Subgroups

Definition: A subset H of a group G is a subgroup of G if H is itself a group under the operation in G.

Note: Every group G has at least two subgroups: G itself and the subgroup $\{e\}$, containing only the identity element. All other subgroups are said to be proper subgroups.

Examples

1. GL(n,R), the set of invertible $n \times n$ matrices with real entries is a group under matrix multiplication. We denote by SL(n,R) the set of $n \times n$ matrices with real entries whose determinant is equal to 1. SL(n,R) is a proper subgroup of GL(n,R) . (GL(n,R), is called the general linear group and SL(n,R) the special linear group.)

2. In the group D_4, the group of symmetries of the square, the subset$\{e,r,r^2,r^3\}$ forms a proper subgroup, where r is the transformation defined by rotating $\frac{\pi}{2}$ units about the z-axis.

3. In Z_9 under the operation +, the subset {0, 3, 6} forms a proper subgroup.

Problem 1: Find two different proper subgroups of S_3.

Utpal Mondal - TGC Mathematics

We will prove the following two theorems in class:

Theorem: Let H be a nonempty subset of a group G. H is a subgroup of G iff
- (i) H is closed under the operation in G and
- (ii) every element in H has an inverse in H.

For finite subsets, the situation is even simpler:

Theorem: Let H be a nonempty *finite* subset of a group G. H is a subgroup of G iff H is closed under the operation in G .

Problem 2: Let H and K be subgroups of a group G.
(a) Prove that $H \cap K$ is a subgroup of G.
(b) Show that $H \cup K$ need not be a subgroup

Example: Let Z be the group of integers under addition. Define H_n to be the set of all multiples of n. It is easy to check that H_n is a subgroup of Z. Can you identify the subgroup $H_n \cap H_m$? Try it for $H_6 \cap H_9$.

Note that the proof of part (a) of Problem 2 can be extended to prove that the intersection of any number of subgroups of *G*, finite or infinite, is again a subgroup.

<u>Cyclic Groups and Subgroups</u>

We can always construct a subset of a group *G* as follows:
Choose any element *a* in *G*. Define $\langle a \rangle = \{a^n \mid n \in Z\}$, i.e. $\langle a \rangle$ is the set consisting of all powers of *a*.

<u>Problem 3:</u> Prove that $\langle a \rangle$ is a subgroup of *G*.

<u>Definition:</u> $\langle a \rangle$ is called the cyclic subgroup generated by *a*. If $\langle a \rangle = G$, then we say that *G* is a cyclic group. It is clear that cyclic groups are abelian.

For the next result, we need to recall that two integers *a* and *n* are relatively prime if and only if gcd(*a*, *n*)=1. We have proved that if gcd(*a*, *n*)=1, then there are integers *x* and *y* such that $ax + by = 1$. The converse of this statement is also true:

<u>Theorem</u>: Let *a* and *n* be integers. Then gcd(*a*, *n*)=1 if and only if there are integers *x* and *y* such that $ax + by = 1$.

<u>Problem 4:</u> (a) Let $U_n = \{a \in Z_n \mid$ gcd(*a*,*n*)=1$\}$. Prove that U_n is a group under multiplication modulo *n*. (U_n is called the group of units in Z_n.)
(b) Determine whether or not U_n is cyclic for *n*= 7, 8, 9, 15.

We will prove the following in class.
<u>Theorem</u>: Let *G* be a group and $a \in G$.

(1) If *a* has infinite order, then $\langle a \rangle$ is an infinite subgroup consisting of the distinct elements a^k with $k \in Z$.

(2) If *a* has finite order *n*, then $\langle a \rangle$ is a subgroup of order *n* and $\langle a \rangle = \{e = a^0, a^1, a^2, \ldots, a^{n-1}\}$.

<u>Theorem:</u> Every subgroup of a cyclic group is cyclic.

<u>Problem 5</u>: Find all subgroups of U_{18}.

Note: When the group operation is addition, we write the inverse of *a* by $-a$ rather than a^{-1}, the identity by 0 rather than *e*, and a^k by *ka*. For example, in the group of integers under addition, the subgroup generated by 2 is $\langle 2 \rangle = \{2k \mid k \in Z\}$.

<u>Problem 6</u>: Show that the additive group $Z_2 \times Z_3$ is cyclic, but $Z_2 \times Z_2$ is not.

