MTH-204: Abstract Algebra
Lecture-1

Santosha Kumar Pattanayak

1 Definition and Examples

Definition 1. *A* **binary operation** $*$ *on a set S is a function from $S \times S$ to S. If $(a, b) \in S \times S$ then we write $a * b$ to indicate the image of the element (a, b) under the function $*$.*

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

1. *$x * (y * z) = (x * y) * z$ for all x, y, z in G.*
2. *There is an element $e \in G$ satisfying $e * x = x$ and $x * e = x$ for all x in G.*
3. *For each element x in G there is an element y in G satisfying $x * y = e$ and $y * x = e$.*

Thus, to describe a group one must specify two things:

1. a set, and
2. a binary operation on the set.

Then, one must verify that the binary operation is associative, that there is an identity in the set, and that every element in the set has an inverse.

Convention If it is clear what the binary operation is, then the group $(G, *)$ may be referred to by its *underlying set* G alone.

Examples of Groups:

1. $(\mathbb{Z}, +)$ is a group with identity 0. The inverse of $x \in \mathbb{Z}$ is $-x$.
2. $(\mathbb{Q}, +)$ is a group with identity 0. The inverse of $x \in \mathbb{Q}$ is $-x$.
3. $(\mathbb{R}, +)$ is a group with identity 0. The inverse of $x \in \mathbb{R}$ is $-x$.
4. $(\mathbb{Q} - \{0\}, \cdot)$ is a group with identity 1. The inverse of $x \in \mathbb{Q} - \{0\}$ is x^{-1}.
5. $(\mathbb{R} - \{0\}, \cdot)$ is a group with identity 1. The inverse of $x \in \mathbb{R} - \{0\}$ is x^{-1}.

6. $(\mathbb{Z}_n, +)$ is a group with identity 0, where $+$ is the addition modulo n operation, that is $x + y = r$ if the reminder when $x + y$ is divided by n is r. The inverse of $x \in \mathbb{Z}_n$ is $n - x$ if $x \neq 0$, the inverse of 0 is 0.

7. $(\mathbb{R}^n, +)$ where $+$ is vector addition. The identity is the zero vector $(0, 0, \ldots, 0)$ and the inverse of the vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is the vector $-\mathbf{x} = (-x_1, -x_2, \ldots, -x_n)$.

8. $(\mathbb{Z}_2^n, +)$ where $+$ is vector addition modulo 2 operation. The identity is the zero vector $(0, 0, \ldots, 0)$ and the inverse of the vector $\mathbf{x}$ is the vector itself.

9. $(M_2(K), +)$ where K is any one of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_n$ is a group whose identity is the zero matrix

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

and the inverse of the matrix

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

is the matrix

$$-A = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}.$$

Note that the binary operations in the above examples are all commutative. For historical reasons, there is a special name for such groups:

Definition 3. *A group $(G, *)$ is said to be* **abelian** *if $x * y = y * x$ for all x and y in G. A group is said to be* **non-abelian** *if it is not abelian.*

Examples of Non-Abelian Groups:

1. For each $n \in \mathbb{N}$, the set S_n of all permutations on $[n] = \{1, 2, \ldots, n\}$ is a group under compositions of functions. This is called the **symmetric group of degree** n. We discuss this group in detail in the next lecture. The group S_n is non-abelian if $n \geq 3$.

2. Let K be any one of $\mathbb{Q}, \mathbb{R}$ or $\mathbb{Z}_p$, where p is a prime number. Define $GL(2, K)$ to be the set of all matrices in $M_2(K)$ with non-zero determinant. Then $(GL(2, K), \cdot)$ is a group. Here $\cdot$ represents matrix multiplication. The identity of $GL(2, K)$ is the identity matrix

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

and the inverse of

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

is

$$\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}.$$

$GL(2, K)$ is called the **general linear group of degree** 2 **over** K. These groups are non-abelian. We discuss them in more detail later.

Lemma 1.1. *If $(G, *)$ is a group then:*

(a) The identity of G is unique.

(b) The inverse of each element in G is unique.

Proof. Assume that e and e' are identities of G. Then $e = e.e' = e'$.

If x and y are both inverses of some element $a \in G$, then $x.a = a.x = a.y = y.a = e$. Then $x = x.e = x.(a.y) = (x.a).y = e.y = y$.

Now we can speak of *the* identity of a group and *the* inverse of an element of a group. Since the inverse of $a \in G$ is unique, the following definition makes sense:

Definition 4. *Let $(G, *)$ be a group. Let a be any element of G. We define a^{-1} to be the inverse of a in the group G.*

The above definition is used when we think of the group's operation as being a type of multiplication or product. If instead the operation is denoted by $+$, we have instead the following definition.

Definition 5. *Let $(G, +)$ be a group. Let a be any element of G. We define $-a$ to be the inverse of a in the group G.*

Remark 1.2. *Let $(G, *)$ be a group with identity e. It is easy to check that the following hold for all elements a, b, c, d in G:*

1. *If $a * c = a * b$, then $c = b$.* [Left cancellation law for groups.]
2. *If $c * a = b * a$, then $c = b$.* [Right cancellation law for groups.]
3. *Given a and b in G there is a* unique *element x in G such that $a * x = b$.*
4. *Given a and b in G there is a* unique *element x in G such that $x * a = b$.*
5. *If $a * b = e$ then $a = b^{-1}$ and $b = a^{-1}$.* [Characterization of the inverse of an element.]
6. *If $a * b = a$ for just one a, then $b = e$.*
7. *If $b * a = a$ for just one a, then $b = e$.*
8. *If $a * a = a$, then $a = e$.* [The only idempotent in a group is the identity.]
9. $(a^{-1})^{-1} = a$.
10. $(a * b)^{-1} = b^{-1} * a^{-1}$.

Remark 1.3 (Laws of Exponents for Groups)**.** *Let $(G, *)$ be a group with identity e. Then for all $n, m \in \mathbb{Z}$ we have*

$$a^n * a^m = a^{n+m} \quad \text{for all } a \in G,$$
$$(a^n)^m = a^{nm} \quad \text{for all } a \in G,$$

and whenever $a, b \in G$ and $a * b = b * a$ we have

$$(a * b)^n = a^n * b^n.$$

MTH-204: Abstract Algebra
Lecture-2

Santosha Kumar Pattanayak

1 Symmetric Group

If n is a positive integer, we denote $[n] = \{1, 2, \ldots, n\}$. A **permutation** of $[n]$ is a one-to-one, onto function from $[n]$ to $[n]$ and S_n is the set of all permutations of $[n]$.

Let us discuss the different ways to specify a function from $[n]$ to $[n]$ and how to tell when we have a permutation. It is traditional (but not compulsory) to use lower case Greek letters such as σ, τ, α, β, etc., to indicate elements of S_n. To be specific let $n = 4$. We may define a function $\sigma : [4] \to [4]$ by specifying its values at the elements $1, 2, 3$, and 4. For example, let's say:

$$\sigma(1) = 2 \qquad \sigma(2) = 3 \qquad \sigma(3) = 1 \qquad \sigma(4) = 4.$$

Another way to specify σ is by exhibiting a table which gives its value:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}.$$

We call this the *two line* or *two row* notation. The function σ just defined is one-to-one and onto, that is, it is a permutation of [4].

For another example, let

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

The function τ is not one-to-one since $1 \neq 3$ but $\tau(1) = \tau(3)$. This problem can always be identified by the existence of the same element more than once in the second line of the two line notation. τ is also not onto since the element 2 does not appear in the second line.

Let

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

be the two line notation of an arbitrary function $\sigma : [n] \to [n]$. Then:

(1) σ is *one-to-one* if and only if no element of $[n]$ appears more than once in the second line.

(2) σ is *onto* if and only if every element of $[n]$ appears in the second line at least once.

Thus σ is a permutation if and only if the second row is just a rearrangement or shuffling of the numbers $1, 2, \ldots, n$.

The composition of two permutations:

If σ and τ are elements of S_n, then $\sigma\tau$ is defined to be the **composition** of the functions σ and τ. That is, $\sigma\tau$ is the function whose rule is given by:

$$\sigma\tau(x) = \sigma(\tau(x)), \quad \text{for all } x \in [n].$$

We sometimes call $\sigma\tau$ simply the *product* of σ and τ. Let's look at an example to see how this works. Let σ and τ be defined as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

It follows that

$$\begin{array}{rcrcrl} \sigma\tau(1) & = & \sigma(\tau(1)) & = & \sigma(2) & = 1 \\ \sigma\tau(2) & = & \sigma(\tau(2)) & = & \sigma(3) & = 3 \\ \sigma\tau(3) & = & \sigma(\tau(3)) & = & \sigma(1) & = 2 \end{array}$$

Thus we have

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

One can also find products of permutations directly from the two line notation as follows:

$$\text{First Step:} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & - & - \end{pmatrix}$$

$$\text{Second Step:} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & - \end{pmatrix}$$

$$\text{Third Step:} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Whenever we need to prove two functions are equal, we require the following definition:

Definition 1. *If $\sigma : A \to B$ and $\tau : A \to B$ are functions then $\sigma = \tau$ if and only if*

$$\sigma(x) = \tau(x), \quad \textit{for all } x \in A.$$

In particular, if σ and τ are in S_n then $\sigma = \tau$ if and only if

$$\sigma(x) = \tau(x), \quad \textit{for all } x \in [n].$$

The identity of S_n:

The identity of S_n is the so-called **identity function**

$$\iota : [n] \to [n].$$

which is defined by the rule:

$$\iota(x) = x, \quad \text{for all } x \in [n].$$

In the two line notation ι is described by

$$\iota = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

The function ι is clearly one-to-one and onto and satisfies

$$\iota\sigma = \sigma \quad \text{and} \quad \sigma\iota = \sigma, \qquad \text{for all } \sigma \in S_n.$$

So ι is the identity of S_n with respect to the binary operation of composition.

[Note that we use the Greek letter ι (iota) to indicate the identity of S_n.]

The inverse of an element $\sigma \in S_n$:

If $\sigma \in S_n$, then by definition $\sigma : [n] \to [n]$ is one-to-one and onto. Hence the rule

$$\sigma^{-1}(y) = x \quad \text{if and only if} \quad \sigma(x) = y$$

defines a function $\sigma^{-1} : [n] \to [n]$. The function σ^{-1} is also one-to-one and onto (check this!) and satisfies

$$\sigma\sigma^{-1} = \iota \qquad \text{and} \qquad \sigma^{-1}\sigma = \iota,$$

so it is the inverse of σ in the group sense also.

In terms of the two line description of a permutation, if

$$\sigma = \begin{pmatrix} \cdots & x & \cdots \\ \cdots & y & \cdots \end{pmatrix}$$

then

$$\sigma^{-1} = \begin{pmatrix} \cdots & y & \cdots \\ \cdots & x & \cdots \end{pmatrix}$$

The inverse of a permutation in the two line notation may be obtained by interchanging the two lines and then reordering the columns so that the numbers on the top line are in numerical order. Here's an example:

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

Interchanging the two lines we have:

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

Reordering the columns we obtain

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

Lemma 1.1. *For any three functions*

$$\alpha : A \to B, \quad \beta : B \to C, \quad \gamma : C \to D$$

we have

$$(\gamma\beta)\alpha = \gamma(\beta\alpha).$$

Proof Let $x \in A$. Then

$$(\gamma\beta)\alpha(x) = \gamma\beta(\alpha(x)) = \gamma(\beta(\alpha(x))).$$

and

$$\gamma(\beta\alpha)(x) = \gamma(\beta\alpha(x)) = \gamma(\beta(\alpha(x))).$$

It follows that

$$(\gamma\beta)\alpha(x) = \gamma(\beta\alpha)(x) \quad \text{for all } x \in A.$$

Hence $(\gamma\beta)\alpha = \gamma(\beta\alpha)$.

Corollary 1.2. *The binary operation of composition on S_n is associative.*

With this corollary, we complete the proof that S_n under the binary operation of composition is a group.

The Cycle Diagram of a Permutation

An important way to visualize an element σ of S_n is as follows. Arrange n dots in the plane. Number the dots 1 through n. For all $i \in [n]$, if $\sigma(i) = j$ draw an arrow from dot number i to dot number j. We call this picture the **cycle diagram** of σ. To get a nice picture, it is best to use the following technique for drawing the diagram.

1. Draw a dot and number it 1. Let $i_1 = \sigma(1)$. If $i_1 \neq 1$ draw another dot and label it i_1.
2. Draw an arrow from dot 1 to dot i_1. (Note that $i_1 = 1$ is possible.)
3. Assume that dots numbered $1, i_1, i_2, \ldots, i_k$ have been drawn. Consider two cases:
   - **(i)** There is an arrow leaving every dot drawn so far. In this case let i_{k+1} be the smallest number in $[n]$ not yet labeling a dot. If there are no such then stop, you have completed the diagram, otherwise draw a new dot and label it i_{k+1}
   - **(ii)** There is a dot numbered j with no arrow leaving it. In this case let $i_{k+1} = \sigma(j)$. If there is no dot labeled i_{k+1} draw a new dot and label it i_{k+1}. Draw an arrow from dot j to dot i_{k+1}.
4. Now repeat step 3 with $k + 1$ replacing k.

We now give a more precise definition of a "cycle".

Definition 2. *Let $i_1, i_2, \ldots, i_k$ be a list of k distinct elements from $[n]$. Define a permuation σ in S_n as follows:*

$$\begin{aligned} \sigma(i_1) &= i_2 \\ \sigma(i_2) &= i_3 \\ \sigma(i_3) &= i_4 \\ &\vdots \quad \vdots \quad \vdots \\ \sigma(i_{k-1}) &= i_k \\ \sigma(i_k) &= i_1 \end{aligned}$$

and if $x \notin \{i_1, i_2, \ldots, i_k\}$ then

$$\sigma(x) = x$$

Such a permutation is called a **cycle** *or a k-***cycle** *and is denoted by*

$$(i_1\ i_2\ \cdots\ i_k).$$

If $k = 1$ then the cycle $\sigma = (i_1)$ is just the identity function, i.e., $\sigma = \iota$.

For example, let σ be the 3-cycle defined by $\sigma = (3\ 2\ 1)$. σ may be considered as an element of S_3 in which case in two line notation we have

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

Notice that according to the definition if $x \notin \{3, 2, 1\}$ then $\sigma(x) = x$. So we could also consider (3 2 1) as an element of S_4. In which case we would have:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

Or we could consider (3 2 1) as an element of S_5. In which case we would have:

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

Similarly, (3 2 1) could be an element of S_n for any $n \geq 3$. Note also that we could specify the same permutation by any of the following

$$\sigma = (3\ 2\ 1), \quad \sigma = (2\ 1\ 3), \quad \sigma = (1\ 3\ 2).$$

In this case, there are three numbers 1, 2, 3 in the cycle, and we can begin the cycle with any one of these. In general, there are k different ways to write a k-cycle. One can start with any number in the cycle.

Definition 3. *Two cycles $(i_1\ i_2\ \cdots\ i_k)$ and $(j_1\ j_2\ \cdots\ j_\ell)$ are said to be* **disjoint** *if the sets $\{i_1, i_2, \ldots, i_k\}$ and $\{j_1, j_2, \ldots, j_\ell\}$ are disjoint.*

So, for example, the cycles (1 2 3) and (4 5 8) are disjoint, but the cycles (1 2 3) and (4 2 8) are not disjoint.

Lemma 1.3. *If σ and τ are disjoint cycles, then $\sigma\tau = \tau\sigma$.*

Proof Let $\sigma = (a_1 \cdots a_k)$ and $\tau = (b_1 \cdots b_\ell)$. Let $\{c_1, \cdots, c_m\}$ be the elements of $[n]$ that are in neither $\{a_1, \ldots, a_k\}$ nor $\{b_1, \cdots, b_\ell\}$. Thus

$$[n] = \{a_1, \ldots, a_k\} \cup \{b_1, \cdots, b_\ell\} \cup \{c_1, \cdots, c_m\}.$$

We want to show $\sigma\tau(x) = \tau\sigma(x)$ for all $x \in [n]$. To do this we consider first the case $x = a_i$ for some i. Then $a_i \notin \{b_1, \cdots, b_\ell\}$ so $\tau(a_i) = a_i$. Also $\sigma(a_i) = a_j$, where $j = i + 1$ or $j = 1$ if $i = k$. So also $\tau(a_j) = a_j$. Thus

$$\sigma\tau(a_i) = \sigma(a_i) = a_j = \tau(a_j) = \tau(\sigma(a_i) = \tau\sigma(a_i).$$

Thus, $\sigma\tau(a_i) = \tau\sigma(a_i)$. It is left to the reader to show that $\sigma\tau(x) = \tau\sigma(x)$ if $x = b_i$ or $x = c_i$, which will complete the proof.

Lemma 1.4. *Every element $\sigma \in S_n$, $n \geq 2$, can be written as a product*

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_m \tag{1}$$

where $\sigma_1, \sigma_2, \ldots, \sigma_m$ are pairwise disjoint cycles, that is, for $i \neq j$, σ_i and σ_j are disjoint. If all 1-cycles of σ are included, the factors are unique except for the order.

The factorization is called the **disjoint cycle decomposition of σ.**

To save time we omit a formal proof of this theorem. The process of finding the disjoint cycle decomposition of a permutation is quite similar to finding the cycle diagram of a permutation. Consider, for example, the permutation $\alpha \in S_{15}$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 11 & 7 & 6 & 5 & 4 & 3 & 10 & 2 & 12 & 14 & 1 & 15 & 9 & 8 \end{pmatrix}.$$

The disjoint cycle decomposition of α is

$$\alpha = (1\ 13\ 15\ 8\ 10\ 12)(2\ 11\ 14\ 9)(3\ 7)(4\ 6)(5).$$

To obtain this, one starts a cycle with 1, since $\alpha(1) = 13$ we have the partial cycle (1 13. Next, we observe that $\alpha(13) = 15$. This gives the partial cycle (1 13 15. We continue in this way till we obtain the cycle (1 13 15 8 10 12). Then we pick the smallest number in [15] not used so far, namely, 2. We start a new cycle with 2: Noting that $\alpha(2) = 11$ we have the partial cycle (2 11. Continuing we obtain the cycle (2 11 14 9). And we continue in this way till all the elements of [15] are in some cycle.

Definition 4. *An element of S_n is called a* **transposition** *if and only if it is a 2-cycle.*

Note that the transposition $(i\ j)$ interchanges i and j and leaves the other elements of $[n]$ fixed. It *transposes* i and j.

Lemma 1.5. *Every element of S_n can be written as a product of transpositions.*

Proof. We see that every cycle can be written as a product of transpositions as follows:

$$(i_1\ i_2\ i_3\ \cdots i_k) = (i_1\ i_k)\cdots(i_1\ i_3)(i_1\ i_2).$$

Then, since each permutation is a product of cycles, we can obtain each permutation as a product of transpositions. □

Proposition 1.6. *The identity permutation is a product of even number of transpositions.*

Proof. Let $id = t_1t_2\cdots t_{m-1}t_m$ where t_i's are transpositions. We need to show that m is even. Note that $m \neq 1$ as a single transposition is not the identity.

If $m = 2$ we are done.

We proceed by (strong) induction. Suppose that the theorem is true for any integer less than m, $m \geq 2$. We will show that it holds for m. Let $t_m = (a, b)$

The idea is that we will try to rewrite the permutation in such a way that we shift a as far left as possible until we eventually remove a from the permutation. The last pair of transpositions $t_{m-1}t_m$ must be one of these four cases:

$(ab)(ab), (bc)(ab), (ac)(ab), (cd)(ab)$.

If $t_{m-1}t_m = (ab)(ab) = id$, we are left with $m-2$ transpositions and by induction $m-2$ is even and so m is even.

If $t_{m-1}t_m = (bc)(ab)$, then we can replace it by $(ac)(bc)$ since $(bc)(ab) = (ac)(bc)$.

If $t_{m-1}t_m = (ac)(ab)$, then we can replace it by $(ab)(bc)$ since $(ac)(ab) = (ab)(bc)$.

If $t_{m-1}t_m = (cd)(ab)$, then we can replace it by $(ab)(cd)$ since $(cd)(ab) = (ab)(cd)$.

So we have rewritten $t_{m-1}t_m$ in such a way that a no longer occurs in the last transposition.

Successively, we rewrite the pairs $t_{m-1}t_m$, then $t_{m-2}t_{m-1}$, $t_{m-2}t_{m-1}$, and so on. Eventually, we will reach the first case above, $(ab)(ab)$, where we can cancel out two transpositions. If we don't, then the left most transposition t_1 will have the only occurrence of a. This would contradict the assumption that the permutation is the identity, because if only one transposition contains a, then the permutation does not fix a.

Once we cancel the two transpositions, then there are only $m-2$ transpositions in the permutation, and we can apply our induction hypothesis. □

Theorem 1.7. *Every element of S_n can be written as a product of transpositions. The factors of such a product are not unique, however, if $\sigma \in S_n$ can be written as a product of m transpositions and if the same σ can also be written as a product of n transpositions, then k and ℓ have the same parity.*

Proof. The first part of this theorem follows from the above lemma. If $\sigma = t_1t_2\cdots t_m = s_1s_2\cdots s_n$, where t_i and s_j are transpositions, then $id = \sigma.\sigma^{-1} = t_1t_2\cdots t_ms_ns_{n-1}\cdots s_2s_1$. Since the identity permutation is even, $m+n$ is even. So m and n are both even or both odd.

□

Definition 5. *A permutation is **even** if it is a product of an even number of transpositions and is **odd** if it is a product of an odd number of transpositions. We define the function* $\text{sign} : S_n \to \{1, -1\}$ *by*

$$\text{sign}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

*If $n = 1$ then there are no transpositions. In this case to be complete we define the identity permutation ι to be **even**.*

Remark. Let $A = [a_{ij}]$ be an $n \times n$ matrix. The determinant of A may be defined by the sum

$$\det(A) = \sum_{\sigma \in S_n} \text{sign}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}.$$

For example, if $n = 2$ we have only two permutations ι and $(1\ 2)$. Since $\text{sign}(\iota) = 1$ and $\text{sign}((1\ 2)) = -1$ we obtain

$$\det(A) = a_{11}a_{22} - a_{12}a_{21}.$$

MTH-204: Abstract Algebra
Lecture-3

Santosha Kumar Pattanayak

1 Subgroups

Definition 1. *Let $(G, *)$ be a group. A subset H of G is called a subgroup if H itself is a group with respect to $*$. More precisely, H is a subgroup of G if the restriction of $*$ to $H \times H$ is a group operation on H.*

For convenience we sometimes write $H \leq G$ to mean that H is a subgroup of G.

Examples: 1. For a group G, the subsets $\{e\}$ and G are subgroups called the trivial subgroups of G.

2. The subset $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$ for every n.

3. For $n \in \mathbb{N}$, let A_n be the set of all even permutations in the group S_n. Then A_n is a subgroup, called the alternating subgroup.

4. $SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) \mid \det(A) = 1\}$ is a subgroup of $GL(n, \mathbb{R})$.

