Groups and Symmetries

Definition: Symmetry
A symmetry of a shape is a rigid motion that takes vertices to vertices, edges to edges.
Note: A rigid motion preserves angles and distances.

Definition: Group
A group $(G, *)$ is a set G and an operation $*$ such that G is closed under $*$ and that:
1. There exists e such that $e*x=x=x*e$ for all $x\in G$ (existence of identity e).
2. For every $x\in G$ there exists x^{-1} such that $x*x^{-1}=e=x^{-1}*x$ (existence of inverses).
3. For all $x, y, z\in G$, $x*(y*z)=(x*y)*z$ (associativity).

Examples
- D_3 is the group of symmetries of a regular 3-gon. $D_3=\{e, r, r^2, s, sr, sr^2\}$, $(D_3, \circ)$ with $r=60°$ rotation clockwise and $s=$ reflection about y-axis
- D_n is the group of symmetries of a regular n -gon.

Claim
The identity of $(G, *)$ is unique.

Proof: Assume the e_1 and e_2 are identities of $(G, *)$. $e_1=e_1*e_2=e_2\Leftrightarrow e_1=e_2$. So there is only one identity.

Claim
Given $x\in G$, x^{-1} is unique.

Proof: Let $y=x^{-1}$ and $z=x^{-1}$ but $y\neq z$. Now $y=y*e=y*(x*z)=(y*x)*z=e*z=z$, so $y=z$. Contradiction! So x^{-1} is unique given x.

Definition: Commute
If $x*y=y*x$ then x and y are said to commute.

Definition: Abelian
If all elements in $(G, *)$ commute, then $(G, *)$ is said to be Abelian.

Definition: Order (Group)
The order of a group G, denoted $|G|$, is the number of elements in G.

Examples
$|Q_8|=8$, $|V_4|=4$, $|D_3|=6$, $|D_4|=8$, $|\mathbb{Z}|=\infty$, $|\mathbb{Q}|=\infty$.

Definition: Order (Element)
The order of an element $x\in G$, written $|x|$, is the smallest positive integer n such that $x^n=e$.

Examples
- In D_3, $r\cdot r\cdot r=r^3=e$ so $|r|=3$.
- $|e|=1$.

- In $V_4=\{e,a,b,ab\}$, $|e|=1$, $a\cdot a=e\Rightarrow|a|=2$, $b\cdot b=e\Rightarrow|b|=2$, $|ab|=2$.
- In $Q_8=\{1,-1,i,-i,j,-j,k,-k\}$, $|1|=1$, $|-1|=2$, $|i|=|j|=|k|=4$.

Definition: Subgroup
H is a subgroup of G iff H is a subset of G which is a group under the same operation as G .

Example
In D_4 , $\{e,r,r^{2,}r^3\}$ is a subgroup since it is closed under × ($r_n \times r_m = r^{n+m}$), has inverses ($r^{-1}=r^3$, $(r^2)^{-1}=r^2$), and $e\in\{e,r,r^{2,}r^3\}$.

Definition: Proper Subgroup
H is a proper subgroup of G iff H is a subgroup of G and $H\neq G$, $H\neq\{e\}$.

Note
Does G always have a proper subgroup? No. $\{e,r,r^2\}$ has no proper subgroups.

Definition: Set of Generators
S is a set of generators of a group G iff every $g\in G$ can be expressed as:

- multiplication: $g=s_1^{m_1}\times s_2^{m_2}\times\cdots\times(s_k^{m_k})$
- addition: $g=m_1 s_1+m_2 s_2+\cdots+(m_k s_k)$

where $m_i\in\mathbb{Z}$ and $s_i\in S$ (repetitions of s_i 's are allowed). Any such combinations of s_i 's is called a word.

Definition: Relation
A relation is an equation that tells use the “rules” for using $*$ in $(G,*)$.

Example
If we specify that $r^3=e$, $s^2=s$, $sr=r^2 s$, the group generated by $\{r,s\}$ is $\{e,r,r^{2,}s,rs,r^2 s\}$. We called this group D_3 . So $D_3=\langle r,s|r_3=s^2=e,sr=r^2 s\rangle$.

Definition: Free Group
A free group on n generators is $\langle a_{1,}\ldots,a_n\rangle$ (a group with n generators and no relations).

Definition: Cyclic
A group (or subgroup) is cyclic iff it can be generated by only one element.

Example
$\langle a|a^5=e\rangle=\{e,a,a^{2,}a^{3,}a^4\}$ is cyclic.

Definition
C_n is the cyclic group of order n. $C_n=\langle g|g^n=e\rangle$.

Definition: Infinite, Finite
A group G is infinite iff $|G|=\infty$. A group G is finite iff $|G|=n<\infty$.

Example
$(\mathbb{Z},+)$ is infinite.

Example
In $(\mathbb{Z},+)$, what does $\{2\}$ generate?
$0\in\langle 2\rangle$, $2\in\langle 2\rangle$, $2+2+\cdots\in\langle 2\rangle$, $-2\in\langle 2\rangle$, $(-2)+(-2)+\cdots\in\langle 2\rangle$. So $2\mathbb{Z}\overset{\text{def}}{=}\langle 2\rangle=\{2\text{n}|\forall n\in\mathbb{Z}\}$ is the set of even numbers.

Theorem: The Subgroup Criterion
If $H\subset G$ is a non-empty subset, then $\forall x,y\in H\Rightarrow x y^{-1}\in H$ if and only if H is a subgroup.

Proof:
($\Rightarrow$) Assume $\forall x,y\in H\Rightarrow x y^{-1}\in H$. Let $y=x$, then $x x^{-1}=e\in H$. Let $x=e$, then $y^{-1}\in H$. So H is closed under inverses, i.e. $y^{-1}\in H$ whenever $y\in H$. So take x and y^{-1} to be two arbitrary elements in H. Then $x(y^{-1})^{-1}=x y\in H$, so it is closed under multiplication.
($\Leftarrow$) Assume H is a subgroup of G. So if $x,y\in H$, then $y^{-1}\in H$. Since H is closed under multiplication, $x y^{-1}\in H$.

Definition
$\mathbb{Z}_n=\{\text{intergers}\, mod\ n\}$.

Claim
Let p be a prime. $\mathbb{Z}_p$ has no proper subgroup.

Proof: Let $0<n<p$. Since p is a prime, $\gcd(n,p)=1$. So $n\neq 0 \bmod p$, $2\text{n}\neq 0 \bmod p$, etc., $(p-1)n\neq 0 \bmod p$. So $\mathbb{Z}_p$ has no proper subgroup.

