Chapter 1

Groups

1.1 Definitions and Elementary Properties

Definition 1.1.1. *A **binary operation** $*$ on a set S is a function*

$$\begin{aligned} * : S \times S &\to S \\ (a, b) &\mapsto a * b. \end{aligned}$$

*$*$ is called **associative** if $(a * b) * c = a * (b * c) \quad \forall a, b, c \in S$.*
*$*$ is called **commutative** if $a * b = b * a \quad \forall a, b \in S$.*

Definition 1.1.2. *A **group** consists of a set G together with a binary operation*

$$\begin{aligned} * : G \times G &\mapsto G \\ (g, h) &\mapsto g * h, \end{aligned}$$

such that the following conditions are satisfied:

1. *$(a * b) * c = a * (b * c) \quad \forall a, b, c \in S$ (associativity),*
2. *There exists an element $e \in G$ such that $e * a = a$ and $a * e = a \quad \forall a \in G$ (identity),*
3. *For each $a \in G$, there exists an element $b \in G$ such that $a * b = e$ and $b * a = e$ (inverse).*

Definition 1.1.3. *A group $(G, *)$ is called **abelian** (or commutative) if $a * b = b * a \quad \forall a, b \in G$.*

Definition 1.1.4. *Let H be a non-empty subset of the group G. Suppose that the product in G of two elements of H lies in H and that the inverse in G of any element of H lies in H. Then H is called a **subgroup** of G, written $H \leq G$.*

Notation: For $X \subset G$, write
$$\langle X \rangle = \bigcap_{X \subset H \leq G} H.$$
This is called **the subgroup of** G **generated by** X.
Exercise: show that $\langle X \rangle$ is a subgroup.

Example 1.1.5.

1. ***Cyclic groups*** C_n
Let $n \in \mathbb{N}$. $C_n := \{e = x^0, x, x^2, \ldots, x^{n-1}\}$, *with multiplication* $x^j * x^k := x^{(j+k) \bmod n}$.
Also, the infinite cyclic group is $C_\infty := \{x^n \mid n \in \mathbb{Z}\}$ *with* $x^j * x^k := x^{j+k}$.

2. ***Permutation groups***
Let X *be a set.* $S_X := \{f : X \mapsto X \mid f \text{ is a bijection}\}$. *Multiplication is composition*
$$\begin{aligned} S_X \times S_X &\mapsto S_X \\ (f, g) &\mapsto g \circ f. \end{aligned}$$
Notation: *In case* $X = \{1, \ldots, n\}$ *for some* $n \in \mathbb{N}$, *write* S_n *for* S_X *(called a* ***symmetric group****).*
If $G \leq S_n$ *for some* n, G *is a* ***permutation group*** *of degree* n.

3. ***Linear groups***
A ***field*** $(\mathbb{F}, +, \cdot)$ *consists of a set* $\mathbb{F}$ *together with binary operations* $+$ *and* $\cdot$*, such that:*
   (a) $(\mathbb{F}, +)$ *forms an abelian group,*
   (b) $(\mathbb{F} - \{0\}, \cdot)$ *forms an abelian group (where* 0 *is the identity for* $(\mathbb{F}, +)$*),*
   (c) $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in \mathbb{F}$ *(distributivity).*

   Let $\mathbb{F}$ *be a field.* $GL_n(\mathbb{F}) := \{\text{invertible } n \times n \text{ matrices with entries from } \mathbb{F}\}$. *The group operation is matrix multiplication.* GL_n *is called the* ***general linear group****.*
If $G \leq GL_n(\mathbb{F})$ *for some* $\mathbb{F}$ *and* n *then* G *is called a* ***linear group*** *of degree* n.

4. ***Symmetry groups*** *Let* $X \subset \mathbb{R}^n$. *The group of symmetries of* X, *denoted* $Sym(X)$, *is the subgroup of* S_X *containing only isometries (that is, functions* $f : X \mapsto X$ *such that* $\|f(x) - f(y)\| = \|x - y\| \quad \forall x, y \in X$*).*
Notation: *In case* $N = 2$ *and* $X =$ *the regular* n*-gon,* $Sym(X)$ *is called the* n^{th} ***dihedral group****, written* D_{2n}.

Proposition 1.1.6. *Let* G *be a group. Then* $\exists$ *exactly one element* $e \in G$ *such that* $e * g = g$ *and* $g * e = g \quad \forall g \in G$.

Proof. By definition, such an element exists. If $e, e' \in G$ both have the property then

$$e = e * e' = e'.$$

$\square$

Proposition 1.1.7. *Let G be a group and let $g \in G$. Then $\exists$ exactly one element $h \in G$ such that $g * h = e$ and $h * g = e$.*

Proof. By definition, such an element exists. Suppose h, h' are both inverses to g. Then

$$h' = h' * e = h' * (g * h) = (h' * g) * h = e * h = h.$$

$\square$

Notation: The inverse to g will be denoted g^{-1}.

Proposition 1.1.8. *Let G be a group and let $x, y, z \in G$.*

1. *If $xz = yz$ then $x = y$.*
2. *If $zx = zy$ then $x = y$.*

Proof.

1. $x = xe = x(zz^{-1}) = (xz)z^{-1} = (yz)z^{-1} = y(zz^{-1}) = ye = y$.
2. Likewise.

$\square$

Note: $xz = zy \not\Rightarrow x = y$; "mixed" cancellation doesn't work.

Corollary 1.1.9. *Let G be a group and let $g, h \in G$ such that $g * h = e$. Then $h = g^{-1}$ (and $g = h^{-1}$).*

Proof. $g * h = e$ is given; $g * g^{-1} = e$ by the definition of g^{-1}. So by cancellation, $h = g^{-1}$. $\square$

Proposition 1.1.10. *In a group G, $(gh)^{-1} = h^{-1}g^{-1}$.*

Proof.

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e.$$

$\therefore h^{-1}g^{-1}$ is the inverse of gh. $\square$

Proposition 1.1.11. *Let G be a group and $g, h \in G$. Then*

1. $\exists!$ *solution x in G to the equation $gx = h$.*

2. $\exists!$ *solution x in G to the equation $xg = h$.*

Proof.
1. $x = g^{-1}h$.

2. $x = hg^{-1}$.

□

Proposition 1.1.12. *A non-empty subset H of a group G is a subgroup iff $x, y \in H$ implies xy^{-1} lies in H.*

Proof. Exercise. □

G is called a **finite** group if its underlying set is finite. In this case, the number of elements in G is called the **order** of G, written $|G|$.

Definition 1.1.13. *Let $x \in G$. The **order** of x, written $|x|$, is the least integer k (if any) such that $x^k = e$.*

Note: some, or even all elements of a group might have finite order even if $|G|$ is infinite.

Definition 1.1.14. *Let $(G, *)$ and $(H, \vartriangle)$ be groups. A function $f : G \mapsto H$ is called a (group) **homomorphism** if $f(x * y) = f(x) \vartriangle f(y) \quad \forall x, y \in G$. A homomorphism $f : G \mapsto H$ which is a bijection is called an **isomorphism**.*

Notation: $\phi : G \overset{\cong}{\longmapsto} H$ means that ϕ is an isomorphism from G to H.
$G \cong H$ means that there exists an isomorphism $\phi : G \overset{\cong}{\longmapsto} H$.

Isomorphisms preserve all group properties. e.g. if $\phi : G \overset{\cong}{\longmapsto} H$ then:

$$G \text{ is abelian } \iff H \text{ is abelian,}$$
$$|x| = |\phi(x)| \quad \forall x \in G, \text{ etc.}$$

Lemma 1.1.15. *Let $\phi : G \mapsto H$ be a homomorphism, and let e, e' be the identities in G, H respectively. Then $\phi(e) = e'$.*

Proof. Let $h = \phi(e)$.

$$h^2 = \phi(e)\phi(e) = \phi(e^2) = \phi(e) = h = he'$$

$\therefore$ by cancellation, $h = e'$. □

Corollary 1.1.16. *Let $\phi : G \mapsto H$ be a homomorphism. Then $\forall g \in G, \phi(g^{-1}) = \phi(g)^{-1}$.*

Proof.
$$\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e) = e'.$$
Thus, $\phi(g)^{-1} = \phi(g^{-1})$. □

Proposition 1.1.17. *Let $\phi : G \mapsto H$ be a group isomorphism. Let $\phi^{-1} : H \mapsto G$ be the inverse function to the bijection ϕ. Then ϕ^{-1} is an isomorphism.*

Proof. Must show ϕ^{-1} is a homomorphism. Let $h_1, h_2 \in H$. Since ϕ is a bijection, $\exists! g_1, g_2 \in G$ such that $\phi(g_1) = h_1, \phi(g_2) = h_2$.
$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = h_1 h_2$$
So $\phi^{-1}(h_1 h_2) = g_1 g_2 = \phi^{-1}(h_1)\phi^{-1}(h_2)$. □

Proposition 1.1.18. *The composition of group homomorphisms is a homomorphism.*
The composition of group isomorphisms is a isomorphism.

Proof. Trivial. □

Notation: $Aut(G) = \{\text{self-isomorphisms of } G\} \leq S_G$.

Fundamental Problem of Group Theory:
Make a list of all possible types of groups. ie. Make a list of groups such that every group is isomorphic to exactly one group on the list.

Given two groups (defined, for example, by multiplication tables, or by generators and relations), the problem of determining whether or not the groups are isomorphic is, in general, very difficult (NP-hard).

1.2 New Groups from Old

1.2.1 Quotient Groups

Definition 1.2.1. *Let $\phi : G \mapsto H$ be a homomorphism. The* ***kernel*** *of ϕ is*

$$\ker\phi := \{g \in G \mid \phi(g) = e\}.$$

The ***image*** *of ϕ is*

$$\mathrm{Im}\phi := \{h \in H \mid h = \phi(g) \text{ for some } g \in G\}.$$

Proposition 1.2.2. $\ker\phi \leq G$ *and* $\mathrm{Im}\phi \leq G$.

Proof. Trivial. ◻

Definition 1.2.3. *For $x, y \in G$, we say y is* ***conjugate*** *to x (in G) if $\exists g \in G$ such that $y = gxg^{-1}$.*

Proposition 1.2.4. *Conjugacy is an equivalence relation.*

Proof. Trivial. ◻

Notation: If A, B are subsets of G, let $AB := \{ab \mid a \in A, b \in B\}$. For $g \in G, H \leq G$, the set gH is called the **left coset** of H generated by g; Hg is the **right coset** of H generated by g.

Definition 1.2.5. *A subgroup N of G is called* ***normal****, written $N \lhd G$, if $gN = Ng$ for all $g \in G$.*

Proposition 1.2.6. *$N \leq G$ is normal $\iff gxg^{-1} \in N \quad \forall x \in N, g \in G$.*

Proof.

$\Rightarrow$: Suppose N is normal. Then for all $x \in N, g \in G$, $gx \in gN = Ng$, so $gx = yg$ for some $y \in N$. Thus, $gxg^{-1} = y \in N$.

$\Leftarrow$: Suppose $gxg^{-1} \in N \quad \forall x \in N, g \in G$. If $z \in gN$ then $z = gx$ for some $x \in N$. Hence,

$$z = gx(g^{-1}g) = (gxg^{-1})g \in Ng$$

$\therefore gN \subset Ng$. Similarly, $Ng \subset gN$.

◻

Corollary 1.2.7. *Let $\phi : G \mapsto H$ be a homomorphism. Then $\ker\phi \lhd G$.*

Proof. Let $x \in \ker\phi$ and let $g \in G$. Then

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

so $gxg^{-1} \in \ker\phi$. $\square$

Conversely:

Theorem 1.2.8. *Suppose $N \lhd G$. Then $\exists$ a group H and a homomorphism $\phi : G \mapsto H$ such that $N = \ker\phi$.*

Proof. Exercise: check the details of the following:

1. For $g, g' \in G$, define $g \sim g'$ if $g'g^{-1} \in N$.
2. Check that $\sim$ is an equivalence relation.
3. Define $H := G/N :=$ {set of equivalence classes of G under $\sim$}.
4. Define binary operation $*$ on G/N by $\overline{x} * \overline{y} = \overline{xy}$. Check that this is well-defined, ie. suppose $x' \sim x$ and $y' \sim y$. Is $x'y' \sim xy$?
   Well, $x' \sim x$ means $x'x^{-1} = n_1 \in N$, so $x' = n_1x$. Likewise, $y' \sim y$ means $y'y^{-1} = n_2 \in N$, so $y' = n_2y$. So
   $$x'y' = n_1xn_2y = n_1(xn_2x^{-1})xy = n_1n_2'xy,$$
   where $n_2' = xn_2x^{-1} \in N$ since N is normal. Hence, $x'y' \sim xy$.
5. Check that $(G/N, *)$ forms a group.
6. Define $\phi : G \mapsto H$ by $\phi(x) = \overline{x}$.
7. Check that ϕ is a group homomorphism.
8. Check that $N = \ker\phi$.

$\square$

G/N (as constructed above) is called a **quotient group**.

1.2.2 Product Groups

Let G, H be groups. The **product group** is the set $G \times H$, with multiplication

$$(g, h) \cdot (g', h') := (gg', hh').$$

Clearly the projection maps

$$\begin{aligned} \Pi_G : G \times H &\mapsto G \\ (g, h) &\mapsto g \end{aligned}$$

and

$$\begin{aligned} \Pi_H : G \times H &\mapsto H \\ (g, h) &\mapsto h \end{aligned}$$

are group homomorphisms.

Proposition 1.2.9. *Let A, G, H be groups.*

1. *Universal Property of Product:*
   Given group homomorphisms $p : A \mapsto G$ and $q : A \mapsto H$, $\exists!$ group homomorphism $\phi : A \mapsto G \times H$ such that:

$$\begin{tikzcd} & A \arrow[dl, "p"'] \arrow[d, dashed, "\exists!\phi"] \arrow[dr, "q"] & \\ G & G \times H \arrow[l, "\Pi_G"] \arrow[r, "\Pi_H"'] & H \end{tikzcd}$$

   This says that $G \times H$ is the product of G and H in the category of groups.