Definition 2. *Let a be an element of the group G. If there exists $n \in \mathbb{N}$ such that $a^n = e$ we say that a has **finite order**. and we define*

$$\mathrm{o}(a) = \min\{n \in \mathbb{N} \mid a^n = e\}$$

*If $a^n \neq e$ for all $n \in \mathbb{N}$, we say that a has **infinite order** and we define*

$$\mathrm{o}(a) = \infty.$$

*In either case we call $\mathrm{o}(a)$ the **order** of a.*

Definition 3. *Let a be an element of the group G. Define*

$$\langle a \rangle = \{a^i : i \in \mathbb{Z}\}.$$

*We call $\langle a \rangle$ the **subgroup of G generated by a**.*

Remark Note that

$$\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \ldots\}.$$

In particular, $a = a^1$ and $e = a^0$ are in $\langle a \rangle$.

Lemma 1.1. *If G is a finite group, then every element of G has finite order.*

Proof Let a be any element of G. Consider the infinite list

$$a^1, a^2, a^3, \ldots, a^i, \ldots$$

of elements in G. Since G is finite, all the elements in the list cannot be different. So there must be positive integers $i < j$ such that $a^i = a^j$. Since $i < j$, $j - i$ is a positive integer. Then we have

$$a^{j-i} = a^{j+(-i)} = a^j a^{-i} = a^i a^{-i} = a^0 = e.$$

That is, $a^n = e$ for the positive integer $n = j - i$. So a has finite order, which is what we wanted to prove.

Theorem 1.2. *Let G be an arbitrary group, $x \in G$, and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$, where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x| \mid m$.*

Proof. By the Euclidean algorithm, there exist integers r and s such that $d = mr + ns$. We have

$$x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1.$$

This proves our first claim.

Next, let $n = |x|$ and $x^m = 1$. We have x^d=1, where $d = (|x|, m)$. Note that $0 < d \leq |x|$ and $|x|$ is the smallest positive integer k such that $x^k = 1$. This implies that $d = |x|$ and $|x| = (|x|, m)$. Thus, $|x| \mid m$. □

Lemma 1.3. *For G a group, any non empty subset H of G is a subgroup of G if and only if for every $a, b \in H$ we have $ab^{-1} \in H$.*

Proof. If $H \leq G$, the two given statements clearly hold as H contains the identity of G and is closed under inverses and multiplication.

To prove the converse, let x be any element of H (which exists as $H \neq \emptyset$). We have $xx^{-1} \in H \implies 1 \in H$. As H contains 1, for any element h of H, H contains $1h^{-1} = h^{-1}$, that is, it is closed under inverses. For any x and y in H, as $y^{-1} \in H$, we have that $x(y^{-1})^{-1} = xy \in H$, that is, H is closed under multiplication.

To prove the second part, we see that $x, x^2, x^3, \ldots \in H$ for any $x \in H$. Using above Lemma, we see that x is of finite order n. Then $x^{-1} = x^{n-1} \in H$ so H is closed under inverses. □

Lemma 1.4. *Let $H = \langle x \rangle$. Then $|H| = |x|$ (where if one side of the inequality is infinite, so is the other).*

Proof. This proof is trivial. □

Proposition 1.5. *Consider a group G, and a family of its subgroups H_i, $i \in I$. Then $\bigcap_{i \in I} H_i$ is a subgroup of G. Not always $\bigcup_{i \in I} H_i$ is a subgroup of G.*

Proof. If $a, b \in \bigcap_{i \in I} H_i$, then $a, b \in H_i$ for all i. Since H_i is a subgroup, we have $ab^{-1} \in H_i$ for all i. So $ab^{-1} \in \bigcap_{i \in I} H_i$. So $\bigcap_{i \in I} H_i$ is a subgroup of G. Consider $3\mathbb{Z}$ and $5\mathbb{Z}$ with the operation of addition: their union is not a subgroup of $\mathbb{Z}$, because for example $8 \notin 3\mathbb{Z} \cup 5\mathbb{Z}$. □

We now introduce some important subgroups.

Definition 1.6. *Let G be a group and A be any nonempty subset of A. Define*

$$C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}.$$

This subset is called the centralizer of A in G.

Since $gag^{-1} = g$ if and only if $ga = ag$, $C_G(A)$ is the set of all elements that commute with every element of A.

Now observe that $C_G(A)$ is a subgroup of G as first of all, $1 \in C_G(A)$ so $C_G(A) \neq \emptyset$, and second of all, if $x, y \in C_G(A)$, we have $xax^{-1} = a$ and $yay^{-1} = a$, that is, $y^{-1}ay = a$ for all $a \in A$. We then have $a = xax^{-1} = x(y^{-1}ay)x^{-1} = (xy^{-1})a(xy^{-1})^{-1}$ so $xy^{-1} \in C_G(A)$. Thus, $C_G(A) \leq G$.

Definition 1.7. *Let G be a group. Define*

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$

This subset is called the center of G.

$Z(G)$ is the set of all elements that commute with every element of G.

As $Z(G) = C_G(G)$, we have $Z(G) \leq G$.

Definition 1.8. *Let G be a group and A be a subset of G. Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Define*

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}.$$

This set is called the normalizer of A in G.

The proof that $N_G(A) \leq G$ is similar to that we used to prove that $C_G(A) \leq G$.

Note that $C_G(A) \leq N_G(A)$.

If G is an abelian group, $Z(G) = G$. Further, for any subset A of G, $N_G(A) = C_G(A) = G$ as $gag^{-1} = gg^{-1}a = a$ for all $a \in A, g \in G$.

MTH-204: Abstract Algebra
Lecture-4

Santosha Kumar Pattanayak

1 Cosets and Lagrange's Theorem

Lagrange's Theorem, one of the most important results in finite group theory, states that the order of a subgroup must divide the order of the group. This theorem provides a powerful tool for analyzing finite groups; it gives us an idea of exactly what type of subgroups we might expect a finite group to possess. Central to understanding Lagranges's Theorem is the notion of a coset.

2 Cosets

Let G be a group and H a subgroup of G. Define a **left coset** of H with representative $g \in G$ to be the set

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

Right cosets can be defined similarly by

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

If left and right cosets coincide or if it is clear from the context to which type of coset that we are referring, we will use the word *coset* without specifying left or right.

Example 1. Let H be the subgroup of $\mathbb{Z}_6$ consisting of the elements 0 and 3. The cosets are

$$\begin{aligned} 0 + H = 3 + H &= \{0, 3\} \\ 1 + H = 4 + H &= \{1, 4\} \\ 2 + H = 5 + H &= \{2, 5\}. \end{aligned}$$

We will always write the cosets of subgroups of $\mathbb{Z}$ and $\mathbb{Z}_n$ with the additive notation we have used for cosets here. In a commutative group, left and right cosets are always identical. ■

Example 2. Let H be the subgroup of S_3 defined by the permutations $\{(1), (123), (132)\}$. The left cosets of H are

$$\begin{aligned} (1)H = (123)H = (132)H &= \{(1), (123), (132)\} \\ (12)H = (13)H = (23)H &= \{(12), (13), (23)\}. \end{aligned}$$

The right cosets of H are exactly the same as the left cosets:

$$H(1) = H(123) = H(132) = \{(1), (123), (132)\}$$
$$H(12) = H(13) = H(23) = \{(12), (13), (23)\}.$$

It is not always the case that a left coset is the same as a right coset. Let K be the subgroup of S_3 defined by the permutations $\{(1), (12)\}$. Then the left cosets of K are

$$(1)K = (12)K = \{(1), (12)\}$$
$$(13)K = (123)K = \{(13), (123)\}$$
$$(23)K = (132)K = \{(23), (132)\};$$

however, the right cosets of K are

$$K(1) = K(12) = \{(1), (12)\}$$
$$K(13) = K(132) = \{(13), (132)\}$$
$$K(23) = K(123) = \{(23), (123)\}.$$

■

The following lemma is quite useful when dealing with cosets and the proof is easy.

Lemma 2.1. *Let H be a subgroup of a group G and suppose that $g_1, g_2 \in G$. The following conditions are equivalent.*

1. $g_1 H = g_2 H$;
2. $H g_1^{-1} = H g_2^{-1}$;
3. $g_1 H \subseteq g_2 H$;
4. $g_2 \in g_1 H$;
5. $g_1^{-1} g_2 \in H$.

In all of our examples the cosets of a subgroup H partition the larger group G. The following theorem proclaims that this will always be the case.

Theorem 2.2. *Let H be a subgroup of a group G. Then the left cosets of H in G partition G. That is, the group G is the disjoint union of the left cosets of H in G.*

Proof. Let $g_1 H$ and $g_2 H$ be two cosets of H in G. We must show that either $g_1 H \cap g_2 H = \emptyset$ or $g_1 H = g_2 H$. Suppose that $g_1 H \cap g_2 H \neq \emptyset$ and $a \in g_1 H \cap g_2 H$. Then by the definition of a left coset, $a = g_1 h_1 = g_2 h_2$ for some elements h_1 and h_2 in H. Hence, $g_1 = g_2 h_2 h_1^{-1}$ or $g_1 \in g_2 H$. By Lemma 2.1, $g_1 H = g_2 H$. □

Remark. The above theorem can also be proved in the following way. Define a relation R on G by xRy if $x^{-1}y \in H$. It is easy to check that R is an equivalence relation on G and the equivalence classes are nothing but the left cosets of H. We have $[x] = \{y \in G : xRy\} = \{y \in G : x^{-1}y \in H\} = \{y \in G : y \in xH\} = xH$. Since the equivalences classes partition the set, we get that G is the disjoint union of the left cosets of H in G.

Remark. There is nothing special in this theorem about left cosets. Right cosets also partition G; the proof of this fact is exactly the same as the proof for left cosets except that all group multiplications are done on the opposite side of H.

Let G be a group and H be a subgroup of G. Define the **Index** H in G to be the number of left cosets of H in G. We will denote the index by $[G : H]$.

Example 3. Let $G = \mathbb{Z}_6$ and $H = \{0, 3\}$. Then $[G : H] = 3$. ■

Example 4. Suppose that $G = S_3$, $H = \{(1), (123), (132)\}$, and $K = \{(1), (12)\}$. Then $[G : H] = 2$ and $[G : K] = 3$. ■

Theorem 2.3. *Let H be a subgroup of a group G. The number of left cosets of H in G is the same as the number of right cosets of H in G.*

Proof. Let $\mathcal{L}_H$ and $\mathcal{R}_H$ denote the set of left and right cosets of H in G, respectively. If we can define a bijective map $\phi : \mathcal{L}_H \to \mathcal{R}_H$, then the theorem will be proved. If $gH \in \mathcal{L}_H$, let $\phi(gH) = Hg^{-1}$. By Lemma 2.1, the map ϕ is well-defined; that is, if $g_1H = g_2H$, then $Hg_1^{-1} = Hg_2^{-1}$. To show that ϕ is one-to-one, suppose that

$$Hg_1^{-1} = \phi(g_1H) = \phi(g_2H) = Hg_2^{-1}.$$

Again by Lemma 5.1, $g_1H = g_2H$. The map ϕ is onto since $\phi(g^{-1}H) = Hg$. □

3 Lagrange's Theorem

Proposition 3.1. *Let H be a subgroup of G with $g \in G$ and define a map $\phi : H \to gH$ by $\phi(h) = gh$. The map ϕ is bijective; hence, the number of elements in H is the same as the number of elements in gH.*

Proof. We first show that the map ϕ is one-to-one. Suppose that $\phi(h_1) = \phi(h_2)$ for elements $h_1, h_2 \in H$. We must show that $h_1 = h_2$, but $\phi(h_1) = gh_1$ and $\phi(h_2) = gh_2$. So $gh_1 = gh_2$, and by left cancellation $h_1 = h_2$. To show that ϕ is onto is easy. By definition every element of gH is of the form gh for some $h \in H$ and $\phi(h) = gh$. □

Theorem 3.2 (Lagrange)**.** *Let G be a finite group and let H be a subgroup of G. Then $|G|/|H| = [G : H]$ is the number of distinct left cosets of H in G. In particular, the number of elements in H must divide the number of elements in G.*

Proof. The group G is partitioned into $[G : H]$ distinct left cosets. Each left coset has $|H|$ elements; therefore, $|G| = [G : H]|H|$. □

Corollary 3.3. *Suppose that G is a finite group and $g \in G$. Then the order of g must divide the number of elements in G. In particular $a^{|G|} = e$ for every $a \in G$.*

Proof. Let $H = \langle g \rangle$. Then $|H| = o(g)$ and by Lagrange's theorem $o(g)$ divides $|G|$.

□

Corollary 3.4. *Let $|G| = p$ with p a prime number. Then G is cyclic and any $g \in G$ such that $g \neq e$ is a generator.*

Proof. Let g be in G such that $g \neq e$. Then by Corollary 3.3, the order of g must divide the order of the group. Since $|\langle g \rangle| > 1$, it must be p. Hence, g generates G. □

Corollary 3.4 suggests that groups of prime order p must somehow look like $\mathbb{Z}_p$.

Corollary 3.5. *Let H and K be subgroups of a finite group G such that $G \supset H \supset K$. Then*

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

Proof. Observe that

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

□

The converse of Lagrange's Theorem is false. The group A_4 has order 12; however, it can be shown that it does not possess a subgroup of order 6. According to Lagrange's Theorem, subgroups of a group of order 12 can have orders of either 1, 2, 3, 4, or 6. However, we are not guaranteed that subgroups of every possible order exist. To prove that A_4 has no subgroup of order 6, we will assume that it does have a subgroup H such that $|H| = 6$ and show that a contradiction must occur. The group A_4 contains eight 3-cycles; hence, H must contain a 3-cycle. We will show that if H contains one 3-cycle, then it must contain every 3-cycle, contradicting the assumption that H has only 6 elements.

Theorem 3.6. *Two cycles τ and μ in S_n have the same length if and only if there exists a $\sigma \in S_n$ such that $\mu = \sigma\tau\sigma^{-1}$.*

Proof. Suppose that

$$\begin{aligned} \tau &= (a_1, a_2, \ldots, a_k) \\ \mu &= (b_1, b_2, \ldots, b_k). \end{aligned}$$

Define σ to be the permutation

$$\begin{aligned} \sigma(a_1) &= b_1 \\ \sigma(a_2) &= b_2 \\ &\vdots \\ \sigma(a_k) &= b_k. \end{aligned}$$

Then $\mu = \sigma\tau\sigma^{-1}$.

Conversely, suppose that $\tau = (a_1, a_2, \ldots, a_k)$ is a k-cycle and $\sigma \in S_n$. If $\sigma(a_i) = b$ and $\sigma(a_{(i \bmod k)+1}) = b'$, then $\mu(b) = b'$. Hence,

$$\mu = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k)).$$

Since σ is one-to-one and onto, μ is a cycle of the same length as τ. □

Corollary 3.7. *The group A_4 has no subgroup of order 6.*

Proof. Since $[A_4 : H] = 2$, there are only two cosets of H in A_4. In as much as one of the cosets is H itself, right and left cosets must coincide; therefore, $gH = Hg$ or $gHg^{-1} = H$ for every $g \in A_4$. By above theorem, if H contains one 3-cycle, then it must contain every 3-cycle, contradicting the order of H. □

4 Fermat's and Euler's Theorems

The **Euler ϕ-function** is the map $\phi : \mathbb{N} \to \mathbb{N}$ defined by $\phi(n) = 1$ for $n = 1$, and, for $n > 1$, $\phi(n)$ is the number of positive integers m with $1 \leq m < n$ and $\gcd(m, n) = 1$.

Recall that $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ is a group with respect to the binary operation addition modulo n. Note that multiplication modulo n is also a binary operation on $\mathbb{Z}_n$ and with respect to this operation we say that a nonzero element a is a unit (or has an inverse) if there exists $b \in \mathbb{Z}_n$ such that $ab \equiv 1 \ mod \ n$. If n is not a prime, not all nonzero element in $\mathbb{Z}_n$ is a unit. For example in $\mathbb{Z}_9$, 4 is a unit as $4.7 \equiv 1 \ mod \ 9$ whereas 6 is not a unit.

It is easy to check that the set of all units in $\mathbb{Z}_n$ is a group under multiplication modulo n. We will denote this group by $U(n)$. Let $r \in \mathbb{Z}_n$ such that r is coprime to n. Then there exists integers q and t such that $qr + tn = 1$. Then $qr \equiv 1 \ mod \ n$ and hence r is a unit in $\mathbb{Z}_n$. So $U(n) = \{r \in \mathbb{N} : r < n \ and \ (r, n) = 1\}$ and hence $|U(n)| = \phi(n)$.

So we proved the following theorem:

Theorem 4.1. *Let $U(n)$ be the group of units in $\mathbb{Z}_n$. Then $|U(n)| = \phi(n)$.*

For example, $|U(12)| = \phi(12) = 4$ since the numbers that are relatively prime to 12 are 1, 5, 7, and 11. For any prime p, $\phi(p) = p - 1$.

The following theorem is an important result in number theory, due to Leonhard Euler.

Theorem 4.2 (Euler's Theorem)**.** *Let a and n be integers such that $n > 0$ and $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Proof. The order of the group $U(n)$ is $\phi(n)$. Consequently, $a^{\phi(n)} = 1$ for all $a \in U(n)$; or $a^{\phi(n)} - 1$ is divisible by n. Therefore, $a^{\phi(n)} \equiv 1 \pmod{n}$. □

If we consider the special case of Euler's Theorem in which $n = p$ is prime and recall that $\phi(p) = p - 1$, we obtain the following result, due to Pierre de Fermat.

Theorem 4.3 (Fermat's Little Theorem)**.** *Let p be any prime number and suppose that $p \nmid a$. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for any integer b, $b^p \equiv b \pmod{p}$.

MTH-204: Abstract Algebra
Lecture-5

Santosha Kumar Pattanayak

1 Normal Subgroups and Factor Groups

If H is a subgroup of a group G, then right cosets are not always the same as left cosets; that is, it is not always the case that $gH = Hg$ for all $g \in G$. The subgroups for which this property holds play a critical role in group theory: they allow for the construction of a new class of groups, called factor or quotient groups.

Normal Subgroups

A subgroup H of a group G is normal in G if $gH = Hg$ for all $g \in G$. That is, a normal subgroup of a group G is one in which the right and left cosets are precisely the same.

Example 1. Let G be an abelian group. Every subgroup H of G is a normal subgroup. Since $gh = hg$ for all $g \in G$ and $h \in H$, it will always be the case that $gH = Hg$. ■

Example 2. Let H be the subgroup of S_3 consisting of elements (1) and (12). Since

$$(123)H = \{(123), (13)\}$$

and

$$H(123) = \{(123), (23)\},$$

H cannot be a normal subgroup of S_3. However, the subgroup N, consisting of the permutations (1), (123), and (132), is normal since the cosets of N are

$$N = \{(1), (123), (132)\}$$
$$(12)N = N(12) = \{(12), (13), (23)\}.$$

■

The following theorem is fundamental to our understanding of normal subgroups.

Theorem 1.1. *Let G be a group and N be a subgroup of G. Then the following statements are equivalent.*

1. *The subgroup N is normal in G.*

2. *For all* $g \in G$, $gNg^{-1} \subset N$.

3. *For all* $g \in G$, $gNg^{-1} = N$.

Proof. (1) $\Rightarrow$ (2). Since N is normal in G, $gN = Ng$ for all $g \in G$. Hence, for a given $g \in G$ and $n \in N$, there exists an n' in N such that $gn = n'g$. Therefore, $gng^{-1} = n' \in N$ or $gNg^{-1} \subset N$.

(2) $\Rightarrow$ (3). Let $g \in G$. Since $gNg^{-1} \subset N$, we need only show $N \subset gNg^{-1}$. For $n \in N$, $g^{-1}ng = g^{-1}n(g^{-1})^{-1} \in N$. Hence, $g^{-1}ng = n'$ for some $n' \in N$. Therefore, $n = gn'g^{-1}$ is in gNg^{-1}.

(3) $\Rightarrow$ (1). Suppose that $gNg^{-1} = N$ for all $g \in G$. Then for any $n \in N$ there exists an $n' \in N$ such that $gng^{-1} = n'$. Consequently, $gn = n'g$ or $gN \subset Ng$. Similarly, $Ng \subset gN$. □

Factor Groups

If N is a normal subgroup of a group G, then the cosets of N in G form a group G/N under the operation $(aN)(bN) = abN$. This group is called the quotient group of G and N. Our first task is to prove that G/N is indeed a group.

Theorem 1.2. *Let N be a normal subgroup of a group G. The cosets of N in G form a group G/N of order $[G : N]$.*

Proof. The group operation on G/N is $(aN)(bN) = abN$. This operation must be shown to be well-defined; that is, group multiplication must be independent of the choice of coset representative. Let $aN = bN$ and $cN = dN$. We must show that

$$(aN)(cN) = acN = bdN = (bN)(dN).$$

Then $a = bn_1$ and $c = dn_2$ for some n_1 and n_2 in N. Hence,

$$\begin{aligned} acN &= bn_1dn_2N \\ &= bn_1dN \\ &= bn_1Nd \\ &= bNd \\ &= bdN. \end{aligned}$$

The remainder of the theorem is easy: $eN = N$ is the identity and $g^{-1}N$ is the inverse of gN. The order of G/N is, of course, the number of cosets of N in G. □

It is very important to remember that the elements in a factor group are *sets of elements* in the original group.

Example 3. Consider the normal subgroup of S_3, $N = \{(1), (123), (132)\}$. The cosets of N in S_3 are N and $(12)N$. The factor group S_3/N has the following multiplication table.

	N	$(12)N$
N	N	$(12)N$
$(12)N$	$(12)N$	N

This group is isomorphic to $\mathbb{Z}_2$. At first, multiplying cosets seems both complicated and strange; however, notice that S_3/N is a smaller group. The factor group displays a certain amount of information about S_3. Actually, $N = A_3$, the group of even permutations, and $(12)N = \{(12), (13), (23)\}$ is the set of odd permutations. The information captured in G/N is parity; that is, multiplying two even or two odd permutations results in an even permutation, whereas multiplying an odd permutation by an even permutation yields an odd permutation. ■

Example 4. Consider the normal subgroup $3\mathbb{Z}$ of $\mathbb{Z}$. The cosets of $3\mathbb{Z}$ in $\mathbb{Z}$ are

$$\begin{aligned} 0 + 3\mathbb{Z} &= \{\ldots, -3, 0, 3, 6, \ldots\} \\ 1 + 3\mathbb{Z} &= \{\ldots, -2, 1, 4, 7, \ldots\} \\ 2 + 3\mathbb{Z} &= \{\ldots, -1, 2, 5, 8, \ldots\}. \end{aligned}$$

The group $\mathbb{Z}/3\mathbb{Z}$ is given by the multiplication table below.

$+$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$0+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$1+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$
$2+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$

In general, the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ is normal. The cosets of $\mathbb{Z}/n\mathbb{Z}$ are

$$\begin{gathered} n\mathbb{Z} \\ 1 + n\mathbb{Z} \\ 2 + n\mathbb{Z} \\ \vdots \\ (n-1) + n\mathbb{Z}. \end{gathered}$$

The sum of the cosets $k+\mathbb{Z}$ and $l+\mathbb{Z}$ is $k+l+\mathbb{Z}$. Notice that we have written our cosets additively, because the group operation is integer addition. ■

Example 5. Consider the dihedral group D_n, generated by the two elements r and s, satisfying the relations

$$\begin{aligned} r^n &= id \\ s^2 &= id \\ srs &= r^{-1}. \end{aligned}$$

The element r actually generates the cyclic subgroup of rotations, R_n, of D_n. Since $srs^{-1} = srs = r^{-1} \in R_n$, the group of rotations is a normal subgroup of D_n; therefore, D_n/R_n is a group. Since there are exactly two elements in this group, it must be isomorphic to $\mathbb{Z}_2$. ■

Let G be a group and H,K are two subgroups of G. We define the product of H and K by $HK = \{hk : h \in H, k \in K\}$. Then HK need not be a subgroup of G. For example let $G = S_3$, $H = \{e, (1,2)\}$ and $K = \{e, (2,3)\}$. Then HK has exactly 4 elements and by Lagrange's theorem HK can not be a subgroup of S_3.