Homomorphisms and Isomorphisms

Definition: One-to-One
1:1 means $f(x)=f(y)\Leftrightarrow x=y$, $\forall x,y$.

Definition: Onto
Onto means if $f:A\to B$ then for all $b\in B$ there exists $a\in A$ such that $f(a)=b$. Equivalently, $f:A\to B$ is onto if and only if $f(A)$ is all of B.

Definition: Homomorphism
f is an homomorphism iff $f(a*b)=f(a)\square f(b)$ where $f:(A,*)\to(B,\square)$.

Definition: Isomorphism
f is an isomorphism iff f is a homomorphism, 1:1, and onto.

Properties of Homomorphisms
Let $f:(G,*)\to(K,\square)$ be a homomorphism.
1. $\operatorname{Im}(f)$ is a subgroup of K.
2. If H is a subgroup of G, then $f(H)$ is a subgroup of K.

3. f sends inverses to inverses, i.e. $f(x)=y \Rightarrow f(x^{-1})=y^{-1}$.
4. f sends identities to identities, i.e. $f(e_G)=e_K$.
5. If $x_1 x_2 = x_2 x_1$, then $f(x_1 x_2)=f(x_2 x_1)=f(x_1)f(x_2)=f(x_2)f(x_1)$.

Definition: Trivial Homomorphism

$f:(G,*)\to\{e\}$ is called the trivial homomorphism.

Properties of Isomorphism

Let $f:(G,*)\to(K,\square)$ be a homomorphism.

1. All properties of homomorphism.
2. f preserves the order of elements, i.e. $f(x)=y \Rightarrow |x|_G=|y|_K$.
3. $|G|=|K|$.
4. G and K can be written be the same number of generators and the same relations. In other words, G and K have the same $\langle \square | \square \rangle$ form.

Example

All groups are isomorphic to themselves.

Definition: Symmetric Group

The symmetric group (on n letters) S_n is the group of permutations that permute up to n symbols/letters.

Examples

- $(2\,3\,4)$: A B C D $\to$ A D B C .
- $(1\,2\,4\,7)$: A B C D E F G $\to$ G A C B E F D .
- $(1\,2)(3\,5)$: A B C D E $\to$ B A E D C .

Definition: Disjoint

If there are no common numbers in two different sets of brackets, they are said to be disjoint.

Definition: *n*-Cycle

A bracket with n distinct numbers is called an n-cycle.
Note: A 2-cycle is also called a transposition.

Example

Is S_3 abelian? $(2\,3)\circ(1\,2\,3)$: A B C $\xrightarrow{(123)}$ C A B $\xrightarrow{(23)}$ C B A , but $(1\,2\,3)\circ(2\,3)$: A B C $\xrightarrow{(23)}$ A C B $\xrightarrow{(123)}$ B A C . So S_3 is not abelian.

Conventions

- Write the smallest number first. So if “1” gets moved first, write “1”, if “2” gets moved first, write “2”, etc.
- Only write each number once to avoid confusion. Also end the bracket when the first repeating number appears.

Claim

Using the convention gives a unique way of writing a permutation. However, there are many ways to write a permuation as a product of 2-cycles.

Theorem
All n -cycles (except the identity e) can be written as a product of 2-cycles and therefore all permutations.

Theorem
The 2-cycles generate S_n .

Question
How big is S_n? $n!$.

Example
Write $(3\ \ 7\ \ 4\ \ 6\ \ 8)(5\ \ 10\ \ 9)$ as a product of 2-cycles.
$(3\ \ 7\ \ 4\ \ 6\ \ 8)=(3\ \ 8)(3\ \ 6)(3\ \ 4)(3\ \ 7)$, $(5\ \ 10\ \ 9)=(5\ \ 9)(5\ \ 10)$. So
$(3\ \ 7\ \ 4\ \ 6\ \ 8)(5\ \ 10\ \ 9)=(3\ \ 8)(3\ \ 6)(3\ \ 4)(3\ \ 7)(5\ \ 9)(5\ \ 10)$.

Definition: Even, Odd
A permutation is even iff it can be written as the product of an even number of 2-cycles.
A permutation is odd iff it can be written as the product of an odd number of 2-cycles.

Claim
If σ can be written as an even number of 2-cycles, then it can never be written as an odd element.

Claim
$A_n=\{\text{even permutations of } S_n\}$ is a subgroup of S_n , and hence a group.
Note: $|A_n|=\frac{|S_n|}{2}$.

Theorem
The following are sets of generators for S_n .

- All 2 cycles.
- $(1\ \ 2),(1\ \ 3),\ldots,(1\ \ n)$ since $(a\ \ b)=(1\ \ a)(1\ \ b)(1\ \ a)$.
- $(1\ \ 2),(2\ \ 3),\ldots,((n-1)\ \ n)$ since $(1\ \ k)=((k-1)\ \ k)\cdots(2\ \ 3)(1\ \ 2)(2\ \ 3)\cdots((k-1)\ \ k)$.
- $(1\ \ 2)$ and $(1\ \ 2\ \ \cdots\ \ n)$.

Remarks
If $f: A\rightarrow B$ is an isomorphism, then $g(b)$ is the preimage of f when $f(a)=b$ and $g(b)=a$. g is also an isomorphism.

Definition: Center
The center of a group G is $Z(G)=\{z\in G | z*g=g*z\ \forall\ g\in G\}$, elements that commute with everything.
Note: $\{e\}$ is called the trivial center.

Definition: Direct Sum
The direct sum $A\oplus B$ is the set of coordinates $\{(a,b) | a\in A, b\in B\}$.

Facts

1. $Z(G \oplus K) = Z(G) \oplus Z(K)$.
2. If H_1 is a subgroup of G and H_2 is a subgroup of K, then $H_1 \oplus H_2$ is a subgroup of $G \oplus K$.

Remark
Direct sums can be abelian or not, cyclic or not, etc., all the same definitions apply.

Definition: Left Multiplication Function
$L_g(x) = g * x,\ \ g, x \in G$ is the left multiplication function.

Lemma
L_g is 1:1 and onto when applied to the group G.

Proof: Let $L_g(x) = L_g(y) \Rightarrow g * x = g * y \Rightarrow g^{-1} * g * x = g^{-1} * g * y \Rightarrow x = y$, so L_g is 1:1. Now assume L_g is not onto. Then $\{L_g(x_1), \ldots, L_g(x_n)\}$ is not the entire group. So $L_g(x_i) = L_g(x_j)$ for some $i \neq j$, then $g * x_i = g * x_j \Rightarrow x_i = x_j$. Contradiction, so L_g is onto.