Utpal Mondal - FCC Mathematics

Problem 7: Let G be a group of order n. Prove that G is cyclic if and only if G contains an element of order n.

The notion of cyclic group can be generalized as follows. : Let S be a nonempty subset of a group G. Let $\langle S \rangle$ be the set of all possible products, in every order, of elements of S and their inverses.
We will prove the following theorem in class.
Theorem: Let S be a nonempty subset of a group G.

(1) $\langle S \rangle$ is a subgroup of G that contains S.

(2) If H is a subgroup of G that contains S, then H contains $\langle S \rangle$.

(3) $\langle S \rangle$ is the intersection of all subgroups of G that contain S.

The second part of this last theorem states that $\langle S \rangle$ is the smallest subgroup of G that contains $\langle S \rangle$. The group $\langle S \rangle$ is called the subgroup of G generated by S.
Note that when S = $\{a\}$, $\langle S \rangle$is just the cyclic subgroup generated by a. In the case when $\langle S \rangle$=G, we say that G is generated by S, and the elements of S are called generators of G.

Example: Recall that we showed that every element in D_4 could be represented by r^k or ar^k for k=0, 1, 2, 3, where r is the transformation defined by rotating $\frac{\square}{2}$ units about the z-axis, and a is rotation / / units about the line y=x in the x-y plane. Thus D_4 is generated by S =$\{a, r\}$.

Problem 8: Show that U_{15} is generated by $\{2, 13\}$.

Utpal Mondal - TGC Mathematics

Cyclic Groups

Cyclic groups are groups in which every element is a power of some fixed element. (If the group is abelian and I'm using $+$ as the operation, then I should say instead that every element is a *multiple* of some fixed element.) Here are the relevant definitions.

Definition. Let G be a group, $g \in G$. The **order** of g is the smallest positive integer n such that $g^n = 1$. If there is no positive integer n such that $g^n = 1$, then g has **infinite order**.

In the case of an abelian group with $+$ as the operation and 0 as the identity, the order of g is the smallest positive integer n such that $ng = 0$.

Definition. If G is a group and $g \in G$, then the **subgroup generated by** g is

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$

If the group is abelian and I'm using $+$ as the operation, then

$$\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}.$$

Utpal Mondal - TGC Mathematics

Definition. A group G is **cyclic** if $G = \langle g \rangle$ for some $g \in G$. g is a **generator** of $\langle g \rangle$.

If a generator g has order n, $G = \langle g \rangle$ is **cyclic of order** n. If a generator g has infinite order, $G = \langle g \rangle$ is **infinite cyclic**.

Example. (**The integers and the integers mod n are cyclic**) Show that $\mathbb{Z}$ and $\mathbb{Z}_n$ for $n > 0$ are cyclic.

$\mathbb{Z}$ is an infinite cyclic group, because every element is a multiple of 1 (or of -1). For instance, $117 = 117 \cdot 1$.

(Remember that "$117 \cdot 1$" is really shorthand for $1 + 1 + \cdots + 1$ — 1 added to itself 117 times.)

In fact, it is the only infinite cyclic group up to **isomorphism**.

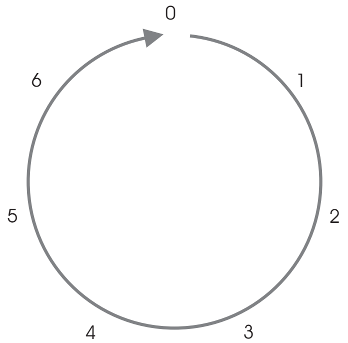
Notice that a cyclic group can have more than one generator.

If n is a positive integer, $\mathbb{Z}_n$ is a cyclic group of order n generated by 1.

For example, 1 generates $\mathbb{Z}_7$, since

$$\begin{aligned}
1 + 1 &= 2 \\
1 + 1 + 1 &= 3 \\
1 + 1 + 1 + 1 &= 4 \\
1 + 1 + 1 + 1 + 1 &= 5 \\
1 + 1 + 1 + 1 + 1 + 1 &= 6 \\
1 + 1 + 1 + 1 + 1 + 1 + 1 &= 0
\end{aligned}$$

In other words, if you add 1 to itself repeatedly, you eventually cycle back to 0.



a cyclic group of order 7

Notice that 3 also generates $\mathbb{Z}_7$:

$$\begin{aligned} 3+3&=6 \\ 3+3+3&=2 \\ 3+3+3+3&=5 \\ 3+3+3+3+3&=1 \\ 3+3+3+3+3+3&=4 \\ 3+3+3+3+3+3+3&=0 \end{aligned}$$

