Adam Van Tuyl

Groups and Rings

McMaster University

Department of
Mathematics &
Statistics

McMaster University
Department of Mathematics & Statistics

Adam Van Tuyl

Groups and Rings

MATH 4GR3 — 2024

Course notes illustrated, adapted and edited by Zachary Lucier

Last updated December 1, 2024

This page is left blank intentionally.

Notes from the Editor

Working on a project of this scale is no easy feat! I really could not have done this alone.

I would like to extend my sincerest gratitude to Dr. Adam Van Tuyl for making me fall in love with algebra and for filling in the gaps from my previous Galois Theory instruction.

I would also like to thank and recognize Jeanne Lin for providing handwritten notes from the lectures. These were immensely helpful, especially for the few days I couldn't make it to lecture—I really could not have done this without you.

Finally, a big thank you to all my classmates that supported and motivated me to bring this project to completion. I have made similar attempts in other courses with varying degrees of success, and the distinguishing factor was accountability.

To the reader,

I hope this text inspires and motivates you to study! The main reason for developing this template and style was to break free of the monotony I endured with texts in all of my previous undergraduate mathematics courses. They all lacked contrasting visual cues that distinguished theorems from definitions and examples, etc., all used the same font and, most of all, they lacked colour.

This resource is for the budding algebraist and fellow aesthete. What better way to uncover the beauty of algebra than in an equally beautiful package?

Happy reading,

Zachary Lucier

Foreword

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nam a nulla efficitur, tristique nulla ac, tincidunt orci. Cras consectetur accumsan arcu non bibendum. Aliquam mi massa, congue sit amet sagittis nec, efficitur eget justo. Curabitur elementum eu ante vel blandit. Quisque in nibh hendrerit, feugiat ex a, auctor turpis. Vivamus eget elit vitae urna lacinia euismod vitae tempor ante. Cras eu dignissim eros. Cras condimentum eu velit ut rhoncus.

Etiam venenatis magna orci, vitae mollis ex volutpat id. Cras non dignissim est, at lobortis risus. Aliquam vel libero ultricies, elementum magna sit amet, pretium ante. Morbi non mauris nisi. Donec ultricies porta neque viverra dictum. Pellentesque sollicitudin enim mauris. Donec malesuada sagittis elit sit amet consequat. Aliquam scelerisque tellus sit amet nisi tempor, molestie faucibus nulla vestibulum. Nam vitae molestie dui. Mauris mollis lectus et est porttitor malesuada.

Morbi vel odio ullamcorper, tincidunt tellus eu, convallis purus. Morbi rutrum leo non sem placerat, at eleifend dolor molestie. Nulla nec placerat enim. Morbi porttitor, lectus et suscipit elementum, neque arcu pulvinar sem, eu facilisis sapien diam id diam. Morbi a nisi rutrum, varius leo vel, convallis augue. Integer libero quam, semper non diam eu, porta faucibus neque. Etiam pellentesque lectus vitae lacus auctor, et vehicula magna tincidunt. Duis eros magna, placerat a nisi et, dignissim suscipit diam. Integer non velit et arcu lobortis elementum. Ut nec aliquam dui, eu convallis enim. Vestibulum nisl leo, faucibus in urna et, mattis mollis lacus.

Duis feugiat elit ut lorem sollicitudin tempor. Praesent rutrum, nibh consectetur viverra dapibus, nunc leo cursus mauris, id imperdiet dolor nisi vel lorem. Suspendisse in fermentum sem, a volutpat leo. Nullam in pretium nisi. Mauris aliquet a lectus quis tempus. Aenean tristique libero id nisl porta rhoncus. Aenean commodo sem et nisi ornare, nec posuere arcu euismod. Mauris eget nunc porttitor, rhoncus est et, ultricies purus. Nulla eu orci nec magna pellentesque ultricies sit amet non tellus

Contents

Chapter 1

Review

1.1 Lecture 1 — Groups and Basic Definitions

Definition 1.1 (group). A **group** G is a set with a binary operation $*$ such that

(a) There is an element $e \in G$ such that $a*e = e*a = a$ for all $a \in G$ *(identity)*;

(b) $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$ *(associativity)*;

(c) For each element $a \in G$ there is an element $a^{-1} \in G$ such that $a * a^{-1} = e$ *(inverse)*.

The group G is said to be **abelian** if $a * b = b * a$ for all $a, b \in G$.

Definition 1.2 (group order). The **order** of a group G is simply its cardinality $|G|$. We say that G is a **finite** group if $|G| < \infty$.

Proposition 1.3. Let G be a group. Then

(a) The identity $e \in G$ is unique;

(b) For each $a \in G$ the inverse a^{-1} is unique;

(c) If $a * b = a * c$, then $b = c$;

(d) $(a^{-1})^{-1} = a$;

(e) $(a * b)^{-1} = b^{-1} * a^{-1}$.

We will often omit the group operation symbol $(*)$ if the operation is clear. That is, we will denote $a * b$ by ab. If the group operation is understood as multiplication, we have, for $n \in \mathbb{Z}$,

$$a^n = \begin{cases} \underbrace{a * a * \cdots * a}_{n \text{ times}} & \text{if } n \geq 1, \\ e & \text{if } n = 0, \\ \underbrace{(a^{-1}) * (a^{-1}) * \cdots * (a^{-1})}_{|n| \text{ times}} & \text{if } n < 0. \end{cases}$$

Similar rules apply when the group operation is interpreted as addition, where we denote the inverse of a as $-a$ and write

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ times}} & \text{if } n \geq 1, \\ e & \text{if } n = 0, \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{|n| \text{ times}} & \text{if } n < 0. \end{cases}$$

Definition 1.4 (element order). The order of $a \in G$, denoted $|a|$, is the smallest nonnegative integer n such that $a^n = e$. If there is no such n, $|a| = \infty$.

Example 1.5.

(a) $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ with operation $+$ and identity 0;

(b) $\mathrm{GL}_n(\mathbb{R}) = \{$all $n \times n$ invertible matrices with entries in $\mathbb{R}\}$ (not abelian);

(c) $D_n =$ dihedral group of order $2n =$ symmetries of the n-gon

(d) $S_n = \{\sigma \mid \sigma$ is a permutation of $\{1, \dots, n\}\}$

Definition 1.6 (subgroup). A **subgroup** H of G is a subset $H \subseteq G$ such that H is also a group under the same operation.

Proposition 1.7 (Subgroup Criterion). Let G be a group and H a subset of G. Then H is a subgroup of G if and only if

(a) $e \in H$;

(b) If $a, b \in H$, then $ab \in H$;

(c) If $a \in H$, the $a^{-1} \in H$.

We can collapse the last two conditions into one.

Proposition 1.8 (Subgroup Criterion (condensed)). Let G be a group and H a subset of G. Then H is a subgroup of G if and only if $e \in H$ and $ab^{-1} \in H$ for any $a, b \in H$.

Definition 1.9 (cyclic subgroup). Let $a \in G$. The **cyclic subgroup** of G generated by a, denoted $\langle a \rangle$, is the subset

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \subseteq G.$$

We say that a is the **generator** of $\langle a \rangle$.

Theorem 1.10. If $a \in G$, $\langle a \rangle$ of G is a subgroup of G.

Proof. We verify that the criteria in Proposition 1.7 hold.

(a) $e \in \langle a \rangle$ since $e = a^0$.

(b) Suppose $x, y \in \langle a \rangle$. Then $x = a^m$ and $y = a^n$ for $m, n \in \mathbb{Z}$. So $xy = a^m a^n = a^{m+n} \in \langle a \rangle$.

(c) Let $x \in \langle a \rangle$. Then $x = a^n$ for some $n \in \mathbb{Z}$. We also have $a^{-n} \in \langle a \rangle$ and $xa^{-n} = a^n a^{-n} = a^0 = e$. So $x^{-1} \in \langle a \rangle$.

□

Definition 1.11 (cyclic group). A group G is said to be **cyclic** if $G = \langle a \rangle$ for some $a \in G$.

Example 1.12. $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ is a cyclic group generated by 1:

$$\langle 1 \rangle = \{1 \cdot 0, 1 \cdot 1, \dots, 1 \cdot (n-1)\} = \mathbb{Z}_n.$$

Theorem 1.13. $\mathbb{Z}_n = \langle a \rangle$ if and only if $\gcd(a, n) = 1$.

Theorem 1.14 (Lagrange). If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

Corollary 1.15. If $a \in G$, then $|a|$ divides $|G|$.

Proof. Given $a \in G$, consider the subgroup $\langle a \rangle$. Then $|a| = |\langle a \rangle|$. By Lagrange's Theorem, $|\langle a \rangle|$ divides $|G|$. □

Corollary 1.16. If $|G| = p$ with p prime, then G is cyclic.

Proof. Let $a \in G$ be an element other than the identity. So $|a|$ divides $|G| = p$. But $|a| \neq 1$ since a isn't the identity. So we must have $|a| = p$. In particular, $|\langle a \rangle| = p$. Thus, $\langle a \rangle = G$. □

You may notice a thematic question:

> If we know the factorization of $|G|$, what can we say about its structure?

The next chapter will attempt to tackle this question.

We finish with a sketch of the proof for Lagrange's Theorem.

Fix a subgroup H of G. The left coset of H with representative g is the set

$$gH = \{gh \mid h \in H\}.$$

We have the following facts:

(a) $g_1H = g_2H$ if and only if $g_1^{-1}g_2 \in H$;

(b) Either $g_1H = g_2H$ or $g_1H \cap g_2H = \varnothing$, i.e. cosets partition the group;

(c) $|gH| = |H|$.

Suppose $g_1H, g_2H, \dots, g_nH$ are the distinct left cosets of H. Then $G = g_1H \cup g_2H \cup \dots \cup g_nH$. So $|G| = |g_1H| + |g_2H| + \cdots + |g_n||H|$. But $|g_iH| = |H|$. So $|G| = |H| + \cdots + |H| = n|H|$. So $|H|$ divides $|G|$.

1.2 Lecture 2 — Equivalence Relations, Quotient Groups

Definition 1.17 (equivalence relation)**.** An **equivalence relation** R on a set X is a subset $R \subseteq X \times X$ such that

(a) $(x, x) \in R$ for all $x \in X$ *(reflexive)*,

(b) if $(x, y) \in R$, then $(y, x) \in R$ *(symmetric)*, and

(c) if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$ *(transitive)*.

We sometimes write $x \sim y$ for $(x, y) \in R$.

An equivalence relation "partitions" the set X.

Fix $x \in X$. then the **equivalence class** of x is the set

$$[x] = \{y \in X \mid (x, y) \in R\}.$$

Lemma 1.18. If $\sim$ is an equivalence relation, then for any $x, y \in X$, either

$$[x] \cap [y] = \varnothing \quad \text{or} \quad [x] = [y].$$

Proof. Suppose for a contradiction that $[x] \cap [y] \neq \varnothing$. So there exists $a \in [x] \cap [y]$. Since $a \in [x]$, we have $x \sim a$ and $a \in [y]$ implies $y \sim a$. So $a \sim y$, and thus, by transitivity, $x \sim y$. Let $b \in [x]$. Then $x \sim b$. So $b \sim x$. By transitivity, $b \sim y$ and $y \sim b$, i.e. $b \in [y]$. Thus $[x] \subset [y]$. Let $b \in [y]$. Then $y \sim b$. Since $x \sim y$ and $y \sim b$, $x \sim b$. So $b \in [x]$ and thus $[y] \subseteq [x]$. This along with the fact that $[x] \subseteq [y]$ contradicts our first assumption. ▢

Theorem 1.19. Let X be a set and R an equivalence relation on X. Let $[x_1], \dots, [x_n]$ be the distinct equivalence classes. Then

$$X = [x_1] \cup [x_2] \cup \dots \cup [x_n].$$

Proof. Since each $[x_i] \subseteq X$, it is clear that $[x_1] \cup [x_2] \cup \dots \cup [x_n] \subseteq X$.

Let $y \in X$ be arbitrary. Then $[y]$ is an equivalence class and $[y] = [x_i]$ for some i. So $y \in [y] = [x_i] \subseteq [x_1] \cup [x_2] \cup \dots \cup [x_n]$. Therefore, $X = [x_1] \cup [x_2] \cup \dots \cup [x_n]$ and $[x_i] \cap [x_j] = \varnothing$ by Lemma 1.18. ▢

Example 1.20. Let $X = \{\text{all McMaster Students}\}$ and $R = \{(x, y) \in X \times X \mid x \text{ and } y \text{ have the same height}\}$. Then R is an equivalence relation. So $[\text{Bob}] = \{\text{all students with the same height as Bob}\}$.

Example 1.21. Let G be a group and H a subgroup. Let $R = \{(g_1, g_2) \in G \times G \mid {g_1}^{-1}g_2 \in H\}$. This is an equivalence relation. Observe:

(a) $(g, g) \in R$ since $g^{-1}g = e \in H$.

(b) if $(g_1, g_2) \in R$, then

$$\begin{aligned} {g_1}^{-1}g_2 \in H &\implies ({g_1}^{-1}g_2)^{-1} = {g_2}^{-1}g_1 \in H \\ &\implies (g_2, g_1) \in R. \end{aligned}$$

(c) $(g_1, g_2), (g_2, g_3) \in R$ implies ${g_1}^{-1}g_2, {g_2}^{-1}g_3 \in H$. So ${g_1}^{-1}g_2{g_2}^{-1}g_3 = {g_1}^{-1}g_3 \in H$ and thus $(g_1, g_3) \in R$.

Note that $[g] = gH$ (the left coset of H).

Let $b \in [g]$. So $(g, b) \in R \implies g^{-1}b \in H$. So $b = gh \in gH$. Thus $[g] \subseteq gH$. Let $k \in gH$. So $k = gh$ for some $h \in H$. Thus $g^{-1}k = h \in H$. So $(g, k) \in R \implies k \in [g]$. Thus $gH \subseteq [g]$.

Given a group G and a subgroup H, we can form the set

$$G/H = \{gH \mid g \in G\} \quad \textit{(the set of all left cosets)}.$$

Example 1.22. Let $G = \mathbb{Z}_{12} = \{0, 1, 2, \dots, 11\}$ (group under $+$). Let $H = \langle 3 \rangle = \{0, 3, 6, 9\}$.

We have cosets

$$\begin{aligned} 0 + H &= \{0, 3, 6, 9\} = 3 + H \\ 1 + H &= \{1, 4, 7, 10\} = 4 + H \\ 2 + H &= \{2, 5, 8, 11\} = 5 + H \end{aligned}$$

So $G/H = \{0 + H, 1 + H, 2 + H\}$.

This leads to a natural question: does G/H have a group structure? If so, we require a binary operation, say $\star$. We would like for $(aH) \star (bH) = (ab) \star H$, which is almost right! This operation $\star$ depends upon the coset representative, i.e. if $a_1H = a_2H$ and $b_1H = b_2H$. Then why is $a_1b_1H = a_2b_2H$? This is false in general!

For example, take $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ and the subgroup $H = \{(1), (12)\}$. Then $(13)H = (123)H$ but $(13)(23)H = (132)H$. Now $(23)H = (132)H$ but $(123)(132)H = (1H)$.

The workaround is to introduce restrictions on the subgroup H.

Definition 1.23 (normal subgroup)**.** A subgroup N of G is **normal** if $gN = Ng$ for all $g \in G$. Equivalently, $gNg^{-1} \subset N$ for all $g \in G$.

Lemma 1.24. If N is a normal subgroup of G, then $(aH) \star (bH) = (ab) \star H$ is well-defined.

Proof. Suppose that $a_1N = a_2N$ and $b_1N = b_2N$. We want to show that $a_1b_1N = a_2b_2N$. This is equivalent to showing $(a_1b_1)^{-1}a_2b_2 \in N$. That is, ${b_1}^{-1}{a_1}^{-1}a_2b_2 \in N$.

Since $a_2 \in a_2N = a_1N$, there is $n_1 \in N$ such that $a_2 = a_1n_1$. Since $b_2 \in b_2N = b_1N = Nb_1$, There is $n_2 \in N$ such that $b_2n_2b_1$.

So

$$\begin{aligned} {b_1}^{-1}{a_1}^{-1}a_2b_2 &= {b_1}^{-1}{a_1}^{-1}a_1n_1n_2b_1 \\ &= {b_1}^{-1}(n_1n_2)b_1 \in {b_1}^{-1}Nb_1 \subseteq N \end{aligned}$$

□

Theorem 1.25. If N is any normal subgroup of G, then $G/N = \{gN \mid g \in G\}$ is a group under the operation $(aN)(bN) = (ab)N$.

> *Remark.* The identity in the group G/N is $eN = N$.

It should be easy see that all abelian groups are normal. For example $\mathbb{Z}/\langle 3 \rangle = \{0+H, 1+H, 2+H\}$ is a group.

Chapter 2

Group Structure

2.1 Lecture 3 — The Fundamental Theorem of Finite Abelian Groups I: Setting the stage

We'll begin with a motivating question: How many "distinct" groups are there of order $n \geq 1$?

What do we mean by "distinct"? Take for example $U(8) = \{a \mid \gcd(a, 8) = 1, a \in \{0, \dots, 7\}\} = \{1, 3, 5, 7\}$, which is a group under multiplication. Consider also $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ under addition. These groups are <u>not</u> distinct. This can be seen by constructing Cayley tables.

$U(8)$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$Z_2 \times \mathbb{Z}_2$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

We can see that these are the "same" groups by identifying as follows.

$$\begin{aligned} 1 &\leftrightarrow (0,0) \\ 3 &\leftrightarrow (1,0) \\ 5 &\leftrightarrow (0,1) \\ 7 &\leftrightarrow (1,1) \end{aligned}$$

Definition 2.1. Let $(G, *)$ and $(H, \cdot)$ be groups. Then a **group homomorphism** is a function $f : G \to H$ such that

$$f(a * b) = f(a) \cdot f(b),$$

for any $a, b \in G$.

Proposition 2.2. Let $f: G \to H$ be a homomorphism.

(a) $f(e_G) = e_H$

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

(c) If $G_1 \subseteq G$ is a subgroup, then $f(G_1) = \{f(g) \mid g \in G_1\} \subseteq H$ is a subgroup

(d) If $H_1 \subseteq$ is a subgroup, then $f^{-1}(H_1) = \{g \in g \mid f(g) \in H_1\} \subset G$ is a subgroup

Definition 2.3 (kernel, image). Let $f: G \to H$ be a homomorphism. The **kernel** of f is the set

$$\ker f = \{g \in G \mid f(g) = e_H\}.$$

The **image** of f is the set

$$\operatorname{im} f = \{f(g) \mid g \in G\} \subset H.$$

Proposition 2.4. Let $f: G \to H$ be a homomorphism.

(a) $\ker f$ is a normal subgroup of G.

(b) $\ker f = \{e_G\}$ if and only if f is injective.

(c) $\operatorname{im} f$ is a subgroup of H.

Definition 2.5 (group isomorphism). A group homomorphism $f: G \to H$ is called a **group isomorphism** if f is both injective and surjective, i.e. f is a bijection. If there exists such a homomorphism between G and H, we say that G and H are **isomorphic**, and we write $G \cong H$.

Example 2.6. As seen previously, $U(8) \cong \mathbb{Z}_2 \times Z_2$ and the isomorphism f is the identification we had made

So in our motivating question, when we say "distinct", we mean up to isomorphism.

Example 2.7. $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times Z_2$ because the group $\mathbb{Z}_4$ has an element of order 4 and $\mathbb{Z}_2 \times Z_2$ has no such element.

Theorem 2.8 (First Isomorphism Theorem). Let $f: G \to H$ be a group homomorphism. Then

$$G/\ker f \cong \operatorname{im} f \subset H.$$

Let's refine our motivating question: For each integer $n \geq 1$, list all groups G with $|G| = n$ such that any group of order n is isomorphic to one group in the list.

Example 2.9. Suppose that p is prime. If $|G| = p$, then $G \cong \mathbb{Z}_p$.

Proof. From the Lecture 1, if $|G| = p$, we proved that G is cyclic, i.e. $G = \langle a \rangle$ for some $a \in G$. So $G = \{a^0 = e, a^1, \dots, a^{p-1}\}$.

Define a map $\phi : G \to \mathbb{Z}_p$ by $\phi(a^i) = i$. This is clearly a bijection. It is also a homomorphism since, if $i + j = k \pmod p$, $\phi(a^i a^j) = \phi(a^k) = k = i + j = \phi(a^i) + \phi(a^j)$. $\square$

Proposition 2.10. There is only one group of order p prime up to isomorphism: $\mathbb{Z}_p$

Let's look at cases for small n.

n	all non-isomorphic groups
1	$\{0\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_2 \times \mathbb{Z}_3, S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_8, D_4, Q_8, \mathbb{Z}_4 \times \mathbb{Z}_2$

Example 2.11. If G is cyclic, and $|G| = n$, then $G \cong \mathbb{Z}_n$.

Theorem 2.12. If $\gcd(m, n) = 1$, then $\mathbb{Z}_{mn} = \mathbb{Z}_m \times \mathbb{Z}_n$.

Example 2.13. $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_{12} = \mathbb{Z}_{2^2} \times \mathbb{Z}_3$.

As a counterexample, where $\gcd(m, n) \neq 1$,

Theorem 2.14 (Fundamental Theorem of Finite Abelian Groups)**.** Every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order, i.e. of the form

$$\mathbb{Z}_{p_1^{d_1}} \times \mathbb{Z}_{p_2^{d_2}} \times \cdots \times \mathbb{Z}_{p_r^{d_r}},$$

where the p_i's are not necessarily distinct.

We can thus answer our refined motivating question.

Example 2.15. Write all non-isomorphic abelian groups of order 100.

Solution. Observe that

$$\begin{aligned}100 &= 2^2 \cdot 5^2\\ &= 2^1 \cdot 2^1 \cdot 5^2\\ &= 2^1 \cdot 2^1 \cdot 5^1 \cdot 5^1\\ &= 2^2 \cdot 5^1 \cdot 5^1.\end{aligned}$$

This gives the following groups:

- $\mathbb{Z}_{2^2} \times \mathbb{Z}_{5^2}$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
- $\mathbb{Z}_{2^2} \times \mathbb{Z}_5 \times \mathbb{Z}_5$

□

Corollary 2.16. If n is square-free, i.e. $n = p_1^1 p_2^1 \cdots p_r^1$, then there is only one abelian group of order n up to isomorphism, notably,

$$\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}.$$

Example 2.17. $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$ is the only abelian group of order 15.

2.2 Lecture 4 — The Fundamental Theorem of Finite Abelian Groups II: Proof

To prove the Fundamental Theorem of Finite Abelian Groups, we need to recall definitions and results relating to direct products. Direct products come in two flavours.

Definition 2.18 (external direct product). Let $(G, \circ)$ and $(H, \cdot)$ be groups. The **external direct product** of G and H is the group

$$G \times H = \{(g, h) \mid g \in G,\ h \in H\}$$

where the group operation $*$ is defined by

$$(g_1, h_2) * (g_2, h_2) = (g_1 \circ g_2, h_1 \cdot h_2).$$

Definition 2.19 (internal direct product). Let G be a group with subgroups H and K such that

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

Then G is the **internal direct product** of H and K.

Theorem 2.20. Suppose G is an internal direct product of subgroups H and K. Then $G \cong H \times K$.

This gives us a natural way to extend the definition of the internal direct product.

Let G be a group with subgroups $H_1, H_2, \ldots, H_n$ such that

- $G = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n \mid h_i \in H_i\}$,
- $H_i \cap \left(\bigcup_{i \neq j} H_j\right) = \{e\}$,
- $h_i h_j = h_j h_i$ for all $i \neq j$ $h_i \in H_i$ and $h_j \in H_j$.

Then G is the internal direct product of $H_1, H_2, \ldots, H_n$ and $G \cong H_1 \times H_2 \times \cdots \times H_n$, by Theorem 2.20.

Lemma 2.21. Let G be an abelian group and p a prime such that $p \mid |G|$. Then G has a subgroup of order p.

Proof. The proof is by induction on $|G| = n$.

If $|G| = 2$, then $G \cong \mathbb{Z}_2$, and so the result holds (the subgroup is trivial).

Let $|G| = n > 2$ and $e \neq g \in G$. So $|g| = qt$ for some prime q. Then $|g^t| = q$. If $q = p$, we are done (take $H = \langle g^t \rangle$). Assume otherwise. Let $N = \langle g^t \rangle \subseteq G$. Then since G is abelian, N is normal and so G/N is a group. We also have, by Lagrange,

$$|G/N| = |G|/|N| = n/q.$$

Now $p \mid (n/q)$ since $\gcd(p, q) = 1$. So G/N is a group where $p \mid |G/N|$ and $|G/N| < n$. By induction, G/N has an element of order p, say $aN \in G/N$. So $(aN)^p = eN = N$, or, equivalently, $a^p \in N$. Since $|N| = q$, $(a^p)^q = a^{pq} = e$. So $|a| \mid pq$ and thus $|a|$ must be one of 1, p, q and pq. We must have $|a| \neq 1$ since $a \neq e$. If $|a| = p$, we are done. If $|a| = pq$, then $|a^q| = p$ and we are done. If $|a| = q$, then $(aN)^q = eN = N$. Since $|aN| = p$, this means $p \mid q$. but $\gcd(p, q) = 1$ so this musn't be the case. □

Definition 2.22 (p-group)**.** A group G is a p-group (p prime) if for all $g \in G$, $|g| = p^t$ for some integer t.

Example 2.23. $\mathbb{Z}_4$ is a 2-group.

$$|0| = 2^0, \quad |1| = 2^2, \quad |2| = 2^1, \quad |3| = 2^3$$

$\mathbb{Z}_2 \times \mathbb{Z}_2$ is also a 2-group.

$$|(0,0)| = 2^0, \quad |(0,1)| = 2^1, \quad |(1,0)| = 2^1, \quad |(1,1)| = 2^2$$

Lemma 2.24. G is a p-group $\iff |G| = p^\alpha$ for some $\alpha \in \mathbb{Z}_{\geq 0}$.

Proof. ($\Rightarrow$) Let $a \in G$. Then $|a| \mid |G| = p^\alpha$. So $|a| = p^t$.

($\Leftarrow$) Suppose G is a p-group, but some prime $q \neq p$ has the property that $q \mid |G|$. By Lemma 2.21, G has an element of order q. But this contradicts that G is a p-group. So no such q exists. □

We introduce some technical lemmas to which no proof will be given until the next lecture.

Lemma 2.25. Suppose G is a finite abelian group with $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and the p_i's are distinct. For each p_i, set $G_i = \{g \in G \mid |g| = p_i^t \text{ for some } t\}$. Then G is the internal direct product of $G_1, \ldots, G_r$, and each G_i is a p_i-group.

Lemma 2.26. Let G be a finite abelian p-group and let $a \in G$ with maximal order (i.e. $|a| = p^m$, and $|h| \leq p^m$ for all $h \in G$ with $h \neq a$). Then

$$G \cong \langle a \rangle \times K \cong \mathbb{Z}_{p^m} \times K,$$

where K is another p-group.

We are now able to give the proof of the Fundamental Theorem of Finite Abelian Groups.