2. *Given a function $\phi : A \mapsto G \times H$, ϕ is a group homomorphism if and only if $\Pi_G \circ \phi$ and $\Pi_H \circ \phi$ are group homomorphisms.*

1.2.3 Free Products

Let G, H be groups. The free product of G and H is $G * H := \{\text{words in } G \amalg H\}/\sim$, where $\sim$ is the equivalence relation generated by the following: for $g, g' \in G$,

$$x_1 \cdots x_n g g' y_1 \cdots y_m \sim x_1 \cdots x_n (g g') y_1 \cdots y_m,$$

and for $h, h' \in H$,

$$x_1 \cdots x_n h h' y_1 \cdots y_m \sim x_1 \cdots x_n (h h') y_1 \cdots y_m.$$

Note: Given $A \subset X \times X$, the equivalence relation generated by A is

$$\bigcap \{B \subset X \times X \mid B \text{ is an equivalence relation and } A \subset B\}.$$

Multiplication in $G * H$ is given by juxtaposition: $(v_1 \cdots v_n) * (w_1 \cdots w_m) = v_1 \cdots v_n w_1 \cdots w_m$.

Proposition 1.2.10. *Universal Property of Free Product:*

$$\begin{tikzcd}
G \arrow[dr, "g \mapsto g"] \arrow[ddr, "p"'] & & H \arrow[dl, "h \mapsto h"'] \arrow[ddl, "q"] \\
& G * H \arrow[d, dashed, "\exists ! \phi"] & \\
& A &
\end{tikzcd}$$

(Here, G and H each embed into the words of length 1 in $G \times H$).
This says that $G * H$ is the coproduct of G and H in the category of groups.

$F(x) = \{x^n \mid n \in \mathbb{Z}\} (= C_\infty)$ is called the free group on the generator x.
$F(x, y) := F(x) * F(y)$ is the free group on 2 generators.
More generally, given a set S,

$$F(S) = \{\text{words in } S\}$$

is called the **free group on** S. A group homomorphism $F(S) \mapsto G$ is uniquely determined by any (set) function $S \mapsto G$.

1.3 Centralizers, Normalizers, and Commutators

Let G be a group, $X \subset G$.
Notation:

$$\begin{aligned}
\mathrm{C}_G(X) &:= \{g \in G \mid gxg^{-1} = x \quad \forall x \in X\} \quad \text{is the } \textbf{centralizer} \text{ of } X \text{ in } G\\
\mathrm{N}_G(X) &:= \{g \in G \mid gXg^{-1} = X\} \quad \text{is the } \textbf{normalizer} \text{ of } X \text{ in } G\\
&= \{g \in G \mid gX = Xg\}
\end{aligned}$$

These definitions do not require that X be a subgroup, but note that $\mathrm{C}_G(X) = \mathrm{C}_G(\langle X\rangle)$. Also,

$$\begin{aligned}
\mathrm{Z}(G) &:= \mathrm{C}_G(G) \quad \text{is the } \textbf{center} \text{ of } G\\
&= \{g \in G \mid gx = xg \quad \forall x \in G\}
\end{aligned}$$

Note: $\mathrm{Z}(G) = G \iff G$ is abelian.

Example 1.3.1. *Let* $G = GL_n(\mathbb{F})$. *Then* $\mathrm{Z}(G) = \{cI \mid c \in \mathbb{F}^\times\}$.

Proposition 1.3.2. $\mathrm{C}_G(X)$ *and* $\mathrm{N}_G(X)$ *are subgroups of* G.

Proof.

$$\begin{aligned}
g, g' \in \mathrm{C}_G(X) &\Rightarrow\ (gg')(x)(gg')^{-1} = g(g'xg'^{-1})g^{-1} = gxg^{-1} = x \quad \forall x \in X\\
g \in \mathrm{C}_G(X) &\Rightarrow\ g^{-1}xg = g^{-1}(gxg^{-1})g = (g^{-1}g)x(g^{-1}g) = x \quad \forall x \in X
\end{aligned}$$

Likewise,

$$\begin{aligned}
g, g' \in \mathrm{N}_G(X) &\Rightarrow\ (gg')X(gg')^{-1} = g(g'Xg'^{-1})g^{-1} = gXg^{-1} = X\\
g \in \mathrm{N}_G(X) &\Rightarrow\ g^{-1}Xg = g^{-1}(gXg^{-1})g = (g^{-1}g)X(g^{-1}g) = X
\end{aligned}$$

□

Clearly, $\mathrm{Z}(G) = \mathrm{C}_G(G)$ is always abelian, but for arbitrary H, $\mathrm{C}_G(H)$ need not be abelian. For example, in the extreme case, $\mathrm{C}_G(\{e\}) = G$, which might not be abelian.

For $H \leq G$, by construction, $H \triangleleft \mathrm{N}_G(H)$, and $H \triangleleft G \iff \mathrm{N}_G(H) = G$.

Proposition 1.3.3. *For* $A \leq B \leq G$,

$$g \in \mathrm{N}_G(\mathrm{N}_B(A)) \Rightarrow\ g(\mathrm{N}_B(A))g^{-1} \subset \mathrm{N}_G(A).$$

Proof. If $b \in \mathrm{N}_B(A)$ and $g \in \mathrm{N}_G(\mathrm{N}_B(A))$ then $b' = gbg^{-1} \in \mathrm{N}_B(A)$, so

$$(gbg^{-1})a(gbg^{-1})^{-1} = b'a(b')^{-1} \in A$$

□

Note: $K \lhd H$ and $H \lhd G \not\Rightarrow K \lhd G$. For a counterexample, take

$$\begin{aligned} G &= S_4 \\ H &= \langle (1\ 2\ 3\ 4), (1\ 3)(2\ 4) \rangle \cong D_8 \\ K &= \langle (1\ 2\ 3\ 4) \rangle \cong C_4 \end{aligned}$$

Notation: For $a, b \in G$, let $[a, b] := aba^{-1}b^{-1}$.

Definition 1.3.4. *The **commutator subgroup** G' is the subgroup of G generated by*

$$\{[a, b] \mid a, b \in G\}.$$

Proposition 1.3.5. $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$.

Corollary 1.3.6. $G' \lhd G$.

$G_{ab} := G/G'$ is abelian. Universal property: given any homomorphism $\phi : G \mapsto H$ with H abelian,

$$\begin{tikzcd} G \arrow[r, two heads] \arrow[dr, "\phi"'] & G_{ab} \arrow[d, dashed, "\exists!"] \\ & H \end{tikzcd}$$

That is, if $\phi : G \mapsto H$ with H abelian then $G' \subset \ker \phi$.

1.4 Isomorphism Theorems

Theorem 1.4.1 (First Isomorphism Theorem)**.** *Let $\phi : G \mapsto H$ be a group homomorphism. Then* $G/\ker\phi \cong \mathrm{Im}\phi$.

Proof. Set $N := \ker\phi$. Elements of G/N are cosets Ng, where $g \in G$. Define $\psi : G/N \mapsto \mathrm{Im}\phi$ by $\psi(Ng) = \phi(g)$.

1. ψ is well defined:
   Suppose $Ng = Ng'$. Then $g = ng'$ for some $n \in N$. Hence,
   $$\phi(g) = \phi(ng') = \phi(n)\phi(g') = e_H\phi(g') = \phi(g'),$$
   since $n \in N = \ker\phi$.
2. ψ is a homomorphism – easy.
3. ψ is surjective – easy.
4. ψ is injective:
   If $\psi(Ng_1) = \psi(Ng_2)$ then
   $$\phi(g_1) = \phi(g_2) \Rightarrow \phi(g_1g_2^{-1}) = e_H \Rightarrow g_1g_2^{-1} \in N \Rightarrow Ng_1 = Ng_2$$

$\square$

Proposition 1.4.2. *If H, K subgroups of G then $HK \leq G \iff HK = KH$.*

Proof.

$\Rightarrow$: Suppose $HK \leq G$. Let $x \in HK$. Then $x^{-1} \in HK$. Write $x^{-1} = hk$ for some $h \in H, k \in K$. Then
$$x = (hk)^{-1} = k^{-1}h^{-1} \in KH,$$
so $HK \subset KH$, and similarly, $KH \subset HK$.

$\Leftarrow$: Suppose $HK = KH$. Let $x, x' \in HK$. Write $x = kh, x' = h'k'$, for some $h, h' \in H, k, k' \in K$. Then
$$\begin{aligned} x'x^{-1} &= h'k'h^{-1}k^{-1} \\ &= h'h''k''k^{-1}, \quad \text{letting } k'h^{-1} = h''k'', \text{ since } HK = KH \\ &\in HK \end{aligned}$$

$\square$

Corollary 1.4.3. *Let H, K be subgroups of G. If $H \subset \mathrm{N}_G(K)$ then $HK \leq G$ and $K \triangleleft HK$.*

Proof. Let $x = hk \in HK$. Then $x = (hkh^{-1})h \in KH$, since $hkh^{-1} \in K$. So, $HK \subset KH$. Similarly, if $x = kh \in HK$ then $x = h(h^{-1}kh) \in HK$, whence $KH \subset HK$. Hence

$$HK = KH \leq G.$$

Also, $K \subset \mathrm{N}_G(K)$ (always) and $H \subset \mathrm{N}_G(K)$ (given), so

$$HK \subset \mathrm{N}_G(K) \Rightarrow \; K \triangleleft HK.$$

$\square$

Corollary 1.4.4. *If $K \triangleleft G$ then $HK \leq G$ for any $H \leq G$.*

Proof. If $K \triangleleft G$ then $\mathrm{N}_G(K) = G$, so automatically, $H \subset \mathrm{N}_G(K)$. $\square$

Theorem 1.4.5 (Second Isomorphism Theorem)**.** *Let H, K be subgroups of G such that*

$$H \subset \mathrm{N}_G(K).$$

Then $H \cap K \triangleleft H$, $K \triangleleft HK$, and

$$\frac{HK}{K} \cong \frac{H}{H \cap K}$$

Proof. $K \triangleleft HK$ was shown above. Define $\phi : H \mapsto HK/K$ by $\phi(h) = Kh \in HK/K$. ie. ϕ is the composition

$$H \hookrightarrow HK \mapsto\!\!\!\!\rightarrow HK/K$$

1. ϕ is a homomorphism (composition of homomorphisms).

2. ϕ is surjective

   Proof. Let $Kx \in HK/K$, where $x \in HK$. By above, $HK \leq G$, so $HK = KH$; thus let $x = kh$, for some $k \in K, h \in H$. Hence,

   $$Kx = Kkh = Kh = \phi(h)$$

3. $\ker \phi = H \cap K$

   Proof.

   $$\begin{aligned} \ker \phi &= \{y \in H \mid \phi(y) = e\} \\ &= \{y \in H \mid Ky = e\} \\ &= \{y \in H \mid y \in K\} \\ &= H \cap K \end{aligned}$$

$H \cap K \lhd H$ and
$$\frac{H}{H \cap K} = \frac{H}{\ker \phi} \cong \mathrm{Im}\phi = \frac{HK}{K}.$$
$\square$

Theorem 1.4.6 (Third Isomorphism Theorem)**.** *Let $K \lhd G$ and $H \lhd G$ with $K \subset H$. Then $H/K \lhd G/K$ and*
$$\frac{G/K}{H/K} \cong G/H.$$

Proof. Define ϕ by composition
$$G \mapsto\!\!\!\rightarrow G/K \mapsto\!\!\!\rightarrow \frac{G/K}{H/K}.$$
Check that $\ker \phi = H$ (exercise). $\square$

1.5 The Pullback

Definition 1.5.1. *Let $\phi : G \mapsto H$ and $j : B \mapsto H$ be group homomorphisms. Define the* ***pullback*** *$G \times_H B$ of ϕ and j by*
$$G \times_H B := \{(g, b) \in G \times B \mid \phi(g) = j(b)\}.$$

The pullback gives:

$$\begin{tikzcd}
G \times_H B \arrow[r, "\Pi_G"] \arrow[d, "\Pi_B"'] & G \arrow[d, "\phi"] \\
B \arrow[r, "j"'] & H
\end{tikzcd}$$

Proposition 1.5.2. *$G \times_H B \leq G \times B$.*

Proof. If (g, b) and (g', b') belong to $G \times_H B$ then
$$\phi(gg') = \phi(g)\phi(g') = j(b)j(b') = j(bb').$$
If $(g, b) \in G \times_H B$ then
$$\phi(g^{-1}) = \phi(g)^{-1} = j(b)^{-1} = j(b^{-1}).$$
$\square$

Proposition 1.5.3. *Let $\phi : G \mapsto H$, $j : B \mapsto H$ and $i : A \mapsto B$ be homomorphisms. Then*

$$\begin{tikzcd} A \times_B (B \times_H G) \arrow[r, "\Pi_{B\times_H G}"] \arrow[d, "\Pi_A"'] \arrow[dr, phantom, "p.b."] & B \times_H G \arrow[r, "\Pi_G"] \arrow[d, "\Pi_B"] \arrow[dr, phantom, "p.b."] & G \arrow[d, "\phi"] \\ A \arrow[r, "i"'] & B \arrow[r, "j"'] & H \end{tikzcd}$$

and $A \times_B (B \times_H G) \cong A \times_H G$. (Composition of pullbacks is a pullback).

Proof.

$$A \times_B (B \times_H G) = \{(a, (b, g)) \mid a \in A, (b, g) \in B \times_H G, i(a) = \Pi_B(b, g) = b\}$$

In this description, b is redundant because it is determined by a via $b = i(a)$. Also, $(b, g) \in B \times_H G$ means that $j(b) = \phi(g)$. So,

$$A \times_B (B \times_H G) \cong \{(a, g) \mid j(i(a)) = \phi(g)\} = A \times_H G.$$

□

Note some special cases:

1. If $H = \{e\}$ then $j(b) = \phi(g)$ holds $\forall b, g$, so $B \times_{\{e\}} G = B \times G$.
2. If $B \leq H$ and j is the inclusion, then

$$\begin{aligned} B \times_H G &= \{(b, g) \mid j(b) = \phi(g)\}, \quad \text{so } b \text{ is redundant} \\ &\cong \{g \in G \mid \phi(g) \in B\} \\ &= \phi^{-1}(B) \end{aligned}$$

Proposition 1.5.4. *Let*

$$\begin{tikzcd} B \times_H G \arrow[r, "\Pi_G"] \arrow[d, "\Pi_B"'] & G \arrow[d, "\phi"] \\ B \arrow[r, "j"] & H \end{tikzcd}$$

be a pullback. Then $\ker \Pi_B \cong \ker \phi$ *and* $\ker \Pi_G \cong \ker j$.

