MAT311: Abstract Algebra

Mahmudul Hasan Turjoy

Last updated: February 3, 2025

Preface

These lecture notes were taken in the course *MAT311: Abstract Algebra* taught by *Arnab Chakraborty* at BRAC University as part of the BSc. in Mathematics program Fall 2024.

These notes are not endorsed by the lecturer, and I often modified them after lectures. They are not accurate representations of what was actually lectured, and in particular, all errors are surely mine. If you find anything that needs to be corrected or improved, please inform me: mh.turjoy@yahoo.com.

— Mahmudul Hasan Turjoy

Contents

Lecture 0

23 Oct 2024

0.1 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n

$\mathbb{Z}$ = Set of integers.
Define a relation on $\mathbb{Z}$ by -

$$a \sim b \text{ if } n \mid (a-b).$$

Properties of this relation:

- $a \sim a$ (Reflexivity)
- $a \sim b \Rightarrow b \sim a$ (Symmetry)
- $a \sim b, b \sim c \Rightarrow a \sim c$ (Transitivity)

Hence, this is an equivalence relation.
If $a \sim b$, we say b is congruent to a modulo n and denote as $a \equiv b \pmod{n}$.
Let $\overline{a}$:= The set of all integers congruent to a mod n, then $\overline{a} = \{a + kn : k \in \mathbb{Z}\}$ is called equivalence class / congruence class / residue class of a mod n.
There are precisely n distinct equivalence classes mod n, namely

$$\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}.$$

Example. $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

Define an addition on $\mathbb{Z}/n\mathbb{Z}$ via -

$$\overline{a} \oplus \overline{b} = \overline{a+b}$$

Example. $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$.

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Notice that for all $a, b \in \mathbb{Z}/3\mathbb{Z}$ the following properties hold:

- $(a \oplus b) \in \mathbb{Z}/3\mathbb{Z}$ (**Closure**).
- $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ (**Associativity**).
- $a \oplus \overline{0} = \overline{0} \oplus a = a$ (**Identity element**).
- For all $a \in \mathbb{Z}/3\mathbb{Z}$, there exists $b \in \mathbb{Z}/3\mathbb{Z}$ such that $a \oplus b = b \oplus a = \overline{0}$ (**Inverse element**).

These properties hold for $\mathbb{Z}/n\mathbb{Z}$ in general.
Now let's move on to a totally different kind of set.

0.2 Rotational Symmetries of an Equilateral Triangle

Consider the set of all roational symmetries of an equilateral triangle.

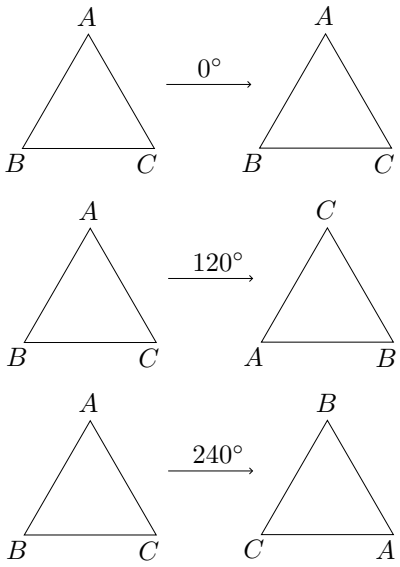


Figure 1: Symmetries of Triangle

A symmetry is something we do to an object that leaves the object intact. In case of the equilateral triangle we have three roational symmetires: roatation by $0°, 120°$ and $240°$. The operation here is to compose two symmetries, meaning apply one after another. Notice, composition of two symmetries is again a symmetry **(Closure)**. Composition of three symmetries is associative, because we really applying symmetries from the left to right **(Associativity)**. We consider rotation by $0°$ or 'do nothing' is also a symmetry. When we compose this with another symmetry, the other symmetry is unchanged **(Identity)**. Finally, given any symmetry, we can undo the symmetry **(Inverse elemnet)**.
Although, our earlier example of $\mathbb{Z}/3\mathbb{Z}$ and the Symmetries of a triangle is totally different set, both share four common properties.
A set equipped with an operation that follows these four properties is called a *Group*.

Lecture 1

28 Oct 2024

> "The axioms for a groups are short and natural... Yet somehow hidden behind these axioms is the monster simple group, a huge and extraordinary mathematical object, which appears to rely on numerous bizzare coincidences to exists. The axioms for groups give no obvious hint that anything like this exits."
>
> — Richard Borcherds, Mathematicians: An Outer View...

> "The one thing I would really like to know before I die is why the monster group exists."
>
> — John Conway, in a 2014 interview on Numberphile

1.1 Groups

Definition 1 (Binary Operation)**.** A binary operation $*$ on a set G is a function $* : G \times G \longrightarrow G$. For any $a, b \in G$, we will write $a * b$ for $*(a, b)$.

Example. Modular addition on $\mathbb{Z}/n\mathbb{Z}$, composition of symmetries of equilateral triangle.

Definition 2 (Group)**.** A group is an ordered pair $(G, *)$, where G is a set and $*$ is a binary operation on G satisfying the following axioms:

- **Associativity:** $(a * b) * c = a * (b * c)$; for all $a, b, c \in G$.
- **Identity:** There exists an element $e \in G$, called identity of G, such that for all $a \in G, a * e = e * a = a$.
- **Inverse:** For all $a \in G, a \neq e$, there exists $b \in G$ such that $a * b = b * a = e$. We call b is the inverse of a and write $b = a^{-1}$.

Example. $(\mathbb{Q}, +), (\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{Q} \setminus 0, \times)$.

Definition 3. A group G is called *abelian* (Or *commutative*) if $a * b = b * a$, for all $a, b \in G$. Otherwise, it is called *non-abelian* (Or *non-commutative*).

Example.

- $(R, +)$ is an abelian group.
- Group of the symmetries of an equilateral triangle is a non-abelian group.

Informally, we say G is a group under $*$ if $(G, *)$ is a group, or just G is a group when the operation $*$ is clear from the context.

Example. Consider $G = \{x \in \mathbb{R} : 0 \leq x < 1\}$.
For all $x, y \in G$ define $*$ via -

- $x * y = x + y - [x + y]$.

- $x + y \pmod 1$.

Prove that $(G, *)$ is an abelian group.

Proof. For all $x, y \in G$,

$$0 \leq x + y \pmod 1 < 1 \Rightarrow 0 \leq x * y < 1 \textbf{(Closure)}.$$

For all $x, y, z \in G$,

$$\begin{aligned}(x * y) * z &= (x + y \pmod 1) * z \\ &= (x + y \pmod 1) + z \pmod 1 \\ &= (x + y) + z \pmod 1 \\ &= x + (y + z) \pmod 1 \\ &= x + (y + z \pmod 1) \pmod 1 \\ &= x * (y + z \pmod 1) \\ &= x * (y * z) \textbf{ (Associativity)}.\end{aligned}$$

For all $x \in G$,

$$x * 0 = x + 0 \pmod 1 = x.$$

Similarly, $0 * x = x$ **(Identity)**.

For all $x \neq 0 \in G, (1 - x) \in G$ and

$$x * (1 - x) = x + 1 - x \bmod 1 = 1 \bmod 1 = 0 \ \&$$

$$(1 - x) * x = 1 - x + x \bmod 1 = 1 \bmod 1 = 0$$

And for $0 \in G, 0 * 0 = 0 + 0 \pmod 1 = 0$ **(Inverse)**
For all $x, y \in G$

$$\begin{aligned}x * y &= x + y \pmod 1 \\ &= y + x \pmod 1 \\ &= y * x\end{aligned}$$

Hence, G is an Abelian group.

1.2 Matrix Groups

Example. $GL_n(R) = \{x \in \mathbb{R}^{n \times n} : x \text{ is invertible}\}$ under matrix multiplication forms a group.

Proof. For all $A, B \in GL_n(R), AB$ is an $n \times n$ matrix. If A and B is invertible, $(AB)^{-1} = B^{-1}A^{-1} \in GL_n(R)$ **(Closure)**.
Matrix multiplication is associative **(Associativity)**.
Identity matrix $I_n \in GL_n(R)$ since it is invertible **(Identity)**.
Inverse exists by defintion **(Inverse)**.

Example. $SL_n(R) = \{x \in \mathbb{R}^{n \times n} : det(x) = 1\}$ under matrix multiplication forms a group.

Proof. For all $A, B \in GL_n(R), AB$ is an $n \times n$ matrix. If $\det(A) = \det(B) = 1$, then

$\det(AB) = \det(A) \times \det(B) = 1 \times 1 = 1$ **(Closure)**.
Matrix multiplication is associative **(Associativity)**.
Identity matrix $I_n \in GL_n(R)$ since $\det(I_n) = 1$.
For all $A \in GL_n(R)$, inverse exists as $\det(A) \neq 0$ and $\det(A^{-1}) = \frac{1}{\det(A)} = 1$ **(Inverse)**

Lecture 2

30 Oct 2024

2.1 Group Propositions

Proposition 1. If $(G, *)$ is a group, then

1. The identitiy e is unique.
2. For all $a \in G, a^{-1}$ is unique.
3. For all $a \in G, (a^{-1})^{-1} = a$.
4. For all $a, b \in G, (a * b)^{-1} = b^{-1}a^{-1}$.
5. For all $a_1, a_2, ...a_n \in G$, the value of $a_1 * a_2 * ... * a_n$ is independent of how the expression is bracketed **(Generalized associative law)**.

Proof. 1. If there were two distinct identity say e' and e'', then for all $a \in G$,

$$a * e' = e' * a = a$$

also

$$\begin{gathered} a * e'' = e'' * a = a \\ \Rightarrow a * e'' = a * e' \\ \Rightarrow a^{-1} * a * e'' = a^{-1} * a * e' \\ \Rightarrow e'' = e' \text{ (Contradiction!)} \end{gathered}$$

Hence, indentity is unique.
2. Let for all $a \in G$, there exists two distinct inverse b, c,

$$a * b = b * a = e$$

also

$$a * c = c * a = e$$

Now, $b = b * e = b * (a * c) = (b * a) * c = e * c = c$ (Contradiction!)
Hence, inverse is unique for each element of a group.
3. According to the defintion, $a * a^{-1} = a^{-1} * a = e$. By mentally interchanging the roles of a and a^{-1}, we can see that a satisfies the defining property for the inverse of a^{-1}, hence, $(a^{-1})^{-1} = a$.
4. $(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$.
Since, G is a group, only inverse can have such property. Hence, $(a * b)^{-1} = b^{-1} * a^{-1}$.
5. **Left as exercise**.

Lemma 1 (Cancellation Lemma). For all a, u, w

- $a * u = a * w \Rightarrow u = w$
- $u * a = w * a \Rightarrow u = w$

2.2 Subgroups

Definition 4 (Subgroup). A subset of H of G is a subgroup if H is non-empty and is closed under products and inverses. We write $H \leq G$.

Example. $(\mathbb{Z}, +) \leq (Q, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.
For an equilateral triangle, the group of rotational symmetries is a subgroup of the group of all symmetries (rotaion and reflection).

Any group G has at least two subgroups: trivial group $\{e\}$ and the group itself (aka. improper subgroup).
When we say that H is a subgroup of G we shall always mean that the operation for the group H is the operation on G restricted to H. In general, it is possible that the subset H has the structure of a group with respect to some operation other than the operation on G restricted to H.

Example. $\mathbb{Q} \setminus 0$ under multiplication is not a subgroup of $\mathbb{R}$ under addition even though both are groups and $\mathbb{Q} \setminus 0$ is indeed a subset of $\mathbb{R}$.

Lemma 2 (The Subgroup Criterion). $H \leq G$ is a subgroup if and only if $H \neq \varnothing$ and for all $x, y \in H, xy^{-1} \in H$.

Proof. The forward direction is trivial.
For backward direction,
Since, $H \neq \varnothing$, there exists $x, x \in H$, which means $xx^{-1} = e \in H$ **(Identity)**.
For all $x \in H, ex^{-1} = x^{-1} \in H$ **(Inverse)**.
Associativity holds inherently **(Associativity)**.
For all $x, y \in H, y^{-1} \in H$, and so is $x(y^{-1})^{-1} = xy \in H$ **(Closure)**.

Lemma 3. If H is a nonempty finite subset of of a group G and H is closed under multiplication, then H is a subgroup of G.