However, if one of them is a normal subgroup then their product is a subgroup.

Theorem 1.3. *Let H be a subgroup of a group G (not necessarily normal in G) and N a normal subgroup of G. Then HN is a subgroup of G and $H \cap N$ is a normal subgroup of H.*

Proof. We will first show that $HN = \{hn : h \in H, n \in N\}$ is a subgroup of G. Suppose that $h_1n_1, h_2n_2 \in HN$. Since N is normal, $(h_2)^{-1}n_1h_2 \in N$. So

$$(h_1n_1)(h_2n_2) = h_1h_2((h_2)^{-1}n_1h_2)n_2$$

is in HN. The inverse of $hn \in HN$ is in HN since

$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1}).$$

Next, we prove that $H \cap N$ is normal in H. Let $h \in H$ and $n \in H \cap N$. Then $h^{-1}nh \in H$ since each element is in H. Also, $h^{-1}nh \in N$ since N is normal in G; therefore, $h^{-1}nh \in H \cap N$. □

Theorem 1.4. *Let H and K be two subgroups of a group G. Then $|HK| = \frac{|H||K|}{|H \cap K|}$.*

Proof. Certainly the set HK has $|H||K|$ symbols. However, not all symbols need represent distinct group elements. That is, we may have $hk = h'k'$ although $h \neq h'$ and $k \neq k'$. We must determine the extent to which this happens.

For every $t \in H \cap K$, $hk = (ht)(t^{-1}k)$, so each group element in HK is represented by at least $|H \cap K|$ products in HK.

But $hk = h'k'$ implies $t = h^{-1}h' = k(k')^{-1} \in H \cap K$ so that $h' = ht$ and $k' = t^{-1}k$. Thus each element in HK is represented by exactly $|H \cap K|$ products. So,

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

□

Remark: Alternate Proof: We will see the following outlined proof when we study about group actions.

The group $H \times K$ acts on the set $HK \subseteq G$ via $(h, k)x := hxk^{-1}$. The action is transitive. The stabilizer of $1 \in HK$ is easily seen to be isomorphic to $H \cap K$. Then the orbit-stabilizer theorem implies that $|HK| \cdot |H \cap K| = |H \times K| = |H| \cdot |K|$.

This proof also works when H, K are infinite.

MTH-204: Abstract Algebra
Lecture-6

Santosha Kumar Pattanayak

1 Group Homomorphisms

A **homomorphism** between groups $(G, \cdot)$ and $(H, \circ)$ is a map $\phi : G \to H$ such that

$$\phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2)$$

for $g_1, g_2 \in G$. The range of ϕ in H is called the **homomorphic image** of ϕ.

A homomorphism $\phi : G \to H$ is called an isomorphism if ϕ is a bijection between G and H.

Two groups are related in the strongest possible way if they are isomorphic; however, a weaker relationship may exist between two groups. For example, the symmetric group S_n and the group $\mathbb{Z}_2$ are related by the fact that S_n can be divided into even and odd permutations that exhibit a group structure like that $\mathbb{Z}_2$, as shown in the following multiplication table.

	even	odd
even	even	odd
odd	odd	even

We use homomorphisms to study relationships such as the one we have just described.

Example: Let G be a group and $g \in G$. Define a map $\phi : \mathbb{Z} \to G$ by $\phi(n) = g^n$. Then ϕ is a group homomorphism, since

$$\phi(m + n) = g^{m+n} = g^m g^n = \phi(m)\phi(n).$$

This homomorphism maps $\mathbb{Z}$ onto the cyclic subgroup of G generated by g. ■

Example: Let $G = GL_2(\mathbb{R})$. If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in G, then the determinant is nonzero; that is, $\det(A) = ad - bc \neq 0$. Also, for any two elements A and B in G, $\det(AB) = \det(A)\det(B)$. Using the determinant, we can define a homomorphism $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ by $A \mapsto \det(A)$. ■

Example: Recall that the circle group $\mathbb{T}$ consists of all complex numbers z such that $|z| = 1$. We can define a homomorphism ϕ from the additive group of real numbers $\mathbb{R}$ to $\mathbb{T}$ by $\phi : \theta \mapsto$

$\cos\theta + i\sin\theta$. Indeed,

$$\begin{aligned}\phi(\alpha+\beta) &= \cos(\alpha+\beta) + i\sin(\alpha+\beta)\\ &= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta)\\ &= (\cos\alpha + i\sin\alpha) + (\cos\beta + i\sin\beta)\\ &= \phi(\alpha)\phi(\beta).\end{aligned}$$

Geometrically, we are simply wrapping the real line around the circle in a group-theoretic fashion. ■

Example: The map $sign : S_n \to \{1, -1\}$ is a homomorphism, as $sign(\sigma.\tau) = sign(\sigma).sign(\tau)$.

Many groups may appear to be different at first glance, but can be shown to be the same by a simple renaming of the group elements. For example, $\mathbb{Z}_4$ and the subgroup of the circle group $\mathbb{T}$ generated by i can be shown to be the same by demonstrating a one-to-one correspondence between the elements of the two groups and between the group operations. In such a case we say that the groups are isomorphic.

Example: To show that $\mathbb{Z}_4 \cong \langle i\rangle$, define a map $\phi : \mathbb{Z}_4 \to \langle i\rangle$ by $\phi(n) = i^n$. We must show that ϕ is bijective and preserves the group operation. The map ϕ is one-to-one and onto because

$$\begin{aligned}\phi(0) &= 1\\ \phi(1) &= i\\ \phi(2) &= -1\\ \phi(3) &= -i.\end{aligned}$$

Since

$$\phi(m+n) = i^{m+n} = i^m i^n = \phi(m)\phi(n),$$

the group operation is preserved. ■

Example: $log : \mathbb{R}^+ \to \mathbb{R}$ where $\mathbb{R}^+$ denotes the positive real numbers with the operation multiplication, is an isomorphism since from calculus we know that log is one to one and onto and $log(xy) = logx + logy$ for all positive real numbers x and y.

Example: We can define an isomorphism ϕ from the additive group of real numbers $(\mathbb{R}, +)$ to the multiplicative group of positive real numbers $(\mathbb{R}^+, \cdot)$ with the exponential map; that is,

$$\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y).$$

Of course, we must still show that ϕ is one-to-one and onto, but this can be determined using calculus. ■

Example: The integers are isomorphic to the subgroup of $\mathbb{Q}^*$ consisting of elements of the form 2^n. Define a map $\phi : \mathbb{Z} \to \mathbb{Q}^*$ by $\phi(n) = 2^n$. Then

$$\phi(m+n) = 2^{m+n} = 2^m 2^n = \phi(m)\phi(n).$$

By definition the map ϕ is onto the subset $\{2^n : n \in \mathbb{Z}\}$ of $\mathbb{Q}^*$. To show that the map is injective, assume that $m \neq n$. If we can show that $\phi(m) \neq \phi(n)$, then we are done. Suppose that $m > n$ and assume that $\phi(m) = \phi(n)$. Then $2^m = 2^n$ or $2^{m-n} = 1$, which is impossible since $m - n > 0$. ■

Example: The groups $\mathbb{Z}_8$ and $\mathbb{Z}_{12}$ cannot be isomorphic since they have different orders; however, it is true that $U(8) \cong U(12)$. We know that

$$\begin{aligned} U(8) &= \{1, 3, 5, 7\} \\ U(12) &= \{1, 5, 7, 11\}. \end{aligned}$$

An isomorphism $\phi : U(8) \to U(12)$ is then given by

$$\begin{aligned} 1 &\mapsto 1 \\ 3 &\mapsto 5 \\ 5 &\mapsto 7 \\ 7 &\mapsto 11. \end{aligned}$$

The map ϕ is not the only possible isomorphism between these two groups. We could define another isomorphism ψ by $\psi(1) = 1$, $\psi(3) = 11$, $\psi(5) = 5$, $\psi(7) = 7$. In fact, both of these groups are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ ■

Example: Even though S_3 and $\mathbb{Z}_6$ possess the same number of elements, we would suspect that they are not isomorphic, because $\mathbb{Z}_6$ is abelian and S_3 is nonabelian. To demonstrate that this is indeed the case, suppose that $\phi : \mathbb{Z}_6 \to S_3$ is an isomorphism. Let $a, b \in S_3$ be two elements such that $ab \neq ba$. Since ϕ is an isomorphism, there exist elements m and n in $\mathbb{Z}_6$ such that

$$\begin{aligned} \phi(m) &= a \\ \phi(n) &= b. \end{aligned}$$

However,

$$ab = \phi(m)\phi(n) = \phi(m + n) = \phi(n + m) = \phi(n)\phi(m) = ba,$$

which contradicts the fact that a and b do not commute. ■

Theorem 1.1. *Let $\phi : G \to H$ be an isomorphism of two groups. Then the following statements are true.*

1. *$\phi^{-1} : H \to G$ is an isomorphism.*
2. *$|G| = |H|$.*
3. *If G is abelian, then H is abelian.*
4. *If G is cyclic, then H is cyclic.*
5. *If G has a subgroup of order n, then H has a subgroup of order n.*

Proof. Assertions (1) and (2) follow from the fact that ϕ is a bijection. We will prove (3) here and proofs of the others are similar.

(3) Suppose that h_1 and h_2 are elements of H. Since ϕ is onto, there exist elements $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Therefore,

$$h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2) = \phi(g_2g_1) = \phi(g_2)\phi(g_1) = h_2h_1.$$

□

The following proposition lists some basic properties of group homomorphisms.

Proposition 1.2. *Let $\phi : G_1 \to G_2$ be a homomorphism of groups. Then*

1. *If e is the identity of G_1, then $\phi(e)$ is the identity of G_2;*
2. *For any element $g \in G_1$, $\phi(g^{-1}) = [\phi(g)]^{-1}$;*
3. *If H_1 is a subgroup of G_1, then $\phi(H_1)$ is a subgroup of G_2;*
4. *If H_2 is a subgroup of G_2, then $\phi^{-1}(H_2) = \{g \in G : \phi(g) \in H_2\}$ is a subgroup of G_1. Furthermore, if H_2 is normal in G_2, then $\phi^{-1}(H_2)$ is normal in G_1.*

Proof. (1) Suppose that e and e' are the identities of G_1 and G_2, respectively; then

$$e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e).$$

By cancellation, $\phi(e) = e'$.

(2) This statement follows from the fact that

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

(3) The set $\phi(H_1)$ is nonempty since the identity of H_2 is in $\phi(H_1)$. Suppose that H_1 is a subgroup of G_1 and let x and y be in $\phi(H_1)$. There exist elements $a, b \in H_1$ such that $\phi(a) = x$ and $\phi(b) = y$. Since

$$xy^{-1} = \phi(a)[\phi(b)]^{-1} = \phi(ab^{-1}) \in \phi(H_1),$$

$\phi(H_1)$ is a subgroup of G_2.

(4) Let H_2 be a subgroup of G_2 and define H_1 to be $\phi^{-1}(H_2)$; that is, H_1 is the set of all $g \in G_1$ such that $\phi(g) \in H_2$. The identity is in H_1 since $\phi(e) = e$. If a and b are in H_1, then $\phi(ab^{-1}) = \phi(a)[\phi(b)]^{-1}$ is in H_2 since H_2 is a subgroup of G_2. Therefore, $ab^{-1} \in H_1$ and H_1 is a subgroup of G_1. If H_2 is normal in G_2, we must show that $g^{-1}hg \in H_1$ for $h \in H_1$ and $g \in G_1$. But

$$\phi(g^{-1}hg) = [\phi(g)]^{-1}\phi(h)\phi(g) \in H_2,$$

since H_2 is a normal subgroup of G_2. Therefore, $g^{-1}hg \in H_1$. □

Let $\phi : G \to H$ be a group homomorphism and suppose that e is the identity of H. Then $\phi^{-1}(\{e\})$ is a subgroup of G. This subgroup is called the **kernel** of ϕ and will be denoted by $\ker \phi$. In fact, this subgroup is a normal subgroup of G since the trivial subgroup is normal in H. We state this result in the following theorem, which says that with every homomorphism of groups we can naturally associate a normal subgroup.

Theorem 1.3. *Let $\phi : G \to H$ be a group homomorphism. Then the kernel of ϕ is a normal subgroup of G.*

Example 9. Let us examine the homomorphism $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ defined by $A \mapsto \det(A)$. Since 1 is the identity of $\mathbb{R}^*$, the kernel of this homomorphism is all 2×2 matrices having determinant one. That is, $\ker \phi = SL_2(\mathbb{R})$. ■

Example 10. The kernel of the group homomorphism $\phi : \mathbb{R} \to \mathbb{C}^*$ defined by $\phi(\theta) = \cos\theta + i \sin\theta$ is $\{2\pi n : n \in \mathbb{Z}\}$. Notice that $\ker \phi \cong \mathbb{Z}$. ■

Example 11. Suppose that we wish to determine all possible homomorphisms ϕ from $\mathbb{Z}_7$ to $\mathbb{Z}_{12}$. Since the kernel of ϕ must be a subgroup of $\mathbb{Z}_7$, there are only two possible kernels, $\{0\}$ and all of $\mathbb{Z}_7$. The image of a subgroup of $\mathbb{Z}_7$ must be a subgroup of $\mathbb{Z}_{12}$. Hence, there is no injective homomorphism; otherwise, $\mathbb{Z}_{12}$ would have a subgroup of order 7, which is impossible. Consequently, the only possible homomorphism from $\mathbb{Z}_7$ to $\mathbb{Z}_{12}$ is the one mapping all elements to zero. ■

Example 12. Let G be a group. Suppose that $g \in G$ and ϕ is the homomorphism from $\mathbb{Z}$ to G given by $\phi(n) = g^n$. If the order of g is infinite, then the kernel of this homomorphism is $\{0\}$ since ϕ maps $\mathbb{Z}$ onto the cyclic subgroup of G generated by g. However, if the order of g is finite, say n, then the kernel of ϕ is $n\mathbb{Z}$. ■

MTH-204: Abstract Algebra
Lecture-7

Santosha Kumar Pattanayak

1 Isomorphism Theorems

The main goal in group theory is to classify all groups; however, it makes sense to consider two groups to be the same if they are isomorphic. For two groups G and H, we say G is related to H if G and H are isomorphic. The proof of the following theorem is easy.

Theorem 1.1. *The isomorphism of groups determines an equivalence relation on the class of all groups.*

Hence, we can modify our goal of classifying all groups to classifying all groups **up to isomorphism**; that is, we will consider two groups to be the same if they are isomorphic.

Though at first it is not evident that factor groups correspond exactly to homomorphic images, we can use factor groups to study homomorphisms. We already know that with every group homomorphism $\phi : G \to H$ we can associate a normal subgroup of G, $\ker \phi$; the converse is also true. Every normal subgroup of a group G gives rise to homomorphism of groups.

Let H be a normal subgroup of G. Define the canonical map

$$\phi : G \to G/H$$

by

$$\phi(g) = gH.$$

This is indeed a homomorphism, since

$$\phi(g_1 g_2) = g_1 g_2 H = g_1 H g_2 H = \phi(g_1)\phi(g_2).$$

The kernel of this homomorphism is H. The following theorems describe the relationships among group homomorphisms, normal subgroups, and factor groups.

Theorem 1.2 (First Isomorphism Theorem)**.** *If $\psi : G \to H$ is a group homomorphism with $K = \ker \psi$, then K is normal in G. Let $\phi : G \to G/K$ be the canonical homomorphism. Then there exists a unique isomorphism $\eta : G/K \to \psi(G)$ such that $\psi = \eta\phi$.*

Proof. We already know that K is normal in G. Define $\eta : G/K \to \psi(G)$ by $\eta(gK) = \psi(g)$. We must first show that this is a well-defined map. Suppose that $g_1 K = g_2 K$. For some $k \in K$, $g_1 k = g_2$; consequently,

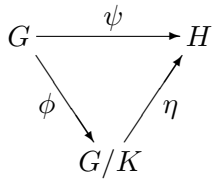
$$\eta(g_1 K) = \psi(g_1) = \psi(g_1)\psi(k) = \psi(g_1 k) = \psi(g_2) = \eta(g_2 K).$$

Since $\eta(g_1K) = \eta(g_2K)$, η does not depend on the choice of coset representative. Clearly η is onto $\psi(G)$. To show that η is one-to-one, suppose that $\eta(g_1K) = \eta(g_2K)$. Then $\psi(g_1) = \psi(g_2)$. This implies that $\psi(g_1^{-1}g_2) = e$, or $g_1^{-1}g_2$ is in the kernel of ψ; hence, $g_1^{-1}g_2K = K$; that is, $g_1K = g_2K$. Finally, we must show that η is a homomorphism, but

$$\begin{aligned}\eta(g_1Kg_2K) &= \eta(g_1g_2K)\\ &= \psi(g_1g_2)\\ &= \psi(g_1)\psi(g_2)\\ &= \eta(g_1K)\eta(g_2K).\end{aligned}$$

□

Mathematicians often use diagrams called **commutative diagrams** to describe such theorems. The following diagram "commutes" since $\psi = \eta\phi$.



Example 13. Let G be a cyclic group with generator g. Define a map $\phi : \mathbb{Z} \to G$ by $n \mapsto g^n$. This map is a surjective homomorphism since

$$\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n).$$

Clearly ϕ is onto. If $|g| = m$, then $g^m = e$. Hence, $\ker\phi = m\mathbb{Z}$ and $\mathbb{Z}/\ker\phi = \mathbb{Z}/m\mathbb{Z} \cong G$. On the other hand, if the order of g is infinite, then $\ker\phi = 0$ and ϕ is an isomorphism of G and $\mathbb{Z}$. Hence, two cyclic groups are isomorphic exactly when they have the same order. Up to isomorphism, the only cyclic groups are $\mathbb{Z}$ and $\mathbb{Z}_n$. In particular, if G is a group of order p, where p is a prime number, then G is isomorphic to $\mathbb{Z}_p$. ■

Theorem 1.3 (Second Isomorphism Theorem)**.** *Let H be a subgroup of a group G (not necessarily normal in G) and N a normal subgroup of G. Then*

$$H/H \cap N \cong HN/N.$$

Proof. Since N is normal in G, HN is a subgroup of G and $H \cap N$ is a normal subgroup of H.

We define a map ϕ from H to HN/N by $h \mapsto hN$. The map ϕ is onto, since any coset $hnN = hN$ is the image of h in H. We also know that ϕ is a homomorphism because

$$\phi(hh') = hh'N = hNh'N = \phi(h)\phi(h').$$

By the First Isomorphism Theorem, the image of ϕ is isomorphic to $H/\ker\phi$; that is,

$$HN/N = \phi(H) \cong H/\ker\phi.$$

Since

$$\ker \phi = \{h \in H : h \in N\} = H \cap N,$$

$HN/N = \phi(H) \cong H/H \cap N.$ □

Theorem 1.4. (Correspondence Theorem) *Let N be a normal subgroup of a group G. Then $H \mapsto H/N$ is a one-to-one correspondence between the set of subgroups H containing N and the set of subgroups of G/N. Furthermore, the normal subgroups of H correspond to normal subgroups of G/N.*

Proof. Let H be a subgroup of G containing N. Since N is normal in H, H/N makes sense. Let aN and bN be elements of H/N. Then $(aN)(b^{-1}N) = ab^{-1}N \in H/N$; hence, H/N is a subgroup of G/N.

Let S be a subgroup of G/N. This subgroup is a set of cosets of N. If $H = \{g \in G : gN \in S\}$, then for $h_1, h_2 \in H$, we have that $(h_1N)(h_2N) = hh'N \in S$ and $h_1^{-1}N \in S$. Therefore, H must be a subgroup of G. Clearly, H contains N. Therefore, $S = H/N$. Consequently, the map $H \mapsto H/H$ is onto.

Suppose that H_1 and H_2 are subgroups of G containing N such that $H_1/N = H_2/N$. If $h_1 \in H_1$, then $h_1N \in H_1/N$. Hence, $h_1N = h_2N \subset H_2$ for some h_2 in H_2. However, since N is contained in H_2, we know that $h_1 \in H_2$ or $H_1 \subset H_2$. Similarly, $H_2 \subset H_1$. Since $H_1 = H_2$, the map $H \mapsto H/H$ is one-to-one.

Suppose that H is normal in G and N is a subgroup of H. Then it is easy to verify that the map $G/N \to G/H$ defined by $gN \mapsto gH$ is a homomorphism. The kernel of this homomorphism is H/N, which proves that H/N is normal in G/N.

Conversely, suppose that H/N is normal in G/N. The homomorphism given by

$$G \to G/N \to \frac{G/N}{H/N}$$

has kernel H. Hence, H must be normal in G. □

Notice that in the course of the proof of the above theorem, we have also proved the following theorem.

Theorem 1.5 (Third Isomorphism Theorem)**.** *Let G be a group and N and H be normal subgroups of G with $N \subset H$. Then*

$$G/H \cong \frac{G/N}{H/N}.$$

Example 14. By the Third Isomorphism Theorem,

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}).$$

Since $|\mathbb{Z}/mn\mathbb{Z}| = mn$ and $|\mathbb{Z}/m\mathbb{Z}| = m$, we have $|m\mathbb{Z}/mn\mathbb{Z}| = n$. ■

Cayley's Theorem

Cayley proved that if G is a group, it is isomorphic to a group of permutations on some set; hence, every group is a permutation group. Cayley's Theorem is what we call a representation theorem. The aim of representation theory is to find an isomorphism of some group G that we wish to study into a group that we know a great deal about, such as a group of permutations or matrices.

Example 6. Consider the group $\mathbb{Z}_3$. The Cayley table for $\mathbb{Z}_3$ is as follows.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

The addition table of $\mathbb{Z}_3$ suggests that it is the same as the permutation group $G = \{(0), (012), (021)\}$. The isomorphism here is

$$\begin{aligned} 0 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} &= (0) \\ 1 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} &= (012) \\ 2 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} &= (021). \end{aligned}$$

■

Theorem 1.6 (Cayley)**.** *Every group is isomorphic to a group of permutations.*

Proof. Let G be a group. We must find a group of permutations $\overline{G}$ that is isomorphic to G. For any $g \in G$, define a function $\lambda_g : G \to G$ by $\lambda_g(a) = ga$. We claim that λ_g is a permutation of G. To show that λ_g is one-to-one, suppose that $\lambda_g(a) = \lambda_g(b)$. Then

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

Hence, $a = b$. To show that λ_g is onto, we must prove that for each $a \in G$, there is a b such that $\lambda_g(b) = a$. Let $b = g^{-1}a$.