Theorem: Cayley's Theorem
Let G be any group. There exists an isomorphism f such that $f: G \rightarrow$ subgroup of $S_{|G|}$. In particular, if $|G| = n$, G is isomorphic to a subgroup of S_n.

Proof: L_g is 1:1 and onto, so L_g permutes the elements of G. If $|G| = n$, then $L_g \in S_n$. Let $f: G \rightarrow S_n, f(g) = L_g$. $f(ab) = L_{ab} = L_a L_b = f(a) f(b)$, so f is a homomorphism. f is 1:1 since $f(x) = f(y) \Rightarrow L_x = L_y \Rightarrow x * g = y * g, \forall g \in G \Rightarrow x * e = y * e \Rightarrow x = y$. Since f is 1:1 and takes n elements ($g \in G$) to n elements $L_g \in S_n$, f is onto. Hence f is an isomorphism.

Theorem: Lagrange's Theorem
Let H be a subgroup of G. Then $|H|$ is a factor of $|G|$.

Proof: Let $g_1 \notin H$ but $g_1 \in G$, then $g_1 H = \{g_1 * h | \forall h \in H\}$ has the same number of elements as H (lemma applied to L_{g_1}). Take $g_2 \notin H, g_1 H$ but $g_2 \in G$, then $|g_2 H| = |H|$. If $|G|$ is finite, then we get $|G| = k|H|$ where k is the number of g_i's, since $G = H \cup g_1 H \cup \cdots \cup g_k H$.

Corollary
Since $|g| = |\langle g \rangle|$, then $|g|$ is a factor of $|G|$ whenever $g \in G$.

Example
Let $|G| = p$ a prime number. If $x \in G$, then $|x| = 1$ or $|x| = p$. If $|x| = 1$, then $x = e$ (i.e. $\langle x \rangle = \{e\}$). Otherwise $G = \langle x \rangle$, which has no proper subgroup. This also shows that G is cyclic.

Normal Subgroups and Quotient Groups

Definition: Partition
A partition of G is a collection of disjoint subsets such that their union is G.

Definition: Equivalence Relation

An equivalence relation $\sim$ is a relation such that:

1. $x \sim x \quad \forall x \in G$ (reflexive).
2. $x \sim y \Leftrightarrow y \sim x \quad \forall x, y \in G$ (commutative).
3. $x \sim y,\ y \sim z \Rightarrow x \sim z \quad \forall x, y, z \in G$ (transitive).

Definition: Conjugation
If $x = g^{-1} y g$ for some $g \in G$, then x is conjugate to y.

Claim
Conjugacy is an equivalence relation.

Proof:
1. $x = e^{-1} x e$.
2. Let $x = g^{-1} y g$. Let $h = g^{-1}$. Then $y = h^{-1} x h$.
3. Let $x = g^{-1} y g$ and $y = h^{-1} z h$. Then $x = g^{-1} h^{-1} z h g = k^{-1} z k$ where $k = hg$.

Definition: Equivalence Class
An equivalence class is a complete set of elements that are equivalent to each other other. In other words, x is in the equivalence class of y if and only if $x \sim y$.

Claim
Equivalence relation partition all groups G in to equivalence classes.

Proof: Assume two equivalence classes, say of x and y, are not disjoint. Then there exists z such that $z \sim x$ and $z \sim y$. Therefore $x \sim y$ and $y \sim x$, so they are the same classes. Contradiction. Hence two equivalence classes are disjoint. Now $x \sim x$, therefore any $x \in G$ is in the equivalent class of x. So the union of all equivalent classes is G. Therefore equivalence classes partition G.

Definition: Normal Subgroup
H is a normal subgroup in G iff $g^{-1} h g \in H$ for all $g \in G$ and all $h \in H$.

Definition: Normal Subgroup
H is a normal subgroup in G iff $g^{-1} H g \stackrel{\text{def}}{=} \{g^{-1} h g \mid \forall h \in H\} = H$ for all $g \in G$.

Example
$H = \{e, r, r^2\}$ is a normal subgroup of D_3

Definition: Conjugacy Class
The conjugacy class of $x \in G$ is the set $\{g^{-1} x g \mid \forall g \in G\}$ (equivalence class of x where the equivalence relation is conjugation).

Example
In D_3, the conjugacy class of r is $\{r, r^2\}$. It is also the conjugacy class of r^2 by transitivity, since $r \sim r^2$.
The conjugacy class of e is $\{e\}$

Definition: Normal Subgroup

H is a normal subgroup in G iff H is a union of conjugacy classes in G.

Example
$H=\{e,r,r^2\}=\{e\}\cup\{r,r^2\}$ is a union of conjugacy classes, so H is a normal in G.

Definition: Coset
A coset of H in G is $gH=\{gh|\forall h\in H\}$ for some fix $g\in G$.

Example
$sH=\{se,sr,sr^2\}=\{s,r^2s,rs\}$ is a coset of H. $eH=H$ is also a coset of H.

Definition: Index
The index of H in G, denoted $([G:H])$, is the number of distinct cosets of H in G.

Definition: Normal Subgroup
H is a normal subgroup in G iff $gH=Hg$ for all $g\in G$.

Example
If G is abelian, H is always normal in G if H is a subgroup in G.

Claim
Let H be a subgroup of G. The following are equivalent:

1. $g^{-1}hg\in H$ for all $g\in G$ and all $h\in H$.
2. $g^{-1}Hg=H$ for all $g\in G$.
3. H is a union of conjugacy classes in G.
4. $gH=Hg$ for all $g\in G$.
5. H is a normal subgroup in G, denoted $H\triangleq G$.

Proof:
($2\Rightarrow 1$) Assume $g^{-1}Hg\stackrel{\text{def}}{=}\{g^{-1}hg|\forall h\in H\}=H$ for all $g\in G$. Therefore elements of $\{g^{-1}hg|\forall h\in H\}$ are also elements of H.
($3\Rightarrow 2$) Assume H is a union of conjugacy classes in G, i.e. $H=\bigcup_{h\in H}\{g^{-1}hg|\forall g\in G\}$. So
$H=\bigcup\{g^{-1}hg|\forall g\in G,\forall h\in H\}=g^{-1}Hg$.
($1\Rightarrow 3$) Assume $g^{-1}hg\in H$ for all $g\in G$ and all $h\in H$. So the conjugacy class of h is in H. Suppose H is not a union of conjugacy classes in G. Then there exists $z\in H$ not in a conjugacy class. Now $g^{-1}zg\in H$, so the conjugacy class of z is in H. Contradiction.
($2\Leftrightarrow 4$) $g^{-1}Hg=H\Leftrightarrow gg^{-1}Hg=gH\Leftrightarrow Hg=gH$.

