9.1.4 **Euclidean Algorithm**
Let R be an ED, $a,b\in R$ nonzero.

1. If $b\big|a$, then $\gcd(a,b)=b$

2. If $b \nmid a$, then

$$a = bq_0 + r_0, b = r_0 + q_1 + r_1, r_0 = r_1q_2 + r_2, \ldots, r_{n-2} = r_{n-1}q_n + r_n, r_{n-1} = r_nq_{n+1} + 0$$

Thus, r_n is the $\gcd(a,b)$.

Exercise 9.2 We know that the polynomial ring over a field an ED, find the gcd of the following two polynomials in $\mathbb{Z}_2[x]$

$$f(x) = x^5 + x^2 + x + 1 \qquad g(x) = x^3 + x^2 + x + 1$$

by long division, we have

$$\gcd(f(x), g(x)) = x^2 + 1$$

■

9.2 Principal Ideal Domain

Definition 9.2.1 Principal Ideal Domain (PID)
Let R be an ID, we say R is a principal ID (PID), if every ideal of R is principal.

R **Existence of gcd in PID**
Let R be a PID, $0 \neq a, b \in R$ such that $\langle a, b\rangle = \langle d\rangle$ since it is a PID. Thus, $d = \gcd(a,b)$ always exists.

■ **Example 9.2 Examples of PID**

1. All EDs are PID
2. $\mathbb{Z}[x]$ is an ID but not a PID (thus not ED). Consider $I = \langle x, 2\rangle$, note that

$$\mathbb{Z}[x] \big/ I \cong \mathbb{Z}_2$$

is a field. Thus, I is maximal in $\mathbb{Z}[x]$. Suppose for a contradiction that $I = \langle f(x)\rangle$, then

$$x = f(x)g(x), 2 = f(x)g(x), g, h \in \mathbb{Z}[x]$$

Based on degrees, we have $f(x) \in \{\pm 1, \pm 2\}$. Since I is maximal, it is proper. We can only have $f(x) = \pm 2$. Then, $x = \pm g(x)$ but this is impossible in $\mathbb{Z}[x]$. Contradiction. Therefore, $\mathbb{Z}[x]$ is not a PID.
3. **PID is not necessarily an ED** check Dummit and Foote P277,281,282

■

Theorem 9.2.1 Nonzero Prime Ideals Are Maximal in PID (76er)
Every nonzero prime ideal in a PID is maximal.
WARNING:
This is not true for $\langle 0\rangle$. Even though it is indeed prime, but not maximal and $\mathbb{Z} \big/ \langle 0\rangle \cong \mathbb{Z}$, which is an ID not a field.

Demostración. Let $0 \neq P \trianglelefteq R$ be a prime ideal where R is a PID. Say $P = \langle a\rangle, a \in R$. Let $J \trianglelefteq R$ such that $\langle a\rangle \subseteq J \subseteq R$, say $J = \langle b\rangle, b \in R$. So, $a \in \langle b\rangle \Longrightarrow a = bx, x \in R$. Since P is prime, $x \in P$ or $b \in P$.

1. If $b \in P$, then $J \subseteq \langle a \rangle$, so $J = P$
2. If $x \in P$, then $x = ay, y \in R$ and $a = bx = aby$ means that $by = 1$ since we are in an ID at least. Thus, $b \in R^\times$ and $J = R$.

From both case, we see that P is maximal in R. ■

Proposition 9.2.2 $R[x]$ **PID** $\iff$ R **Field**

Definition 9.2.2 Irreducible & Reducible & Prime
Let R be an ID. Let $x \in R$ be a nonzero and non-unit element.

1. We say x is irreducible if whenever $x = ab, a, b \in R$, then $a \in \mathbb{R}^\times$ or $b \in R^\times$; otherwise, we say x is reducible (nonzero, nonunit as well)
2. We say x is prime if whenever $x \mid ab, a, b \in R$, then $x \mid a$ or $x \mid b$.

R

1. In $\mathbb{Z}$: the primes are $\pm p$ with p prime numbers
2. x is prime if and only if $\langle x \rangle$ is prime (besides the zero ideal)

Proposition 9.2.3 Prime $\implies$ Irreducible (ID)
Let R be an ID and $x \in R$ is prime, then x is irreducible.

Theorem 9.2.4 Irreducible $\iff$ Prime (PID) (76er)
Let R be a PID and $x \in R$ if and only if x is irreducible.