Proof. By Lemma 2.25, $G \cong G_1 \times G_2 \times \cdots \times G_r$ with each G_i a p_i group. By Lemma 2.26, we claim that for any p-group H, $H \cong \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \cdots \times \mathbb{Z}_{p^{a_s}}$. We proceed by induction on $|H|$. If $|H| = 2$, then $H \cong \mathbb{Z}_2$ if $|H| > 2$, take $g \in H$ with g having max order, say $|g| = p^{\ell}$. By 2.26, $H \cong \mathbb{Z}_{p^{\ell}} \times K$ where $|K| < |H|$ and K is a p-group. By induction applied fo K,

$$H \cong \mathbb{Z}_{p^{\ell}} \times \mathbb{Z}_{p^{b_1}} \times \cdots \times \mathbb{Z}_{p^{b_s}}.$$

Consequently,

$$\begin{aligned} G &\cong G_1 \times \cdots \times G_r \\ &\cong (\mathbb{Z}_{p^{a_1}} \times \cdot \times \mathbb{Z}_{p^{a_s}}) \times (\mathbb{Z}_{p^{b_1}} \times \cdot \times \mathbb{Z}_{p^{b_r}}) \times \cdots \end{aligned}$$

□

2.3 Lecture 5 — The Fundamental Theorem of Finite Abelian Groups III: Proving the technical lemmas

We restate and prove the technical lemmas from last lecture (2.25 and 2.26).

Lemma 2.27. Suppose G is a finite abelian group with $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and the p_i's are distinct. For each p_i, set $G_i = \{g \in G \mid |g| = p_i^t \text{ for some } t\}$. Then G is the internal direct product of $G_1, \dots, G_r$, and each G_i is a p_i-group.

Proof. First we show that each G_i is a p_i-subgroup. They are subgroups since all the properties hold:

- $|e| = 1 = p_i^0$ so $e \in G_i$,
- Let $a, b \in G_i$. So $|a| = p_i^t$ and $|b| = p_i^s$ for some s, t. Then $|ab| = \operatorname{lcm}(|a|, |b|) = \operatorname{lcm}(p_i^t, p_i^s) = p_i^{\max\{t,s\}}$ so $ab \in G_i$.
- Let $a \in G_i$. So $|a| = |a^{-1}| = p_i^t$. So $a^{-1} \in G_i$

In particular, each G_i is a p_i-group since every element has prime power order, by definition.

We now check the three conditions for direct products (in no particular order).

Let $g \in G_i \cap \left(\bigcup_{i \neq j} G_j\right)$. So if $g \in G_i$, $|g| = p_i^s$ for some s. But $g \in \left(\bigcup_{i \neq j} G_j\right)$, so $g \in G_j$ for some j So $|g| = p_j^t$ for some t. Thus, $p_i^s = p_j^t$ but this happens if and only if $s = t = 0$. So we must have that $g = e$.

To show $G = G_1 \cdots G_r = \{g_1 \cdots g_r \mid g_i \in G_i\}$, it is enough to show $G \subseteq G_1 \cdots G_r$. Let $g \in G$. So $|g| \mid |G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. So $|g| = p_1^{\beta_1} \cdots p_r^{\beta_r}$ with $0 \leq \beta_i \leq \alpha_i$. Let $a_i = |g|/p_i^{\beta_i}$. So $\gcd(a_1, \dots, a_r) = 1$. By Bezout, there exist $c_1, \dots, c_r$ such that $c_1a_1 + \cdots + c_ra_r = 1$. So $g = g^1 = g^{c_1a_1+\cdots+c_ra_r} = g^{c_1a_1} \cdots g^{c_ra_r}$. Consider $(g^{c_ia_i})$. Then $(g^{c_ia_i})^{p_i^{\beta_i}} = g^{c_ia_ip_i^{\beta_i}} = g^{c_i|g|} = e$. So $|g^{c_ia_i}| \mid |p_i^{\beta_i}$ and thus $g^{c_ia_i} \in G_i$. Thus $g = (g^{c_1a_1}) \cdots (g^{c_ra_r}) \in G_1 \cdots G_r$.

The last condition is trivial since G is abelian. □

Lemma 2.28. Let G be a finite abelian p-group and let $a \in G$ with maximal order (i.e. $|a| = p^m$, and $|h| \leq p^n$ for all $h \in G$ with $h \neq a$). Then

$$G \cong \langle a \rangle \times K \cong \mathbb{Z}_{p^n} \times K,$$

where K is another p-group.

Proof. Assume $|G| = p^\alpha$ and let $|a| = p^n$ be the element of maximum order. Let K be the largest subgroup of G such that

$$\langle a \rangle \cap K = \{0\}.$$

There is at least one possible K (taking $K = \{0\}$), so K is well-defined. Our goal is to prove $G = \langle a\rangle + K$. Suppose for a contradiction that there is an element $b \in G \backslash (\langle a\rangle + K)$. Let k be the smallest integer such that

$$p^k b = \underbrace{b + \cdots + b}_{p^k \text{ times}} \in \langle a\rangle + K.$$

Since $p^\alpha b = 0$ for some α, $p^\alpha b = 0 \in \langle a\rangle + K$. So such an integer k exists. Since k is minimal, $c = p^{k-1}b \notin \langle a\rangle + K$, but $pc = p^k b \in \langle a\rangle + K$. Thus, $pc = ta + k$ for some integer t. Since $|a| = p^n$, $p^n x = 0$ for all $x \in G$ because a has maximal order. From here, $0 = p^n c = p^{-1}(pc) = p^{n-1}(ta + k) = p^{n-1}ta + p^{n-1}k$. Rearranging yields $\underbrace{p^{n-1}ta}_{\in\langle a\rangle} = \underbrace{p^{n-1}k}_{\in K} \in \langle a\rangle \cap K = \{0\}$ which gives $p^{n-1}ta = 0$. Since $|a| = p^n$ and $(p^{n-1}t)a = 0$, $p^n \mid p^{n-1}t$ which implies $p \mid t$ and so $t = mp$ for some m. Now,

$$\begin{aligned} pc &= ta + k \\ &= mpa + k \\ &\Leftrightarrow k = pc - mpa \\ &\quad\;\; = p(c - ma) \end{aligned}$$

So $pd = k \in K$. On the other hand, $d \notin K$ because that would give $c = ma + d \in \langle a\rangle + K$.

Consider the following fact: Let $H = \{x + zd \mid x \in K,\ z \in \mathbb{Z}\}$. Then H is a subgroup of G that properly contains K.

Since K was the largest subgroup such that $\langle a\rangle \cap K = \{0\}$, we have $\langle a\rangle \cap H \neq \{0\}$.

Let $0 \neq w \in \langle a\rangle \cap H$. Hence

$$w = sa = k_1 + rd \text{ with } k_1 \in K, r \in \mathbb{Z}.$$

We claim $p \nmid r$. If $p \mid r$, we have $r = py$ and since $pd \in K$, we have $0 \neq w = sa = k_1 + pyd \in \langle a\rangle \cap K = \{0\}$, which yields a contradiction.

Since $p \nmid r$, $\gcd(p, r) = 1$ which implies $pu + rv = 1$ for some u, v. Now,

$$\begin{aligned} c &= c \cdot 1 \\ &= c(pu + rv) \\ &= u(pc) + vrc \\ &= u(ta + k) + vr(d + ma) \\ &= u(ta + k) + v(rd + mra) \\ &= u(ta + k) + v(sa = k_1 + rma) \\ &= \underbrace{(ut + vs + vrm)a}_{\in\langle a\rangle} + \underbrace{uk - vk_1}_{\in K} \in \langle a\rangle + K. \end{aligned}$$

This is a contradiction, so there is no such b. □

2.4 Lecture 6 — Composition Series and Solvable Groups

The Fundamental Theorem of Finite Abelian Groups classifies all finite abelian groups. But what about non-abelian groups? In the 20th century, there was a tremendous amount of effort put into the classification of non-abelian groups (completed in 2004). The main idea is to reduce to understanding solvable and simple groups.

Definition 2.29 (subnormal series). A **subnormal series** of a group G is a finite sequence of subgroups

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\},$$

where H_i is normal in H_{i+1} for $i = 0, \dots, n-1$. If, in addition, each H_i is normal in G, we call the series a **normal series**.

We denote subnormal series by $\{H_i\}$ and define the **length** of $\{H_i\}$ to be the number of inclusions.

Example 2.30. In an abelian group G, every subnormal series is also a normal series.

$$\mathbb{Z} \supset 11\mathbb{Z} \supset 253\mathbb{Z} \supset 2024\mathbb{Z} \supset \{0\}$$

Example 2.31. Consider the following subnormal series in D_4:

$$D_4 \supset \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \supset \{(1), (1\,2)(3\,4)\} \supset \{(1)\}$$

This is not a normal series since $\{(1), (1\,2)(3\,4)\}$ is not normal in D_4.

Definition 2.32. A subnormal series $\{K_i\}$ is a **refinement** of a subnormal series $\{H_i\}$ if $\{H_i\} \subset \{K_i\}$, i.e. if the H_i's appear among the K_i's.

Example 2.33. The subnormal series

$$\mathbb{Z} \supset 11\mathbb{Z} \supset 253\mathbb{Z} \supset 506\mathbb{Z} \supset 1012\mathbb{Z} \supset 2024\mathbb{Z} \supset \{0\}$$

is a refinement of that presented in Example 2.30.

Definition 2.34. Two subnormal series $\{H_i\}$ and $\{K_i\}$ are said to be **isomorphic** if there is a one-to-one correspondence between the sets $\{H_{i+1}/H_i\}$ and $\{K_{i+1}/K_i\}$.

> *Remark.* Suppose $\langle a\rangle \supset \langle b\rangle \supset \mathbb{Z}_n$. Recall $|\langle a\rangle| = \frac{n}{a}$ and $|\langle b\rangle/\langle a\rangle| = \frac{n/b}{n/a} = \frac{a}{b}$.

Example 2.35. Consider the following subnormal series.

$$\begin{aligned} \{H_i\} &: \mathbb{Z}_{2024} \supset \langle 11\rangle \supset \langle 22\rangle \supset \langle 506\rangle \supset \langle 0\rangle \\ \{K_i\} &: \mathbb{Z}_{2024} \supset \langle 23\rangle \supset \langle 46\rangle \supset \langle 506\rangle \supset \langle 0\rangle \end{aligned}$$

Then we have the following quotients.

$$\begin{array}{cc} \{H_{i+1}/H_i\} : & \{K_{i+1}/K_i\} : \\ \mathbb{Z}_{2024}/\langle 11\rangle = \langle 1\rangle/\langle 11\rangle \cong \mathbb{Z}_{11}, & \mathbb{Z}_{2024}/\langle 23\rangle = \langle 1\rangle/\langle 11\rangle \cong \mathbb{Z}_{23} \\ \langle 11\rangle/\langle 22\rangle \cong \mathbb{Z}_2 & \langle 23\rangle/\langle 46\rangle \cong \mathbb{Z}_2 \\ \langle 22\rangle/\langle 506\rangle \cong \mathbb{Z}_{23} & \langle 46\rangle/\langle 506\rangle \cong \mathbb{Z}_{11} \\ \langle 506\rangle/\langle 0\rangle \cong \mathbb{Z}_4 & \langle 506\rangle/\langle 0\rangle \cong \mathbb{Z}_4 \end{array}$$

Definition 2.36 (simple group). If G has no non-trivial subgroups, we say that G is **simple**.

Example 2.37. Consider $\mathbb{Z}_p$ with p prime. This group is simple by application of Lagrange's Theorem.

Definition 2.38. A subnormal series $\{H_i\}$ of G is a **composition series** if all H_{i+1}/H_i are simple.

A normal series $\{H_i\}$ of G is a **principal series** if all H_{i+1}/H_i are simple.

Example 2.39. The series in Example 2.35 are not composition series since $\mathbb{Z}_4$ is not a simple group. However,

$$\mathbb{Z}_{2024} \supset \langle 23\rangle \supset \langle 46\rangle \supset \langle 506\rangle \supset \langle 1012\rangle \supset \langle 0\rangle$$

has quotients $\mathbb{Z}_{23}, \mathbb{Z}_2, \mathbb{Z}_{11}, \mathbb{Z}_2, \mathbb{Z}_2$.

Note that $2024 = 23 \cdot 11 \cdot 2^3$.

Remark. Not every group has a composition/principal series.

Example 2.40. Consider the subnormal series

$$\mathbb{Z} \supset H_1 \supset H_2 \supset \cdots \supset H_k \supset \langle 0 \rangle.$$

Then $H_k \cong t\mathbb{Z}$ for some integer t. Then $H_k/\langle 0 \rangle \cong t\mathbb{Z}$, which is not simple.

Remark. Composition series, if they exist, they may not be unique.

Example 2.41. Both

$$\mathbb{Z}_{2024} \supset \langle 11 \rangle \supset \langle 22 \rangle \supset \langle 506 \rangle \supset \langle 1012 \rangle \supset \langle 0 \rangle$$

and

$$\mathbb{Z}_{2024} \supset \langle 23 \rangle \supset \langle 46 \rangle \supset \langle 92 \rangle \supset \langle 1012 \rangle \supset \langle 0 \rangle$$

are compostition series. (Check!)

We can easily get around the non-uniqueness of composition series by allowing isomorphism.

Theorem 2.42 (Jordan-Hölder)**.** Any two composition series of G are isomorphic.

We will postpone the proof until next lecture.

Definition 2.43. A group G is **solvable** if it has a subnormal series such that all H_{i+1}/H_i are abelian.

Example 2.44. Famously, the alternating group A_n is not solvable for integers $n \geq 5$.

Example 2.45. We apply the Jordan-Hölder Theorem to the Fundamental Theorem of Arithmetic. We know that every integer can be factored into primes (existence). We use Jordan-Hölder to show uniqueness.

Proof. Suppose

$$n = p_1 p_2 \cdots p_r = q_1 q_1 \cdots q_s \quad \textit{(not necessarily distinct).}$$

We form the composition series

$$\mathbb{Z}_n \supset \langle p_1 \rangle \supset \langle p_1 p_2 \rangle \supset \cdots \supset \langle p_1 p_2 \cdots p_r \rangle \supset \langle 0 \rangle,$$

with $\langle p_1 \cdots p_i \rangle / \langle p_1 \cdots p_{i-1} \rangle \cong \mathbb{Z}_{p_i}$ simple. We also have the composition series

$$\mathbb{Z}_n \supset \langle q_1 \rangle \supset \langle q_1 q_2 \rangle \supset \cdots \supset \langle q_1 q_2 \cdots q_s \rangle \supset \langle 0 \rangle,$$

with $\langle q_1 \cdots q_j \rangle / \langle q_1 \cdots q_{j-1} \rangle \cong \mathbb{Z}_{q_j}$ simple. By Jordan-Hölder, the series are isomorphic, so $r = s$ and $\mathbb{Z}_{p_i} \cong \mathbb{Z}_{q_j}$ if and only if $p_i = q_j$. □

This proof can be used to find composition series for $\mathbb{Z}_n$. For example, take $n = 2024 = 23 \cdot 2 \cdot 11 \cdot 2 \cdot 2$. So

$$\mathbb{Z}_{2024} \supset \langle 23 \rangle \supset \langle 23 \cdot 2 \rangle \supset \langle 23 \cdot 2 \cdot 11 \rangle \supset \langle 23 \cdot 2 \cdot 11 \cdot 2 \rangle \supset \langle 23 \cdot 2 \cdot 11 \cdot 2 \cdot 2 \rangle = \langle 0 \rangle$$

is a composition series.

2.5 Lecture 7 — The Jordan-Hölder Theorem

Theorem 2.46 (Jordan-Hölder)**.** Suppose $\{H_i\}$ and $\{K_j\}$ are two composition series of G. Then $\{H_i\}$ and $\{K_j\}$ are isomorphic. That is, there is a one-to-one correspondence between the sets $\{H_{i+1}/H_i\}$ and $\{K_{j+1}/K_j\}$.

We use the Second Isomorphism Theorem and a couple of lemmas to prove this result.

Theorem 2.47 (Second Isomorphism Theorem)**.** Let H be any subgroup of G and let N be a normal subgroup of G. Then

(a) $HN = \{hn \mid h \in H, n \in N\}$ is a subgroup of G,

(b) $H \cap N$ is normal in H, and

(c) $H/(H \cap N) \cong HN/N$.

Lemma 2.48. Suppose H is normal in a subgroup K of G. For any subgroup L of G, $H \cap L$ is normal in $K \cap L$.

Proof. Let $t \in H \cap L$ and $s \in K \cap L$. Since $t \in L$ and $s \in L$, $sts^{-1} \in L$. Since $t \in H$ and $s \in K$, $sts^{-1} \in sHs^{-1} \subseteq H$, as H is normal in K. So $sts^{-1} \in s(H \cap L)s^{-1} \subseteq H \cap L$. In particular, $sts^{-1} \in L$. □

Lemma 2.49. If A is normal in B and N is normal in both A and B, then A/N is normal in B/N.

Proof. We want to show that $bN(A/N)(bN)^{-1} \subseteq A/N$ for all $bN \in B/N$. Take $\ell \in bN(A/N)(bN)^{-1}$. Then $\ell = bNaNb^{-1}N$ for some $a \in A$. In particular, $\ell = bab^{-1}N$. But A is normal in B. So $bab^{-1} \in bAb^{-1} \subseteq A$. So $bab^{-1}N = aN \in A/N$. □

We are now ready to prove the Jordan-Hölder Theorem (2.46).

Proof. The proof is by induction on the length of the smallest composition series of G. If $n = 1$, then $G = \{e\}$. So $G/\{e\} \cong G$, and so G is simple. So this is the only possible composition series for G (note that in a composition series, H_{n-1} is normal in $G = H_n$ so this forces $H_{n-1} = H_0 = \{e\}$).

Suppose that for all k with $1 \leq k < n$, all composition series for G of length k are isomorphic. We now want to show any two composition series of length n are isomorphic. Consider the following two composition series:

$$G = H_n \supset H_{n-1} \supset \dots \supset H_1 \supset H_0 = \{e\} \tag{2.1}$$

and

$$G = K_n \supset K_{n-1} \supset \dots \supset K_1 \supset K_0 = \{e\}. \tag{2.2}$$

By lemma 2.48,

$$\begin{gathered}H_i \cap K_{m-1} \text{ is normal in } H_{i+1} \cap K_{m-1} \text{ for } i = 0, \dots, n-2\\ \text{and}\\ H_{n-1} \cap K_j \text{ is normal in } H_{n-1} \cap K_{j+1} \text{ for } j = 0, \dots, m-2.\end{gathered}$$

So we have two new subnormal series

$$\begin{gathered}G = H_n \supset H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset H_{n-2} \cap K_{m-1} \supset \cdots \supset H_0 \cap K_{m-1} = \{e\}\\ \text{and}\\ G = K_m \supset K_{m-1} \supset H_{n-1} \cap K_{m-1} \supset H_{n-1} \cap K_{m-2} \supset \cdots \supset H_{n-1} \cap K_0 = \{e\}.\end{gathered}$$

We want to show that the above are two new composition series, i.e. each quotient is simple. It should be clear that H_n/H_{n-1} and K_m/K_{m-1} are simple, by construction.

Claim. $H_{n-1} \cap K_{m-1}$ is normal in H_{n-1} and $H_{n-1}/(H_{n-1} \cap K_{m-1})$ is simple. We'll come back to proving this claim. Assume it to be true.

By the Second Isomorphism Theorem (2.47),

$$\frac{H_{i+1} \cap K_{m-1}}{H_i \cap K_{m-1}} = \frac{H_{i+1} \cap K_{m-1}}{H_i \cap (H_{i+1} \cap K_{m-1})} \cong \frac{H_i(H_{i+1} \cap K_{m-1})}{H_i}$$

for $i = 0, \dots, n-2$.

We claim that $H_i(H_{i+1} \cap K_{m-1})$ is normal in H_{i+1}. Let $a \in H_i$ and $b \in H_{i+1} \cap K_{m-1}$ so that $ab \in H_i(H_{i+1} \cap K_{m-1})$. Let $\ell \in H_{i+1}$. Since H_i is normal in H_{i+1}, $\ell a \ell^{-1} \in H_i$. Also $\ell b \ell^{-1} \in H_{i+1}$ since $b, \ell \in H_{i+1}$. Finally, since K_{m-1} is normal in G, $\ell b \ell^{-1} \in K_{m-1}$. So

$$\ell ab \ell^{-1} = \ell a e b \ell^{-1} = (\ell a \ell^{-1})(\ell b \ell^{-1}) \in H_i(H_{i+1} \cap K_{m-1}).$$

Because H_i is normal in $H_i(H_{i+1} \cap K_{m-1})$, and H_{i+1}, and $H_i(H_{i+1} \cap K_{m-1})$ is normal in H_{i+1}, by 2.49,

$$\tfrac{H_i(H_{i+1} \cap K_{m-1})}{H_i} \text{ is normal in } \tfrac{H_{i+1}}{H_i}.$$

But H_{i+1}/H_i is simple. So

$$\frac{H_i(H_{i+1} \cap K_{m-1})}{H_i} = \frac{H_i}{H_i} \text{ or } = \frac{H_{i+1}}{H_i} \quad \Longleftrightarrow \quad H_i(H_{i+1} \cap K_{m-1}) = H_i \text{ or } = H_{i+1}.$$

By removing non-proper inclusions,

$$H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset H_{n-2} \cap K_{m-1} \supset \cdots \supset H_0 \cap K_{m-1} \tag{2.3}$$

is a composition series. By the same reasoning,

$$K_{m-1} \supset H_{n-1} \cap K_{m-1} \supset H_{n-1} \cap K_{m-2} \supset \cdots \supset H_{n-1} \cap K_0 \tag{2.4}$$

is also a composition series. By the induction hypothesis, the composition series (2.3) is equivalent to

$$H_{n-1} \supset H_{n-2} \supset \cdots \supset H_0.$$

Considering composition series (2.1) and (2.2), if $H_{n-1} = K_{m-1}$ then the first quotients are equivalent, i.e. $H_n/H_{n-1} \cong K_m/K_{m-1}$ and the rest are equivalent by induction.

If $H_{n-1} \neq K_{m-1}$, consider

$$\begin{aligned} G = H_n \supset H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset H_{n-2} \cap K_{m-1} \supset \cdots \supset H_0 \cap K_{m-1} \qquad (2.5) \\ \text{and} H = K_m \supset K_{m-1} \supset H_{n-1} \cap K_{m-1} \supset H_{n-1} \cap K_{m-2} \supset \cdots \supset H_{n-1} \cap K_0. \qquad (2.6) \end{aligned}$$

Note $K_{m-1}/(H_{n-1} \cap K_{m-1}) \cong H_{n-1}K_{m-1}/H_{n-1} = G/H_{n-1}$ by the Second Isomorphism Theorem 2.47. Similarly, $H_{n-1}/(H_{n-1} \cap K_{m-1}) \cong G/K_{n-1}$. □

Bonus content! We now prove those claims we put off.

We claimed that

(a) $H_{n-1} \cap K_{m-1}$ is normal in H_{n-1}, and

(b) $H_{n-1}/(H_{n-1} \cap K_{m-1})$ is simple.

Proof. To prove the first claim, take $h \in H_{n-1} \cap K_{m-1}$ and $g \in H_{n-1}$. We want to show $ghg^{-1} \in H_{n-1} \cap K_{m-1}$. Since $h, g, g^{-1} \in H_{n-1}$, we have $ghg^{-1} \in H_{n-1}$. Because K_{m-1} is normal in G and $g \in H_{n-1} \subseteq G$, we have $ghg^{-1} \in K_{m-1}$. Thus, $ghg^{-1} \in H_{n-1} \cap K_{m-1}$, as desired.

Now to prove the second claim, first observe that by the Second Isomorphism Theorem (2.47),

$$H_{n-1}/(H_{n-1} \cap K_{m-1}) \cong H_{n-1}K_{m-1}/K_{m-1}.$$

We first want to show $H_{n-1}K_{m-1}/K_{m-1}$ is normal in G/K_{m-1}. So let $hkK_{m-1} \in H_{n-1}K_{m-1}/K_{m-1}$ and $gK_{m-1} \in G/K_{m-1}$. Since $h \in H_{n-1}$ and H_{n-1} is normal in G, $ghg^{-1} \in H_{n-1}$. Since $k \in K_{m-1}$ and K_{m-1} is normal in G, $gkg^{-1} \in K_{m-1}$. So

$$(gK_{m-1})(hkK_{m-1})(g^{-1}K_{m-1}) = g(hk)g^{-1}K_{m-1}.$$

But $(ghg^{-1})(gkg^{-1}) = ghkg^{-1} \in H_{n-1}K_{m-1}$, and so $g(hk)g^{-1}K_{m-1} \in H_{n-1}K_{m-1}/K_{m-1}$. Thus, $H_{n-1}K_{m-1}/K_{m-1}$is normal in $G/K_{m-1} = K_m/K_{m-1}$. But K_m/K_{m-1} is simple, so either

$$H_nK_{m-1}/K_{m-1} = \underbrace{K_{m-1}/K_{m-1}}_{\text{the trivial group}} \quad \text{or} \quad H_nK_{m-1}/K_{m-1} = K_m/K_{m-1}.$$

In both cases, the group is simple. □

Chapter 3

Group Actions

3.1 Lecture 8 — Group Actions and Examples

In this lecture, we will introduce group actions. As an example from linear algebra, if V is a vector space over a field $\mathbb{F}$, then $\mathbb{F}$ "acts" on V by scalar multiplication, i.e.

$$(\mathbb{F} \times V) \to V, \qquad (c, v) \mapsto cv.$$

Definition 3.1 (group action). Let X be a set and G a group. A **left action** of G on X is a map $G \times X \to X$ defined by

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

such that

(a) $(e, x) \mapsto e \cdot x = x$, and

(b) $(g_1, (g_2, x)) \mapsto g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$.

We call X a G-set.

> *Remark.* "$\cdot$" does *not* always mean multiplication.

Example 3.2. The map $G \times X \to X$ defined by $(g, x) \mapsto x$ is trivially a group action.

Example 3.3. If $X = G$, then we can view the group operation as a group action $G \times G \to G$, $(g, x) \mapsto g * x$, where $*$ is the operation in the group G.

Example 3.4. Let $X = \mathbb{R}^2$ and take $G = \mathrm{GL}_2(\mathbb{R})$ (all 2×2 invertible matrices). Define a map

$$\begin{gathered} G \times X \to X, \\ \left(A, \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) \mapsto A \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}. \end{gathered}$$

This is indeed a group action. The identity criterion obviously holds. Let $A, B \in G$. Then

$$\begin{aligned} \left(A, \left(B, \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right)\right) &= \left(A, B\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) \\ &= AB\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \end{aligned}$$

But also

$$\left(AB, \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) = AB\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Example 3.5. Let $X = G$ and let H be a subgroup of G. Define an H-action on G by

$$\begin{aligned} H \times G &\to G \\ (h, g) &\mapsto hgh^{-1} \end{aligned}$$

This is a group action since $e \in H$ and $(h, g) \mapsto ege^{-1} = g$ and, for any $h_1, h_2 \in H$,

$$\begin{aligned} (h_1, (h_2, g)) &\mapsto (h_1, h_2gh_2^{-1}) \\ &\mapsto h_1(h_2gh_2^{-1})h_1^{-1} \\ &= (h_1h_2)g(h_2^{-1}h_1^{-1}) \\ &= (h_1h_2)g(h_1h_2)^{-1} \end{aligned}$$

and also $(h_1h_2, g) \mapsto (h_1h_2)g(h_1h_2)^{-1}$.

