A group \((G, *)\) is a set \(G\) with a binary operation \(\ast : G \times G \to G\) satisfying

\begin{enumerate}
  \item \(\ast\) is associative: For all \(a, b, c \in G\), \((a \ast b) \ast c = a \ast (b \ast c)\).
  \item \(\ast\) has a two-sided identity \(e\): For all \(a \in G\), \(a \ast e = e \ast a = a\).
  \item \(\ast\) has two-sided inverses: For all \(a \in G\), there is an \(i(a)\) with \(a \ast i(a) = i(a) \ast a = e\).
\end{enumerate}

A group is abelian if also

\item \(\ast\) is commutative: For all \(a, b \in G\), \(a \ast b = b \ast a\).

A monoid is a set which satisfies G1 and G2 (associative with two-sided identity). A semigroup is a set which satisfies G1 (associative with no other assumptions).

We usually just write \(G\) for \((G, \ast)\).

The order \(|G|\) of a group (monoid, semigroup) \(G\) is the cardinality of the set \(G\).

**Examples**

1. The set of maps \(X \to X\) forms a monoid \(X^X\) under composition.
2. The set of permutations \(X \to X\) forms a group \(S_X\) under composition.
   [If the set is \(X = \{1, \ldots, n\}\) we write this group as \(S_n\).]
3. The set \(M_n(\mathbb{R})\) of \(n \times n\) matrices with entries in \(\mathbb{R}\) forms a monoid under matrix multiplication (and a group under matrix addition).
4. The set \(GL_n(\mathbb{R})\) of invertible \(n \times n\) matrices forms a group under multiplication.
5. The set of linear maps (resp. invertible linear maps) from a vector space \(V\) to itself form a monoid (resp. group) under composition.
6. \((\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times), (\mathbb{Q}, \times), (\mathbb{Z}/n\mathbb{Z}, \times)\) are monoids (but not groups).
7. \((\mathbb{Z}, +), (\mathbb{Z}/n\mathbb{Z}, +), (\mathbb{Q} \setminus \{0\}, \times)\) are groups.
8. The vector cross product on \(\mathbb{R}^3\) is not associative, so \((\mathbb{R}^3, \times)\) is not a semigroup.
9. The trivial group \(1 = \{e\}\) with just one element (the identity) is a group.

**Lemma 1.1** In a semigroup, the identity and inverses are uniquely determined by \(\ast\) when they exist.

**Proof.** If \(e\) and \(e'\) are identities, then \(e = e \ast e' = e'\). Now assume \(e\) is a two-sided identity and \(b\) and \(b'\) are inverses of \(a\). Then \(b = b \ast e = b \ast (a \ast b') = (b \ast a) \ast b' = e \ast b' = b'\). \(\square\)

Note that this actually shows that any left identity is equal to any right identity and any left inverse is equal to any right inverse, so when looking for identities and inverses in a group we need only check one side (but we need to know \(G\) is a group first!). It is possible for an element of a monoid to have a left inverse (and possibly more than one) but not a right inverse (e.g., an injective, but not surjective, \(f \in X^X\) for some infinite
If $G$ is a group and $x, y \in G$ then $(xy)^{-1} = y^{-1}x^{-1}$.

Proof. $(xy)(y^{-1}x^{-1}) = ((xy)y^{-1})y = (x(yy^{-1}))x^{-1} = (x1)x^{-1} = xx^{-1} = 1$, so $y^{-1}x^{-1}$ is a (right) inverse to $xy$, and by Lemma 1.1 it is the unique inverse.

Lemma 1.3 (Cancelation laws) Suppose $G$ is a group and $a, x, y \in G$.

If $ax = ay$ then $x = y$. If $xa = ya$ then $x = y$.

Proof. Multiply on left (respectively right) by $a^{-1}$.

Lemma 1.4 (Generalized associativity) If $a_1, \ldots, a_r$ are elements of a semigroup then any two products of $a_1, \ldots, a_r$ in that order are equal.

Proof. Show any such product $= ((\ldots(a_1a_2)a_3)\ldots)a_n$ by induction on $n$. To do this, use induction on the number of terms on the right of the highest level multiply: If $((\ldots)a_n$, use induction to rewrite $\ldots$. If $((\ldots)((\ldots)(\ldots))\ldots)$, rewrite as $((\ldots)(\ldots))(\ldots)$.

Lemma 1.5 (Generalized commutativity) If $a_1, \ldots, a_r$ are elements of a semigroup and $a_ia_j = a_ja_i$ for each $i, j$, then any two products of $a_1, \ldots, a_r$ in any order are equal.