Now we are ready to define our group $\overline{G}$. Let

$$\overline{G} = \{\lambda_g : g \in G\}.$$

We must show that $\overline{G}$ is a group under composition of functions and find an isomorphism between G and $\overline{G}$. We have closure under composition of functions since

$$(\lambda_g \circ \lambda_h)(a) = \lambda_g(ha) = gha = \lambda_{gh}(a).$$

Also,

$$\lambda_e(a) = ea = a$$

and

$$(\lambda_{g^{-1}} \circ \lambda_g)(a) = \lambda_{g^{-1}}(ga) = g^{-1}ga = a = \lambda_e(a).$$

We can define an isomorphism from G to $\overline{G}$ by $\phi : g \mapsto \lambda_g$. The group operation is preserved since

$$\phi(gh) = \lambda_{gh} = \lambda_g \lambda_h = \phi(g)\phi(h).$$

It is also one-to-one, because if $\phi(g)(a) = \phi(h)(a)$, then

$$ga = \lambda_g a = \lambda_h a = ha.$$

Hence, $g = h$. That ϕ is onto follows from the fact that $\phi(g) = \lambda_g$ for any $\lambda_g \in \overline{G}$. □

The isomorphism $g \mapsto \lambda_g$ is known as the **left regular representation** of G.

MTH-204: Abstract Algebra
Lecture-8

Santosha Kumar Pattanayak

1 Direct Products

Given two groups G and H, it is possible to construct a new group from the Cartesian product of G and H, $G \times H$. Conversely, given a large group, it is sometimes possible to decompose the group; that is, a group is sometimes isomorphic to the direct product of two smaller groups. Rather than studying a large group G, it is often easier to study the component groups of G.

External Direct Products

If $(G, \cdot)$ and $(H, \circ)$ are groups, then we can make the Cartesian product of G and H into a new group. As a set, our group is just the ordered pairs $(g, h) \in G \times H$ where $g \in G$ and $h \in H$. We can define a binary operation on $G \times H$ by

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

that is, we just multiply elements in the first coordinate as we do in G and elements in the second coordinate as we do in H. We have specified the particular operations $\cdot$ and $\circ$ in each group here for the sake of clarity; we usually just write $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$.

Proposition 1.1. *Let G and H be groups. The set $G \times H$ is a group under the operation $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ where $g_1, g_2 \in G$ and $h_1, h_2 \in H$.*

Proof. Clearly the binary operation defined above is closed. If e_G and e_H are the identities of the groups G and H respectively, then (e_G, e_H) is the identity of $G \times H$. The inverse of $(g, h) \in G \times H$ is (g^{-1}, h^{-1}). The fact that the operation is associative follows directly from the associativity of G and H. □

Example 7. Let $\mathbb{R}$ be the group of real numbers under addition. The Cartesian product of $\mathbb{R}$ with itself, $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, is also a group, in which the group operation is just addition in each coordinate; that is, $(a, b) + (c, d) = (a + c, b + d)$. The identity is $(0, 0)$ and the inverse of (a, b) is $(-a, -b)$. ■

Example Consider

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

Although $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ both contain four elements, it is easy to see that they are not isomorphic since for every element (a, b) in $\mathbb{Z}_2 \times \mathbb{Z}_2$, $(a, b) + (a, b) = (0, 0)$, but $\mathbb{Z}_4$ is cyclic. ■

The group $G \times H$ is called the **external direct product** of G and H. Notice that there is nothing special about the fact that we have used only two groups to build a new group. The direct product

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n$$

of the groups $G_1, G_2, \ldots, G_n$ is defined in exactly the same manner. If $G = G_1 = G_2 = \cdots = G_n$, we often write G^n instead of $G_1 \times G_2 \times \cdots \times G_n$.

Example The group $\mathbb{Z}_2^n$, considered as a set, is just the set of all binary n-tuples. The group operation is the "exclusive or" of two binary n-tuples. For example,

$$(01011101) + (01001011) = (00010110).$$

This group is important in coding theory, in cryptography, and in many areas of computer science. ■

Theorem 1.2. *Let $(g, h) \in G \times H$. If g and h have finite orders r and s respectively, then the order of (g, h) in $G \times H$ is the least common multiple of r and s.*

Proof. Suppose that m is the least common multiple of r and s and let $n = |(g, h)|$. Then

$$(g, h)^m = (g^m, h^m) = (e_G, e_H)$$
$$(g^n, h^n) = (g, h)^n = (e_G, e_H).$$

Hence, n must divide m, and $n \leq m$. However, by the second equation, both r and s must divide n; therefore, n is a common multiple of r and s. Since m is the *least common multiple* of r and s, $m \leq n$. Consequently, m must be equal to n. □

Corollary 1.3. *Let $(g_1, \ldots, g_n) \in \prod G_i$. If g_i has finite order r_i in G_i, then the order of $(g_1, \ldots, g_n)$ in $\prod G_i$ is the least common multiple of $r_1, \ldots, r_n$.*

Example Let $(8, 56) \in \mathbb{Z}_{12} \times \mathbb{Z}_{60}$. Since $\gcd(8, 12) = 4$, the order of 8 is $12/4 = 3$ in $\mathbb{Z}_{12}$. Similarly, the order of 56 in $\mathbb{Z}_{60}$ is 15. The least common multiple of 3 and 15 is 15; hence, $(8, 56)$ has order 15 in $\mathbb{Z}_{12} \times \mathbb{Z}_{60}$. ■

Example The group $\mathbb{Z}_2 \times \mathbb{Z}_3$ consists of the pairs

$$(0, 0), \quad (0, 1), \quad (0, 2), \quad (1, 0), \quad (1, 1), \quad (1, 2).$$

In this case, unlike that of $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$, it is true that $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. We need only show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic. It is easy to see that $(1, 1)$ is a generator for $\mathbb{Z}_2 \times \mathbb{Z}_3$. ■

The next theorem tells us exactly when the direct product of two cyclic groups is cyclic.

Theorem 1.4. *The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$.*

Proof. Assume first that if $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$. We need to show $\gcd(m,n) = 1$. To show this, we will prove the contrapositive; that is, we will show that if $\gcd(m,n) = d > 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n$ cannot be cyclic. Notice that mn/d is divisible by both m and n; hence, for any element $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$,

$$\underbrace{(a,b) + (a,b) + \cdots + (a,b)}_{mn/d \text{ times}} = (0,0).$$

Therefore, no (a,b) can generate all of $\mathbb{Z}_m \times \mathbb{Z}_n$.

The converse follows since $lcm(m,n) = mn$ if and only if $\gcd(m,n) = 1$ and order of (a,b) is mn where a and b are generators of $\mathbb{Z}_m$ and $\mathbb{Z}_n$ respectively. □

Corollary 1.5. *Let $n_1, \ldots, n_k$ be positive integers. Then*

$$\prod_{i=1}^{k} \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 \cdots n_k}$$

if and only if $\gcd(n_i, n_j) = 1$ for $i \neq j$.

Corollary 1.6. *If*

$$m = p_1^{e_1} \cdots p_k^{e_k},$$

where the p_is are distinct primes, then

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}.$$

Proof. Since the greatest common divisor of $p_i^{e_i}$ and $p_j^{e_j}$ is 1 for $i \neq j$, the proof follows from above corollary. □

Later we will prove that all finite abelian groups are isomorphic to direct products of the form

$$\mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$$

where $p_1, \ldots, p_k$ are (not necessarily distinct) primes.

Internal Direct Products

The external direct product of two groups builds a large group out of two smaller groups. We would like to be able to reverse this process and conveniently break down a group into its direct product components; that is, we would like to be able to say when a group is isomorphic to the direct product of two of its subgroups.

Let G be a group with subgroups H and K satisfying the following conditions.

- $G = HK = \{hk : h \in H, k \in K\}$;
- $H \cap K = \{e\}$;

- $hk = kh$ for all $k \in K$ and $h \in H$.

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

Example 12. The group $U(8)$ is the internal direct product of

$$\begin{aligned} H &= \{1, 3\} \\ K &= \{1, 5\}. \end{aligned}$$

■

Example 13. The dihedral group D_6 is an internal direct product of its two subgroups

$$\begin{aligned} H &= \{id, r^3\} \\ K &= \{id, r^2, r^4, s, r^2s, r^4s\}. \end{aligned}$$

It can easily be shown that $K \cong S_3$; consequently, $D_6 \cong \mathbb{Z}_2 \times S_3$. ■

Example 14. Not every group can be written as the internal direct product of two of its proper subgroups. If the group S_3 were an internal direct product of its proper subgroups H and K, then one of the subgroups, say H, would have to have order 3. In this case H is the subgroup $\{(1), (123), (132)\}$. The subgroup K must have order 2, but no matter which subgroup we choose for K, the condition that $hk = kh$ will never be satisfied for $h \in H$ and $k \in K$. ■

Theorem 1.7. *Let G be the internal direct product of subgroups H and K. Then G is isomorphic to $H \times K$.*

Proof. Since G is an internal direct product, we can write any element $g \in G$ as $g = hk$ for some $h \in H$ and some $k \in K$. Define a map $\phi : G \to H \times K$ by $\phi(g) = (h, k)$.

The first problem that we must face is to show that ϕ is a well-defined map; that is, we must show that h and k are uniquely determined by g. Suppose that $g = hk = h'k'$. Then $h^{-1}h' = k(k')^{-1}$ is in both H and K, so it must be the identity. Therefore, $h = h'$ and $k = k'$, which proves that ϕ is, indeed, well-defined.

To show that ϕ preserves the group operation, let $g_1 = h_1k_1$ and $g_2 = h_2k_2$ and observe that

$$\begin{aligned} \phi(g_1g_2) &= \phi(h_1k_1h_2k_2) \\ &= \phi(h_1h_2k_1k_2) \\ &= (h_1h_2, k_1k_2) \\ &= (h_1, k_1)(h_2, k_2) \\ &= \phi(g_1)\phi(g_2). \end{aligned}$$

We will leave the proof that ϕ is one-to-one and onto as an exercise. □

Example 15. The group $\mathbb{Z}_6$ is an internal direct product isomorphic to $\{0, 2, 4\} \times \{0, 3\}$. ■

We can extend the definition of an internal direct product of G to a collection of subgroups $H_1, H_2, \ldots, H_n$ of G, by requiring that

- $G = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n : h_i \in H_i\}$;
- $H_i \cap \langle \cup_{j \neq i} H_j \rangle = \{e\}$;
- $h_i h_j = h_j h_i$ for all $h_i \in H_i$ and $h_j \in H_j$.

The following theorem is just a generalization of the above theorem and the proof is the same.

Theorem 1.8. *Let G be the internal direct product of subgroups H_i, where $i = 1, 2, \ldots, n$. Then G is isomorphic to $\prod_i H_i$.*

MTH-204: Abstract Algebra
Lecture-9

Santosha Kumar Pattanayak

1 Automorphisms and Semi-direct Products

An **automorphism** of a group G is an isomorphism with itself.

Example: The map $1 \mapsto -1$ is an automorphism of $\mathbb{Z}$.

Example: If G is abelian then $x \mapsto x^{-1}$ is an automorphism.

Example: The complex conjugation is an automorphism of the additive group of complex numbers; that is, the map $\phi(a+bi) = a-bi$ is an isomorphism from $\mathbb{C}$ to $\mathbb{C}$.

Example: The map $a+ib \mapsto a-ib$ is an automorphism of $\mathbb{C}^*$.

Example: The map $A \mapsto B^{-1}AB$ is an automorphism of $SL_2(\mathbb{R})$ for all B in $GL_2(\mathbb{R})$.

We will denote the set of all automorphisms of G by $Aut(G)$. Prove that $Aut(G)$ is a subgroup of S_G, the group of permutations of G.

Definition: Let G be a group and $g \in G$. Define a map $i_g : G \to G$ by $i_g(x) = gxg^{-1}$. Prove that i_g defines an automorphism of G. Such an automorphism is called an **inner automorphism**. The set of all inner automorphisms is denoted by $Inn(G)$.

Proposition 1.1. *The set $Inn(G)$ is a normal subgroup of $Aut(G)$.*

Proof. It is easy to check that $Inn(G)$ is a subgroup of $Aut(G)$. Let $\phi \in Aut(G)$ and $i_g \in Inn(G)$. Then we must show that $\phi.i_g.\phi^{-1} \in Inn(G)$.

We claim that $\phi.i_g.\phi^{-1} = i_{\phi(g)}$. This is because $\phi.i_g.\phi^{-1}(x) = \phi.i_g(\phi^{-1}(x)) = \phi(g\phi^{-1}(x)g^{-1}) = \phi(g)x\phi(g)^{-1} = i_{\phi(g)}(x)$.

□

Theorem 1.2. *For a group G we have $G/Z(G) \cong Inn(G)$.*

Proof. Define $\phi : G \to Inn(G)$ by $g \mapsto i_g$. Then ϕ is a homomorphism and $ker(\phi) = \{g \in G : i_g = id\} = \{g \in G : i_g(x) = x\} = \{g \in G : gx = xg\} = Z(G)$. From the definition the map ϕ is onto. So by the first isomorphism theorem we have $G/Z(G) \cong Inn(G)$.

□

Remark: From the above theorem we have $G \cong Inn(G)$ if $Z(G) = \{e\}$. For example if $G = S_n$ then since $Z(S_n) = \{e\}$ we have $S_n \cong Inn(S_n)$.

Definition 1.3. *Suppose that H and K are groups and let $\phi : K \to Aut(H)$ be a homomorphism. We may define an action of K on H as $k \cdot h = \phi(k)(h)$. Then we define the* **external semi-direct product** *$H \rtimes_\phi K$ of H and K with respect to ϕ as follows. As a set $H \rtimes_\phi K = H \times K$. The group operation of $H \rtimes_\phi K$ is defined by*

$$\begin{aligned}(h_1, k_1)(h_2, k_2) &= (h_1(k_1 \cdot h_1), k_1 k_2) \\ &= (h_1 \phi(k_1)(h_1), k_1 k_2).\end{aligned}$$

The following theorem is easy to prove.

Theorem 1.4. *Let H and K be groups and let $\phi : K \to Aut(H)$ be a homomorphism. Then*

1. *$H \rtimes_\phi K$ is a group of order $|H||K|$.*
2. *Let $\tilde{H} = \{(h, 1_K) : h \in H\}$ and $\tilde{K} = \{(1_H, k) : k \in K\}$. Then $\tilde{H}, \tilde{K} \leq H \rtimes_\phi K$ with $\tilde{H} \cong H$ and $\tilde{K} \cong K$.*
3. *$H \trianglelefteq H \rtimes_\phi K$.*
4. *$H \cap K = 1$.*
5. *$HK = H \rtimes_\phi K$.*
6. *$\forall h \in H$ and $k \in K$, $khk^{-1} = k \cdot h = \phi(k)(h)$.*

The following proposition says that the direct product is same as the semi-direct product if ϕ is the trivial homomorphsim.

Proposition 1.5. *Let H and K be groups and let $\phi : K \to AutH$ be a homomorphism. The following are equivalent.*

1. *The identity map between $H \rtimes K$ and $H \times K$ is a group homomorphism (and hence isomorphism).*
2. *ϕ is the trivial homomorphism from K into $Aut(H)$.*
3. *$K \trianglelefteq H \rtimes K$.*

Like in the case of direct product here also we can define internal semi-direct product of two subgroups H and K of G. The following theorem says that for two subgroups, their internal semi-direct product is same as their external semi-direct product. The proof is the same.

Theorem 1.6. *Suppose that G is a group and $H, K \leq G$ such that*

1. *$H \trianglelefteq G$, and*
2. *$H \cap K = 1$.*

Let $\phi : K \to Aut(H)$ be the homomorphism defined by $\phi(k)(h) = khk^{-1}$. Then, $HK \cong H \rtimes K$. In particular, if $G = HK$ with H and K satisfying (1) and (2) above then G is the semidirect product of H and K.

Definition 1.7. *Let H be a subgroup of G. A subgroup K is called a complement of H in G if $G = HK$ and $H \cap K = 1$.*

MTH-204: Abstract Algebra
Lecture-10

Santosha Kumar Pattanayak

1 Group Actions

Group actions generalize group multiplication. If G is a group and X is an arbitrary set, a group action of an element $g \in G$ and $x \in X$ is a product, gx, living in X. Many problems in algebra may best be attacked via group actions. For example, the proofs of the Sylow theorems and of Burnside's Counting Theorem are most easily understood when they are formulated in terms of group actions.

2 Groups Acting on Sets

Let X be a set and G be a group. A **(left) action** of G on X is a map $G \times X \to X$ given by $(g, x) \mapsto gx$, where

1. $ex = x$ for all $x \in X$;
2. $(g_1 g_2)x = g_1(g_2 x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these considerations X is called a **G-set**. Notice that we are not requiring X to be related to G in any way. It is true that every group G acts on every set X by the trivial action $(g, x) \mapsto x$; however, group actions are more interesting if the set X is somehow related to the group G.

Example 1. Let $G = GL_2(\mathbb{R})$ and $X = \mathbb{R}^2$. Then G acts on X by left multiplication. If $v \in \mathbb{R}^2$ and I is the identity matrix, then $Iv = v$. If A and B are 2×2 invertible matrices, then $(AB)v = A(Bv)$ since matrix multiplication is associative. ■

Example 2. Let $G = D_4$, the symmetry group of a square. If $X = \{1, 2, 3, 4\}$ is the set of vertices of the square, then we can consider D_4 to consist of the following permutations:

$$\{(1), (13), (24), (1432), (1234), (12)(34), (14)(23), (13)(24)\}.$$

The elements of D_4 act on X as functions. The permutation $(13)(24)$ acts on vertex 1 by sending it to vertex 3, on vertex 2 by sending it to vertex 4, and so on. It is easy to see that the axioms of a group action are satisfied. ■

In general, if X is any set and G is a subgroup of S_X, the group of all permutations acting on X, then X is a G-set under the group action

$$(\sigma, x) \mapsto \sigma(x)$$

for $\sigma \in G$ and $x \in X$.

Example 3. If we let $X = G$, then every group G acts on itself by the left regular representation; that is, $(g, x) \mapsto \lambda_g(x) = gx$, where λ_g is left multiplication:

$$\begin{aligned} e \cdot x &= \lambda_e x = ex = x \\ (gh) \cdot x &= \lambda_{gh} x = \lambda_g \lambda_h x = \lambda_g(hx) = g \cdot (h \cdot x). \end{aligned}$$

If H is a subgroup of G, then G is an H-set under left multiplication by elements of H. ■

Example 4. Let G be a group and suppose that $X = G$. If H is a subgroup of G, then G is an H-set under **conjugation**; that is, we can define an action of H on G,

$$H \times G \to G,$$

via

$$(h, g) \mapsto hgh^{-1}$$

for $h \in H$ and $g \in G$. Clearly, the first axiom for a group action holds. Observing that

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

we see that the second condition is also satisfied. ■

Example 5. Let H be a subgroup of G and $\mathcal{L}_H$ the set of left cosets of H. The set $\mathcal{L}_H$ is a G-set under the action

$$(g, xH) \mapsto gxH.$$

Again, it is easy to see that the first axiom is true. Since $(gg')xH = g(g'xH)$, the second axiom is also true. ■

If G acts on a set X and $x, y \in X$, then x is said to be **G-equivalent** to y if there exists a $g \in G$ such that $gx = y$. We write $x \sim_G y$ or $x \sim y$ if two elements are G-equivalent.

Proposition 2.1. *Let X be a G-set. Then G-equivalence is an equivalence relation on X.*

Proof. The relation $\sim$ is reflexive since $ex = x$. Suppose that $x \sim y$ for $x, y \in X$. Then there exists a g such that $gx = y$. In this case $g^{-1}y = x$; hence, $y \sim x$. To show that the relation is transitive, suppose that $x \sim y$ and $y \sim z$. Then there must exist group elements g and h such that $gx = y$ and $hy = z$. So $z = hy = (hg)x$, and x is equivalent to z. □

If X is a G-set, then each partition of X associated with G-equivalence is called an **orbit** of X under G. We will denote the orbit that contains an element x of X by O_x. So

$$O_x = \{g.x : g \in G\}.$$

Example 6. Let G be the permutation group defined by

$$G = \{(1), (123), (132), (45), (123)(45), (132)(45)\}$$

and $X = \{1, 2, 3, 4, 5\}$. Then X is a G-set. The orbits are $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1, 2, 3\}$ and $\mathcal{O}_4 = \mathcal{O}_5 = \{4, 5\}$. ■

Now suppose that G is a group acting on a set X and let g be an element of G. The **fixed point set** of g in X, denoted by X_g, is the set of all $x \in X$ such that $gx = x$. We can also study the group elements g that fix a given $x \in X$. This set is more than a subset of G, it is a subgroup. This subgroup is called the **stabilizer subgroup** or **isotropy subgroup** of x. We will denote the stabilizer subgroup of x by G_x. Note that

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

Remark. It is important to remember that $X_g \subset X$ and $G_x \subset G$.

Example 7. Let $X = \{1, 2, 3, 4, 5, 6\}$ and suppose that G is the permutation group given by the permutations

$$\{(1), (12)(3456), (35)(46), (12)(3654)\}.$$

Then the fixed point sets of X under the action of G are

$$\begin{aligned} X_{(1)} &= X, \\ X_{(35)(46)} &= \{1, 2\}, \\ X_{(12)(3456)} &= X_{(12)(3654)} = \emptyset, \end{aligned}$$

and the stabilizer subgroups are

$$\begin{aligned} G_1 = G_2 &= \{(1), (35)(46)\}, \\ G_3 = G_4 = G_5 &= G_6 = \{(1)\}. \end{aligned}$$

It is easily seen that G_x is a subgroup of G for each $x \in X$. ■

Proposition 2.2. *Let G be a group acting on a set X and $x \in X$. The stabilizer, G_x, of x is a subgroup of G.*

Proof. Clearly, $e \in G_x$ since the identity fixes every element in the set X. Let $g, h \in G_x$. Then $gx = x$ and $hx = x$. So $(gh)x = g(hx) = gx = x$; hence, the product of two elements in G_x is also in G_x. Finally, if $g \in G_x$, then $x = ex = (g^{-1}g)x = (g^{-1})gx = g^{-1}x$. So g^{-1} is in G_x. □

We will denote the number of elements in the fixed point set of an element $g \in G$ by $|X_g|$ and denote the number of elements in the orbit of x of $x \in X$ by $|O_x|$. The next theorem demonstrates the relationship between orbits of an element $x \in X$ and the left cosets of G_x in G.

Theorem 2.3 (Orbit-Stabilizer Theorem)**.** *Let G be a finite group and X a finite G-set. If $x \in X$, then $|O_x| = [G : G_x]$.*

Proof. We know that $|G|/|G_x|$ is the number of left cosets of G_x in G by Lagrange's Theorem. We will define a bijective map ϕ between the orbit O_x of X and the set of left cosets $\mathcal{L}_{G_x}$ of G_x in G. Let $y \in O_x$. Then there exists a g in G such that $gx = y$. Define ϕ by $\phi(y) = gG_x$. First we must show that this map is well-defined and does not depend on our selection of g. Suppose that h is another element in G such that $hx = y$. Then $gx = hx$ or $x = g^{-1}hx$; hence, $g^{-1}h$ is in the stabilizer subgroup of x. Therefore, $h \in gG_x$ or $gG_x = hG_x$. Thus, y gets mapped to the same coset regardless of the choice of the representative from that coset.

To show that ϕ is one-to-one, assume that $\phi(x_1) = \phi(x_2)$. Then there exist $g_1, g_2 \in G$ such that $x_1 = g_1x$ and $x_2 = g_2x$. Since there exists a $g \in G_x$ such that $g_2 = g_1g$,

$$x_2 = g_2x = g_1gx = g_1x = x_1;$$

consequently, the map ϕ is one-to-one. Finally, we must show that the map ϕ is onto. Let gG_x be a left coset. If $gx = y$, then $\phi(y) = gG_x$. □

3 The Class Equation

Let X be a finite G-set and X_G be the set of fixed points in X; that is,

$$X_G = \{x \in X : gx = x \text{ for all } g \in G\}.$$

Since the orbits of the action partition X,

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

where $x_k, \ldots, x_n$ are representatives from the distinct nontrivial orbits of X.