Proof. Here, we just have to prove **inverse** property. Suppose $a \in H$. Since is H is closed under multiplication, the infinte collection of elements $a, a^2, a^3, ..., a^m, ...$ must all fit into H, which is a finite subset of G. Thus there must be repetations in this collection of elements; that is, for some integers r, s with $r > s > 0, a^r = a^s \Rightarrow a^{r-s} = e$. Since, $r - s - 1 \geq 0, a^{r-s-1} \in H$ and since $aa^{r-s-1} = a^{r-s} = e, a^{-1} = a^{r-s-1}$. Thus, $a^{-1} \in H$, completes the proof of the lemma.

Lecture 3

04 Nov 2024

3.1 Order of Group and its elements

Order of a group G, denoted as $|G|$ is the number of its element. If $|G|$ is a finite, then G is finite group; otherwise it is infinte group which has infinte order. $(R, +)$ has infinte order; whereas symmetries of a triangle , $\mathbb{Z}/n\mathbb{Z}$ or $(\mathbb{Z}/n\mathbb{Z})^\times$ has finite order.

> **Note.** $\mathbb{Z}/n\mathbb{Z}$ is a group under addition and $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group under multiplication, consists of the elements of $\mathbb{Z}/n\mathbb{Z}$ that do have multiplicative inverse. Former is called **additive group** and the latter is called **multiplicative group**.

Example. $|(\mathbb{Z}/n\mathbb{Z})^\times| = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\} = \varphi(n)$.
The function is called **Euler's totient function**.

> **Definition 5.** For a group G and $x \in G$, the *order* of x is the smallest positive integer n such that $x^n = e$, and is denoted by $|x|$. In this case, x is said to be order of n. If no positive power x is the identity, the order of x is defined to be infinity and x is said to be of infinite order.

Example. $\mathbb{Z}/n\mathbb{Z}$ has order 6. Elements of $\mathbb{Z}/n\mathbb{Z}$ has following orders: $|\overline{0}| = 1, |\overline{1}| = 6, |\overline{2}| = 3, |\overline{3}| = 2, |\overline{4}| = 3, |\overline{5}| = 6$. Notice, order of any element is less than or equals to the order of the group.

Example. In additive groups $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$, every nonzero element has infinte order. whereas, in the multiplicative groups $\mathbb{R}^\times$ or $\mathbb{Q}^\times$ the element -1 has order 2 and all other nonidentity elements have infinite order.

Example. In the group $GL_n(R)$, order of $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ is 2 because $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

3.2 Cyclic Groups

> **Definition 6.** A group H is cyclic if H can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n : n \in \mathbb{Z}\}$ (where as usual the operation is multiplication).

In additive notion H is cyclic if $H = \{nx : n \in \mathbb{Z}\}$. In both cases we will write $H = \langle x \rangle$ and say H is generated by x.

Example (A cyclic group may have more than one generator).

- $\mathbb{Z}/p\mathbb{Z} = \langle \overline{1} \rangle = ... = \langle \overline{p-1} \rangle$
- $(\mathbb{Z}, +) = \langle \overline{-1} \rangle = \langle \overline{1} \rangle$
- $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle = \langle \overline{2} \rangle$

Example. The 6th complex roots of unity form a cyclic group under multiplication. Here, z is a generator, but z^2 is not, because its power fail to produce the odd powers of z.

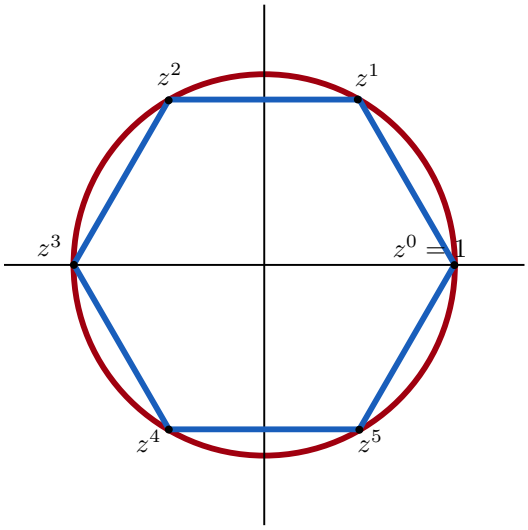


Figure 3.1: The 6th complex roots of unity form a cylic group under multiplication

3.3 Centralizers and Normalizers

Definition 7 (Centralizer). The *centralizer* of a subset A of group G is the set $C_G(A) = \{g \in G : gag^{-1} = a \text{ for all } a \in A\}$. Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements of G which commute with every element of A.

We show $C_G(A)$ is a subgroup of G. First of all, $C_G(A) \neq \emptyset$ as $e \in C_G(A)$ because the identity commutes with every element of G, in particular for all $a \in A$.
Let $x, y \in C_G(A)$, that is, for all $a \in A$

$$xax^{-1} = a \text{ and } yay^{-1} = a.$$

We have to prove xy^{-1} also exits in $C_G(A)$.

$$\begin{aligned}(xy^{-1})a(xy^{-1})^{-1} &= (xy^{-1})a(yx^{-}1) \\ &= x(yay^{-1})x^{-1} \\ &= xax^{-1} \\ &= a\end{aligned}$$

In special case when $A = a$ we will write simply $C_G(a)$ instead of $C_G(a)$. In this case $a^n \in C_G(a)$ for all $n \in \mathbb{Z}$.
To be continued...

Lecture 4

06 Nov 2024

Note. $x, y \in C_G(A)$ does not necessarily mean $xy = yx$.

Definition 8 (Center). Define $Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}$, the set of elements commuting with all the elements of G. This subset of G is called the *center* of G.

Note. $Z(G) = C_G(G)$, so the argument above proves $Z(G) \leq G$ as a special case.

Definition 9 (Normalizer). Let $gAg^{-1} := \{gag^{-1} : a \in A\}$. The *normalizer* of $A \in G$ is the set $N_g(A) = \{g \in G : gAg^{-1} = A\}$.

$N_G(A)$ is a subgroup of G (follows from the same steps which demonstrated that $C_G(A) \leq G$ with appropriate modifications).

4.1 Cayley's Table

To be written...

Lecture 5

11 Nov 2024

5.1 Congruence Modulo Subgroup H

Definition 10. Let G be a group, H a subgroup of G; for $a, b \in G$ we say a *is congruent to* $b \pmod{H}$, written as $a \equiv b \bmod H$ if $ab^{-1} \in H$.

Lemma 4. The relation $a \equiv b \pmod{H}$ is an equivalence relation.

Proof. 1. Since H is a subgroup, for all $a \in H, aa^{-1} = e \in H$. Hence, $a \equiv a \pmod{H}$ **(reflexivity)**.
2. Let $a \equiv b \pmod{H}$, equivalently, $ab^{-1} \in H$. So, $(ab^{-1})^{-1} \in H$. But $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}$. Hence, $ba^{-1} \in H$ equivalently, $b \equiv a \pmod{H}$ **(symmetry)**.
3. Let $a \equiv b \pmod{H}$ and $b \equiv c \pmod{H}$, which are equivalent to $ab^{-1} \in H$ and $bc^{-1} \in H$ respectively. But together they imply $(ab^{-1})(bc^{-1}) \in H$. $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$. From which it follows $a \equiv c \pmod{H}$. **(Transitivity)**.
Hence, $a \equiv b \pmod{H}$ is an equivalence relation.

Remark. The $a \equiv b \pmod{H}$ is a generalization of the "mod" we see in integers. Recall that $(\mathbb{Z}, +)$ is a group. So ab^{-1} is the generalization of $a - b = a + (-b)$. Now, $a \equiv b \pmod{n}$ means $n \mid a - b$. This can be interpreted as $a - b \in n\mathbb{Z}$, where $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. Observe that all subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$. So to generalize this for any group G and any subgroup H, we interpret $a \equiv b \pmod{H}$ as $ab^{-1} \in H$.

5.2 Cosets

Definition 11 (Cosets). If H is a subgroup of $G, a \in G$, then $Ha = \{ha : h \in H\}$. Ha is called a right coset of H in G. Similarly, $aH = \{ah : h \in H\}$ is a left coset in G.

Is Ha a subgroup of G? Not in general. Let $a \notin Ha$. Then identity $e \notin H$. Because otherwise $e * a = a \in Ha$ (contradiction).

Lemma 5. For all $a \in G$, $Ha = \{x \in G : a \equiv x \pmod{H}\}$.

Proof. Let $[a] = \{x \in G : a \equiv x \pmod{H}\}$
For all $c \in Ha \Rightarrow c = h_1 a$ (for some $h_1 \in H$). $a(h_1 a)^{-1} = aa^{-1}h_1^{-1} = h_1^{-1} \in H$ from which it follows $h_1 a = c \in [a]$. Hence, $Ha \subseteq [a]$.
Conversely, for all $x \in [a], ax^{-1} \in H \Rightarrow (ax^{-1})^{-1} = xa^{-1} \in H$. Therefore, $(xa^{-1})a = x \in Ha$. Hence, $[a] \subseteq Ha$.
Therefore, $Ha = [a] = \{x \in G : a \equiv x \pmod{H}\}$.

Equivalence classes yield a decomposition of G into disjoint subsets. Thus, *any two right cosets of H in G either are identical or have no element in common.*

Lemma 6. There is a one-to-one correspondence between any two right cosets of H in G.

Proof. Let $f : Ha \to Hb$ be a map where $f(ha) = hb$. Trivially, f is a bijective map.

$|H| = |He| = |Hx|$ for all $x \in G$.
All right cosets / left cosets have the same cardinality.
Since any $a \in G$ is in a unique right coset Ha, the right cosets fill out G. Thus if k represents the number of distinct right cosets of H in G we must have that $k|H| = |G|$. Which proves the famous *Lagrange's Theorem*, namely,

Theorem 1 (Lagrange's Theorem)**.** If G is a finite group and H is a subgroup of G, then order of H is a divisor of order of G.

Definition 12 (Index of H in G)**.** If $H \leq G$ then the index of H in G is the number of distinct right cosets of H in G. We denote it by $[G : H]$.

Notice,

$$[G : H] = \frac{|G|}{|H|}.$$

And if $K < H < G$, then

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

Lecture 6

13 Nov 2024

6.1 Dihedral Groups

Consider the set of all symmetries of a regular n-gon. They form a group under composition of transformations. We call this a *Dihedral Group*. Denoted as D_n (or D_{2n} in some texts). Notice D_n has $2n$ elements. Let's level n vertices from 1 to n. Then for 1 we have n choices. For 2 we have 2 choices since vertex 2 is adjacent to vertex 1. And since symmetries are rigid motions, once we specify vertex 1 and 2, positions of the remaining vertices are determined automatically. Hence,

$$|D_n| = 2n.$$

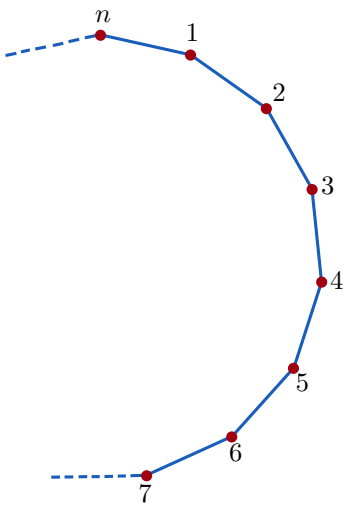


Figure 6.1: A regular n-gon

Now, for D_3 or D_4 we can explicitely exhibit all the symmtries and do computations, but for higher n it becomes complicated. Therefore, viewing D_n as an abstract group is convenient. Label a regular n-gon consecutively from 1 to n clockwise. Let r be the rotation anti-clockwise about the origin by $\frac{2\pi}{n}$ radian. Let s be the reflection about the line of symmetry through vertex 1 and the origin. Then, the following properties are true:

1. $1, r, r^2, \ldots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$.
2. $s^2 = 2$.
3. $r^i s$ has to be a reflection, that is, $r^i s \neq r^j$ for any i and j.
4. $sr^i \neq sr^j$, for all $0 \leq i, j \leq n-1$ with $i \neq j$, so

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

   i.e., each element can be written *uniquely* in the form sr^i for some $k = 0$ or 1 and $0 \leq i \leq n-1$.
5. $rs = sr^{-1}$. Because

   $$(rs)^2 = e \Rightarrow rs \cdot rs = e \Rightarrow rs = s^{-1}r^{-1} \Rightarrow rs = sr^{-1}.$$

6. By induction, $r^i s = sr^{-i}$, for all $0 \leq i < n$.

Using **(1)**, **(2)**, **(3)**, we can compute any finite number of produts of D_n and represent it in the form sr^i, where $k = 0$ or 1 and $0 \leq i \leq n-1$. For example, if $n = 12$,

Example. $(sr^9)(sr^6) = s(r^9 s)r^6 = s(sr^{-9})r^6 = s^2 r^{-9+6} = r^{-3} = r^9$.