Definition: Quotient Group
The quotient group G/H is the set of cosets $\{gH\}\,\forall g\in G$ with the operation $xH*yH=x*yH$ where $*$ is the group operation from G.
Note: This only works if H is a normal subgroup in G.

Example
Let $H=\{e,r,r^2\}\subset D_3$ be normal. Then $D_3/H=\{eH,sH\}$.

Fact
$|G/H|=\frac{|G|}{|H|}$ (since L_g is 1:1).

Properties of Quotient Groups
- $G/G=\{gG|\forall g\in G\}\cong\{e\}$.
- If G is abelian, then G/H is abelian.
  Proof: $xHyH=xyH=yxH=yHxH$ since $xy=yx$.
- If G is cyclic, then G/H is cyclic.
  Proof: $G=\{g^{\alpha}|\alpha=1,\ldots,n\}$. The cosets in G/H are $\{g^{\alpha}H\}$, so gH generates G/H whenever g generates G .
- If G is finitely generated, then G/H is finitely generated.
  Proof: If $g_{1,}\ldots,g_n$ generate G , then $g_1H,\ldots,g_nH$ generate G/H .

Claim
$xHyH=xyH$ if and only if H is normal.

Proof:
($\Rightarrow$) $xHyH=xyH\Rightarrow x^{-1}xHyH=x^{-1}xyH\Rightarrow HyH=yH$, so $h_i y h_j=y h_k$ (fixing h_i and h_j we get $\forall h_k$), so $h_i y=y h_k h_j^{-1}$. Let $\tilde{h}=h_k h_j^{-1}$ which can be anything in H . Then $h_i y=y\tilde{h}\rightarrow Hy=yH$, so H is normal.
($\Leftarrow$) Clear from definition.

Definition: Kernel, Image
Let $f:G\rightarrow G'$. Then $\text{Ker}(f)=\{g\in G|f(g)=e\}$, and $\text{Im}(f)=\{g'\in G'|\exists g\in G \text{ such that } f(g)=g'\}$.

Theorem: 1st Isomorphism Theorem
Let $f:G\rightarrow G'$ be a homomorphism. Then $\text{Ker}(f)\trianglelefteq G$ and $G/\text{Ker}(f)\cong\text{Im}(f)$.

Proof:
Want: $\text{Ker}(f)\trianglelefteq G$. Let $x\in\text{Ker}(f)$. Then $f(g^{-1}xg)=f(g^{-1})f(x)f(g)=f(g)^{-1}ef(g)=e$, so $g^{-1}xg\in\text{Ker}(f)$. Now, $f(z)f(ez)=f(e)f(z)\rightarrow f(e)=e$, so $\text{Ker}(f)\neq\emptyset$. Hence $\text{Ker}(f)\trianglelefteq G$.
Want: $G/\text{Ker}(f)\cong\text{Im}(f)$. Let $K=Ker(f)$. Let $\varphi:G/\text{Ker}(f)\rightarrow\text{Im}(f)$ where $\varphi(xK)=f(x)$. Then φ is a homomorphism since $\varphi(aKbK)=\varphi(abK)=f(ab)=f(a)f(b)=\varphi(aK)\varphi(bK)$. φ is onto $\text{Im}(f)$ since φ is onto $\text{Im}(\varphi)$ by definition of image, and $\text{Im}(\varphi)=\text{Im}(f)$ by construction. φ is 1:1 since $\varphi(aK)=\varphi(bK)\Rightarrow f(a)=f(b)\Rightarrow f(a)f(b)^{-1}=e\Rightarrow f(a)f(b^{-1})=e\Rightarrow f(ab^{-1})=e\Rightarrow ab^{-1}\in K$, so $ab^{-1}K=K\Rightarrow ab^{-1}KbK=KbK\Rightarrow aK=bK$. Hence $\varphi:G/\text{Ker}(f)\rightarrow\text{Im}(f)$ is an isomorphism and so $G/\text{Ker}(f)\cong\text{Im}(f)$.

Corollary
Let $f:G\rightarrow G'$ be a homomorphism. $\text{Ker}(f)=\{e_G\}$ if and only if f is an isomorphism.

Proof:
($\Rightarrow$) $\text{Ker}(f)=\{e_G\}$, then by the 1st Isomorphism Theorem, $G/\{e_G\}\cong\text{Im}(f)$ and so $G\cong\text{Im}(f)$. Take $\varphi:G/\text{Ker}(f)\rightarrow\text{Im}(f)$ defined by $\varphi(xK)=f(x)$ as in the proof of 1st Isomorphism Theorem. Here $K=\{e\}$, so $\varphi(x)=f(x)$, and we already know that φ is an isomorphism, and hence f is an isomorphism.
($\Leftarrow$) f is an isomorphism, so f is 1:1 and $f(e_G)=e_{G'}$, therefore $\text{Ker}(f)$ can only contain one element, e_G .

Definition: Commutator Subgroup

The commutator subgroup $[G,G]$ is the subgroup of G that is generated by all $xyx^{-1}y^{-1}$ for all $x,y\in G$.

Claim
$[G,G]$ is abelian.

Proof: Let $H=[G,G]$. $xyx^{-1}y^{-1}H=H$ since $xyx^{-1}y^{-1}\in H$. So $xyx^{-1}y^{-1}H\,yH=H\,yH\Rightarrow xyx^{-1}H=yH\Rightarrow xyx^{-1}H\,xH=yH\,xH\Rightarrow xyH=yxH\Rightarrow(xH)(yH)=(yH)(xH)$. Hence $H=[G,G]$ is abelian.

Claim
If G/H is abelian, then $[G,G]\subseteq H$.

Proof: $xyH=yxH$ since G/H abelian. So $xyHx^{-1}Hy^{-1}H=yxHx^{-1}Hy^{-1}H\Rightarrow xyx^{-1}y^{-1}H=H$, so $xyx^{-1}y^{-1}\in H$. Therefore all generators of $[G,G]$ is in H, so $[G,G]\subseteq H$.

Remark
The commutator subgroup $[G,G]$ is the smallest subgroup H of G such that its quotient G/H is abelian. Since bigger H implies few cosets, so $G/[G,G]$ is the largest abelian quotient of G.

Definition: Abelianisation
The abelianisation of a group G is $G/[G,G]$.