Now consider the special case in which G acts on itself by conjugation, $(g, x) \mapsto gxg^{-1}$. The center of G,

$$Z(G) = \{x : xg = gx \text{ for all } g \in G\},$$

is the set of points that are fixed by conjugation. The nontrivial orbits of the action are called the **conjugacy classes** of G. If $x_1, \ldots, x_k$ are representatives from each of the nontrivial conjugacy classes of G and $|O_{x_1}| = n_1, \ldots, |O_{x_k}| = n_k$, then

$$|G| = |Z(G)| + n_1 + \cdots + n_k.$$

The stabilizer subgroups of each of the x_i's, $C(x_i) = \{g \in G : gx_i = x_ig\}$, are called the **centralizer subgroups** of the x_i's. From Theorem 12.3, we obtain the **class equation**:

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)].$$

One of the consequences of the class equation is that the order of each conjugacy class must divide the order of $|G|$.

Example 8. It is easy to check that the conjugacy classes in S_3 are the following:

$$\{(1)\}, \quad \{(123),(132)\}, \quad \{(12),(13),(23)\}.$$

The class equation is $6 = 1 + 2 + 3$. ■

Example 9. The conjugacy classes for $D_4 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$ are

$$\{1\}, \{x^2\}, \{x, x^3\}, \{y, x^2y\}, \{xy, x^3y\}.$$

The center of a group is counted separately in the class equation because each element in the center forms its own conjugacy class of size 1

The center is $Z(D_4) = \{1, x^2\}$.

So the class equation is $8 = 2 + 2 + 2 + 2$. ■

Example 10. For S_n it takes a bit of work to find the conjugacy classes. We begin with cycles. Suppose that $\sigma = (a_1, \ldots, a_k)$ is a cycle and let $\tau \in S_n$. By Theorem 5.9,

$$\tau\sigma\tau^{-1} = (\tau(a_1), \ldots, \tau(a_k)).$$

Consequently, any two cycles of the same length are conjugate. Now let $\sigma = \sigma_1\sigma_2\cdots\sigma_r$ be a cycle decomposition, where the length of each cycle σ_i is r_i. Then σ is conjugate to every other $\tau \in S_n$ whose cycle decomposition has the same lengths.

The number of conjugate classes in S_n is the number of ways in which n can be partitioned into sums of positive integers. For example, we can partition the integer 3 into the following three sums:

$$\begin{aligned} 3 &= 1+1+1 \\ 3 &= 1+2 \\ 3 &= 3; \end{aligned}$$

therefore, there are three conjugacy classes. ■

Theorem 3.1. *Let G be a group of order p^n where p is prime. Then G has a nontrivial center.*

Proof. We apply the class equation

$$|G| = |Z(G)| + n_1 + \cdots + n_k.$$

Since each $n_i > 1$ and $n_i \mid G$, p must divide each n_i. Also, $p \mid |G|$; hence, p must divide $|Z(G)|$. Since the identity is always in the center of G, $|Z(G)| \geq 1$. Therefore, $|Z(G)| \geq p$ and there exists some $g \in Z(G)$ such that $g \neq 1$. □

Corollary 3.2. *Let G be a group of order p^2 where p is prime. Then G is abelian.*

Proof. By above theorem we have $|Z(G)| = p$ or p^2. If $|Z(G)| = p^2$, then we are done. Suppose that $|Z(G)| = p$. Then $Z(G)$ and $G/Z(G)$ both have order p and must both be cyclic groups. Choosing a generator $aZ(G)$ for $G/Z(G)$, we can write any element $gZ(G)$ in the quotient group as $a^mZ(G)$ for some integer m; hence, $g = a^mx$ for some x in the center of G. Similarly, if $hZ(G) \in G/Z(G)$,

there exists a y in $Z(G)$ such that $h = a^n y$ for some integer n. Since x and y are in the center of G, they commute with all other elements of G; therefore,

$$gh = a^m x a^n y = a^{m+n} xy = a^n y a^m x = hg,$$

and G must be abelian. $\square$

MTH-204: Abstract Algebra
Lecture-11

Santosha Kumar Pattanayak

1 Burnside's and Sylow's theorems

1.1 Burnside's Counting Theorem

Suppose that we are to color the vertices of a square with two different colors, say black and white. We might suspect that there would be $2^4 = 16$ different colorings. However, some of these colorings are equivalent. If we color the first vertex black and the remaining vertices white, it is the same as coloring the second vertex black and the remaining ones white since we could obtain the second coloring simply by rotating the square 90°.

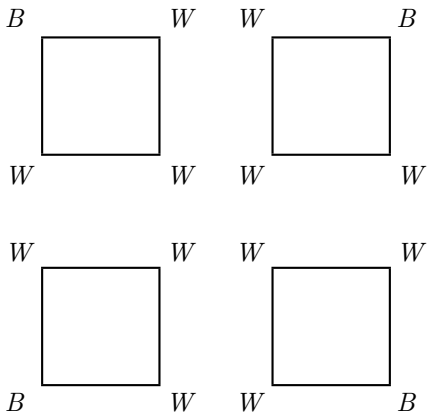


Figure 1: Equivalent colorings of square

Burnside's Counting Theorem offers a method of computing the number of distinguishable ways in which something can be done. The proof of Burnside's Counting Theorem depends on the following lemma.

Lemma 1.1. *Let X be a G-set and suppose that $x \sim y$. Then G_x is isomorphic to G_y. In particular, $|G_x| = |G_y|$.* where have we used this lemma?

Proof. Let G act on X by $(g, x) \mapsto g \cdot x$. Since $x \sim y$, there exists a $g \in G$ such that $g \cdot x = y$. Let $a \in G_x$. Since

$$gag^{-1} \cdot y = ga \cdot g^{-1}y = ga \cdot x = g \cdot x = y,$$

we can define a map $\phi : G_x \to G_y$ by $\phi(a) = gag^{-1}$. The map ϕ is a homomorphism since

$$\phi(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \phi(a)\phi(a).$$

Suppose that $\phi(a) = \phi(b)$. Then $gag^{-1} = gbg^{-1}$ or $a = b$; hence, the map is injective. To show that ϕ is onto, let b be in G_y; then $g^{-1}bg$ is in G_x since

$$g^{-1}bg \cdot x = g^{-1}b \cdot gx = g^{-1}b \cdot y = g^{-1} \cdot y = x;$$

and $\phi(g^{-1}bg) = b$. □

Theorem 1.2 (Burnside)**.** *Let G be a finite group acting on a set X and let k denote the number of orbits of X. Then*

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

Proof. We look at all the fixed points x of all the elements in $g \in G$; that is, we look at all g's and all x's such that $gx = x$. If viewed in terms of fixed point sets, the number of all g's fixing x's is

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

That is

$$\sum_{g\in G}|X_g| = |\{(g, x) \in G \times X : g.x = x\}| = \sum_{x\in X}|G_x|.$$

By orbit stabilizer theorem we have $|G| = |O_x||G_x|$.

So

$$\sum_{g\in G}|X_g| = \sum_{x\in X}|G_x| = \sum_{x\in X}\frac{|G|}{|O_x|} = |G|\sum_{x\in X}\frac{1}{|O_x|} = |G|\sum_{O\in Set\ of\ orbits}\ \sum_{x\in O}|O| = |G|\sum_{O\in Set\ of\ orbits}1 = |G|.k$$

. □

Example 11. Let $X = \{1, 2, 3, 4, 5\}$ and suppose that G is the permutation group $G = \{(1), (13), (13)(25), (25)\}$. The orbits of X are $\{1, 3\}$, $\{2, 5\}$, and $\{4\}$. The fixed point sets are

$$\begin{aligned} X_{(1)} &= X \\ X_{(13)} &= \{2, 4, 5\} \\ X_{(13)(25)} &= \{4\} \\ X_{(25)} &= \{1, 3, 4\}. \end{aligned}$$

Burnside's Theorem says that

$$k = \frac{1}{|G|}\sum_{g\in G}|X_g| = \frac{1}{4}(5 + 3 + 1 + 3) = 3.$$

■

2 The Sylow Theorems

We already know that the converse of Lagrange's Theorem is false. If G is a group of order m and n divides m, then G does not necessarily possess a subgroup of order n. For example, A_4 has order 12 but does not possess a subgroup of order 6. However, the Sylow Theorems do provide a partial converse for Lagrange's Theorem: in certain cases they guarantee us subgroups of specific orders. These theorems yield a powerful set of tools for the classification of all finite nonabelian groups.

We will use the idea of group actions to prove the Sylow Theorems. A group G acts on itself by conjugation via the map $(g, x) \mapsto gxg^{-1}$. Let $x_1, \ldots, x_k$ be representatives from each of the distinct conjugacy classes of G that consist of more than one element. Then the class equation can be written as

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

where $Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}$ is the center of G and $C(x_i) = \{g \in G : gx_i = x_i g\}$ is the centralizer subgroup of x_i.

Let p be a prime. A group G called a p-group if $|G|$ is a power of p.

Theorem 2.1 (Sylow Theorems)**.** *Let G be a group, $|G| = p^m r$, where p is a prime and $gcd(r, p) = 1$. Then*

1. *there exists a subgroup P such that $|P| = p^m$ (Sylow p-subgroup)*
2. *Any two p-sylow subgroups are conjugate to each other.*
3. *the number of p-sylow subgroups of G is $1 \pmod p$, i.e., $n_p \equiv 1 \pmod p$.*

Proof of (1): Let X be the set of subsets of G of cardinality p^m,i.e., $X = \{K \subset G : |K| = p^m\}$. We claim that $p \nmid |X|$. We have

$$\begin{aligned} |X| &= \binom{|G|}{p^m} = \binom{p^m r}{p^m} \\ &= \frac{p^m r(p^m r - 1)(p^m r - 2)\cdots(p^m - p^m + 1)}{1 \cdot 2 \cdot 3 \cdot \cdots \cdot p^m} \\ &= \frac{r(p^m r - 1)(p^m r - 2)\cdots(p^m - (p^m - 1))}{1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p^m - 1)} \qquad = r \prod_{i=1}^{p^m - 1} \frac{p^m r - i}{i} \end{aligned}$$

Let $i = p^k r'$ where $k \leq m, \gcd(p, r) = 1$, then $\frac{p^m r - i}{i} = \frac{p^{m-k} r - r'}{r'}$. Therefore the numerator does not have p as divisor, hence $p \nmid |X|$.

Let G acts on X, by left multiplication: $g.K = gK$ for $g \in G, K \in X$. Recall that the action of G on X induces a partition of X into orbits: $X = \sqcup O_S$, where the disjoint union is taken over a set of representatives.

We get $|X| = \sum |O_S|$ and since p does not divide $|X|$, there is at least one S for which p does not divide $|O_S|$. Let us pick this S, and denote by P its stabilizer. We claim that $|P| = p^m$.

By Orbit-Stabilizer Theorem, we have $|O_S| = |G|/|P| = p^m r/|P|$. By choice of the S we picked, p does not divide $|O_S|$, that is p does not divide $p^m r/|P|$ and $|P|$ has to be a multiple of p^m, or equivalently p^m divides $|P|$. So $|P| \geq p^m$.

We claim that $|P| \leq p^m$. Let us define the map $\lambda_x, x \in S$, by $\lambda_x : P \to S, g \mapsto gx$. In words, this map goes from P, which is a subgroup of G, to S, which is an element of X, that is a subset of G with cardinality p^m. Note that this map is well-defined since $gx \in S$ for any $x \in S$ and any $g \in P$ by definition of P being the stabilizer of S. It is also clearly injective ($gx = hx$ implies $g = h$ since x is an element of the group G and thus is invertible). If we have an injection from P to S, that means $|P| \leq |S| = p^m$. We are done.

Proof of (2): Let P be a Sylow p-subgroup of G and let R be a p-group of G. We will prove that R (being a p-group in general) is contained in a conjugate of P. Let R act by multiplication on the set Y of left cosets of P: $Y = \{gP, g \in G\}$.

We want to prove that there is an orbit of size 1 under this action. By Lagrange's Theorem, we know that $|Y| = |G|/|P| = p^m r/p^m = r$ and thus p does not divide $|Y|$ by assumption on r.

We have a partition of Y by its orbits, we get $|Y| = \sum |O_y|$ and there exists one orbit O_y such that $p \nmid |O_y|$.

By the Orbit-Stabilizer Theorem, we have $|O_y|$ divides $|R|$, which has order a power of p, so there is an orbit of size 1. Let $gP \in Y$ be the element whose orbit size is 1.

We have $hgP = gP$ for $h \in R$, since gP belongs to its orbit. Thus $g^{-1}hg \in P$ iff $h \in gPg^{-1}$ for all $h \in R$.

We have just proved that the p-group R is contained in a conjugate of P. All we needed for the proof is that R is a p-group, so the same proof holds for the case of a Sylow p-subgroup, for which we get that R is contained in a conjugate of P, and both have same cardinality, which concludes the proof. We will use the fact that the proof works for R a p-group in general for proving one corollary.

Proof of (3): Consider the set X be the set of all Sylow p- subgroups of G. We have $|X| = n_p$. By the 1st Sylow Theorem, this set is non-empty and there exists at least one Sylow p-subgroup P in X, whose order is p^m.

Let P act on X by conjugation, i.e., $gQ = gQg^{-1}, g \in P$, $Q \in X$. Note that in the case where P is the only Sylow p-subgroup, then we can take $Q = P$. By the Orbit-Stabilizer Theorem, we have $|O_Q| = |P|/|G_Q| = p^m/|G_Q|$. So $|O_Q| = 1$ or a power of p.

Again we have $|X| = \sum |O_Q| = \sum |O_{Q'} + \sum |O_{Q"}|$, where Q' and Q" denote subgroups whose orbit has respectively one element or at least two elements. Since p divides the second sum, we have $|X| \equiv$ number of orbits of size 1 mod p. To conclude the proof, we thus have to show that there is only one Sylow p-subgroup whose orbit has size 1, namely P itself

Let us assume there is another Sylow p-subgroup Q whose orbit has only one element, namely: $gQg^{-1} = Q, g \in P$, which translates into $gQ = Qg$ for all $g \in P$ and so $PQ = QP$. This says that PQ is a subgroup of G.

We know that $|PQ| = |P||Q|/|P \cap Q = p^m p^m/|P \cap Q|$. So $|PQ|$ is a power of p, say p^c for some c which cannot be bigger than m, since $|G| = p^m r$. Hence $p^m = |P| \leq |PQ| \leq p^m$. So $|P| = |PQ|$

and so $P = Q$ as they have same cardinality.

Corollary 2.2. (Cauchy) *Let G be a finite group and p a prime such that p divides the order of G. Then G contains a subgroup of order p.*

Proof. Let P be a Sylow p-subgroup of G (which exists by the 1st Sylow Theorem), and pick $x \neq 1$ in P. The order $|x|$ of x is a power of p by definition of a p-group, say $|x| = p^k$. Then $x^{p^{k-1}}$ has order p. □

Example 1. Let us consider the group A_5. We know that $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$. By Cauchy's Theorem, we are guaranteed that A_5 has subgroups of orders 2, 3 and 5. The Sylow Theorems give us even more information about the possible subgroups of A_5. ■

Corollary 2.3. *1. Every p-subgroup of G is contained in a Sylow p-subgroup.*
2. The number n_p of Sylow p-subgroups divides r.

Proof. 1. We know that if P is a Sylow p-subgroup, then so is gPg^{-1}, $g \in G$, by the 2nd theorem. The proof of the theorem itself shows that any p-group is included in gPg^{-1} and we are done.

2. Let the group G act by conjugation on the set of its subgroups. In particular, G acts on the Sylow p-subgroup P, and the orbit of P has size the number of Sylow p-subgroups in G, denoted by n_p. By the Orbit-Stabilizer Theorem, n_p divides $|G| = p^m r$. But p cannot be a prime factor of n_p since $n_p \equiv 1 (mod\ p)$, from which it follows that n_p must divide r. □

MTH-204: Abstract Algebra
Lecture-12

Santosha Kumar Pattanayak

1 Applications of Sylow's theorems

The Sylow Theorems allow us to prove many useful results about finite groups. By using them, we can often conclude a great deal about groups of a particular order if certain hypotheses are satisfied. Recall that a group G is said to be simple if it has no non-trivial normal subgroups.

Example: Using the Sylow Theorems, we can determine that A_5 has subgroups of orders 2, 3, 4, and 5. The Sylow p-subgroups of A_5 have orders 3, 4, and 5. The Third Sylow Theorem tells us exactly how many Sylow p-subgroups A_5 has. Since the number of Sylow 5-subgroups must divide 60 and also be congruent to 1 (mod 5), there are either one or six Sylow 5-subgroups in A_5. All Sylow 5-subgroups are conjugate. If there were only a single Sylow 5-subgroup, it would be conjugate to itself; that is, it would be a normal subgroup of A_5. Since A_5 has no normal subgroups, this is impossible; hence, we have determined that there are exactly six distinct Sylow 5-subgroups of A_5. ■

Theorem 1.1. *If p and q are distinct primes with $p < q$, then every group G of order pq has a single subgroup of order q and this subgroup is normal in G. Hence, G cannot be simple. Furthermore, if $q \not\equiv 1 \pmod{p}$, then G is cyclic.*

Proof. We know that G contains a subgroup H of order q. The number of conjugates of H divides pq and is equal to $1 + kq$ for $k = 0, 1, \ldots$. However, $1 + q$ is already too large to divide the order of the group; hence, H can only be conjugate to itself. That is, H must be normal in G.

The group G also has a Sylow p-subgroup, say K. The number of conjugates of K must divide q and be equal to $1+kp$ for $k = 0, 1, \ldots$. Since q is prime, either $1+kp = q$ or $1+kp = 1$. If $1+kp = 1$, then K is normal in G. In this case, we can easily show that G is an internal direct product of H and K. Since H is isomorphic to $\mathbb{Z}_q$ and K is isomorphic to $\mathbb{Z}_p$, $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. □

Example: Every group of order 15 is cyclic. This is true because $15 = 5 \cdot 3$ and $5 \not\equiv 1 \pmod{3}$. ■

Example: Let us classify all of the groups of order $99 = 3^2 \cdot 11$ up to isomorphism. First we will show that every group G of order 99 is abelian. By the Third Sylow Theorem, there are $1 + 3k$ Sylow 3-subgroups, each of order 9, for some $k = 0, 1, 2, \ldots$. Also, $1 + 3k$ must divide 11; hence, there can only be a single normal Sylow 3-subgroup H in G. Similarly, there are $1 + 11k$ Sylow

11-subgroups and $1 + 11k$ must divide 9. Consequently, there is only one Sylow 11-subgroup K in G. By Corollary 12.5, any group of order p^2 is abelian for p prime; hence, H is isomorphic either to $\mathbb{Z}_3 \times \mathbb{Z}_3$ or to $\mathbb{Z}_9$. Since K has order 11, it must be isomorphic to $\mathbb{Z}_{11}$. Therefore, the only possible groups of order 99 are $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11}$ or $\mathbb{Z}_9 \times \mathbb{Z}_{11}$ up to isomorphism. ■

To determine all of the groups of order $5 \cdot 7 \cdot 47 = 1645$, we need the following theorem.

Theorem 1.2. *Let $G' = \langle [a, b] = aba^{-1}b^{-1} : a, b \in G \rangle$ be the subgroup consisting of all finite products of elements of the form $aba^{-1}b^{-1}$ in a group G. Then G' is a normal subgroup of G and G/G' is abelian.*

Proof. If $y \in G'$ then $g^{-1}yg = yy^{-1}g^{-1}yg = y[y^{-1}, g^{-1}] \in G'$ for all $g \in G$. Hence G' is normal in G. Let $xG', yG' \in G/G'$. Then $[xG', yG'] = xyx^{-1}y^{-1}G' = [x, y]G' = G'$ as $[x, y] \in G'$ for $x, y \in G$. So G/G' is abelian.

□

The subgroup G' of G is called the **commutator subgroup** of G.

Example: We will now show that every group of order $5 \cdot 7 \cdot 47 = 1645$ is abelian, and cyclic by Corollary 8.11. By the Third Sylow Theorem, G has only one subgroup H_1 of order 47. So G/H_1 has order 35 and must be abelian by above theorem. Hence, the commutator subgroup of G is contained in H which tells us that $|G'|$ is either 1 or 47. If $|G'| = 1$, we are done. Suppose that $|G'| = 47$. The Third Sylow Theorem tells us that G has only one subgroup of order 5 and one subgroup of order 7. So there exist normal subgroups H_2 and H_3 in G, where $|H_2| = 5$ and $|H_3| = 7$. In either case the quotient group is abelian; hence, G' must be a subgroup of H_i, $i = 1, 2$. Therefore, the order of G' is 1, 5, or 7. However, we already have determined that $|G'| = 1$ or 47. So the commutator subgroup of G is trivial, and consequently G is abelian. ■

Finite Simple Groups

Given a finite group, one can ask whether or not that group has any normal subgroups. Recall that a simple group is one with no proper nontrivial normal subgroups. As in the case of A_5, proving a group to be simple can be a very difficult task; however, the Sylow Theorems are useful tools for proving that a group is not simple. Usually some sort of counting argument is involved.

Example: Let us show that no group G of order 20 can be simple. By the Third Sylow Theorem, G contains one or more Sylow 5-subgroups. The number of such subgroups is congruent to 1 (mod 5) and must also divide 20. The only possible such number is 1. Since there is only a single Sylow 5-subgroup and all Sylow 5-subgroups are conjugate, this subgroup must be normal. ■

Example: Let G be a finite group of order p^n, $n > 1$ and p prime. We know that, G has a nontrivial center. Since the center of any group G is a normal subgroup, G cannot be a simple group. Therefore, groups of orders 4, 8, 9, 16, 25, 27, 32, 49, 64, and 81 are not simple. In fact, the groups of order 4, 9, 25, and 49 are abelian as these numbers are of the form p^2 for some prime p. ■

Example: No group of order $56 = 2^3 \cdot 7$ is simple. We have seen that if we can show that there is only one Sylow p-subgroup for some prime p dividing 56, then this must be a normal subgroup and we are done. By the Third Sylow Theorem, there are either one or eight Sylow 7-subgroups. If there is only a single Sylow 7-subgroup, then it must be normal.

On the other hand, suppose that there are eight Sylow 7-subgroups. Then each of these subgroups must be cyclic; hence, the intersection of any two of these subgroups contains only the identity of the group. This leaves $8 \cdot 6 = 48$ distinct elements in the group, each of order 7. Now let us count Sylow 2-subgroups. There are either one or seven Sylow 2-subgroups. Any element of a Sylow 2-subgroup other than the identity must have as its order a power of 2; and therefore cannot be one of the 48 elements of order 7 in the Sylow 7-subgroups. Since a Sylow 2-subgroup has order 8, there is only enough room for a single Sylow 2-subgroup in a group of order 56. If there is only one Sylow 2-subgroup, it must be normal. ■

For other groups G it is more difficult to prove that G is not simple. Suppose G has order 48. In this case the technique that we employed in the last example will not work.