Proof.

$$\begin{aligned}\ker \Pi_B &= \{(b,g) \in B \times G \mid b = e \text{ and } \phi(g) = j(b)\}\\ &= \{(e,g) \in B \times G \mid \phi(g) = j(e) = e\}\\ &= \{e\} \times \ker\phi \subset B \times G\\ &\cong \ker\phi\end{aligned}$$

□

Now consider the special case where $B \leq H$ and j is inclusion. Set $A = B \times_H G = \phi^{-1}(B)$.

Proposition 1.5.5.

1. *If $B \lhd H$ then $A \lhd G$.*
2. *If $B \lhd H$ and ϕ is onto then $G/A \cong H/B$.*

Proof.

1. Suppose $B \lhd H$. Let $a \in A$. Then for $g \in G$,
$$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g)^{-1} \in B, \quad \text{since } \phi(a) \in B \lhd H,$$
so $gag^{-1} \in A$.
2. Let ψ be the composition
$$G \overset{\phi}{\longmapsto\!\!\!\!\rightarrow} H \overset{q}{\longmapsto\!\!\!\!\rightarrow} H/B,$$
where q is the quotient map. Then $\phi(A) \subset B = \ker q$ so $A \subset \ker\psi$. If $g \in \ker\psi$ then $\phi(g) \in \ker q = B$, so $g \in \phi^{-1}(B) = A$. Thus, $\ker\psi = A$. Hence,
$$\frac{G}{A} = \frac{G}{\ker\psi} \cong \mathrm{Im}\psi = \frac{H}{B}$$
since both ϕ and q are onto.

□

Theorem 1.5.6 (Fourth Isomorphism Theorem)**.** *Suppose $N \lhd G$. Then the quotient map $q : G \mapsto\!\!\!\rightarrow G/N$ induces a bijection between the subgroups of G which contain N and the subgroups of G/N. Explicitly,*

$$\begin{aligned}A \leq G &\mapsto q(A) \leq G/N, \quad \textit{and}\\ X \leq G/N &\mapsto q^{-1}(X) \leq G\end{aligned}$$

Moreover, this bijection satisfies

1. *$A \leq B$ iff $q(A) \leq q(B)$, and in this case $B : A = q(B) : q(A)$.*

2. *$q(A \cap B) = q(A) \cap q(B)$.*

3. *$A \lhd B$ iff $q(A) \lhd q(B)$.*

Proof. Exercise. □

1.6 Symmetric Groups

$$|S_n| = n!$$

Notation for elements of S_n: Consider $\sigma \in S_6$ given by:

$$\begin{aligned}
\sigma(1) &= 2 \\
\sigma(2) &= 4 \\
\sigma(3) &= 5 \\
\sigma(4) &= 6 \\
\sigma(5) &= 3 \\
\sigma(6) &= 1
\end{aligned}$$

Mapping Notation:

$$\sigma = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 6 & 3 & 1 \end{matrix}$$

Cycle Notation:

$$\sigma = (1\ 2\ 4\ 6)(3\ 5)$$

Usually omit cycles of length one. eg. $\tau = (1\ 4\ 3)$ means $(1\ 4\ 3)(2)(5)(6)$.

The group operation on S_n is $*$ given by

$$\sigma * \tau = \tau \circ \sigma$$

Note: Dummit and Foote use the opposite convention: $\sigma_\vartriangle\tau = \sigma \circ \tau$. However, the results are isomorphic; $(S_n, *) \cong (S_n, \vartriangle)$.

Notation: S_X := permutations of X with $f * g = g \circ f$.

S'_X := permutations of X with $f * g = f \circ g$.

$$\begin{aligned}
\sigma\tau &= ((1\ 2\ 4\ 6)(3\ 5))(1\ 4\ 3) = (1\ 2\ 3\ 5)(4\ 6) \\
\tau\sigma &= (1\ 4\ 3)((1\ 2\ 4\ 6)(3\ 5)) = (1\ 6)(2\ 4\ 5\ 6)
\end{aligned}$$

So S_n is not abelian.

Note: There is an ambiguity in the cycle notation: $(1\ 2\ 4\ 6)(3\ 5)$ could mean either σ or $(1\ 2\ 4\ 6) * (3\ 5)$. This is not important because these are equal.

1.6.1 Conjugation in S_n

Example 1.6.1. *Let* $\sigma = (1\ 2\ 3)(4\ 5), \tau = (2\ 5)$. *Then*

$$\tau\sigma\tau^{-1} = (2\ 5)(1\ 2\ 3)(4\ 5)(2\ 5) = (1\ 5\ 3)(4\ 2).$$

This is obtained from σ *by switching* 2 *and* 5 *(in the cycle notation).*

Proposition 1.6.2. *Let* $\sigma, \tau \in S_n$, *with*

$$\sigma = (a_1^{(1)}\ \cdots\ a_1^{(r_1)})\cdots(a_n^{(1)}\ \cdots\ a_n^{(r_n)}).$$

Then

$$\tau\sigma\tau^{-1} = (\tau^{-1}(a_1^{(1)})\ \cdots\ \tau^{-1}(a_1^{(r_1)}))\cdots(\tau^{-1}(a_n^{(1)})\ \cdots\ \tau^{-1}(a_n^{(r_n)})).$$

Proof. In general, $(\tau\sigma\tau^{-1})(j) = \tau^{-1}(\sigma(\tau(j)))$. So

$$(\tau\sigma\tau^{-1})(\tau^{-1}a_1^{(1)}) = \tau^{-1}(\sigma(\tau(\tau^{-1}a_1^{(1)}))) = \tau^{-1}(\sigma(a_1^{(1)})) = \tau^{-1}a_1^{(2)}$$

etc. □

Notice that $\tau\sigma\tau^{-1}$ has the same cycle type as σ.

Corollary 1.6.3. σ *is conjugate to* σ' $\iff$ σ *and* σ' *have the same cycle type.*

Proof. Above shows that any conjugate of σ has the same cycle type as σ. Conversely, suppose that σ, σ' have the same cycle type. Let

$$\sigma = (a_1^{(1)}\ \cdots\ a_1^{(r_1)})\cdots(a_n^{(1)}\ \cdots\ a_n^{(r_n)})$$
$$\sigma' = (a_1^{(1)\prime}\ \cdots\ a_1^{(r_1)\prime})\cdots(a_n^{(1)\prime}\ \cdots\ a_n^{(r_n)\prime})$$

Choose $\tau \in S_n$ such that $\tau^{-1}(a_i^{(j)}) = a_i^{(j)\prime}$. Then $\sigma' = \tau\sigma\tau^{-1}$. □

1.6.2 The Alternating Group

Define the polynomial Δ by

$$\Delta(x_1, \ldots, x_n) = \prod_{i<j}(x_i - x_j)$$

For $\sigma \in S_n$, let

$$\sigma(\Delta)(x_1, \ldots, x_n) = \Delta(x_\sigma(1), \ldots, x_\sigma(n)).$$

Here, all the same factors appear, but with some signs reversed.
$\therefore \sigma\Delta = \pm\Delta$.

Define $\epsilon : S_n \mapsto \{1, -1\}$ by

$$\epsilon(\sigma) = \begin{cases} 1 & \text{if } \sigma\Delta = \Delta \\ -1 & \text{if } \sigma\Delta = -\Delta \end{cases}.$$

$\{1, -1\}$ is a group under multiplication ($\cong C_2$), and ϵ is a group homomorphism.
Set $A_n := \ker \epsilon \lhd S_n$. This is the **alternating group**.

Proposition 1.6.4. *Let $\gamma = (p\ q) \in S_n$ be a transposition (ie. 2-cycle). Then $\gamma \notin A_n$ (ie. $\gamma\Delta = -\Delta$).*

Proof. Say $p < q$.

$$\begin{aligned} \Delta &= \prod_{i<j}(x_i - x_j) \\ &= (x_p - x_q)\Big(\prod_{i<p}(x_i - x_p)\Big)\Big(\prod_{i>p}(x_p - x_i)\Big)\Big(\prod_{i<q}(x_i - x_q)\Big)\Big(\prod_{i>q}(x_q - x_i)\Big)\Big(\prod_{\substack{i<j \\ i \neq p,q \\ j \neq p,q}}(x_i - x_j)\Big) \end{aligned}$$

By applying γ to Δ:

- $(x_p - x_q)$ becomes $(x_q - x_p) = -(x_p - x_q)$,
- The factors $(\prod_{i<p}(x_i - x_p))$ and $(\prod_{i<q}(x_i - x_q))$ switch,
- The factors $(\prod_{i>p}(x_p - x_i))$ and $(\prod_{i>q}(x_q - x_i))$ switch, and
- The factor

  $$\Big(\prod_{\substack{i<j \\ i \neq p,q \\ j \neq p,q}}(x_i - x_j)\Big)$$

  is unchanged.

Thus, $\gamma\Delta = -\Delta$. ◻

Any permutation can be written (in many ways) as a product of transpositions.

Corollary 1.6.5. *$\sigma \in A_n \iff \sigma$ is the product of an even number of transpositions.*

1.7 Group Actions

Theorem 1.7.1 (Lagrange's Theorem)**.** *Let G be finite, $H \leq G$. Then $|H|$ divides $|G|$, and*

$$G : H := \frac{|G|}{|H|} = \#\text{ of left cosets of } H \text{ in } G = \#\text{ of right cosets of } H \text{ in } G.$$

*($G : H$ is called the **index** of H in G).*

Proof. Define the equivalence relation $\sim$ by $g \sim g' \iff gH = g'H$. For $g \in G$, $|H| = |gH|$ (because the map $x \mapsto gx$ is a bijection). Hence, $\sim$ partitions G into equivalence classes (cosets of H), each containing $|H|$ elements. ie.

$$\begin{aligned} |G| &= (\text{number of equiv. classes}) \times (\text{number of elts. per equiv. class}) \\ &= (\text{number of left cosets}) \times |H| \end{aligned}$$

Similarly, $|G| = (\text{number of right cosets}) \times |H|$. □

Corollary 1.7.2. *If $H \triangleleft G$ then $|G/H| = |G|/|H|$.*

Corollary 1.7.3. *For $x \in G$, $|x|$ divides $|G|$.*

Proof. Set $H = \langle x \rangle$. Then $|x| = |H| \,\Big|\, |G|$. □

Corollary 1.7.4. *If $|G| = p$, a prime number, then $G \cong C_p$.*

Proof. Let $x \in G$, $x \neq e$. Then $|x| = p$, so $G = \langle x \rangle \cong C_p(x)$. □

Definition 1.7.5. *A **left action** of a group G on a set X consists of an operation*

$$\begin{aligned} G \times X &\mapsto X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

such that:

1. $(gh) \cdot x = g \cdot (h \cdot x) \quad \forall g, h \in G, x \in X$*, and*
2. $e.x = x \quad \forall x \in X$.

Equivalently, an action of G on X is a group homomorphism $G \mapsto S'_X$.

Example 1.7.6.
1. $\mathbb{F}$ *a field,* $G = GL_n(\mathbb{F}), X = \mathbb{F}^n$.
   G acts on X by matrix multiplication, $A \cdot x = Ax$.

2. *G any group, $X = G$.*
   G acts by left multiplication on X, ie. $g \cdot x = gx$.

3. *G a group, $N \triangleleft G$.*
   G acts by conjugation on N, ie. $g \cdot x = gxg^{-1}$.

$$(gh) \cdot x = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = g(h \cdot x)g^{-1} = g \cdot (h \cdot x).$$

   In this example, the image of $G \mapsto S'_X$ lies in $\mathrm{Aut}(N)$*, ie.*

$$g \cdot (xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = (g \cdot x)(g \cdot y).$$

   Note special case where $N = G$.

Similarly, we may define a right action (it is a group homomorphism $G \mapsto S_X$). Given a right action $\odot$ of G on X, can define a left action of G on X by

$$g \cdot x := x \cdot g^{-1}.$$

Example 1.7.7. *$G = S_n, X = \{1, \ldots, n\}$. Then*

$$X \times G \mapsto X \text{ by } j \cdot \sigma = \sigma(j)$$

yields a right action of G on X, ie.

$$j \cdot (\sigma\tau) = (\sigma\tau)(j) = (\tau \circ \sigma)(j) = \tau(\sigma(j)) = (j \cdot \sigma) \cdot \tau.$$

$\therefore$ Define left action $G \times X \mapsto X$ by $\sigma \cdot j := j \cdot \sigma^{-1} = \sigma^{-1}(j)$.

Definition 1.7.8. *Let $G \times X \mapsto X$ be a (left) action of G on X. Let $x \in X$. The* ***orbit*** *of x is*

$$\mathrm{Orb}(x) := \{g \cdot x \mid g \in G\} \subset X.$$

The ***stabilizer*** *of x is*

$$\mathrm{Stab}(x) := \{g \in G \mid g \cdot x = x\} \subset G.$$

Proposition 1.7.9. $\mathrm{Stab}(x) \leq G$.

Proposition 1.7.10. $\mathrm{Orb}(x) = \mathrm{Orb}(y) \iff y \in \mathrm{Orb}(x)$.

Proof.

$\Rightarrow$ Suppose $\mathrm{Orb}(x) = \mathrm{Orb}(y)$. Then

$$y = e \cdot y \in \mathrm{Orb}(y) = \mathrm{Orb}(x).$$

$\Leftarrow$ Suppose $y \in \text{Orb}(x)$. Write $y = g \cdot x$, for some $g \in G$.
$\therefore g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = g^{-1}g \cdot x = e \cdot x = x$ and thus $x \in \text{Orb}(y)$.

If $z \in \text{Orb}(y)$ then $z = g' \cdot y = g' \cdot (g \cdot x) = (gg') \cdot x$ so $z \in \text{Orb}(x)$. Hence $\text{Orb}(x) \subset \text{Orb}(y)$, and similarly, $\text{Orb}(y) \subset \text{Orb}(x)$.