Claim
If $A\trianglelefteq G$, $B\trianglelefteq G'$, then $A\oplus B\trianglelefteq G\oplus G'$ and $\dfrac{G\oplus G'}{A\oplus B}\cong\dfrac{G}{A}\oplus\dfrac{G'}{B}$.

Proof: Define $f:G\oplus G'\rightarrow\dfrac{G}{A}\oplus\dfrac{G'}{B}$ by $f((g,g'))=(gA,gB)$. Then
$f((g_1,g_1')(g_2,g_2'))=f((g_1g_2,g_1'g_2'))=(g_1g_2A,g_1'g_2'B)=(g_1A,g_1'B)(g_2A,g_2'B)=f((g_1,g_1'))f((g_2,g_2'))$, so f is a homomorphism.
$\mathrm{Ker}(f)=\{(g,g')\in G\oplus G'|f((g,g'))=(eA,eB)\}$, but $f(g,g')=(gA,g'B)=(eA,eB)\Rightarrow g\in A,g'\in B$, so
$\mathrm{Ker}(f)=\{(g,g')\in G\oplus G'|g\in A,g'\in B\}=A\oplus B$.
$\mathrm{Im}(f)=\left\{(gA,g'B)\in\dfrac{G}{A}\oplus\dfrac{G'}{B}\middle|\exists(g,g')\in G\oplus G'\text{ such that }f(g,g')=(gA,g'B)\right\}=\dfrac{G}{A}\oplus\dfrac{G'}{B}$, so f is onto.

Definition: Lattice
A group lattice is a diagram with subgroups as vertices and edges mean that the lower subgroup sits inside the upper subgroup.

Theorem: 2nd Isomorphism Theorem
Let H, J be subgroups of G and $J\trianglelefteq G$. Then:

1. $HJ\overset{\text{def}}{=}\{hj|\forall h\in H,j\in J\}$ is a subgroup.
2. $H\cap J\trianglelefteq G$.
3. $\dfrac{HJ}{J}\trianglelefteq\dfrac{H}{H\cap J}$.

Proof: $e_He_J=e_Ge_G=e$, so $HJ\neq\emptyset$. Let $g,\tilde{g}\in HJ$, $g=hj$, $\tilde{g}=\tilde{h}\tilde{j}$. Then $g\tilde{g}^{-1}=hj\tilde{j}^{-1}\tilde{h}^{-1}$. Since $j\tilde{j}^{-1}\in J$, so

$h(j\tilde{j}^{-1})\tilde{h}^{-1} \in J$ because $J \triangleq G$. Hence $g\tilde{g}^{-1} \in J$, so $g\tilde{g}^{-1} = ej'$ for $e \in H$ and some $j' \in J$, and hence $g\tilde{g}^{-1} \in HJ$. So HJ is a subgroup by the subgroup criterion.

Now, define $f: H \to \frac{HJ}{J}$ by $f(x) = xeJ$. Then $f(xy) = xeyeJ = xeyeJJ = xeJyeJ = f(x)f(y)$, so f is a homomorphism. $\mathrm{Ker}(f) = \{h \in H | f(h) = eeJ\} = \{h \in H | hJ = eJ\} = \{h \in H | h \in J\} = H \cap J$.

$\mathrm{Im}(f) = \left\{ hjJ \in \frac{HJ}{J} \middle| \exists h \in H \text{ such that } f(h) = hjJ \right\} = \left\{ hjJ \in \frac{HJ}{J} \middle| \exists h \in H \text{ such that } heJ = hjJ \right\} = \frac{HJ}{J}$, so f is onto.

Therefore, by the 1st Isomorphism Theorem, $H \cap J \triangleq G$ and $\frac{HJ}{J} \triangleq \frac{H}{H \cap J}$.

Theorem: 3rd Isomorphism Theorem

Let $H \triangleq G$, $J \triangleq G$, and $H \subset J$. Then:

1. $\frac{J}{H} \triangleq \frac{G}{H}$.
2. $\frac{G/H}{J/H} \cong \frac{G}{J}$.

Note that $H \triangleq J$ since $gH = Hg \;, \forall g \in G$ and $H \subset J$, so $jH = Hj \;, \forall j \in J \subset G$.

Proof: Define $f: \frac{G}{H} \to \frac{G}{J}$ by $f(xH) = xJ$. Then $f(xHyH) = f(xyH) = xyJ = xyJJ = xJyJ = f(x)f(y)$, so f is a homomorphism. $\mathrm{Ker}(f) = \left\{ gH \in \frac{G}{H} \middle| f(gH) = eJ \right\} = \left\{ gH \in \frac{G}{H} \middle| gJ = eJ \right\} = \left\{ gH \in \frac{G}{H} \middle| g \in J \right\} = \frac{J}{H}$.

$\mathrm{Im}(f) = \left\{ gJ \in \frac{G}{J} \middle| f(gH) = gJ \right\} = \left\{ gJ \in \frac{G}{J} \middle| gJ = gJ \right\} = \frac{G}{J}$, hence f is onto. Therefore, by the 1st Isomorphism Theorem, $\frac{J}{H} \triangleq \frac{G}{H}$ and $\frac{G/H}{J/H} \cong \frac{G}{J}$.

Definition: Maximal Normal Subgroup

H is a maximal normal subgroup of G if the only normal subgroups of G containing H are H and G.

Claim

$\frac{G}{H}$ has no proper normal subgroups if and only if H is a maximal normal subgroup in G.

Proof:

($\Rightarrow$) Assume $\frac{G}{H}$ has no proper subgroups. Suppose H is not maximal. Let $A \triangleq G$ such that $H \subset A$. Then $A \triangleq H$ since $gH = Hg \;, \forall g \in G$, especially for $g \in A$. So $\frac{A}{H}$ is a group. By part 1 of 3rd Isomorphism Theorem, $\frac{A}{H} \triangleq \frac{G}{H}$. Contradiction.

($\Leftarrow$) Assume H is a maximal normal subgroup in G. Suppose $\frac{G}{H}$ has a proper normal subgroup $\frac{A}{H}$ (can choose coset representatives such that A is a subgroup of G). By part 2 of 3rd Isomorphism Theorem, $\frac{G/H}{A/H} \cong \frac{G}{A}$. Since $\frac{G}{A}$ is isomorphic to a group, it is a group. Hence $A \triangleq G$. But $A \supset H$, so H is not maximal. Contradiction.