Example: To demonstrate that a group G of order 48 is not simple, we will show that G contains either a normal subgroup of order 8 or a normal subgroup of order 16. By the Third Sylow Theorem, G has either one or three Sylow 2-subgroups of order 16. If there is only one subgroup, then it must be a normal subgroup.

Suppose that the other case is true, and two of the three Sylow 2-subgroups are H and K. We claim that $|H \cap K| = 8$. If $|H \cap K| \leq 4$, then,

$$|HK| = \frac{16 \cdot 16}{4} = 64,$$

which is impossible. So $H \cap K$ is normal in both H and K since it has index 2. The normalizer of $H \cap K$ contains both H and K, and $|H \cap K|$ must both be a multiple of 16 greater than 1 and divide 48. The only possibility is that $|N(H \cap K)| = 48$. Hence, $N(H \cap K) = G$. ■

The following famous conjecture of Burnside was proved in a long and difficult paper by Feit and Thompson.

Theorem 1.3. (Odd Order Theorem) *Every finite simple group of nonprime order must be of even order.*

The proof of this theorem laid the groundwork for a program in the 1960s and 1970s that classified all finite simple groups. The success of this program is one of the outstanding achievements of modern mathematics.

MTH-204: Abstract Algebra
Lecture-13

Santosha Kumar Pattanayak

1 Finite Abelian Groups

The ultimate goal of group theory is to classify all groups up to isomorphism; that is, given a particular group, we should be able to match it up with a known group via an isomorphism. For example, we have already proved that any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$; hence, we "know" all finite cyclic groups. It is probably not reasonable to expect that we will ever know all groups; however, we can often classify certain types of groups or distinguish between groups in special cases. In this lecture we will characterize all finite abelian groups.

Note that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ when $\gcd(m, n) = 1$. In fact, much more is true. Every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order; that is, every finite abelian group is isomorphic to a group of the type

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}}.$$

First, let us examine a slight generalization of finite abelian groups. Suppose that G is a group and let $\{g_i\}$ be a set of elements in G, where i is in some index set I (not necessarily finite). The smallest subgroup of G containing all of the g_i's is the subgroup of G **generated** by the g_i's. If this subgroup of G is in fact all of G, then G is generated by the set $\{g_i : i \in I\}$. In this case the g_i's are said to be the **generators** of G. If there is a finite set $\{g_i : i \in I\}$ that generates G, then G is **finitely generated**.

Example: Obviously, all finite groups are finitely generated. For example, the group S_3 is generated by the permutations (12) and (123). The group $\mathbb{Z} \times \mathbb{Z}_n$ is an infinite group but is finitely generated by $\{(1, 0), (0, 1)\}$. ■

Example: Not all groups are finitely generated. Consider the rational numbers $\mathbb{Q}$ under the operation of addition. Suppose that $\mathbb{Q}$ is finitely generated with generators $p_1/q_1, \ldots, p_n/q_n$, where each p_i/q_i is a fraction expressed in its lowest terms. Let p be some prime that does not divide any of the denominators $q_1, \ldots, q_n$. We claim that $1/p$ cannot be in the subgroup of Q that is generated by $p_1/q_1, \ldots, p_n/q_n$, since p does not divide the denominator of any element in this subgroup. This fact is easy to see since the sum of any two generators is

$$p_i/q_i + p_j/q_j = (p_i q_j + p_j q_i)/(q_i q_j).$$

■

Theorem 1.1. *Let H be the subgroup of a group G that is generated by $\{g_i \in G : i \in I\}$. Then $h \in H$ exactly when it is a product of the form*

$$h = g_{i_1}^{\alpha_1} \cdots g_{i_n}^{\alpha_n},$$

where the g_{i_k}'s are not necessarily distinct.

The reason that powers of a fixed g_i may occur several times in the product is that we may have a nonabelian group. However, if the group is abelian, then the g_i's need occur only once. For example, a product such as $a^{-3}b^5a^7$ could always be simplified (in this case, to a^4b^5).

Proof. Let K be the set of all products of the form $g_{i_1}^{\alpha_1} \cdots g_{i_n}^{\alpha_n}$, where the g_{i_k}'s are not necessarily distinct. Certainly K is a subset of H. We need only show that K is a subgroup of G. If this is the case, then $K = H$, since H is the smallest subgroup containing all the g_i's.

Clearly, the set K is closed under the group operation. Since $g_i^0 = 1$, the identity is in K. It remains to show that the inverse of an element $g = g_1^{k_1} \cdots g_{i_n}^{k_n}$ in K must also be in K. However,

$$g^{-1} = (g_1^{k_1} \cdots g_{i_n}^{k_n})^{-1} = (g_1^{-k_n} \cdots g_{i_n}^{-k_1}).$$

□

Now let us restrict our attention to finite abelian groups. We can express any finite abelian group as a finite direct product of cyclic groups. We shall prove that every finite abelian group is isomorphic to a direct product of cyclic p-groups. Before we state the main theorem concerning finite abelian groups, we shall consider a special case.

Theorem 1.2. *A finite abelian group is isomorphic to the direct product of its distinct Sylow subgroups.*

Proof. Let $|G| = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$ where p_i's are distinct primes. Then by Sylow's 1st theorem G has a Sylow p_i subgroup of order $p_i^{m_i}$ for each i. Since G is abelian, all subgroups of G are normal. Since all Sylow p_i-subgroups are conjugate to each other, we have a unique Sylow p_i-subgroup (say H_i) for each i. Since these subgroups are all normal the map $\phi : H_1 \times H_2 \times \cdots \times H_n \to G$ given by $\phi(h_1, h_2, \cdots, h_n) = h_1 h_2 \cdots h_n$ is a group homomorphism. Since the orders of the groups H_i are pairwise coprime, the homomorphism ϕ must be injective, and since the domain and target of ϕ both have the same number of elements, ϕ must, since injective, be bijective. Thus G is isomorphic via ϕ to the direct product of its Sylow subgroups. □

We shall now state the Fundamental Theorem of Finite Abelian Groups.

Theorem 1.3. (Fundamental Theorem of Finite Abelian Groups) *Every finite abelian group G is isomorphic to a direct product of cyclic groups of the form*

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}}$$

where the p_i's are primes (not necessarily distinct).

Example: Suppose that we wish to classify all abelian groups of order $540 = 2^2 \cdot 3^3 \cdot 5$. The Fundamental Theorem of Finite Abelian Groups tells us that we have the following six possibilities.

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$;
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$;
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$;
- $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$;
- $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$;
- $\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$.

■

The proof of the Fundamental Theorem relies on the following lemma.

Lemma 1.4. *Let G be a finite abelian p-group and suppose that $g \in G$ has maximal order. Then G can be written as $\langle g \rangle \times H$ for some subgroup H of G.*

Proof. Suppose that the order of G is p^n. We shall induct on n. If $n = 1$, then G is cyclic of order p and must be generated by g. Suppose now that the statement of the lemma holds for all integers k with $1 \leq k < n$ and let g be of maximal order in G, say $|g| = p^m$. Then $a^{p^m} = e$ for all $a \in G$. Now choose h in G such that $h \notin \langle g \rangle$, where h has the smallest possible order. Certainly such an h exists; otherwise, $G = \langle g \rangle$ and we are done. Let $H = \langle h \rangle$.

We claim that $\langle g \rangle \cap H = \{e\}$. It suffices to show that $|H| = p$. Since $|h^p| = |h|/p$, the order of h^p is smaller than the order of h and must be in $\langle g \rangle$ by the minimality of h; that is, $h^p = g^r$ for some number r. Hence,

$$(g^r)^{p^{m-1}} = (h^p)^{p^{m-1}} = h^{p^m} = e,$$

and the order of g^r must be less than or equal to p^{m-1}. Therefore, g^r cannot generate $\langle g \rangle$. Notice that p must occur as a factor of r, say $r = ps$, and $h^p = g^r = g^{ps}$. Define a to be $g^{-s}h$. Then a cannot be in $\langle g \rangle$; otherwise, h would also have to be in $\langle g \rangle$. Also,

$$a^p = g^{-sp}h^p = g^{-r}h^p = h^{-p}h^p = e.$$

We have now formed an element a with order p such that $a \notin \langle g \rangle$. Since h was chosen to have the smallest order of all of the elements that are not in $\langle g \rangle$, $|H| = p$.

Now we will show that the order of gH in the factor group G/H must be the same as the order of g in G. If $|gH| < |g| = p^m$, then

$$H = (gH)^{p^{m-1}} = g^{p^{m-1}}H;$$

hence, $g^{p^{m-1}}$ must be in $\langle g \rangle \cap H = \{e\}$, which contradicts the fact that the order of g is p^m. Therefore, gH must have maximal order in G/H. By the Correspondence Theorem and our induction hypothesis,

$$G/H \cong \langle gH \rangle \times K/H$$

for some subgroup K of G containing H. We claim that $\langle g\rangle \cap K = \{e\}$. If $b \in \langle g\rangle \cap K$, then $bH \in \langle gH\rangle \cap K/H = \{H\}$ and $b \in \langle g\rangle \cap H = \{e\}$. It follows that $G = \langle g\rangle K$ implies that $G \cong \langle g\rangle \times H$. □

Proof of the Fundamental Theorem: The proof of the Fundamental Theorem of Finite Abelian Groups follows very quickly from the above lemma. Suppose that G is a finite abelian group. Then G is isomorphic to direct product of its Sylow p_i-subgroups. So it is sufficient to show that each Sylow p_i-subgroup H_i is a product of cyclic p_i subgroups. Note that each H_i is of order a power of p_i. Let g be an element of maximal order in H_i. If $\langle g\rangle = H_i$, then we are done; otherwise, $H_i \cong \mathbb{Z}_{|g|} \times K_i$ for some subgroup K_i contained in H_i by the lemma. Since $|K_i| < |H_i|$, by induction K_i is a product of cyclic p_i-subgroups and hence H_i is a product of cyclic p_i subgroups.

We now state the more general theorem for all finitely generated abelian groups. The proof is complicated and we skip it.

Theorem 1.5. (Fundamental Theorem of Finitely Generated Abelian Groups) *Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups of the form*

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

where the p_i's are primes (not necessarily distinct).

MTH-204: Abstract Algebra
Lecture-14

Santosha Kumar Pattanayak

1 Rings

Definition: Let R be a non-empty set which has two laws of composition defined on it. (we call these law "addition" and "multiplication" respectively and use the familiar notation). We say that R is a *ring* if the following hold:

1. $a + b \in R$ and $ab \in R$ $\forall a, b \in R$
2. $a + b = b + a$ $\forall a, b \in R$ (Commutativity of addition)
3. $a + (b + c) = (a + b) + c$ $\forall a, b, c \in R$ (Associativity of addition)
4. There exists an element $0 \in R$ such that $a + 0 = a$ for all $a \in R$
5. Given $a \in R$ there exists an element $-a \in R$ such that $a + (-a) = 0$
6. $a(bc) = (ab)c$ for all $a, b, c \in R$ (Associativity of multiplication)
7. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ (Distributive Laws)

Thus a ring is an additive Abelian group on which an operation of multiplication is defined; this operation being associative and distributive with respect to the addition.

R is called a *commutative ring* if it satisfies in addition $ab = ba$ for all $a, b \in R$. The term *non-commutative ring* usually stands for "a not necessarily commutative ring"

Integral Domain: An integral domain is a commutative ring R with identity $1 \neq 0$ with no zero divisors; that is, $ab = 0$ implies that $a = 0$ or $b = 0$.

Field: A Field is an integral domain in which every nonzero element has a multiplicative inverse.

The following can be deduced from the axioms for a ring:

1. The element 0 is unique
2. Given $a \in R$, $-a$ is uniquely
3. $-(-a) = a$ for all $a \in R$

4. $a + b = a + c$ if and only if $b = c$ for $a, b, c \in R$

5. Given $a, b \in R$, the equation $x + a = b$ has a unique solution $x = b + (-a)$

6. $-(a + b) = -a - b$ for all $a, b \in R$

7. $-(a - b) = -a + b$ for all $a, b \in R$

8. $a \cdot 0 = 0 \cdot a = 0$ for all $a \in R$

9. $a(-b) = (-a)b = -ab$ for all $a, b \in R$

10. $(-a)(-b) = ab$ for all $a, b \in R$

11. $a(b - c) = ab - ac$ for all $a, b, c \in R$

Examples: 1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are rings with usual addition and multiplication.

2. For a ring R, the set of all $n \times n$ matrices $M_n(R)$ is a non-commutative ring with respect to usual matrix addition and multiplication.

3. The integers modulo n: $\mathbb{Z}_n$ form a commutative ring with identity under addition and multiplication modulo n.

4. The quaternions $\mathbb{H} = \{a + ib + jc + kd | a, b, c, d \in \mathbb{R}\}$ form a non-commutative ring with identity under the appropriate addition and a multiplication which satisfies the rules: $i^2 = j^2 = k^2 = ijk = -1$. In fact one can find an inverse for any non-zero quaternion using the trick: $(a + ib + jc + kd)(a - ib - jc - kd) = a^2 + b^2 + c^2 + d^2$ as in the similar method for finding the inverse of a complex number.

5. $C(\mathbb{R}) = \{f : \mathbb{R} \to R : f \textit{ is continuous}\}$ is a non-commutative ring under the operations $fg(x) = f(x)g(x)$ and $(f + g)(x) = f(x) + g(x)$.

6. The set 2^A of all subsets of a set A is a ring. The addition is the symmetric difference $\triangle(A, B) = (A \setminus B) \cup (B \setminus A)$ and the multiplication the set operation intersection $\cap$. Its additive identity is the empty set $\emptyset$, and its multiplicative identity is the set A.

7. For any group G and for a ring R, the group ring $R[G]$ is the set of formal sums $\sum r_i g_i$ of elements of G with coefficients in R.

8. For a ring R, the ring of formal power series in x denoted by $R[[x]]$.

9. For a ring R the ring of formal Laurent series in x is denoted by $R((x))$.

10. $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ with usual addition and multiplication of complex numbers is a commutative ring with identity called the ring of Gaussian integers.

11. For a ring R, the set of polynomials in n variables $x_1, x_2, \cdots, x_n$ denoted by $R[x_1, x_2, \cdots, x_n]$ is a ring with usual polynomial addition and multiplication.

1.1 Subrings and Ideals

A subset S of a ring R is called a *subring* of R if S itself is a ring with respect to the laws of composition of R.

Lemma 1.1. *A non-empty subset S of a ring R is a subring of R if and only if $a - b \in S$ and $ab \in S$ whenever $a, b \in S$*

Proof. If S is a subring then obviously the given condition is satisfied. Conversely, suppose that the condition holds. Take any $a \in S$. We have $a - a \in S$ hence $0 \in S$. Hence for any $x \in S$ we have $0 - x \in S$ so $-x \in S$. Finally, if $a, b \in S$ then by the above $-b \in S$. Therefore $a - (-b) \in S$, i.e., $a + b \in S$. So S is closed with respect to both addition and multiplication. Thus S is a subring since all the other axioms are automatically satisfied. □

Ideal: A subset I of a ring R is called an *ideal* if

1. I is a subring of R
2. For all $a \in I, r \in R$ $ar \in I$ and $ra \in I$

If I is an ideal of R we denote this fact by $I \lhd R$.

Proposition 1.2. *A non-empty subset I of a ring R is an ideal of R if and only if $a - b \in I, ar \in I$ and $ra \in I$ whenever $a, b \in I$ and $r \in R$*

Proof. Easy. □

1.2 Cosets and Homomorphism

Let I be an ideal of a ring R and $x \in R$. Then the set of elements $\{x + i : i \in I\}$ is called the *coset* of x in R with respect to I. It is denoted by $x + I$

When dealing with cosets, it is more important to realise that, in general, a given coset can be represented in more than one way. The next lemma shows how the coset representatives are related.

Lemma 1.3. *Let R be a ring with an ideal I and $x, y \in R$. Then $x + I = y + I \iff x - y \in I$*

Proof. Easy. □

We denote the set of all cosets of R with respect to I by R/I. We can give R/I the structure of a ring as follows: Define $(x + I) + (y + I) = (x + y) + I$ and $(x + I)(y + I) = xy + I$ for $x, y \in R$.

The key point here is that the sum and the product of R/I are well-defined, that is, they are independent of the coset representatives chosen.

The ring R/I is called the *residue class ring* of R with respect to I

The zero element of R/I is $0 + I = i + I$ for any $i \in I$. If S is a subset of R with $S \supseteq I$ we denote by S/I the subset $\{s + I : s \in S\}$ of R/I.

Proposition 1.4. *Let I be an ideal of a ring R. Then*

1. *Every ideal of the ring R/I is of the form K/I where K is an ideal of R and $K \supseteq I$. Also conversely, if K is an ideal of R and $K \supseteq I$ then K/I is an ideal of R/I*

2. *There is a one to one correspondence between ideals of the ring R/I and the ideals of R containing I*

Proof. 1. If J is an ideal of R/I, define $K = \{x \in R : x + I \in J\}$. Then K is an ideal of R containing I.

2. The correspondence is given by $K \leftrightarrow K/I$ where K is an ideal of R containing I.

□

Homomorphism: A mapping θ of a ring R into a ring S is said to be a (ring) *homomorphism* if $\theta(x + y) = \theta(x) + \theta(y)$ and $\theta(xy) = \theta(x)\theta(y)$ for all $x, y \in R$.

θ defined by $\theta(r) = 0$ for all $r \in R$ is a homomorphism. It is called the *zero homomorphism.*

ϕ defined by $\phi(r) = r$ for all $r \in R$ is also a homomorphism. It is called the *identity homomorphism*

Let I be an ideal of R. Then $\sigma : R \to R/I$ defined by $\sigma(x) = x + I$ for all $x \in R$ is a homomorphism of R onto R/I. This is called the *natural* (or *canonical*) *homomorphism.*

Lemma 1.5. *Let R, S be rings and $\theta : R \to S$ a homomorphism. Then :*

1. $\theta(0_R) = 0_S$

2. $\theta(-r) = -\theta(r)$ *for all* $r \in R$

3. $K = \{x \in R : \theta(x) = 0_S\}$ *is an ideal of* R

4. $\theta R = \{\theta(r) : r \in R\}$ *is a subring of* S

Proof. Easy. □

K is called the *kernel* of θ and θR is called the (homomorphic) *image* of R. The ideal K is sometimes denoted by $\ker \theta$.

Isomorphism: Let θ be a homomorphism of a ring R into a ring S. Then θ is called an *isomorphism* if θ is a one to one and onto map. We say that R and S are isomorphic rings and denote this by $R \cong S$.

1.3 The Isomorphism Theorems

Question: Given a ring R, what rings can occur as its homomorphic images?

The importance of the first isomorphism theorem lies in the fact that it shows the answer to lie with R itself. It tells us that if we know all the ideals of R then we know all the homomorphic images of R. Only the first isomorphism theorem contains new information. The other two are simply its application.

Theorem 1.6. *Let θ be a homomorphism of a ring R into a ring S. Then $\theta R \cong R/I$ where $I = \ker\theta$*

Proof. Define $\sigma : R/I \to R$ by $\sigma(x+I) = \theta(x)$ for all $x \in R$. The map σ is well defined since for $x, y \in R$, $x + I = y + I \Rightarrow x - y \in I = \ker\theta \Rightarrow \theta(x-y) = 0 \Rightarrow \theta(x) = \theta(y)$. The map σ is easily seen to be the required isomorphism. □

Theorem 1.7. *Let I be an ideal and L a subring of a ring R. Then $L/(L \cap I) \cong (L+I)/I$*

Proof. Let σ be the natural homomorphism $R \to R/I$. Restrict σ to the ring L. We have $\sigma L = (L+I)/I$. The kernel of σ restricted to L is $L \cap I$. Now apply previous theorem. □

Theorem 1.8. *Let I, K be ideals of a ring R such that $I \subseteq K$. Then $(R/I)/(K/I) \cong R/K$*

Proof. K/I is an ideal of R/I and so $(R/I)/(K/I)$ is defined. Define a map $\gamma : R/I \to R/K$ by $\gamma(x+I) = x + K$ for all $x \in R$. The map γ is easily seen to be well defined and a homomorphism onto R/K. Further,

$$\begin{aligned} \gamma(x+I) = K &\iff x + K = K \\ &\iff x \in K \\ &\iff x + I \in K/I \end{aligned}$$

Therefore $\ker\gamma = K/I$. Now apply the first isomorphism theorem. □

MTH-204: Abstract Algebra
Lecture-15

Santosha Kumar Pattanayak

1 Prime and Maximal Ideals

1.1 Zorn's Lemma, Well-ordering Principle, The Axiom of Choice

1. A non-empty set $\mathfrak{S}$ is said to be *partially ordered* if there exists a binary relation $\leq$ in $\mathfrak{S}$ which is defined for certain pairs of elements in $\mathfrak{S}$ and satisfies:
   (a) $a \leq a$
   (b) $a \leq b$, $b \leq c \Rightarrow a \leq c$
   (c) $a \leq b$, $b \leq a \Rightarrow a = b$
2. Let $\mathfrak{S}$ be a partially ordered set. A non-empty subset τ is said to be *totally ordered* if for every pair $a, b \in \tau$ we have either $a \leq b$ or $b \leq a$
3. Let $\mathfrak{S}$ be a partially ordered set. An elements $x \in \mathfrak{S}$ is called a *maximal element* if $x \leq y$ with $y \in \mathfrak{S} \Rightarrow x = y$. Similarly, for a *minimal* element
4. Let τ be a totally ordered subset of a partially ordered set $\mathfrak{S}$. We say that τ has an *upper bound* in $\mathfrak{S}$ if there exists $c \in \mathfrak{S}$ such that $x \leq c$ for all $x \in \tau$.

Theorem 1.1 (Zorn's Lemma (Axiom)). *If a partially ordered set $\mathfrak{S}$ has the property that every totally ordered subset of $\mathfrak{S}$ has an upper bound in $\mathfrak{S}$, then $\mathfrak{S}$ contains a maximal element.*

A non-empty set $\mathfrak{S}$ is said to be *well-ordered* if it is totally ordered and every non-empty subset of $\mathfrak{S}$ has a minimal element.

Theorem 1.2 (The Well ordering Principle). *Any non-empty set can be well-ordered.*

The Axiom of Choice: Given a class of sets, there exists a "choice function", i.e., a function which assigns to each of these sets one of its elements.

It can be shown that Axiom of Choice is logically equivalent to Zorn's Lemma which is logically equivalent to the Well-ordering Principle.

Maximal Ideal: An ideal I of a ring R is said to be maximal if $I \neq R$ and I is not properly contained in any other ideal of R.

Ideal Generators: If R is commutative and has a 1, then the ideal of R generated by a subset A of R is defined by:

$$< A >= \{r_1a_1 + \cdots + r_na_n \mid r_i \in R, a_i \in A, n \in \mathbb{N}\}.$$

Proposition 1.3. *Let $I \neq R$ be an ideal of a ring R. Then there exists a maximal ideal M of R such that $M \supseteq I$.*

Proof. We will prove this by using Zorn's Lemma. Let $\mathfrak{S}$ be the set of all proper ideals of R containing I. Partially order $\mathfrak{S}$ by inclusion. Let $\{T_\alpha\}_{\alpha\in\Lambda}$ be a totally ordered subset of $\mathfrak{S}$. Let $T = \cup_{\alpha\in\Lambda}T_\alpha$. Then $T \lhd_r R$ and $T \supseteq I$. Moreover T is proper since $T = R \Rightarrow 1 \in T \Rightarrow 1 \in T_\alpha$ for some $\alpha \in \Lambda \Rightarrow T_\alpha = R$. Thus $T \neq R$ and so $T \in \mathfrak{S}$. Thus $T \neq R$ and so $T \in \mathfrak{S}$. Now $T \supseteq T_\alpha$ for all $\alpha \in \Lambda$. Hence Zorn's Lemma applies and $\mathfrak{S}$ contains a maximal element, say M. Clearly M is a maximal ideal and $M \supseteq I$. □

Corollary 1.4. *A ring with identity contains a maximal ideal.*

Proof. Take $I = 0$ in the above theorem. □

Remark: This is not true for rings without 1. For example take the abelian group $(\mathbb{Q}, +)$ and define the multiplication of any two elements to be zero, i.e., $xy = 0$ for any x, y. Then this is a ring without a maximal ideal because $(\mathbb{Q}, +)$ doesn't have a maximal subgroup.