Notice, the set $\{1, r, r^2, \ldots, r^{n-1}\}$ is an abelian subgroup of D_n.

6.2 Generators, Relations & Presentation of a Group

All the elements of D_n is generated by r, s. We call them generators of D_n. r, s satisfy some equations which are called relations. In general, if some group G is generated by some $S \subseteq G$ and there is some collection of relations, say $R_1, R_2, ..., R_m$ (R_i is an equation in the elements from $S \cup \{1\}$) such that any relation among the elements of S can be deduced from these, we shall call these generators and relations a *presentation* of G and write

$$G = \langle S | R_1, R_2, ..., R_m \rangle.$$

One presentation for the dihedral group D_n is

$$D_n = \langle r, s | r^n = s^2 = e, rs = sr^{-1} \rangle.$$

If G is a finite group then, for $x, y \in G$, $\langle x, y \rangle$ is the set of any possible combination of products of x, y. $\langle x, y \rangle$ forms a subgroup of G. We call it *free group* generated by x, y.

Lecture 7

18 Nov 2024

7.1 Symmetric Groups, Cycle & Cycle Structure

Definition 13. Let Ω be any nonempty set and let S_Ω be the set of all bijections from Ω to itself. Then S_Ω forms a group under function composition: $\circ$. $(S, \circ)$ is called *symmetric group* on the set Ω.

When $\Omega = \{1, 2, ..., n\}$, we write it as S_n.

Example. Let $\Omega = \{a, b\}$.

$$S_\Omega = \left\{ \begin{array}{cc} a & b \\ \downarrow & \downarrow \\ a & b \end{array} \quad , \quad \begin{array}{cc} a & b \\ \searrow\!\swarrow & \\ a & b \end{array} \right\}$$

$|S_\Omega| = 2$.

Example. If $\Omega = \{a, b, c\}$, $|S_\Omega| = 6$.

Order of S_n is $n!$. Let $\sigma \in S_n$, then
$\sigma(1)$ has n choices to send 1 to any n element.
$\sigma(2)$ has $(n-1)$ choices.
$\sigma(3)$ has $(n-2)$ choices.
.
.
.
$\sigma(n)$ has (1) choices.
Hence, there is precisely $n(n-1)(n-2)\cdots 2 \cdot 1 = n!$ bijections from n to itself.

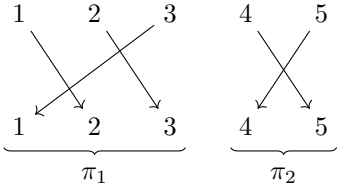
Definition 14. A *cycle* is a string of integers which represents the element of S_n which cyclically permutes these integers (and fixes all other integers).

Let

$$\sigma = \begin{pmatrix} 1 & \to & 2 \\ 2 & \to & 3 \\ 3 & \to & 1 \end{pmatrix} \in S_3.$$

$\sigma^3 = e$. σ is called cycle of length $|\sigma| = 3$ generated by σ.

Again, let $\sigma \in S_5$ and σ acts as follows:



$\sigma = \pi_1 \circ \pi_2$, where π_1 has the cycle structure $(3+1+1)$ and π_2 has the cycle structure $(2+1+1+1)$.
Two cycles are called *disjoint* if they have no elements in common. π_1, π_2 are examples of disjoint cycles. Notice, *two dijoint cycles commutes* as we can see they do not interact with

each other.

Theorem 2. Every elements in S_n can be written as composition of disjoint cycles.

Lecture 8

20 Nov 2024

8.1 Cycle Notation

Cycle Notation: The cycle which sends a_i to $a_{i+1}, 1 \leq i \leq m-1$ and sends a_m to a_1 is written as $(a_1, a_2 ... a_m)$.

Example (Cycle Decomposition Algorithm)**.** Let $n = 13$ and let $\sigma \in S_{13}$ be defined by

$$\sigma(1) = 12, \quad \sigma(2) = 13, \quad \sigma(3) = 3, \quad \sigma(4) = 1, \quad \sigma(5) = 11,$$
$$\sigma(6) = 9, \quad \sigma(7) = 5, \quad \sigma(8) = 10, \quad \sigma(9) = 6, \quad \sigma(10) = 4,$$
$$\sigma(11) = 7, \quad \sigma(12) = 8, \quad \sigma(13) = 2.$$

Method	**Example**
To start a new cycle, pick the smallest element of $\{1, 2, \ldots, n\}$ which has not yet appeared in a previous cycle — call it a (if you are just starting, $a = 1$); begin the new cycle: $(a$	(1
Read off $\sigma(a)$ from the given description of σ — call it b. If $b = a$, close the cycle with a right parenthesis (without writing b down); this completes a cycle — return to step 1. If $b \neq a$, write b next to a in this cycle: $(a\ b$	$\sigma(1) = 12 = b, 12 \neq 1$ so write: (1 12
Read off $\sigma(b)$ from the given description of σ — call it c. If $c = a$, close the cycle with a right parenthesis to complete the cycle — return to step 1. If $c \neq a$, write c next to b in this cycle: $(a\ b\ c$. Repeat this step using the number c as the new value for b until the cycle closes.	$\sigma(12) = 8,\ 8 \neq 1$ so cycle runs: (1 12 8
Naturally, this process stops when all the numbers from $\{1, 2, \ldots, n\}$ have appeared in some cycle.	$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(3)(5\ 11\ 7)(6\ 9)$
Final Step: Remove all cycles of length 1	$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$

Example (Computing Products in S_n)**.** While computing products in S_n one reads the permutations from *right to left.* Let's compute $(1\ 2\ 3) \circ (1\ 2)(3\ 4)$.

Reading off permutations	Computing product
$1 \to 2 \to 3$	(1 3
$3 \to 4$	(1 3 4
$4 \to 1$	(1 3 4)

Hence, $(1\ 2\ 3) \circ (1\ 2)(3\ 4) = (1\ 3\ 4)$.

S_n is non-abelian group for all $n \geq 3$.

8.2 Cyclic Permutation, Transposition & Alternating Group

Definition 15 (Cyclic Permutation)**.** $\pi \in S_\Omega$ has a cycle of length r, and all other cycles are of length 1, then, π is a *cyclic permutation.*

Definition 16 (Transposition)**.** A cyclic permutation of length 2 is called a *transposition.*

Proposition 2. Any r cycle can be decomposed into a product of $(r-1)$ transpositions.

Example. Let $\tau = (1\ 3\ 4\ 6\ 7\ 9) \in S_9$
Method 1: $\tau = (1\ 3\ 4\ 6\ 7\ 9) = (1\ 9)(1\ 7)(1\ 6)(1\ 4)(1\ 3)$
Method 2: $\tau = (1\ 3\ 4\ 6\ 7\ 9) = (1\ 3)(3\ 4)(4\ 6)(6\ 7)(7\ 9)$
Both products of transpositions method 1 or method 2 represent the same permutation τ. Note that the order of the disjoint cycle τ is τ but in both expressions of τ as the product of transpositions, τ has 5 (odd numnber of) permutations. Hence τ is an *odd permutation.* Similarly, if a permutation is the product of an even number of transpositions, it is called *even permutation.*

Definition 17 (Alternating Group)**.** Let A_n be the subset of S_n consisting of all even permutations. Since product of two even permutations is even, A_n is a subgroup of S_n. A_n is called the *alternating group* of degree n.

Lecture 9

2 Dec 2024

9.1 Normal Subgroup

Definition 18 (Normal Subgroup). Let G be a group. A subgroup N of G is a normal subgroup if $gN = Ng$, for all $g \in G$. Equivalently, a subgroup N is normal in the group G if $gNg^{-1} = N$, for all $g \in G$. We denote $N \lhd G$.

Example. A_3 is normal in S_3. Because, A_3 has index 2 in S_3, meaning A_3 has exactly two cosets: A_3 and its complement in S_3. Hence, left and right cosets coincide.

In general, A_n is normal in S_n. Furthermore, a subgroup of index 2 is always normal because the left and right cosets coincide.

Example (Trivial Examples). $\{e\} \in G$ and the group G itself is normal in G.

Example (Center of G). Center of the group G is a normal subgroup.

Remark. Is every abelian subgroup normal? No.
Counter example: $\{e, s\} \in D_3$ is abelian subgroup. But not normal, since, for instance, $r\{e, s\} \neq \{e, s\}r$.

9.2 Quotient Group

Theorem 3. Let $N \lhd G$. If $g_1N = g_1'N$ and $g_2N = g_2'N$, then $g_1g_2N = g_1'g_2'N$.

Proof. Let $x \in g_1g_2N$, then $x = g_1g_2n$, for some $n \in N$. Since, $g_2N = g_2'N = Ng_2'$, $g_2n = g_2'n_1 = n_2g_2'$ for some $n_1, n_2 \in N$. So, $x = g_1g_2'n_1 = g_1n_2g_2'$. $g_1n_2 = g_1'n_3$, for some $n_3 \in N$. Hence, $x = g_1'n_3g_2' = g_1'g_2'n'$, for some $n' \in N$. Hence, $x \in g_1'g_2'N$, which implies $g_1g_2N \subseteq g_1'g_2'N$.
Using similar argument, $g_1'g_2'N \subseteq g_1g_2N$. Hence, $g_1g_2N = g_1'g_2'N$. □

Cosets of a subgroup N in a group G naturally partition G. However, not all subgroups allow these cosets to have a meaningful group structure. When N is a normal subgroup ($gN = Ng$ for all $g \in G$), we can define an operation on cosets that mimics the group operation in G. Specifically:

$$(gN) \cdot (hN) = (gh)N.$$

This operation is well-defined only if N is normal, ensuring that the choice of representatives g and h does not affect the result as the previous theorem asserts.

Definition 19 (Coset Multiplication). Let $N \lhd G$. Then define a multiplication $\cdot$ on two cosets of N via-

$$g_1N \cdot g_2N := g_1g_2N$$

Theorem 4 (Quotient Group). Under the multiplication operation above, the set of all cosets of the normal subgroup N forms a group, called the *quotient group of G modulo N*

and denoted as G/N.

Proof. To show that G/N forms a group under coset multiplication, we verify the group axioms: closure, associativity, identity, and inverses.

1. **Closure:** Let $g_1N, g_2N \in G/N$. Then their product is defined as:

$$(g_1N)(g_2N) = g_1g_2N.$$

   Since $g_1g_2 \in G$, it follows that $g_1g_2N \in G/N$. Thus, G/N is closed under this operation.

2. **Associativity:** Let $g_1N, g_2N, g_3N \in G/N$. Then:

$$\big((g_1N)(g_2N)\big)(g_3N) = (g_1g_2N)(g_3N) = (g_1g_2g_3)N.$$

   Similarly:

$$(g_1N)\big((g_2N)(g_3N)\big) = (g_1N)(g_2g_3N) = (g_1g_2g_3)N.$$

   Therefore, coset multiplication is associative.

3. **Identity:** The coset eN, where e is the identity element of G, acts as the identity in G/N. For any $gN \in G/N$:

$$(eN)(gN) = egN = gN, \quad \text{and} \quad (gN)(eN) = geN = gN.$$

   Thus, eN is the identity element in G/N.

4. **Inverses:** For any $gN \in G/N$, the coset $g^{-1}N$ serves as its inverse. We verify:

$$(gN)(g^{-1}N) = g(g^{-1})N = eN, \quad \text{and} \quad (g^{-1}N)(gN) = g^{-1}gN = eN.$$

   Hence, every element in G/N has an inverse.

Since G/N satisfies the group axioms, it forms a group under the given multiplication operation. □

Lecture 10

4 Dec 2024

If G is a finite group and N is normal subgroup of G, then

$$|G/N| = [G : N] = \frac{|G|}{|N|}$$

Example. Let $N = \{e\}$, then $G/N \cong G$. Again if $N = G$, then $G/N \cong \{e\}$.
Note: We will learn what $\cong$ means shortly.