For $n \in \mathbb{Z}$ define

$$a^n = \begin{cases} a.a \ldots a \text{ (n times)} & \text{if } n > 0, \\ 1 & \text{if } n = 0, \\ a^{-1}a^{-1} \ldots a^{-1} \text{ (n times)} & \text{if } n < 0. \end{cases}$$

Define $na$ similarly if $G$ is written additively. Using Lemmas 1.4 and 1.5 it is clear that $a^{n+m} = a^na^m$ (or $(n+m)a = na+ma$) for any $n, m \in \mathbb{Z}$. For abelian groups $(ab)^n = a^nb^n$, but this is not true in general for non-abelian groups.

The order $|x|$ of $x \in G$ is the minimum $n > 0$ such that $x^n = 1$ (or $\infty$ if no such $n$ exists).

Lemma 1.6 If $G$ is a group and $x \in G$ then

(a) $x^n = 1$ iff $|x| | n$,
(b) $x^n = x^m$ iff $n \equiv m \mod |x|$,
(c) $|x^r| = |x|/\gcd(r, |x|)$.

Proof. (a): Write $n = q|x| + r$, $0 \leq r < |x|$. Then $x^n = (x^{|x|})^q x^r = x^r$, so $x^n = 1$ iff $r = 0$ iff $|x| | n$. (b): Multiply by $x^{-m}$ and use (a). (c): Clearly $(x^r)^{|x|} = 1$ so $|x^r| | |x|$ and $|x^r| = |x|/d$ for some $d$. Now $(x^r)^{|x|/d} = 1$ iff $|x| | r|x|/d$ iff $d | r$ iff $d | \gcd(r, |x|)$. Largest $d$ is clearly $\gcd(r, |x|)$. \qed
Subobjects

Definition A subgroup of the group \((G, \ast)\) is a subset \(H \subseteq G\) which is a group under the restriction of \(\ast\) to \(H\) and has the same identity and inverses. We write \(H \leq G\). Similarly for submonoids and subsemigroups. A subgroup is proper if \(H \neq G\), and non-trivial if \(H \neq \{e\}\).

For a subgroup, \(H\) automatically must have the same identity and inverses, but for a submonoid you need to check that \(H\) has the same identity as \(G\), e.g., \(\{0\}\) is not a submonoid of \((\mathbb{N}, \times)\). In all cases, a subobject of a subobject is a subobject.

Example Let \(O_2(\mathbb{R})\) be the set of linear maps on \(\mathbb{R}^2\) which preserve distances (orthogonal maps). Then \(O_2(\mathbb{R})\) is the set of rotations and reflections about the origin in \(\mathbb{R}^2\). Let \(D_n\) be the set of such maps in the plane that leave a given regular \(n\)-gon centered at the origin unchanged and let \(C_n\) be the set of these that are rotations. Then \(O_2(\mathbb{R})\), \(D_n\), and \(C_n\) are all groups, and

\[
\{1\} \leq C_n \leq D_n \leq O_2(\mathbb{R}) \leq GL_2(\mathbb{R}) \leq S_{\mathbb{R}^2}.
\]

Lemma 2.1 A subset \(H \subseteq G\) is a subgroup of \(G\) if and only if

(i) \(H \neq \emptyset\) and (ii) \(\forall x, y \in H : xy^{-1} \in H\).

Lemma 2.2 If \(\{H_i \mid i \in I\}\) is a (possibly infinite) collection of subgroups of \(G\) then \(\bigcap_{i \in I} H_i \leq G\).

Definition If \(S\) is any subset of a group \(G\), the subgroup generated by \(S\) is \(\langle S \rangle = \bigcap_{S \subseteq H \subseteq G} H\), the intersection of all subgroups of \(G\) containing \(S\). By Lemma 2.2 this is a subgroup, and it is the smallest subgroup of \(G\) containing the set \(S\).

Lemma 2.3 \(\langle S \rangle = \{x_{1}^{\pm 1} x_{2}^{\pm 1} \ldots x_{k}^{\pm 1} \mid x_{i} \in S, k \in \mathbb{N}\}\), where this set contains all (finite) products of elements and inverses of elements of \(S\) (possibly with repetitions).

Definition A group \(G\) is finitely generated if \(G = \langle S \rangle\) for some finite subset \(S \subseteq G\). A group is cyclic if \(G = \langle x \rangle = \{\langle x \rangle \} = \{x^n \mid n \in \mathbb{Z}\}\) for some \(x \in G\). Note \(|\langle x \rangle| = |x|\).

Example The group \(C_n\) defined above is cyclic.