$\square$

Corollary 1.7.11. *Given an action of G on X, the relation $x \sim y \iff \text{Orb}(x) = \text{Orb}(y)$ is an equivalence relation.*

Theorem 1.7.12. *Let G be a finite group. Let $G \times X \mapsto X$ be an action of G on X. Then for $x \in X$,*

$$|\text{Orb}(x)|\,|\text{Stab}(x)| = |G|.$$

Note: Lagrange's Theorem is a special case. ie. $H \leq G$, $X = \{\text{left cosets of } H\}$.

$$G \times X \mapsto X \text{ by } g \cdot C = gC$$

defines a left action. Set $x = H$.

Proof.

$$\frac{|G|}{|\text{Stab}(X)|} = G : \text{Stab}(X) = \#\text{ of left cosets of Stab}(X) \text{ in } G$$

Define

$$\begin{aligned} \theta : \{\text{left cosets of Stab}(X) = H\} &\mapsto \text{Orb}(x) \\ gH &\mapsto g \cdot x \end{aligned}$$

1. θ is well-defined:
   Suppose $gH = g'H$. Then $g = g'h$ for some $h \in H$. Hence,

   $$g \cdot x = (g'h) \cdot x = g' \cdot (h \cdot x) = g' \cdot x, \quad \text{since } h \in \text{Stab}(x).$$

2. θ is surjective:
   If $y \in \text{Orb}(x)$ then $y = g \cdot x$, for some $g \in G$. Thus $y = \theta(gH)$.

3. θ is injective:
   Suppose $\theta(gH) = \theta(g'H)$. Then $g \cdot x = g' \cdot x$. Hence,

   $$x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g' \cdot x) = (g^{-1}g') \cdot x.$$

   $\therefore g^{-1}g' \in H$, ie. $g' = gh$ for some $h \in H$. Thus $g'H = gH$.

$\therefore \theta$ is a bijection and the theorem follows. $\square$

Corollary 1.7.13. *Let G be a finite group acting on a finite set X. Then*

$$|X| = \sum \frac{|G|}{|\mathrm{Stab}(x)|},$$

where the sum is taken over one element from each orbit.

Proof. The equivalence relation $x \sim y \iff \mathrm{Orb}(x) = \mathrm{Orb}(y)$ partitions X into disjoint subsets. So

$$\begin{aligned} |X| &= \sum |\mathrm{Orb}(x)|, \quad \text{summed over one element from each orbit} \\ &= \sum \frac{|G|}{|\mathrm{Stab}(x)|} \end{aligned}$$

$\square$

Consider the action of G on itself by conjugation. ie. $X = G$ and $g \cdot x = gxg^{-1}$. Then

$$\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\} = \{g \in G \mid gxg^{-1} = x\} = \mathrm{C}_G(x).$$

Corollary 1.7.14. *Class Formula:*

$$|G| = \sum \frac{|G|}{|\mathrm{C}_G(x)|},$$

summed over one element from each conjugacy class.

Corollary 1.7.15. *Let p be prime and let G be a p-group (ie. $|G|$ is a power of p). Then $\mathrm{Z}(G) \neq \{e\}$.*

Proof. $\mathrm{C}_G(e) = G$. By the class formula,

$$\begin{aligned} |G| &= \sum_{\text{all conj. classes}} \frac{|G|}{|\mathrm{C}_G(x)|} \\ &= \frac{|G|}{|\mathrm{C}_G(e)|} + \sum_{\substack{\text{remaining conj.} \\ \text{classes}}} \frac{|G|}{|\mathrm{C}_G(x)|} \\ \therefore\ p^n &= 1 + \sum_{\substack{\text{remaining conj.} \\ \text{classes}}} \frac{|G|}{|\mathrm{C}_G(x)|} \end{aligned}$$

$\therefore \exists x \neq e$ such that $\frac{|G|}{|\mathrm{C}_G(x)|}$ is not divisible by p. Since $|G| = p^n$, this can happen only when $|\mathrm{C}_G(x)| = p^n$, ie. when $\mathrm{C}_G(X) = G$. ie. $\exists e \neq x \in G$ such that $\mathrm{C}_G(x) = G$, ie. $x \in \mathrm{Z}(G)$. $\square$

Corollary 1.7.16. *If* $|G| = p^2$ *where* p *is prime then* G *is abelian.*

Proof. Let $x \neq e$ such that $x \in Z(G)$. If $G = \langle x \rangle$ then G is abelian. Otherwise, $|x| = p$, and since $x \in Z(G)$, $\langle x \rangle \triangleleft G$. So, $\exists y \in G$ such that $\bar{y}$ generates $G/\langle x \rangle \cong C_p$. Then x and y generate G, and since $x \in Z(G)$, $x \leftrightarrow y$. Hence G is abelian. $\square$

1.8 Semi Direct Products

Let H, K be subgroups of G. Define $\mu : H \times K \mapsto G$ by $\mu(h, k) = hk$.

Proposition 1.8.1. *If $H \cap K = \{e\}$ then μ is injective.*

Proof. Suppose $hk = h'k'$. Then

$$(h')^{-1}h = k'k^{-1} \in H \cap K = \{e\}$$

so $h'^{-1} = e = k'k^{-1}$. ie. $h = h'$ and $k = k'$. □

Assuming (for the rest of this section) that $H \cap K = \{e\}$, the above says

$$\mu : H \times K \mapsto HK \subset G$$

is a bijection. We wish to compare $H \times K$ to HK (which, in general, may not be a subgroup of G). Suppose that $H \triangleleft G$. Then $HK = KH$ is a subgroup of G, but is not necessarily isomorphic to $H \times K$. Besides $H \times K$, what other possibilities are there for HK?

Suppose $g = hk$ and $g' = h'k'$ lie in HK. Then

$$gg' = hkh'k' = hkh'k^{-1}kk' = h''k''$$

where $h'' = h(kh'k^{-1}) \in H$ and $k'' = kk' \in K$.

ie., Labelling elements of HK by the corresponding element in $H \times K$, the group operation in HK can be written

$$(h, k)(h', k') = (hk \cdot h', kk')$$

where $k \cdot h' := kh'k^{-1}$ (the restriction to K of the conjugation action of G on the normal subgroup H). Recall that this action satisfies $k \cdot (h_1h_2) = (k \cdot h_1)(k \cdot h_2)$, ie. it is a homomorphism into $\mathrm{Aut}(H)$.

Reverse the process:

Definition 1.8.2. *Given groups H, K together with a group homomorphism $\phi : K \mapsto \mathrm{Aut}(H)$, (an action of K on H – denote $k \cdot h = \phi(k)(h)$), the* ***semidirect product*** *$H \rtimes K$ is the set $H \times K$ with the binary operation*

$$(h, k)(h', k') := (h(k \cdot h'), kk').$$

Proposition 1.8.3. *$H \rtimes K$ forms a group.*

Proof.

$$\begin{aligned}
((h,k)(h',k'))(h'',k'') &= (h(k\cdot h'), kk')(h'',k'') \\
&= (h(k\cdot h')(kk'\cdot h''), kk'k''), \quad \text{and} \\
(h,k)((h',k')(h'',k'')) &= (h,k)(h'(k'\cdot h''), k'k'') \\
&= (h(k\cdot(h'(k'\cdot h''))), kk'k'').
\end{aligned}$$

However, since $\mathrm{Im}\phi \subset \mathrm{Aut}(H)$,

$$k\cdot(h'(k'\cdot h'')) = (k\cdot h')(k\cdot(k'\cdot h'')) = (k\cdot h')(kk'\cdot h'').$$

$\therefore ((h,k)(h',k'))(h'',k'') = (h,k)((h',k')(h'',k''))$.

$$\begin{aligned}
(e,e)(h',k') &= (e(e\cdot h'), ek') = (eh', ek') = (h',k'), \quad \text{and} \\
(h,k)(e,e) &= (h(k\cdot e), ke) = (he, ke) = (h,k).
\end{aligned}$$

(Here, $k\cdot e = e$ since $\mathrm{Im}\phi \subset \mathrm{Aut}(H)$.) Hence (e,e) is the identity.

$$\begin{aligned}
(h,k)(k^{-1}\cdot h^{-1}, k^{-1}) &= (h(k\cdot(k^{-1}\cdot h^{-1})), kk^{-1}) \\
&= (h((kk^{-1})\cdot h^{-1}), kk^{-1}) \\
&= (h(e\cdot h^{-1}), kk^{-1}) \\
&= (hh^{-1}, kk^{-1}) \\
&= (e,e), \quad \text{and} \\
(k^{-1}\cdot h^{-1}, k^{-1})(h,k) &= ((k^{-1}\cdot h^{-1})(k^{-1}\cdot h), k^{-1}k) \\
&= (k^{-1}\cdot(h^{-1}h), k^{-1}k), \quad \text{since } \mathrm{Im}\phi \subset \mathrm{Aut}(H) \\
&= (k^{-1}\cdot e, e) \\
&= (e,e).
\end{aligned}$$

Hence $(h,k)^{-1} = (k^{-1}\cdot h^{-1}, k^{-1})$. □

Define

$$\begin{aligned}
i_H : H &\mapsto H \rtimes K \\
h &\mapsto (h,e), \quad \text{and} \\
i_K : K &\mapsto H \rtimes K \\
k &\mapsto (e,k)
\end{aligned}$$

Proposition 1.8.4. *i_H and i_K are (injective) group homomorphisms.*

Proof.

$$(h,e)(h',e) = (h(e \cdot h'), ee) = (hh', e)$$
$$(e,k)(e,k') = (e(k \cdot e), kk') = (ee, kk') = (e, kk')$$

□

Using i_H and i_K, regard H and K as subgroups of $H \rtimes K$.

$$\text{ie. } H \cong i_H(H) = \{(h,e)\} \leq H \rtimes K$$
$$K \cong i_K(K) = \{(e,k)\} \leq H \rtimes K$$

Proposition 1.8.5. *$H \lhd (H \rtimes K)$ and $(H \rtimes K)/H \cong K$.*

Proof. Define $\phi : H \rtimes K \twoheadrightarrow K$ by $\phi(h,k) = k$. Then

$$\phi((h,k)(h',k')) = \phi(h(k \cdot h'), kk') = kk'$$

so ϕ is a group homomorphism.

$$\ker \phi = \{(h,e) \in H \rtimes K\} = i_H(H) \cong H.$$

□

Returning to the motivating example, $H \lhd G, K \leq G, H \cap K = \{e\}$, and by construction,

$$HK \cong H \rtimes K.$$

Proposition 1.8.6. *If both $H \lhd G$ and $K \lhd G$ with $H \cap K = \{e\}$ then $\mu : H \times K \mapsto HK$ is an isomorphism.*

Proof. For $h \in H, k \in K$,

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K, \quad \text{and}$$
$$hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$$

So $hkh^{-1}k^{-1} \in H \cap K = \{e\}$.

$$\text{ie. } hk = kh \quad \forall h \in H, k \in K.$$

Hence

$$\mu(h,k)\mu(h',k') = hkh'k' = hh'kk' = \mu(hh',kk') = \mu((h,k)(h',k')).$$

$\therefore$ μ is a homomorphisms, so $\mu : H \times K \xmapsto{\cong} HK$. □

Proposition 1.8.7. *Let H, K be groups and let $\phi : K \mapsto \mathrm{Aut}(H)$. TFAE:*

1. *$H \times K \cong H \rtimes K$.*
2. *ϕ is the trivial homomorphism.*
3. *$K \lhd (H \rtimes K)$.*

Proof.
$1 \Rightarrow 2$:
$$\forall h, h' \in H, k, k' \in K, \quad (hh', kk') = (h, k)(h', k') = (h(k \cdot h'), kk')$$
$\therefore \phi(k)(h') = k \cdot h' = h' \quad \forall h'$, ie. $\phi(k) = 1_H$.

$2 \Rightarrow 3$: Since H, K generate $H \rtimes K$, it suffices to check $hKh^{-1} \subset K, \ \forall h \in H$. Note that
$$(h, e)^{-1} = (h^{-1}, e),$$
so
$$\begin{aligned}(h, e)(e, k)(h^{-1}, e) &= (h(e \cdot e), ek)(h^{-1}, e) \\ &= (h, k)(h^{-1}, e) \\ &= (h(k \cdot h^{-1}), ke) \\ &= (hh^{-1}, ke), \quad \text{by 2} \\ &= (e, k) \in K\end{aligned}$$

$3 \Rightarrow 1$: This is the previous proposition. □

In particular, this proposition says that if G has normal subgroups H, K such that $H \cap K = \{e\}$ and $HK = G$ then $G \cong H \times K$.

Theorem 1.8.8. *Let $\phi : G \mapsto K$ be a group homomorphism. Suppose $\exists$ a group homomorphism $s : K \mapsto G$ such that $\phi s = 1_K$. (s is called a* ***section*** *or a* ***right splitting*** *of ϕ.) Then*
$$G \cong (\ker \phi) \rtimes K$$

Proof. Observe that existence of a function $s : K \mapsto G$ such that $\phi s = 1_K$ implies that ϕ is onto and s is injective. Let $H = \ker \phi$. Set
$$\tilde{K} = \mathrm{Im} s \xleftarrow{\cong} s\, K.$$

Then
$$(\ker \phi) \rtimes K \cong H \rtimes \tilde{K} \cong H\tilde{K} \leq G$$

so it suffices to show $H\tilde{K} = G$.

Given $g \in G$, let $k = \phi(g) \in K$ and let

$$\tilde{k} = s(k) = s\phi(g) \in \tilde{K}.$$

Then

$$\phi(\tilde{k}) = \phi s\phi(g) = \phi(g),$$

since $\phi s = 1_K$. Hence $g\tilde{k}^{-1} \in \ker\phi = H$, and so $g \in H\tilde{K}$. Thus $G = H\tilde{K}$. $\square$

A right splitting of ϕ does not make G a product. In contrast, a left splitting does imply that G is a product:

Theorem 1.8.9. *Let $H \lhd G$. Let $i : H \mapsto G$ be the inclusion map. Suppose $\exists$ a group homomorphism $r : G \mapsto H$ such that $ri = 1_H$. Then*

$$G \cong H \times G/H.$$

Proof. Define $\theta : G \mapsto H \times (G/H)$ by

$$\theta(g) = (rg, qg)$$

where $q : G \twoheadrightarrow G/H$ is the quotient projection $g \mapsto gH$. Then θ is a homomorphism.