Example. Let $G = (\mathbb{Z}, +)$. Then $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ is normal in $\mathbb{Z}$. Because for all $g \in \mathbb{Z}, g + n\mathbb{Z} + (-g) = n\mathbb{Z}$. Now, let $N = n\mathbb{Z}$. Then distinct cosets of $n\mathbb{Z}$ are:

$$\begin{aligned}\overline{0} &= 0 + n\mathbb{Z}\\ \overline{1} &= 1 + n\mathbb{Z}\\ &\vdots\\ \overline{n-1} &= (n-1) + n\mathbb{Z}\end{aligned}$$

We denote the quotient group as $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$. Notice, from the definition, coset multiplication here is: $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = a + b + n\mathbb{Z}$ which is exactly how we initially defined the operation on $\mathbb{Z}/n\mathbb{Z}$, i.e., $\overline{a} + \overline{b} = \overline{a + b}$.

Example. $G = \mathbb{R}$ and $N = 2\pi\mathbb{Z}$. Then, $G/N = \{\theta + 2\pi\mathbb{Z} : 0 \leq \theta < 2\pi\}$. And multiplication would be like $(\theta_1 + 2\pi\mathbb{Z}) + (\theta_2 + 2\pi\mathbb{Z}) = (\theta_1 + \theta_2 + 2\pi\mathbb{Z})$.

Example. We know A_n is a normal subgroup of S_n. And since index of A_n in S_n is 2, A_n has two cosets: $eA_n, (1\ 2)A_n$. Cayley table for the quotient group modulo A_n is:

$\cdot$	eA_n	$(1\ 2)A_n$
eA_n	eA_n	$(1\ 2)A_n$
$(1\ 2)A_n$	$(1\ 2)A_n$	eA_n

10.1 Group Homomorphism

Group homomorphism between two groups is aptly called *structure preserving* map as it respect their algebraic structure.

Definition 20 (Group Homomorphism). Given two groups, $(G, *)$ and $(H, \cdot)$, a *group homomorphism* is a map $f : G \to H$ such that for all $g_1, g_2 \in G$,

$$f(g_1 * g_2) = f(g_1) \cdot f(g_2).$$

Definition 21 (Isomorphism). A group homomorphism that is bijective is called *isomorphism*.

When two groups are isomorphic (there's an isomorphism between those groups), they are essentially the same. They differ in that their elements are labeled differently. The isomorphism

gives us the key to the labeling, and with it, knowing a given computation in one group, we can carry out the analogous computation in the other. If two groups G, H are isomorphic, we write $G \cong H$.

Proposition 3. If $f : G \to H$ is a homomorphism, then:

1. $f(e_G) = e_H$;
2. $f(x^{-1}) = f(x)^{-1}$, for all $x \in G$.

Proof. To prove (1) we calculate,

$$\begin{aligned} & f(e_G * e_G) = f(e_G) \cdot f(e_G) \\ \Rightarrow\ & f(e_G) = f(e_G) \cdot f(e_G) \\ \Rightarrow\ & f(e_G) \cdot f(e_G)^{-1} = f(e_G) \cdot f(e_G) \cdot f(e_G)^{-1} \\ \Rightarrow\ & e_H = f(e_G) \end{aligned}$$

To prove (2),

$$\begin{aligned} & f(xx^{-1}) = f(e_G) = e_H \\ \Rightarrow & f(x)f(x^{-1}) = e_H \\ \Rightarrow & f(x^{-1}) = f(x)^{-1} \end{aligned}$$

Example. $f : G \to \{e\}$ is homomorphism.

Proof. For all $g_1, g_2 \in G$,

$$f(g_1 g_2) = e.$$

Then,

$$f(g_1) \cdot f(g_2) = e \cdot e = e.$$

Example. Let $G = (R, +), H = (R^\times, \times)$.
Define $f : G \to H$ such that $f(x) = e^x$. f is a homomorphism, but not isomorphism.

Proof. For all $x, y \in \mathbb{R}$,

$$\begin{aligned} f(x + y) &= e^{x+y} \\ &= e^x \times x^y \\ &= f(x) \times f(y). \end{aligned}$$

The map is not isomorphism because it is not surjective, e.g., there's no $x \in G$ such that $f(x) = -1 \in H$.

Lecture 11

9 Dec 2024

11.1 Kernel and Image of Group Homomorphism

Let G and H be groups and let f be a group Homomorphism from G to H (Next few lectures will be assuming this statement). Then,

Definition 22 (Kernel). If e_H is the identity element of H, then we define *kernel* of f is the preimage of the singleton set $\{e_H\}$. In symbols:

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

and

Definition 23 (Image). We define *image* of f to be all elements of H which are image of some element of G.

$$\text{Im } f := f(G) = \{h \in H : f(g) = h; \text{ for some } g \in G\}$$

Lemma 7. $\ker f$ and $\text{Im } f$ are subgroups of G and H respectively.

Proof. $f(e_G) = e_H$, hence $e_G \in \ker f$.
Let $x, y \in \ker f$. Then, $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e_H e_H^{-1} = e_H$. According to subgroup criterion, $\ker f$ is a subgroup of G.
We will prove second part shortly.

Lemma 8. $\ker f$ is a normal subgroup of G.

Proof. For all $x \in \ker f$.

$$\begin{aligned} f(gxg^{-1}) &= f(g)f(x)f(g^{-1}) \\ &= f(g)e_H f(g)^{-1} \\ &= f(g)f(g)^{-1} \\ &= e_H. \end{aligned}$$

Lemma 9. f is injective if and only if $\ker f = \{e_G\}$.

Proof. ($\Rightarrow$)
If f is injective, then, image of every elements of G is unique. Hence, $f(x) = e_H$ if and only if $x = e_G$. Hence, $\ker f = \{e_G\}$.
($\Leftarrow$)
Assume

$$\begin{aligned} & f(x) = f(y) \\ \Rightarrow & f(x)f(y)^{-1} = e_H \\ \Rightarrow & f(x)f(y^{-1}) = e_H \\ \Rightarrow & f(xy^{-1}) = e_H \end{aligned}$$

Since, ker $f = \{e_G\}$, it must be that $xy^{-1} = e_H$ which implies $x = y$.
Hence, f is injective.

Lemma 10. Let $N \lhd G$, then the canonical map $\pi_N : G \to G/N$ such that $\pi_N(a) = aN$ is a surjective homomorphism with ker $\pi_N = N$.

Proof. The map π_N is well-defined because for any $a \in G$, the coset aN is uniquely determined. There is no ambiguity in assigning $\pi_N(a) = aN$.
Let $a, b \in G$. Since N is normal in G, then $\pi_N(ab) = abN = aNbN = \pi_N(a)\pi_N(b)$. Hence, π_N is a homomorphism.
Lastly, identity of G/N is N. We know $nN = N$ iff $n \in N$. Hence, ker $f = N$.

Corollary. A subgroup N is normal if and only if it is the kernel of a group homomorphism.

Lecture 12

11 Dec 2024

Proposition 4. If $A \leq G$, then $f(A) \leq H$. In particular, Im $f = f(G) \leq H$.

Proof. $f(A)$ is non-empty since $e_H \in f(A)$.
Let $x, y \in f(A)$, then $x = f(a_1), y = f(a_2)$, for $a_1, a_2 \in A$.
We know $a_1 a_2^{-1} \in A$, therefore, $f(a_1 a_2^{-1}) \in f(A)$.
Now, $xy^{-1} = f(a_1)f(a_2)^{-1} = f(a_1)f(a_2^{-1}) = f(a_1 a_2^{-1}) \in f(A)$.
According to subgroup criterion, $f(A) \leq H$.

Proposition 5. Let $f^{-1}(B) = \{x \in G : f(x) \in B\}$. Then, if $B \leq H$, then $f^{-1}(B) \leq G$. Furthermore, if $B \lhd H$, then $f^{-1}(B) \lhd G$.

Proof. **Part 1**
We need to show that $f^{-1}(B)$ is a subgroup of G.
Firstly, $f^{-1}(B)$ is nonempty because $e_G \in f^{-1}(B)$.
Now, let $x, y \in f^{-1}(B)$. Then $f(x), f(y) \in B$. Since B is a subgroup of H, $f(y)^{-1} \in B$, so:

$$f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in B.$$

Thus, $xy^{-1} \in f^{-1}(B)$, showing that $f^{-1}(B) \leq G$.
Part 2
We need to show that for all $g \in G$ and $x \in f^{-1}(B)$, $gxg^{-1} \in f^{-1}(B)$. $x \in f^{-1}(B)$, so $f(x) \in B$. Let's show $f(gxg^{-1}) \in B$. We have:

$$f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)f(x)f(g)^{-1}.$$

Since $f(x) \in B$ and B is normal in H (i.e., B is invariant under conjugation), we have:

$$f(g)f(x)f(g)^{-1} = f(gxg^{-1}) \in B.$$

Thus, $f(gxg^{-1}) \in B$, which implies $gxg^{-1} \in f^{-1}(B)$.
Hence, $f^{-1}(B) \lhd G$.

12.1 Isomorphism Theorems

Emmy Noether (1882–1935) was one of most influential mathematicians of the 20th century known for her groundbreaking contributions in abstract algebra and theoretical physics. In 1927, she first introduced three isomorphism theorems (sometimes called Noether's isomorphism theorems) of group theory that generalize earlier ideas of abstract algebra. Noether's work exemplified abstraction and generalization. She moved mathematics away from computational techniques and concrete problems toward a more conceptual and unified framework. This approach is now a hallmark of pure mathematics.

Theorem 5 (First Isomorphism Theorem). Let $f : G \to H$ be a group homomorphism. Then, there exits an injective homomorphism $f' : G/\ker f \to H$ such that the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle \pi_{\ker f}}\downarrow & \nearrow_{f'} & \\ G/\ker f & & \end{array}$$

In particular, $G/\ker f \cong f(G)$.

Proof. Let $N = \ker f$.
$\pi_N : G \to G/N$.

Define f': Let $f' : G/N \to H$ such that $f'(aN) = f(a)$. The map is well-defined. Let $X \in G/N$. If $X = gN = g'N$, then $f'(X) = f'(gN) = f(g)$ and also $f'(X) = f'(g'N) = f(g')$. Since $gN = g'N$, it follows that $g = g'n$ for some $n \in N$. Using this, $f(g) = f(g'n) = f(g')f(n)$, and because $n \in \ker f$, we know $f(n) = e_H$. Therefore, $f(g) = f(g')$, so the map is well-defined.

f' is a **homomorphism:**

$$\begin{aligned} f'(aNbN) &= f'(abN) \\ &= f(ab) \\ &= f(a)f(b) \\ \Rightarrow f'(aNbN) &= f'(aN)f'(bN) \end{aligned}$$

f' is injective: By this lemma, we know f' is injective if and only if $\ker f' = \{e_{G/N}\} = \{N\}$. $f'(aN) = f(a) = e_H$ if and only if $a \in \ker f = N$.

$$\ker f' = \{aN : a \in N\} = \{N\} = \{e_{G/N}\}$$

Hence, f' is injective.

The Diagram Commutes: For all $g \in G, \pi_{\ker f}(g) = g\ker f$ and $f'(g\ker f) = f(g)$. Hence, $f = f' \circ \pi_{\ker f}$

$f'(G/\ker f) = f(G)$. f' is a homomorphism, f' is injective and f' is surjective onto it's image $f(G)$. Hence, f' is bijective map from $G/\ker f$ to $f(G)$. Hence, f' is an isomorphism from $G/\ker f$ to $f(G)$ which means f' is an isomorphism from $G/\ker f$ to $f(G)$. Hence, $G/\ker f \cong f(G)$.

□

Lecture 13

17 Dec 2024

Theorem 6 (Second Isomorphism Theorem)**.** Given a group G with a subgroup H and a normal subgroup N, $H/(H \cap N) \cong HN/N$.

Proof. It is easy to check $HN \leq G$, $N \lhd HN$ and $(H \cap N) \lhd H$. So we directly move on to proving the isomorphic part.
Define $\phi : H \to HN/N$ such that $\phi(h) = hN$. ϕ is homomorphism because for all $x, y \in H$,

$$\phi(xy) = xyN = xNyN = \phi(x)\phi(y).$$

Suppose $xN \in HN$, and $x = hn, h \in H, n \in N$. Hence, $xN = hnN = hN = \phi(h)$. Hence, $\text{im}\ \phi = \phi(H) = HN/N$.
Now, $\ker \phi = \{h \in H : \phi(h) = eN = N\}$. Note that $h \in \ker\phi \Rightarrow \phi(h) = N \Rightarrow hN = N \Rightarrow h \in N \Rightarrow h \in (H \cap N)$. Again, if $x \in (H \cap N) \Rightarrow x \in N \Rightarrow \phi(x) = N$. Hence, $\ker \phi = H \cap N$.
Using first isomorphism theorem, $H/(H \cap N) \cong HN/N$. □

Theorem 7 (Third Isomorphism Theorem)**.** Given a group G with normal subgroups N and H, such that $N \subseteq H, (G/N)/(H/N) \cong G/H$.