Lemma 2.4 If \(x, y \in G\) commute and \(\gcd(|x|, |y|) = 1\) then \(|xy| = |x||y|\).

Proof. Let \(n = |xy|\). Now \((xy)^{|x||y|} = (x^{|x|})(y^{|y|})^{|x|} = 1\), so \(n\) \(|x||y|\). Conversely, \((xy)^n = 1\), so \(x^n y^n = 1\) and \(z = x^n = y^{-n} \in \langle x \rangle \cap \langle y \rangle\). But \(|z|\) is then a factor of both \(|x|\) and \(|y|\). Thus \(|z| = 1\), so \(z = 1\). Now \(|x| \mid n\) and \(|y| \mid n\), so \(\gcd(|x|, |y|) \mid n\), but \(\text{lcm}(|x|, |y|) = |x||y|\) \(\gcd(|x|, |y|) = |x||y|\) so \(|x||y| \mid n\). Hence \(|n = |x||y|\). □

In general, if \(x\) and \(y\) commute then \(|xy|\) is a factor of \(\text{lcm}(|x|, |y|)\), but need not be equal to the lcm. If \(x\) and \(y\) do not commute then \(|xy|\) can be almost anything.
Cosets

If $S$ and $T$ are two subsets of $G$, write $ST = \{st \mid s \in S, t \in T\}$. Similarly, if $x \in G$, $xS = \{xs \mid s \in S\}$ and $Sx = S\{x\} = \{sx \mid s \in S\}$. This “product” is associative: $S(TU) = (ST)U = \{stu \mid s \in S, t \in T, u \in U\}$. Also, if $H \leq G$ then $HH \subseteq H = 1H \subseteq HH$, so $H = HH$.

**Definition** A left coset of a subgroup $H$ is a set of the form $xH$. A right coset of $H$ is a set of the form $Hx$. The set of left cosets is written $G/H$. The index of $H$ in $G$ is the number of left cosets: $[G:H] = |G/H|$.

Sometimes the set of right cosets is written $H \backslash G$.

**Lemma 2.5** Let $G$ be a group and $H \leq G$. Define $x \sim y$ iff $y^{-1}x \in H$. Then $\sim$ is an equivalence relation with equivalence classes $xH$, $x \in G$. Hence left cosets $xH$ and $yH$ are always either equal or disjoint and $G/H = G/\sim$.

**Lemma 2.6** The number of left cosets of $H$ in $G$ is the same as the number of right cosets of $H$ in $G$.

**Proof.** The bijection $G \to G$ given by $x \mapsto x^{-1}$ maps right cosets $Hx$ to left cosets $x^{-1}H$ and vice versa. □

**Theorem (Lagrange)** If $H \leq G$ then $|G| = [G:H]|H|$.

**Proof.** $G$ is the disjoint union of the cosets $xH$ since these are just the equivalence classes of an equivalence relation. But $|H| = |xH|$ (the map $h \mapsto xh$ is a bijection between $H$ and $xH$), so $|G| = \sum_{xH \in G/H} |xH| = [G:H]|H|$. □

**Example** If $x \in G$ then $|x| = |\langle x \rangle|$ so $|x| | |G|$. In particular, $x^{[G]} = 1$ for any $x \in G$.

**Quotient groups**

**Definition** A subgroup $H \leq G$ is normal ($H \trianglelefteq G$) iff for all $x \in G$, $xH = Hx$.

Note: If $G$ is abelian and $H \leq G$ then $H \trianglelefteq G$.

**Lemma 2.7** A subgroup $H$ of $G$ is normal iff the equivalence relation $\sim$ above satisfies the condition $x \sim x'$, $y \sim y'$ implies $xy \sim x'y'$.

If $H \trianglelefteq G$ then we can define multiplication on $G/H$ by $\bar{x}\bar{y} = \bar{xy}$ (i.e., $(xH)(yH) = xyH$). Note that this “multiplication” is the same as the multiplication defined on sets above since $(xH)(yH) = x(Hy)H = x(yH)H = xyH$. Under this multiplication $G/H$ is a group and is called the quotient group of $G$ by $H$.
More on Normal Subgroups

Lemma 3.1 If \( H \leq G \) then \( H \leq G \) iff \( xhx^{-1} \in H \) for all \( x \in G, h \in H \).

Proof. Condition is equivalent to \( xHx^{-1} \subseteq H \). But then \( H = x(x^{-1})H(x^{-1})^{-1}x^{-1} \subseteq xHx^{-1} \subseteq H \), so \( xHx^{-1} = H \), which is equivalent to \( xH = Hx \).