If $\theta(g) = \theta(g')$ then $r(g) = r(g')$ and $gH = g'H$, so let $g' = gh$ for some $h \in H$. Hence

$$r(g) = r(g') = r(g)r(h),$$

so

$$e = r(h) = ri(h) = h.$$

$\therefore g' = gh = ge = g$. Thus θ is injective.

To show θ is surjective, it suffices to show $H \times \{e\} \subset \mathrm{Im}\theta$ and $\{e\} \times (G/H) \subset \mathrm{Im}\theta$, since these generate $H \times (G/H)$.

Given $h \in H$,

$$\theta(h) = (r(h), hH) = (h, e).$$

Given $q(g) = gH \in G/H$, let $h = r(g)$ and set $g' = h^{-1}g$. Then

$$\begin{aligned}\theta(g') &= (r(h^{-1}g), q(h^{-1}g)) \\ &= (r(h^{-1})r(g), q(g)) \\ &= (h^{-1}h, q(g)) \\ &= (e, q(g))\end{aligned}$$

So θ is onto. $\square$

Example 1.8.10. *Use* $\phi = \epsilon : S_3 \mapsto C_2$. *Then* $\ker\phi \cong A_3$. *Let*

$$\begin{aligned} s : C_2 \mapsto S_3 \quad &\textit{by} \\ s(1) &= e \\ s(-1) &= (1\ 2) \end{aligned}$$

s is a right splitting. Thus $S_3 \cong A_3 \rtimes C_2$.

1.9 Sylow Theorems

Throughout this section, p denotes a prime and G is a finite group.

Suppose $|G| = n$. If $H \leq G$ then by Lagrange, $|H| \,\Big|\, n$. However, the converse is false, eg. if $G = S_5$ then $n = 120$, but G has no subgroups of order $15, 30$, or 40. However, $\exists$ a partial converse:

Theorem 1.9.1 ((First) Sylow Theorem)**.** *If $p^t \,\Big|\, |G|$ then $\exists H \leq G$ such that $|H| = p^t$.*

Proof. Write $|G| = mp^t$. Find $r \geq 0$ such that $p^r \mid m$ but $p^{r+1} \nmid m$.

Lemma 1.9.2. *$p^r \,\Big|\, \binom{mp^t}{p^t}$ but $p^{r+1} \nmid \binom{mp^t}{p^t}$.*

Proof.

$$\binom{mp^t}{p^t} = \frac{(mp^t)(mp^t - 1)\cdots(mp^t - p^t + 1)}{(p^t)(p^t - 1)\cdots 3 \cdot 2 \cdot 1}$$

If $0 < j < p^t$ then

$$\begin{aligned} \#\text{ of times } p \text{ divides } p^t - j &= \#\text{ of times } p \text{ divides } j \\ &= \#\text{ of times } p \text{ divides } mp^t - j \end{aligned}$$

$\therefore$ Powers of p cancel except for those in the factor m. $\square$

Proof of Theorem continued. Let $\mathcal{S} = \{S \subset G \mid |S| = p^t\}$. Define right action

$$\mathcal{S} \times G \mapsto \mathcal{S} \quad \text{by} \quad S \cdot g = Sg.$$

$\mathcal{S}$ has $\binom{mp^t}{p^t}$ elements, so there exists an orbit $X = \{S_1, S_2, \ldots, S_k\}$ (of size k) such that $p^{r+1} \nmid k$. (If p^{r+1} divided the number of elements in each orbit then p^{r+1} would divide $|\mathcal{S}|$).

Orb$(S_1) = X$ by definition. Set $H := \text{Stab}(S_1) \leq G$. Then

$$|H| = \frac{|G|}{|X|} = \frac{mp^t}{k} = \left(\frac{m}{k}\right)p^t.$$

By construction, $p^{r+1} \nmid k$ so p divides m at least as many times as p divides k. Thus $|H|$ is divisible by p^t, and in particular,

$$|H| \geq p^t.$$

Pick $s \in S_1$. Then $\forall h \in H$, $sh \in S_1$ but $h \neq h' \Rightarrow sh \neq sh'$. Hence

$$p^t = |S_1| \geq |H|.$$

$\therefore |H| = p^t$. $\square$

Definition 1.9.3. *Suppose $|G| = n$. Let p be a prime and let p^t be the largest power of p dividing n. Then a subgroup of G having order p^t is called a **Sylow p-subgroup** of G.*

Notation: $\mathrm{Syl}_p(G) := \{\text{Sylow } p\text{-subgroups of } G\}$.

Corollary 1.9.4 (Corollary to Sylow Theorem)**.** *$\mathrm{Syl}_p(G)$ is non-empty $\forall p$.*

Suppose $H \leq G$. Then $\forall g \in G$, $gHg^{-1} \leq G$ and

$$H \xmapsto{\cong} gHg^{-1}$$
$$x \mapsto gxg^{-1}$$

In particular, $|gHg^{-1}| = |H|$. (gHg^{-1} is called a **conjugate subgroup** of H in G.)

$$P \in \mathrm{Syl}_p(G) \Rightarrow \; gPg^{-1} \in \mathrm{Syl}_p(G) \quad \forall g \in G.$$

Pick $P \in \mathrm{Syl}_p(G)$. Let

$$X = \{\text{Sylow } p\text{-subgroups of } G \text{ which are conjugate to } P\}.$$

G acts on X by $g \cdot S = gSg^{-1}$.

If $Q \leq G$, can restrict to get an action of Q on X. For an action of Q on $\mathrm{Syl}_p(G)$, have

$$|Q| = |\mathrm{Orb}_Q(S)|\,|\mathrm{Stab}_Q(S)|.$$

Here,

$$\mathrm{Stab}_Q(S) = \{q \in Q \mid qSq^{-1} = S\} = \mathrm{N}_Q(S).$$

Lemma 1.9.5. *If Q is a p-subgroup then for any Sylow p-subgroup S,*

$$\mathrm{N}_Q(S) = S \cap Q.$$

Proof. Let $H = \mathrm{N}_Q(S)$. From the definition, $S \cap Q \subset H$. Conversely, $H \subset Q$, so it suffices to show $H \subset S$. Consider SH.

$$SH = HS \leq G, \quad \text{since } S \triangleleft H.$$

$$|SH| = \frac{|S|\,|H|}{|S \cap H|} = |S|\frac{|H|}{|S \cap H|} \geq |S|.$$

$H = \mathrm{N}_Q(S) \leq Q \Rightarrow |H|$ is a power of $p \Rightarrow |SH|$ is a power of p. But S is a Sylow p-subgroup and $S \subset SH$, so $S = SH$.

$\therefore H =\subset$. Thus $H = S \cap Q$. $\square$

Lemma 1.9.6. $|X| \equiv 1 \mod p$.

Proof. Write $X = \{P = S_1, \ldots, S_r\}$. For any Q the action of Q on X divides X into orbits:

$$|X| = \sum_{orbits} (\text{\# of elts. in that orbit}).$$

Apply this with $Q = S_1 = P$:

$$\mathrm{Stab}_P(S) = \mathrm{N}_P(S) = P \cap S.$$

$\therefore |\mathrm{Stab}_P(S)| \,\Big|\, |P|$, with equality only when $S = P$. Hence,

$$|\mathrm{Orb}_P(S)| = \frac{|P|}{|\mathrm{Stab}_P(S)|}$$

is one when $S = P$, and is divisible by p otherwise. So

$$\begin{aligned} |X| &= \sum_{\text{orbits}} (\text{\# of elts. in that orbit}) \\ &= 1 + \sum_{\substack{\text{orbits not} \\ \text{containing } P}} (\text{\# of elts. in that orbit}) \\ &\equiv 1 \mod p. \end{aligned}$$

□

Lemma 1.9.7. *If Q is a p-subgroup then $Q \subset P_j$ for some $P_j \in X$.*

Proof. Again,

$$|X| = \sum_{orbits} (\text{\# of elts. in that orbit}).$$

Unless $Q \subset P_j$ for some j then for each j, $Q \cap P_j$ will be a proper subset of Q, so that

$$|\mathrm{Orb}_Q(P_j)| = \frac{|Q|}{|\mathrm{Stab}_Q(P_j)|} \text{ is divisible by } p \quad \forall j.$$

But if $p \mid (\text{\# of elements in orbit})$ for each orbit then $p \,\Big|\, |X|$, contradicting the last lemma.
$\therefore Q \subset P_j$ for some j. □

Corollary 1.9.8. $\mathrm{Syl}_p(G) = X$.

Proof. For $S \in \mathrm{Syl}_p(G)$, $|S|$ is a power of $p \Rightarrow S \subset P_j$ for some $P_j \in X$. But $|S| = |P_j|$ since both are Sylow p-subgroups.
$\therefore S = P_j \in X$. □

Lemma 1.9.9. $|\mathrm{Syl}_p(G)| \mid |G|$.

Proof. Consider the action of G on $\mathrm{Syl}_p(G)$. Let $P \in \mathrm{Syl}_P(G)$.

$$|G| = |\mathrm{Orb}_G(P)|\,|\mathrm{Stab}_G(P)|$$

$$\mathrm{Orb}_G(P) = \{\text{subgroups of } G \text{ conjugate to } P\} = X = \mathrm{Syl}_p(G).$$

$\therefore |\mathrm{Syl}_P(G)|$ divides G. □

In summary:

Theorem 1.9.10 ((Main) Sylow Theorem)**.** *Let G be a finite group and let p be a prime.*

1. $|\mathrm{Syl}_p(G)| \equiv 1 \mod p$.
2. $|\mathrm{Syl}_p(G)| \mid |G|$.
3. *Any two Sylow p-subgroups of G are conjugate (and in particular, isomorphic).*
4. *Every p-subgroup of G is contained in some Sylow p-subgroup. In particular, every element whose order is a power of p is contained in some Sylow p-subgroup.*

Proof. Showed that if $X = \{\text{Sylow } p\text{-subgroups conjugate to } P\}$ then $\mathrm{Syl}_P(G) = X \iff 3$.
Also showed $|X| \equiv 1 \mod p \iff 1$.
Also showed: every p-subgroup of G is contained in some $S \in X \iff 4$.
Also showed $|\mathrm{Syl}_P(G)| \mid |G| \iff 2$. □

Corollary 1.9.11. *Let P be a Sylow p-subgroup of G. Then $P \lhd G \iff P$ is the unique Sylow p-subgroup.*

Proof.

$\Leftarrow$: Suppose $\exists!$ Sylow p-subgroup. Since gPg^{-1} is a Sylow p-subgroup $\forall g$,

$$gPg^{-1} = P \quad \forall G,$$

ie. $P \lhd G$.

$\Rightarrow$: Suppose $P \lhd G$. Then the only subgroup of G conjugate to P is P. By Sylow Theorem, 3, P is the only Sylow p-subgroup.

□

Corollary 1.9.12. *Let P be a Sylow p-subgroup of G. Let $N = \mathrm{N}_G(P)$. Then*

$$\mathrm{N}_G(N) = N.$$

In particular, $N \lhd G$ iff $P \lhd G$.

Proof. Set $H := \mathrm{N}_G(N)$. Then $\forall h \in H$, $hPh^{-1} \subset N$ and $|hPh^{-1}| = |P|$, so hPh^{-1} is a Sylow p-subgroup of G. But then hPh^{-1} is also a Sylow p-subgroup of N. However, $P \lhd N$, so P is the unique Sylow p-subgroup of N.

$\therefore hPh^{-1} = P$, so $h \in \mathrm{N}_G(P) = N$. Hence $H \subset N$, so $H = N$.

In particular, if $N \lhd G$ then $N = H = G$ so $P \lhd G$. □

1.10 Applications of Sylow's Theorem

1. Suppose $|G| = 15$. Then

$$\left.\begin{array}{r}|\mathrm{Syl}_5(G)| \equiv 1 \mod 5\\ |\mathrm{Syl}_5(G)| \,\big|\, 15\end{array}\right. \Rightarrow |\mathrm{Syl}_5(G)| = 1,$$

$\therefore$ $\exists!$ element of $\mathrm{Syl}_5(G)$. Let H be the unique Sylow 5-subgroup, so $H \triangleleft G$. Similarly,

$$\left.\begin{array}{r}|\mathrm{Syl}_3(G)| \equiv 1 \mod 3\\ |\mathrm{Syl}_3(G)| \,\big|\, 15\end{array}\right. \Rightarrow |\mathrm{Syl}_3(G)| = 1,$$

so $\exists!$ Sylow 3-subgroup K, and so $K \triangleleft G$.

Pick generators $h \in H, k \in K$; $|h| = 5, |k| = 3$. H, K are normal $\Rightarrow hk = kh$, so $|hk| = 15$. Hence, G has an element of order 15, so $G \cong C_{15}$.

2. Suppose $|G| = 10$.

$$\left.\begin{array}{r}|\mathrm{Syl}_5(G)| \equiv 1 \mod 5\\ |\mathrm{Syl}_5(G)| \,\big|\, 10\end{array}\right. \Rightarrow |\mathrm{Syl}_5(G)| = 1.$$

Let H be the unique Sylow 5-subgroup. Then $H \triangleleft G$. Pick a generator h.

$$\left.\begin{array}{r}|\mathrm{Syl}_2(G)| \equiv 1 \mod 2\\ |\mathrm{Syl}_2(G)| \,\big|\, 10\end{array}\right. \Rightarrow |\mathrm{Syl}_2(G)| = 1 \text{ or } 5.$$

Case I: $|\mathrm{Syl}_2(G)| = 1$. Then $G \cong C_{10}$, using argument above.

Case II: $|\mathrm{Syl}_2(G)| = 5$.
Let K be a Sylow 2-subgroup; $K = \{e, k\}$. If $hk = kh$ then $|hk| = 10$ and we would be in Case I. Hence,

$$hkh^{-1} = k_2 = \text{generator of a different Sylow 2-subgroup.}$$

Similarly, $h^2kh^{-2}, h^3kh^{-3}, h^4kh^{-4}$ must be the generators of the other Sylow 2-subgroups. (Again, if $h^ikh^{-i} = h^jkh^{-j}$ for $i \neq j$ then $h^{j-i}k = kh^{j-i}$ and we would be in Case I.)