Demostración. One direction is done by the previous proposition. Let $p \in R$ be an irreducible, so $p \notin R^\times$ and $p \neq 0$. We show $\langle p \rangle$ is prime. Let M be a maximal ideal of R which contains $\langle p \rangle$. Say $M = \langle m \rangle$, $m \in R$. Since R is PID, we have

$$p \in \langle m \rangle \implies p = mx, x \in R \implies m \in R^\times \text{ or } x \in R^\times$$

but we know $\langle m \rangle$ is maximal and proper, so it cannot contain any units. Thus, $x \in R^\times$. Then, it means that $\langle p \rangle = \langle m \rangle$ by associates. Thus, $\langle p \rangle$ is maximal and implies that it is prime. ■

Corollary 9.2.5 Let R be a PID and $x \in R$, then $\langle x \rangle$ is maximal if and only if x is irreducible.

Exercise 9.3 Let $R = \mathbb{Z}[\sqrt{-5}]$, prove that 2 is irreducible but not prime to show that R is not a PID.

Demostración. Note that

$$(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3$$

So $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$ but there does not exist $a, b \in \mathbb{Z}$ such that $1 \pm \sqrt{-5} = 2(a + b\sqrt{-5})$ by parity. Thus, 2 is not prime in R.
We claim 2 is irreducible. Note that $2 \neq 0, 2 \notin R^\times$ since $N(2) \neq 1$. Suppose $2 = xy, x, y \in R$, then

$$N(2) = N(x)N(y) = 4$$

so, $N(x), N(y) \in \{1,2,4\}$. Note that $N(a+b\sqrt{-5}) = a^2+5b^2 = 2$ has no integer solution. So, one of $N(x), N(y)$ must be 1. Hence, $x \in R^\times$ or $y \in R^\times$. This implies that 2 is an irreducible. And we conclude that R is not a PID. ■

■

9.3 Unique Factorization Domain

Definition 9.3.1 Unique Factorization Domain (UFD)
Let R be an ID, we say R is a unique factorization domain (UFD) if every nonzero, non-unit element can be uniquely written as a product of irreducibles in R, up to reordering and associates.

■ **Example 9.3 Examples of UFD**

1. $\mathbb{Z}$ prime factorization
2. Every field is a UFD in a vacously true fashion since all elements are in $R^\times$

■

Theorem 9.3.1 Irreducible $\iff$Prime (UFD) (76er)
Let R be a UFD, the every irreducible is prime.

Demostración. One direction is followed from ID. Let $p \in R$ be an irreducible. In particular, $0 \neq p$ and $p \notin R^\times$, suppose $x, y \in R$ such that $p \mid xy$, then, $xy = pz$ for some $z \in R$. By uniqueness, p must be an associate of an irreducible factor of x or an irreducible factor of y. WLOG, say $p = uq$ where $u \in R^\times$ and q is an irreducible factor of x. Then, $u^{-1}p = q$ implies that $p \mid q$ and $q \mid x$, so $p \mid x$. Thus, p is prime. ■

Definition 9.3.2 Noetherian
Let R be a ring, we say R is Noetherian if whenever

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

is a chain of ideals of R there exists $N \in \mathbb{N}$ such that $I_k = I_N$ for $k \geq N$.

■ **Example 9.4 Examples of Noetherian**

1. $\mathbb{C}[x_1, x_2, x_3, \dots]$ is not Noetherian, since we can just keep extending the chain like

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \langle x_1, x_2, x_3 \rangle \subset \dots$$

2. All finite rings are Noetherian

■

Lemma 9.4 PID$\Longrightarrow$Noetherian (76er)
Let R be a PID, then R is Noetherian.

Demostración. Let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

be a chain of ideals of R, then

$$I = \bigcup_{i=1}^{\infty} I_i \trianglelefteq R$$

(totally ordered ideals' union is an ideal)
Since R is PID, I is principal. Say $I = \langle a \rangle$ for some $a \in R$. Thus, the exists $N \in \mathbb{N}$ such that $a \in I_N$ and this implies that $I = I_N$ and $I_k = I_N = I$ for all $k \geq N$. R is Noetherian. ■

Theorem 9.4.1 Every PID is a UFD

R Associate of an irreducible is still irreducible.

Definition 9.4.1 Fields of Fractions (f.o.f)
Let R be an ID, then the fields of fractions of R (indeed a field) is

$$F = \left\{ \frac{r}{s} : r,s \in R, s \neq 0 \right\}$$

Theorem 9.4.2 Gauss' Lemma (76er)
R is a UFD, F is a field of fractions. Let $f(x) \in R[x]$. Suppose $f(x) = A(x)B(x)$ in $F[x]$ be non-constant factorization of f, then there exists $a(x), b(x) \in R[x]$ such that

$$f(x) = a(x)b(x)$$

with $\deg a(x) = \deg A(x)$, $\deg b(x) = \deg B(x)$.