The "same" group can be written using multiplicative notation this way:

$$\mathbb{Z}_7 = \{1, a, a^2, a^3, a^4, a^5, a^6\}.$$

In this form, a is a generator of $\mathbb{Z}_7$.
It turns out that in $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, every nonzero element generates the group.
On the other hand, in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, only 1 and 5 generate. □

Utpal Mondal - TGC Mathematics

Lemma. Let $G = \langle g \rangle$ be a finite cyclic group, where g has order n. Then the powers $\{1, g, \ldots, g^{n-1}\}$ are distinct.

Proof. Since g has order n, g, g^2, $\ldots g^{n-1}$ are all different from 1.

Now I'll show that the powers $\{1, g, \ldots, g^{n-1}\}$ are distinct. Suppose $g^i = g^j$ where $0 \le j < i < n$. Then $0 < i - j < n$ and $g^{i-j} = 1$, contrary to the preceding observation.

Therefore, the powers $\{1, g, \ldots, g^{n-1}\}$ are distinct. □

Lemma. Let $G = \langle g \rangle$ be infinite cyclic. If m and n are integers and $m \ne n$, then $g^m \ne g^n$.

Proof. One of m, n is larger — suppose without loss of generality that $m > n$. I want to show that $g^m \ne g^n$; suppose this is false, so $g^m = g^n$. Then $g^{m-n} = 1$, so g has finite order. This contradicts the fact that a generator of an infinite cyclic group has infinite order. Therefore, $g^m \ne g^n$. □

The next result characterizes subgroups of cyclic groups. The proof uses the Division Algorithm for integers in an important way.

Theorem. Subgroups of cyclic groups are cyclic.

Proof. Let $G = \langle g \rangle$ be a cyclic group, where $g \in G$. Let $H < G$. If $H = \{1\}$, then H is cyclic with generator 1. So assume $H \ne \{1\}$.

To show H is cyclic, I must produce a generator for H. What is a generator? It is an element whose powers make up the group. *A thing should be smaller than things which are "built from" it* — for example, a brick is smaller than a brick building. Since elements of the subgroup are "built from" the generator, the generator should be the "smallest" thing in the subgroup.

What should I mean by "smallest"?

Well, G is cyclic, so everything in G is a power of g. With this discussion as motivation, let m be the smallest positive integer such that $g^m \in H$.

Why is there such an integer m? Well, H contains something other than $1 = g^0$, since $H \neq \{1\}$. That "something other" is either a positive or negative power of g. If H contains a positive power of g, it must contain a *smallest* positive power, by well ordering.

On the other hand, if H contains a negative power of g — say g^{-k}, where $k > 0$ — then $g^k \in H$, since H is closed under inverses. Hence, H again contains positive powers of g, so it contains a *smallest* positive power, by Well Ordering.

So I have g^m, the smallest positive power of g in H. I claim that g^m generates H. I must show that every $h \in H$ is a power of g^k. Well, $h \in H < G$, so at least I can write $h = g^n$ for some n. But by the Division Algorithm, there are unique integers q and r such that

$$n = mq + r, \quad \text{where} \quad 0 \leq r < m.$$

It follows that

$$g^n = g^{mq+r} = (g^m)^q \cdot g^r, \quad \text{so} \quad h = (g^m)^q \cdot g^r, \quad \text{or} \quad g^r = (g^m)^{-q} \cdot h.$$

Now $g^m \in H$, so $(g^m)^{-q} \in H$. Hence, $(g^m)^{-q} \cdot h \in H$, so $g^r \in H$. However, g^m was the *smallest positive power of g lying in H*. Since $g^r \in H$ and $r < m$, the only way out is if $r = 0$. Therefore, $n = qm$, and $h = g^n = (g^m)^q \in \langle g^m \rangle$.

This proves that g^m generates H, so H is cyclic. □

Example. (**Subgroups of the integers**) Describe the subgroups of $\mathbb{Z}$.

Every subgroup of $\mathbb{Z}$ has the form $n\mathbb{Z}$ for $n \in \mathbb{Z}$.