Example 3.6. Let $X = \{a_1, a_2, \dots, a_n\}$ and let $G = S_n$ (symmetric group on n elements). Then G acts on X by

$$\begin{aligned} G \times X &\to X, \\ (\sigma, a_i) &\mapsto a_{\sigma(i)}. \end{aligned}$$

For example, take $X = \{a_1, a_2, a_3\}$ and $G = S_3$. Consider

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Then $(\sigma, a_1) \mapsto a_2$, $(\sigma, a_2) \mapsto a_1$ and $(\sigma, a_3) \mapsto a_3$.

This is all great, but why should we care about group actions? In short, they provide us with *equivalence relations*.

Definition 3.7 (group-equivalent)**.** Two elements $x, y \in X$ are said to be G-equivalent if there is an element $g \in G$ such that $y = g \cdot x$. We write $x \sim y$ or, to specify the group, $x \sim_G y$.

Theorem 3.8. Let X be a G-set. Then "G-equivalent" is an equivalence relation

Proof. We verify that the required properties hold.

(a) (reflexive) $x \sim x$ since $x = e \cdot x$

(b) (symmetric) Suppose $x \sim y$. Then there exists an element $g \in G$ such that $y = g \cdot x$. So $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x$.

(c) (transitive) If $x \sim y$, then $y = g_1 \cdot x$ and if $y \sim z$, then $z = g_2 \cdot y$. So $z = g_2 \cdot y = g_2 \cdot (g_1 \cdot x) = (g_1 g_2) \cdot x$ and thus $x \sim z$

□

Definition 3.9 (orbit)**.** Let X be a G-set and fix $x \in X$. Define

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

We call $\mathcal{O}_x$ the **orbit** of x.

We give a few properties without proof.

Proposition 3.10. Let X be a G-set.

(a) $O_x = \{y \mid x \sim y\}$

(b) $\mathcal{O}_{x_i} = \mathcal{O}_{x_j}$ or $\mathcal{O}_{x_i} \cap \mathcal{O}_{x_j} = \varnothing$ for all $x_i, x_j \in X$.

(c) If $\mathcal{O}_{x_1}, \dots, \mathcal{O}_{x_s}$ are distinct orbits, then

$$X = \bigcup_{i=1}^{s} \mathcal{O}_{x_i},$$

i.e. the orbits partition X.

Example 3.11. Let $X = \{1,2,3\}$ and $H = \left\{\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right\}$. Define an action

$$\begin{aligned} H \times H &\to X, \\ (\sigma_i, j) &\mapsto \sigma_i(j). \end{aligned}$$

Then we have the following orbits.

$$\begin{aligned} \mathcal{O}_1 &= \{\sigma_1(1), \sigma_2(1)\} = \{1,2\} \\ \mathcal{O}_2 &= \{\sigma_1(2), \sigma_2(2)\} = \{2,1\} \\ \mathcal{O}_3 &= \{\sigma_1(3), \sigma_2(3)\} = \{3\} \end{aligned}$$

Thus $X = \{1,2,3\} = \mathcal{O}_1 \cup \mathcal{O}_3$.

3.2 Lecture 9 — Group Actions and the Class Equation

Definition 3.12. The **fixed points** of $g \in G$ are elements of the set

$$X_g = \{x \in X \mid g \cdot x = x\} \subset X.$$

The **stablilizer** subgroup of $x \in X$ is defined by

$$G_x = \{g \in G \mid g \cdot x = x\} \subset G.$$

Lemma 3.13. The stabilizer G_x is a subgroup of G.

Proof. First note that $G_x \neq \emptyset$ since $e \cdot x = x$ and thus $e \in G_x$. Let $g \in G_x$. So $g \cdot x = x$ and thus $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$. But this is the case if and only if $(g^{-1}g) \cdot x = g^{-1}x$ and so $x = g^{-1} \cdot x$. So $g^{-1} \in G_x$. Now take $g, h \in G_x$. Then

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

So $gh \in G_x$ □

Theorem 3.14. Let X be a G-set and let $x \in X$. Then

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

Proof. Recall that $[G : G_x]$ is the number of distinct left cosets of G_x. Let $\mathcal{L}_{G_x}$ be the set of distinct left cosets, i.e.

$$\mathcal{L}_{G_x} = \{gG_x \mid g \in G\}.$$

Note that if $y \in \mathcal{O}_x$, there exists a $g \in G$ such that $y = g \cdot x$. Define a map $\Phi : \mathcal{O}_x \to \mathcal{L}_{G_x}$ by $y \mapsto gG_x$, where $y = g \cdot x$. If we can show Φ is a bijection, then $|\mathcal{O}_x| = |\mathcal{L}_{G_x}|$.

To see the map is surjective, take $gG_x \in \mathcal{L}_{G_x}$. Then $y = g \cdot x \in \mathcal{O}_x$ and so $\Phi(y) = gG_x$.

To see the map is injective, observe that if $\Phi(y_1) = g_1G_x = g_2G_x = \Phi(y_2)$ with $y_1 = g_1 \cdot x$ and $y_2 = g_2 \cdot x$. So there exists $g \in G_x$ such that $g_2 = g_1 g$. So

$$\begin{aligned}y_2 &= g_2 \cdot x\\ &= (g_1 g) \cdot x\\ &= g_1 \cdot (g \cdot x)\\ &= g_1 \cdot x\end{aligned}$$

So Φ is injective and thus $|\mathcal{O}_x| = |\mathcal{L}_{G_x}|$, as desired □

Example 3.15. Take $X = \{1,2,3,4\}$, $G = \{\sigma_1, \sigma_2\} = \{(1), (1\,2)(3\,4)\}$, and the action

$$\begin{aligned} G \times X &\to X, \\ (\sigma, i) &\mapsto \sigma(i). \end{aligned}$$

Then $\mathscr{O}_1 = \{\sigma_1(1), \sigma_2(1)\} = \{1,2\}$ and $G_1 = \{\sigma \in G \mid \sigma(1) = 1\} = \{\sigma_1\}$. Indeed,

$$|\mathscr{O}_1| = |G|/|G_1| = 2/1 = 2.$$

> *Remark.* If $|\mathscr{O}_x| = 1$, then $\{g \cdot x \mid g \in X\} = \{x\}$. So if X is a G-set, then the set of all fixed points is
>
> $$X_G = \{x \mid g \cdot x = x \text{ for all } g \in G\} = \mathscr{O}_{x_1} \cup \cdots \cup \mathscr{O}_{x_s},$$
>
> where $|\mathscr{O}_{x_i}| = 1$.

Let X be a G-set, and let $x_1, \ldots, x_n$ be the distinct coset representatives. Then

$$X = \underbrace{\mathscr{O}_{x_1} \cup \cdots \cup \mathscr{O}_{x_s}}_{|\mathscr{O}_{x_i}|>1} \cup \underbrace{\mathscr{O}_{x_{s+1}} \cup \cdots \cup \mathscr{O}_{x_n}}_{|\mathscr{O}_{x_i}|=1},$$

and, as such,

$$|X| = |\mathscr{O}_{x_1}| + \cdots + |\mathscr{O}_{x_s}| + |X_G| = [G : G_{x_1}] + \cdots + [G : G_{x_s}] + |X_G|.$$

We specialize these results to the following case:

$$\begin{aligned} G \times G &\to G, \\ (g, x) &\mapsto gxg^{-1} \end{aligned}$$

This group action is called **conjugation**. So the set of fixed points using this operation is

$$Z(G) = \{x \in G \mid gxg^{-1} = x \text{ for all } g \in G\}.$$

We call $Z(G)$ the **center** of G. One can show $Z(G)$ is a subgroup of G.

The **stabilizer** subgroup of $x \in G$ is

$$C(x) = \{g \mid gxg^{-1} = x\},$$

i.e. all things of G that commute with x. We call $C(G)$ the **centralizer** of G. One can also show $C(G)$ is a subgroup of G.

The orbits of $x \in G$ are called **conjugacy classes**.

$$\mathscr{O}_x = \{gxg^{-1} \mid g \in G\}.$$

Theorem 3.16 (Class Equation)**.** Let G be a finite group and consider the group action of conjugation. If $x_1, \dots, x_n$ are the distinct coset representatives of this action, then

$$G = \mathcal{O}_{x_1} \cup \cdots \cup \mathcal{O}_{x_n}.$$

Furthermore, if $|\mathcal{O}_{x_i}| > 1$ for $i = 1, \dots, s$, and $|\mathcal{O}_{x_i}| = 1$ for $i = s+1, \dots, n$, then

$$|G| = |\mathcal{O}_{x_1}| + \cdots + |\mathcal{O}_{x_s}| + |Z(G)| = [G : C(x_1)] + [G : C(x_s)] + |Z(G)| \tag{3.1}$$

We call (3.1) the **class equation**.

3.3 Lecture 10 — The Class Equation: Applications and Examples

Theorem 3.17. If $|G| = p^r$, then $|Z(G)| \geq p$.

Proof. By the class equation,

$$|Z(G)| = |G| - \sum_{i=1}^{s} [G : C(x_i)].$$

We have that $[G : C(x_i)] = \frac{|G|}{|C(x_i)|} \geq 2$. Since $|G| = p^r$, $|C(x_i)| = p^{r-n_i}$ and thus $[G : C(x_i)] = p^{n_i}$ for some $n_i \geq 1$. Note that it must be the case $n_i \geq 1$ since $[G : C(x_i)] \geq 2 \geq p^0$. Thus every term on the right hand side is divisible by p. In particular, p divides $Z(G)$ and so $|Z(G)| \geq p$. □

Theorem 3.18. If $|G| = p^2$, then G is abelian. That is, $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Proof. It is enough to show that $|Z(G)| = p^2$, which would imply that $Z(G) = G$. By the previous result (Theorem 3.17), either $|Z(G)| = p^2$ or $|Z(G)| = p$. Suppose for a contradiction that $|Z(G)| = p$. Note that $Z(G)$ is normal in G. Take any $g \in G$ and $a \in Z(G)$. Then $gag^{-1} = gg^{-1}a = a \in Z(G)$. So $G/Z(G)$ is defined and we have $|G/Z(G)| = p$. So $G/Z(G)$ is cyclic, i.e. there exists $h \in G$ such that $\langle hZ(G) \rangle = G/Z(G)$.

For any $g \in G$, $gZ(G) \in \langle hZ(G) \rangle$. Thus there is an integer m such that

$$gZ(G) = (hZ(G))^m = h^m Z(G).$$

since $g \in Z(G)$, there is $x \in Z(G)$ such that $g = h^m x$. Take $g_1, g_2 \in G$. So there exist integers m_1, m_2 and $x_1, x_2 \in Z(G)$ such that $g_1 = h^{m_1} x_1$ and $g_2 = h^{m_2} x_2$.

$$\begin{aligned} g_1 g_2 &= h^{m_1} x_1 h^{m_2} x_2 \\ &= h^{m_1} h^{m_2} x_1 x_2 \\ &= h^{m_1+m_2} x_1 x_2 \\ &= h^{m_2} h^{m_1} x_1 x_2 \\ &= h^{m_2} x_2 h^{m_1} x_1 \\ &= g_2 g_1. \end{aligned}$$

So G is abelian. □

Example 3.19. Determine the class equation for Q_8 (the Quaternion group), defined as $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$, where

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad I = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad J = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \quad K = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},$$

and $i^2 = -1$. The set has the following relations:

$$\begin{gathered} I^2 = J^2 = K^2 = -1, \\ IJ = K,\ JK = I,\ KI = J, \\ JI = -K,\ KJ = -I,\ IK = -J. \end{gathered}$$

The Cayley table for this group is given as follows.

	1	-1	I	$-I$	J	$-J$	K	$-K$
1	1	-1	I	$-I$	J	$-J$	K	$-K$
-1	-1	1	$-I$	I	$-J$	J	$-K$	K
I	I	$-I$	-1	1	K	$-K$	$-J$	J
$-I$	$-I$	I	1	-1	$-K$	K	J	$-J$
J	J	$-J$	$-K$	K	-1	1	$-I$	I
$-J$	$-J$	J	K	$-K$	1	-1	I	$-I$
K	K	$-K$	J	$-J$	I	$-I$	-1	1
$-K$	$-K$	K	$-J$	J	$-I$	I	1	-1

We have the following inverses.

$$\begin{aligned} (1)^{-1} &= 1 & \qquad (-1)^{-1} &= -1 \\ (I)^{-1} &= -I & (-I)^{-1} &= I \\ (J)^{-1} &= -J & (-J)^{-1} &= J \\ (K)^{-1} &= -K & (-K)^{-1} &= K \end{aligned}$$

We have the following orbits.

$$\begin{aligned} \mathcal{O}_1 &= \{1\} & \qquad \mathcal{O}_{-1} &= \{-1\} \\ \mathcal{O}_I &= \{I, -I\} & \mathcal{O}_{-I} &= \{I, -I\} \\ \mathcal{O}_J &= \{J, -J\} & \mathcal{O}_{-J} &= \{J, -J\} \\ \mathcal{O}_K &= \{K, -K\} & \mathcal{O}_{-K} &= \{K, -I\} \end{aligned}$$

We also have $Z(Q_8) = \mathcal{O}_1 \cup \mathcal{O}_{-1}$.

So, using the class equation,

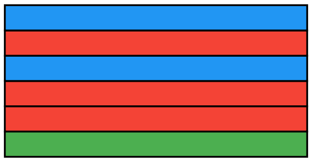
$$8 = |Q_8| = |Z(Q_8)| + |\mathcal{O}_I| + |\mathcal{O}_J| + |\mathcal{O}_K| = 2 + 2 + 2 + 2.$$

This shows $|Q_8| = p^3$ for $p = 2$ prime, but Q_8 is not abelian.

3.4 Lecture 11 — Counting and Burnside's Equation

We would like to apply group actions to solve counting problems.

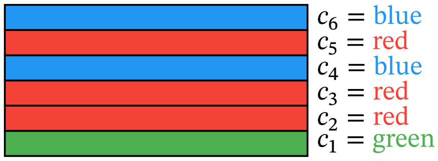
Problem: We have a flag with six equal stripes. We can colour the bands with red, blue, or green. We want to count the number of possible flags. Below is an example of such a flag.



Note that a flag can be represented by a six tuple,

$$(c_1, c_2, c_3, c_4, c_5)$$

with $c_i \in \{\text{red}, \text{green}, \text{blue}\}$.



Let $X = \{\text{all such six tuples}\}$. We have $|X| = 3^6$. Let τ be the permutation that corresponds to "flipping" the flag:

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

Let $G = \{(1), \tau\}$. Make X into a G-set by

$$G \times X \to X$$
$$(\sigma, (c_1, \dots, c_6)) \mapsto \begin{cases} (c_1, \dots, c_6) & \text{if } \sigma = (1), \\ (c_6, \dots, c_1) & \text{if } \sigma = \tau. \end{cases}$$

For any $x \in X$, $\mathcal{O}_x = \{\sigma \cdot x \mid \sigma \in G\} = \{(c_1, \dots, c_6), (c_6, \dots, c_1)\}$, where $x = (c_1, \dots, c_6)$. So

$$|\mathcal{O}_x| = \begin{cases} 1 & \text{if } x = \tau \cdot x, \\ 2 & \text{if } x \neq \tau \cdot x. \end{cases}$$

Recall that orbits partition X:

$$X = \mathcal{O}_{x_1} \cup \mathcal{O}_{x_2} \cup \cdots \cup \mathcal{O}_{x_k}.$$

So the solution to our problem is to count the number of distinct orbits (each orbit consists of distinct flags).

Recall that the stabilizer of x is the set

$$G_x = \{g \in G \mid g \cdot x = x\}.$$

Lemma 3.20. Suppose X is a G-set and $x \sim y$, i.e. $y = g \cdot x$ for some $g \in G$. Then if $G_x \cong G_y$, then $|G_x| = |G_y|$.

Proof. Let $g \in G$ be such that $y = g \cdot x$ and so $g^{-1} \cdot y = x$. Define a map

$$\begin{aligned} \Phi : \ G_x &\to G_y, \\ a &\mapsto gag^{-1} \end{aligned}$$

Note $gag^{-1} \in G_y$ since

$$\begin{aligned} gag^{-1} \cdot y &= ga \cdot (g^{-1} \cdot y) \\ &= ga \cdot x \\ &= g \cdot (a \cdot x) \\ &= g \cdot x \\ &= y \end{aligned}$$

This is a homomorphism since

$$\begin{aligned} \Phi(ab) &= gdbg^{-1} \\ &= (gag^{-1})(gbg^{-1}) \\ &= \Phi(a)\Phi(b) \end{aligned}$$

It is injective since if

$$\Phi(a) = gag^{-1} = gbg^{-1} = \Phi(b),$$

we have $a = b$ by cancellation. It is surjective since if $h \in G_y$, then $g^{-1}hg \in G_x$ since

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

Thus $\Phi(g^{-1}hg) = g(g^{-1}hg)g^{-1} = h$. $\square$

Theorem 3.21 (Burnside)**.** Let G be a finite group acting on a set X. If k is the number of distinct orbits of X, then

$$k = \frac{1}{|G|}\sum_{g\in G}|X_g|, \quad \text{where } X_g = \{x \mid g\cdot x = x\}.$$

Proof. We want to count all solutions to $g\cdot x = x$. We can count in two ways.

Method 1: Fix g and count all $x \in X$ such that $g\cdot x = x$. So if we sum over all $g \in G$, then number of solutions is

$$\sum_{g\in G}|X_g|.$$

Method 2: Fix an $x \in X$ and count all $g \in G$ such that $g\cdot x = x$. Summing over all x,

$$\sum_{x\in X}|G_x|.$$

We will equate these. So

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

We will first refine the index of summation on the RHS. Recall $X = \mathcal{O}_{x_1}\cup\cdots\cup\mathcal{O}_{x_k}$.

$$\sum_{x\in X}|G_x| = \sum_{x\in\mathcal{O}_{x_1}}|G_x| + \cdots + \sum_{x\in\mathcal{O}_{x_k}}|G_x|.$$

By Lemma 3.20, $|G_x| = |G_y|$ for all $x, y \in \mathcal{O}_{x_i}$. So

$$\sum_{x\in\mathcal{O}_{x_i}}|G_x| = |G_{x_i}||\mathcal{O}_{x_i}|.$$

Thus,

$$\sum_{x\in X}|G_x| = |G_{x_1}||\mathcal{O}_{x_1}| + \cdots + |G_{x_k}||\mathcal{O}_{x_k}|.$$

But $|\mathcal{O}_{x_i}| = |G|/|G_{x_i}| = [G : G_{x_i}]$. Thus

$$\sum_{x\in X}|G_x| = |G_{x_1}|\frac{|G|}{|G_{x_1}|} + \cdots + |G_{x_k}|\frac{|G|}{|G_{x_k}|} = k|G|.$$

So

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

□

Let's come back around to the flag problem. Our group is $G = \{(1), \tau\}$, so $|G| = 2$. We compute:

$$X_{(1)} = \{x \mid (1)\cdot x = x\} = X \Rightarrow |X_{(1)}| = 3^6$$
$$X_\tau = \{x \mid \tau\cdot x = x\} = \{(c_1,c_2,c_3,c_4,c_5,c_6) \mid c_1 = c_6, c_2 = c_5, c_3 = c_4\} \Rightarrow |X_\tau| = 3^3$$

So the number of flags = the number of orbits which, by Burnside's Theorem, is

$$\frac{1}{2}(|X_{(1)}| + |X_{\tau}|) = 378.$$

Chapter 4

The Sylow Theorems

4.1 Lecture 12 — Sylow Theorem I

Recall that Lagrange's Theorem states that the order of a subgroup divides the order of the group containing it.

The Sylow theorems give us a partial converse, i.e. if $|G| = n$ and if we know the factorization of n, we can deduce *some* things about its subgroups.

Theorem 4.1 (Sylow Theorem I)**.** Let G be a finite group. If p is prime and if p^k divides $|G|$, then G has a subgroup of order p^k.

Example 4.2. Take S_7. We know $|S_7| = 7! = 2^4 \cdot 3^2 \cdot 5 \cdot 7$. By the theorem, S_7 has subgroups of order $2, 2^2, 2^3, 2^4, 3, 3^2, 5, 7$.

Recall the following definition

Definition 4.3 (p-group)**.** A group G is a p-group (p prime) if for all $g \in G$, $|g| = p^t$ for some integer t.

A subgroup H of G is a p-subgroup if H is a p-group.

Theorem 4.4 (Cauchy)**.** Let G be a finite group and p a prime with p dividing $|G|$. Then G has a subgroup of order p.

We already proved this for abelian groups (Lemma 2.21). To prove the general case, we use the class equation (3.1).

Proof. If $|G| = p$ (p prime), then G is cyclic and G is a subgroup of itself of order p.

This takes care of cases where $p = 2, 3$.

Assume $|G| = n$ and that the result holds for positive integers $k < n$. If $n = p$, we are done. Via the class equation, there exist $x_1, x_2, \dots, x_n \in G$ such that

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_n)],$$

with $[G : C(x_i)] > 1$ for each i. Note that if $|G| = |Z(G)|$, then G is abelian and the result is true by Lemma 2.21. We consider two cases.

Case 1: Suppose p does *not* divide $[G : C(x_i)]$ for some i. So $|G| = [G : C(x_i)]|C(x_i)|$. Thus p must divide $|C(x_i)|$ and $|C(x_i)| < |G|$. So by induction, $C(x_i)$ has an element of order p and so does G.

Case 2: Suppose p divides $[G : C(x_i)]$ for all i. So p divides $|Z(G)|$, since

$$|Z(G)| = |G| - [G : C(x_1)] - \cdots - [G : C(x_n)].$$

But $Z(G)$ has an element of order p and so does G. □

Corollary 4.5. G is a p-group if and only if $|G| = p^t$ for some integer t.

Proof. Suppose $|G| = p^t$. Let $g \in G$. So $|g|$ divides $|G| = p^t$ and we must have $|g| = p^r$ for some integer $r \leq t$.

Now suppose G is a p-group. Suppose that q is a prime different than p such that q divides $|G|$. But then by Theorem 4.4, G has an element of order q. This contradicts that G is a p-group. □

We state a theorem without proof.

Theorem 4.6 (Correspondence Theorem)**.** Let $L \subseteq G/N$. Then L is a subgroup if and only if there is a subgroup H of G with

$$N \subseteq H \subset G$$

and $H/N = L$.

We can now prove the first Sylow theorem.

Proof. The proof is by induction on $|G| = n$. The result evidently holds if $|G| = p$ (p prime), since $G \cong \mathbb{Z}_p$ and thus has a subgroup of order p^0 and p^1 (both trivial subgroups).

Assume $|G| = n$ and that the result holds for integers $\ell < n$. We can assume n is not prime. By the class equation, there exist $x_1, \dots, x_n \in G$ such that

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_n)],$$

with $[G : C(x_i)] > 1$ for each i.

Case 1: Suppose p does *not* divide $[G : C(x_i)]$ for some i. So $|G| = [G : C(x_i)]|C(x_i)|$. Thus p^k must divide $|C(x_i)|$ and $|C(x_i)| < |G|$. So by induction, $C(x_i)$ has a subgroup of order p^k and so does G.

Case 2: Suppose p divides $[G : C(x_i)]$ for each i. Then by the class equation, p divides $|Z(G)|$. By Theorem 4.4 (Cauchy), there exists $g \in Z(G)$ with $N = \langle g \rangle \subseteq Z(G)$ with $|G| = p$. We claim that N is normal in G. Take $h \in G$ and $m \in N$. Then $hmh^{-1} = hh^{-1}m = m \in N$, so $m \in Z(G)$. Thus the quotient G/N is well-defined. Because $|N| = p$, $|G/N| = n/p$. So p^{k-1} divides $|G/N| = n/p$. So G/N has a subgroup of order p^{k-1}. Call this subgroup $L \subset G/N$. By the correspondence theorem (Theorem 4.6), there is a subgroup H of G with

$$N \subseteq H \subset G$$

and $H/N = L$. So $|L| = |H|/|N| = p^{k-1}$. So $|H| = p^{k-1}|N| = p^k$. □

Example 4.7. Let G be a finite abelian group with $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Then

$$G \cong \mathbb{Z}_{p_1^{r_{1,1}}} \times \mathbb{Z}_{p_1^{r_{1,2}}} \times \cdots \times \mathbb{Z}_{p_1^{r_{1,s_1}}} \times \mathbb{Z}_{p_2^{r_{2,1}}} \times \cdots$$

Note that $\mathbb{Z}_{p_1^{r_{1,1}}} \times \mathbb{Z}_{p_1^{r_{1,2}}} \times \cdots \times \mathbb{Z}_{p_1^{r_{1,s_1}}}$ is a p_1-subgroup of G. Also,

$$|\mathbb{Z}_{p_1^{r_{1,1}}} \times \mathbb{Z}_{p_1^{r_{1,2}}} \times \cdots \times \mathbb{Z}_{p_1^{r_{1,s_1}}}| = p^{\alpha_1}.$$

Example 4.8. Suppose N is normal in G and both G/N and N are p-groups. Then G is also a p-group.

Infinite case: Let $g \in G$. If $g \in N$, then $|g| = p^t$. If $g \notin N$, consider $gN \in G/N$. So $|(gN)| = p^\ell$. This means $(g)^{p^\ell} \in N$. But N is a p-group, so $((g)^{p^l})^{p^t} = e$.

4.2 Lecture 13 — Sylow Theorem II

Definition 4.9. A Sylow p-subgroup P of G is a subgroup that is a maximal p-subgroup in G. That is, if $|G| = pm$ for an integer m with $\gcd(p, m) = 1$, then any subgroup of order p^r is a Sylow p-subgroup.

> *Remark.* The first Sylow theorem implies that there always exist at least one Sylow p-subgroup.

The first Sylow theorem used the conjugation group action. The proof of the second and third Sylow theorem use a different group action.

Let $S = \{\text{all subgroups of } G\}$. We define a G-action on S by

$$\begin{aligned} &G \times S \to S, \\ &(g, K) \mapsto gKg^{-1} = g \cdot K. \end{aligned}$$

Definition 4.10. We say that subgroups L and K are **congruent** if there exists $g \in G$ such that

$$L = gKg^{-1}.$$

If H is a subgroup of G, we say that L and K are H-congruent if there exists $h \in H$ such that

$$L = hKh^{-1}.$$

Definition 4.11 (normalizer). The **normalizer** of a subgroup H of G is the set

$$N(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Proposition 4.12. Let H be a subgroup of G. The normalizer $N(H)$ has the following properties:

(a) $H \subseteq N(H) \subseteq G$;

(b) H is normal in $N(H)$;

(c) $N(H)$ is the largest normal subgroup of G such that H is normal in it.

Lemma 4.13. Let P be a Sylow p-subgroup and suppose $x \in G$ is such that $|x| = p^m$ for some integer m. If $xPx^{-1} = P$, then $x \in P$

Proof. Note first that $x \in N(P)$ and, since P is normal in $N(P)$, $\langle xP \rangle$ is a cyclic subgroup of $N(P)/P$. Note also that $|xP| = p^\ell$ for some integer ℓ, since

$$(xP)^{p^m} = x^{p^m}P = eP = P.$$

So $|xP|$ divides p^m.

By the Correspondence Theorem (4.6), there exists a subgroup H such that

$$P \subseteq H \subseteq N(P),$$

and $H/P = \langle xP \rangle$. So $|H| = |\langle xP \rangle||P|$, i.e. $|H|$ is a power of p. But P is the largest subgroup that is a power of p. So $H = P$ and thus $xP = e$ or, more succinctly $x \in P$. □

Lemma 4.14. Let H and K be subgroups of G. The number of distinct H-conjugates of K is $[H : N(K) \cap H]$.