Lemma 1.5. *A (non-zero) ring R is a field if and only if its only ideals are $\{0\}$ and R.*

Note that we don't need elements to define the ideals $\{0\}$ and R. $\{0\}$ can be defined as the ideal that all other ideals contain, and R is the ideal that contains all other ideals. Alternatively, we can reword this as "R is a field if and only if it has only two ideals" to avoid mentioning explicit ideals.

Proof. ($\Rightarrow$) Let I be an ideal of R and R be a field. Suppose $x \neq 0 \in I$. Then as x is a unit, $I = R$.

($\Leftarrow$) Suppose $x \neq 0 \in R$. Then the ideal generated by x, (x) is an ideal of R. It is not $\{0\}$ since it contains x. So $(x) = R$. In other words $1_R \in (x)$. But (x) is defined to be $\{y.x : y \in R\}$. So there is some $u \in R$ such that $u.x = 1_R$. So x is a unit. Since x was arbitrary, R is a field. □

This is another reason why fields are special. They have the simplest possible ideal structure. There is an easy way to recognize if an ideal is maximal.

Lemma 1.6. *An ideal I of R is maximal if and only if R/I is a field.*

Proof. R/I is a field if and only if $\{0\}$ and R/I are the only ideals of R/I. By the ideal correspondence, this is equivalent to saying I and R are the only ideals of R which contains I, i.e. I is maximal. So done. □

This is a nice result. This makes a correspondence between properties of ideals I and properties of the quotient R/I. Here is another one:

Prime Ideal: An ideal I of a ring R is said to be a prime ideal if $ab \in I$ for $a, b \in R$ then either $a \in I$ or $b \in I$.

Examples: A non-zero ideal $n\mathbb{Z}$ of $\mathbb{Z}$ is prime if and only if n is a prime.

To show this, first suppose $n = p$ is a prime, and $a \cdot b \in p\mathbb{Z}$. So $p \mid a \cdot b$. So $p \mid a$ or $p \mid b$, i.e. $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

For the other direction, suppose $n = pq$ is a composite number $(p, q \neq 1)$. Then $n \in n\mathbb{Z}$ but $p \notin n\mathbb{Z}$ and $q \notin n\mathbb{Z}$, since $0 < p, q < n$.

So instead of talking about prime numbers, we can talk about prime ideals instead, because ideals are better than elements.

We prove a result similar to the above:

Lemma 1.7. *An ideal I of R is prime if and only if R/I is an integral domain.*

Proof. Let I be prime. Let $a + I, b + I \in R/I$, and suppose $(a + I)(b + I) = 0_{R/I}$. By definition, $(a+I)(b+I) = ab+I$. So we must have $ab \in I$. As I is prime, either $a \in I$ or $b \in I$. So $a+I = 0_{R/I}$ or $b + I = 0_{R/I}$. So R/I is an integral domain.

Conversely, suppose R/I is an integral domain. Let $a, b \in R$ be such that $ab \in I$. Then $(a + I)(b + I) = ab + I = 0_{R/I} \in R/I$. Since R/I is an integral domain, either $a + I = 0_{R/I}$ or $b + I = 0_{R/i}$, i.e. $a \in I$ or $b \in I$. So I is a prime ideal. □

Prime ideals and maximal ideals are the main types of ideals we care about. Note that every field is an integral domain. So we immediately have the following result:

Proposition 1.8. *Every maximal ideal is a prime ideal.*

Proof. An ideal I of R is maximal implies R/I is a field implies R/I is an integral domain implies I is prime. □

The converse is not true. For example, $\{0\} \subseteq \mathbb{Z}$ is prime but not maximal. Less stupidly, $(X) \in \mathbb{Z}[X, Y]$ is prime but not maximal (since $\mathbb{Z}[X, Y]/(X) \cong \mathbb{Z}[Y]$). We can provide a more explicit proof of this, which is essentially the same.

Alternative proof. Let I be a maximal ideal, and suppose $a, b \notin I$ but $ab \in I$. Then by maximality, $I+(a) = I+(b) = R = (1)$. So we can find some $p, q \in R$ and $n, m \in I$ such that $n+ap = m+bq = 1$. Then

$$1 = (n + ap)(m + bq) = nm + apm + bqn + abpq \in I,$$

since $n, m, ab \in I$. This is a contradiction. □

Note that for any ring R, there is a unique ring homomorphism $\mathbb{Z} \to R$, given by

$$\begin{aligned} \iota : \mathbb{Z} &\to R \\ n \geq 0 &\mapsto \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}} \\ n \leq 0 &\mapsto -(\underbrace{1_R + 1_R + \cdots + 1_R}_{-n \text{ times}}) \end{aligned}$$

Any homomorphism $\mathbb{Z} \to R$ must be given by this formula, since it must send the unit to the unit, and we can show this is indeed a homomorphism by distributivity. So the ring homomorphism is unique.

We then know $\ker(\iota)$ is an ideal of $\mathbb{Z}$. Thus $\ker(\iota) = n\mathbb{Z}$ for some n.

Characteristic of a ring: Let R be a ring, and $\iota : \mathbb{Z} \to R$ be the unique such map. The *characteristic* of R is the unique non-negative n such that $\ker(\iota) = n\mathbb{Z}$.

Example: The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ all have characteristic 0. The ring $\mathbb{Z}/n\mathbb{Z}$ has characteristic n. In particular, all natural numbers can be characteristics.

Lemma 1.9. *Let R be an integral domain. Then its characteristic is either 0 or a prime number.*

Proof. Consider the unique map $\phi : \mathbb{Z} \to R$, and $\ker(\phi) = n\mathbb{Z}$. Then n is the characteristic of R by definition.

By the first isomorphism theorem, $\mathbb{Z}/n\mathbb{Z} = Im(\phi) \leq R$. So $\mathbb{Z}/n\mathbb{Z}$ is an integral domain. So $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. So $n = 0$ or a prime number. □

MTH-204: Abstract Algebra
Lecture-16

Santosha Kumar Pattanayak

1 Integral Domain and Field of Fractions

Lemma 1.1. *Let R be a finite ring which is an integral domain. Then R is a field.*

Proof. Let $a \in R$ be non-zero, and consider the ring homomorphism

$$\begin{aligned} a \cdot - : R &\to R \\ b &\mapsto a \cdot b \end{aligned}$$

We want to show this is injective. For this, it suffices to show the kernel is trivial. If $r \in \ker(a \cdot -)$, then $a \cdot r = 0$. So $r = 0$ since R is an integral domain. So the kernel is trivial.

Since R is finite, $a \cdot -$ must also be surjective. In particular, there is an element $b \in R$ such that $a \cdot b = 1_R$. So a has an inverse. Since a was arbitrary, R is a field. □

So far, we know fields are integral domains, and subrings of integral domains are integral domains. We have another good source of integral domain as follows:

Lemma 1.2. *Let R be an integral domain. Then $R[X]$ is also an integral domain.*

Proof. We need to show that the product of two non-zero elements is non-zero. Let $f, g \in R[X]$ be non-zero, say

$$\begin{aligned} f &= a_0 + a_1 X + \cdots + a_n X^n \in R[X] \\ g &= b_0 + b_1 X + \cdots + b_m X^m \in R[X], \end{aligned}$$

with $a_n, b_m \neq 0$. Then the coefficient of X^{n+m} in fg is $a_n b_m$. This is non-zero since R is an integral domain. So fg is non-zero. So $R[X]$ is an integral domain. □

So, for instance, $\mathbb{Z}[X]$ is an integral domain.

We can also iterate this.

Notation 1.3. *Write $R[X, Y]$ for $(R[X])[Y]$, the polynomial ring of R in two variables. In general, write $R[X_1, \cdots, X_n] = (\cdots((R[X_1])[X_2])\cdots)[X_n]$.*

Then if R is an integral domain, so is $R[X_1, \cdots, X_n]$.

We now mimic the familiar construction of $\mathbb{Q}$ from $\mathbb{Z}$. For any integral domain R, we want to construct a field F that consists of "fractions" of elements in R. Recall that a subring of any field is an integral domain. This says the converse — every integral domain is the subring of some field.

Field of fractions Let R be an integral domain. A *field of fractions* F of R is a field with the following properties

1. $R \leq F$
2. Every element of F may be written as $a \cdot b^{-1}$ for $a, b \in R$, where b^{-1} means the multiplicative inverse to $b \neq 0$ in F.

For example, $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$.

Theorem 1.4. *Every integral domain has a field of fractions.*

Proof. The construction is exactly how we construct the rationals from the integers — as equivalence classes of pairs of integers. We let

$$S = \{(a, b) \in R \times R : b \neq 0\}.$$

We think of $(a, b) \in S$ as $\frac{a}{b}$. We define the equivalence relation $\sim$ on S by

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

We need to show this is indeed a equivalence relation. Symmetry and reflexivity are obvious. To show transitivity, suppose

$$(a, b) \sim (c, d), \quad (c, d) \sim (e, f),$$

i.e.

$$ad = bc, \quad cf = de.$$

We multiply the first equation by f and the second by b, to obtain

$$adf = bcf, \quad bcf = bed.$$

Rearranging, we get

$$d(af - be) = 0.$$

Since d is in the denominator, $d \neq 0$. Since R is an integral domain, we must have $af - be = 0$, i.e. $af = be$. So $(a, b) \sim (e, f)$. This is where being an integral domain is important.

Now let

$$F = S/\sim$$

be the set of equivalence classes. We now want to check this is indeed the field of fractions. We first want to show it is a field. We write $\frac{a}{b} = [(a, b)] \in F$, and define the operations by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

These *are* well-defined, and make $(F, +, \cdot, \frac{0}{1}, \frac{1}{1})$ into a ring. There are many things to check, but those are straightforward, and we will not waste time doing that here.

Finally, we need to show every non-zero element has an inverse. Let $\frac{a}{b} \neq 0_F$, i.e. $\frac{a}{b} \neq \frac{0}{1}$, or $a \cdot 1 \neq b \cdot 0 \in R$, i.e. $a \neq 0$. Then $\frac{b}{a} \in F$ is defined, and

$$\frac{b}{a} \cdot \frac{a}{b} = \frac{ba}{ba} = 1_F.$$

So $\frac{a}{b}$ has a multiplicative inverse. So F is a field.

We now need to construct a subring of F that is isomorphic to R. To do so, we need to define an injective isomorphism $\phi : R \to F$. This is given by

$$\begin{aligned} \phi : R &\to F \\ r &\mapsto \frac{r}{1}. \end{aligned}$$

This is a ring homomorphism, as one can check easily. The kernel is the set of all $r \in R$ such that $\frac{r}{1} = 0$, i.e. $r = 0$. So the kernel is trivial, and ϕ is injective. Then by the first isomorphism theorem, $R \cong Im(\phi) \subseteq F$.

Finally, we need to show everything is a quotient of two things in R. We have

$$\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1},$$

as required. □

This gives us a very useful tool. Since this gives us a field from an integral domain, this allows us to use field techniques to study integral domains. Moreover, we can use this to construct new interesting fields from integral domains.

Example Consider the integral domain $\mathbb{C}[X]$. Its field of fractions is the field of all rational functions $\frac{p(X)}{q(X)}$, where $p, q \in \mathbb{C}[X]$.

1.1 Factorization in integral domains

We now move on to tackle the problem of factorization in rings. For sanity, we suppose throughout the section that R is an integral domain. We start by making some definitions.

Unit: An element $a \in R$ is a *unit* if there is a $b \in R$ such that $ab = 1_R$. Equivalently, if the ideal $(a) = R$.

Division: For elements $a, b \in R$, we say a *divides* b, written $a \mid b$, if there is a $c \in R$ such that $b = ac$. Equivalently, if $(b) \subseteq (a)$.

Associates: We say $a, b \in R$ are *associates* if $a = bc$ for some unit c. Equivalently, if $(a) = (b)$. Equivalently, if $a \mid b$ and $b \mid a$.

In the integers, this can only happen if a and b differ by a sign, but in more interesting rings, more interesting things can happen.

When considering division in rings, we often consider two associates to be "the same". For example, in $\mathbb{Z}$, we can factorize 6 as

$$6 = 2 \cdot 3 = (-2) \cdot (-3),$$

but this does not violate unique factorization, since 2 and -2 are associates (and so are 3 and -3), and we consider these two factorizations to be "the same".

Irreducible We say $a \in R$ is *irreducible* if $a \neq 0$, a is not a unit, and if $a = xy$, then x or y is a unit.

For integers, being irreducible is the same as being a prime number. However, "prime" means something different in general rings.

Prime: We say $a \in R$ is *prime* if a is non-zero, not a unit, and whenever $a \mid xy$, either $a \mid x$ or $a \mid y$.

It is important to note all these properties depend on the ring, not just the element itself. **Example:** $2 \in \mathbb{Z}$ is a prime, but $2 \in \mathbb{Q}$ is not (since it is a unit).

Similarly, the polynomial $2X \in \mathbb{Q}[X]$ is irreducible (since 2 is a unit), but $2X \in \mathbb{Z}[X]$ not irreducible.

We have two things called prime, so they had better be related.

Lemma 1.5. *A principal ideal (r) is a prime ideal in R if and only if $r = 0$ or r is prime.*

Proof. ($\Rightarrow$) Let (r) be a prime ideal. If $r = 0$, then done. Otherwise, as prime ideals are proper, i.e. not the whole ring, r is not a unit. Now suppose $r \mid a \cdot b$. Then $a \cdot b \in (r)$. But (r) is prime. So $a \in (r)$ or $b \in (r)$. So $r \mid a$ or $r \mid b$. So r is prime.

($\Leftarrow$) If $r = 0$, then $(0) = \{0\} \lhd R$, which is prime since R is an integral domain. Otherwise, let $r \neq 0$ be prime. Suppose $a \cdot b \in (r)$. This means $r \mid a \cdot b$. So $r \mid a$ or $r \mid b$. So $a \in (r)$ and $b \in (r)$. So (r) is prime. □

Note that in $\mathbb{Z}$, prime numbers exactly match the irreducibles, but prime numbers are also prime (surprise!). In general, it is not true that irreducibles are the same as primes. However, one direction is always true.

Lemma 1.6. *Let $r \in R$ be prime. Then it is irreducible.*

Proof. Let $r \in R$ be prime, and suppose $r = ab$. Since $r \mid r = ab$, and r is prime, we must have $r \mid a$ or $r \mid b$. wlog, $r \mid a$. So $a = rc$ for some $c \in R$. So $r = ab = rcb$. Since we are in an integral domain, we must have $1 = cb$. So b is a unit. □

We now do a long interesting example.

Example: Let

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \leq \mathbb{C}.$$

By definition, it is a subring of a field. So it is an integral domain. What are the units of the ring? There is a nice trick we can use, when things are lying inside $\mathbb{C}$. Consider the function

$$N : R \to \mathbb{Z}_{\geq 0}$$

given by

$$N(a + b\sqrt{-5}) \mapsto a^2 + 5b^2.$$

It is convenient to think of this as $z \mapsto z\bar{z} = |z|^2$. This satisfies $N(z \cdot w) = N(z)N(w)$. This is a desirable thing to have for a ring, since it immediately implies all units have norm 1 — if $r \cdot s = 1$, then $1 = N(1) = N(rs) = N(r)N(s)$. So $N(r) = N(s) = 1$.

So to find the units, we need to solve $a^2 + 5b^2 = 1$, for a and b units. The only solutions are ± 1. So only $\pm 1 \in R$ can be units, and these obviously are units. So these are all the units.

Next, we claim $2 \in R$ is irreducible. We again use the norm. Suppose $2 = ab$. Then $4 = N(2) = N(a)N(b)$. Now note that nothing has norm 2. $a^2 + 5b^2$ can never be 2 for integers $a, b \in \mathbb{Z}$. So we must have, wlog, $N(a) = 4, N(b) = 1$. So b must be a unit. Similarly, we see that $3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible (since there is also no element of norm 3).

We have four irreducible elements in this ring. Are they prime? No! Note that

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

We now claim 2 does not divide $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$. So 2 is not prime.

To show this, suppose $2 \mid 1 + \sqrt{-5}$. Then $N(2) \mid N(1 + \sqrt{-5})$. But $N(2) = 4$ and $N(1 + \sqrt{-5}) = 6$, and $4 \nmid 6$. Similarly, $N(1 - \sqrt{-5}) = 6$ as well. So $2 \nmid 1 \pm \sqrt{-5}$.

There are several life lessons here. First is that primes and irreducibles are not the same thing in general. We've always thought they were the same because we've been living in the fantasy land of the integers. But we need to grow up.

The second one is that factorization into irreducibles is not necessarily unique, since $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are two factorizations into irreducibles.

However, there is one situation when unique factorizations holds. This is when we have a Euclidean algorithm available.

MTH-204: Abstract Algebra
Lecture-17

Santosha Kumar Pattanayak

1 Euclidean Domain, Principal Ideal Domain and Unique Factorization Domain

Euclidean domain: An integral domain R is a *Euclidean domain* (ED) if there is a *Euclidean function* $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that

1. $\phi(a \cdot b) \geq \phi(b)$ for all $a, b \neq 0$
2. If $a, b \in R$, with $b \neq 0$, then there are $q, r \in R$ such that

$$a = b \cdot q + r,$$

and either $r = 0$ or $\phi(r) < \phi(b)$.

Example: (1) $\mathbb{Z}$ is a Euclidean domain with $\phi(n) = |n|$.

(2) For any field $\mathbb{F}$, $\mathbb{F}[X]$ is a Euclidean domain with

$$\phi(f) = \deg(f).$$

(3) The Gaussian integers $R = \mathbb{Z}[i] \leq \mathbb{C}$ is a Euclidean domain with $\phi(z) = N(z) = |z|^2$.

Before we move on to prove unique factorization, we first derive something we've previously mentioned. Recall we showed that every ideal in $\mathbb{Z}$ is principal, and we proved this by the Euclidean algorithm. So we might expect this to be true in an arbitrary Euclidean domain.

Principal ideal domain A ring R is a *principal ideal domain* (PID) if it is an integral domain, and every ideal is a principal ideal, i.e. for all ideal I of R, there is some a such that $I = (a)$.

Example: $\mathbb{Z}$ is a principal ideal domain.

Proposition 1.1. *Let R be a Euclidean domain. Then R is a principal ideal domain.*

We have already proved this, just that we did it for a particular Euclidean domain $\mathbb{Z}$. Nonetheless, we shall do it again.

Proof. Let R have a Euclidean function $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$. We let I be a non-zero ideal of R, and let $b \in I \setminus \{0\}$ be an element with $\phi(b)$ minimal. Then for any $a \in I$, we write

$$a = bq + r,$$

with $r = 0$ or $\phi(r) < \phi(b)$. However, any such r must be in I since $r = a - bq \in I$. So we cannot have $\phi(r) < \phi(b)$. So we must have $r = 0$. So $a = bq$. So $a \in (b)$. Since this is true for all $a \in I$, we must have $I \subseteq (b)$. On the other hand, since $b \in I$, we must have $(b) \subseteq I$. So we must have $I = (b)$. □

This is exactly, word by word, the same proof as we gave for the integers, except we replaced the absolute value with ϕ.

Example: $\mathbb{Z}$ is a Euclidean domain, and hence a principal ideal domain. Also, for any field $\mathbb{F}$, $\mathbb{F}[X]$ is a Euclidean domain, hence a principal ideal domain.

Also, $\mathbb{Z}[i]$ is a Euclidean domain, and hence a principal ideal domain.

What is a non-example of principal ideal domains?

In $\mathbb{Z}[X]$, the ideal $(2, X)$ is not a principal ideal. Suppose it were. Then $(2, X) = (f)$. Since $2 \in (2, X) = (f)$, we know $2 \in (f)$, i.e. $2 = f \cdot g$ for some g. So f has degree zero, and hence constant. So $f = \pm 1$ or ± 2.

If $f = \pm 1$, since ± 1 are units, then $(f) = \mathbb{Z}[X]$. But $(2, X) \neq \mathbb{Z}[X]$, since, say, $1 \notin (2, X)$. If $f = \pm 2$, then since $X \in (2, X) = (f)$, we must have $\pm 2 \mid X$, but this is clearly false. So $(2, X)$ cannot be a principal ideal.

Example: Let $A \in M_{n\times n}(\mathbb{F})$ be an $n \times n$ matrix over a field $\mathbb{F}$. We consider the following set

$$I = \{f \in \mathbb{F}[X] : f(A) = 0\}.$$

This is an ideal — if $f, g \in I$, then $(f + g)(A) = f(A) + g(A) = 0$. Similarly, if $f \in I$ and $h \in \mathbb{F}[X]$, then $(fg)(A) = f(A)g(A) = 0$.

But we know $\mathbb{F}[X]$ is a principal ideal domain. So there must be some $m \in \mathbb{F}[X]$ such that $I = (m)$ for some m.

Suppose $f \in \mathbb{F}[X]$ such that $f(A) = 0$, i.e. $f \in I$. Then $m \mid f$. So m is a polynomial that divides all polynomials that kill A, i.e. m is the *minimal polynomial* of A.

We have just proved that all matrices have minimal polynomials, and that the minimal polynomial divides all other polynomials that kill A. Also, the minimal polynomial is unique up to multiplication of units.

Let's get further into number theory-like things. For a general ring, we cannot factorize things into irreducibles uniquely. However, in some rings, this is possible.

Unique factorization domain: An integral domain R is a *unique factorization domain* (UFD) if

1. Every non-unit may be written as a product of irreducibles;

2. If $p_1 p_2 \cdots p_n = q_1 \cdots q_m$ with p_i, q_j irreducibles, then $n = m$, and they can be reordered such that p_i is an associate of q_i.

This is a really nice property, and here we can do things we are familiar with in number theory. So how do we know if something is a unique factorization domain?

Our goal is to show that all principal ideal domains are unique factorization domains. To do so, we are going to prove several lemmas that give us some really nice properties of principal ideal domains.

Recall we saw that every prime is an irreducible, but in $\mathbb{Z}[\sqrt{-5}]$, there are some irreducibles that are not prime. However, this cannot happen in principal ideal domains.

Lemma 1.2. *Let R be a principal ideal domain. If $p \in R$ is irreducible, then it is prime.*

Note that this is also true for general unique factorization domains, which we can prove directly by unique factorization.

Proof. Let $p \in R$ be irreducible, and suppose $p \mid a \cdot b$. Also, suppose $p \nmid a$. We need to show $p \mid b$.

Consider the ideal $(p, a) \lhd R$. Since R is a principal ideal domain, there is some $d \in R$ such that $(p, a) = (d)$. So $d \mid p$ and $d \mid a$.