Demostración. Say $f(x) = A(x)B(x)$ in $F[x]$. Then, by clearing denominators, there exists $0 \neq d \in \mathbb{R}$ such that $df(x) = \alpha(x)\beta(x)$ where $\alpha(x), \beta(x)$ are R-multiples of $A(x), B(x)$ respectively. Hence, $\deg \alpha(x) = \deg A(x)$ and $\deg \beta(x) = \deg B(x)$. Note that if $d \in R^\times$. Otherwise, suppose $d \notin R^\times$. Since R is UFD, we can factor d into irreducibles in R and let p be an irreducible factor of d. Then, $\langle p \rangle$ is prime and consider the claim

$$(R/\langle p \rangle)[x] \cong R[x]/\langle p \rangle [x]$$

we know the left hand side is an Integral Domain. Now, in $(R/\langle p \rangle)[x]$. Note that in this ID,

$$df(x) = \alpha(x)\beta(x) \in F[x] \Longrightarrow 0 = \tilde{\alpha}(x)\tilde{\beta}(x) \in (R/\langle p \rangle)[x]$$

by reducing coefficients mod $\langle p \rangle$. WLOG, $\tilde{\alpha}(x) = 0$ since we are dealing with ID. Therefore, $p \mid \alpha(x)$ in $R[x]$. Since we are in ID, we may cancel p from both sides of the equation

$$df(x) = \alpha(x)\beta(x)$$

continuing this way, we can cancel all prime factors of d until it has no prime factors left and becomes a unit, then say $u \in R^\times$,

$$uf(x) = a'(x)b(x)$$

where $\deg a'(x) = \deg A(x)$, $\deg b(x) = \deg B(x)$, where $a'(x), b(x) \in R[x]$. Let

$$a(x) = u^{-1}a'(x)$$

and we are done. ■

R Note that the we have R-multiples of $a(x)$ as $A(x)$... This might be useful

Corollary 9.4.3 Let R be a UFD, F be a fields of fractions, say $f(x) \in F[x]$. We have the following results:

1. If $f(x)$ is reducible over F, then $f(x)$ is reducible over R.**(Reducibility Check)**
2. If $f(x)$ is irreducible and **non-constant** in $R[x]$, then $f(x)$ is irreducible in $F[x]$.
3. Suppose a gcd (common divisor of all of them) of the coefficients of $f(x)$ is 1, then $f(x)$ is irreducible over R if and only if $f(x)$ is irreducible over F.

Demostración. We first have the example of a monic polynomial to satisfy this.
Why? One direction is by the second corollary of Gauss
Now, suppose $f(x)$ is irreducible over F, say

$$f(x) = g(x)h(x) \in R[x]$$

but then, the $\deg g(x) = 0$ or $\deg h(x) = 0$ since the units in $F[x]$ are non-zero constants. WLOG, say $g(x) = d \in R$ and we have $f(x) = dh(x)$. Then, $d \mid 1$ and $d \in R^\times$. ■

■ **Example 9.5** Note that $2 \in \mathbb{Z}[x]$ is irreducible, but $2 \in \mathbb{Q}[x]$ is **not irreducible**.

■ **Example 9.6** $2x \in \mathbb{Z}[x]$ is reducible in $\mathbb{Z}[x]$ (since 2 is irreucible in $\mathbb{Z}[x]$), but irreducible in $\mathbb{Q}[x]$. ■

■

Proposition 9.4.4 Let R be a UFD if and only if $R[x]$ is a UFD.

Demostración. If $R[x]$ is a UFD, it is quite clear that R is a UFD.
For the converse, suppose R is a UFD.