Group Actions

Definition: Group Action

A group action $G\cdot X\rightarrow X$ is such that $g_1\cdot(g_2\cdot x)=(g_1*g_2)\cdot x$, where $g_{2,}g_2\in G$ (G a group), $x\in X$ (X a set), $\cdot$ is the group action, $*$ is the group operation.

Definition: Orbit

The orbit of $x\in X$ is the set of images of x after being acted on by all $g\in G$. That is, $O(x)=\{g\cdot x|\forall\, g\in G\}$.
Note: $O(x)\subset X$.

Definition: Stabilizer

The stabilizer of $x\in X$ is $\mathrm{Stab}_G(x)=\{g\in G|g\cdot x=x\}$.
Note: $\mathrm{Stab}_G(x)\subset G$.

Definition: Faithful

A group action is called faithful if $g\cdot x=x\Leftrightarrow g=e$.

Remark

A group action is faithful if and only if $\mathrm{Stab}_G=\{e\}$.

Definition: Transitive

A group action is transitive if for all $x, y\in X$ there exists $g\in G$ such that $x=g\cdot y$.

Remark

$O(X)=X$ if and only if $G\cdot X\rightarrow X$ is transitive.

Definition: Centralizer

In the case where $G=G$, $X=G$, $g\cdot x=g^{-1}x\,g$, the stabilizer of $x\in X$ is $\mathrm{Stab}_G(x)=\{g\in G|g^{-1}x\,g=x\}$. It is called a centralizer.

- The centralizer of $A\subset X=G$ is $C_G(A)=\{g\in G|g\,a=a\,g\quad\forall\, a\in A\}$.
- The centralizer of $x\in X=G$ is $C_G(x)=\{g\in G|g\,x=x\,g\}$.

Remark

The centralizer of G is $C_G(G)=Z(G)$, the center of G.

Definition: Normalizer

The normalizer of $x\in G$ is $N_G(x)=\{g\in G|g^{-1}x\,g=x\}=C_G(x)$.
The normalizer of $A\subset G$ is $N_G(A)=\{g\in G|g^{-1}a\,g\in A\}$.

Lemma

$\mathrm{Stab}_G(x)$ is a subgroup.

Proof: $e\cdot x=x$, hence $e\in\mathrm{Stab}_G(x)$. Let $g_{1,}g_2\in\mathrm{Stab}_G(x)$. Then $g_2\cdot x=x\Rightarrow g_2^{-1}g_2\cdot x=g_2^{-1}x\Rightarrow e\cdot x=g_2^{-1}x\Rightarrow x=g_2^{-1}x$, so $g_2^{-1}\in\mathrm{Stab}_G(x)$. So $(g_1g_2^{-1})\cdot x=g_1\cdot(g_2^{-1}\cdot x)=g_1\cdot x=x$, hence $g_1g_2^{-1}\in\mathrm{Stab}_G(x)$. So by the subgroup criterion, $\mathrm{Stab}_G(x)$ is a subgroup.

Theorem: Orbit-Stabilizer Theorem
$|O(x)| = \dfrac{|G|}{|\mathrm{Stab}_G(x)|}$.

Proof: Fix $x \in X$. $O(x) = \{g \cdot x | \forall\, g \in G\}$. Define $f : O(X) \to \dfrac{G}{\mathrm{Stab}_G(x)}$ by $f(g \cdot x) = g H_x$ where $H_x = \mathrm{Stab}_G(x)$. f is onto since all $g H_x$ will have preimage $g \cdot x$. Now let $g_1 H_x = g_2 H_x$. Then $g_1 = g_2 h$ for some $h \in H_x$, so $g_1 \cdot x = g_2 \cdot (h \cdot x) = g_2 \cdot x$. Hence f is 1:1. So if $|G| < \infty$, then $|O(x)| = \left|\dfrac{G}{H_x}\right| = \dfrac{|G|}{|H_x|}$.

Theorem: Class Equation
Let $G = G$, $X = G$, $g \cdot x = g^{-1} x g$. Then $|G| = |Z(G)| + \sum_{x \notin \mathrm{Stab}_G(x)} \dfrac{|G|}{|\mathrm{Stab}_G(x)|}$ with no repetition of x 's conjugate to each other.

Proof: Conjugacy class of $z \in Z(G)$ is $\{z\}$. Conjugacy class partition G , so $|G| = |Z(G)| + \sum_{x \notin Z(G)} |\text{conjugacy class of } x|$. Now, $O(x) = \{g \cdot x | \forall\, g \in G\} = \{g^{-1} x g | \forall\, g \in G\}$ is the conjugacy class of x , and $|O(x)| = \dfrac{|G|}{|\mathrm{Stab}_G(x)|}$ by the orbit-stabilizer theorem. Hence $|G| = |Z(G)| + \sum_{x \notin \mathrm{Stab}_G(x)} \dfrac{|G|}{|\mathrm{Stab}_G(x)|}$.

Lemma
$|O(x)|$ is a factor of $|G|$.

Proof: $|O(x)| = \dfrac{|G|}{|\mathrm{Stab}_G(x)|}$ by orbit-stabilizer theorem. $\mathrm{Stab}_G(x)$ is a subgroup of G , and so $|\mathrm{Stab}_G(x)|$ is a factor of $|G|$ by Lagrange's theorem.

Claim
If p is prime, then $|G| = p^k$ if and only if $|Z(G)| > 1$.

Proof: Let $G = G$, $X = G$, $g \cdot x = g^{-1} x g$. The by the class equation, $|G| = |Z(G)| + \sum |O(x)|$, so $|O(x)|$ has p as a factor. Suppose $|Z(G)| = 1$. Then $p_k = 1 + \sum_i p^{\alpha_i}$, but p should be a factor of both sides. Hence $|Z(G)| > 1$. In fact, $|Z(G)| = p^{\alpha}$ for some $\alpha \leq k$.

Theorem: Cauchy's Theorem
Let $|G| = k p^m$ where p is prime and p is not a factor of k . Then there exists $x \in G$ such that $|x| = p$.

Proof: Let $X = \{(x_1, \ldots, x_p) | x_1 \cdots x_p = e \ \ , x_i \in G\}$ the set of p -tuples in G such that $x_1 \cdots x_p = e$. $|X|$ is a multiple of p . Let $m \in \mathbb{Z}_p$ act on X by sending $m \cdot (x_1, \ldots, x_p)$ to $(x_{m+1}, \ldots, x_p, x_1, \ldots, x_m)$. Each order of an orbit has either 1 or p p -tuples. Now $(e, \ldots, e)$ has orbit $\{(e, \ldots, e)\}$. Since orbits partition X , there exists some other orbit hat has one element as well. Call the element in this orbit $(g_1, \ldots, g_p)$. $m \cdot (g_1, \ldots, g_p) = (g_1, \ldots, g_p) \forall\, m \in \mathbb{Z}_p$, so $g_1 = \cdots = g_p$ and $g_1 \cdots g_p = (g_1)^p = e$. Therefore $x = g_1$ is the desired element.