Since $d \mid p$, there is some q_1 such that $p = q_1 d$. As p is irreducible, either q_1 or d is a unit.

If q_1 is a unit, then $d = q_1^{-1} p$, and this divides a. So $a = q_1^{-1} p x$ for some x. This is a contradiction, since $p \nmid a$.

Therefore d is a unit. So $(p, a) = (d) = R$. In particular, $1_R \in (p, a)$. So suppose $1_R = rp + sa$, for some $r, s \in R$. We now take the whole thing and multiply by b. Then we get

$$b = rpb + sab.$$

We observe that ab is divisible by p, and so is p. So b is divisible by p. So done. □

This is similar to the argument for integers. For integers, we would say if $p \nmid a$, then p and a are coprime. Therefore there are some r, s such that $1 = rp + sa$. Then we continue the proof as above. Hence what we did in the middle is to do something similar to showing p and a are "coprime".

Another nice property of principal ideal domains is the following:

Lemma 1.3. *Let R be a principal ideal domain. Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be a chain of ideals. Then there is some $N \in \mathbb{N}$ such that $I_n = I_{n+1}$ for some $n \geq N$.*

So in a principal ideal domain, we cannot have an infinite chain of bigger and bigger ideals.

Ascending chain condition: A ring satisfies the *ascending chain condition* (ACC) if there is no infinite strictly increasing chain of ideals.

Noetherian ring: A ring that satisfies the ascending chain condition is known as a *Noetherian ring*.

So we are proving that every principal ideal domain is Noetherian.

Proof. The obvious thing to do when we have an infinite chain of ideals is to take the union of them. We let

$$I = \bigcup_{n\geq 1}^{\infty} I_n,$$

which is again an ideal. Since R is a principal ideal domain, $I = (a)$ for some $a \in R$. We know $a \in I = \bigcup_{n=0}^{\infty} I_n$. So $a \in I_N$ for some N. Then we have

$$(a) \subseteq I_N \subseteq I = (a)$$

So we must have $I_N = I$. So $I_n = I_N = I$ for all $n \geq N$. □

Notice it is not important that I is generated by one element. If, for some reason, we know I is generated by finitely many elements, then the same argument work. So if every ideal is finitely generated, then the ring must be Noetherian. It turns out this is an if-and-only-if — if you are Noetherian, then every ideal is finitely generated. We will prove this later on in the course.

Finally, we have done the setup, and we can prove the proposition promised.

Proposition 1.4. *Let R be a principal ideal domain. Then R is a unique factorization domain.*

Proof. We first need to show any (non-unit) $r \in R$ is a product of irreducibles.

Suppose $r \in R$ cannot be factored as a product of irreducibles. Then it is certainly not irreducible. So we can write $r = r_1 s_1$, with r_1, s_1 both non-units. Since r cannot be factored as a product of irreducibles, wlog r_1 cannot be factored as a product of irreducibles (if both can, then r would be a product of irreducibles). So we can write $r_1 = r_2 s_2$, with r_2, s_2 not units. Again, wlog r_2 cannot be factored as a product of irreducibles. We continue this way.

By assumption, the process does not end, and then we have the following chain of ideals:

$$(r) \subseteq (r_1) \subseteq (r_2) \subseteq \cdots \subseteq (r_n) \subseteq \cdots$$

But then we have an ascending chain of ideals. By the ascending chain condition, these are all eventually equal, i.e. there is some n such that $(r_n) = (r_{n+1}) = (r_{n+2}) = \cdots$. In particular, since $(r_n) = (r_{n+1})$, and $r_n = r_{n+1} s_{n+1}$, then s_{n+1} is a unit. But this is a contradiction, since s_{n+1} is not a unit. So r must be a product of irreducibles.

To show uniqueness, we let $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, with p_i, q_i irreducible. So in particular $p_1 \mid q_1 \cdots q_m$. Since p_1 is irreducible, it is prime. So p_1 divides some q_i. We reorder and suppose $p_1 \mid q_1$. So $q_1 = p_1 \cdot a$ for some a. But since q_1 is irreducible, a must be a unit. So p_1, q_1 are associates. Since R is a principal ideal domain, hence integral domain, we can cancel p_1 to obtain

$$p_2 p_3 \cdots p_n = (a q_2) q_3 \cdots q_m.$$

We now rename aq_2 as q_2, so that we in fact have

$$p_2 p_3 \cdots p_n = q_2 q_3 \cdots q_m.$$

We can then continue to show that p_i and q_i are associates for all i. This also shows that $n = m$, or else if $n = m + k$, saw, then $p_{k+1} \cdots p_n = 1$, which is a contradiction. □

MTH-204: Abstract Algebra
Lecture-18

Santosha Kumar Pattanayak

1 Polynomial Factorization and Gauss Lemma

Greatest common divisor: d is a *greatest common divisor* (gcd) of $a_1, a_2, \cdots, a_n$ if $d \mid a_i$ for all i, and if any other d' satisfies $d' \mid a_i$ for all i, then $d' \mid d$.

Note that the gcd of a set of numbers, if exists, is not unique. It is only well-defined up to a unit.

This is a definition that says what it means to be a greatest common divisor. However, it does not always have to exist.

Lemma 1.1. *Let R be a unique factorization domain. Then greatest common divisors exists, and is unique up to associates.*

Proof. We construct the greatest common divisor using the good-old way of prime factorization.

We let $p_1, p_2, \cdots, p_m$ be a list of all irreducible factors of a_i, such that no two of these are associates of each other. We now write

$$a_i = u_i \prod_{j=1}^{m} p_j^{n_{ij}},$$

where $n_{ij} \in \mathbb{N}$ and u_i are units. We let

$$m_j = \min_i \{n_{ij}\},$$

and choose

$$d = \prod_{j=1}^{m} p_j^{m_j}.$$

As, by definition, $m_j \leq n_{ij}$ for all i, we know $d \mid a_i$ for all i.

Finally, if $d' \mid a_i$ for all i, then we let

$$d' = v \prod_{j=1}^{m} p_j^{t_j}.$$

Then we must have $t_j \leq n_{ij}$ for all i, j. So we must have $t_j \leq m_j$ for all j. So $d' \mid d$.

Uniqueness is immediate since any two greatest common divisors have to divide each other. □

1.1 Factorization in polynomial rings

Since polynomial rings are a bit more special than general integral domains, we can say a bit more about them.

Recall that for F a field, we know $F[X]$ is a Euclidean domain, hence a principal ideal domain, hence a unique factorization domain. Therefore we know

1. If I is an ideal of $F[X]$, then $I = (f)$ for some $f \in F[X]$.
2. If $f \in F[X]$, then f is irreducible if and only if f is prime.
3. Let f be irreducible, and suppose $(f) \subseteq J \subseteq F[X]$. Then $J = (g)$ for some g. Since $(f) \subseteq (g)$, we must have $f = gh$ for some h. But f is irreducible. So either g or h is a unit. If g is a unit, then $(g) = F[X]$. If h is a unit, then $(f) = (g)$. So (f) is a maximal ideal. Note that this argument is valid for any PID, not just polynomial rings.
4. Let (f) be a prime ideal. Then f is prime. So f is irreducible. So (f) is maximal. But we also know in complete generality that maximal ideals are prime. So in $F[X]$, prime ideals are the same as maximal ideals. Again, this is true for all PIDs in general.
5. Thus f is irreducible if and only if $F[X]/(f)$ is a field.

To use the last item, we can first show that $F[X]/(f)$ is a field, and then use this to deduce that f is irreducible. But we can also do something more interesting — find an irreducible f, and then generate an interesting field $F[X]/(f)$.

So we want to understand reducibility, i.e. we want to know whether we can factorize a polynomial f. Firstly, we want to get rid of the trivial case where we just factor out a scalar, e.g. $2X^2 + 2 = 2(X^2 + 1) \in \mathbb{Z}[X]$ is a boring factorization.

Content: Let R be a UFD and $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$. The *content* $c(f)$ of f is

$$c(f) = \gcd(a_0, a_1, \cdots, a_n) \in R.$$

Again, since the gcd is only defined up to a unit, so is the content.

Primitive polynomial: A polynomial is *primitive* if $c(f)$ is a unit, i.e. the a_i are coprime.

Note that this is the best we can do. We cannot ask for $c(f)$ to be exactly 1, since the gcd is only well-defined up to a unit.

We now want to prove the following important lemma:

Lemma 1.2 (Gauss' lemma)**.** *Let R be a UFD, and $f \in R[X]$ be a primitive polynomial. Then f is reducible in $R[X]$ if and only if f is reducible $F[X]$, where F is the field of fractions of R.*

We can't do this right away. We first need some preparation. Before that, we do some examples.

Example: Consider $X^3 + X + 1 \in \mathbb{Z}[X]$. This has content 1 so is primitive. We show it is not reducible in $\mathbb{Z}[X]$, and hence not reducible in $\mathbb{Q}[X]$.

Suppose f *is* reducible in $\mathbb{Q}[X]$. Then by Gauss' lemma, this is reducible in $\mathbb{Z}[X]$. So we can write

$$X^3 + X + 1 = gh,$$

for some polynomials $g, h \in \mathbb{Z}[X]$, with g, h not units. But if g and h are not units, then they cannot be constant, since the coefficients of $X^3 + X + 1$ are all 1 or 0. So they have degree at least 1. Since the degrees add up to 3, we wlog suppose g has degree 1 and h has degree 2. So suppose

$$g = b_0 + b_1 X, \quad h = c_0 + c_1 X + c_2 X^2.$$

Multiplying out and equating coefficients, we get

$$b_0 c_0 = 1$$
$$c_2 b_1 = 1$$

So b_0 and b_1 must be ± 1. So g is either $1 + X, 1 - X, -1 + X$ or $-1 - X$, and hence has ± 1 as a root. But this is a contradiction, since ± 1 is not a root of $X^3 + X + 1$. So f is not reducible in $\mathbb{Q}$. In particular, f has no root in $\mathbb{Q}$.

We see the advantage of using Gauss' lemma — if we worked in $\mathbb{Q}$ instead, we could have gotten to the step $b_0 c_0 = 1$, and then we can do nothing, since b_0 and c_0 can be many things if we live in $\mathbb{Q}$.

Now we start working towards proving this.

Lemma 1.3. *Let R be a UFD. If $f, g \in R[X]$ are primitive, then so is fg.*

Proof. We let

$$f = a_0 + a_1 X + \cdots + a_n X^n,$$
$$g = b_0 + b_1 X + \cdots + b_m X^m,$$

where $a_n, b_m \neq 0$, and f, g are primitive. We want to show that the content of fg is a unit.

Now suppose fg is not primitive. Then $c(fg)$ is not a unit. Since R is a UFD, we can find an irreducible p which divides $c(fg)$.

By assumption, $c(f)$ and $c(g)$ are units. So $p \nmid c(f)$ and $p \nmid c(g)$. So suppose $p \mid a_0$, $p \mid a_1$, ..., $p \mid a_{k-1}$ but $p \nmid a_k$. Note it is possible that $k = 0$. Similarly, suppose $p \mid b_0, p \mid b_1, \cdots, p \mid b_{\ell-1}, p \nmid b_\ell$.

We look at the coefficient of $X^{k+\ell}$ in fg. It is given by

$$\sum_{i+j=k+\ell} a_i b_j = a_{k+\ell} b_0 + \cdots + a_{k+1} b_{\ell-1} + a_k b_\ell + a_{k-1} b_{\ell+1} + \cdots + a_0 b_{\ell+k}.$$

By assumption, this is divisible by p. So

$$p \mid \sum_{i+j=k+\ell} a_i b_j.$$

However, the terms $a_{k+\ell} b_0 + \cdots + a_{k+1} b_{\ell-1}$, is divisible by p, as $p \mid b_j$ for $j < \ell$. Similarly, $a_{k-1} b_{\ell+1} + \cdots + a_0 b_{\ell+k}$ is divisible by p. So we must have $p \mid a_k b_\ell$. As p is irreducible, and hence prime, we must have $p \mid a_k$ or $p \mid b_\ell$. This is a contradiction. So $c(fg)$ must be a unit. □

Corollary 1.4. *Let R be a UFD. Then for $f, g \in R[X]$, we have that $c(fg)$ is an associate of $c(f)c(g)$.*

Again, we cannot say they are equal, since content is only well-defined up to a unit.

Proof. We can write $f = c(f)f_1$ and $g = c(g)g_1$, with f_1 and g_1 irreducible. Then

$$fg = c(f)c(g)f_1g_1.$$

Since f_1g_1 is primitive, so $c(f)c(g)$ is a gcd of the coefficients of fg, and so is $c(fg)$, by definition. So they are associates. □

Finally, we can prove Gauss' lemma.

Lemma 1.5 (Gauss' lemma)**.** *Let R be a UFD, and $f \in R[X]$ be a primitive polynomial. Then f is reducible in $R[X]$ if and only if f is reducible $F[X]$, where F is the field of fractions of R.*

Proof. We will show that a primitive $f \in R[X]$ is reducible in $R[X]$ if and only if f is reducible in $F[X]$.

One direction is almost immediately obvious. Let $f = gh$ be a product in $R[X]$ with g, h not units. As f is primitive, so are g and h. So both have degree > 0. So g, h are not units in $F[X]$. So f is reducible in $F[X]$.

The other direction is less obvious. We let $f = gh$ in $F[X]$, with g, h not units. So g and h have degree > 0, since F is a field. So we can clear denominators by finding $a, b \in R$ such that $(ag), (bh) \in R[X]$ (e.g. let a be the product of denominators of coefficients of g). Then we get

$$abf = (ag)(bh),$$

and this is a factorization in $R[X]$. Here we have to be careful — (ag) is one thing that lives in $R[X]$, and is not necessarily a product in $R[X]$, since g might not be in $R[X]$. So we should just treat it as a single symbol.

We now write

$$(ag) = c(ag)g_1,$$
$$(bh) = c(bh)h_1,$$

where g_1, h_1 are primitive. So we have

$$ab = c(abf) = c((ag)(bh)) = u \cdot c(ag)c(bh),$$

where $u \in R$ is a unit, by the previous corollary. But also we have

$$abf = c(ag)c(gh)g_1h_1 = u^{-1}abg_1h_1.$$

So cancelling ab gives

$$f = u^{-1}g_1h_1 \in R[X].$$

So f is reducible in $R[X]$. □

We will do another proof performed in a similar manner.

Proposition 1.6. *Let R be a UFD, and F be its field of fractions. Let $g \in R[X]$ be primitive. We let $J =< g >\subset R[X]$ be the ideal generated by g in $R[X]$ and $I =< g >\subset F[X]$ be the ideal generated by g in $F[X]$. Then*

$$J = I \cap R[X].$$

In other words, if $f \in R[X]$ and we can write it as $f = gh$, with $h \in F[X]$, then in fact $h \in R[X]$.

Proof. The strategy is the same — we clear denominators in the equation $f = gh$, and then use contents to get that down in $R[X]$.

We certainly have $J \subseteq I \cap R[X]$. Now let $f \in I \cap R[X]$. So we can write

$$f = gh,$$

with $h \in F[X]$. So we can choose $b \in R$ such that $bh \in R[X]$. Then we know

$$bf = g(bh) \in R[X].$$

We let

$$(bh) = c(bh)h_1,$$

for $h_1 \in R[X]$ primitive. Thus

$$bf = c(bh)gh_1.$$

Since g is primitive, so is gh_1. So $c(bh) = uc(bf)$ for u a unit. But bf is really a product in $R[X]$. So we have

$$c(bf) = c(b)c(f) = bc(f).$$

So we have

$$bf = ubc(f)gh_1.$$

Cancelling b gives

$$f = g(uc(f)h_1).$$

So $g \mid f$ in $R[X]$. So $f \in J$. □

MTH-204: Abstract Algebra
Lecture-19

Santosha Kumar Pattanayak

1 Polynomial Factorization: Continued

Recall that we proved the following proposition in last class.

Proposition 1.1. *Let R be a UFD, and F be its field of fractions. Let $g \in R[X]$ be primitive. We let $J =< g > \subset R[X]$ be the ideal generated by g in $R[X]$ and $I =< g > \subset F[X]$ be the ideal generated by g in $F[X]$. Then*

$$J = I \cap R[X].$$

In other words, if $f \in R[X]$ and we can write it as $f = gh$, with $h \in F[X]$, then in fact $h \in R[X]$.

From this we can get ourselves a large class of UFDs.

Theorem 1.2. *If R is a UFD, then $R[X]$ is a UFD.*

In particular, if R is a UFD, then $R[X_1, \cdots, X_n]$ is also a UFD.

Proof. We know $R[X]$ has a notion of degree. So we will combine this with the fact that R is a UFD.

Let $f \in R[X]$. We can write $f = c(f)f_1$, with f_1 primitive. Firstly, as R is a UFD, we may factor

$$c(f) = p_1 p_2 \cdots p_n,$$

for $p_i \in R$ irreducible (and also irreducible in $R[X]$). Now we want to deal with f_1.

If f_1 is not irreducible, then we can write

$$f_1 = f_2 f_3,$$

with f_2, f_3 both not units. Since f_1 is primitive, f_2, f_3 also cannot be constants. So we must have $\deg f_2, \deg f_3 > 0$. Also, since $\deg f_2 + \deg f_3 = \deg f_1$, we must have $\deg f_2, \deg f_3 < \deg f_1$. If f_2, f_3 are irreducible, then done. Otherwise, keep on going. We will eventually stop since the degrees have to keep on decreasing. So we can write it as

$$f_1 = q_1 \cdots q_m,$$

with q_i irreducible. So we can write

$$f = p_1 p_2 \cdots p_n q_1 q_2 \cdots q_m,$$

a product of irreducibles.

For uniqueness, we first deal with the p's. We note that

$$c(f) = p_1 p_2 \cdots p_n$$

is a unique factorization of the content, up to reordering and associates, as R is a UFD. So cancelling the content, we only have to show that primitives can be factored uniquely.

Suppose we have two factorizations

$$f_1 = q_1 q_2 \cdots q_m = r_1 r_2 \cdots r_\ell.$$

Note that each q_i and each r_i is a factor of the primitive polynomial f_1, so are also primitive. Now we do (maybe) the unexpected thing. We let F be the field of fractions of R, and consider $q_i, r_i \in F[X]$. Since F is a field, F is a Euclidean domain, hence principal ideal domain, hence unique factorization domain.

By Gauss' lemma, since the q_i and r_i are irreducible in $R[X]$, they are also irreducible in $F[X]$. As $F[X]$ is a UFD, we find that $\ell = m$, and after reordering, r_i and q_i are associates, say

$$r_i = u_i q_i,$$

with $u_i \in F[X]$ a unit. What we want to say is that r_i is a unit times q_i in $R[X]$. Firstly, note that $u_i \in F$ as it is a unit. Clearing denominators, we can write

$$a_i r_i = b_i q_i \in R[X].$$

Taking contents, since r_i, q_i are primitives, we know a_i and b_i are associates, say

$$b_i = v_i a_i,$$

with $v_i \in R$ a unit. Cancelling a_i on both sides, we know $r_i = v_i q_i$ as required. □

The key idea is to use Gauss' lemma to say the reducibility in $R[X]$ is the same as reducibility in $F[X]$, as long as we are primitive. The first part about contents is just to turn everything into primitives.

Note that the last part of the proof is just our previous proposition. We could have applied it, but we decide to spell it out in full for clarity.

Example: We know $\mathbb{Z}[X]$ is a UFD, and if R is a UFD, then $R[X_1, \cdots, X_n]$ is also a UFD.

This is a useful thing to know. In particular, it gives us examples of UFDs that are not PIDs. However, in such rings, we would also like to have an easy to determine whether something is reducible. Fortunately, we have the following criterion:

Proposition 1.3 (Eisenstein's criterion)**.** *Let R be a UFD, and let*

$$f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$$

be primitive with $a_n \neq 0$. Let $p \in R$ be irreducible (hence prime) be such that

1. *$p \nmid a_n$;*
2. *$p \mid a_i$ for all $0 \leq i < n$;*
3. *$p^2 \nmid a_0$.*

Then f is irreducible in $R[X]$, and hence in $F[X]$ (where F is the field of fractions of F).

It is important that we work in $R[X]$ all the time, until the end where we apply Gauss' lemma. Otherwise, we cannot possibly apply Eisenstein's criterion since there are no primes in F.

Proof. Suppose we have a factorization $f = gh$ with

$$\begin{aligned} g &= r_0 + r_1 X + \cdots + r_k X^k \\ h &= s_0 + s_1 X + \cdots + s_\ell X^\ell, \end{aligned}$$

for $r_k, s_\ell \neq 0$.

We know $r_k s_\ell = a_n$. Since $p \nmid a_n$, so $p \nmid r_k$ and $p \nmid s_\ell$. We can also look at bottom coefficients. We know $r_0 s_0 = a_0$. We know $p \mid a_0$ and $p^2 \nmid a_0$. So p divides exactly one of r_0 and s_0. wlog, $p \mid r_0$ and $p \nmid s_0$.

Now let j be such that

$$p \mid r_0, \quad p \mid r_1, \cdots, \quad p \mid r_{j-1}, \quad p \nmid r_j.$$

We now look at a_j. This is, by definition,

$$a_j = r_0 s_j + r_1 s_{j-1} + \cdots + r_{j-1} s_1 + r_j s_0.$$

We know $r_0, \cdots, r_{j-1}$ are all divisible by p. So

$$p \mid r_0 s_j + r_1 s_{j-1} + \cdots + r_{j-1} s_1.$$

Also, since $p \nmid r_j$ and $p \nmid s_0$, we know $p \nmid r_j s_0$, using the fact that p is prime. So $p \nmid a_j$. So we must have $j = n$.

We also know that $j \leq k \leq n$. So we must have $j = k = n$. So $\deg g = n$. Hence $\ell = n - h = 0$. So h is a constant. But we also know f is primitive. So h must be a unit. So this is not a proper factorization. □

Example: Consider the polynomial $X^n - p \in \mathbb{Z}[X]$ for p a prime. Apply Eisenstein's criterion with p, and observe all the conditions hold. This is certainly primitive, since this is monic. So

$X^n - p$ is irreducible in $\mathbb{Z}[X]$, hence in $\mathbb{Q}[X]$. In particular, $X^n - p$ has no rational roots, i.e. $\sqrt[n]{p}$ is irrational (for $n > 1$).

Example: Consider a polynomial

$$f = X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1 \in \mathbb{Z}[X],$$

where p is a prime number. If we look at this, we notice Eisenstein's criteria does not apply. What should we do? We observe that

$$f = \frac{X^p - 1}{X - 1}.$$

So it might be a good idea to let $Y = X - 1$. Then we get a new polynomial

$$\hat{f} = \hat{f}(Y) = \frac{(Y+1)^p - 1}{Y} = Y^{p-1} + \binom{p}{1} Y^{p-2} + \binom{p}{2} Y^{p-3} + \cdots + \binom{p}{p-1}.$$

When we look at it hard enough, we notice Eisenstein's criteria can be applied — we know $p \mid \binom{p}{i}$ for $1 \leq i \leq p-1$, but $p^2 \nmid \binom{p}{p-1} = p$. So $\hat{f}$ is irreducible in $\mathbb{Z}[Y]$.

Now if we had a factorization

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

then we get

$$\hat{f}(Y) = g(Y+1)h(Y+1)$$

in $\mathbb{Z}[Y]$. So f is irreducible.

Hence none of the roots of f are rational (but we already know that — they are not even real!).