1. **Existence:** Let $0 \neq f(x) \in R[x]$ such that $f(x) \notin R^\times$. If $\deg f(x) = 0$, we are done since R is UFD. Assume $\deg f(x) > 0$. Let d be the gcd of the coefficients of $f(x)$. Then, $f(x) = dg(x)$ where $\deg f(x) = \deg g(x)$ with $g(x) \in R[x]$ and a gcd of the coefficients of $g(x)$ is 1. By replacing $f(x)$ with $g(x)$ if necessary, we may assume $d = 1$. Let F be the field of fractions of R. Then, $F[x]$ is Euclidean domain (implies PID and UFD). We know

$$f(x) = Q_1(x) \dots Q_n(x)$$

in $F[x]$, where $Q_i(x)$ irreducible in $F[x]$. Then, by applying Gauss' Lemma inductively, we have

$$f(x) = P_1(x) \dots P_n(x)$$

in $R[x]$, where $P_i(x)$ is a R-muliple of $Q_i(x)$. Thus, $P_i(x)$ is irreducible in $F[x]$. Since a gcd of the coefficients of $P_i(x)$ is 1, $P_i(x)$ is irreducible in $R[x]$.
2. **Uniqueness:** Let $0 \neq f(x) \in R[x]$ such that $f(x) \notin R^\times$. WLOG assume a gcd of the coefficients' of $f(x)$ is
   a) Let F be the field of fractions of R. Say

$$Q_1(x)Q_2(x) \dots Q_m(x) = f(x) = P_1(x)P_2(x) \dots P_n(x)$$

where $P_i(x), Q_j(x) \in R[x]$ are irreducibles. Since a gcd of the coefficients of each $P_i(x), Q_j(x)$ is 1 due to the fact that we already get rid of d. Then, by the corollary of Gauss' Lemma, we have each $P_i(x), Q_j(x)$ are inrreducibles in $F[x]$. Note that $F[x]$ is an Euclidean Domain (UFD), we have $m = n$ and WLOG each $P_i(x)$ is an associate (in $F[x]$) of $Q_i(x)$ $i = 1, 2, \dots, n$. For each i,

$$P_i(x) = \frac{a}{b}Q_i(x), 0 \neq \frac{a}{b} \in F, (a, b \in R)$$

This implies that

$$bP_i(x) = aQ_i(x)$$

then, a and b are gcds of the coefficients of this polynomial. Thus, from before, we have that $a = ub$ where $u \in R^\times$. Therefore, we got that

$$bP_i(x) = ubQ_i(x) \Longrightarrow P_i(x) = uQ_i(x)$$

as required.

■

■ **Example 9.7** We know that $\mathbb{Z}$ is UFD, and $Z[x]$ is a UFD, which is **not a PID**! ■

■ **Example 9.8** Let R be a UFD, then $R[x_1]$ is a UFD, inductively, we have

$$R[x_1][x_2]\dots[x_n] = R[x_1, x_2, \dots, x_n] \textbf{ is a UFD}$$

■

9.5 PMATH347 Final Exam

1. Tuesday Aug 13, 12:30-3:00 PM, MC1085
2. Office Hours: Aug 7,8,12 from 1:00 to 2:30
3. There are 7 questions, 10 marks each, and 70 marks in total
   a) [4,3,3] Elementary Ring Theory
   b) [3,3,4] Prime vs. Maximal Ideals
   c) [3,4,3] Group Theory
   d) [2,5,3] Group Actions
   e) [3,3,4] Integral Domain and Fields
   f) [3,3,4] Divisability in Integral Domain
   g) [10] Example and DNE

Good Luck On the Final Exam!!!

III Assignment Section

10 Group Related Results 48

11 Ring Related Results 51

10. Group Related Results

1. Let G. If every element of G has finite order, then G is not necessarily a finit group since

$$(\mathbb{Z}_2[x],+)$$

has order 2 for every element, but infinite size
2. Let G be a group. If G has finitely many subgroups, then G is a finite group.
3. Let $G=\mathbb{Z}_{11}^{\times}$, the generators of G is given by

$$\{8^m : \gcd(10,m)=1, 1\leq m\leq 10\}=\{8,6,2,7\}$$

4. If G is a abelian and $a,b\in G$ with $\gcd(|a|,|b|)=1$, then $|ab|=\operatorname{lcm}(|a|,|b|)$
5. If $\gcd(m,n)=1$, then $\mathbb{Z}_n\times\mathbb{Z}_m$ is cyclic.
6. The normalizer of $H\leq G$ in a group is the largest group of G that contains H as a normal subgroup.

$$N_G(H)=\{g\in G : gHg^{-1}=H\}$$

7. Let G be a group and let $H,K\leq G$ and consider

$$HK=\{hk : h\in H, k\in K\}$$

   a) Example such that G,H,K such that $HK\not\leq G$:

$$G=S_3, H=\langle(12)\rangle, K=\langle(23)\rangle, HK=\{e,(12),(23),(12)(23)\}$$

   since $(12)(23)=(123)$ and $(123)^2=(132)\notin HK$.
   b) If $H\leq N_G(K)$, then $HK\leq G$
   c) If $K\trianglelefteq G$, then $HK\leq G$ (trivial from above, since $N_G(K)=G$ and $H\leq G=N_G(K)$)
8. If $G/Z(G)$ is cyclic, then G is abelian
9. Example of a group G such that $G/Z(G)$ is abelian but G is not abelian"

$$G=Q$$

the quaternion group. Then, $Z(G) = \{-1, 1\}$, $G/Z(G)$ is abelian since every element has at most order 2 but G is not abelian.