Proof. Observe, $|\{hKh^{-1} \mid h \in H\}| = |\mathcal{O}_K|$. This is the number of orbits of K under the action defined earlier. So this equals $[H : H_K]$, where $H_K = \{h \in H \mid h \cdot K = K \Leftrightarrow hKh^{-1} = K\} = N(K) \cap H$. We thus have $[H : N(K) \cap H]$. □

Theorem 4.15 (Sylow Theorem II)**.** Let G be a finite group and p be a prime such that p divides $|G|$. If P_1 and P_2 are two Sylow p-subgroups of G, they are conjugates, i.e. there exists $g \in G$ such that

$$P_2 = gP_1g^{-1}.$$

Proof. Suppose $|G| = p^r m$, with $\gcd(p, m) = 1$, and let P be a Sylow p-subgroup with $|P| = p^r$. Let $S = \{gPg^{-1} \mid g \in G\}$. By Lemma 4.14, the number of distinct conjugates is given by

$$|S| = [G : N(P) \cap G] = [G : N(P)].$$

We have $|G| = [g : N(P)]|N(P)|$. Since $P \subseteq N(P)$ and p^r divides $|N(P)|$. This forces the fact that p does not divide $[G : N(P)] = |S|$.

Let Q be any other Sylow p-subgroup. We want to show $Q \in S$. For each $P_i \in S$, consider the Q-conjugates of P_i, i.e.

$$\{qP_iq^{-1} \mid q \in Q\} \subseteq S$$

Also, $|\{qP_i \mid q \in G\}| = [Q : N(P_i)capQ]$, by Lemma 4.14. Since $|Q| = |N(P_i) \cap Q|[Q : N(P_i)hQ] = p^r$. So we have that p^ℓ divides $[Q : N(P_i) \cap Q]$.

Let $A_i = \{qP_iq^{-1} \mid q \in Q\}$. The collection of all $P_i's$ partitions the set S. Note that

$$|A_i| = [Q : N(P_i) \cap Q] = p^{\ell_i},$$

with $\ell_i \geq 0$.

If each $|A_i| \geq p$, this forces the fact that p divides $|S|$. But p does <u>not</u> divide $|S|$. So $|A_i| = 1$ if and only if $\{qP_iq^{-1} \mid q \in Q\} = \{P_i\}$. But $|q| = p^m$ for some m and $qP_iq^{-1} = P_i$. By Lemma 4.13, this means $q \in P_i$. So for all $q \in Q$, $q \in P_i$, i.e. $Q \subseteq P_i$. But $|Q| = |P_i|$. So $Q = P_i$. □

Corollary 4.16. Let G be a group and P be a Sylow p-subgroup of G. Then P is normal if and only if P is the only Sylow p-subgroup of G.

Proof. Suppose P and Q are Sylow p-subgroups. Then they are conjugates by the second Sylow theorem (4.15). That is, $Q = gPg^{-1}$ for all $g \in G$. But P is normal in G. So $P = gPg^{-1}$. Thus, $P = Q$.

Now suppose P is the unique Sylow p-subgroup of G. Then for any $g \in G$, $gPg^{-1} = P$ since $|gPg^{-1}| = |P|$, i.e. gPg^{-1} is also a Sylow p-subgroup. So P is normal since this is true for all $g \in G$. □

4.3 Lecture 14 — Sylow Theorem III

Recall that if $|G| = p^r m$ with p not dividing m, then any subgroup P of G with $|P| = p^r$ is a Sylow p-subgroup. The first Sylow theorem shows that a Sylow p-subgroup always exists.

The third Sylow theorem counts the number of Sylow p-subgroups.

Theorem 4.17 (Sylow Theorem III)**.** Let G be a group with p prime dividing $|G|$. If n_p is the number of distinct Sylow p-subgroups, then

(a) $n_p \equiv 1 \pmod{p}$, and

(b) n_p divides $|G|$.

Example 4.18. Show that any group G with $|G| = 45 = 3^2 \cdot 5$ has exactly one Sylow 5-subgroup.

Solution. By the third Sylow theorem,

- $n_5 \in \{1, 6, 11, 16, 21, 26, 31, 36, 41\}$, and
- $n_5 \in \{1, 3, 5, 9, 15, 45\}$

So we must have that $n_5 = 1$. □

In the previous lecture, we saw that if P is the only Sylow p-subgroup, then P is normal. So in any group G with $|G| = 45$, the Sylow 5-subgroup is normal. Recall also that G is simple if it has no normal subgroups.

Corollary 4.19. There are no simple groups of order 45.

Lemma 4.20. Let H and K be subgroups of G. The number of distinct H-conjugates of K is

$$[H : N(K) \cap H].$$

Lemma 4.21. Suppose $|x| = p^a$ and $xPx^{-1} = P$ for some Sylow p-subgroup. Then $x \in P$.

These lemmas will help prove the third Sylow theorem.

Proof. Let $S = \{P = P_1, P_2, \dots, P_k\}$ be the set of all the distinct Sylow p-subgroups of G.

We want $n_p = k$. We can make S into a P-set via the action

$$\begin{aligned} &P \times S \to S,\\ &(x, P_i) \mapsto xP_ix^{-1} = x \cdot P_i \end{aligned}$$

Note that $xP_ix^{-1} \in S$ by the second Sylow theorem since any two Sylow p-subgroups are related by conjugation.

Since $\cdot$ is a group action, S is partitioned by the orbits. If $P = P_1$, the orbit of P is

$$\mathcal{O}_P = \{xPx^{-1} \mid x \in P\} = P.$$

If $P_i \neq P_1$, the orbit of P_i is

$$\mathcal{O}_{P_i} = \{xP_ix^{-1} \mid x \in P\}.$$

Now,

$$\begin{aligned} |\mathcal{O}_{P_i}| &= \text{number of distinct } P\text{-conjugates of } P_i\\ &= [P : N(P_i) \cap P]\\ &= \frac{|P|}{|N(P_i) \cap P|}\\ &= p^{a_i}, \quad \text{with } a_i \geq 0. \end{aligned}$$

In addition, if $P_i \neq P$, then $|\mathcal{O}_{P_i}| > 1$ because if $\{xP_ix^{-1} \mid x \in P\} = \{P_i\}$, i.e. $xP_ix^{-1} = P_i$ for all $x \in P$. But Lemma 4.21 forces $P = P_1 = P_i$. So $|\mathcal{O}_{P_i}| = p^{a_i}$ with $a_i \geq 1$. To summarize, we have the partition

$$P = \mathcal{O}_P \cup \mathcal{O}_{P_2} \cup \cdots \cup \mathcal{O}_{P_t}$$

So

$$\begin{aligned} |S| &= |\mathcal{O}_P| + |\mathcal{O}_{P_2}| + \cdots + |\mathcal{O}_{P_t}|\\ &= 1 + p^{a_1} + p^{a_2} + \cdots + p^{a_t}. \end{aligned}$$

Thus, $n_p = |S| \equiv 1 \pmod{p}$.

At the same time, S is a G-set via the action

$$\begin{aligned} &G \times S \to S,\\ &(g, P_i) \mapsto gP_ig^{-1} = g * P_i. \end{aligned}$$

For any $P \in S$, the orbit under the action $*$ is

$$\mathcal{O}_P\{gPg^{-1} \mid g \in G\} = S$$

(by the second Sylow theorem). So

$$\begin{aligned} |\mathcal{O}_P| &= [G : N(P) \cap G]\\ &= [G : N(P)]\\ &= \frac{|G|}{|N(P)|}. \end{aligned}$$

So $|N(P)||\mathcal{O}_P| = |G|$. But $n_p = |\mathcal{O}_P|$, so n_p divides $|G|$. $\square$

We now look at some applications of this result.

Recall that if $|G| = p$ with p prime, then $G \cong \mathbb{Z}_p$.

Theorem 4.22. Suppose $|G| = pq$ with p, q primes and $p < q$. Then G has a unique Sylow q-subgroup and G is not simple. Additionally, if $q \not\equiv 1 \pmod{p}$, then $G \cong \mathbb{Z}_{pq}$.

Proof. We need n_q to be the number of distinct Sylow q-subgroups. So $n_q \in \{1, q, p, pq\}$. We note that $q \equiv 0 \pmod{q}$, $pq \equiv \ \pmod{q}$ and $p \equiv p \pmod{q}$ since $p < q$. So $n_q = 1$ and thus there is only one Sylow q-subgroup.

Now count n_p = number of Sylow p-subgroups if $q \neq 1 \pmod{p}$. So $n_p \in \{1, q, p, pq\}$. Note $p \equiv 0 \pmod{p}$, $pq \equiv 0 \pmod{p}$. We are given $q \not\equiv 1 \pmod{p}$. So $n_p = 1$. To summarize, we have a Sylow q-subgroup, say Q and a Sylow p-subgroup, say P, with $|Q| = q$ and $|P| = p$. We claim G is the internal direct product of P and Q.

We need to check:

- $Q \cap P = \{e\}$
- $QP = G$
- $qp = pq$ for all $p \in P$ and $q \in Q$ (use the fact that P and Q are normal)

These hold (check!) so $G \cong Q \times P \cong \mathbb{Z}_q \times \mathbb{Z}_p \cong \mathbb{Z}_{pq}$. □

Example 4.23. Suppose $|G| = 77 = 7 \cdot 11$. Since $11 \not\equiv 1 \pmod{p}$, $G \cong \mathbb{Z}_{77}$.

Example 4.24. If $|G| = 15 = 3 \cdot 5$, we have that $3 < 5$ and $5 \not\equiv 1 \pmod{3}$, so $G \cong \mathbb{Z}_{15}$.

4.4 Lecture 15 — Applications of the Sylow Theorems

The Sylow Theorems have two main applications/goals:

(1) For some n, classify all groups with $|G| = n$.

(2) For some n, we can show that all groups with $|G| = n$ are not simple. Equivalently, G must have a nontrivial subgroup.

Example 4.25. For application (1), as seen last lecture, if $|G| = pq$ with p and q prime, $p < q$ and $q \not\equiv 1 \pmod{p}$. Then $G \cong \mathbb{Z}_{pq}$. So if $|G| = 15 = 3 \cdot 5$, then $G \cong \mathbb{Z}_{15}$.

Let's look at some examples of application (2). We rely on a variant of Corollary 4.16.

Theorem 4.26. Suppose p divides $|G|$. Then G has a unique Sylow p-subgroup P if and only if P is normal in G.

Example 4.27. Show that any group G with $|G| = 20 = 2^2 \cdot 5$ is not simple.

Proof. By the Third Sylow Theorem (4.17), if n_5 is the number of Sylow 5-subgroups of G, we must have

$$n_5 \in \{1, 2, 4, 5, 10, 20\},$$

and $n_5 \equiv 1 \pmod{5}$. The only integer satisfying this condition in the above set is 1. So $n_5 = 1$. Thus there is only one Sylow 5-subgroup and it must be normal. So G is not simple. □

Example 4.28. Show that any group G with $|G| = 56 = 2^3 \cdot 7$ is not simple.

Proof. By the Third Sylow Theorem (4.17), if n_7 is the number of Sylow 7-subgroups of G, we must have

$$\{1, 8, 15, 22, 29, 36, 43, 50\} \quad (n_7 \equiv 1 \pmod{7}),$$

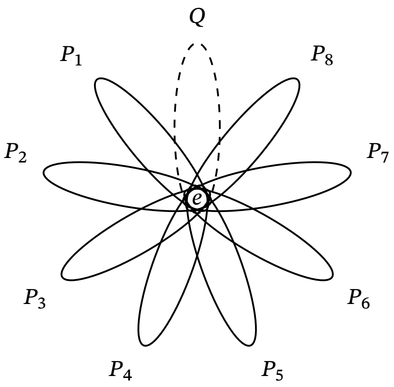
and

$$n_7 \in \{1, 2, 4, 7, 8, 14, 28, 56\} \quad (n_7 \text{ divides } |G|).$$

As such, $n_7 = 1$ or $n_7 = 8$. In the case that $n_7 = 1$, G has a unique Sylow 7-group, which must be normal and so G is not simple.

What happens if $n_7 = 8$? Let $P_1, P_2, \ldots, P_8$ be these 8 Sylow 7-subgroups of G. Note that $|P_i| = 7$ for each i. Now for $i \neq j$, $|P_i \cap P_j|$ divides $|P_i|$ and so must be 1 or 7. But it cannot be 7 since this would imply that $P_i \cap P_j = P_i$ or $P_i \cap P_j = P_j$. So we must have that $|P_i \cap P_j| = 1$.

In total, these Sylow 7-subgroups cover $6 \cdot 8 + 1 = 49$ elements of G. Now by the First Sylow Theorem (4.1), there exists a Sylow 2-group Q with $|Q| = 8$. Also, $|Q \cap P_i| = 1$ for each i. So Q contains e and 7 other elements. Thus, Q must be the unique Sylow 2-subgroup of G, which must be normal.



□

Example 4.29. Suppose $|G| = p^n k$ with p prime and $p > k$. Prove that G is not simple.

Proof. Since $|G| = p^n k$, G has at least one Sylow p-subgroup of order p^n. If n_p is the number of Sylow p-subgroups of G, then $n_p \equiv 1 \pmod{p}$. So $n_p = 1 + ap$, $a \in \mathbb{Z}$, $a \geq 0$. But also, n_p divides $|G| = p^n k$. That is, $1 + ap$ divides $p^n k$. But $\gcd(1 + ap, p^n) = 1$. So we must have $1 + ap$ divides k. Thus, $k \geq 1 + ap$. If $a \geq 1$, this means $k \geq 1 + ap \geq 1 + p > k$, a contradiction. So $a = 0$ and thus $n_p = 1$. It follows that G is not simple. □

Example 4.30. Any group of order 33 is not simple since $33 = 11 \cdot 3$.

Theorem 4.31. Let $G' = \langle aba^{-1}b^{-1} \mid a, b \in G \rangle$. Then,

(a) G' is normal in G,

(b) G/G' is abelian, and

(c) if N is normal in G and G/N is abelian, then $G' \subseteq N$.

G' as defined above is called the **commutator** of G.

Example 4.32. Show all groups G with $|G| = 255 = 3 \cdot 5 \cdot 17$ are cyclic.

Proof. Since $(3 \cdot 5) < 17$, the previous result implies G has one Sylow 17-subgroup, which is normal. Let H be this Sylow 17-subgroup. Then G/H is a group with order $255/17 = 15$. By the previous fact, $G/H \cong \mathbb{Z}_{15}$, which is abelian. Let G' be the commutator subgroup. By Theorem 4.31, $G' \subseteq H$. So $|G'| = 1$ or $|G'| = 17$. If $|G'| = 1$, then $G/G' \cong G$ is abelian. So $G \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{255}$ by the FToFAG. Now suppose $|G'| = 17$. We count the number of Sylow 3-subgroups and Sylow 5-subgroups.

Divisors of 255	mod 3	mod 5
1	1	1
3	0	3
5	2	0
17	2	2
$3 \cdot 5 = 15$	0	0
$3 \cdot 17 = 51$	0	1
$5 \cdot 17 = 85$	1	0
$3 \cdot 5 \cdot 17 = 255$	0	0

So the number of Sylow 3-subgroups is 1 or 85 and the number of Sylow 5-subgroups is 1 or 51.

We cannot have both 85 Sylow 3-subgroups and 51 Sylow 5-subgroups. Indeed, if Q is a Sylow 3-subgroup and P is a Sylow 5-subgroup, then $|Q \cap P| = 1$. The Sylow 3-subgroup of order 85 consists of $2 \times 85 + 1 = 170 + 1$ elements and the Sylow 5-subgroup of order 51 consists of $4 \times 51 + 1 = 204 + 1$ elements, which would yield $374 + 1$ distinct elements, more than $|G|$.

If there is only one Sylow 3-subgroup Q, then Q is normal and $|G/Q| = 5 \cdot 17$. But then, by a theorem, this implies $G/Q \cong \mathbb{Z}_{5 \cdot 17}$. So by Theorem 4.31 $G' \subseteq Q$. In particular, $|G'| = 17$ and $|Q| = 3$, yielding a contradiction.

If there is only one Sylow 5-subgroup P, then P is normal and $|G/P| = 3 \cdot 17$. By the same theorem, $G/P \cong \mathbb{Z}_{3 \cdot 17}$, so $G' \subseteq P$ which would imply $|G'| = 17$ divides $|P| = 5$, yielding another contradiction.

As such we must have $|G'| = 1$ and so $G/G' \cong G$ is abelian. □

4.5 Lecture 16 — Group Theory and Linear Algebra

Let $\mathscr{M}_n(\mathbb{R})$ be the set of all $n \times n$ matrices with entries in $\mathbb{R}$. Ignoring matrix multiplication, $\mathscr{M}_n(\mathbb{R})$ is a perfectly valid group under addition (check!). It is however the case that $\mathscr{M}_n(\mathbb{R})$ is not a group under matrix multiplication—many matrices (eg. the zero matrix) do not have a defined multiplicative inverse.

Recall that $A \in \mathscr{M}_n(\mathbb{R})$ is invertible if and only if $\det(A) \neq 0$.

Definition 4.33 (general linear group)**.** Let

$$\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathscr{M}_n(\mathbb{R}) \mid \det(A) \neq 0\}.$$

Then $\mathrm{GL}_n(\mathbb{R})$ is called the **general linear group** of degree n over $\mathbb{R}$.

We have the following facts:

- $\mathrm{GL}_n(\mathbb{R})$ is a group under multiplication.
- $|\mathrm{GL}_n(\mathbb{R})| = \infty$.
- $\mathrm{GL}_n(\mathbb{R})$ is not abelian.
- The identity is I_n.
- Given $A \in \mathrm{GL}_n(\mathbb{R})$, its inverse is A^{-1}.

Recall that $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ is a group under multiplication

Theorem 4.34. The map $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ given by $A \mapsto \det(A)$ is a group homomorphism.

Proof. Let $A, B \in \mathrm{GL}_n(\mathbb{R})$. Then $\det(AB) = \det(A)\det(B)$. So det is a group homomorphism. □

We can use the kernel of det to find the canonical normal subgroup:

$$\ker(\det) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\}.$$

Definition 4.35 (special linear group)**.** The **special linear group** of degree n over $\mathbb{R}$, denoted $\mathrm{SL}_n(\mathbb{R})$, is the kernel of det. That is, $\mathrm{SL}_n(\mathbb{R})$ consists of all $n \times n$ matrices over $\mathbb{R}$ with determinant 1.

By the First Isomorphism Theorem,

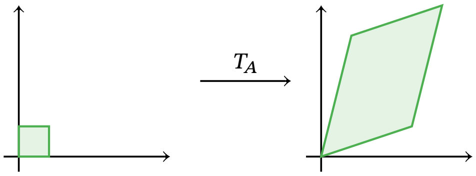
$$\mathrm{GL}_n(\mathbb{R}) / \mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*.$$

Recall that a matrix A corresponds to a unique linear transformation $T_A : \mathbb{R}^n \to \mathbb{R}^n$ given by $T_A(\mathbf{x}) = A\mathbf{x}$.

Example 4.36. Let $A = \begin{bmatrix} 1 & 3 \\ 4 & 1 \end{bmatrix}$. What does T_A do to the unit square?

Observe the following.

$$T_A\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \begin{bmatrix} 1 \\ 4 \end{bmatrix}, \quad T_A\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 3 \\ 1 \end{bmatrix}, \quad T_A\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 4 \\ 5 \end{bmatrix}.$$



Recall that if S is a set with volume V in $\mathbb{R}^n$, the volume of $T_A(S)$ is $|\det(A)|B$. In particular, if $A \in \mathrm{SL}_n(\mathbb{R})$, then the map $T_A : \mathbb{R}^n \to \mathbb{R}^n$ maps the unit cube to a parallelepiped of volume 1.

Recall that a matrix A is **orthogonal** if $A^\intercal = A^{-1}$.

Example 4.37. Take $A = \begin{bmatrix} \frac{3}{5} & -\frac{4}{5} \\ \frac{4}{5} & \frac{3}{5} \end{bmatrix}$.

$$\begin{aligned} AA^\intercal &= \begin{bmatrix} \frac{3}{5} & -\frac{4}{5} \\ \frac{4}{5} & \frac{3}{5} \end{bmatrix} \begin{bmatrix} \frac{3}{5} & \frac{4}{5} \\ -\frac{4}{5} & \frac{3}{5} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ &= I_2. \end{aligned}$$

Equivalently, a matrix A is orthogonal if its columns have norm 1 and are linearly independent.

Definition 4.38. Let

$$\mathrm{O}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^\intercal = A^{-1}\}.$$

Then $\mathrm{O}_n(\mathbb{R})$ is called the **orthogonal group** of degree n over $\mathbb{R}$.

It's easy to see that $\mathrm{O}_n(\mathbb{R})$ is a group under multiplication (check that it satisfies the subgroup criterion as a subgroup of $\mathrm{GL}_n(\mathbb{R})$!).

Proposition 4.39. If $A \in \mathrm{O}_n(\mathbb{R})$, then $\det(A) = \pm 1$.

Proof. We compute.

$$\begin{aligned} 1 &= \det(I_n) \\ &= \det(AA^{-1}) \\ &= \det(A)\det(A^{-1}) \\ &= \det(A)\det(A^{\mathsf{T}}) \\ &= \det(A)\det(A) \\ &= \det(A)^2 \end{aligned}$$

So $\det(A) = \pm 1$. ▢

Elements of $\mathrm{O}_n(\mathbb{R})$ preserve distance. Recall that, given

$$\mathbf{v} = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \qquad \text{and} \qquad \mathbf{w} = \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix},$$

the distance between $\mathbf{v}$ and $\mathbf{w}$ is

$$d(\mathbf{v}, \mathbf{w}) = \sqrt{(v_1 - w_1)^2 + \cdots + (v_n - w_n)^2} = \|\mathbf{v} - \mathbf{w}\|.$$

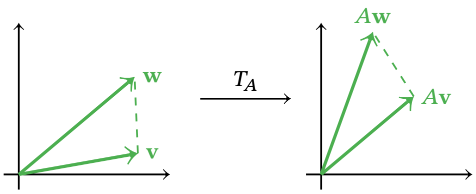
This actually characterizes elements of $\mathrm{O}_n(\mathbb{R})$.

Theorem 4.40. $A \in \mathrm{O}_n(\mathbb{R})$ if and only if

$$d(A\mathbf{v}, A\mathbf{w}) = d(\mathbf{v}, \mathbf{w}),$$

for all $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$.

Here's the picture, where the dashed lines have equal length.



Definition 4.41. We define the **special orthogonal group**, denoted $\mathrm{SO}_n(\mathbb{R})$, as

$$\begin{aligned} \mathrm{SO}_n(\mathbb{R}) &= \mathrm{O}_n(\mathbb{R}) \cap \mathrm{SL}_n(\mathbb{R}) \\ &= \{\text{all } n \times n \text{ orthogonal matrices with determinant } 1\}. \end{aligned}$$

We consider the special case for $\mathrm{O}_n(\mathbb{R})$ when $n = 2$.

Note that any $A \in \mathrm{O}_2(\mathbb{R})$ is entirely determined by where it takes $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

If $A \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$, then $a^2 + b^2 = 1$. Note that this implies

$$A = \begin{bmatrix} a & * \\ b & * \end{bmatrix}.$$

Since the columns of A must be orthogonal, then either

$$A = \begin{bmatrix} a & b \\ b & -a \end{bmatrix}, \quad \text{or} \tag{4.1}$$

$$A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \tag{4.2}$$

If we are in case (4.1), then

$$A = \begin{bmatrix} a & b \\ b & -a \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}, \quad \text{for } \theta \in [0, 2\pi),$$

i.e. A rotates vectors about the origin by an angle θ.

If we are in case (4.2), then

$$A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \underbrace{\begin{bmatrix} a & b \\ b & -a \end{bmatrix}}_{\text{rotation}} \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}}_{\text{flip about } x\text{-axis}}.$$

Chapter 5

Midterm

5.1 Lecture 17 — Midterm Review Questions

I. Finite Abelian Groups

A. Find all abelian groups of order 108.

B. Show that there are two abelian groups of order 108 with an element of order 54.

C. Suppose G is a finite abelian group such that 10 divides $|G|$. Prove that G has a cyclic subgroup of order 10.

D. Give an example of an abelian group such that 4 divides $|G|$, but G has no cyclic subgroup of order 4.

II. Solvable Groups

A. Find a composition series of $\mathbb{Z}_{20}$.

B. Suppose G has a series of subgroups

$$G = P_n \supset P_{n-1} \supset \cdots \supset P_1 \supset P_0 = \{e\},$$

where P_i is normal in P_{i+1} and $|P_{i+1}/P_i|$ is a prime number. Prove that G is a solvable group.

III. The Characteristic Equation

A. Suppose $|G| = 20$. Explain why

$$20 = 1 + 2 + 3 + 6 + 10$$

is not a valid class equation.

B. Suppose G is an abelian group with $|G| = 2024$. What is its class equation.

IV. Sylow Theorems

A. If $|G| = 175$, prove that G is abelian.

B. Let P be a Sylow p-subgroup of G. Prove P is the only Sylow p-subgroup contained in the normalizer of P,

$$N(P) = \{x \mid xPx^{-1} = P\}.$$

C. Suppose $|G| = p^r m$, where p is prime and m is some integer with $p \nmid m$, and suppose H is a normal subgroup of G with $|H| = p^\ell$. Prove H is a subgroup of all Sylow p-subgroups of G.

5.2 Lecture 18 — Midterm Test

Part A

Do all of Questions 1-6.

1. *(2 pts)* Write out all the non-isomorphic abelian groups of order 36.
2. *(2 pts)* Find a composition series for the group $\mathbb{Z}_{36}$. Justify your answer.
3. *(2 pts)* Let G be a finite group with $|G| = 36$. How many Sylow 3-subgroups can G have?
4. *(2 pts)* Iris is a student in MATH 4GR3 and she needs to find the class equation for a group G with $|G| = 36$. She shows you her answer:

   $$36 = 18 + 9 + 5 + 4.$$

   Although you don't know G, why do you know that Iris has an incorrect answer?
5. *(2 pts)* The following statement is false: "If G is a group with $|G| = 36$, and since $18 \mid 36$, then G must have an element of order 18." Give an example to show that this statement is false.
6. *(2 pts)* Prove that there is no simple group of order $190 = 2 \cdot 5 \cdot 19$.

Part B

Do three of Questions 7-10.

7. *(5 pts)* Let G be any finite abelian group with $|G| = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, with $a_i \geq 1$. Prove that G has a subgroup of order $p_1 p_2 \cdots p_r$.
8. *(5 pts)* Suppose that G is a finite group with subnormal series

   $$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\},$$

   where H_i is normal in H_{i+1}. Suppose that $|H_{i+1}/H_i| = s_{i+1}$ for $i = 0, 1, \ldots, n-1$. Prove that $|G| = s_1 s_2 \cdots s_n$.
9. *(5 pts)* Let G be a finite group such that the prime p divides $|G|$. Show that if $\{P_1, \ldots, P_s\}$ are all the distinct Sylow p-subgroups of G, then for any $g \in G$,

   $$\{gP_1g^{-1}, \ldots, gP_sg^{-1}\} = \{P_1, \ldots, P_s\}.$$

   That is, show that $\{gP_1g^{-1}, \ldots, gP_sg^{-1}\} = \{P_1, \ldots, P_s\}$ is also the set of all Sylow p-subgroups of G, but in a "shuffled" order.
10. *(5 pts)* Let G be a finite group with $|G| = p^r m$ with $p \nmid m$. Suppose $P_1, \ldots, P_s$ are all the distinct Sylow p-subgroups of G. Prove that $P_1 \cap P_2 \cap \cdots P_s$ is a normal subgroup of G.