For example, here is the subgroup generated by 13:

$$13\mathbb{Z} = \langle 13 \rangle = \{\ldots - 26, -13, 0, 13, 26, \ldots\}. \quad □$$

Utpal Mondal - TGC Mathematics

Example. Consider the following subset of $\mathbb{Z}$:

$$H = \{30x + 42y + 70z \mid x, y, z \in \mathbb{Z}\}.$$

(a) Prove that H is a subgroup of $\mathbb{Z}$.

(b) Find a generator for H.

(a) First,

$$0 = 30 \cdot 0 + 42 \cdot 0 + 70 \cdot 0 \in H.$$

If $30x + 42y + 70z \in H$, then

$$-(30x + 42y + 70z) = 30(-x) + 42(-y) + 70(-z) \in H.$$

If $30a + 42b + 70c, 30d + 42e + 70f \in H$, then

$$(30a + 42b + 70c) + (30d + 42e + 70f) = 30(a + d) + 42(b + e) + 70(c + f) \in H.$$

Hence, H is a subgroup. □

(b) Note that $2 = (30, 42, 70)$. I'll show that $H = \langle 2 \rangle$.

First, if $30x + 42y + 70z \in H$, then

$$30x + 42y + 70z = 2(15x + 21y + 35z) \in \langle 2 \rangle.$$

Therefore, $H \subset \langle 2 \rangle$.

Conversely, suppose $2n \in \langle 2 \rangle$. I must show $2n \in H$.

The idea is to write 2 as a linear combination of 30, 42, and 70. I'll do this in two steps.

First, note that $(30, 42) = 6$, and

$$30 \cdot 3 + 42 \cdot (-2) = 6.$$

(You can do this by juggling numbers or using the Extended Euclidean algorithm.) Now $(6, 70) = 2$, and

$$6 \cdot 12 + 70 \cdot (-1) = 2.$$

Plugging $6 = 30 \cdot 3 + 42 \cdot (-2)$ into the last equation, I get

$$\begin{aligned}(30 \cdot 3 + 42 \cdot (-2)) \cdot 12 + 70 \cdot (-1) &= 2\\ 30 \cdot 36 + 42 \cdot (-24) + 70 \cdot (-1) &= 2\end{aligned}$$

Now multiply the last equation by n:

$$2n = 30 \cdot 36n + 42 \cdot (-24n) + 70 \cdot (-n) \in H.$$

This shows that $\langle 2 \rangle \subset H$.

Therefore, $H = \langle 2 \rangle$. □

Utpal Mondal - TGC Mathematics

Lemma. Let G be a group, and let $g \in G$ have order m. Then $g^n = 1$ if and only if m divides n.

Proof. If m divides n, then $n = mq$ for some q, so $g^n = (g^m)^q = 1$.

Conversely, suppose that $g^n = 1$. By the Division Algorithm,

$$n = mq + r \quad \text{where} \quad 0 \le r < m.$$

Hence,

$$g^n = g^{mq+r} = (g^m)^q g^r \quad \text{so} \quad 1 = g^r.$$

Since m is the smallest positive power of g which equals 1, and since $r < m$, this is only possible if $r = 0$. Therefore, $n = qm$, which means that m divides n. □

Example. (**The order of an element**) Suppose an element g in a group G satisfies $g^{45} = 1$. What are the possible values for the order of g?

The order of g must be a divisor of 45. Thus, the order could be

$$1, \quad 3, \quad 5, \quad 9, \quad 15, \quad \text{or} \quad 45.$$

And the order is certainly not (say) 7, since 7 doesn't divide 45. □

Thus, the order of an element is the *smallest* power which gives the identity the element in two ways. It is *smallest* in the sense of being *numerically* smallest, but it is also *smallest* in the sense that it *divides* any power which gives the identity.

Next, I'll find a formula for the order of an element in a cyclic group.

Proposition. Let $G = \langle g \rangle$ be a cyclic group of order n, and let $m < n$. Then g^m has order $\dfrac{n}{(m,n)}$.

Remark. Note that the order of g^m (the element) is the same as the order of $\langle g^m \rangle$ (the subgroup).