10. Let p, q be primes, if G is a group of order pq, then G is abelian or $Z(G) = \{e\}$.

Theorem 10.0.1 Correspondence Theorem

a) Let G be a group, let $N \trianglelefteq G$ and $H \leq G$ such that $N \leq H$, then $N \trianglelefteq H$ and $H/N \leq G/N$.
b) Let G be a group and let $N \trianglelefteq G$, then every subgroup $\overline{H} \leq G/N$ is of the form $\overline{H} = H/N$ for some $H \leq G$ containing N.
c) Let G be a group and let $N \trianglelefteq G$, then every normal subgroup $\overline{H} \trianglelefteq G/N$ is of the form $\overline{H} = H/N$ for some $H \trianglelefteq G$ containing N.

12. Let G be a group and $a, b \in G$. The commutator of a, b is defined to be

$$[a,b] = aba^{-1}b^{-1}, [G,G] = \langle [a,b] : a,b \in G \rangle$$

is the smallest subgroup of H of G such that G/H is abelian.

13. Q, D_8 are not isomorphic since Q has every subgroup to be normal but not true for D_8
14. $\mathbb{Z}_2 \times \mathbb{Z}_3 \ncong \mathbb{Z}_{12}$, one is cyclic, and one is not.
15. $S_4 \ncong D_8 \times \mathbb{Z}_3$, since S_4 has a trivial centre while $(e,2) \in Z(D_8, \mathbb{Z}_3)$
16. If $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ is a homomorphism, then $\varphi(x) = ax$ for some $a \in \mathbb{Z}_m$

Theorem 10.0.2 Second Isomorphism Theorem
Let G be a group and let A, B be subgroups of G such that $A \leq N_G(B)$, then $B \trianglelefteq AB$ and $A \cap B \trianglelefteq A$, and

$$AB/B \cong A/A \cap B$$

the homormorphism needed here is $\varphi : AB \to A/A \cap B$ with $\varphi(ab) = \overline{a}$

Theorem 10.0.3 Third Isomorphism Theorem
Let G be a group and let $A, B \trianglelefteq G$ with $A \leq B$. Prove that $B/A \trianglelefteq G/A$ and

$$(G/A)/(B/A) \cong G/B$$

the homomorphism needed here is $\varphi : G/A \to G/B$ with $\varphi(gA) = gB$

17. Let G be a finite group, then
    a) suppose $H \leq G$ such that $[G : H] = n$, then there exists a homomorphism $\varphi : G \to S_n$ defined in terms of how g permutes the left cosets of H in G when G acts on G/H by left multiplication.
    b) suppose $H \leq G$ such that $[G : H] = n$, let K be the kernel, then $K \subseteq H$ and G/K is isomorphic to a subgroup of S_n.
    c) Suppose $H \leq G$ such that $[G : H] = p$ where p is the smallest prime dividing the order of G. Prove that H is normal in G.
18. Let G be a finite group and $H, K \leq G$, then

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

19. Six non-isomorphic groups of order p^4, where p is a prime:
    a) **Abelian:** easy to write down, 5 of them

b) **Non-abelian:**

$$\left\{ \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} : x, y, z \in \mathbb{Z}_p \right\} \times \mathbb{Z}_p$$

11. Ring Related Results

1. The following are not subrings of $F(\mathbb{R})$:
   a) $I = \{f \in F(\mathbb{R}) : f(x) \geq 0, \forall x \in \mathbb{R}\}$ since $f(x) = x^2 \in I$ but $-f \notin I$
   b) $I = \{f \in F(\mathbb{R}) : f(-x) = -f(x), \forall x \in \mathbb{R}\}$ since $\sin(x) \in I$ but $f^2 \notin I$
   c) $I = \{f \in F(\mathbb{R}) : f$ has finitely many zeros in the interval $(0,1)\} \cup \{0\}$ since

$$f(x) = \begin{cases} \cos(1/x) & x \neq 0 \\ 0 & x = 0 \end{cases}$$

   note that $f \notin I$ but $f + 2, 2 \in I$.
   d) $I = \{f \in F(\mathbb{R}) : f$ has infinitely many zeros in the interval $(0,1)\}$ since

$$f(x) = \begin{cases} 1 & x \in \mathbb{Q} \\ 0 & x \notin \mathbb{Q} \end{cases} \qquad g(x) = \begin{cases} 1 & x \notin \mathbb{Q} \\ 0 & x \in \mathbb{Q} \end{cases}$$