    Hint. The previous question will help. Even if you don't do Question 9, you can assume it is true for this question.

Chapter 6

Ring Theory

6.1 Lecture 19 — Review of Rings I

Definition 6.1 (ring). A **ring** R is a set with binary operations $+$ and $\times$ called **addition** and **multiplication**, respectively, such that for all $a, b, c \in R$,

(a) $a + b = b + a$ for all $a, b \in R$ *(commutativity of addition)*,

(b) $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$ *(associativity of addition)*,

(c) there exists an element $0 \in R$ such that $a + 0 = 0 + a = a$ for every $a \in R$ *(additive identity)*,

(d) for every $a \in R$, there exists an element $b \in R$ such that $a + b = 0$ and we write $-a$ for b *(additive inverse)*,

(e) $(ab)c = a(bc)$ for all $a, b, c \in R$ *(associativity of multiplication)*, and

(f) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in R$ *(distributivity)*.

> *Remark.* A ring R is an abelian group under addition with additional structure.

We consider a few special cases for rings.

Definition 6.2 (ring with identity). A ring R is said to be a **ring with idenity** if there exists an element $1 \in R$ such that $a \times 1 = 1 \times a = a$.

Definition 6.3 (commutative ring). A ring R is said to be a **commutative ring** if $ab = ba$ for all $a, b \in R$.

Definition 6.4 (integral domain). A ring R is said to be an **integral domain** if

(a) R is a ring with identity,

(b) R is a commutative ring, and

(c) if $ab = 0$, then $a = 0$ or $b = 0$, i.e. R has no zero divisors.

Definition 6.5 (division ring). A ring R is said to be a **division ring** if R is a ring with identity and, if for all $a \in R$ with $a \neq 0$, there is an element $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Definition 6.6 (field). A ring R is said to be a **field** if R is a commutative division ring.

Definition 6.7 (unit). We say $a \in R$ with $a \neq 0$ is a **unit** if there exists $a^{-1} \in R$ such that $a^{-1}a = 1$.

Example 6.8. Consider the following with the usual operations:

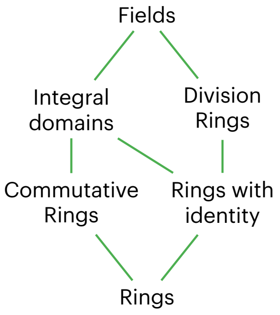
- $\mathbb{Q}[x]$, the polynomials with rational coefficients, are an integral domain.
- $\mathbb{Z}$ is an integral domain.
- $\mathbb{R}$, $\mathbb{Z}_p$ with p prime, $\mathbb{C}$ and $\mathbb{Q}$ are all fields.
- $\mathcal{M}_n(\mathbb{R})$ is not an integral domain,

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

- $E = \{2n \mid n \in \mathbb{Z}\}$ is a ring without identity.
- $\mathbb{Z}_n$ with n not prime is not an integral domain.
- $\mathcal{M}_n(\mathbb{R})$ is not a commutative ring.

Proposition 6.9. Every field F is also an integral domain.

Proof. Suppose $ab = 0$. If $a = 0$, we are done. Suppose $a \neq 0$. So $a^{-1} \in F$. So $a^{-1}(ab) = a^{-1} \cdot 0 = 0$. Also $a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$. So b must be 0. □



Definition 6.10. A **subring** of a ring R is a subset $S \subseteq R$ that is also a ring under the same operations.

Proposition 6.11 (Subring Criteria)**.** Let S be a subset of a ring R. Then S is a subring if

(a) $S \neq \varnothing$,

(b) $a - b \in S$ for all $a, b \in S$, and

(c) $ab \in S$ for all $a, b \in S$.

An ideal is a special type of subring that has the "absorption property".

Definition 6.12 (ideal)**.** A subset I of a ring R is an **ideal** of R if

(a) $I \neq \varnothing$,

(b) $a - b \in I$ for all $a, b \in I$, and

(c) $ar \in I$ and $ra \in I$ for all $a \in I$ and $r \in R$.

Example 6.13. Let $R = \mathbb{Z}$ and $I = \{2024n \mid n \in \mathbb{Z}\}$. Show that I is an ideal of $\mathbb{Z}$.

Proof. We check the three conditions:

(a) $I \neq \varnothing$ since $2024 \cdot 1 \in I$.

(b) Let $a, b \in I$ so $a = 2024m$ and $b = 2024n$ with $m, n \in \mathbb{Z}$. So $a - b = 2024(m - n) \in I$.

(c) Let $a \in I$. So $a \in 2024m$. Let $r \in \mathbb{Z}$. Then $ra = r(2024m) = 2024(rm) \in I$.

□

In the same way we need normal subgroups to form quotient groups, we need ideals to form quotient rings.

Let R be a ring with I an ideal. Note R is an abelian group under addition. So I is a normal subgroup of R. So

$$R/I = \{a + I \mid a \in R\}$$

is defined as a group with addition $(a+I)+(b+I) = (a+b)+I$. Recall that $a+I = b+I$ if and only $a - b \in I$. To give R/I a ring structure, we need to define multiplication.

We want $(a + I)(b + I) = ab + I$ but need to check that this is well-defined. Our definition depends on a choice of representative so wee need to show our operation does not depend on this choice.

Lemma 6.14. Suppose $a_1 + I = a_2 + I$ and $b_1 + I = b_2 + I$. Then

$$a_1 b_1 + I = a_2 b_2 + I.$$

Proof. We are given $a_1 - a_2 \in I$ and $b_1 - b_2 \in I$. Since I is an ideal,

$$(a_1 - a_2)b_1 = a_1 b_1 - a_2 b_1 \in I$$

and

$$a_2(b_1 - b_2) = a_2 b_1 - a_2 b_2 \in I.$$

But this means

$$a_1 b_1 + I = a_2 b_2 + I.$$

□

Theorem 6.15. If R is a ring with ideal I, then R/I is a ring under the operations

$$(a + I) + (b + I) = (a + b) + I, \quad \text{and}$$
$$(a + I)(b + I) = ab + I.$$

Every ring R has at least two ideals $\{0\}$ and R is an ideal (trivial ideals).

Theorem 6.16. The ideals of a field are precisely those which are trivial.

Proof. Suppose I is not the zero ideal. Then there exist $a \in I$ with $a \neq 0$. Since $a^{-1} \in R$, $a^{-1}a = 1 \in I$. But for all $r \in R$, $r = r \cdot 1 \in I$ So $R \subseteq I \subseteq R$. So $I = R$. □

6.2 Lecture 20 — Review of Rings II

Definition 6.17 (ring homomorphism). Let R and S be rings. A **ring homomorphism** is a function $\varphi\colon R \to S$ such that

(a) $\varphi(a+b) = \varphi(a) + \varphi(b)$, and

(b) $\varphi(ab) = \varphi(a)\varphi(b)$.

Definition 6.18 (ring isomorphism). A ring homomorphism $\varphi\colon R \to S$ is called a **ring isomorphism** if φ is a bijection.

If there exists such a bijection φ, we say that R and S are **isomorphic** and write $R \cong S$.

Proposition 6.19. Let $\varphi\colon R \to S$ be a ring homomorphism. Then,

(a) $\varphi(0_R) = 0_S$,

(b) $\varphi(-a) = -\varphi(a)$,

(c) $\varphi(a^n) = \varphi(a)^n$,

(d) $\varphi(R) = \{\varphi(r) \mid r \in R\} \subseteq S$ is a subring, and

(e) If $1_R \in R$ and $1_S \in S$ and if φ is surjective, then $\varphi(1_R) = 1_S$

Proof.

(a) Note $0_R = 0_R + 0_R$. So

$$\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R).$$

Subtracting $\varphi(0_R)$ from both sides yields the desired result.

(e) To show $\varphi(1_R) = 1_S$, we need to show $\varphi(1_R)$ "acts like" 1_S. Take any $b \in S$. Since φ is surjective, we have $a \in R$ with $\varphi(a) = b$. So $b = \varphi(a) = \varphi(1_R \cdot a) = \varphi(1_R) \cdot \varphi(a) = \varphi(1_R) \cdot b$. By the same argument, $b = \varphi(a) = \varphi(a \cdot 1_R) = \varphi(a) \cdot \varphi(1_R) = b \cdot \varphi(1_R)$. Since the multiplicative identity is unique, $1_S = \varphi(1_R)$.

□

Definition 6.20 (kernel). The **kernel** of a ring homomorphism $\varphi\colon R \to S$, denoted $\ker\varphi$, is the set

$$\ker\varphi = \{r \in R \mid \varphi(r) = 0_S\}.$$

Theorem 6.21. Let $\varphi : R \to S$ be a ring homomorphism. Then,

(a) $\ker\varphi$ is an ideal of R, and

(b) $\ker\varphi = \{0_R\}$ if and only if φ is injective.

Proof of (a). We verify that $\ker\varphi$ satisfies the properties of an ideal.

- $\ker\varphi \neq \varnothing$ since $0_R \in R$ and $\varphi(0_R) = 0_S$.
- Let $a \in \ker\varphi$ and $r \in R$. Then $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0_S = 0_S$. So $ra \in \ker\varphi$.
- Let $a, b \in \ker\varphi$. Then $\varphi(a - b) = \varphi(a) - \varphi(b) = 0_S - 0_S = 0_S$. So $a - b \in \ker\varphi$.

□

A consequence of the above result is that any homomorphism $\varphi : R \to S$ gives a quotient ring $R/\ker\varphi$.

Theorem 6.22 (First Isomorphism Theorem)**.** Let $\varphi : R \to S$ be a ring homomorphism. Then

$$R/\ker\varphi \cong \varphi(R).$$

Example 6.23. Let $R = \mathbb{Z}$ and $S = \mathbb{Z}_{2024}$. Define a ring homomorphism

$$\begin{aligned}\varphi : \mathbb{Z} &\to \mathbb{Z}_{2024}, \\ n &\mapsto n \pmod{2024}.\end{aligned}$$

This map is onto. So $\varphi(\mathbb{Z}) = \mathbb{Z}_{2024}$. By the First Isomorphism Theorem, $\mathbb{Z}/\ker\varphi \cong \mathbb{Z}_{2024}$. We claim $\ker\varphi = \{2024k \mid k \in \mathbb{Z}\}$.

Definition 6.24 (principal ideal)**.** We call an ideal I of a ring R a **principal ideal** if there exists $a \in R$ such that

$$I = \{ra \mid r \in R\}.$$

We write $I = \langle a\rangle$ and say that a **generates** the ideal I.

So $\ker\varphi = \langle 2024\rangle$. So $\mathbb{Z}/\langle 2024\rangle \cong \mathbb{Z}_{2024}$. In fact,

$$\mathbb{Z}/\langle m\rangle \cong \mathbb{Z}_m.$$

Theorem 6.25 (Second Isomorphism Theorem)**.** Let I be a subring of R and

J and ideal of R. Then $I \cap J$ is an ideal of U and

$$I/I \cap J \cong (I+J)/J.$$

Theorem 6.26 (Third Isomorphism Theorem)**.** Let I and J be ideals of R with $I \subseteq J \subseteq R$. Then

$$(R/I)/(J/I) \cong R/J.$$

Theorem 6.27 (Fourth Isomorphism Theorem)**.** Let I be an ideal of R. Then there is a one-to-one correspondence between the ideals of R/I and the ideals J of R that contain I, i.e.

$$I \subseteq J \subseteq R.$$

Suppose now that R is a commutative ring.

Definition 6.28 (maximal ideal)**.** An ideal M is a **maximal ideal** of R if for every ideal J of R with $M \subseteq J \subseteq R$, either $J = M$ or $J = R$.

Definition 6.29. An ideal P is a **prime ideal** of R if $P \neq R$ and whenever $ab \in P$, $a \in P$ or $b \in P$.

Theorem 6.30. M is a maximal ideal of R if and only if R/M is a field.

Example 6.31. $\langle 2024 \rangle$ in $\mathbb{Z}$ is *not* maximal since $\mathbb{Z}/\langle 2024 \rangle \cong \mathbb{Z}_{2024}$ but $\mathbb{Z}_{2024}$ is not a field.

Example 6.32. $\langle m \rangle$ in $\mathbb{Z}$ is a maximal ideal if and only if m is prime.

Theorem 6.33. P is a prime ideal if and only if R/P is an integral domain.

Example 6.34. P is a prime ideal of $\mathbb{Z}$ if and only if

$$P = \langle p \rangle,\ (p \text{ prime}) \qquad \text{or} \qquad P = \langle 0 \rangle.$$

Note $\mathbb{Z}/\langle 0 \rangle \cong \mathbb{Z}$ is a domain, so $\langle 0 \rangle$ is prime.

Theorem 6.35. Every maximal ideal is a prime ideal.

Proof. M is maximal if and only if R/M is a field, which is an integral domain. An ideal M is prime if and only if R/M is an integral domain. □

> *Remark.* $\langle 0 \rangle$ is prime but not maximal.

6.3 Lecture 21 — Polynomial Rings

We will assume in this section that R is a commutative ring with identity.

Definition 6.36 (polynomial)**.** An expression $p(x)$ of the form

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with $a_n \neq 0$ and $a_0, \dots, a_n \in R$ is called a **polynomial** over R with indeterminate x.

- $a_0, \dots, a_n$ are the **coefficients** of $p(x)$.
- We call a_n the **leading coefficient**.
- $p(x)$ is said to be a **monic polynomial** if $a_n = 1$.
- The **degree** of $p(x) \neq 0$ is $\deg p(x) = n$. If $p(x) = 0$, we define $\deg p(x) = -\infty$.

The set of all such polynomials over R, denoted $R[x]$, is called the **polynomial ring** over R.

As preemptively indicated, it is in fact the case that $R[x]$ is a ring.

Theorem 6.37. $R[x]$ is a commutative ring with identity under the usual operations.

Example 6.38. Take $R = \mathbb{Z}_3$. Count the number of polynomials of degree 2.

Solution. A polynomial of degree 2 has the form $a_2x^2 + a_1x + a_0$. We must have $a_2 \in \{1, 2\}$ and $a_1, a_0 \in \{0, 1, 2\}$. This gives us $2 \cdot 3 \cdot 3 = 18$ possibilities. ▢

You may ask yourself: "If R has property P, does $R[x]$ *also* have property P?". The short answer to this question is it depends.

Theorem 6.39. If R is an integral domain, then $R[x]$ is also an integral domain.

Proof. Suppose $p(x) = a_m x^m + \cdots + a_1 x + a_0$ and $q(x) = b_n x^n + \cdots + b_1 x + b_0$. Then $p(x)q(x) = a_m b_n x^{m+n} + \cdots$. Since $a_m \neq 0$ and $b_n \neq 0$, and since R is an integral domain (in particular has no zero divisors), $a_m b_n \neq 0$. So $p(x)q(x) \neq 0$. Thus $R[x]$ is an integral domain. ▢

Corollary 6.40. If R is an integral domain and $p(x), q(x) \in R[x]$, then

$$\deg(p(x)q(x)) = \deg p(x) + \deg q(x).$$

Example 6.41. If $R = \mathbb{Z}_4$ (not an integral domain) and if $p(x) = 2x^{100} + 1$ and $q(x) = 2x^{2024} + 1$, then $p(x)q(x) = 4x^{2124} + 2x^{100} + 2x^{2024} = 2x^{2024} + 2x^{100} + 1$.

Example 6.42. If F is a field, is $F[x]$ a field?

Solution. No. The element x has no inverse. Suppose $q(x)x = 1$. Then $\deg q(x) + \deg x = 0$. This implies $\deg q(x) < 0$, which can't happen. □

Theorem 6.43. Let $\alpha \in R$ then the map $\varphi_\alpha : R[x] \to R$ given by

$$p(x) = a_n x^n + \cdots + a_0 \mapsto p(\alpha) = a_n \alpha^n + \cdots + a_0$$

is a homomorphism. We call φ_α the **evaluation homomorphism** at α.

Note that $S = R[x]$ s a commutative ring with identity. We can use this ring of coefficients S to make a new polynomial ring $S[y]$, elements of which have the form

$$g(x) = f_n(x)y^n + f_{n-1}(x)y^{n-1} + f_0(x).$$

We write $S[y] = (R[x])[y] = R[x, y]$. We can continue to form coefficient rings in this manner and more generally form $R[x_1, x_2, \dots, x_n]$.

Consider $F[x]$ with F a field. Then we can carry out polynomial division.

Example 6.44. Compute $(6x^3 + 25x^2 + 16x + 17) \div (3x^2 + 2x + 1)$.

Solution. We long-divide.

$$\begin{array}{r|r}
 & 2x + 7 \\ \cline{2-2}
3x^2 + 2x + 1 & 6x^3 + 25x^2 + 16x + 17 \\
 & -6x^3 - 4x^2 - 2x \phantom{{}+17} \\ \cline{2-2}
 & 21x^2 + 14x + 17 \\
 & -21x^2 - 14x - 7 \\ \cline{2-2}
 & 10
\end{array}$$

So $(6x^3 + 25x^2 + 16x + 17) \div (3x^2 + 2x + 1) = 2x + 7$. □

We can always long-divide if the ring of coefficients is a field.

Theorem 6.45 (Division Algorithm in $F[x]$)**.** Suppose F is a field and $a(x), b(x) \in F[x]$ with $b(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$$a(x) = b(x)q(x) + r(x),$$

with $r(x) = 0$ or $\deg r(x) < \deg b(x)$.

The proof is delayed to next lecture.

Example 6.46. Let $R = \mathbb{Z}$, $a(x) = 2x^2 + 1$ and $b(x) = 3x + 1$. When we carry out long division, we will have

$$2x^2 + 1 = (3x + 1)(ax + b) + c.$$

But then we will require $a = 2/3$. So we need the field property.

Definition 6.47 (root)**.** Let $p(x) \in R[x]$. If $\alpha \in R$ is such that $p(\alpha) = 0$, we call α a **root** of $p(x)$ in R.

Corollary 6.48. Let F be a field. Then α is a root of $p(x) \in F[x]$ if and only if $p(x) = (x - \alpha)q(x)$ for some $q(x) \in F[x]$.

Proof. If $p(x) = (x - \alpha)q(x)$, then $p(\alpha) = (\alpha - \alpha)q(\alpha) = 0$ and so α is a root.

If α is a root, we can apply the division algorithm to $p(x)$ and $(x - \alpha)$. Thus $p(x) = (x - \alpha)q(x) + r(x)$. Now since α is a root $0 = p(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = r(\alpha)$. Thus $r(\alpha) = 0$. But $r(x)$ is a constant so we must have $r(x) = 0$. □

6.4 Lecture 22 — The Division Algorithm in $F[x]$

Theorem 6.49 (Division Algorithm in $\mathbb{Z}$)**.** Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique integers q and r such that

$$a = bq + r,$$

with $0 \leq r < |b|$.

Theorem 6.50. Given any $a, b \in \mathbb{Z}$, there exist $s, t \in \mathbb{Z}$ such that

$$\gcd(a, b) = as + bt$$

We prove similar results for $F[x]$.

Theorem 6.51 (Division Algorithm in $F[x]$)**.** Suppose F is a field and $a(x), b(x) \in F[x]$ with $b(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$$a(x) = b(x)q(x) + r(x),$$

with $r(x) = 0$ or $\deg r(x) < \deg b(x)$.

Proof. We present two parts to the proof: existence (I) and uniqueness (II).

(I) If $a(x) = 0$, we must have $q(x) = r(x) = 0$ and so $0 = a(x) = b(x) \cdot 0 + 0$. If $\deg a(x) < \deg b(x)$, let $q(x) = 0$ and $r(x) = a(x)$. Then $a(x) = b(x) \cdot 0 + a(x)$. If $\deg a(x) \geq \deg b(x)$, we proceed by strong induction on the degree of $a(x)$. That is, we assume the statement is true for all polynomials $a'(x)$ with $\deg a'(x) < \deg a(x)$. Suppose

$$a(x) = a_m x^m + \cdots + a_0 \qquad \text{and} \qquad b(x) = b_n x^n + \cdots + b_0,$$

with $a_m, b_n \neq 0$ and $m \geq n$. Since F is a field, $\frac{a_m}{b_n} \in F$. Thus, $\frac{a_m}{b_n} x^{m-n} \in F[x]$. Define

$$\begin{aligned} a'(x) &= a(x) - \frac{a_m}{b_n} x^{m-n} b(x) \\ &= a_m x^m + \cdots + a_0 - \frac{a_m}{b_n} x^{m-n}(b_n x^n + \cdots + b_0) \\ &= a_m x^m + (\text{lower order terms}) - a_m x^m - (\text{lower order terms}). \end{aligned}$$

So $\deg a'(x) < \deg a(x)$. By strong induction, there exist $q'(x), r'(x) \in F[x]$ such that

$$a'(x) = b(x)q'(x) + r'(x).$$

Thus, $a(x) - \frac{a_m}{b_n}x^{m-n}b(x) = b(x)q'(x) + r'(x)$. Re-arranging,

$$\begin{aligned} a(x) &= b(x)q'(x) + \frac{a_m}{b_n}x^{m-n}b(x) + r'(x) \\ &= b(x)\left(q'(x) + \frac{a_m}{b_n}x^{m-n}\right) + r'(x). \end{aligned}$$

So let $q(x) = q'(x) + \frac{a_m}{b_n}x^{m-n}$ and $r(x) = r'(x)$. Note $r(x) = r'(x) = 0$ or $\deg r(x) = \deg r'(x) < \deg b(x)$.

(II) Suppose $a(x) = b(x)q(x) + r(x) = b(x)q'(x) + r'(x)$. So $b(x)(q(x) - q'(x)) = r'(x) - r(x)$. If $q(x) \neq q'(x)$, $b(x)(q(x) - q'(x)) \neq 0$. So $\deg(b(x)(q(x) - q'(x))) \geq \deg b(x)$. But then

$$\deg(r'(x) - r(x)) \leq \max\{\deg r(x), \deg r'(x)\} < \deg b(x),$$

which cannot happen. So we must have $q'(x) = q(x)$ and $r'(x) = r(x)$.

□

Definition 6.52 (greatest common divisor)**.** A monic polynomial $d(x)$ is a **greatest common divisor** (gcd) of $p(x)$ and $q(x)$ if $d(x)$ divides both $p(x)$ and $q(x)$ and if $d'(x)$ also divides $p(x)$ and $q(x)$, then $d'(x)$ divides $d(x)$. We write $d(x) = \gcd(p(x), q(x))$.

Theorem 6.53. Let $p(x), q(x) \in F[x]$ be nonzero. Then there exist $a(x), b(x) \in F[x]$ such that

$$\gcd(p(x), q(x)) = a(x)p(x) + b(x)q(x).$$

Proof. Let $S = \{a(x)p(x) + b(x)q(x) \mid a(x), b(x) \in F[x]\}$. Let $d(x) \in S$ be the element such that $\deg d(x) \leq \deg t(x)$ for all $t(x) \in S$. Also, by re-scaling, we may assume $d(x)$ is monic. We claim $\gcd(p(x), q(x)) = d(x)$. We first show $d(x)$ divides $p(x)$. Applying the division algorithm,

$$p(x) = d(x)\tilde{q}(x) + r(x),$$

with $r(x) = 0$ or $\deg r(x) < \deg d(x)$. In the case $\deg r(x) < \deg d(x)$,

$$\begin{aligned} r(x) &= p(x) - d(x)\tilde{q}(x) \\ &= p(x) - (a(x)p(x) + b(x)q(x))\tilde{q}(x) \\ &= (1 - a(x)\tilde{q}(x))p(x) - q(x)(b(x)\tilde{q}(x)) \in S. \end{aligned}$$

But then S has an element of smaller degree than $d(x)$, yielding a contradiction. So we must have $r(x) = 0$. A similar argument shows $d(x)$ divides $q(x)$.

Now suppose $d'(x)$ divides both $p(x)$ and $q(x)$. So $p(x) = d'(x)p'(x)$ and $q(x) = d'(x)q'(x)$. Thus $d(x) = p(x)a(x) + q(x)b(x) = d'(x)p'(x)a(x) + d'(x)q'(x)b(x) = d'(x)(p'(x)a(x) + q'(x)b(x))$. Thus, $d'(x)$ divides $d(x)$. □

Note that the Division algorithm gives a Euclidean algorithm to determine $\gcd(a(x), b(x))$:

$$\begin{aligned}
a(x) &= b(x)q_1(x) + r_1(x) \\
b(x) &= r_1(x)q_2(x) + r_2(x) \\
r_1(x) &= r_2(x)q_3(x) + r_3(x) \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n(x) + \underbrace{r_n(x)}_{\neq 0} \\
r_{n-1} &= r_n(x)q_n(x) + 0
\end{aligned}$$

The monic version of $r_n(x)$ is the gcd of $a(x)$ and $b(x)$.

6.5 Lecture 23 — Irreducible Polynomials

A common theme in previous lectures is that $\mathbb{Z}$ and $F[x]$ for a field F are "similar". In $\mathbb{Z}$, we have the notion of a prime number. We would like something similar for $F[x]$.

Note that any polynomial $p(x) \in F[x]$ can be factored. Take for example $p(x) = x^2 + x + 1 = \frac{1}{c}(cx^2 + cx + c)$ with $c \neq 0$. We need some extra conditions to get away from trivial examples such as this one.

Definition 6.54 (reducible/irreducible polynomial)**.** A nonconstant polynomial $f(x) \in F[x]$ is **reducible** if there exist polynomials $g(x), h(x) \in F[x]$ such that $f(x) = g(x)h(x)$ with $0 < \deg g(x) < \deg f(x)$ and $0 < \deg h(x) < \deg f(x)$. Otherwise, $f(x)$ is **irreducible**.

Remark. Reducibility depends on the field F:

- $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$;
- $x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$ is reducible in $\mathbb{R}[x]$.

Proposition 6.55. If $f(x)$ has degree > 1 and $f(x)$ has a root $\alpha \in F$, then $f(x)$ is reducible.

Proof. Since $f(\alpha) = 0$, $f(x) = (x-\alpha)g(x)$, for some polynomial $g(x)$. But $\deg f(x) > 1$. So we must have $\deg g(x) \geq 1$. □

Example 6.56. Show $p(x) = x^3 + x^2 + 2$ is irreducible in $\mathbb{Z}[x]$.

Proof. If $p(x)$ was reducible, we would have $p(x) = q(x)r(x)$, where one of $q(x), r(x)$ has degree 1 and the other has degree 2. Say $\deg q(x) = 1$. Then $q(x) = ax + b$, $a, b \in \mathbb{Z}_3$. So $p(x)$ has a root in $\mathbb{Z}_3$. But

$$p(0) = 2, \quad p(1) = 4 = 1, \quad \text{and} \quad p(2) = 14 = 2.$$

So $p(x)$ has no root, yielding a contradiction. Thus, $p(x)$ is irreducible. □

Theorem 6.57.

(a) $f(x) \in \mathbb{C}[x]$ is irreducible if and only if $\deg f(x) = 1$.

(b) $f(x) \in \mathbb{R}[x]$ is irreducible if and only if $\deg f(x) = 1$ or $f(x) = ax^2 + bx + c$ with $b^2 - 4ac < 0$.