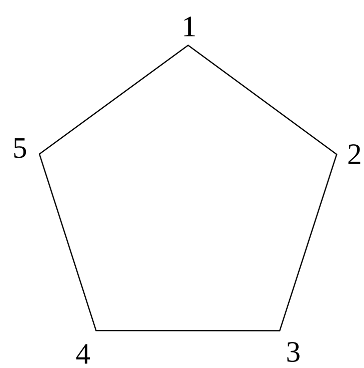
$\therefore$ Can list the ten elements of G:

$$\begin{array}{cc} e & k\\ h & hkh^{-1}\\ h^2 & h^2kh^{-2}\\ h^3 & h^3kh^{-3}\\ h^4 & h^4kh^{-4}\end{array}$$

From this, we can construct the group table. eg. what is hk?
Well, $hk \neq h^j$ for any j, so hk has order 2.

$$\begin{aligned}
\therefore\ hkhk &= e \\
hkh &= k^{-1} = k \\
\therefore\ hk &= h(hkh) \\
&= h^2kh \\
&= h^2(hkh)h \\
&= h^3kh^2 \\
&= h^3kh^{-3}.
\end{aligned}$$

This group must be D_{10}.



$$\begin{aligned}
h &\mapsto (1\ 2\ 3\ 4\ 5) \\
k &\mapsto (2\ 5)(3\ 4)
\end{aligned}$$

Conclusion: If $|G| = 10$ then $G \cong C_{10}$ or $G \cong D_{10}$.
In passing: note the existence of an element k of order 2 in D_{10} gives a splitting

$$D_{10} \underset{s}{\rightleftarrows} D_{10}/H \cong C_2$$

where if $C_2 = \{e, x\}$ then $s(x) = k$. Thus

$$D_{10} \cong H \rtimes C_2 = C_5 \rtimes C_2.$$

The corresponding homomorphism $\phi : C_2 \mapsto \mathrm{Aut}(C_5)$ is given by $k \cdot h = h^{-1} = h^4$. ($\mathrm{Aut}(C_5) \cong C_4$ is generated by the map τ, taking h to h^2. The only element of order 2 in $\mathrm{Aut}(C_5)$ is $\tau \circ \tau$, which is $h \mapsto h^4$.)

3. Suppose $|G| = 12$. Then

$$|\mathrm{Syl}_2(G)| = 1 \text{ or } 3,$$
$$|\mathrm{Syl}_3(G)| = 1 \text{ or } 4.$$

Case I: $|\mathrm{Syl}_2(G)| = 3$ and $|\mathrm{Syl}_3(G)| = 4$.
Since two distinct groups of order 3 intersect only in the identity, and each Sylow 3-subgroup has 2 elements of order 3, G has $4 \times 2 = 8$ elements of order 3. The remaining 4 elements must form a Sylow 2-subgroup.

$\therefore$ There aren't enough elements left to form any more Sylow 2-subgroups. This is a contradiction, so Case I doesn't occur.

Case II: $|\mathrm{Syl}_2(G) = 1$.
Let H be the unique Sylow 2-subgroup, so $H \lhd G$. $|H| = 4$, so either $H \cong C_4$ or $H \cong C_2 \times C_2$.

Case IIa: $H \cong C_4(\sigma)$.
Let τ be an element of some Sylow 3-subgroup, $|\tau| = 3$.

$$\begin{matrix} \tau\sigma\tau^{-1} \in H \\ |\tau\sigma\tau^{-1}| = |\sigma| = 4 \end{matrix} \;\Rightarrow\; \tau\sigma\tau^{-1} = \text{either } \sigma \text{ or } \sigma^3.$$

If $\tau\sigma\tau^{-1} = \sigma^3$ then

$$\tau\sigma^3\tau^{-1} = (\tau\sigma\tau^{-1})^3 = \sigma^9 = \sigma.$$

Moreover, $\tau^3 = e$, so

$$\sigma = \tau^3\sigma\tau^{-3} = \tau^2(\tau\sigma\tau^{-1})\tau^2 = \tau^2\sigma^3\tau^{-2} = \tau(\tau\sigma^3\tau^{-1})\tau^{-1} = \sigma^3.$$

This is a contradiction. Thus, $\tau\sigma\tau^{-1} = \sigma$.

Using the fact that τ and σ commute, $|\tau\sigma| = 12$. Thus $G \cong C_{12}$.

Equivalent way of phrasing argument that $\tau\sigma\tau^{-1} = \sigma$: Let $T = \{e, \tau, \tau^2\}$. H is normal $\Rightarrow T$ acts on H via $\tau \cdot \sigma := \tau\sigma\tau^{-1}$.

$$|\mathrm{Orb}(\sigma)|\,|\mathrm{Stab}(\sigma)| = |T| = 3.$$

σ has order 2 $\Rightarrow x \cdot \sigma$ has order 2 $\forall x \in T$. So $\mathrm{Orb}(\sigma) \subset \{\sigma, \sigma^3\}$. Since $|\mathrm{Orb}(\sigma)|$ divides 3, $\mathrm{Orb}(\sigma) = \{\sigma\}$.

$\therefore\ \tau\sigma\tau^{-1} = \sigma$.

Another rephrasing: $H \lhd G$.

$$\begin{tikzcd} G \arrow[r, shift left] & G/H \cong C_3, \arrow[l, dashed, shift left, "s"] \end{tikzcd}$$

where s takes the generator a to τ. ie. The existence of an element τ of order 3 in G gives a splitting, so

$$G \cong C_4 \rtimes_\phi C_3$$

for some $\phi : C_3 \mapsto \mathrm{Aut}(C_4)$. However, $\mathrm{Aut}(C_4) \cong C_2 = \{1_{C_4}$ and $\sigma \mapsto \sigma^3\}$. so the only homomorphism $C_3 \mapsto \mathrm{Aut}(C_4)$ is trivial.

$\therefore\ G \cong C_4 \times C_3 \cong C_{12}$.

Case IIb: $H \cong C_2 \times C_2$.

Let

$$H = \{e, \sigma_1, \sigma_2, \sigma_3\}, \quad \sigma_j^2 = e.$$

Let $T = \{e, \tau, \tau^2\}$ be some Sylow 3-subgroup.

$$\begin{tikzcd} G \arrow[r, shift left] & G/H \cong C_3, \arrow[l, dashed, shift left, "s"] \end{tikzcd}$$

and thus,

$$G \cong H \rtimes_\phi T,$$

with $\phi : T \mapsto \mathrm{Aut}(H) \cong$ permutations of $\{\sigma_1, \sigma_2, \sigma_3\} \cong S_3$. So

$$(\phi(\tau))(\sigma_1) = \tau\sigma_1\tau^{-1} = \sigma_1, \sigma_2, \text{ or } \sigma_3.$$

Case IIbi: $\tau\sigma_1\tau^{-1} = \sigma_1$. Then since the order of $\phi(\tau)$ must divide the order of τ, which is 3, $\phi(\tau) = \mathrm{id}$. Hence $\phi = \mathrm{id}$ and

$$G \cong H \times T \cong C_2 \times C_2 \times C_3.$$

Case IIIbii: $\tau\sigma_1\tau^{-1} \neq \sigma_1$.

So $\tau\sigma_1\tau^{-1} = \sigma_2$ or σ_3. By symmetry, assume $\tau\sigma_1\tau^{-1} = \sigma_2$. Then $\phi(\tau)$ must be a 3-cycle, so $\tau\sigma_2\tau^{-1} = \sigma_3$.

Elements of G:

$$\begin{array}{cccc} e & \sigma_1 & \sigma_2 & \sigma_3 \\ \tau & \tau\sigma_1 & \tau\sigma_2 & \tau\sigma_3 \\ \tau^2 & \tau^2\sigma_1 & \tau^2\sigma_2 & \tau^2\sigma_3 \end{array}$$

Each σ_j has order 2, and the elements τ, τ^2, $\tau\sigma_j$ and $\tau^2\sigma_j$ each have order 3. Multiplication is determined by $\tau\sigma_1\tau^{-1} = \sigma_2$ and $\tau\sigma_2\tau^{-1} = \sigma_3$. eg.

$$\sigma_1\tau = \tau\tau^{-1}\sigma_1\tau = \tau\tau^2\sigma_1\tau^{-2} = \tau\tau\sigma_2\tau^{-1} = \tau\sigma_3.$$

What group is this? Let T_1, T_2, T_3, T_4 be the Sylow 3-subgroups. ie.

$$\begin{aligned} T_j &= \{e, \tau\sigma_j, (\tau\sigma_j)^2\} \quad j = 1, 2, 3, \\ T_4 &= \{e, \tau, \tau^2\} \end{aligned}$$

Let $X = \{T_1, T_2, T_3, T_4\}$. Conjugation by elements of G permutes elements of X, ie. have morphism

$$\theta : G \mapsto S_X = S_4.$$

What is $\theta(\tau)$?

$$\begin{aligned} \tau T_1\tau^{-1} &= \{\tau e\tau^{-1}, \tau(\tau\sigma_1)\tau^{-1} = \tau\sigma_2, \tau(\tau\sigma_1)^2\tau^{-1}\} = T_2 \\ \tau T_2\tau^{-1} &= \{\tau e\tau^{-1}, \tau(\tau\sigma_2)\tau^{-1} = \tau\sigma_3, \quad \cdots \quad \} = T_3 \\ \tau T_3\tau^{-1} &= T_1 \\ \tau T_4\tau^{-1} &= T_4 \end{aligned}$$

ie. $\tau \overset{\theta}{\longmapsto} (1\ 2\ 3)$.
What is $\theta(\sigma_1)$? $\sigma_1 T_1\sigma_1^{-1} = ?$
Suffices to compute $\sigma_1(\tau\sigma_1)\sigma_1^{-1}$.

$$\sigma_1(\tau\sigma_1)\sigma_1^{-1} = \sigma_1\tau = \tau\sigma_3.$$

$\therefore\ \sigma_1(\tau\sigma_1)\sigma_1^{-1} = T_3$. $|\sigma_1| = 2 \Rightarrow \sigma_1 T_3\sigma_1^{-1} = T_1$. Likewise, $\sigma_1 T_4\sigma_1^{-1} = T_2$. So $\sigma_1 \mapsto (1\ 3)(2\ 4)$.
What is $\theta(\sigma_2)$?

$$\sigma_2 T_1\sigma_2^{-1} = \sigma_2\tau\sigma_1\sigma_2^{-1} = \tau\sigma_1^2\sigma_2^{-1} = \tau\sigma_2 \in T_2$$

etc., get $\sigma_2 \mapsto (1\ 2)(3\ 4)$.

$$G \cong A_4.$$

Case III: $|\mathrm{Syl}_2(G)| = 3$, so $|\mathrm{Syl}_3(G)| = 1$.
Let $T = \{e, \tau, \tau^2\}$ be the unique Sylow 3-subgroup, so $T \lhd G$. Let H be a Sylow 2-subgroup. $|H| = 4$, so $H \cong C_4$ or $C_2 \times C_2$. Then

$$H \hookrightarrow G \twoheadrightarrow G/T$$

is an isomorphism (it is an injection since $H \cap T = \{e\}$ for degree reasons, and since $|H| = 4 = |G/T|$, it is bijective). This splits $q : G \twoheadrightarrow G/T$, so

$$G \cong T \rtimes_\phi H.$$

Case IIIa: $H \cong C_2 \times C_2$.

Let $H = \{e, \sigma_1, \sigma_2, \sigma_3\}$.

$$\phi : H \mapsto \mathrm{Aut} T = \mathrm{Aut} C_3 \cong C_2.$$

If $\phi(h) = 1_T \ \forall h \in H$ then $G = T \times H$, transposing to Case II. So ϕ is non-trivial, ie. $\phi(h)(\tau) = \tau^2$ for some $h \in H$. Then

$$\ker \phi = C_2$$

so $\exists h \in H$ such that $h \neq e$ and $\phi(h) = 1_T$. $\phi(h')(\tau) = \tau^2$ for the other two non-trivial elements h' of H. By symmetry, suppose $\phi(\sigma_3) = 1_T$, ie.

$$\begin{aligned} \phi(\sigma_1)(\tau) &= \sigma_1 \tau \sigma_1^{-1} = \tau^2, \\ \phi(\sigma_2)(\tau) &= \sigma_2 \tau \sigma_2^{-1} = \tau^2, \\ \phi(\sigma_3)(\tau) &= \sigma_3 \tau \sigma_3^{-1} = \tau. \end{aligned}$$

This determines multiplication in G.

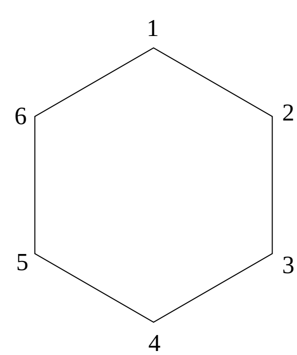
What group is this? $\sigma_3 \tau = \tau \sigma_3$, so $|\sigma_3 \tau| = |\sigma_3|\,|\tau| = 2 \cdot 3 = 6$. Set $x = \sigma_3 \tau$. Elements of G:

$$\begin{array}{cccccc} e & x & x^2 & x^3 & x^4 & x^5 \\ \sigma_1 & x\sigma_1 & x^2\sigma_1 & x^3\sigma_1 & x^4\sigma_1 & x^5\sigma_1 \end{array}$$

Multiplication of elements in this form can be derived from:

$$\sigma_1 x = \sigma_1 x \sigma_1^{-1} \sigma_1 = \sigma_1 \sigma_3 \tau \sigma_1^{-1} \sigma_1 = \sigma_3 (\sigma_1 \tau \sigma_1^{-1}) \sigma_1 = \sigma_3 \tau^2 \sigma_1 = \sigma_3^5 \tau^5 \sigma_1 = x^5 \sigma_1.$$

So $G \cong D_{12}$.



$$x \mapsto (1\ 2\ 3\ 4\ 5\ 6)$$
$$\sigma_1 \mapsto (2\ 6)(3\ 5)$$

What are the 3 Sylow 2-subgroups? One is $H = \{e, \sigma_1, \sigma_2, \sigma_3\}$. Note that

$$\sigma_3 = \sigma_3^3\tau^3 = x^3,$$
$$\sigma_2 = \sigma_3\sigma_1 = x^3\sigma_1$$

$\therefore H = \{e, \sigma_1, x^3\sigma_1, x^3\}$.