Remark

Recall that $N_G(A)=\{g\in G|g^{-1}a\,g\in A\}$ and $C_G(A)=\{g\in G|g\,a=a\,g \ \ \forall\, a\in A\}$ for a subgroup $A\subset G$. In general, if $A\trianglelefteq G$ then $N_G(A)=G$.

The Sylow Theorems

Theorem: Sylow Theorem 1

Let $|G|=k\,p^m$ where p is prime and $p\nmid k$. Then G contains a subgroup of order p^m.

Proof: Let X be the collection of subsets of G of p^m elements. Use induction on $|G|$. Induction hypothesis: G has a subgroup of order p^m.

- If $|G|=1$, then $G=\{e\}$, therefore vacuously true.
- If $|G|=2$, then $G=\{e,a\}$, therefore G is its own subgroup of order 2^1.
- Now let $|G|=n=k\,p^m$. Assume induction hypothesis for all $|G|<k\,p^m$.
  - Case 1: If p is a factor of $|Z(G)|$, then Cauchy's Theorem implies $Z(G)$ has an element of order p (since $Z(G)$ is a group); call it g. g generates a subgroup of order p; call it N. Since $N\subset Z(G)$, $x\,n=n\,x\ ,\forall\, n\in N,\forall\, x\in G$, hence $x^{-1}n\,x\in N\ ,\forall\, n\in N,\forall\, x\in G$, so $N\trianglelefteq G$. Now $\left|\frac{G}{N}\right|=\frac{|G|}{|N|}=\frac{k\,p^m}{p}=k\,p^{m-1}$, so by induction hypothesis $\frac{G}{N}$ has a subgroup, say $\frac{P}{N}$, of order p^{m-1}. $|P|=\frac{|P|}{|N|}|N|=\left|\frac{P}{N}\right||N|=p^{m-1}p=p^m$. Therefore P is a subgroup of G of order p^m.
  - Case 2: If p is not a factor of $|Z(G)|$, then let $g_1,\dots,g_r$ be representatives of distinct conjugacy classes of $G-Z(G)$. By the class equation, $|G|=|Z(G)|+\sum_i\frac{|G|}{|C_G(g_i)|}$. p cannot be factor of all $\frac{|G|}{|C_G(g_i)|}$ or else p is a factor of $|Z(G)|$. Therefore there exists a g_i such that $\frac{|G|}{|C_G(g_i)|}=\frac{k\,p^m}{l\,p^m}=\frac{k}{l}$ where $\text{gcf}(l,p)=1$. By the Orbit-Stabilizer Theorem, $\frac{|G|}{|C_G(g_i)|}=|\text{conjugacy class of } g_i|$. Let $H=C_G(g_i)$. Then $|H|=l\,p^m\neq k\,p^m$ since $g_i\notin Z(G)$, so $|H|<|G|$. By induction hypothesis, H has a subgroup of order p^m, which is also a subgroup of G.

Definition: Sylow *p*-Subgroup

Let $|G|=k\,p^m$ where p is prime and $p\nmid k$. A subgroup of G of order p^m is called a Sylow p-subgroup.

Theorem: Sylow Theorem 2

Let $|G|=k\,p^m$ where p is prime and $p\nmid k$. Any two Sylow p-subgroups are conjugate, i.e. there exists $g\in G$ such that $g^{-1}P\,g=Q$ for all P and Q subgroups of order p^m.

Theorem: Sylow Theorem 3

Let $|G|=k\,p^m$ where p is prime and $p\nmid k$. If n_p is the number of Sylow p-subgroups, then $n_p\equiv 1\,mod\,p$ and $n_p|k$.

Proof: Let $H_1,\dots,H_t$ be the subgroups of G of order p^m. Now let H_1 act on $\{H_1,\dots,H_t\}$ by conjugation (i.e. $h\cdot H_j=h^{-1}H_j h$). Then $\text{Stab}_{H_1}(H_j)=K_j=H_1\cap H_j$ (**). Now, $K_1=H_1$, so $O(H_1)=H_1$. Now if $j\neq 1$, $|K_j|$ is a smaller power of p than p^m. Then the Orbit-Stabilizer Theorem implies $|O(H_j)|$ is multiples of p since they are factors of $|H_1|$. Since t is the number of subgroups being acted on, so $t=1+(\text{multiples of } p)\equiv 1 \text{ mod } p$. Hence the number of Sylow p-subgroups is $n_p\equiv 1 \text{ mod } p$.

Now let G act on $\{H_1,\dots,H_t\}$ by conjugation. Suppose H_r (for some r) is not in the orbit of H_1. Now let H_r act on $\{H_1,\dots,H_t\}$ by conjugation. The G-orbit of H_1 is partitioned into H_r-orbits, the size of which are multiples of p by

the Orbit-Stabilizer Theorem since H_r is not in H_1 's orbit. So the G -orbit of H_1 has $0 \bmod p$ elements in it, which contradicts $n_p \equiv 1 \bmod p$. Hence H_r cannot exists and the G -orbit of H_1 is $\{H_{1,} \ldots, H_t\}$. In other words, $O(H_1)=\{g \cdot H_1 | \forall g \in G\}=\{g^{-1} H_1 g | \forall g \in G\}=\{H_{1,} \ldots, H_t\}$. So given any H_i and H_j , $H_1=g_i^{-1} H_i g_i$ and $H_1=g_j^{-1} H_j g_j$, so $g_i^{-1} H_i g_i=g_j^{-1} H_j g_j \Rightarrow H_i=(g_i g_j^{-1}) H_j (g_j g_i^{-1})=g^{-1} H_j g$ for $g=g_j g_i^{-1}$. Therefore Any two Sylow p -subgroups are conjugate.

Now, Orbit-Stabilizer Theorem implies $|O(H_1)|=\dfrac{|G|}{|\mathrm{Stab}_G(H_1)|}$ and so $t=n_p$ is a factor of $|G|=k p^m$. Since we know $t \equiv 1 \bmod p$, t is not a factor of p^m , hence t is a factor of k . Therefore $n_p | k$.