We can reduce polynomials over $\mathbb{Q}$ to polynomials over $\mathbb{Z}$ up to a rational factor.

Lemma 6.58. Let $p(x) \in \mathbb{Q}[x]$. Then there exist $r, s, a_0, a_1, \dots, a_n \in \mathbb{Z}$ such that $\gcd(r,s) = 1$, $\gcd(a_0, a_1, \dots, a_n) = 1$ and

$$p(x) = \frac{r}{s}(a_n x^n + \cdots + a_1 x + a_0).$$

Example 6.59. Take $p(x) = \frac{3}{5} + \frac{2}{3}x + \frac{3}{10}x^2$.

$$\begin{aligned} p(x) &= \frac{3}{5} + \frac{2}{3}x + \frac{3}{10}x^2 \\ &= \frac{1}{5 \cdot 3 \cdot 10}\left(3 \cdot 10 \cdot 3 + 5 \cdot 10 \cdot 2x + 5 \cdot 3 \cdot 3x^2\right) \\ &= \frac{5}{5 \cdot 3 \cdot 10}\left(3 \cdot 5 \cdot 3 + 10 \cdot 2x + 3 \cdot 3x^2\right) \\ &= \frac{1}{30}(18 + 20x + 9x^2) \end{aligned}$$

Lemma 6.60 (Gauss)**.** Let $p(x)$ be a polynomial in $\mathbb{Z}[x]$ such that $p(x) = \alpha(x)\beta(x)$ with $\alpha(x), \beta(x) \in \mathbb{Q}[x]$. Then $p(x) = a(x)b(x)$ with $a(x), b(x) \in \mathbb{Z}[x]$ and $\deg a(x) = \deg \alpha(x)$ and $\deg b(x) = \deg \beta(x)$.

Remark. Judson states that $p(x)$ needs to be monic but this is not the case.

Corollary 6.61. Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{Z}$ and $a_0 \neq 0$. if $p(x)$ has a root $\frac{r}{s} \in \mathbb{Q}$, then it has a root $\alpha \in \mathbb{Z}$ and α divides a_0.

Proof. Suppose $p(r/s) = 0$. So $p(x) = (x - r/s)q(x)$ and $(x - r/s), q(x) \in \mathbb{Q}[x]$. By Gauss' Lemma (6.60), there exist $(x - \alpha), \tilde{q}(x) \in \mathbb{Z}$ such that $p(x) = (x - \alpha)\tilde{q}(x)$. Thus α is a root of $p(x)$ and $\alpha \in \mathbb{Z}$.

If we write

$$\tilde{q}(x) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0,$$

we have

$$\begin{aligned} p(x) &= x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \\ &= (x - \alpha)(b_{n-1}x^{n-1} + \cdots + b_1 x + b_0) \\ &= \cdots + \alpha b_0. \end{aligned}$$

So $a_0 = \alpha b_0$ and thus α divides a_0. □

Example 6.62. Show $p(x) = x^3 - 7x + 5$ has no roots in $\mathbb{Q}$.

Proof. If $p(x)$ did have a root, it would have an integer root α, we would have that α divides 5. So $\alpha = \pm 1, \pm 5$. But $p(\alpha) \neq 0$ for these choices of α. So $p(x)$ has no roots in $\mathbb{Q}$. □

Theorem 6.63 (Eisenstein's Criterion)**.** Let $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$. Suppose there exists a prime p such that

(a) p divides $a_0, a_1, \dots, a_{n-1}$,

(b) p does not divide a_n, and

(c) p^2 does not divide a_0.

Then $p(x)$ is irreducible.

Proof. The proof uses Gauss' Lemma (6.60). If $p(x)$ was reducible, we would have

$$p(x) = (b_rx^r + \cdots + b_0)(c_sx^s + \cdots + c_0) \in \mathbb{Z}[x],$$

where $r + s = n$. Since p^2 does not divide $a_0 = b_0c_0$, but p divides a_0 then p does not divide one of b_0, c_0. Say p does not divide b_0 but divides c_0. Since $a_n = b_rc_s$ and p does not divide a_n, p divides neither b_r nor c_s. Let k be the smallest integer such that p does not divide c_k. Then

$$a_k = b_0c_k + b_1c_{k-1} + \cdots b_kc_0 \Leftrightarrow b_0c_k = a_k - b_1c_{k-1} - \cdots - b_kc_0.$$

If $k < n$, then p divides the RHS but not the left. So we must have $k = n$. But now this implies $\deg(c_sx^s + \cdots + c_0) \geq n$, yielding a contradiction. Thus, $p(x)$ is irreducible. □

Example 6.64. $x^n - 2024$ is irreducible over $\mathbb{Q}[x]$ for all $n \geq 2$. Consider $p = 23$. Then p divides 2024 but p^2 does not. Obviously p does not divide 1. So by Eisenstein's criterion, $x^n - 2024$ is irreducible.

6.6 Lecture 24 — Ideals in $F[x]$

Recall that an ideal I in a commutative ring R is **principal** if there exists an element $a \in R$ such that

$$I = \{ra \mid r \in R\} = \langle a \rangle.$$

Recall also that every ideal of $\mathbb{Z}$ is principal. Extending from the similarities between $\mathbb{Z}$ and $F[x]$ seen in previous lectures, it is also the case that every ideal of $F[x]$ is principal.

Theorem 6.65. Every ideal I of $F[x]$ is principal.

Proof. If $I = \{0\}$, then $I = \langle 0 \rangle$ and clearly I is principal. So assume $I \neq \{0\}$. Let $p(x) \in I$ with $p(x) \neq 0$ and $\deg p(x) \leq \deg q(x)$ for all $q(x) \in I$. If $\deg p(x) = 0$, then $p(x) = c$ for some $c \in F$. So $c \in I$. But $c^{-1} \in F \subset F[x]$, so $c^{-1}c = 1 \in I$. Thus, $I = F[x] = \langle 1 \rangle$. So suppose $\deg p(x) > 0$. We claim $I = \langle p(x) \rangle$.

Since $p(x) \in I$, clearly $\langle p(x) \rangle \subseteq I$.

Let $t(x) \in I$. By the Division Algorithm,

$$t(x) = p(x)q(x) + r(x),$$

with $r(x) = 0$ or $\deg r(x) < \deg p(x)$. If $r(x) \neq 0$, we have

$$r(x) = \underbrace{t(x)}_{\in I} - \underbrace{p(x)}_{\in I} q(x) \in I.$$

But $\deg r(x) < \deg p(x)$, and $p(x)$ should have the smallest degree in I. This is a contradiction. So it must be that

$$t(x) = p(x)q(x) \in \langle p(x) \rangle.$$

□

Example 6.66. Theorem 6.65 is not true in general for $F[x, y]$. Consider $\langle x^2, y \rangle = \{f(x, y)x^2 + g(x, y)y \mid f(x, y), g(x, y) \in F[x, y]\}$. We claim $\langle x^2, y \rangle$ is not principal.

Suppose $\langle x^y, y \rangle = \langle p(x, y) \rangle$ for some $p(x, y) \in F[x, y]$. So $p(x, y)$ divides both x^2 and y. Thus, $p(x, y)$ must be constant, i.e. $p(x, y) = c$ for some $c \in F$. Then $\langle x^2, y \rangle = \langle c \rangle = \langle 1 \rangle$. But $1 \notin \langle x^2, y \rangle$; a contradiction.

Recall that in $\mathbb{Z}$, $\langle a \rangle$ is a maximal ideal if and only if a is prime. We provide a similar result for $F[x]$.

Theorem 6.67. In $F[x]$, $\langle f(x) \rangle$ is a maximal ideal if and only if $f(x)$ is irreducible.

Proof. First, suppose $I = \langle f(x)\rangle$ is maximal and $f(x) = p(x)q(x)$ for some $p(x), q(x) \in F[x]$. So $f(x) \in \langle p(x)\rangle$. Thus, $I \subseteq \langle p(x)\rangle$. Because I is maximal, either $I = \langle p(x)\rangle$ or $\langle p(x)\rangle = F[x]$. In the case that $I = \langle p(x)\rangle$, $p(x) \in \langle f(x)\rangle$. So $\deg f(x) \leq \deg p(x) \leq \deg f(x)$. Then it must be that $f(x) = p(x)$. If $\langle p(x)\rangle = F[x]$, then $1 \in \langle p(x)\rangle$. So $p(x)$ divides 1 and thus $\deg p(x) = 0$. So $f(x)$ is irreducible.

Now let $I = \langle f(x)\rangle$ with $f(x)$ irreducible and suppose J is a principal ideal such that $I \subseteq J \subseteq F[x]$. Since $J = \langle q(x)\rangle$ for some $q(x) \in F[x]$, we have $f(x) \in \langle q(x)\rangle$, so $f(x) = p(x)q(x)$ for some $p(x) \in F[x]$. Since $f(x)$ is irreducible, either $\deg q(x) = 0$ or $\deg q(x) = \deg f(x)$. In the case that $\deg q(x) = 0$, $q(x) = c$ for some $c \in F$. So $J = F[x]$. In the case that $\deg q(x) = \deg f(x)$, $f(x) = cq(x)$ and thus $\langle f(x)\rangle = \langle q(x)\rangle$. So $\langle f(x)\rangle$ is maximal. □

Practice Problems

A. Apply the division algorithm to $a(x) = 4x^5 - x^3 + x^2 + 4$ and $b(x) = x^3 - 2$ in $\mathbb{Z}_5[x]$.

B. For any polynomial $p(x) \in \mathbb{R}[x]$, we know $p(x)$ has at most $\deg p(x)$ roots. Show that is false in $\mathbb{Z}_{10}[x]$.

C. Prove the rational root test: Suppose

$$p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

If $\frac{r}{s} \in \mathbb{Q}$ with $\gcd(r, s) = 1$, then r divides a_0 and s divides a_n. Use this to show $7x^2 + 2$ has no real roots.

D. Prove $x^p + a$ is reducible in $\mathbb{Z}_p[x]$ for any $a \in \mathbb{Z}_p$ where p is prime.

Chapter 7

Integral Domains

7.1 Lecture 25 — Fields from Domains

Given an integral domain D, we would like to construct a field F_D. A motivating example is forming $\mathbb{Q}$ form $\mathbb{Z}$.

Recall that a domain D

- is commutative,
- has identity, and
- has no zero divisors.

Let $S = \{(a, b) \in D^2 \mid b \neq 0\}$. Define a relation $\sim$ on S by

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Lemma 7.1. $\sim$ is an equivalence relation.

Proof. We verify that the conditions hold.

(a) Since D is commutative, $ab = ba$ and thus $(a, b) \sim (a, b)$, i.e. $\sim$ is reflexive.

(b) Suppose $(a, b) = (c, d)$. So $ad = bc$. Since D is commutative, $cb = da$ and thus $(c, d) \sim (a, b)$. That is, $\sim$ is symmetric.

(c) Suppose $(a, b) \sim (c, d)$ and $(c, d) = (e, f)$. So $ad = bc$ and $cf = de$. We multiply and obtain $adf = bcf$ and $bcf = bde$. Note $b, d, e \neq 0$. So $adf = bde$. In particular $af = be$ since $d \neq 0$ and D is a domain. So $(a, b) \sim (e, f)$ and $\sim$ is transitive.

□

Definition 7.2 (field of fractions)**.** Let D be an integral domain. The **field of**

fractions of D is the set of all equivalence classes

$$F_D = \{[(a,b)] \mid (a,b) \in S\}.$$

Example 7.3. When $D = \mathbb{Z}$, $S = \{(a,b) \in D^2 \mid b \neq 0\}$. Consider $(2,7) \in S$. So

$$\begin{aligned}[(2,7)] &= \{(c,d) \in S \mid (2,7) \sim (c,d)\} \\ &= \{(c,d) \in S \mid 2d = 7c\} \\ &= \left\{(c,d) \in S \mid \frac{2}{7} = \frac{c}{d}\right\},\end{aligned}$$

i.e. when we write $\frac{2}{7} \in \mathbb{Q}$, we really mean "all ways" to write $\frac{2}{7}$. For example,

$$\frac{2}{7} = \frac{-2}{-7} = \frac{4}{14} = \frac{20}{70}.$$

We can define addition and multiplication on F_D:

$$[(a,b)] + [(c,d)] = [(ad + bc, bd)] \quad \text{and} \quad [(a,b)] \cdot [(c,d)] = [(ac, bd)]$$

Lemma 7.4. Both operations defined above are well-defined.

Proof. We prove only multiplication. Suppose $[(a,b)] = [(a',b')]$ and $[(c,d)] = [(c',d')]$. We want to show $[(a,b)] \cdot [(c,d)] = [(a',b')] \cdot [(c',d')]$, i.e. $[(ac,bd)] = [(a'c',b'd')]$.

We are given $ab' = a'b$ and $cd' = c'd$. So $ab'cd' = a'bc'd$, thus $(ac)(b'd') = (a'c')(bd)$ and $[(ac,bd)] = [(a'c',b'd')]$. □

Theorem 7.5. The field of fractions of a domain is a field with the previously defined addition and multiplication.

Proof. We verify that F_D all the properties of a field.

- Addititve identity is $[(0,1)]$. Indeed, $[(a,b)]+[(0,1)] = [a \cdot 1 + b \cdot 0, 1 \times b] = [a,b]$.
- Multiplicative identity is $[(1,1)]$.
- Suppose $[a,b] \in F_D$ and $a \neq 0$. Then $[(b,a)] \in F_D$ and this is the inverse since $[(a,b)][(b,a)] = [(ab,ba)] = [(1,1)]$.
- $[(a,b)] + ([(c,d)] + [(e,f)]) = ([(a,b)] + [(c,d)]) + [(e,f)]$ (check!)

The rest is an exercise. □

Theorem 7.6. Let D be a domain. Then D can be embedded into F_D. That is, there exists an injective homomorphism $\varphi : D \to F_D$ and thus F_D has a subring isomorphic to D.

Proof. Let $D' = \{[(d,1)] \mid d \in D\} \subseteq F_D$. Define a map $\varphi : D \to D' \subseteq F_D$ by $d \mapsto [(d,1)]$. It is a ring homomorphism since

$$\begin{aligned}\varphi(d_1 + d_2) &= [(d_1 + d_2, 1)] \\ &= [(d_1, 1)] + [(d_2, 1)] \\ &= \varphi(d_1) + \varphi(d_2)\end{aligned}$$

and

$$\begin{aligned}\varphi(d_1 d_2) &= [(d_1 d_2, 1)] \\ &= [(d_1, 1)][(d_2, 1)] \\ &= \varphi(d_1)\varphi(d_2).\end{aligned}$$

Then the map is injective and surjective on D'. It is left as an exercise to show D' is a subring of F_D. □

Theorem 7.7. Suppose E is a field that contains a domain D. Then there is a subfield $E' \subseteq E$ such that $F_D \cong E'$.

Corollary 7.8. If E is a field of characteristic 0, then E has a subfield isomorphic to $\mathbb{Q}$.

Proof. Let 1_E be the identity in E. Set $D = \{n \cdot 1_E \mid n \in \mathbb{Z}\} \cong \mathbb{Z}$. So $F_{\mathbb{Z}} \cong \mathbb{Q} \cong E' \subseteq E$. □

7.2 Lecture 26 — Unique Factorization Domains

Let R be a commutative ring with identity and let $a, b \in R$.

Definition 7.9 (divides, $a|b$)**.** We say that a **divides** b and write $a \mid b$ if $b = ac$ for some $c \in R$.

Definition 7.10 (unit)**.** We say that $a \in R$ is a **unit** if there exists $u \in R$ such that $au = 1$, i.e. a has a multiplicative inverse u.

Definition 7.11 (associates)**.** We say that a and b are **associates** if there exists a unit $u \in R$ such that $a = ub$.

Let D be an integral domain.

Definition 7.12 (irreducible)**.** Let $p \in D$ be nonzero. We say that p is **irreducible** if p is not a unit and whenever $p = ab$, then a or b is a unit.

Definition 7.13 (prime)**.** Let $p \in D$ be nonzero. We say that p is **prime** if whenever p divides ab, either p divides a or p divides b.

Lemma 7.14. If $p \in D$ is prime, them p is irreducible.

Proof. Suppose $p = ab$ for some $a, b \in D$. Clearly, $p|ab$. Since p is prime, either $p \mid a$ or $p|b$. Without loss of generality, suppose $p|a$. Then $a = pc$ for some c. Thus, $p = pcb$. Since we are in an integral domain, we can multiply by p^{-1} on both sides. This yields $1 = cb$. So b is a unit and thus p is irreducible. ▢

Example 7.15. If $p \in D$ is irreducible, it is not necessarily the case that p is prime.

Take for example the domain $D = \mathbb{Q}[x^2, xy, y^2]$, i.e. all polynomials in x^2, xy, y^2 with rational coefficients. Observe $xy \in D$ is irreducible — it cannot be factored into two terms of degree 1. But xy is not prime since xy divides x^2y^2 and xy divides neither x^2 nor y^2.

Definition 7.16. An integral domain D is a **unique factorization domain (UFD)** if

(a) Every nonzero $a \in D$ that is not a unit can be written as

$$a = p_1 p_2 \cdots p_r$$

with each p_i irreducible, and

(b) if $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ with each p_i and each q_j irreducible, then $r = s$ and there exists a permutation $\pi \in S_r$ such that p_i and $q_{\pi(i)}$ are associates.

Example 7.17. The integers $\mathbb{Z}$ form a UFD since every integer $a \in \mathbb{Z}$ can be written uniquely as

$$a = (-1)^t p_1^{b_1} \cdots p_s^{b_s}, \qquad \text{with } p_i \text{ prime.}$$

Note that -1 is a unit in $\mathbb{Z}$.

Take for example,

$$20 = 2 \times 2 \times 5 = (-2) \times (2) \times (-5).$$

Example 7.18. Though all UFDs are integral domains, not all integral domains are UFDs.

Set

$$S = \{f \in \mathbb{R}[x] \mid f(x) = a_0 + 0x + a_2x^2 + \cdots + a_nx^n\},$$

i.e. S is the set of all polynomials with real coefficients such that the coefficient of the x term is 0. Then S is a subring of $\mathbb{R}[x]$ that is an integral domain. In this ring, x^2 is irreducible as it cannot be factored as a product of two degree 1 polynomials. For the same reason, x^3 is irreducible. Now consider the following:

$$x^6 = (x^2)(x^2)(x^2) = (x^3)(x^3).$$

Since x^6 has two possible factorizations with irreducible factors, S cannot be a UFD.

Definition 7.19. A domain D is called a **principal ideal domain (PID)** if every ideal of D is principal.

Example 7.20. Take for example $\mathbb{Z}$ and $F[x]$ with F a field. (Why?)

Our goal will be to show that all PIDs are UFDs.

Lemma 7.21. Let D be a domain and let $a, b \in D$. Then

(a) $a|b$ if and only if $\langle b \rangle \subseteq \langle a \rangle$,

(b) a and b are associates if and only if $\langle a \rangle = \langle b \rangle$, and

(c) a is a unit if and only if $\langle a \rangle = D$.

Proof.

(a) Given $a|b$, $b = ac$ for some $c \in D$. but then $b \in \langle a \rangle$ and thus $\langle b \rangle \subseteq \langle a \rangle$.

Now given $\langle b \rangle \subseteq \langle a \rangle$, $b \in \langle b \rangle \subseteq \langle a \rangle$ and so $b = ac$ for some c. Thus, $a|b$.

(b) If a and b are associates, there is a unit u so that $a = ub$ and thus $u^{-1}a = b$. So both $b|a$ and $a|b$. By (a), $\langle b \rangle \subset \langle a \rangle \subset \langle b \rangle$ and so $\langle a \rangle = \langle b \rangle$.

Given $\langle a \rangle = \langle b \rangle$, we have $\langle a \rangle \subseteq \langle b \rangle$ $\langle b \rangle \subseteq \langle a \rangle$. So both $b|a$ and $a|b$. Thus, $a = bc$ and $b = at$. So $a = atc$ and thus $1 = tc$. So c is a unit and thus a and b are associates.

(c) Suppose a is a unit. So $au = 1 \Leftrightarrow a = 1 \cdot u^{-1}$. So $a|1$ and $1|a$. Thus $\langle a \rangle = \langle 1 \rangle = D$.

The other direction is left as an exercise.

□

Theorem 7.22. Let D be a PID. Then p is irreducible if and only if $\langle p \rangle$ is a maximal ideal.

Proof. Suppose first that p is irreducible and a is such that $\langle p \rangle \subseteq \langle a \rangle$. So $a|p$. Since p is irreducible, either a is an associate of p or a is a unit in the case where a is an associate, $\langle p \rangle$. In the other case that a is a unit, $\langle a \rangle = D$. So $\langle p \rangle$ is maximal.

Now suppose that $\langle p \rangle$ is a maximal ideal and a and b are such that $p = ab$. So $\langle p \rangle \subseteq \langle a \rangle$. Since $\langle p \rangle$ is maximal, either $\langle p \rangle = \langle a \rangle$ or $\langle a \rangle = D$. In the case that $\langle a \rangle = D$, a is a unit. In the other case where $\langle p \rangle = \langle a \rangle$, a is an associate of p, so b is a unit. Therefore, p is irreducible. □

Corollary 7.23. Let D be a PID. Then p is prime if and only if p is irreducible.

Proof. The forwards implication is trivial and always true. So suppose p is irreducible. So $\langle p \rangle$ is a maximal ideal by Theorem 7.22 and thus a prime ideal. If $ab \in \langle p \rangle$, then either $a \in \langle p \rangle$ or $b \in \langle p \rangle$. Equivalently, either $p|a$ or $p|b$. □

Example 7.24. In $\mathbb{Z}$ and $F[x]$, prime is equivalent to irreducible.

7.3 Lecture 27 — Principal Ideal Domains

Recall that an integral domain is a principal ideal domain (PID) if every ideal in the domain is principal. Common examples are $\mathbb{Z}$ and $F[x]$ for F a field. The goal of this lecture is to show that all PIDs are UFDs.

Lemma 7.25. Let D be a PID and let $I_1, I_2, \dots$ be a collection of ideals of D such that

$$I_1 \subseteq I_2 \subseteq \cdots.$$

Then there is an integer N such that

$$I_N = I_{N+1} = I_{N+2} = \cdots.$$

Proof. Let $I = \bigcup_{i=1}^{\infty} I_i$. We claim that I is an ideal. Indeed,

- $I \neq \varnothing$ since $0 \in I_1 \subseteq I$.
- Let $a, b \in I$. Then $a \in I_i$ and $b \in I_j$ for some i, j. Without loss of generality, suppose $i \leq j$. Then $a \in I_i \subseteq I_j$, so $a, b \in I_j$. Thus, $a - b \in I_j \subseteq I$.
- Let $a \in I$. So $a \in I_i$ for some i. For any $r \in D$, $ra \in I_i \subseteq I$.

Since D is a PID, there exists an element $d \in D$ such that $I = \langle d \rangle$. Since $d \in I = \bigcup_{i=1}^{\infty} I_i$, there exists and integer N such that $d \in I_N$. So

$$\langle d \rangle \subseteq I_N \subseteq I_{N+1} \subseteq \cdots \subseteq I = \langle d \rangle.$$

Therefore, $\langle d \rangle = I_N = I_{N+1} = \cdots$. □

Definition 7.26 (Noetherian ring)**.** A ring R is a **Noetherian ring** if it satisfies the ascending chain condition, i.e. for any chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$, there is an integer N such that $I_N = I_{N+1} = \cdots$.

Corollary 7.27. Every PID is Noetherian.

Lemma 7.28. Let S be a nonempty collection of ideals in a PID. Then there is an ideal $J \in S$ such that for all $I \in S$ with $J \subseteq I$, $J = I$, i.e. S has a maximal element.

Proof. Suppose for a contradiction that S had no such maximal element. Take $I_1 \in S$. Since I_1 is not maximal, there exists $I_2 \in S$ such that $I_1 \subsetneq I_2$. Again, I_2 is not maximal so there is $I_3 \in S$ such that $I_1 \subsetneq I_2 \subsetneq I_3$. Continuing in this way,

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots.$$

But this contradicts the ascending chain condition and the fact that every PID is Noetherian. □

Lemma 7.29. Let R be a PID. If $a \in R$ is not a unit, then a can be written as a product of irreducible elements.

Proof. Let S be the collection of principal ideals $\langle a \rangle$ of R such that a is not a unit and a cannot be written as a product of irreducibles. Our goal is to show $S = \varnothing$.

Suppose otherwise for a contradiction, i.e. $S \neq \varnothing$. Then by Lemma 7.28, there exists a maximal $\langle a \rangle \in S$. But we also know that $a = bc$ with a not reducible, so b and c are not units. But then

$$\langle a \rangle \subseteq \langle b \rangle \quad \text{and} \quad \langle a \rangle \subseteq \langle c \rangle.$$

So $\langle b \rangle, \langle c \rangle \notin S$. So b and c can be factored into irreducibles as $b = p_1 \cdots p_r$ and $c = q_1 \cdots q_s$. But then $a = bc = p_1 \cdots p_r q_1 \cdots q_s$ is a product of irreducibles, yielding a contradiction. So $S = \varnothing$. □

Theorem 7.30. Every PID is also a UFD.

Proof. Let D be a PID. Let $a \in D$ with a not a unit. By Lemma 7.29, a can be written as a product of irreducibles.

Suppose $a = p_1 \cdots p_r$ and $a = q_1 \cdots q_s$ are two ways to write a as a product of irreducibles. Without loss of generality, suppose $r \leq s$. Since D is a PID, p_1 is also prime. Since $p_1 | q_1 \cdots q_s$, we must have $p_1 | q_i$ for some i. Relabeling, assume $p_1 | q_1$, that is, $q_1 = u_1 p_1$. Note that u_1 must be a unit since q_1 is irreducible. Thus,

$$p_1 p_2 \cdots p_r = u_1 p_1 q_2 \cdots q_s.$$

In the case that $r < s$, we end up with

$$1 = u_1 \cdots u_r q_{r+1} \cdots q_s.$$

But this cannot happen, since the q_i's are not units. So it must be that $r = s$ and thus $p_i = u_i q_i$ for all i. As such, the factorization for a is unique. □

Corollary 7.31. If F is a field, $F[x]$ is a UFD.

Note that the converse of Theorem 7.30 is false; there are UFDs that are not PIDs.

Example 7.32. $F[x_1, \dots, x_n]$ is a UFD but not a PID.

Definition 7.33 (Euclidean domain, Euclidean valuation)**.** Let D be an integral domain. Suppose that there is a function $v : D \setminus \{0\} \to \mathbb{N}$ that satisfies the following:

(a) If $a, b \in D$, then $v(a) \leq v(ab)$.

(b) Let $a, b \in D$ with $b \neq 0$. Then there exist $q, r \in d$ such that $a = bq + r$ with $r = 0$ or $v(r) < v(b)$.

Then D is called a **Euclidean domain** and v is called a **Euclidean valuation**.

The function v associates to the elements of D a “size”.

Example 7.34. Take $D = \mathbb{Z}$. We may use

$$\begin{aligned} v : \mathbb{Z} \setminus \{0\} &\to \mathbb{N}, && (7.1)\\ a &\mapsto |a|. && (7.2) \end{aligned}$$

Now take $D = F[x]$. We may use

$$\begin{aligned} v : \mathbb{F}[x] \setminus \{0\} &\to \mathbb{N}, && (7.3)\\ p(x) &\mapsto \deg p(x). && (7.4) \end{aligned}$$

(Check that the above functions satisfy the conditions of a valuation!)