2. If R is a ring and $f, g \in R[x]$, then not necessarily $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$ since there might be zero divisors in $R[x]$
3. If R is a ring such that $r^2 = r, \forall r \in R$, then R is commutative (this is nice!)
4. If $S \leq R$ of finite order, then $|S|$ divides $|R|$ by Lagrange within the underlying additive group
5. If R is commutative and unital ring such that $char(R) = p$ is prime, then for all $a, b \in R$, $(a+b)^p = a^p + b^p$
6. If R is a finite unital ring and $R^\times$ is a group of odd order, then $char(R) = 2$
7. A left zero-divisor is not necessarily a right zero divisor in a non-commutative ring. The example is the unilateral shift operator on the vector space of infinite sequences.
8. Every nonzero element of $M_n(\mathbb{R})$ is either a unit or a zero divisor.
9. For a norm N, we have
   a) $N(x) = 0 \iff x = 0$
   b) $\forall x, y \in R, N(xy) = N(x)N(y)$
   c) $x \in R$ is a unit $\iff N(x) = 1$
10. Let R, S be rings and $\varphi : R \to S$ be a homomorphism and $S \neq \{0\}$.

a) If φ is surective and R is unital, then S is unital
b) Example of a homomorphism such that R is unital and S is non-unital

$$\varphi : \mathbb{Z} \to \mathbb{Z} \oplus 2\mathbb{Z}$$

by $\varphi(x) = (x,0)$.
c) Example of a homomorphism such that R,S are unital but the unity of S is not $\varphi(1)$:

$$\varphi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$$

by $\varphi(x) = (x,0)$ but $(1,0) \neq (1,1)$
d) If φ is surjective, R is unital, and $char(R)$ is positive, then $char(S) \leq char(R)$
e) Let $J \trianglelefteq S$, then

$$\varphi^{-1}(J) = \{x \in R : \varphi(x) \in J\}$$

is an ideal of R.

11. Every ideal of $M_n(R)$ is of the form $M_n(I)$ where $I \trianglelefteq R$.
12. The only ideals of $M_n(F)$, where F is a field, are $\langle 0 \rangle$ and $M_n(F)$

Theorem 11.0.1 Chinese Remainder Theorem
If R is commutative and unital ring, and I,J are comaximal ideals of R, then

$$R \Big/ (IJ) \cong R \Big/ I \oplus R \Big/ J$$

the needed isomorphism is

$$\varphi : R \to R \Big/ I \oplus R \Big/ J$$

$\varphi(x) = (\overline{x},\overline{x})$

13. Let R be a unital ring and let I be a proper ideal of R, then there exists a prime ideal $P \trianglelefteq R$ such that $I \subseteq P$ and whenever P' is a prime ideal of R such that $I \subseteq P' \subseteq P$, then $P' = P$
14. Let R be a commutative and unital ring. Let $I = \cup\{P : P \trianglelefteq R \text{ is prime}\}$. As I is an intersection of ideals, it is itself an ideal, then every element of I is nilpotent.
15. $R = \mathbb{Z}[x,y] = \mathbb{Z}[x][y]$ is a PID if and only if $\mathbb{Z}[x]$ is a field, which is not. Thus, R is not a PID and not an ED.
16. Let R be a unital ring, then every maximal ideal of R is prime.
17. Example of an ideal $I \trianglelefteq R = 2\mathbb{Z}$ that is maximal but not prime: $4\mathbb{Z}$
18. $\mathbb{Z}[i], \mathbb{Z}[\sqrt{-2}]$ are EDs but $\mathbb{Z}[\sqrt{-n}]$ $n \geq 3$ square-free are not UFD (Ask prof: what's role of square-free playing here?)
19. $n > 1$ is a square-free such that $n = 1 \mod 4$ then $\mathbb{Z}[\sqrt{n}]$ is not UFD. (the general ideal is to show something that is irreducible but not prime! 2 is a solid choice for a lot of these questions...)

Good Luck On Your PMATH347 Final!
Last Updated: 08/08/2019