Proof. Since (m,n) divides m, it follows that $\dfrac{m}{(m,n)}$ is an integer. Therefore, n divides $\dfrac{mn}{(m,n)}$, and by the last lemma,

$$(g^m)^{\frac{n}{(m,n)}} = 1.$$

Now suppose that $(g^m)^k = 1$. By the preceding lemma, n divides mk, so

$$\frac{n}{(m,n)} \biggm| k \cdot \frac{m}{(m,n)}.$$

However, $\left(\dfrac{n}{(m,n)}, \dfrac{m}{(m,n)}\right) = 1$, so $\dfrac{n}{(m,n)}$ divides k. Thus, $\dfrac{n}{(m,n)}$ divides any power of g^m which is 1, so it is the order of g^m. □

In terms of $\mathbb{Z}_n$, this result says that $m \in \mathbb{Z}_n$ has order $\dfrac{n}{(m,n)}$.

Example. (**Finding the order of an element**) Find the order of the element a^{32} in the cyclic group $G = \{1, a, a^2, \ldots a^{37}\}$. (Thus, G is cyclic of order 38 with generator a.)

In the notation of the Proposition, $n = 38$ and $m = 32$. Since $(38, 32) = 2$, it follows that a^{32} has order $\dfrac{38}{2} = 19$. □

Utpal Mondal - TCC Mathematics

Example. (**Finding the order of an element**) Find the order of the element $18 \in \mathbb{Z}_{30}$.

In this case, I'm using *additive* notation instead of multiplicative notation. The group is cyclic with order $n = 30$, and the element $18 \in \mathbb{Z}_{30}$ corresponds to a^{18} in the Proposition — so $m = 18$.

$(18, 30) = 6$, so the order of 18 is $\dfrac{30}{6} = 5$. □

Next, I'll give two important Corollaries of the proposition.

Corollary. The generators of $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ are the elements of $\{0, 1, 2, \ldots, n-1\}$ which are relatively prime to n.

Proof. If $m \in \{0, 1, 2, \ldots, n-1\}$ is a generator, its order is n. The Proposition says its order is $\dfrac{n}{(m,n)}$. Therefore, $n = \dfrac{n}{(m,n)}$, so $(m,n) = 1$.

Conversely, if $(m,n) = 1$, then the order of m is

$$\frac{n}{(m,n)} = \frac{n}{1} = n.$$

Therefore, m is a generator of $\mathbb{Z}_n$. □

1 Lagrange's theorem

Definition 1.1. *The **index** of a subgroup H in a group G, denoted $[G : H]$, is the number of left cosets of H in G ($[G : H]$ is a natural number or infinite).*

Theorem 1.2 (Lagrange's Theorem)**.** *If G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$ and*

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

Proof. Recall that (see lecture 16) any pair of left cosets of H are either equal or disjoint. Thus, since G is finite, there exist $g_1, ..., g_n \in G$ such that

- $G = \cup_{i=1}^{n} g_i H$ and
- for all $1 \leq i < j \leq n$, $g_i H \cap g_j H = \emptyset$.

Since $n = [G : H]$, it is enough to now show that each coset of H has size $|H|$.
Suppose $g \in G$. The map $\varphi_g : H \to gH : h \mapsto gh$ is surjective by definition. The map φ_g is injective; for whenever

$$gh_1 = \varphi_g(h_1) = \varphi_g(h_2) = gh_2$$

, multiplying on the left by g^{-1}, we have that $h_1 = h_2$. Thus each coset of H in G has size $|H|$.
Thus

$$|G| = \sum_{i=1}^{n} |g_i H| = \sum_{i=1}^{n} |H| = [G : H]|H|$$

□

Note that in the above proof we could have just as easily worked with right cosets. Thus if G is a finite group and H is a subgroup of G then the number of left cosets is equal to the number of right cosets. More generally, the map $gH \mapsto Hg^{-1}$ is a bijection between the set of left cosets of H in G and the set of right cosets of H in G.

Utpal Mondal - TCC Mathematics

Corollary 1.3. *Let G be a finite group. For all $x \in G$, $|x|$ divides $|G|$. In particular, for all $x \in G$, $x^{|G|} = 1$.*

Proof. By Lagrange's theorem $|x| = |\langle x \rangle|$ divides $|G|$. □

Corollary 1.4. *Every group of prime order is cyclic.*

Proof. Let G be a finite group with $|G|$ prime. Take $x \in G \backslash \{1\}$. By lagrange, $|x|$ divides G and thus, since $|G|$ is prime, $|x| = |G|$ or $|G| = 1$. Since $x \neq 1$, $|x| \neq 1$. Thus $|x| = |G|$ and so, $\langle x \rangle = G$. □

Example: The converse of Lagrange's theorem does not hold. The group A_4 is of size 12 and has no subgroup of size 6. See exercise sheet 8 (Recall from linear algebra that A_4 is the group of all even permutations on 4 elements concretely: the set of permutations

$$(123), (132), (234), (243), (134), (143), (124), (142), (12)(34), (13)(24), (14)(23), e).$$

Definition 1.5. *Let G be a group and S, T subsets of G. We write*

$$ST := \{st \mid s \in S \textit{ and } t \in T\}.$$

Utpal Mondal - TGC Mathematics

Proposition 1.6. *If K and H are subgroups of a finite group G then*

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

Proof. Let $\varphi : H \times K \to HK$ be the map defined by $\varphi(h, k) := hk$. This map is surjective by definition.