13.1 Automorphism

Definition 24 (Automorphism)**.** If $f : G \to G$ is an isomorphism, we call it an *automorphism*.

Example. $f : G \to G$ such that $f(g) = g$ is an automorphism.

Non-example. $f : G \to G$ such that $f(x) = x^{-1}$ is not an isomorphism.

Proof. Because f is not a homomorphism in the first place. For $g_1, g_2 \in G$, $f(g_1g_2) = (g_1g_2)^{-1} = g_2^{-1}g_1^{-1} = f(g_2)f(g_1)$ is not always equals to $f(g_1)f(g_2)$.

Example (Conjugation Action)**.** $\varphi : G \to G$ such that $\varphi(x) = gxg^{-1}$ is an automorphism.

Proof. Firstly, φ is a homomorphism.
For all $x, y \in G$,

$$\begin{aligned}\varphi(xy) &= gxyg^{-1} \\ &= gxg^{-1}gyg^{-1} \\ &= \varphi(x)\varphi(y)\end{aligned}$$

Then, it is easy to show that φ is injective and $|G| = |\operatorname{Im}\varphi|$ which proves φ is surjective too, hence, an automorphism.

Non-example. Define for $g \in G$, $\lambda_g : G \to G$ such that $\lambda_g(a) = ga$. λ_g is not an automorphism because it is not a homomorphism although it is a bijective map.

Lemma 11. λ_g in the previous example defines a permutation of G.

Proof. To prove injectivity, let,

$$\lambda_g(a) = \lambda_g(b) \Rightarrow ga = gb \Rightarrow a = b.$$

To prove surjectivity, for any $c \in G, c = gg^{-1}c = \lambda_g(g^{-1}c)$.
λ_g is bijective and every bijective map from a group to itself is a permutation.

Theorem 8 (Cayley's Theorem)**.** Every group is isomorphic to a group of permutations.

Proof. Define for $g \in G$, $\lambda_g : G \to G$ such that $\lambda_g(a) = ga$ and $\overline{G} = \{\lambda_g : g \in G\}$. We want to prove, $\overline{G}$ is a group under composition of permutations and $G \cong \overline{G}$. To prove $\overline{G}$ is a group,

$$\lambda_g \circ \lambda_h(a) = \lambda_g[ha] = gha = \lambda_{gh}(a) \textbf{ (Closure)}$$

Composition of maps is associative **(Associativity)**.
Inverse and **identity** are $\lambda_{g^{-1}}$ and λ_e respectively for all $g \in G$.
Now, we will define a bijection φ. Let $\varphi : G \to \overline{G}$ such that $\varphi(g) = \lambda_g$.
φ is a homomorphism because for $g_1, g_2 \in G, \varphi(g_1g_2) = \lambda_{g_1g_2} = \lambda_{g_1} \circ \lambda g_2 = \varphi(g_1)\varphi(g_2)$.
Now, λ_e is the identity element in $\overline{G}$. Let $x \in \ker\varphi, x \in G$. Then, $\varphi(x) = \lambda_x = \lambda_e$. So, $\lambda_x(g) = \lambda_e(g)$ for $g \in G$ which is equivalent to $xg = g \Leftrightarrow x = e$. Hence, $\ker\varphi = \{e\}$, so φ is injective.
And since $|G| = |\overline{G}|$, φ is also bijective.
Hence, φ is an isomorphism, so $G \cong \overline{G}$. □

13.2 Conjugacy Classes

Let G act on itself by conjugation. We write $g \cdot x = gxg^{-1}$. The conjugacy class of x is given by

$$\mathrm{Cl}(x) = \{gxg^{-1} : g \in G\}.$$

Example. Consider

$$S_3 = \{(\ ), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

$$\mathrm{Cl}((1\ 2)) = \{(1\ 2), (1\ 3), (2\ 3)\}.$$

$$\mathrm{Cl}((1\ 2\ 3)) = \{(1\ 2\ 3), (1\ 3\ 2)\}.$$

Theorem 9. Conjugacy classes preserve the cycle structure in S_n.

Theorem 10. Therefore, conjugacy classes in S_n corresponds to the partitions of n.

Example. Consider S_4. Number of ways to partition 4, $P(4) = 5$.

$$\begin{aligned} 4 &\longleftrightarrow (1\ 2\ 3\ 4) \\ 3+1 &\longleftrightarrow (1\ 2\ 3)(4) \\ 2+2 &\longleftrightarrow (1\ 2)(3\ 4) \\ 2+1+1 &\longleftrightarrow (1\ 2)(3)(4) \\ 1+1+1+1 &\longleftrightarrow (\ )(\ )(\ )(\ ) \end{aligned}$$

Theorem 11. Conjugacy classes of G partition the group since conjugation defines an equivalence relation.

Proof. Define the conjugacy relation on G as follows: For $g, h \in G$, we say that $g \sim h$ if there exists some $x \in G$ such that

$$h = xgx^{-1}.$$

For any $g \in G$, we can take $x = e$, the identity element of G. Then,

$$xgx^{-1} = ege = g.$$

Thus, $g \sim g$, so the relation is **reflexive**.
Let $g \sim h$, meaning that there exists an element $x \in G$ such that $h = xgx^{-1}$. We want to show that $h \sim g$, i.e., there exists some element $y \in G$ such that $g = yhy^{-1}$. We can choose $y = x^{-1}$. Then,

$$yhy^{-1} = x^{-1}(xgx^{-1})x = g.$$

Thus, $h \sim g$, so the relation is **symmetric**.
Let $g \sim h$ and $h \sim k$, meaning that there exist elements $x, y \in G$ such that $h = xgx^{-1}$ and $k = yhy^{-1}$. We want to show that $g \sim k$, i.e., there exists some element $z \in G$ such that $k = zgz^{-1}$. Substitute $h = xgx^{-1}$ into the expression for k:

$$k = yhy^{-1} = y(xgx^{-1})y^{-1} = (yx)g(x^{-1}y^{-1}).$$

Let $z = yx$. Then we have

$$k = zgz^{-1},$$

so $g \sim k$. Thus, the relation is **reflexive**.
Therefore, Conjugacy relation is an equivalence relation on G.
The equivalence classes under this relation are called the *conjugacy classes* of G which partition G. □

Lecture 14

18 Dec 2024

14.1 Class Equation

Definition 25. $\text{Stab}(x) = \{g \in G : g \cdot x = x\}$.

For conjugation action,

$$\text{Stab}(x) = \{g \in G : gxg^{-1} = x\} = C_G(x).$$

Theorem 12. $|\text{Cl}(a)| = [G : \text{Stab}(a)] = [G : C_G(a)] = \frac{|G|}{|C_G(a)|}$.

Proof. Since $[G : C_G(a)]$ is the number of left cosets of $C_G(a)$, we want to define a bijective map between elements in $\text{Cl}(a)$ and the left cosets of $C_G(a)$.
Let $H = C_G(a)$.
Since the elements of $\text{Cl}(a)$ are conjugates of a, we define f by:

$$f(xax^{-1}) \mapsto xH$$

We claim that f is 1-1. Suppose $f(x) = f(y)$, then $xH = yH$, and thus $xh = y$ for some $h \in H$. But then $x^{-1}y \in H$, so that $x^{-1}y$ commutes with a, and therefore:

$$x^{-1}ya = ax^{-1}y.$$

From this, we conclude that:

$$xax^{-1} = yay^{-1},$$

which proves that f is injective.
As for surjectivity, note that for any $x \in G$, xax^{-1} is in $\text{Cl}(a)$.
However, we also need to show the map is well-defined. That is, we need to show that if xax^{-1} and yay^{-1} are two descriptions of the same element in $\text{Cl}(a)$, then $f(x) = f(y)$. The calculation which shows this is simply the reversal of the steps above. To be precise:

$$xax^{-1} = yay^{-1} \quad \Rightarrow \quad ax^{-1}y = x^{-1}ya \quad \Rightarrow \quad x^{-1}y \in H \quad \Rightarrow \quad xH = yH.$$

Thus, the map is well-defined and bijective, so : $|\text{Cl}(a)| = [G : C_G(a)]$. □

Lemma 12. If $x \in Z(G)$, then $\text{Cl}(x) = \{x\}$.

Theorem 13 (Class Equation). Given a finite group G with center $Z(G)$ and representatives $g_1, g_2, ..., g_n$ of the distinct conjugacy classes not contained in $Z(G)$, then

$$\begin{aligned} |G| &= |Z(G)| + \sum_{i=1}^{n} [G : C_G(g_i)] \\ &= |Z(G)| + \sum_{i=1}^{n} \frac{|G|}{|C_G(g_i)|}. \end{aligned}$$

Proof. $\{x\}$ is a conjugacy class of size 1 if and only if $x \in Z(G)$. Let $Z(G) = \{1, z_1, z_2, ..., z_{k-1}\}$. Since conjugacy classes partition G,

$$G = (\mathrm{Cl}(z_1) \cup \mathrm{Cl}(z_2) \cup \cdots \cup \mathrm{Cl}(z_k)) \cup (\mathrm{Cl}(g_1) \cup \mathrm{Cl}(g_2) \cup \cdots \cup \mathrm{Cl}(g_n)).$$

Hence,

$$\begin{aligned} |G| &= |Z(G)| \cdot 1 + \sum_{i=1}^{n} |\mathrm{Cl}(g_i)| \\ &= |Z(G)| + \sum_{i=1}^{n} [G : C_G(g_i)] \\ &= |Z(G)| + \sum_{i=1}^{n} \frac{|G|}{|C_G(g_i)|}. \end{aligned}$$

□

14.2 Rings and Fields

Definition 26. A ring R is a set together with two binary operations $+$ and $\times$ (called addition and multiplication respectively) satisfying the following axioms:

1. $(R, +)$ is an abelian group.
2. $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b \in R$.
3. Distributive laws hold: $(a+b) \times c = (a \times c) + (b \times c)$ and $a \times (b+c) = (a \times b) + (a \times c)$ for all $a, b, c \in R$.

Remark (Why we need $(R, +)$ to be abelian group?)**.** We need $(R, +)$ to be abelian because otherwise distributive laws will not hold. For instance,

$$(1 + 1) \times (a + b) = 1 \times a + 1 \times b + 1 \times a + 1 \times b$$

But also

$$(1 + 1) \times (a + b) = 1 \times a + 1 \times a + 1 \times b + 1 \times b$$

Definition 27 (Commutative Ring)**.** A ring is said to be *commutative* if multiplication $\times$ is commutative.

Definition 28. A ring is said to *have an identity* if there is an element 1 such that

$$1 \times a = a \times 1 = a, \text{ for all } a \in R.$$

Definition 29 (Division Ring)**.** A ring with identity 1, where $1 \neq 0$, is called a *division ring*, if every element $a \neq 0 \in R$ has a multiplicative inverse, that is, there exists $b \in G$ such that

$$a \times b = b \times a = 1.$$

Definition 30 (Field)**.** A commutative division ring is called *field*.

14.3 Examples of Ring

Example. $\mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{R}$ are all examples of ring and commutative ring. Excluding $\mathbb{Z}$, all of them are division ring, so are fields.

Example (Trivial Ring)**.** $\{0\}$ is a *trivial ring*.

Example (Trivial Example)**.** For any abelian group R, if we define $a \times b := 0$, then R is a ring.

Lecture 15

19 Dec 2024

15.1 More Examples of Ring

Example. $\mathbb{Z}/n\mathbb{Z}$ is an example of a commutative ring because $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group and multiplication modulo n satisfies associativity and commutativity and distributes over addition.

Example. $\mathbb{Z}/6\mathbb{Z}$ is not a division ring, e.g., $\overline{3}$ doesn't have a multiplicative inverse.

Example (Finite Field)**.** $\mathbb{Z}/5\mathbb{Z}$ is a division ring. Also it is commutative ring, hence, it is a field.
Notice, for all prime numbers p, $F_p := \mathbb{Z}/p\mathbb{Z}$ is a field. Number of its elements is finite, hence, it is an example of a finite field.

Example (A ring without multiplicative identity)**.** $2\mathbb{Z}$.