Definition If \( H \leq G \) then the normalizer of \( H \) in \( G \) is the set \( N_G(H) = \{ x \in G \mid xHx^{-1} = H \} \).

Lemma 3.2 If \( H \leq G \) then \( H \leq N_G(H) \leq G \), conversely, if \( H \leq H' \leq G \) then \( H' \leq N_G(H) \). In particular \( H \leq G \) iff \( N_G(H) = G \).

Proof. \( 1 \in N_G(H) \), so \( N_G(H) \neq \emptyset \). If \( x, y \in N_G(H) \), \( xyH = xHy = Hxy \), so \( xy \in N_G(H) \), and \( x^{-1}H = (Hx)^{-1} = (H^{-1})^{-1} = H^{-1} \), so \( x^{-1} \in N_G(H) \). Thus \( N_G(H) \leq G \).

As a consequence, if \( xH = Hx \) for all \( x \in S \) and \( \langle S \rangle = G \) then \( H \leq G \).

Also, if \( K \leq G \) and \( K \leq H \leq G \) then \( K \leq H \).

Warning: If \( K \leq H \leq G \) then it does not follow that \( K \leq G \).

Homomorphisms

Definition A (semigroup) homomorphism from a semigroup \( G \) to another semigroup \( H \) is a map \( f: G \rightarrow H \) with the property \( f(x \star_G y) = f(x) \star_H f(y) \). A monoid homomorphism between two monoids also requires \( f(e_G) = e_H \). A group homomorphism between two groups requires this and also \( f(i_G(x)) = i_H(f(x)) \).

For groups the last two conditions are automatic: \( f(e_G)f(e_G) = f(e_G \star_G e_G) = f(e_G) \), so \( f(e_G) = e_H; f(x^{-1})f(x) = f(e) = e, \) so \( f(x^{-1}) = f(x)^{-1} \). Thus one only needs to check \( f(xy) = f(x)f(y) \). For monoids \( f(e) = e \) is not automatic, e.g., inclusion \( \{0\} \rightarrow (\mathbb{N}, \times) \).

Note: \( H \) is a sub-‘object’ of \( G \) iff the inclusion map \( H \rightarrow G \) is an ‘object’-homomorphism.

Examples The determinant map \( \text{det}: GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\times \). The exponential map \( (\mathbb{C}, +) \rightarrow (\mathbb{C}^\times, \times) \). For \( H \leq G \), the quotient map \( \pi: G \rightarrow G/H; \pi(x) = xH \).

Definition A (semigroup/monoid/group) isomorphism is a (semigroup/monoid/group) homomorphism \( f: G \rightarrow H \) which has a 2-sided inverse (semigroup/monoid/group) homomorphism \( g: H \rightarrow G \). If an isomorphism exists we say \( G \) and \( H \) are isomorphic and write \( G \cong H \). Note that isomorphism is an ‘equivalence relation’.

Example Exponential map \( \exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \times) \) has inverse \( \log: (\mathbb{R}_{>0}, \times) \rightarrow (\mathbb{R}, +) \).
**Lemma 3.3** For semigroups, monoids, or groups, \( f : G \to H \) is an isomorphism iff it is a bijective homomorphism.

**Proof.** An isomorphism has an inverse, so must be bijective. Conversely, a bijective homomorphism \( f \) has an inverse \( g \). Now \( f(g(x)g(y)) = f(g(x))f(g(y)) = xy = f(g(xy)) \), so by injectivity of \( f \), \( g(x)g(y) = g(xy) \). (And for monoids, \( f(g(1)) = 1 = f(1) \), so \( g(1) = 1 \).) Thus \( g \) is a homomorphism. \( \Box \)

**Definition** The kernel, \( \text{Ker} \, f \), of a group homomorphism \( f : G \to H \) is the set of elements of \( G \) mapped to \( 1 \in H \); \( \text{Ker} \, f = \{ x : f(x) = 1 \} \).

**Lemma 3.4** A homomorphism \( f \) is injective iff \( \text{Ker} \, f = \{ 1 \} \).

**Proof.** Use \( f(x) = f(x') \iff f(x^{-1}x') = 1 \). \( \Box \)

**Lemma 3.5** If \( f : G \to H \) is a homomorphism then \( \text{Im} \, f \leq H \) and \( \text{Ker} \, f \leq G \).

**Proof.** If \( x \in G \) and \( k \in \text{Ker} \, f \), then \( f(kxk^{-1}) = f(x)1f(x)^{-1} = 1 \), so \( xhx^{-1} \in \text{Ker} \, f \). Rest is easy. \( \Box \)

Conversely, if \( K \leq G \) then \( K = \text{Ker} \, f \) for some \( f \) (take \( f = \pi : G \to G/K \)), and if \( H \leq G \) then \( H = \text{Im} \, f \) for some \( f \) (e.g., inclusion \( H \to G \)).