To find the others, pick $g \in G$ and compute gHg^{-1}.

$$\begin{aligned} g = x \;\Rightarrow\; gHg^{-1} &= \{e, x\sigma_1x^{-1}, xx^3\sigma_1x^{-1}, xx^3x^{-1}\} \\ &= \{e, x\sigma_1x^5, x^4\sigma_1x^5, x^3\} \\ &= \{e, x(x^5)^5\sigma_1, x^4(x^5)^5\sigma_1, x^3\} \\ &= \{e, x^{26}\sigma_1, x^{29}\sigma_1, x^3\} \\ &= \{e, x^2\sigma_1, x^5\sigma_1, x^3\}. \end{aligned}$$

The other is $\{e, x^4\sigma_1, x\sigma_1, x^3\}$.

Note that different Sylow p-subgroups can intersect non-trivially. eg. Here, x^3 is in all Sylow 2-subgroups.

Case IIIb: $H \cong C_4$.

Let $H = \{e, \sigma, \sigma^2, \sigma^3\}$. Recall

$$G \cong T \rtimes_\phi H,$$
$$T = \{e, \tau, \tau^2\},$$
$$\phi : H \cong C_4 \mapsto \mathrm{Aut}(T) \cong C_2$$

Aside from trivial ϕ (yielding $G \cong T \times H \cong C_3 \times C_4$, which is Case IIa), ϕ acts non-trivially on σ and σ^3. ie. $\sigma\tau\sigma^{-1} = \tau^2$. Elements of G are:

$$\begin{array}{cccc} e & \sigma & \sigma^2 & \sigma^3 \\ \tau & \tau\sigma & \tau\sigma^2 & \tau\sigma^3 \\ \tau^2 & \tau^2\sigma & \tau^2\sigma^2 & \tau^2\sigma^3 \end{array}$$

Multiplication is determined by $\sigma\tau\sigma^{-1} = \tau^2$ (and $\tau^3 = e, \sigma^4 = e$).

In summary, there are 5 (non-isomorphic) groups of order 12: C_{12}, $C_2 \times C_2 \times C_3$, A_4, D_{12}, and $C_3 \rtimes C_4$.

1.11 Solvable and Nilpotent Groups

Let G be a group, $A, B \subset G$.
Notation: $[A, B]$:= subgrp. of G generated by $\{[a, b] \mid a \in A, b \in B\}$. So $[G, G]$ is the commutator subgroup of G.

Inductively define:

$$\begin{aligned} G^{(0)} &:= G, \\ G^{(n)} &:= [G^{(n-1)}, G^{(n-1)}], \quad \text{and} \\ G'^{(0)} &:= G, \\ G'^{(n)} &:= [G^{(n-1)}, G]. \end{aligned}$$

Then

$$\begin{array}{cccccccccccl} G = & G^{(0)} & \geq & G^{(1)} & \geq & G^{(2)} & \geq \cdots \geq & G^{(n)} & \geq \cdots & \textbf{Derived (or commutator) series} \text{ of } G \\ & \parallel & & \parallel & & \leq & & \leq & & \\ & G'^{(0)} & \geq & G'^{(1)} & \geq & G'^{(2)} & \geq \cdots \geq & G'^{(n)} & \geq \cdots & \textbf{Lower central series} \text{ of } G \end{array}$$

Definition 1.11.1. *G is called **solvable** if $\exists N$ such that $G^{(N)} = \{e\}$. G is called **nilpotent** if $\exists N$ such that $G'^{(N)} = \{e\}$.*

Since $G^{(n)} \leq G'^{(n)}$, nilpotent $\Rightarrow$ solvable. We already showed $[G, G] \lhd G$, so $G^{(n)} \lhd G^{(n-1)}$. In fact:

Proposition 1.11.2.

1. *$G^{(n)} \lhd G$ $\forall n$. In particular, $G^{(n)} \lhd G^{(n-1)}$ (because for $A \leq B \leq G$, if $A \lhd G$ then $A \lhd B$).*

2. *$G'^{(n)} \lhd G$ $\forall n$. In particular, $G'^{(n)} \lhd G'^{(n-1)}$.*

Proof.

1. For $g \in G$ and $[a, b]$ a generator of $G^{(n)}$, where $a, b \in G^{(n-1)}$,

$$g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}] \in [G^{(n-1)}, G^{(n-1)}]$$

by induction.

2. For $g \in G$ and $[a, b]$ a generator of $G'^{(n)}$, where $a \in G'^{(n-1)}$ and $b \in G$,

$$g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}] \in [G'^{(n-1)}, G]$$

by induction.

□

Notice that $G^{(n-1)}/G^{(n)} = G_{ab}^{(n-1)}$ is abelian. Conversely:

Proposition 1.11.3. *G is solvable iff $\exists$ a finite sequence of subgroups*

$$\{e\} = H_N \lhd H_{N-1} \lhd \cdots \lhd H_0 = G$$

such that H_{n-1}/H_n is abelian for all n.

Proof. Suppose that such a sequence exists. Since H_{n-1}/H_n is abelian, $[H_{n-1}, H_{n-1}] \leq H_n$ for all n. Inductively,

$$G^{(n)} = [G^{(n-1)}, G^{(n-1)}] \leq [H_{n-1}, H_{n-1}] \leq H_n$$

so $G^{(n)} \leq H_n$ $\forall n$. Thus,

$$G^{(N)} \leq H_N = \{e\}$$

$\therefore G^{(N)} = \{e\}$. □

Lemma 1.11.4. *S_n is solvable iff $n < 5$.*

Proof.

$n = 1, 2$: S_n is abelian and thus solvable.

$n = 3$: Note that $[\sigma, \tau]$ is always an even permutation, so

$$[S_n, S_n] \leq A_n \quad \forall n.$$

When $n = 3$, $A_3 \cong C_3$ is abelian, so S_3 is solvable.

$n = 4$: Since $[S_4, S_4] \leq A_4$, in suffices to check that A_4 is solvable. Let

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Then $H \cong C_2 \times C_2$ is abelian, $H \lhd A_4$, and

$$|A_4/H| = 3,$$

so $A_4/H \cong C_3$ is abelian.

$n \geq 5$: Let $\sigma = (1\ 5\ 3)$, $\tau = (1\ 4\ 2)$. Then

$$\begin{aligned}[\sigma, \tau] &= \sigma\tau\sigma^{-1}\tau^{-1} \\ &= (1\ 5\ 3)(1\ 4\ 2)(1\ 3\ 5)(1\ 2\ 4) \\ &= (1\ 2\ 3) \in [S_n, S_n]\end{aligned}$$

Similarly, every 3-cycle is a commutator of 3-cycles, provided $n \geq 5$. Thus, $\forall k$, $A_n^{(k)}$ contains every 3-cycle.

$\therefore A_n^{(k)} \neq \{e\}\ \forall k$, so A_n is not solvable.

$\square$

Theorem 1.11.5. *Suppose $A \lhd B$. Then B is solvable $\iff$ both A and B/A are solvable. Furthermore, if $A \leq B$ and B is solvable then A is solvable (even if A is not normal in B).*

Proof. Suppose B is solvable and $A \leq B$. Then $A^{(j)} \leq B^{(j)}\ \forall j$, so $B^{(k)} = \{e\}$ for some $k \Rightarrow A^{(k)} = \{e\}$, so A is solvable.

$\Rightarrow$: Suppose now that $A \lhd B$ and let $\pi : B \mapsto B/A$ be the canonical projection. If $x \in B$ lies in B' then $\pi(x) \in (B/A)'$, and conversely, if

$$y = (\overline{u}\,\overline{v}\,\overline{u})^{-1}(\overline{v})^{-1} \in (B/A)'$$

then $y = \pi(uvu^{-1}v^{-1}) \in \pi(B')$. Hence,

$$\begin{aligned}\pi(B') &= (B/A)' \\ \pi(B^{(2)}) &= \pi(B'') = (\pi(B'))' = (B/A)'' = (B/A)^{(2)} \\ &\vdots \\ \pi(B^{(k)}) &= \cdots = (B/A)^{(k)}\end{aligned}$$

Since $\pi(B^{(k)}) = \{e\}$, $(B/A)^{(k)} = \{e\}$, whence B/A is solvable.

$\Leftarrow$: Suppose A and B/A are both solvable. If $\{e\} = (B/A)^{(k)} = \pi(B^{(k)})$ then $B^{(k)} \subset A$. Thus, $B^{(k+j)} = (B^{(k)})^{(j)} \subset A^{(j)}$. So if $A^{(m)} = \{e\}$ then $B^{(k+m)} = \{e\}$. Hence, B is solvable.

$\square$

Theorem 1.11.6. *G is finite and solvable $\Rightarrow \exists$ subgroups*

$$\{e\} = A_m \lhd A_{m-1} \lhd \cdots \lhd A_1 \lhd A_0 = G$$

such that A_j/A_{j+1} is cyclic of prime order $\forall j$.

Proof. The proceding theorem reduces the proof to the case where G is abelian, and it is clear that a finite abelian group has such a composition series. $\square$

Upper Central Series:
Given a group G, inductively define $Z_n(G)$ as follows: Set $Z_0 := \{e\}$. Having defined Z_{n-1} such that $Z_{n-1} \triangleleft G$, define Z_n as the pullback:

$$\begin{tikzcd} Z_n \arrow[r] \arrow[d] & \mathrm{Z}(G/Z_{n-1}) \arrow[d, "\triangle"] \\ G \arrow[r, two heads, "q_{n-1}"] & G/Z_{n-1} \end{tikzcd}$$

where $q_{n-1} : G \mapsto G/Z_{n-1}$ is the quotient map. ie.

$$Z_n := q_{n-1}^{-1}(\mathrm{Z}(G/Z_{n-1})).$$

$Z_n \triangleleft G$ because $\mathrm{Z}(G/Z_{n-1}) \triangleleft G/Z_{n-1}$.

$$q_{n-1}([Z_n, G]) \subset [\mathrm{Z}(G/Z_{n-1}, G/Z_{n-1}] = \{e\},$$

so $[Z_n, G] \subset \ker q_{n-1} = Z_{n-1}$.

Lemma 1.11.7. *G is nilpotent iff $Z_N(G) = G$ for some N.*

Proof.

$\Rightarrow$: Suppose $Z_N = G$.

$$G'^{(1)} = [G, G] = [Z_N, G] \le Z_{N-1}.$$

Inductively,

$$G'^{(k)} = [G'^{(k-1)}, G] \le [Z_{N-(k+1)}, G] \le Z_{N-k}.$$

$\therefore G'^{(N)} \le Z_0 = \{e\}$ so G is nilpotent.

$\Leftarrow$: Suppose $G'^{(N)} = \{e\}$. Inductively (as k decreases), assume

$$[G'^{(k)}, G] = G'^{(k+1)} \le Z_{N-k-1}.$$

Suppose $x \in G'^{(k)}$. Given $\overline{g} = q_{N-k-1}(g) \in G/Z_{N-k-1}$,

$$\begin{aligned} [q_{N-k-1}(x), \overline{g}] &= q_{N-k-1}[x, g] \\ &\in q_{N-k-1}([G'^{(k)}, G]) \\ &\subset q_{N-k-1}(Z_{N-k-1}) \\ &= \{e\}. \end{aligned}$$

$\therefore q_{N-k-1}(x)$ commutes with $\overline{g}\ \ \forall\, \overline{g} \in G/Z_{N-k-1}$ so

$$q_{N-k-1}(x) \in \mathrm{Z}(G/Z_{N-k-1}).$$

$\therefore x \in Z_{N-k}$.

Thus $G'^{(k)} \leq Z_{N-k}\ \forall k$. Therefore,

$$Z_N \geq G'^{(0)} = G$$

$\therefore Z_N = G$ as required.

$\square$

Corollary 1.11.8. *If G is a finite group then G is nilpotent iff $\forall n$, $\mathrm{Z}(G/Z_n) \neq \{e\}$ unless $G/Z_n = \{e\}$.*

Proof. If $\mathrm{Z}(G/Z_n) = \{e\}$ then $Z_{n+1} = q_{n-1}^{-1}\{e\} = Z_n$, so the series

$$Z_0 \leq Z_1 \leq \cdots Z_n \leq Z_{n+1} \leq \cdots$$

never reaches G (unless $Z_n = G$ already).

Conversely, if $\forall n$, $\mathrm{Z}(G/Z_n) \neq \{e\}$ then

$$Z_n < Z_{n+1} \quad \forall n$$

and since G is finite, eventually $Z_n = G$. $\square$

Corollary 1.11.9. *If G is a p-group then G is nilpotent.*

Lemma 1.11.10. *G is nilpotent iff $G/\mathrm{Z}(G)$ is nilpotent. More precisely, $Z_{N+1}(G) = G$ iff $Z_N(G/\mathrm{Z}(G)) = G/\mathrm{Z}(G)$.*

Proof. Set $H := G/\mathrm{Z}(G)$.

$$\begin{tikzcd}
Z_2(G) \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & \mathrm{Z}(G) = Z_1(H) \arrow[d, hook] \\
G \arrow[r, "q_1"'] & H \ = G/\mathrm{Z}(G) = G/Z_1(G)
\end{tikzcd}$$

Suppose inductively that $Z_{n-1}(G)$ is isomorphic to the pullback

$$\begin{tikzcd}
P_{n-1} \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & Z_{n-2}(H) \arrow[d] \\
G \arrow[r, two heads, "q_1"'] & H
\end{tikzcd}$$

By a property of pullbacks (Proposition 1.5.5),

$$G/Z_{n-1}(G) \cong G/P_{n-1} \cong H/Z_{n-2}(H).$$

So

$$\begin{tikzcd}
P_n \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & Z_{n-1}(H) \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & \mathrm{Z}(H/Z_{n-2}(H)) \cong \mathrm{Z}(G/Z_{n-1}(G)) \arrow[d] \\
G \arrow[r, two heads, "q_1"'] & H \arrow[r, two heads] & H/Z_{n-2}(H) \cong G/Z_{n-1}(G)
\end{tikzcd}$$

Then P_n is isomorphic to the composite pullback, which, by definition, is $Z_n(G)$. So

$$Z_n(G) \cong P_n \quad \forall n.$$

If H is nilpotent then $\exists N$ such that $Z_N(H) = H$. Then

$$\begin{tikzcd}
Z_{N+1}(G) \arrow[r] \arrow[d] \arrow[dr, phantom, "p.b."] & Z_N(H) \arrow[d] \\
G \arrow[r, two heads, "q_1"'] & H
\end{tikzcd}$$

shows $Z_{N+1} = G$.