Definition 31 (Quaternions)**.** Let $\mathbb{H}$ to be the set of all quaternions such that

$$\mathbb{H} := \{a + bi + cj + dk : a, b, c, d \in R\}.$$

And define addition + via-

$$(a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b2_i + c_2 i + d_2 k) := (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k.$$

And multiply using distributive laws subject to the relations:

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ ij &= -ji = k \\ jk &= -kj = i \\ ki &= -ik = j \end{aligned}$$

Example. The set of all quaternions $\mathbb{H}$ forms a non-commutative division ring.

Proof. Quaternions form a ring:

- **Addition**: The addition of two quaternions is componentwise and is associative and commutative because real numbers are commutative and associative. The additive identity is $0 = 0 + 0i + 0j + 0k$, and the additive inverse of $q = a + bi + cj + dk$ is $-q = -a - bi - cj - dk$.
- **Multiplication**: The multiplication of quaternions is defined by the distributive law, and is associative.

Quaternions form a division ring: The identity element is $1 = 1 + 0i + 0j + 0k$, and every quaternion $q = a + bi + cj + dk$ has a multiplicative inverse, as shown below. For

any non-zero quaternion $q = a + bi + cj + dk$, the inverse is given by:

$$q^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2},$$

which satisfies $qq^{-1} = 1$, as can be verified by multiplying.
Quaternions form a non-commutative ring: By definition, $ij = -ji$, hence, multiplication is not commutative.

Example (Workout Example). $a = 1 + 2j + 3k$ and $b = j + k$.

$$\begin{aligned} a + b &= (1 + 2j + 3k) + (j + k) \\ &= 1 + (2 + 1)j + (3 + 1)k \\ &= 1 + 3j + 4k. \end{aligned}$$

$$\begin{aligned} a \times b &= (1 + 2j + 3k) \times (j + k) \\ &= (1 + 2j + 3k)j + (1 + 2j + 3k)k \\ &= j + 2j^2 + 3kj + k + 2jk + 3k^2 \\ &= j + 2(-1) + 3(-i) + k + 2i + 3(-1) \\ &= j - 2 - 3i + k + 2i - 3 \\ &= -5 - i + j + k. \end{aligned}$$

15.2 Properties of Ring

Proposition 6. If R is a ring, then for all $a, b \in R$,

1. $0 \cdot a = a \cdot 0 = 0$.
2. $(-a)b = a(-b) = -(ab)$.
3. $(-a)(-b) = ab$.
4. The multiplicative identity is unique.

Proof. 1.

$$\begin{aligned} (0 + 0)a &= 0 \cdot a + 0 \cdot a \\ \Rightarrow 0 \cdot a &= 0 \cdot a + 0 \cdot a \\ \Rightarrow 0 &= 0 \cdot a \\ \Rightarrow 0 \cdot a &= 0. \end{aligned}$$

Similarly, $a \cdot 0 = 0$.

2.

$$\begin{aligned} (a - a)b &= 0 \\ \Rightarrow ab + (-a)b &= 0 \\ \Rightarrow (-a)b &= -(ab). \end{aligned}$$

Similarly, $a(-b) = -(ab)$.

3. Using previous result, $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.
4. Let 1 and $1'$ be two distinct multiplicative identity. Then for $a \in R$, $a \cdot 1 = a = a \cdot 1'$ which implies $1 = 1'$ (contradiction!). Hence, multiplicative identity has to be unique.

15.3 Subring

Definition 32 (Subring)**.** A subset S of ring R is a *subring* if it is a subgroup of R under addition and if is closed under multiplication.

Example. $2\mathbb{Z} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \subset \mathbb{H}$.

15.4 Characteristic

Definition 33 (Characteristic)**.** Let R be a ring with identity 1. If there exists a positive integer n such that $1 + 1 + \cdots + 1 = n1 = 0$, then n is called the characteristic of R, and denoted by $\text{char}(R)$. If no such positive integer exists, then R is said to be characteristic zero.

Example. In $R = \mathbb{Z}/n\mathbb{Z}$, $\text{char}(R) = 0$.

Lecture 16

23 Dec 2024

16.1 Integral Domain

Definition 34 (Zero Divisor). Let R be a ring. A non-zero element $a \in R$ is called a *zero divisor* if there is a non-zero element $b \in R$ such that either $ab = 0$ or $ba = 0$.

Example. $\overline{3}$ is a zero divisor in $\mathbb{Z}/6\mathbb{Z}$ since $\overline{3} \cdot \overline{2} = 0$.

Definition 35 (Unit). Assume R has an identity 1. An element $u \in R$ is called *a unit in* R if there is some $v \in R$ such that $uv = vu = 1$.

The set of units in R is denoted by $R^\times$.

Example. $\overline{5}$ is a unit in $\mathbb{Z}/6\mathbb{Z}$ since $\overline{5} \cdot \overline{5} = \overline{1}$.

Definition 36 (Integral Domain). A commutative ring with identity is called an *integral domain* if it has no zero divisor.

Proposition 7. If R is an integral domain, then for all $a, b \in R$,

1. If $ab = 0$ then $a = 0$ or $b = 0$.
2. If $ab = ac$ then $a = 0$ or $b = c$.

Proof. We will prove 2.

$$\begin{aligned} & ab = ac \\ \Rightarrow\ & ab - ac = 0 \\ \Rightarrow\ & a(b - c) = 0 \\ \Rightarrow\ & a = 0 \text{ or } b = c. \end{aligned}$$

Lemma 13. Any finite integral domain is a field.

Proof. Let R be a finite integral domain. Hence, R is commutative and has an identity 1. We just have to prove R is division ring, that, is for every $a \in R$ there is a $b \in R$ such that $ab = 1$.
For $a \neq 0 \in R$ define $\varphi_a : R \to R$ such that $\varphi_a(x) = ax$. Since $a \neq 0$, φ_a is injective. Since R is finite, $|\varphi_a(R)| = |R|$. Hence, φ_a is also surjective, so, the map is bijective.
Therefore, for all $a \neq 0$, there is b, such that $\varphi_a(b) = 1 \Rightarrow ab = 1$.
Hence, R is a field.

16.2 Ring Homomorphisms

Definition 37 (Ring Homomorphism). A *ring homomorphism* $\varphi : R \to S$ is a map satisfying the following:

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$,
2. $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

Definition 38 (Isomorphism). A bijective ring homomorphism is called an *isomorphism*.

Example (Trivial Homomorphism). $\varphi : R \to S$ such that $\varphi(r) = 0$.

Example (Identity Homomorphism). $\varphi : R \to R$ such that $\varphi(r) = r$.

Example. $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ such that $\varphi(x) = x \mod n$ is homomorphism.

Proof. For all $a, b \in \mathbb{Z}$,

$$\begin{aligned}\varphi(a+b) &= (a+b) \bmod n \\ &= a \bmod n + b \bmod n \\ &= \varphi(a) + \varphi(b).\end{aligned}$$

$$\begin{aligned}\varphi(ab) &= ab \bmod n \\ &= (a \bmod n)(b \bmod n) \\ &= \varphi(a) \cdot \varphi(b).\end{aligned}$$

Definition 39 (Polynomial Ring). Let R be a ring, x be an indeterminate and define $R[x]$ be the set of all formal sums

$$R[x] := a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum a_i x^i.$$

Given two polynomials $f = \sum a_i x^i$ and $g = \sum b_i x^i$ in $R[x]$, the sum of f and g is defined as

$$f + g = \sum (a_i + b_i) x^i,$$

(where we have implicitly assumed that $m \leq n$ and we set $b_i = 0$ for $i > m$). And the product of f and g as

$$fg = \sum_i (\sum_j a_j b_{i-j}) x^i.$$

With this rule of addition and multiplication, $R[x]$ becomes a ring, called *polynomial ring*.

In the definition above, each $a_i \in R$ is called the coefficients of the polynomial; a_i is the coefficient of x^i and the zero element given as the polynomial with zero coefficients.

Example. $\varphi : \mathbb{Q}[x] \to \mathbb{Q}$ such that $\varphi(P(x)) = P(0)$ is a ring homomorphism.

Proof.

$$\begin{aligned}&\varphi[P_1(x) + P_2(x)]\\ &= P_1(0) + P_2(0)\\ &= \varphi[P_1(x)] + \varphi[P_2(x)].\end{aligned}$$

$$\begin{aligned}&\varphi[P_1P_2]\\ &= P_1P_2(0)\\ &= P_1(0)P_2(0)\\ &= \varphi[P_1(x)]\varphi[P_2(x)].\end{aligned}$$

16.3 Kernel and Image of Ring Homomorphism

Definition 40 (Kernel of Ring)**.** For rings, the *kernel* is the set of all elements in R that get mapped to $0 \in S$. In symbols,

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

Proposition 8. Let R and S be rings and $\varphi : R \to S$ a ring homomorphism. Then,

1. The image of φ is a subring of S.
2. $\ker \varphi$ is a subring of R. Furthermore, $\ker \varphi$ is closed under multiplication by every element of R.

Proof. 1. Let $a, b \in \operatorname{Im} \varphi$, then there is $r_1, r_2 \in R$ such that $a = \varphi(r_1)$ and $b = \varphi(r_2)$. Since φ is a homomorphism,

$$a - b = \varphi(r_1) - \varphi(r_2) = \varphi(r_1 - r_2) \in S.$$

Hence, im φ is closed under subtraction.
Again since φ is a homomorphism,

$$ab = \varphi(r_1)\varphi(r_2) = \varphi(r_1r_2) \in S.$$

Therefore, im φ is closed under multiplication.
Hence, im φ is a subring of S.

2. Let $a, b \in \ker \varphi$, then $\varphi(a) = 0$ and $\varphi(b) = 0$. Since φ is a homomorphism,

$$\varphi(a - b) = \varphi(a) - \varphi(b) = 0 - 0 = 0.$$

Hence, $(a - b) \in \ker \varphi$, so $\ker \varphi$ is closed under subtraction.
Again since φ is homomorphism,

$$\varphi(ab) = \varphi(a)\varphi(b) = 0 \cdot 0 = 0.$$

Therefore, $ab \in \ker \varphi$, so $\ker \varphi$ is closed under multiplication.
Hence, $\ker \varphi$ is a subring of R.

Now, for the last part, let $a \in \ker(\varphi)$ and $r \in R$. Then $\varphi(a) = 0$. Since φ is a ring homomorphism, we have:

$$\varphi(ra) = \varphi(r) \cdot \varphi(a) = \varphi(r) \cdot 0 = 0,$$

and

$$\varphi(ar) = \varphi(a) \cdot \varphi(r) = 0 \cdot \varphi(r) = 0.$$

Thus, $ra, ar \in \ker(\varphi)$. Hence, $\ker(\varphi)$ is closed under multiplication by elements of R.

Lecture 17

28 Dec 2024

17.1 Ideals

Let R be a ring, let I be a subset of R and let $r \in R$. We have two subsets

$$rI = \{ra : a \in I\}$$

and

$$Ir = \{ar : a \in I\}.$$

Definition 41 (Left Ideal)**.** A subset I of R is a left ideal of R if I is a subring of R and I is closed under left multiplication by elements of R, that is, $rI \subseteq I$ for all $r \in R$.

Similarly we can define,

Definition 42 (Right Ideal)**.** A subset I of R is a right ideal of R if I is a subring of R and I is closed under right multiplication by elements of R, that is, $Ir \subseteq I$ for all $r \in R$.

We say we have a *two-sided ideal* or simply an *ideal* when I is both a left and right ideal. A left idea is not necessarily a right ideal. But in commutative rings, a left ideal is also a right ideal.

Lemma 14 (Ideal Criterion(?))**.** A subset I of ring R is an ideal if-

- I is non-empty and closed under subtraction.
- I is closed under multiplication by any element of R.

17.2 Examples of Ideal

Example. The kernel of any ring homomorphism is an ideal.

Proof. Was done in this proposition.

Example. $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Proof. $n\mathbb{Z}$ is a subring of $\mathbb{Z}$, which can be easily checked. For any element $x \in n\mathbb{Z}$ and $y \in \mathbb{Z}$, we have

$$yx = y \cdot (kn) = yk \cdot n$$

for some $k \in \mathbb{Z}$. So $yx \in n\mathbb{Z}$, and $n\mathbb{Z}$ is a left ideal. $\mathbb{Z}$ is commutative, so $n\mathbb{Z}$ is also a right ideal.