Claim: If $h \in H$ and $k \in K$ then $\varphi^{-1}(hk) = \{(hd^{-1}, dk) \mid d \in K \cap H\}$.

Clearly, if $d \in K \cap H$ and $h' = hd^{-1}, k' = dk$ then $h' \in H$, $k' \in K$ and $h'k' = hk$. Conversely, if $h' \in H$, $k' \in K$ and $h'k' = hk$ then $k'k^{-1} = h'^{-1}h \in K \cap H$, $h' = h(h'^{-1}h)^{-1}$ and $k' = (h'^{-1}h)k$. This proves the claim.

Therefore for each $x \in HK$, $|\varphi^{-1}(x)| = |H \cap K|$. So,

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

□

20. Normal subgroups

20.1. **Definition and basic examples.** Recall from last time that if G is a group, H a subgroup of G and $g \in G$ some fixed element the set $gH = \{gh : h \in H\}$ is called a left coset of H.

Similarly, the set $Hg = \{hg : h \in H\}$ is called a right coset of H.

Definition. A subgroup H of a group G is called normal if $gH = Hg$ for all $g \in G$.

The main motivation for this definition comes from quotient groups which will be discussed in a couple of weeks.

Let us now see some examples of normal and non-normal subgroups.

Example 1. *Let G be an abelian group. Then any subgroup of G is normal.*

Example 2. *Let G be any group. Recall that the center of G is the set*

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

By Homework#6.3, $Z(G)$ is a subgroup of G. Clearly, $Z(G)$ is always a normal subgroup of G; moreover, any subgroup of $Z(G)$ is normal in G.

Utpal Mondal - TGC Mathematics

Example 3. $G = S_3$, $H = \langle(1,2,3)\rangle = \{e, (1,2,3), (1,3,2)\}$.

Let $g = (1,2)$. Then

$$gH = \{(1,2), (1,2)(1,2,3), (1,2)(1,3,2)\} = \{(1,2), (2,3), (1,3)\}$$
$$Hg = \{(1,2), (1,2,3)(1,2), (1,3,2)(1,2)\} = \{(1,2), (1,3), (2,3)\}.$$

Note that while there exists $h \in H$ s.t. $gh \neq hg$, we still have $gH = Hg$ as sets.

The above computation does not yet prove that H is normal in G since we only verified $gH = Hg$ for a single g. To prove normality we would need to do the same for all $g \in G$. However, there is an elegant way to prove normality in this example, given by the following proposition.

Proposition 20.1. *Let G be a group and H a subgroup of index 2 in G. Then H is normal in G.*

Proof. This will be one of the problems in Homework#10. □

Recall from Lecture 19 that the index of H in G, denoted by $[G : H]$, is the number of left cosets of H in G and that if G is finite, then $[G : H] = \frac{|G|}{|H|}$. In

Example 3 we have $|G| = 6$ and $|H| = 3$, so $[G : H] = 2$ and Proposition 20.1 can be applied.

Finally, we give an example of a non-normal subgroup:

Example 4. $G = S_3$, $H = \langle(1,2)\rangle = \{e, (1,2)\}$.

To prove this subgroup is not normal it suffices to find a single $g \in G$ such that $gH \neq Hg$. We will show that $g = (1,3)$ has this property.

We have $gH = \{(1,3), (1,3)(1,2)\} = \{(1,3), (1,2,3)\}$ and $Hg = \{(1,3), (1,2)(1,3)\} = \{(1,3), (1,3,2)\}$. Since $\{(1,3), (1,2,3)\} \neq \{(1,3), (1,3,2)\}$ (as sets), H is not normal.

20.2. **Conjugation criterion of normality.**

Definition. Let G be a group and fix $g, x \in G$. The element gxg^{-1} is called the conjugate of x by g.