Conversely, if $Z_{N+1}(G) = G$ for some N then the pullback shows

$$H/Z_N(H) \cong G/Z_{N+1}(G) \cong \{e\}$$

so $Z_N(H) = H$. □

Corollary 1.11.11. *G is nilpotent iff the sequence of surjections*

$$\begin{array}{ccccccccc}
Q_0 & \twoheadrightarrow & Q_1 & \twoheadrightarrow & Q_2 & \twoheadrightarrow \cdots \twoheadrightarrow & Q_n & \twoheadrightarrow & \cdots \\
\parallel & & \parallel & & \parallel & & \parallel & & \\
G & & G/\mathrm{Z}(G) & & Q_1/\mathrm{Z}(Q_1) & & Q_{n-1}/\mathrm{Z}(Q_{n-1}) & &
\end{array}$$

eventually reaches $\{e\}$. ($Q_N = \{e\}$ for some N).

Proof.

$\Rightarrow$: Q_n is nilpotent iff Q_{n+1} is nilpotent. So, if $Q_N = \{e\}$ then Q_N is nilpotent, so $Q_0 = G$ is nilpotent.

$\Leftarrow$: Suppose that G is nilpotent with $Z_N(G) = G$. Then $Z_{N-1}(Q_1) = Q_1$ and inductively, $Z_{N-k}(Q_k) = Q_k \ \forall k$. Then

$$\mathrm{Z}(Q_{N-1}) = Z_1(Q_{N-1}) = Q_{N-1}$$

so $Q_N = Q_{N-1}/\mathrm{Z}(Q_{N-1}) = \{e\}$.

$\square$

Corollary 1.11.12. *A finite product of nilpotent groups is nilpotent.*

Proof. By induction, it suffices to consider the product of two nilpotent groups, G_1 and G_2.

$$\begin{aligned} Q_1(G_1 \times G_2) &= \frac{G_1 \times G_2}{\mathrm{Z}(G_1 \times G_2)} \\ &= \frac{G_1 \times G_2}{\mathrm{Z}(G_1) \times \mathrm{Z}(G_2)} \\ &= G_1/\mathrm{Z}(G_1) \times G_2/\mathrm{Z}(G_2) \\ &= Q_1(G_1) \times Q_1(G_2) \end{aligned}$$

By iterating, $Q_n(G_1 \times G_2) = Q_n(G_1) \times Q_n(G_2)$. So if $Q_{N_1}(G_1) = \{e\}$ and $Q_{N_2}(G_2) = \{e\}$ then $Q_{\max\{N_1,N_2\}}(G_1 \times G_2) = \{e\}$. $\square$

Theorem 1.11.13. *Let G be a finite group. For each prime p, let P_p be a Sylow p-subgroup. Then TFAE:*

1. *G is nilpotent.*
2. *$H < G \Rightarrow H < \mathrm{N}_G(H)$ (every proper subgroup of G is a proper subgroup of its normalizer).*
3. *$P_p \lhd G \quad \forall p$.*
4. *$G \cong \prod_p P_p$.*

Proof.

$1 \Rightarrow 2$: Suppose $H < G$. $\mathrm{Z}(G) \leq \mathrm{N}_G(H)$, so unless $\mathrm{Z}(G) \subset H$, it is immediate that $H < \mathrm{N}_G(H)$.

So assume $\mathrm{Z}(G) \subset H$. Write $\overline{G} := G/\mathrm{Z}(G)$ and let

$$q : G \mapsto\!\!\!\!\rightarrow \overline{G}$$

be the quotient map. Set $\overline{H} = q(H) < \overline{G}$. G nilpotent $\Rightarrow$ $\overline{G}$ nilpotent. By induction (assuming 1 $\Rightarrow$ 2 is known for all groups of order less than $|G|$),

$$\overline{H} < \mathrm{N}_{\overline{G}}\left(\overline{H}\right).$$

But then by the 4th Isomorphism Theorem,

$$H = q^{-1}\left(\overline{H}\right) < q^{-1}\mathrm{N}_{\overline{G}}\left(\overline{H}\right) = \mathrm{N}_G(H).$$

2 $\Rightarrow$ 3: Let $N = \mathrm{N}_G(P_p)$. By a corollary to the Sylow Theorem (Corollary 1.9.12), $\mathrm{N}_G(N) = N$. $\therefore$ Hypothesis 2 $\Rightarrow$ $N = G$, so $P_p \lhd G$.

3 $\Rightarrow$ 4: Write

$$|G| = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}.$$

Suppose by induction (on m) that

$$H = P_{p_1} \cdots P_{p_{m-1}} \cong P_{p_1} \times \cdots P_{p_{m-1}}.$$

Then $H \lhd G$, $P_{p_m} \lhd G$, and $H \cap P_{p_m} = \{e\}$. Hence,

$$P_{p_1} \cdots P_{p_m} = HP_{p_m} \cong H \times P_{p_m} \cong P_{p_1} \times \cdots P_{p_m}.$$

However, $|P_{p_1} \cdots P_{p_m}| = |G|$ so $P_{p_1} \cdots P_{p_m} = G$.

4 $\Rightarrow$ 1: It was already shown that p-groups are nilpotent and a finite product of nilpotent groups is nilpotent.

$\square$

1.12 Free Groups

Theorem 1.12.1. *A subgroup of a free group is free.*

Proof. Let S be a set and let $G = F(S)$. Suppose $H \leq G$. Let

$$S' = S \amalg \{\text{inverses of elts. in } S\}.$$

Recall that elements of G are finite length words in S and S'. Let $M(S')$ denote the free monoid on S' (so that in $M(S')$, ss^{-1} does not simplify for $s \in S$). $\exists$ a surjective map of monoids $q : M(S') \mapsto F(S)$ given by

$$q(x) = x \quad \forall x \in M(S').$$

Write $\overline{x}$ for $q(x)$.

Say that a word $x = x_1 \cdots x_k \in M(S')$ (where $x_i \in S'$ $\forall i$) is **reduced** (or a reduced representative) if $\nexists$ a shorter word $y \in M(S')$ s.t. $q(x) = q(y) = x_1 \cdots x_k$ in G.

Well-order S'. This induces a well-order on $M(S')$ by ordering the words first by length, and then lexicographically among words of the same length. Let

$$R = \{\text{reduced words}\} \subset M(S').$$

ie. $x \in R$ iff $x = \min q^{-1}\{q(x)\}$. For $g \in G$, define $\tilde{g} \in M(S')$ by

$$\tilde{g} = \min q^{-1}(Hg).$$

ie. $\tilde{g} = \min\{x \in M(S') \mid H\overline{x} = Hg\}$. Let

$$\tilde{R} = \{\tilde{g} \mid g \in G\} \subset M(S')$$

be the set of chosen coset representatives. Clearly, only reduced words can occur: $\tilde{R} \subset R$.

Lemma 1.12.2. *A left substring of an element in $\tilde{R}$ is in $\tilde{R}$.*

Proof. Suppose $b = cu \in M(S')$ with $b \in \tilde{R}$ and c a proper substring. Check that $c \in \tilde{R}$.

Since $b \in \tilde{R}$ and c is shorter than b, $H\overline{b} \neq H\overline{c}$ (or else, c would be the chosen coset rep. for $H\overline{b}$ rather than b). If $c \notin \tilde{R}$ then $c' < c$ and $H\overline{c'} = Hc$. So

$$H\overline{b} = H\overline{cu} = H\overline{c'}\,\overline{u} = H\overline{c'u}.$$

However, the ordering is such that $x < y \Rightarrow xz < yz$. So $c' < c \Rightarrow c'u < b$, which contradicts the minimality of b. $\square$

Proof of Theorem continued. Given $r \in \tilde{R}$, $s \in S'$, define $v_{rs} \in H$ by

$$v_{rs} = \overline{r}s(\overline{r'})^{-1}, \quad \text{where } r' = \widetilde{\overline{r}s} \in \tilde{R}.$$

ie. r' is the canonical rep. for $H\overline{r}s$. So $H\overline{r'} = H\overline{r}s$, and thus $v_{rs} \in H$.

Notice $v_{rs}^{-1} = \overline{r'}s^{-1}(\overline{r})^{-1}$, and

$$H\overline{r'} = H\overline{rs} \Rightarrow H\overline{r} = H\overline{r'}s^{-1},$$

and since $r \in \tilde{R}$, r is the canonical rep. for $H\overline{r'}s^{-1}$. Thus

$$v_{r,s}^{-1} = v_{r',s^{-1}},$$

so $\{v_{r,s} \mid r \in \tilde{R}, s \in S'\}$ is closed under inverses. Let

$$T = \{v_{rs} \in H \mid r \in \tilde{R}, s \in S', v_{rs} \neq e\}.$$

Note that it is possible to have $v_{r,s} = v_{r',s'}$ without $r = r'$ and $s = s'$.

Define $\phi : F(T) \mapsto H$ by $\phi(v_{rs}) := v_{rs}\ \forall v_{rs} \in T$. To finish the proof that H is free, we show that ϕ is an isomorphism.

Let $h \in H$. Write $h = s_1 \cdots s_\ell$ in terms of generators of G. Set $b_1 = e$ and inductively set $b_{j+1} = \widetilde{\overline{b_j}s_j}$ (ie. b_{j+1} is the canon. rep. for coset $H\overline{b_j}s_j$).

$\therefore$ By construction, $v_{b_j,s_j} = \overline{b_j}s_j\overline{b_{j+1}}^{-1}$. By induction,

$$H\overline{b_{j+1}} = H\overline{b_j}s_j = H\overline{b_{j-1}}s_{j-1}s_j = \cdots H\overline{b_1}s_1 \cdots s_j = Hs_1 \cdots s_j.$$

$\therefore H\overline{b_{\ell+1}} = Hs_1 \cdots s_\ell = Hh = H$, so $\overline{b_{\ell+1}} = e$.

$$\phi(v_{b_1,s_1}v_{b_2,s_2} \cdots v_{b_\ell,s_\ell}) = \overline{b_1}s_1(\overline{b_2})^{-1}\overline{b_2}s_2(\overline{b_2})^{-1} \cdots \overline{b_\ell}s_\ell(\overline{b_{\ell+1}})^{-1} = s_1 \cdots s_\ell = h.$$

$\therefore \phi$ is onto.

Suppose $\phi(x) = e$ for some $x \in F(T)$ and $x \neq e$. Let $x = x_1 \cdots x_\ell$ be an expression for x as a reduced word in the elts. of T. Recall that the elemnts of T can be written as $v_{r,s}$ in many ways. For each $i = 1, \ldots, \ell$, pick the expression $x_i = v_{b_i,s_i}$ in which $b_i \in \tilde{R}$ be minimal. Then v_{b_i,s_i} contains an occurrence of s_i, since if s_i cancelled then, using the fact that $\tilde{R}$ is closed under left substrings, a shorter b_i' and an s_i' could be picked such that $x_i = v_{b_i',s_i'}$.

Since $\phi(x) = e$, within G, the string $\phi(x)$, which initially contains all of $s_1, \ldots, s_\ell$, must reduce to eliminate them. So $\exists m$ such that $\phi(v_{b_m,s_m}v_{b_{m+1},s_{m+1}})$ reduces to eliminate s_m or s_{m+1} (or both). Write $v_{b_m,s_m}v_{b_{m+1},s_{m+1}}$ as:

$$\overline{b_m}s_m(\overline{y})^{-1}\overline{b_{m+1}}s_{m+1}(\overline{z})^{-1},$$

where y = canon. rep. for $H\overline{b_m}s_m$ and z = canon. rep. for $H\overline{b_{m+1}}s_{m+1}$. Cancellation of at least one of s_m, s_{m+1} can happen in one of three ways:

1. $\bar{y} = \overline{b_{m+1}}$ and $s_m = s_{m+1}^{-1}$, or

2. $\overline{b_{m+1}} s_{m+1}$ is a left substring of $\bar{y}$, or

3. $\bar{y} s_m^{-1}$ is a left substring of $\overline{b_{m+1}}$.

If 1: $H\bar{z} = H\overline{b_{m+1}} s_{m+1} = H\bar{y} s_m^{-1} = H\overline{b_m}$, so $z = b_m$ (both lie in $\tilde{R}$ and they represent the same coset). So $v_{b_{m+1}, s_{m+1}} = (v_{b_m, s_m})^{-1}$ and the word x was not reduced, which is a contradiction.

If 2: Since $b_m, y, b_{m+1}, z \in \tilde{R} \subset R$, all are reduced, so $\overline{b_{m+1}} s_{m+1}$ is a left substring of $\bar{y} \Rightarrow b_{m+1} s_{m+1}$ is a left substring of y. Hence $b_{m+1} s_{m+1} \in \tilde{R}$. So $b_{m+1} s_{m+1}$ and z are canon. reps. for the coset $H b_{m+1} s_{m+1}$, so $z = b_{m+1} s_{m+1}$. But then $v_{b_{m+1}, s_{m+1}} = e$ so $v_{b_{m+1}, s_{m+1}} \notin T$, which is a contradiction.

If 3: As in case 2, $y s_m^{-1}$ is a left substring of b_{m+1} so $y s_m^{-1} \in \tilde{R}$ and represents the same coset as b_m. So $b_m = y s_m^{-1}$ and so $v_{b_m, s_m} = e \notin T$, which is a contradiction.

$\therefore$ None of these cases can occur, so $\phi(x) = e$ for $x \neq e$ is not possible. Hence ϕ is an injection. □

Note: it is possible that H is not finitely generated, even if G is finitely generated. e.g. Let $G = F(x, y)$ and let $H = [G, G]$ (the commutator subgroup). Then

$$H = F(x, y, [y, x], [[y, x], x], \ldots, [\cdots [[y, x], x] x \cdots, x], \ldots\}.$$