Example. Let $R = \mathbb{Z}[x]$ be the ring of polynomials in x with integer coefficients and I be the set of polynomials whose terms are of degree at least 2 (i.e., having no terms of degree 0 and 1) together with zero polynomial. Then I is an ideal of R.

Proof. If $f, g \in I$, then $f + g \in I$ since adding polynomials with no terms of degree 0 or 1 results in another polynomial with the same property.
Then, if $f \in I$ and $r \in R$, then $r \cdot f \in I$ because multiplying any polynomial f by r does

not introduce terms of degree 0 or 1 into $r \cdot f$.
Thus, I is closed under addition and closed under multiplication by any element of R. As $0 \in I$, it is non-empty. Therefore, I is an ideal of R.

Example. Let $M_{n\times n}(R)$ be the matrix ring over some ring R. If J is an ideal of R, $M_{n\times n}(J)$ is an ideal of $M_{n\times n}(R)$.

Proof. Non-empty: Since J is an ideal of R, it contains the zero element, i.e., $0 \in J$. Therefore, the zero matrix belongs to $M_{n\times n}(J)$. Hence, $M_{n\times n}(J)$ is non-empty.
Let $A = (a_{ij})$ and $B = (b_{ij})$ be matrices in $M_{n\times n}(J)$, where each entry $a_{ij} \in J$ and $b_{ij} \in J$.
Closure under subtraction: Consider the matrix $A - B$:

$$A - B = (a_{ij} - b_{ij}).$$

Since J is an ideal of R, it is closed under subtraction, so $a_{ij} - b_{ij} \in J$ for all i, j. Therefore, $A - B \in M_{n\times n}(J)$.
Closure under multiplication by any matrix in $M_{n\times n}(R)$ We need to show that both $AB \in M_{n\times n}(J)$ and $BA \in M_{n\times n}(J)$.
Left multiplication by B:
Let $C = AB$, where the entry c_{ij} in the matrix C is given by

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

Since $a_{ik} \in J$ (because $A \in M_{n\times n}(J)$) and J is an ideal of R, and $b_{kj} \in R$, the product $a_{ik}b_{kj} \in J$ because J is closed under multiplication by any element of R. Hence, each entry $c_{ij} \in J$, implying $C = AB \in M_{n\times n}(J)$.
Right multiplication by A: Similarly, $BA \in M_{n\times n}(J)$.
Since $M_{n\times n}(J)$ is non-empty, closed under subtraction, and closed under multiplication by any element of $M_{n\times n}(R)$, it follows that $M_{n\times n}(J)$ is an ideal of $M_{n\times n}(R)$.

Example (All ideals are not two-sided)**.** Consider the ring $M_{2\times 2}(R)$, where R is an commutative ring with identity. Let L_1 be the set of all matrices in $M_{2\times 2}(R)$ with only entries in the first column, i.e.,

$$L_1 = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in R \right\}.$$

Then, L_1 is a left ideal, but not right ideal.
We can similarly define R_1 which is a right ideal but not a left ideal. We can also define L_2, R_2. In general, we can define $L_1, L_2, \cdots, L_n, R_1, R_2, \cdots, R_n$ for $n \times n$ matrices.

Example (Sum of Ideals)**.** If I and J are two ideals of R, we can take the set $I + J$ defined by

$$I + J = \{a + b : a \in I, b \in J\},$$

which also happens to be an ideal of R. This is called the *sum of two* ideals I and J.

Example (Product of Two Ideals)**.** The *product of two ideals* I and J in a ring R, denoted as IJ, is defined as the ideal of R generated by all finite sums of products of elements from I and J. That is,

$$IJ = \left\langle \sum_{k=1}^{n} a_k b_k \mid a_k \in I, b_k \in J, n \in \mathbb{N} \right\rangle.$$

Example (n-fold Ideal)**.** For an ideal I in a ring R, the n-fold ideal I^n is the ideal of R generated by all finite sums of products of n elements, where each element is taken from I. That is,

$$I^n = \left\langle \sum_{k=1}^{m} a_1 a_2 \cdots a_n \mid a_1, a_2, \ldots, a_n \in I, m \in \mathbb{N} \right\rangle.$$

17.3 Quotient Rings

Just like we defined quotient groups where we mod out by a normal subgroup, for rings we can define quotient rings by *mod*-ing out by an appropriate ideal.

Definition 43 (Quotient Ring)**.** Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operations:

$$(r + I) + (r + I) := (r + s) + I$$

$$(r + I)(s + I) := rs + I,$$

where $r, s \in R$. R/I is called quotient ring of R modulo I.

Example. Let $R = \mathbb{Z}$ and $I = n\mathbb{Z}$. Then we have $R/I = \mathbb{Z}/n\mathbb{Z}$, the quotient ring of $\mathbb{Z}$ modulo $n\mathbb{Z}$.
We saw earlier that $\mathbb{Z}/n\mathbb{Z}$ is a ring, in particular, is a field when n is prime.

Example. Let $R = \mathbb{Z}[x]$ and I be the collection of polynomials whose terms are of degree at least 2 with the zero polynomial. Two polynomial $p(x), q(x)$ are in the same coset of I if and only if they differ by a polynomial whose terms are of degree at least 2, i.e., $p(x)$ and $q(x)$ have the same constant and first degree term. Hence, $R/I = \{a + bx : a, b \in R\}$. Furthermore, we add and multiply in this quotient ring as usual and taking $x^2 = 0$ in this ring.
It is interesting to note that R/I has zero divisors though R does not.

17.4 Canonical Projection Map

If I is any ideal, then R/I is a ring and the canonical map

$$\pi : r \to r + I,$$

is a ring homomorphism with kernel I.
We already know π is a group homomorphism, it remains to check that π is also ring homomorphism. This is immediate from the definition of multiplication in R/I:

$$\pi(rs) = rs + I = (r + I)(s + I) = \pi(r)\pi(s).$$

Hence,

Theorem 14. We can realize every ideal as the kernel of some ring homomorphism.

17.5 Isomorphism Theorems for Rings

Theorem 15 (First Isomorphism Theorem)**.** If $\phi : R \to S$ is a homomorphism of rings, then $R/ker\ \phi$ is isomorphic as a ring to $\phi(R)$.

Proof. The proof goes same as first Isomorphism theorem proof that we did previously. Here we just have to consider extra ring multiplication operation. If $I = \ker\ \phi$, then the correspondence $r + I \to \phi(r)$ is a bijection between the rings R/I and $\phi(R)$ which respects addition, in this case, also multiplication, hence is a ring isomorphism. Therefore, $R/ker\ \phi \cong \phi(R)$. □

Example. Let $R = \mathbb{Z}[x]$ and consider the homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$ such that

$$\phi(p(x)) = p(0) \mod 2.$$

Then $R/\ker\ \phi \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. Firstly, $\ker\ \phi = \{p(x) \in \mathbb{Z}[x] : p(0) \in 2\mathbb{Z}\}$ is mapped to $\overline{0} \in \mathbb{Z}/2\mathbb{Z}$. And the set of all polynomials whose constant term is odd mapped to $\overline{1}$. Hence, the homomorphism is surjective. According to the first isomorphism theorem,

$$R/ker\ \phi \cong \mathbb{Z}/2\mathbb{Z}$$

Theorem 16 (Second Isomorphism Theorem)**.** Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b : a \in A, b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)$.

Theorem 17 (Third Isomorphism Theorem)**.** Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.

One can prove both theorems using similar arguments (that were used to prove isomorphism theorems for groups).

Lecture 18

30 Dec 2024

18.1 Ideals Generated By A Subset

Definition 44 (Ideal Genereated By A Subset)**.** Let A be a subset of a ring R with identity $1 \neq 0$. Let $S = \{I_k\}$ be the collection of all left ideals of R that contain A (note that the set is nonempty since $A \subseteq R$ and R is an ideal in itself). The intersection

$$\bigcap_{I_k \in S} I_k,$$

is called the *left ideal generated by* A, and is denoted by $(A)_L$. Alternatively, we can constructively form the set of elements that constitutes this ideal:

$$(A)_L = \left\{ \sum_{k=1}^{m} r_k a_k : r_k \in R, a_k \in A, m \in \mathbb{N} \right\}.$$

The definition is symmetrical for *right ideal generated by a subset.*

Definition 45 (Finitely Generated Ideal)**.** An ideal in a commutative ring is said to be *finitely generated* if there exits $x_1, x_2, ..., x_n$ such that

$$I = Rx_1 + Rx_2 + \cdots + Rx_m, m \in \mathbb{N}.$$

Or for all $i \in I$,

$$i = r_1x_1 + r_2x_2 + \cdots + r_nx_n.$$

Example. $R = \mathbb{Z}, I = 2\mathbb{Z} + 3\mathbb{Z} = (2, 3) = \{2k + 3l : k, l \in \mathbb{Z}\}$. Hence, $2\mathbb{Z} + 3\mathbb{Z}$ is a finitely generated ideal in $\mathbb{Z}$.

Definition 46 (Principle Ideal)**.** *Principle ideal* is an ideal generated by a single element a. Symbolically,

$$(a) = \{ra : r \in R\}$$

Example. $R = \mathbb{Z}, I = 3\mathbb{Z} = (3) = \{k \cdot 3 : k \in \mathbb{Z}\}$. Hence, $3\mathbb{Z}$ is a principle ideal in $\mathbb{Z}$.

Proposition 9. Let I be an ideal of R with identity. Then,

1. $I = R$ if and only if I contains the unit element.
2. $I = R$ if and only if I contains a unit.
3. Assume R is commutative, then R is a field if and only if its only ideals are (0) and $(1) = R$ itself.

Proof.

1. If $I = R$, then its obvious. Now let I contains 1, then $r \cdot 1 = r \in I$, for all $r \in R$. Therefore, $R \subseteq I$. But $I \subseteq R$ by definition. Hence, $I = R$.
2. If $I = R$, then its obvious. Let a be a unit in R. Then, there exits $b \in R$ such that

$ba = 1$. But since I is an ideal $ba = 1 \in I$. From the previous result, $I = R$.

3. Let R be a field and I be a nonzero ideal of R and $x \in I$. Then $xx^{-1} = 1 \in I$. Since $1 \in I$, $I = R$. Hence, only ideals of R are (0) and R itself. Conversely, if (0) and R are the only ideals of R, let u be any nonzero element of R. By hypothesis $(u) = R$ and so $1 \in (u)$. Thus there is some $v \in R$ such that $1 = vu$, which means u is an unit. It is true for all $u \in R$. Hence, R is a commutative division ring, i.e., field.

Lecture 19

4 Jan 2025

19.1 Maximal Ideals

Definition 47 (Maximal Ideal). An ideal M in an arbitrary ring R is a *maximal ideal* if $M \neq R$ and the only ideals that contain M are M and R.

In other words, $M \neq R$ is a maximal ideal if there is no other proper ideal of R that contains M. $M \subset K \subset R \Rightarrow$ either $K = M$ or $K = R$.

Non-example. $6\mathbb{Z}$ is not a maximal ideal of $\mathbb{Z}$ because $6\mathbb{Z} \subset 3\mathbb{Z}$.

Lemma 15. If p is a prime, then $p\mathbb{Z}$ is a maximal ideal.

Proof. Let $p\mathbb{Z} \subset q\mathbb{Z} \subset \mathbb{Z}$. For the inclusion to be true, q must divide p. Since p is a prime, either $q = 1 \Rightarrow q\mathbb{Z} = \mathbb{Z}$ or $q = p \Rightarrow q\mathbb{Z} = p\mathbb{Z}$. Which means $p\mathbb{Z}$ is a maximal ideal.

Example. $(2, x)$ in $\mathbb{Z}[x]$ is a maximal ideal.

Proof. $\mathbb{Z}/2\mathbb{Z}$ is a maximal ideal, $(2, x) = \{2p(x)+q(x) : p(x), q(x) \in \mathbb{Z}[x]\}$ and $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$. Hence, $(2, x)$ is a maximal ideal in $\mathbb{Z}$.

Non-example. $(x) \subset \mathbb{Z}[x]$ is not a maximal ideal since $(x) \subset (2, x) \subset \mathbb{Z}$.

Theorem 18 (Correspondence Theorem). Let R, R' be rings and φ be a homomorphism from R to R' with kernel u. Then there is a one-one correspondence between the set of ideals in R which contain u and the set of ideals in R'.

Proposition 10. Assume R is commutative. Then M is maximal ideal if and only if R/M is a field.

