MAT311: Abstract Algebra

Mahmudul Hasan Turjoy

Last updated: November 12, 2024

Preface

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

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

— Mahmudul Hasan Turjoy

Contents

Lecture 0

22 Oct 2024

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

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

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

Properties of this relation:

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

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

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

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

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

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

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

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

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

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

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

0.2 Rotational Symmetries of an Equilateral Triangle

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

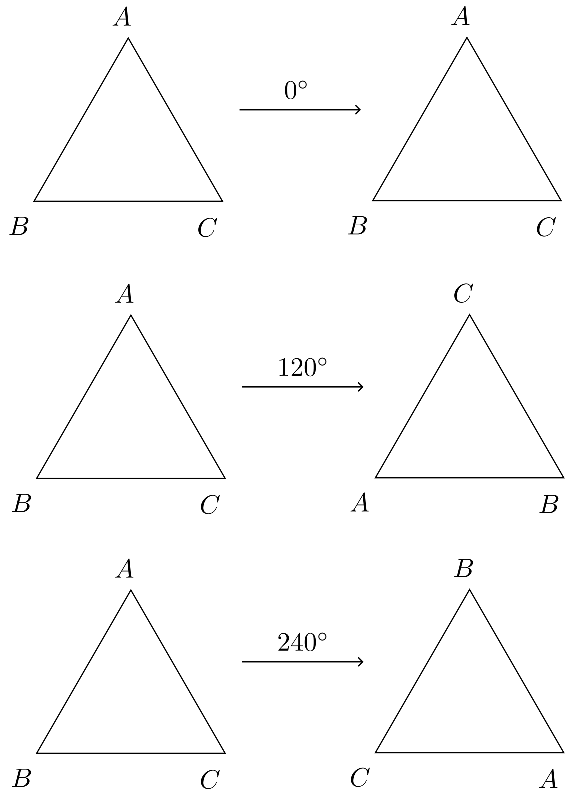

Figure 1: Symmetries of Triangle

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

Lecture 1

28 Oct 2024

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

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

1.1 Groups

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

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

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

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

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

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

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

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

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

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

- $x + y$ (Mod 1).

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

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

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

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

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

For all $x \in G$,

$$x * 0 = x + 0 \text{ (Mod 1)} = x.$$

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

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

$$x * (1 - x) = x + 1 - x \text{ Mod } 1 = 1 \text{ Mod } 1 = 0 \ \&$$

$$(1 - x) * x = 1 - x + x \text{ Mod } 1 = 1 \text{ Mod } 1 = 0$$

And for $0 \in G, 0 * 0 = 0 + 0 \text{ (Mod 1)} = 0$ **(Inverse)**
For all $x, y \in G$

$$\begin{aligned}x * y &= x + y \text{ (Mod 1)} \\ &= y + x \text{ (Mod 1)} \\ &= y * x\end{aligned}$$

Hence, G is an Abelian group.

1.2 Matrix Groups

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

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

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

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

Lecture 2

30 Oct 2024

2.1 Group Propositions

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

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

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

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

also

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

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

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

also

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

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

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

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

2.2 Subgroups

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

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

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

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

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

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

Lecture 3

04 Nov 2024

3.1 Order of Group and its elements

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

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

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

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

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

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

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

3.2 Cyclic Groups

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

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

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

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

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

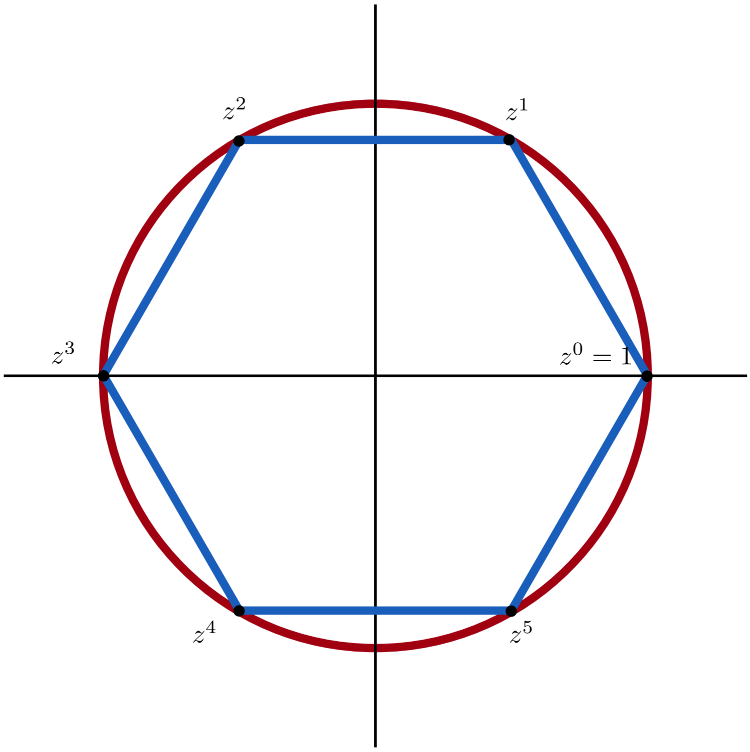

Figure 3.1: The 6th complex roots of unity form a cylic group under multiplication

3.3 Centralizers and Normalizers

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

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

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

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

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

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

Lecture 4

06 Nov 2024

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

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

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

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

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

4.1 Caylay's Table

To be written...

Lecture 5

11 Nov 2024

5.1 Congruence Modulo Subgroup H

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

Lemma 2. The relation $a \equiv b \pmod H$ is an equivalence relation.

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

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

5.2 Cosets

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

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

Lemma 3. For all $a \in G$, $Ha = \{x \in G : a \equiv x \pmod H\}$.

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

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

Lemma 4. There is a one-to-one correspondence between any two right cosets of H in G.

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

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

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