So $\mathbb{Z}$ and $F[x]$ are Euclidean domains.

Our goal for next lecture is to show that every Euclidean domain is a PID.

7.4 Lecture 28 — Euclidean Domains and Factoring in $D[x]$

A **Euclidean Domain** is a domain in which there exists a division algorithm

Definition 7.35. A domain D is a **Euclidean Domain** if there is a valuation $v\colon D \setminus \{0\} \to \mathbb{N}$ such that

(a) $v(a) \le v(ab)$ for all $a, b \in D \setminus \{0\}$, and

(b) for all $a, b \in D$ with $b \neq 0$, there exist $q, r \in D$ such that $a = bq + r$ with $r = 0$ or $v(r) < v(b)$

Example 7.36. If $D = \mathbb{Z}$, we use the valuation $v\colon \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ defined by $a \mapsto |a|$.

If $D = F[x]$, we use the valuation $v\colon F[x] \setminus \{0\} \to \mathbb{N}$ defined by $p(x) \mapsto \deg p(x)$.

Example 7.37. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, $i^2 = -1$. This is a ring with the usual multiplication and addition. Define

$$\begin{aligned} v\colon \mathbb{Z}[i] \setminus \{0\} &\to \mathbb{N}, \\ a + bi &\mapsto a^2 + b^2. \end{aligned}$$

We claim that v is a valuation.

Proof. We check the properties. Let $x = a + bi$ and $y = c + di$. Then

$$xy = (a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

So

$$v(xy) = (ac - bd)^2 + (ad + bc)^2 = (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2$$

Note $v(x) = v(x)v(y)$ (check!). This is not true in general. But then $v(x) \le v(x)v(y) = v(xy)$ is true.

Now let $z = a + bi$ and $w = c + di$ with $w \neq 0$. Viewed as elements of $\mathbb{Q}[i] = \{p + qi \mid p, q \in \mathbb{Q}\}$,

$$\begin{aligned} \frac{z}{w} &= \frac{a + bi}{c + di} \\ &= \frac{(a + bi)(c - di)}{(c + di)(c - di)} \\ &= \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} \end{aligned}$$

Now write

$$\frac{ac+bd}{c^2+d^2} = m_1 + \frac{n_1}{c^2+d^2},$$

where $\left|\frac{n_1}{c^2+d^2}\right| \leq \frac{1}{2}$ and m_1 is the closest integer to $\frac{ac+bd}{c^2+d^2}$. Also,

$$\frac{bc-ad}{c^2+d^2} = m_2 + \frac{n_2}{c^2},$$

where $\left|\frac{n_2}{c^2+d^2}\right| \leq \frac{1}{2}$ and m_2 is the closest integer to $\frac{bc-ad}{c^2+d^2}$. So

$$\frac{z}{w} = (m_1+m_2 i) + \frac{n_1+n_2 i}{c^2+d^2}.$$

Now

$$\begin{aligned} z &= \frac{z}{w}\cdot w \\ &= (m_1+m_2 i)(c+d_i) + \frac{n_1+n_2 i}{c^2+d^2}(c+di) \\ &= wq+r. \end{aligned}$$

Note $z, w, q \in \mathbb{Z}[i]$, so $z - wq = r \in \mathbb{Z}[i]$. Then

$$\begin{aligned} v(r) &= v\left(\frac{n_1+n_2 i}{c^2+d^2}(c+di)\right) \\ &= v(c+di)v\left(\frac{n_1+n_2 i}{c^2+d^2}\right) \\ &= v(c+di)\left(\left(n_1 c^2+d^2\right)^2 + \left(n_2 c^2+d^2\right)^2\right) \\ &\leq v(c+di)(\frac{1}{4}+\frac{1}{4}) \\ &= \frac{1}{2} \leq v(c+di) \qquad\qquad < v(c+di). \end{aligned}$$

□

Theorem 7.38. Every ED is a PID.

Proof. Let D be a Euclidean Domain. Let $I \subset D$ be an ideal. If $I = \{0\}$, then $I = \langle 0 \rangle$. So suppose $I \neq \{0\}$. Let $a \in I$ with $v(a) \leq v(b)$ for all $b \in I$ different from a. We claim $I = \langle a \rangle$.

Since $a \in I$, $\langle a \rangle \subseteq I$. Now let $b \in I$. By the division algorithm, $b = aq + r$ with $r = 0$ or $v(r) < v(a)$. If $r \neq 0$, then $r = b - aq \in I$ and then $v(r) < v(a)$ is a contradiction to the choice of a. So $r = 0$ and thus $I = \langle a \rangle$. □

Corollary 7.39. Every ED is a UFD.

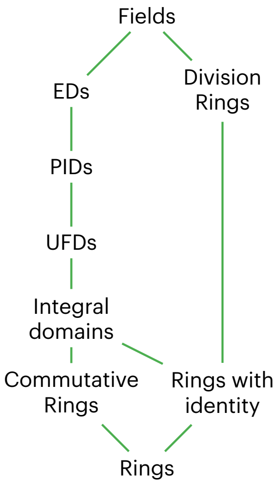
> *Remark.* Proving a domain is not a Euclidean Domain is difficult. It implies showing no such valuation exists.

Example 7.40. Let

$$D = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{-19}}{2}\right) \,\middle|\, a, b \in \mathbb{Z}\right\}.$$

To sketch out the proof, suppose there was a valuation $v : D \setminus \{0\} \to \mathbb{N}$. We need to check that the only units in the ring are ±1. So take any $a \in D \setminus \{0, 1, -1\}$ with $v(a)$ as small as possible. For any $b \in D$, we have $b = aq + r$ with $r = 0$ or $v(r) < v(a)$. But for units $v(-1) = v(1) < v(a)$. So the only choices for r are $0, 1, -1$. So $D/\langle a\rangle \cong \mathbb{Z}_2$ or $D/\langle a\rangle \cong \mathbb{Z}_3$.

In D, $x^2 + x + 5$ has roots $\alpha = \frac{-1\pm\sqrt{-19}}{2}$. But $x^2 + x + 5$ has no roots in $\mathbb{Z}_2$ or $\mathbb{Z}_3$ so $D/\langle a\rangle \ncong \mathbb{Z}_2, \mathbb{Z}_3$.



Theorem 7.41. If D is a UFD, then $D[x]$ is also a UFD.

Corollary 7.42. If D is a UFD, then $D[x_1, \dots, x_n]$ is a UFD.

A special case with applications in algebraic geometry is $\mathbb{C}[x_1, \dots, x_n]$.

Chapter 8

Fields

8.1 Lecture 29 — Field Extensions

The goal for this chapter is to further investigate fields (domains in which each element has an inverse). Standard examples of fields are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$.

A guiding question is as follows: *If F is a field and $p(x) \in F[x]$, is there a "bigger" field in which $p(x)$ has a root?*

Example 8.1. Consider $x^2 + 1 \in \mathbb{R}[x]$. This polynomial has no roots in $\mathbb{R}$ but if we make $\mathbb{R}$ "bigger" and consider the complex numbers $\mathbb{C}$, of which $\mathbb{R}$ is a subfield, then $x^2 + 1$ has the root i.

Definition 8.2. A field E is an **extension** of F if F is a subfield of E. We call F the **base field** of the extension.

> *Remark.* Sometimes we may relax the above definition up to isomorphism. That is, we may say E is an extension of F if E has a subfield F' that is isomorphic to F. For example, say the field of fractions $F_{\mathbb{Z}}$ and $\mathbb{Q}$ are extensions of $\mathbb{Z}$.

Example 8.3.

- $\mathbb{C}$ is an extension of $\mathbb{R}$.
- $\mathbb{R}$ is an extension of $\mathbb{Q}$.

Recall that if $p(x) \in F[x]$ is an irreducible polynomial, then

$$F[x]/\langle p(x)\rangle$$

is a field (equivalently if $\langle p(x)\rangle$ is a maximal ideal). This gives us a way to construct fields.

Example 8.4. Consider $x^2 - 2 \in \mathbb{Q}[x]$. Then $E = Q[x]/\langle x^2-2\rangle$ is a field. Note that E contains a “copy” of $\mathbb{Q}$.

$$\mathbb{Q} \cong \{a + \langle x^2-2\rangle \mid a \in \mathbb{Q}\} \subseteq E.$$

So E is an extension of $\mathbb{Q}$.

Observe that if $p(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, we can view it as

$$p(x) = a_0x^0 + a_1x^1 + \cdots + a_nx^n \in F[x].$$

Now let

$$\alpha = x + \langle x^2-2\rangle \in E.$$

Then

$$\begin{aligned}\alpha^2 + 2\alpha^0 &= (x + \langle x^2-2\rangle)^2 - 2(x + \langle x^2-2\rangle)^0\\ &= (x^2 + \langle x^2-2\rangle) - 2(1 + \langle x^2-2\rangle)\\ &= (x^2 - 2\cdot 1) + \langle x^2-2\rangle\\ &= 0 + \langle x^2-2\rangle.\end{aligned}$$

So α is a root of $x^2 - 2$.

Theorem 8.5 (Fundamental Theorem of Field Theory)**.** Let F be a field and $p(x) \in F[x]$ be nonconstant. Then there exists an extension E of F such that $p(x)$ has a root $\alpha \in E$.

Proof. Since $F[x]$ is a PID, it is also a UFD. So we can uniquely factor $p(x)$:

$$p(x) = p_1(x)p_2(x)\cdots p_r(x),$$

where $p_i(x)$ is irreducible for each i. So it is enough to prove the result for p_1 since it is irreducible. We have that

$$E = F[x]/\langle p(x)\rangle$$

is a field. We claim that E is an extension of F (or has a subfield isomorphic to F). To give a sketch, define

$$\begin{aligned}\varphi : \ & F \to E,\\ & a \mapsto a + \langle p(x)\rangle.\end{aligned}$$

One can check that φ is indeed a ring homomorphism. Observe that φ is injective since

$$\varphi(a) = \varphi(b) \quad\Leftrightarrow\quad a + \langle p(x)\rangle = b + \langle p(x)\rangle \quad\Leftrightarrow\quad a - b \in \langle p(x)\rangle,$$

but $\deg p(x) \geq 1$ and $\deg(a-b) = 0$. So it must be that $a = b$. Thus, $F \cong \operatorname{im}\varphi \subseteq E$.

Let $\alpha = x + \langle p(x)\rangle$ be the class of x in E. If $p_1 = a_n x^n + \cdots + a_1 x^1 + a_0 x^0$, then

$$\begin{aligned} p_1(\alpha) &= a_n\alpha^n + \cdots + a_1\alpha^1 + a_0\alpha^0 \\ &= a_n(x^n + \langle p(x)\rangle) + \cdots + a_0(x^0 + \langle p(x)\rangle) \\ &= a_n x^n + \cdots + a_0 + \langle p(x)\rangle \\ &= p(x) + \langle p(x)\rangle \\ &= \langle p(x)\rangle. \end{aligned}$$

So α is a root. □

Proposition 8.6. If $p(x)$ is irreducible, there exists a bijection between the elements of $F[x]/\langle p(x)\rangle$ and those of the set

$$R = \{r(x) \mid r(x) \in F[x] \text{ and } \deg r(x) < \deg p(x)\}.$$

Proof. Let $g(x)+\langle p(x)\rangle \in F[x]/\langle p(x)\rangle$. By the division algorithm, there exist $q_g(x), r_g(x) \in F[x]$ such that

$$g(x) = p(x)q_g(x) + r_g(x).$$

Therefore,

$$g(x) - r_g(x) = p(x)q_g(x) \in \langle p(x)\rangle,$$

and in particular,

$$g(x) + \langle p(x)\rangle = r_g(x) + \langle p(x)\rangle.$$

Define

$$\begin{aligned} \varphi :\ & F[x]/\langle p(x)\rangle \to R, \\ & g(x) + \langle p(x)\rangle \mapsto r_g(x). \end{aligned}$$

One can then show that φ is indeed a bijection. □

Example 8.7. What are the irreducible elements of $F = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$?

Solution. The polynomial $p(x) = x^2 + x + 1$ is irreducible, since neither 0 nor 1 are roots of $p(x)$. So the elements of F are in one-to-one correspondence with polynomials of degree less than 2.

$$F = \left\{ \begin{array}{r} 0 + \langle x^2 + x + 1\rangle, \\ 1 + \langle x^2 + x + 1\rangle, \\ x + \langle x^2 + x + 1\rangle, \\ x^2 + \langle x^2 + x + 1\rangle \end{array} \right\}$$

□

8.2 Lecture 30 — Algebraic Extensions

We will assume for this lecture that E is an extension of the field F, i.e. $E \supseteq F$ and E is a field.

Definition 8.8 (algebraic element, transcendental element)**.** We say that $\alpha \in E$ is **algebraic** over F if there exists a polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$. Otherwise, we say that α is **transcendental**.

Example 8.9.

- $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since $\sqrt{2}$ is a root of $p(x) = x^2 - 2$.
- $i \in \mathbb{C}$ with $i^2 = -1$ is algebraic over $\mathbb{R}$ since i is a root of $p(x) = x^2 + 1$.
- $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Q}$ (this is hard to prove!)

Remark. It is difficult to prove an element of a field extension is transcendental. But most of $\mathbb{R}$ is comprised of transcendental numbers. A set-theoretic counting argument shows that there are only countably many polynomials over $\mathbb{Q}$ and therefore that there are countably many algebraic numbers. But $\mathbb{R}$ is provably uncountable. So it must be that there are uncountably many transcendental numbers.

Example 8.10. Show $\sqrt{3+\sqrt{5}}$ is algebraic over $\mathbb{Q}$.

Solution. Let $\alpha = \sqrt{3+\sqrt{5}}$. Then

$$\begin{aligned}
\alpha &= \sqrt{3+\sqrt{5}} \\
\alpha^2 &= 3+\sqrt{5} \\
\alpha^2 - 3 &= \sqrt{5} \\
(\alpha^2-3)^2 &= 5 \\
\alpha^4 - 6\alpha^2 + 9 - 5 &= 0 \\
\alpha^4 - 6\alpha^2 + 4 &= 0
\end{aligned}$$

So α is a root of

$$p(x) = x^4 + 6x^2 + 4.$$

□

Definition 8.11 (algebraic extension). An extension E of a field F is **algebraic** if every element of E is algebraic over F.

Example 8.12. $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$.

Definition 8.13 (simple extension). Suppose $\alpha_1, \dots, \alpha_n \in E$. Let $F(\alpha_1, \dots, \alpha_n)$ be the smallest extension of F containing $\alpha_1, \dots, \alpha_n$. If $E = F(\alpha)$ for some $\alpha \in E$, then E is called a **simple extension** of F.

Example 8.14.

- $\mathbb{C} = \mathbb{R}(i)$ is a simple extension of $\mathbb{R}$.
- $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2})$ is a simple extension of $\mathbb{Q}$.

Recall that if F is a field, then $F[x]$ is a domain. So we can form the field of fractions for $F[x]$:

$$F_{F[x]} = \left\{ \frac{p(x)}{q(x)} \;\middle|\; p(x), q(x) \in F[x],\; q(x) \neq 0 \right\}.$$

Theorem 8.15. $\alpha \in E$ is transcendental over F if and only if $F(\alpha) \cong F[x]$.

Essentially, the above theorem states that transcendental α "behaves" like a variable.

Example 8.16. By the above theorem, $\mathbb{Q}(\pi) \cong \mathbb{Q}[x]$. So we can think of elements of $\mathbb{Q}(\pi)$ as $\frac{p(\pi)}{q(\pi)}$, where $p(x), q(x) \in \mathbb{Q}[x]$. For example,

$$\frac{3\pi^2 + 2\pi + 17}{\frac{1}{3}\pi^3 + 5} \in \mathbb{Q}(\pi).$$

Theorem 8.17. Suppose $\alpha \in E$ is algebraic over F. Then there exists a unique monic irreducible polynomial $p(x) \in F[x]$ with minimal degree such that $p(\alpha) = 0$. Furthermore, if $f(x) \in F[x]$ is another polynomial with $f(\alpha) = 0$, then $p(x)$ divides $f(x)$.

Proof. Consider the evaluation homomorphism

$$\begin{aligned}\varphi \colon F[x] &\to E,\\ q(x) &\mapsto q(\alpha).\end{aligned}$$

Then $\ker\varphi = \{f(x) \mid f(\alpha) = 0\} \subseteq F[x]$. Since $F[x]$ is a PID, $\ker\varphi = \langle p'(x)\rangle$ for some polynomial $p'(x) \in F[x]$. We can find a unit $u \in F$ such that $p(x) = up'(x)$ and $p(x)$ is monic. Since $p(x)$ and $p'(x)$ are associates, $\langle p(x)\rangle = \langle p(x)\rangle$. We claim that $p(x)$ is the desires polynomial.

Observe that $p(x)$ has smallest degree by our choice for a generator for $\ker\varphi$. Now suppose for a contradiction that $p(x) = r(x)s(x)$ for $r(x)s(x) \in F[x]$ and $\deg r(x), \deg s(x) \geq 1$. Then $0 = p(\alpha) = r(\alpha)s(\alpha)$. But E is a field. So either $r(\alpha) = 0$ or $s(\alpha) = 0$. So either $r(x) \in \ker\varphi$ or $s(x) \in \ker\varphi$. But this contradicts the choice for $p(x)$. So $p(x)$ must be irreducible.

Finally, if $f(\alpha) = 0$ then $f(x) \in \ker\varphi$, so $p(x)$ divides $f(x)$. □

Definition 8.18 (minimal polynomial)**.** The polynomial $p(x)$ as in Theorem 8.17 is called the **minimal polynomial** for α over F. We say that the root α has degree $\deg p(x)$ over F.

Theorem 8.19. Suppose $\alpha \in E$ is algebraic over F. Then the subfield $F(\alpha)$ of E satisfies

$$F(\alpha) \cong F[x]/\langle p(x)\rangle,$$

where $p(x)$ is the minimal polynomial for α.

Proof. Consider the evaluation homomorphism

$$\begin{aligned}\varphi \colon F[x] &\to F(\alpha),\\ q(x) &\mapsto q(\alpha).\end{aligned}$$

As before, $\ker\varphi = \langle p(x)\rangle$. So by the First Isomorphism Theorem,

$$F[x]/\langle p(x)\rangle \cong \operatorname{im}\varphi \subseteq F(\alpha).$$

Note that $F[x]/\langle p(x)\rangle$ is a field (since $p(x)$ is irreducible) and it contains a copy of F. So $\operatorname{im}\varphi$ contains an isomorphic copy of F. At the same time, $\alpha \in \operatorname{im}\varphi$, since $x \mapsto \alpha$ under φ. So $\operatorname{im}\varphi$ contains F and α, and is a field. But $F(\alpha)$ is the smallest extension of F containing α. So

$$F(\alpha) \subseteq \operatorname{im}\varphi \subseteq F(\alpha).$$

□

Example 8.20. x^2-2 has two roots: $\sqrt{2}$ and $\sqrt{-2}$. So both $\sqrt{2}$ and $\sqrt{-2}$ are algebraic over $\mathbb{Q}$. So

$$\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/\langle x^2 - 2\rangle \cong \mathbb{Q}(\sqrt{-2}).$$

Generalizing the above example, if α and β are roots of the irreducible polynomial $p(x)$, then

$$F(\alpha) \cong F(\beta) \cong F[x]/\langle p(x)\rangle.$$

So different roots of are not algebraically distinguishable.

8.3 Lecture 31 — Field Extensions and Linear Algebra

Observe that if E is an extension of the field F, then E is also an vector space over F, i.e. the elements of E are the “vectors” and the elements of F are the “scalars”, with scalar multiplication

$$F \times E \to E,$$
$$(f, e) \mapsto fe.$$

Example 8.21. $\mathbb{C}$ is an extension of $\mathbb{R}$, so $\mathbb{C}$ is a $\mathbb{R}$-vector space:

$$\mathbb{R} \times \mathbb{C} \to \mathbb{C},$$
$$(r, a + bi) \mapsto ra + rbi.$$

One can easily check that the vector space axioms hold.

Theorem 8.22. Let F be a field and $F(\alpha)$ be a simple extension of F, where $\alpha \in F(\alpha)$ is algebraic over F. Suppose that the degree of the minimal polynomial of α is n. Then every element of $F(\alpha)$ can be written uniquely as

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1},$$

where $b_i \in F$.

Example 8.23.

- $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.
- $\mathbb{C} = \mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\}$.

Recall that if E is an F-vector space, the dimension of E over F is

$$\dim_F E = \text{number of basis elements.}$$

Corollary 8.24. If $E = F(\alpha)$ is a simple extension with $\alpha \in E$ algebraic over F, then

$$\dim_F E = n = \text{degree of } \alpha.$$

Proof. By the previous result,

$$\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$$

is a basis for $F(\alpha)$ over F. □

Example 8.25.

- $\dim_{\mathbb{R}} \mathbb{C} = 2$ and $\dim_{\mathbb{C}} \mathbb{C} = 1$
- $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$

Definition 8.26 (degree). If E is an extension of F, the **degree** of the extension is

$$[E : F] = \dim_F E.$$

If $[E : F] < \infty$, we say that the degree of the extension E over F is **finite**. Otherwise it is infinite.

Example 8.27. $[\mathbb{C} : \mathbb{R}] = 2$.

Theorem 8.28. If $[E : F]$ is finite, then E is an algebraic extension of the field F.

Proof. Let $n = [E : F]$. Let $\alpha \in E$ be arbitrary. Consider the $n + 1$ elements

$$1, \alpha, \alpha^2, \dots, \alpha^n$$

of E. Since $[E : F] = n$, these vectors are linearly dependent. So there exist $b_0, b_1, \dots, b_n \in F$ such that

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0$$

Consider the polynomial $p(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$. Then α is a root of this polynomial. So E is algebraic over F. □

> *Remark.* The converse is not always true. There are fields that are algebraic but $[E : F] = \infty$.

Example 8.29. $E = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots)$ is algebraic but $[E : \mathbb{Q}] = \infty$.

Example 8.30. $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$.

Theorem 8.31. If E is an extension of F and K is an extension of E, then K is an extension of F. Furthermore, if these are finite extensions, then

$$[K : F] = [K : E][E : F].$$

Proof. Suppose $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ is a basis for E over F and suppose $\{\beta_1, \beta_2, \dots, \beta_n\}$ is a basis for F over E. We claim that $\{\alpha_i\beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for K over F with cardinality mn. So we need to show this set is linearly independent and spans K over F. The remainder of the proof is left as an exercise. □

Corollary 8.32. If $F_k \supseteq F_{k-1} \supseteq \cdots \supseteq F_0$ are fields and F_{i+1} is a finite extension of F_i, then

$$[F_k : F_0] = [F_k : F_{k-1}] \cdots [F_1 : F_0].$$

Corollary 8.33. If $\alpha \in E$ is algebraic over F with minimal polynomial $p(x)$ and if $\beta \in F(\alpha)$ with minimal polynomial $q(x)$, then $\deg q(x)$ divides $\deg p(x)$.

Proof. We have $\beta \in F(\alpha)$, so $F(\beta) \subseteq F(\alpha)$. So

$$[F(\alpha) : F] = [F(\alpha) : F(\beta)][F(\beta) : F].$$

But $[F(\alpha) : F] = \deg p(x)$ and $[F(\beta) : F] = \deg q(x)$. So

$$\deg p(x) = [F(\alpha) : F(\beta)] \deg q(x).$$

□

Theorem 8.34. Let E be a field extension of F. Then the following are equivalent:

(a) E is a finite extension of F.

(b) There exists a finite number of algebraic elements $\alpha_1, \alpha_2, \dots, \alpha_n$ such that $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

(c) There exists a sequence of fields

$$F(\alpha_1, \alpha_2, \dots, \alpha_n) \supseteq F(\alpha_1, \alpha_2, \dots, \alpha_{n-1}) \supseteq \cdots \supseteq F$$

such that each $[F(\alpha_1, \alpha_2, \dots, \alpha_{i+1}) : F(\alpha_1, \alpha_2, \dots, \alpha_i)]$ is finite and α_{i+1} is algebraic over $F(\alpha_1, \alpha_2, \dots, \alpha_i)$.

Example 8.35. Consider $E = \mathbb{Q}(\sqrt[3]{5}, \sqrt{5}i)$. Then we have the chain

$$\underbrace{\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}i) \supseteq}_{x^2+5} \underbrace{\mathbb{Q}(\sqrt[3]{5}) \supseteq}_{x^3-5} \mathbb{Q}.$$

So in this example $[\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}i) : \mathbb{Q}] = 6$

Example 8.36. Is $\mathbb{Q}(\sqrt{3}) \cong \mathbb{Q}(\sqrt{2})$?

Solution. As vector spaces, these extensions of $\mathbb{Q}$ are isomorphic.

$$\mathbb{Q}(\sqrt{3}) \cong \mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}^2.$$

They are, however, not isomorphic as fields. Take $1 \in \mathbb{Q}(\sqrt{2})$ and suppose there is an isomorphism

$$\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3}).$$

So it must be that $\varphi(1) = 1$. So

$$\begin{aligned} \varphi(2) &= \varphi(1+1) \\ &= \varphi(1) + \varphi(1) \\ &= 1 + 1 \\ &= 2. \end{aligned}$$

Furthermore,

$$\begin{aligned} \varphi(2) &= \varphi(\sqrt{2}\sqrt{2}) \\ &= \varphi(\sqrt{2})\varphi(\sqrt{2}). \end{aligned}$$

So $\varphi(\sqrt{2})^2 = 2$. So $\varphi(\sqrt{2})$ is a root of 2 in $\mathbb{Q}(\sqrt{3})$. But then in $\mathbb{Q}(\sqrt{3})$, if $(a+b\sqrt{3})^2 = 2$, $a^2 + 2ab\sqrt{3} + 3b^2 = 2$. Since $\sqrt{3}$ is irrational $a = 0$ or $b = 0$. But if $a = 0$, $3b^2 = 2$ and if $b = 0$, $a^2 = 2$, both of which yield a contradiction. □

8.4 Lecture 32 — Algebraic Closure and Splitting Fields

Given a polynomial $p(x) \in F[x]$, we can find an extension E of F such that E has a root of $p(x)$. A guiding question for this lecture is as follows: *Is there an exension E' of F that contains all the roots of all $p(x) \in F[x]$?*

Theorem 8.37. Let E be an extension of F and consider

$$E' = \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}.$$

Then E' is an extension of F, i.e. E' is a subfield of E. We call E' the **algebraic closure** of F in E.

Proof. Given $\alpha, \beta \in E'$, we need to show $\alpha \pm \beta$, $\alpha\beta$ and α/β $(\beta \neq 0)$ all belong to E'. Both α and β are algebraic over F, so $F(\alpha, \beta)$ is a finite extension of F. But then every element of $F(\alpha, \beta)$, is algebraic over F. But $\alpha \pm \beta$, $\alpha\beta$ and α/β $(\beta \neq 0)$ all belong to $F(\alpha, \beta)$. So all these elements are algebraic over F, so they also belong to E'. □

Definition 8.38. A field F is **algebraically closed** if every nonconstant polynomial $p(x) \in F[x]$ has a root.

Example 8.39. $\mathbb{R}$ is not algebraically closed since $x^2 + 1$ has no root.

Theorem 8.40. A field F is algebraically closed if and only if every nonconstant polynomial $p(x) \in F[x]$ factors into linear polynomials.