Proof. Consider canonical map $\varphi : R \to R/M$. Then φ has kernel M.
Assume M is a maximal ideal. Then only two ideals contain M: M and R. Let I be an ideal in R/M. By correspondence theorem, there is an ideal $K \subseteq R$ containing M. However, since M is a maximal ideal, either $K = M$ or $K = R$. Therefore, there are only two ideals in R/M. They are (0) and (R/M) itself. Hence, R/M is a field.
Conversely, let R/M is a field. Then for all ideal I in R/M, there exists a corresponding ideal K in R that contain M. But either $I = R/M$ or $I = (0)$. Which means R has two ideals containing M, which are M and R. Hence, M is a maximal ideal.

19.2 Prime Ideals

Definition 48 (Prime Ideal). Assume R is commutative. An ideal $P \subset R$ is called *prime ideal* if $P \neq R$ and whenever $ab \in P$ for $a, b \in R$, then either $a \in P$ or $b \in P$ or both.

Non-example. $6\mathbb{Z}$ is not a prime ideal of $\mathbb{Z}$ because $3 \times 2 = 6 \in 6\mathbb{Z}$ but $2, 3 \notin 6\mathbb{Z}$.

Lemma 16. $p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$.

Proof. Let $ab \in p\mathbb{Z}$. Then $ab = pk$ for some $k \in \mathbb{Z}$. By prime factorization, either $p|a$ or $p|b$ or both, which implies either $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$ or both.

Lemma 17. Every maximal ideal is a prime ideal.

The converse of the above lemma does not hold.

Proposition 11. Assume R is commutative. An ideal $P \in R$ is a prime ideal if and only if R/P is an integral domain.

Proof. Assume P is a prime ideal. Let $\overline{a}, \overline{b} \in R/P$ and $\overline{a} \cdot \overline{b} = 0$ which implies $\overline{ab} = 0 \Rightarrow ab \in P$. Since P is prime, either $a \in P \Rightarrow \overline{a} = 0$ or $b \in P \Rightarrow \overline{b}$ or both. Therefore, according to the definition, R/P is an integral domain.

Conversely, assume that R/P is an integral domain. Let $ab \in P$. Then $0 + P = ab + P = (a + P)(b + P)$ which implies that $a + P = 0 + P$ or $b + P = 0 + P$, since R/P is an integral domain. Thus, $a \in P$ or $b \in P$ and so P is a prime ideal.

19.3 Fields of Fractions of An Integral Domain

Definition 49 (Field of Fractions of an Integral Domain)**.** Let R be an integral domain. Define $N \subseteq R \times R$ as the set of pairs (a, b) where $b \neq 0$. An equivalence relation $\sim$ on N is defined by

$$(a, b) \sim (p, q) \Leftrightarrow aq = bp.$$

The *field of fractions* of R is the set of equivalence classes under this relation.
We denote the equivalence class of (a, b) by $[a, b]$. This set forms a field with the following operations:

$$[a, b] + [c, d] := [ad + bc, bd].$$

$$[a, b] \cdot [c, d] := [ac, bd].$$

The proof that field of fractions indeed forms a field is simple, but tedious to check. However, it is worth mentioning that the additive and multiplicative identities of such field are given by $[0, 1]$ and $[1, 1]$, respectively.

Lecture 20

4 Jan 2025

20.1 Examples of Field of Fractions

Example. $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$.

Definition 50 (Gaussian Integers). Consider $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ known as *Gaussian integers*. Define

$$(a + bi) + (c + di) := (a + c) + (b + d)i,$$
$$(a + bi) \cdot (c + di) := (ac - bd) + (ad + bc)i.$$

Then, $\mathbb{Z}[i]$ is an integral domain under these operations.

Example. $\mathbb{Q}[i]$ is the field of fractions of $\mathbb{Z}[i]$.

Proof. To prove that $\mathbb{Q}[i]$ is the field of fractions of $\mathbb{Z}[i]$, we verify the following:

1. Every element of $\mathbb{Q}[i]$ can be expressed as a fraction of elements in $\mathbb{Z}[i]$.
2. If an element can be expressed as a fraction of elements in $\mathbb{Z}[i]$, it belongs to $\mathbb{Q}[i]$.

1. By definition, $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$. Let $a, b \in \mathbb{Q}$. Since $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, we can write $a = \frac{m}{n}$ and $b = \frac{p}{q}$, where $m, n, p, q \in \mathbb{Z}$ and $n, q \neq 0$.
Then,

$$a + bi = \frac{m}{n} + \frac{p}{q}i = \frac{mq + npi}{nq},$$

where $mq + npi \in \mathbb{Z}[i]$ and $nq \in \mathbb{Z} \setminus \{0\}$.
Hence, $a + bi \in \mathbb{Q}[i]$ is expressible as $\frac{\alpha}{\beta}$, where $\alpha, \beta \in \mathbb{Z}[i]$ and $\beta \neq 0$.

2. Let $\frac{\alpha}{\beta}$ be a fraction where $\alpha, \beta \in \mathbb{Z}[i]$ and $\beta \neq 0$.
Write $\alpha = a + bi$ and $\beta = c + di$, where $a, b, c, d \in \mathbb{Z}$.
The inverse of β in $\mathbb{Q}[i]$ is given by:

$$\beta^{-1} = \frac{\overline{\beta}}{\beta\overline{\beta}} = \frac{c - di}{c^2 + d^2},$$

where $\overline{\beta} = c - di$ is the complex conjugate of β.
Since $c^2 + d^2 \neq 0$, $\beta^{-1} \in \mathbb{Q}[i]$.
Therefore,

$$\frac{\alpha}{\beta} = \alpha \cdot \beta^{-1} \in \mathbb{Q}[i],$$

completing the proof.

Example. If R is an integral domain, so is $R[x]$. Then the field of fractions of $R[x]$ is given by all the rational functions, which are given by $\frac{f(x)}{g(x)}$, where $f(x), g(x) \in R[x]$ and $g(x) \neq 0$.

20.2 Norm, Euclidean Norm & Euclidean Domain

Definition 51 (Norm, Euclidean Norm & Euclidean Domain)**.** A *norm* of an integral domain D is a function $\nu : D \to \mathbb{N}$ with $\nu(0) = 0$.
If we have that ν also satisfying:

1. For all $a, b \neq 0$, $\nu(a) \leq \nu(ab)$,
2. For all $a, b \in D$, there exists $q, r \in D$ such that $a = bq + r$ with $\nu(r) < \nu(b)$,

then ν is called an *Euclidean norm* and D is called *Euclidean Domain.*

Example. Take $D = \mathbb{Z}$. Then $\nu(a) = |a|$ is an Euclidean norm on $\mathbb{Z}$.

Proof. 1. $\nu(0) = |0| = 0$

2. For all $a, b \neq 0$,
$$\nu(ab) = |ab| = |a| \cdot |b|.$$
But since $|b| \geq 1$, we have
$$\nu(a) \leq \nu(ab).$$

3. By the nature of Euclidean division, we have q, r for all $a, b \in \mathbb{Z}$ such that
$$a = bq + r,$$
where $0 \leq r < b$. Therefore, $\nu(r) = |r| < |b| = \nu(b)$.

Example. Consider $F[x]$, where F is a field. Define $\nu(f(x)) = \deg f(x)$. Then ν is an Euclidean norm and make $F[x]$ an Euclidean domain.

Proof. 1. $\nu(0) = \deg 0 = 0$.

2. For all $f, g \neq 0$,
$$\begin{aligned} \nu(fg) &= \deg f \cdot g \\ &= \deg f + \deg g \end{aligned}$$
Since $\deg g \geq 0$, we have $\nu(f) \leq \nu(fg)$.

3. By the virtue of polynomial division, there exists $q(x), r(x) \in F[x]$ such that
$$f(x) = g(x)q(x) + r(x),$$
with $\deg r < \deg g$.

20.3 Principle Ideal Domain

Definition 52 (Principle Ideal Domain)**.** A *principle ideal domain* is an integral domain D where every ideal is principle ideal.

Lecture 21

6 Jan 2025

21.1 Norm on Gaussian Integers

Example. The Gaussian integers $\mathbb{Z}[i]$ is an Euclidean domain with $\nu(a+bi) = a^2 + b^2$.

Proof. It is easy to check ν is a norm. We want check if nu is also an Euclidean norm. To begin with, if $\alpha = a + ib$ then

$$\nu(\alpha) = \alpha\overline{\alpha} \text{ where } \overline{\alpha} = a - ib$$

It follows that for every $\alpha, \beta \in \mathbb{Z}[i]$,

$$\nu(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = \nu(\alpha)\nu(\beta).$$

So if $\beta = 0$, then $\nu(\beta) \geq 1$ and $\nu(\alpha\beta) = \nu(\alpha)\nu(\beta) \geq \nu(\alpha)$.

To show that ν satisfies Division Algorithm, let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. By rationalizing the denominator we get,

$$\frac{\alpha}{\beta} = r + is, \text{ where } r, s \in \mathbb{Q}.$$

We can choose integers a, b such that $|r - a| \leq \frac{1}{2}$ and $|s - b| \leq \frac{1}{2}$. Then,

$$\begin{aligned} \alpha &= \beta(r + is) \\ &= \beta(a + ib) + \beta((r - a) + i(s - b)) \\ &= \beta\gamma + \delta, \end{aligned}$$

where $\gamma = a + ib$ and $\delta = \beta((r - a) + i(s - b))$. Since $a, b \in \mathbb{Z}$, so $\gamma \in \mathbb{Z}[i]$ and $\delta = \alpha - \beta\delta \in \mathbb{Z}[i]$. And we have

$$\nu(\delta) = \nu(\beta)((r - a)^2 + i(s - b)^2) = \nu(\beta)\frac{1}{2} < \nu(\beta),$$

which completes the proof.

21.2 Irreducible & Prime Elements

Definition 53. Let R be a commutative ring with identity. We say a divides b, if there exists c such that $b = ac$.

Definition 54. Two elements a and b are called associates if there exits a unit u such that $a = ub$.

Let R be an integral domain. Then

Definition 55 (Irreducible)**.** A non-zero non-unit element $a \in R$ is called *irreducible element* if for all $b, c \in R$, $a = bc$ implies that either b or c is a unit.
a is called *reducible* if a is not irreducible.

and

Definition 56 (Prime)**.** A non-zero non-unit element $p \in R$ is called *prime* if for every $a, b \in R$, $p|ab$ implies that either $p|a$ or $p|b$.

Lecture 22

8 Jan 2025

Theorem 19. Every prime element is irreducible.

Proof. Let R be an integral domain, and let p be a prime element in R. By definition, p is prime if whenever p divides a product ab, it must divide at least one of a or b, i.e.,

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b.$$

We want to show that p is irreducible, meaning that if $p = ab$ for some $a, b \in R$, then either a or b is a unit in R.

Since $p = ab$, we apply the definition of primeness to conclude that $p \mid a$ or $p \mid b$. Without loss of generality, suppose $p \mid a$. Then, there exists some $c \in R$ such that $a = pc$. Substituting this into $p = ab$, we get:

$$p = (pc)b = p(cb).$$

Since R is an integral domain, we can cancel p, yielding $1 = cb$, which shows that b is a unit. Thus, p is irreducible. □

But every irreducible element is not prime.

22.1 Unique Factorization Domain

Definition 57. An integral domain U is a *unique factorization domain (UFD)* if every non-zero, non-unit element of U can be written as a product of irreducible elements, and this factorization is unique up to order and multiplication by units. Moreover, in a UFD, every irreducible element is also a prime element.

Let p be an element of a UFD U. Suppose p has two factorizations into irreducibles:

$$p = a_1 \cdots a_n = q_1 \cdots q_m.$$

Since U is a UFD, uniqueness of factorization implies that each a_i is a unit multiple of some q_j, meaning there exist units u_i such that

$$a_1 = u_1 q_1, \quad a_2 = u_2 q_2, \quad \ldots, \quad a_n = u_n q_n.$$

From the standard results:

$$\text{ED} \Rightarrow \text{PID} \Rightarrow \text{UFD}.$$

For example:

- $K[x, y]$ (a polynomial ring over a field K) is a UFD but not a PID.
- $\mathbb{Z}$ is an ED, and hence also a PID and a UFD.

To see that $(2, 3) = \mathbb{Z}$, observe that:

$$(2, 3) = \{2k + 3l \mid k, l \in \mathbb{Z}\}.$$

Since 1 can be written as $1 = 2(2) + 3(-1)$, it follows that $(2, 3) = (1) = \mathbb{Z}$.