Theorem 20.2 (Conjugation criterion)**.** *Let G be a group and H a subgroup of G. Then H is normal in G $\iff$ for all $h \in H$ and $g \in G$ we have $ghg^{-1} \in H$. In other words, H is normal in G $\iff$ for every element of H, all conjugates of that element also lie in H.*

Utpal Mondal : JGC Mathematics

Proof. "$\Rightarrow$" Suppose that H is normal in G, so for every element $g \in G$ we have $gH = Hg$. Hence for every $h \in H$ we have $gh \in gH = Hg$, so $gh = h'g$ for some $h' \in H$. Multiplying both sides on the right by g^{-1}, we get $ghg^{-1} \in H$. Thus, we showed that $ghg^{-1} \in H$ for all $g \in G, h \in H$, as desired.

"$\Leftarrow$" Suppose now for all $g \in G, h \in H$ we have $ghg^{-1} \in H$. This means that $ghg^{-1} = h'$ for some $h' \in H$ (depending on g and h). The equality $ghg^{-1} = h'$ can be rewritten as $gh = h'g$. Since $h'g \in Hg$ by definition, we get that $gh \in Hg$ for all $h \in H, g \in G$, so $gH \subseteq Hg$ for all $g \in G$.

Since the last inclusion holds for all $g \in G$, it will remain true if we replace g by g^{-1}. Thus, $g^{-1}H \subseteq Hg^{-1}$ for all $g \in G$. Using Lemma 19.1 (associativity of multiplication of subsets in a group), multiplying the last inclusion by g on both left and right, we get $Hg \subseteq gH$.

Thus, for all $g \in G$ we have $gH \subseteq Hg$ and $Hg \subseteq gH$, and therefore $gH = Hg$. □

20.3. **Applications of the conjugation criterion.**

Theorem 20.3. *Let G and G' be groups and $\varphi : G \to G'$ a homomorphism. Then* Ker(φ) *is a normal subgroup of G.*

Proof. Let $H = \operatorname{Ker}(\varphi)$. We already know from Lecture 16 that H is a subgroup of G, so it suffices to check normality. We will do this using the conjugation criterion.

So, take any $h \in H$ and $g \in G$. By definition of the kernel we have $\varphi(h) = e'$ (the identity element of G'). Hence $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)e'\varphi(g)^{-1} = e'$, so $ghg^{-1} \in \operatorname{Ker}(\varphi) = H$. Therefore, H is normal by Theorem 20.2. □

Here are two more examples of application of the conjugation criterion

Example 5. *Let A and B be any groups and $G = A \times B$ their direct product. Let $\widetilde{A} = \{(a, e_B) : a \in A\} \subseteq G$, the set of elements of G whose second component is the identity element of B.*

It is not hard to show that $\widetilde{A}$ is a subgroup of G and $\widetilde{A} \cong A$ (one can think of $\widetilde{A}$ as a canonical copy of A in G).

We claim that $\widetilde{A}$ is normal in G. Indeed, take any $g \in G$ and $h \in A$. Thus, $g = (x, y)$ and $h = (a, e_B)$ for some $a, x \in A$ and $y \in B$. Then $g^{-1} = (x^{-1}, y^{-1})$, so $ghg^{-1} = (x, y)(a, e_B)(x^{-1}, y^{-1}) = (xax^{-1}, ye_By^{-1}) = (xax^{-1}, e_B) \in \widetilde{A}$. Thus, $\widetilde{A}$ is normal by Theorem 20.2.

Example 6. *Let F be a field. Let*

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in F, ac \neq 0 \right\} \quad \textit{and} \quad H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in F \right\}$$

In Lecture 12 we proved that G is a subgroup of $GL_2(F)$ (so G itself is a group). We also know that H is a subgroup $GL_2(F)$ (by Homework #7.5); since clearly $H \subseteq G$, it follows that H is a subgroup of G.

Using conjugation criterion, it is not difficult to check that H is normal in G.

Utpal Mondal - TGC Mathematics

Courtesy (Contents are sourced from) **: ---**

1. Subgroup

https://web.ma.utexas.edu/users/rodin/343K/Subgroups.pdf

2. Lagrange's theorem

http://www.math.uni-konstanz.de

3. Normal subgroups

http://people.virginia.edu

4. Cyclic Groups

http://sites.millersville.edu

Utpal Mondal - TGC Mathematics