Proof. Suppose first that F is algebraically closed. Let $p(x)$ be a nonconstant polynomial. Since F is algebraically closed, $p(x)$ has a root α_1 in F. So $p(x) = (x - \alpha_1)q_1(x)$ with $\deg q_1(x) < \deg p(x)$. Now repeat with $q_1(x)$ and obtain another root α_2. Once k is such that $\deg q_k = 1$, we have a factorization

$$c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$$

for $p(x)$.

Now suppose $p(x) \in F[x]$ factors into linear polynomials. Then

$$p(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k),$$

with $c, \alpha_1, \ldots, \alpha_k \in F$. But then α_i is a root of $p(x)$ for each i. □

Corollary 8.41. If F is algebraically closed, then there is no proper algebraic extension of F.

Proof. Suppose E is an algebraic extension of F (so $F \subseteq E$). Let $\alpha \in E$, and let $p(x) \in F[x]$ be its minimal polynomial. But F being algebraically closed implies that $p(x)$ factors into linear factors in $F[x]$. Also, $p(x)$ is irreducible. This forces $p(x) = c(x-\alpha)$. So $\alpha \in F$. Thus $E = F$. □

Theorem 8.42. Every field has a unique algebraic closure (up to isomorphism).

Theorem 8.43 (Fundamental Theorem of Algebra)**.** The field $\mathbb{C}$ is algebraically closed. Equivalently, all polynomials $p(x) \in \mathbb{C}[x]$ can be factored into linear factors.

We will specify our motivating question: *Given a particular $p(x) \in F[x]$, what field contains all the roots of $p(x)$ and is the smallest such field?*

Example 8.44. Consider $p(x) = x^4 - 2x^2 - 3 \in \mathbb{Q}[x]$. We have (in $\mathbb{C}$)

$$\begin{aligned} p(x) &= x^4 - 2x^2 - 3 \\ &= (x^2-3)(x^2+1) \\ &= (x-\sqrt{3})(x+\sqrt{3})(x-i)(x+i). \end{aligned}$$

The field $\mathbb{Q}(\sqrt{3}, i)$ is the smallest field for which $p(x)$ “splits”.

Definition 8.45 (splitting field)**.** An extension E is a **splitting field** for $p(x) \in F[x]$ if there exist $\alpha_1, \alpha_2, \dots, a_n \in E$ such that

$$E = F(\alpha_1, \alpha_2, \dots, a_n)$$

and

$$p(x) = c(x-\alpha_1)\cdots(x-\alpha_n).$$

We say a polynomial $p(x) \in F[x]$ **splits** in E if it is a product of linear functions in $E[x]$.

Example 8.46. Consider $p(x) = x^3 - 5 \in \mathbb{Q}[x]$. This has a root $\sqrt[3]{5}$ in $\mathbb{Q}(\sqrt[3]{5})$, but this is not a splitting field for $p(x)$ since $p(x)$ has two other complex roots:

$$x^3 - 5 = (x - \sqrt[3]{5})(x^2 + \sqrt[3]{5}x + (\sqrt[3]{5})^2),$$

and

$$\operatorname{disc}(p(x)) < 0.$$

Theorem 8.47. Let $p(x) \in F[x]$ be a nonconstant polynomial. Then a splitting field for $p(x)$ exists.

Proof. The proof is by induction on the degree of $p(x)$.

If $\deg p(x) = 1$, then $p(x) = c(x - \alpha)$ with $c, \alpha \in F$, so F is the splitting field.

Assume that for all $q(x) \in F[x]$ with $\deg q(x) < n$, there exists a splitting field. Let $p(x) \in F[x]$ be such that $\deg p(x) = n$. In the case that $p(x)$ is reducible, $p(x) = p_1(x) \cdots p_r(x)$ where $p_1(x), \dots, p_r(x) \in F[x]$ are irreducible. But $\deg p_i(x) < n$ for each i. So by the induction hypothesis, there exist splitting fields E_i for each $p_i(x)$. So $E = \bigcup_{i=1}^{r} E_i$ is the splitting field for $p(x)$. If $p(x)$ is irreducible, there is a field K such that $p(x)$ has a root $\alpha \in K$. So $p(x) = (x - \alpha)q(x)$ for $q(x) \in K[x]$ and $\deg q(x) < n$. In fact, $K = F(\alpha)$. By the induction hypothesis there is a splitting field $K(\alpha_2, \dots, \alpha_n)$ for $q(x)$. But $K(\alpha_2, \dots, \alpha_n) = F(\alpha)(\alpha_2, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_n)$. □

Theorem 8.48. The splitting field of $p(x) \in F[x]$ is unique up to isomorphism.

Theorem 8.49. Suppose that E is the splitting field for $p(x) \in F[x]$. If $\deg p(x) = n$, then

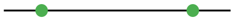
$$[E : F] \leq n!.$$

8.5 Lecture 33 — Geometric Constructions I

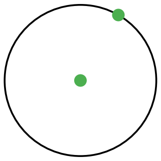
Definition 8.50 (straightedge, compass)**.** A **straightedge** is an *unmarked* tool used to draw lines between points. A **compass** is a tool used to draw circles centered at a fixed point with a fixed radius. Our compass is "collapsible" i.e. lifting the compass resets the separation of the legs.

A **straightedge and compass construction** is any drawing in the plane that can be made using a straightedge and a compass, following the following rules.

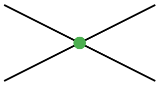
1. Given two points, we can construct a line between them.



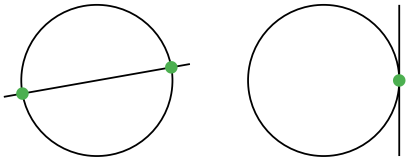
2. Given two points, we can construct a circle centered at a point with the other on the circumference.



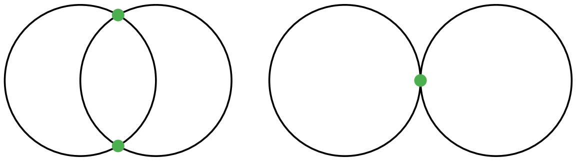
3. Intersecting two lines constructs a point.



4. Intersecting a line and a circle constructs one or two points.



5. Intersecting two circles constructs one or two points.



The following question naturally arises:

> Using the above rules, what can we make?

Example 8.51. We can construct the midpoint between any two points.

Proof. Given two points P_1 and P_2, follow these steps:

(1) Draw a line L_1 between P_1 and P_2.

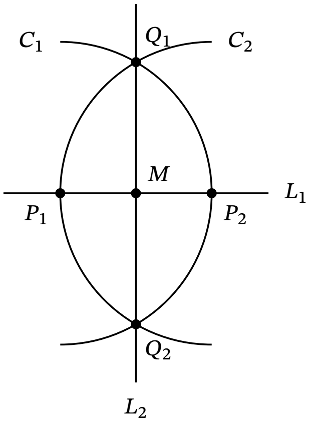
(2) Draw a circle C_1 with center P_1 and circumference point P_2.

(3) Draw a circle C_2 with center P_2 and circumference point P_1.

(4) Label the intersections of these circles Q_1 and Q_2.

(5) Draw a line L_2 passing through Q_1 and Q_2.

(6) The intersection M of L_1 and L_2 is the midpoint of P_1 and P_2



□

Example 8.52. There are other constructions that can be made using the outlined rules:

- The previous example shows that we can construct a perpendicular bisector.
- Given a line segment $\overline{AB}$, we can create a square with side length AB.
- Given a line L and a point P off of L, we can create a line L' passing through P and parallel to L.
- Given a rectangle with area A, we can construct a square with area A.
- Given an angle θ, we can construct the angle $\theta/2$. That is, any angle can be bisected.

Asking what *can* be constructed gave rise to some classical problems:

(a) Trisecting an arbitrary angle.

(b) Squaring the circle.

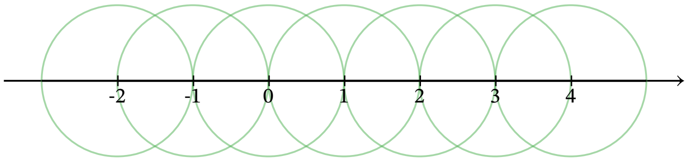
(c) Doubling the cube.

Neither of these constructions are possible! We need field theory to prove this. Constructions (a) and (c) were proved not possible by Wentzel in 1837 and (b) follows from Lindemann's 1882 proof that π is transcendental.

The proofs will be discussed in more detail next lecture. First, we need to set up some vocabulary and prove some intermediate results.

Definition 8.53 (constructible number). A real number α is **constructible** if a line segment of length $|\alpha|$ can be constructed in the plane in a finite number of steps using only a straightedge and compass

Example 8.54. Every element of $\mathbb{Z}$ is constructible.

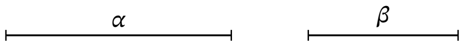


Note that $\frac{1}{2}$ can be constructed by taking a midpoint.

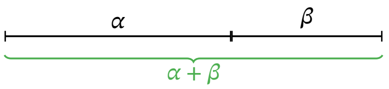
Theorem 8.55. The set of all constructible numbers F is a subfield of $\mathbb{R}$.

Proof. Given $\alpha, \beta \in F$, we need to show $\alpha \pm \beta \in F$, $\alpha\beta \in F$ and $\frac{\alpha}{\beta} \in F$.

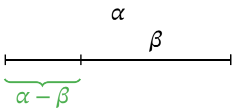
Without loss of generality, suppose $\alpha > \beta$.



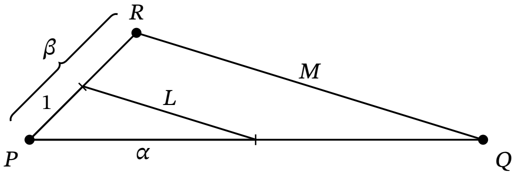
The segments can be joined together to form $\alpha + \beta$.



Similarly, the segments can be superimposed to form $\alpha - \beta$.



To construct $\alpha\beta$, consider the case where $\beta > 1$ and form a triangle with sides of length 1 and α, where the sides of length 1 and α join at the point P. Call the other side L. Extend the side of length 1 to β and call the endpoint R. Draw a line M through R parallel to L and intersect it with an extension of the segment of length α. Call the intersection Q. Then the length PQ is $\alpha\beta$.



This works by similar triangles: $\frac{1}{\alpha} = \frac{\beta}{PQ} \Rightarrow PQ = \alpha\beta$.

The construction of $\frac{\alpha}{\beta}$ is left as an exercise. ▢

8.6 Lecture 34 — Geometric Constructions II

Recall that a number $\alpha \in \mathbb{R}$ is constructible if we can construct a line segment of length $|\alpha|$ using only straightedge and compass operations.

The set

$$\{\alpha \in \mathbb{R} \mid \alpha \text{ is constructible}\} \subseteq \mathbb{R},$$

Is a proper subfield of $\mathbb{R}$ and a proper extension of $\mathbb{Q}$.

Definition 8.56 (constructible). A point $P = (a, b)$ is **constructible** if both a and b are constructible.

Lemma 8.57. Let F be a subfield of $\mathbb{R}$.

(a) If a line L contains points P_1 and P_2 in F, then its equation has the form

$$ax + by + c = 0, \qquad \text{with } a, b, c \in F.$$

(b) If a circle has center P in F and a radius $r \in F$, then its equation has the form

$$x^2 + y^2 + dx + ey + f = 0, \qquad \text{with } d, e, f \in F.$$

Proof. We prove (b).

Let S be a circle with center $P = (a, b) \in F^2$ and radius $r \in F$. Then its equation is

$$\begin{aligned} (x-a)^2 + (y-b)^2 &= r^2 \\ x^2 - 2ax + a^2 + y^2 - 2by + b^2 &= r^2 \\ x^2 + y^2 + (-2a)x + (-2b)y + (a^2 + b^2 + r^2) &= 0. \end{aligned}$$

But since $a, b, r \in F$, it must also be that $(-2a), (-2b), (a^2 + b^2 + r^2) \in F$. □

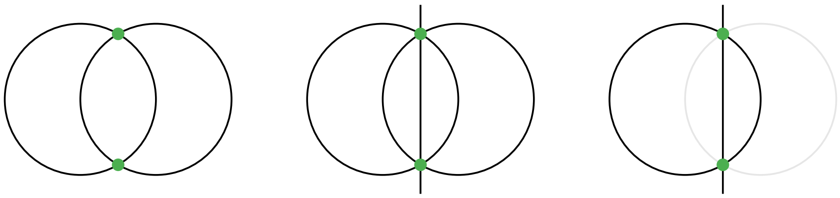
Starting with a field F of constructible numbers, recall how we can add "new" points:

(i) Intersect two lines, each of which passes through two points with coordinates in F.

(ii) Intersect a line and a circle with center and radius in F.

(iii) Intersect two circles with centers and radii in F.

Note that case (iii) reduces to case (ii).



In case (i), since the two equations have the form $ax + by + c = 0$ with coefficients in F, the intersection will have coordinates in F.

In case (ii), we want to solve

$$\begin{cases} ax + by + c = 0, \\ x^2 + y^2 + dx + ey + f = 0, \end{cases}$$

where $a, b, c, d, e, f \in F$. Solve $y = -\frac{a}{b}x - \frac{c}{b}$ and substitute into the second equation and obtain

$$x^2 + \left(-\frac{a}{b}x - \frac{c}{b}\right)^2 + dx + e\left(-\frac{a}{b}x - \frac{c}{b}\right) + f = 0.$$

Expanding gives an equation of the form

$$Ax^2 + Bx + C = 0,$$

where $A, B, C \in F$. So

$$x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A} \quad \text{and} \quad y = -\frac{a}{b}\left(\frac{-B \pm \sqrt{B^2 - 4AC}}{2A}\right) - \frac{c}{b}.$$

But notice that it is not necessarily the case that these solutions x, y lie in F. But $x, y \in F(\sqrt{\alpha})$ where $\alpha = B^2 - 4AC$. So this implies that $\sqrt{\alpha}$ is constructible.

To recap, when creating points by intersecting two lines, we get points with coordinates in F, but when creating points by intersecting a circle and a line, we get points with coordinates in $F(\sqrt{\alpha})$, for some α and observe that $[F(\sqrt{\alpha}) : F] = 1$ or $[F(\sqrt{\alpha}) : F] = 2$. So $F(\alpha)$ is at most a **quadratic extension**.

Theorem 8.58. $\alpha \in \mathbb{R}$ is constructible if and only if there is a sequence of fields

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_k$$

such that $F_i = F_{i-1}(\sqrt{\alpha_i})$ for some $\alpha_i \in F_{i-1}$. In particular,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k,$$

if and only if α is constructible.

Impossible Constructions

(1) **Squaring a circle:** *Given a circle of radius 1, construct a square with the same area as the circle.*

This problem is equivalent to constructing a square with area π and thus segments of length $\sqrt{\pi}$. So this would require $\sqrt{\pi}$ to be constructible. But $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$ since π, and thus $\sqrt{\pi}$, is transcendental.

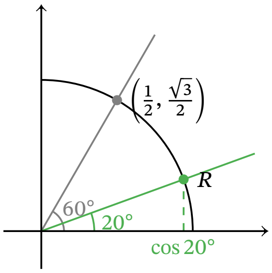
(2) **Doubling a cube:** *Given a cube of volume 1, construct a cube with double its volume.*

This problem is equivalent to constructing a cube with side lengths $\sqrt[3]{2}$. But $\sqrt[3]{2}$ is not constructible since

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^k.$$

(3) Trisect an angle: *Given an angle with measure θ, construct an angle with measure $\theta/3$.*

Note that the point $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ is constructible. This is the point obtained by intersecting the unit circle with a line forming an angle of 60° with the x-axis. A point R on the unit circle trisecting this angle would construct $\cos 20°$.



Using trigonometric identities,

$$\begin{aligned}
\cos 3\theta &= \cos(2\theta + \theta) \\
&= \cos(2\theta)\cos\theta - \sin(2\theta)\sin\theta \\
&= (2\cos^2\theta - 1)\cos\theta - 2\sin^2\theta\cos\theta \\
&= (2\cos^2\theta - 1)\cos\theta - 2(1-\cos^2\theta)\cos\theta \\
&= 4\cos^3\theta - 3\cos\theta.
\end{aligned}$$

So $\cos 20°$ satisfies

$$\begin{aligned}
4(\cos 20°)^3 - 3(\cos 20°) - \cos(60°) &= 0 \\
4(\cos 20°)^3 - 3(\cos 20°) - \frac{1}{2} &= 0.
\end{aligned}$$

Thus, $\cos 20°$ is a root of $p(x) = 4x^3 - 3x - \frac{1}{2}$. But $p(x)$ is irreducible over $\mathbb{Q}$. So $[Q(\cos°) : \mathbb{Q}] = 3 \neq 2^k$.

Homework Assignments

Assignment 1

1. Let G be a group and H be a subgroup of G. For any $g \in G$, prove that

$$gHg^{-1} = \left\{ghg^{-1} \mid h \in H\right\}$$

is also a subgroup of G.

2. Determine all the non-isomorphic abelian groups of order 2024. Justify your answer.

Hint. $2024 = 2^3 \cdot 11 \cdot 23$.

3. Let p and q be distinct primes. Prove that the number of distinct finite abelian groups of order p^4 is the same as the number of distinct finite abelian groups of order q^4. How many distinct finite abelian groups of order $p_1^4 p_2^4 \cdots p_r^4$ are there if $p_1, \dots, p_r$ are all distinct primes?

4. You are given a finite abelian group with $|G| = 16$. As well, you are told that G has an element of order 8 and two elements of order 2. What group is G isomorphic to? Justify your answer.

5. Let G be an abelian group where the operation is addition. Let K be a proper subgroup of G, and suppose that $d \in G \setminus K$, that is d is an element of G not in K. Show that the set

$$H = \{k + zd \mid k \in K, z \in \mathbb{Z}\}$$

is also a subgroup of G with $K \subsetneq H$.

Remark. This exercise justifies a step we used in the proof of the Fundamental Theorem of Finite Abelian Groups given in Lecture 5.

6. Suppose G is an abelian group of order 25. You are able to ask an "oracle" about the order of a particular element in the group. What is the maximum number of times you have to ask the "oracle" for an answer to figure out the structure of G? Justify your answer.

7. Find all composition series of $S_3 \times \mathbb{Z}_3$.

8. Let G and H be solvable groups. Show that $G \times H$ is also solvable.

Assignment 2

1. Show that D_{2024} is a solvable group (for clarity, this is the dihedral group on the 2024-gon, so this group has 4048 elements).

2. Let N be a normal subgroup of G. If N and G/N are solvable groups, show that G is a solvable group.

3. Let $X = \{1, 2, 3, 4, 5, 6\}$ and consider the group $H = \{(1), (1\,4)(2\,5)(3\,6)\}$. The elements of H act on X as functions. Determine all the unique orbits of this action and write X as a partition of these orbits.

4. Find the class equation for D_5. Show all your work.

5. A flag with seven horizontal stripes can be coloured with three different colours. How many distinct flags can you make?

6. What does the First Sylow Theorem tell you about all the groups of order 2024? What does the Third Sylow Theorem tell you about the Sylow 23-subgroups of a group of order 2024?

7. Prove that a noncyclic group of order 21 must have 14 elements of order 3.

   Hint. The theorem given below will be helpful.

   Theorem. Let G be a finite group and suppose that M and N are normal subgroups of G such that $M \cap N = \{e\}$ and $|M||N| = |G|$. Then $G \cong M \times N$.

8. Prove that if G is a group with $|G| = 99$, then $G \cong \mathbb{Z}_{99}$ or $G \cong \mathbb{Z}_3 \times \mathbb{Z}_{33}$.

   Hint. The theorem given previously will be helpful.

9. Go to `http://abstract.ups.edu/aata/aata.html` and review the tutorial in Chapter 14. Also, review the Sage documentation found here:

   `https://doc.sagemath.org/html/en/thematic_tutorials/group_theory.html#conjugacy`

   Now find the class equations for $D_3, D_4, \ldots, D_{10}$. (Note, you will be able to check your answer for Exercise 4).

Assignment 3

1. Let $\mathbf{x} = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}^{\mathsf{T}}$ be a point on the unit sphere in $\mathbb{R}^3$. That is, ${x_1}^2 + {x_2}^2 + {x_3}^2 = 1$. Prove that if $A \in \mathrm{O}_3(\mathbb{R})$, where $\mathrm{O}_3(\mathbb{R})$ is the group of 3×3 orthogonal matrices, then $A\mathbf{x}$ is also on the unit sphere.

2. Let $\varphi : R \to S$ be a homomorphism of rings. If J is an ideal of S and $I = \{r \in R \mid \varphi(r) \in J\}$, then prove that I is an ideal of R and $\ker(\varphi) \subseteq I$.

3. Let T be the set of rational numbers whose denominators (in lowest terms) are not divisible by 101 (which is a prime number). Prove that T is a subring of $\mathbb{Q}$.

4. *This question extends from the previous question.*

   Let I be the elements of T such that 101 divides the numerator of an element of T. Prove that I is an ideal of T and that $T/I \cong \mathbb{Z}_{101}$.

   Hint. Recall that if $101 \nmid s$, then $s \not\equiv 0 \pmod{101}$. Furthermore, since $\mathbb{Z}_{101}$ is a field, there is a $u \in \mathbb{Z}_{101}$ such that $su = 1$ in $\mathbb{Z}_{101}$.

5. Prove or disprove the following statements:

   (i) If R is a commutative ring, then $R[x]$ is a commutative ring.

   (ii) If R has an identity, then $R[x]$ has an identity.

   (iii) If R is a field, then $R[x]$ is a field.

6. Consider the **derivative map** $\mathrm{D} : \mathbb{R}[x] \to \mathbb{R}[x]$ given by

$$\mathrm{D}(a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

   Is D a ring homomorphism? Either prove this statement or give a counterexample.

7. Recall that a nonzero element $a \in R$ is **nilpotent** if there is a positive integer $k \geq 2$ such that $a^k = 0$. Suppose that a_0 is a unit and a_1 is a nilpotent element of R. Prove that $a_0 + a_1 x$ is a unit in $R[x]$.

8. Suppose R is an integral domain. Assume that the division algorithm holds in $R[x]$. Prove that R is a field.

9. Go to `http://abstract.ups.edu/aata/aata.html` and review the tutorial in Chapter 17. Also look for documentation on the SAGE command `quo_rem`. Use SAGE to answer all of the problems of Exercise 3 of Section 17.5.

Assignment 4

1. Prove the Rational Root Theorem.

> **Theorem** (Rational Root Theorem)**.** Let
>
> $$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$
>
> with $a_n \neq 0$. If $\frac{r}{s}$ is a rational number with $\gcd(r, s) = 1$ such that $p\left(\frac{r}{s}\right) = 0$, then r divides a_0 and s divides a_n.

2. If $f(x) = a_n x^n + \cdots + a_0$ is a polynomial in $\mathbb{Z}[x]$ and if p is a prime that does not divide a_n, we can consider the polynomial $\bar{f}(x) = [a_n]x^n + \cdots + [a_0] \in \mathbb{Z}_p[x]$, where $[a_i]$ denotes the equivalence class of a_i in $\mathbb{Z}_p$. It can be shown that if $\bar{f}(x)$ is irreducible in $\mathbb{Z}_p$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$. Use this fact to show the following polynomials are irreducible in $\mathbb{Q}[x]$:

(i) $7x^3 + 6x^2 + 4x + 6$

(ii) $9x^4 + 4x^3 - 3x + 7$

Remark. The proof of this fact can be found in most abstract algebra textbooks. It gives you another tool to check if a polynomial is irreducible.

3. Consider the following subring of $\mathbb{Q}$ that is also a domain:

$$R = \left\{ \frac{n}{2^i} \;\middle|\; n \in \mathbb{Z}, i \geq 0 \right\}.$$

Prove that the field of fractions F_R is isomorphic to $\mathbb{Q}$.

Remark. In the above result, we can replace 2 with any prime p and get a similar result. Consequently, there are an infinite number of domains R with $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$ whose field of fractions is isomorphic to $\mathbb{Q}$.

4. Let D be a PID. Prove that every ideal of D is contained in a maximal ideal.

5. Let D be a Euclidean Domain with corresponding Euclidean valuation v. Prove that $u \in D$ is a unit if and only if $v(u) = v(1)$.

6. The ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ with $i^2 = -1$ is a Euclidean Domain via the Euclidean valuation $v(a + bi) = a^2 + b^2$.

(i) Find all the units of $\mathbb{Z}[i]$.

(ii) Show that if $v(a + bi)$ is a prime number, then the element $a + bi$ is an irreducible element of $\mathbb{Z}[i]$.

Hint. The previous question may be helpful.

7. The ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ with $i^2 = -1$ is a Euclidean Domain via the Euclidean valuation $v(a + bi) = a^2 + b^2$. Find q and r such that $2024 + i = (1 + 2024i)q + r$ with $r = 0$ or $v(r) < v(1 + 2024i)$. In other words, apply the division algorithm to $z = 2024 + i$ and $w = 1 + 2024i$.

8. A ring R has the **descending chain condition** if for every descending chain of ideals of R

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots,$$

there exists an integer N such that $I_N = I_{N+1} = I_{N+2} = \cdots$.

(i) Show that $\mathbb{Q}[x]$ does not have the descending chain condition.

(ii) Prove that an integral domain R is a field if and only if R satisfies the descending chain condition.

Hint. If $a \in R$ is such that $a \neq 0$ and a is not a unit, what can be said about the chain of ideals $(a) \supseteq (a^2) \supseteq (a^3) \supseteq \cdots$?

Assignment 5

1. Suppose that $p(x)$ is an irreducible polynomial of degree 2024 in $\mathbb{Z}_2[x]$. How many elements are in the field $\mathbb{Z}_2[x]/(p(x))$? How does your answer change if $p(x)$ is an irreducible polynomial in $\mathbb{Z}_p[x]$ with p a prime?

2. Show that $\sqrt{1+\sqrt{1+\sqrt{2022}}}$ is algebraic over $\mathbb{Q}$. What is the minimal polynomial of this element?

3. If r and s are nonzero integers, prove that $\mathbb{Q}(\sqrt{r}) = \mathbb{Q}(\sqrt{s})$ if and only if $r = t^2 s$ for some $t \in \mathbb{Q}$.

4. Show that $\mathbb{C}$ is algebraic over $\mathbb{R}$.

5. Let α be an algebraic element of E over F whose minimal polynomial in $F[x]$ has odd degree. Prove that $F(\alpha) = F(\alpha^2)$.

   Hint. Verify that $F(\alpha, \alpha^2) = [F(\alpha^2)](\alpha) = F(\alpha)$.

6. Let $n_1, \dots, n_t$ be t distinct positive integers. Prove that

$$[\mathbb{Q}(\sqrt{n_1}, \dots, \sqrt{n_t}) : \mathbb{Q}] \leq 2^t.$$

7. Compute a basis for the extension $\mathbb{Q}(\sqrt{2024}, i)$ over $\mathbb{Q}$. What is $[\mathbb{Q}(\sqrt{2024}, i) : \mathbb{Q}]$?

8. Prove or disprove: $\mathbb{Q}(\sqrt{5}) \cong \mathbb{Q}(\sqrt{2})$.

9. Prove that the following three statements are equivalent:

   (i) F is an algebraically closed field.

   (ii) Every irreducible polynomial in $F[x]$ has degree 1.

   (iii) Every non-constant polynomial in $F[x]$ splits in F.

10. Is it possible to construct with a straightedge and compass an isosceles triangle of perimeter 8 and area 1?

    Hint. No. You may want to use Exercise 2 of Assignment 4 (I used it in my solution).