(**) $K_j=\mathrm{Stab}_{H_1}(H_j)=\{h \in H_1 | h^{-1} H_j h=H_j\}$, so $K_j \subseteq H_1$. $H_1 \cap H_j \subseteq K_j$, hence $K_j H_j=H_j K_j$ and so $K_j H_j$ is a subgroup. Also, $H_j \trianglelefteq K_j H_j$ since $H_j k=k H_j$. So by the 2nd Isomorphism Theorem, $\dfrac{K_j H_j}{H_j} \cong \dfrac{K_j}{K_j \cap H_j}$. So $|K_j H_j|=\dfrac{|K_j||H_j|}{|K_j \cap H_j|}=p^r$, but $H_j \subseteq K_j H_j$ and $|H_j|=p^m$, so $K_j H_j=H_j$. We have $K \subseteq H_1 \cap H_j \subseteq K_j$, so $K_j=H_1 \cap H_j$.

Lemma
If H , K are subgroup of G , and $H K=K H$, then $H K$ is a subgroup.

Proof: Let $h_1 k_{1,} h_2 k_2 \in H K$. Then $h_1 k_1 k_2^{-1} h_2^{-1}=h_1 k_3 h_2^{-1}=h_1 h_3 k_4=h_4 k_4 \in H K$. Also, $e \in H K$. So the the Subgroup Criterion, $H K$ is a subgroup.

Corollary (of Sylow Theorem 2)
If $n_p=1$, i.e. H is the only Sylow p -subgroup of G , then $H \trianglelefteq G$.

The Fundamental Theorem of Finitely Generated Abelian Groups

Theorem: The Fundamental Theorem of Finitely Generated Abelian Groups
Let G be abelian and finitely generated. Then $G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus \mathbb{Z}^s$ where $m_i | m_{i+1}$, $m_{1,} \ldots, m_t, s \in \mathbb{Z}$, $m_{1,} \ldots, m_t, s \geq 0$, $\mathbb{Z}^s=\underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{s}$. Here $m_{1,} \ldots, m_t$ are called torsion coefficients, and s is the rank.

Theorem
$\mathbb{Z}_n \oplus \mathbb{Z}_m=\mathbb{Z}_{nm}$ if and only if $\gcd(n, m)=1$.

Definition: Canonical Form
We say $\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus \mathbb{Z}^s$ is a group written in canonical form iff $m_i | m_{i+1}$.

Question
How to to between canonical form and generators-and-relations form?

- Given canonical form $\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus \mathbb{Z}^s$, let $x_i=(\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{t-i}, \underbrace{0, \ldots, 0}_{s})$ for $i=1, \ldots, t$, and $y_j=(\underbrace{0, \ldots, 0}_{t}, \underbrace{0, \ldots, 0}_{j-1}, 1, \underbrace{0, \ldots, 0}_{s-j})$ for $j=1, \ldots, s$. Then $\langle x_{1,} \ldots, x_t, y_{1,} \ldots, y_s | \text{abelian}, x_i^{m_i}=e \text{ for } i=1, \ldots, t\rangle$ is the generators-and-relations form.
- Given generators-and-relations form, use the following steps.

1. Rewrite the relations in additive notation, ignoring the ones specifying abelianism.
2. Write out the coefficient matrix, where entries are coefficients of each generator.
3. Diagonalize using the three rules:
   - switch any two rows or columns,
   - multiply -1 to any row or column,
   - add an integer multiple of any row to row, or column to column.
4. Each non-zero entry on the diagonal is a torsion coefficient. A zero means a copy of $\mathbb{Z}$, and a 1 means one too many generator.

Automorphisms

Definition: Automorphism
An automorphism is an isomorphism from a group G to itself.

Definition: Automorphism Group
$\mathrm{Aut}(G)$ is the set of all automorphisms of G .

Claim
For $|G|<\infty$ (i.e. finite groups), $\mathrm{Aut}(G)$ is a group under function composition.

Proof: Let $f_{1,}\ldots,f_n\in\mathrm{Aut}(G)$.

- $f_1(x)=x$ is the identity since $(f_i\circ f_1)(x)=f_i(f_1(x))=f_i(x)$ and $(f_1\circ f_i)(x)=f_1(f_i(x))=f_i(x)$.
- Let $f_i\in\mathrm{Aut}(G)$. f_i^{-1} exists and is 1:1 onto since f_i is 1:1 onto on a finite set to itself. We know $f_i(ab)=f_i(a)f_i(b)$ since f_i a homomorphism, so $f_i^{-1}(f_i(a)f_i(b))=f_i^{-1}(f_i(ab))=ab=f_i^{-1}(f_i(a))f_i^{-1}(f_i(b))$. Hence f_i^{-1} is a homomorphism, 1:1 and onto, so $f_i^{-1}\in\mathrm{Aut}(G)$.
- $(f_i\circ(f_j\circ f_k))(x)=(f_i(f_j(f_k(x))))=((f_i\circ f_j)\circ f_k)(x)$, so associativity holds.
- Let $f_i,f_j\in\mathrm{Aut}(G)$. Then $f_i\circ f_j$ is 1:1 since f_i and f_j are, and $f_i\circ f_j$ is onto since f_i and f_j are. $(f_i\circ f_j)(ab)=f_i(f_j(ab))=f_i(f_j(a)f_j(b))=f_i(f_j(a))f_i(f_j(b))=(f_i\circ f_j)(a)(f_i\circ f_j)(b)$, so $f_i\circ f_j$ is a homomorphism. Hence $\mathrm{Aut}(G)$ is closed under composition.

Therefore, $\mathrm{Aut}(G)$ is a group.

Definition: Characteristic
H is characteristic (as a subgroup of G), denoted $H\,\mathrm{char}\,G$, iff $f(H)=f\;,\forall f\in\mathrm{Aut}(G)$.

Theorem
1. Characteristic subgroups are normal.
2. If H is the only subgroup of a given order, then $H\,\mathrm{char}\,G$.
3. If $K\,\mathrm{char}\,H$ and $H\trianglelefteq G$, then $K\trianglelefteq G$.

Definition: Inner Automorphism
$\mathrm{Inn}(G)$ is the set of inner automorphisms of G . An inner automorphism is a function f such that $f(x)=g^{-1}xg$ for a fixed g .

Claim
$f_g\in\mathrm{Inn}(G)$ is an isomorphism.

Proof: f_g is 1:1 since L_g and R_g are. f_g is onto since only use g 's that give onto f_g 's. f_g is a homomorphism since $f_g(a\,b)=g^{-1}\,a\,b\,g=g^{-1}a\,g\,g^{-1}\,b\,g=f_g(a)\,f_g(b)$.