**Theorem (1st Isomorphism Theorem)** If \( f : G \to H \) is a homomorphism then we can write \( f = \iota \circ \tilde{f} \circ \pi \) where

- \( \pi : G \to \frac{G}{\text{Ker} \, f} \) is the (surjective) projection homomorphism.
- \( \tilde{f} : \frac{G}{\text{Ker} \, f} \to \text{Im} \, f \) is a (bijective) isomorphism.
- \( i : \text{Im} \, f \to H \) is the (injective) inclusion homomorphism.

**Proof.** We know such a decomposition exists as maps, we only need to show \( \tilde{f} \) is a homomorphism. But \( \tilde{f}(xHyH) = \tilde{f}(xyH) = \tilde{f}(xy) = f(x)f(y) = \tilde{f}(xH)f(yH) \). \( \Box \)

**Important consequence:** For any homomorphism \( f : G \to H \), \( \frac{G}{\text{Ker} \, f} \cong \text{Im} \, f \).

**Theorem (2nd Isomorphism Theorem)** Let \( K \leq G \). Then there is a bijection between the subgroups of \( G \) containing \( K \) and the subgroups of \( G/K \). The correspondence is given by \( K \leq H \leq G \) maps to \( H/K \leq G/H \) and \( \mathcal{H} \leq \mathcal{G} \) maps to \( \cup_{x \in \mathcal{H}} xK \leq G \). Moreover, in this correspondence, \( H \leq G \) iff \( H/K \leq G/K \), and if this occurs then \( (G/K)/(H/K) \cong G/H \).

**Proof of last part.** Apply 1st Isomorphism Thm to \( f : G/K \to G/H \); \( f(xK) = xH \). \( \Box \)

**Theorem (3rd Isomorphism Theorem)** If \( H \leq G \) and \( K \leq G \) then \( K \cap H \leq H \), \( K \leq HK \), and \( HK/K \cong H/(K \cap H) \).

**Proof.** Apply 1st Isomorphism Theorem to \( f : H \to G/K \); \( f(x) = xK \). \( \Box \)
Theorem (Cayley) Any group is isomorphic to a subgroup of a permutation group.

Proof. Let $G$ be a group and $S_G$ be the group of bijections $G \to G$. Construct a map

$$\phi: G \to S_G$$

by defining for $x \in G$ a map $\phi(x): G \to G$ by $\phi(x)(y) = xy$. Then $\phi(x) \in S_G$

(inverse is $\phi(x^{-1})$) and $\phi$ is a homomorphism ($\phi(x) \circ \phi(y) = \phi(xy)$). If $\phi(x) = 1$

then $xy = y$ for all $y$ and so $x = 1$. Hence $\text{Ker } \phi = \{1\}$. By the 1st Isomorphism

Theorem, $G \cong \text{Im } \phi$, so $G$ is isomorphic to a subgroup of $S_G$. \hfill \Box

Write $S_n$ for the Symmetric group on set $X = \{1, \ldots, n\}$, i.e., the group of permutations

(bijections $X \to X$) with group operation given by composition. Note that $|S_n| = n!$.

A $k$-cycle $(a_1, \ldots, a_k)$ is a permutation in $S_n$ that maps $a_j$ to $a_{j+1}$ and $a_k$ to $a_1$ but

leaves every other element fixed. A 2-cycle is also called a transposition.

Note: A $k$-cycle has order $k$ in $S_n$. A $k$-cycle can be written in $k$ different ways,

$$(a_1, a_2, \ldots, a_k) = (a_2, a_3, \ldots, a_k, a_1) = \cdots = (a_k, a_1, \ldots, a_{k-1}).$$

The support of a permutation, $\text{supp } \pi = \{i \mid \pi(i) \neq i\}$, is the set of elements that

it moves. As an example, $\text{supp}(a_1, \ldots, a_k) = \{a_1, \ldots, a_k\}$ for $k \geq 2$. Two cycles are
disjoint if their supports are disjoint.

Lemma 4.1 Disjoint cycles commute.

Cycles that are not disjoint do not in general commute, e.g., $(12)(13) = (32)$, $(13)(12) = (123)$.

Lemma 4.2 Any permutation $\pi \in S_n$ can be written as a product of disjoint cycles (of

lengths $\geq 2$), and this representation is unique up to the order of the cycles. Moreover

the support of these cycles are subsets of $\text{supp } \pi$.

Proof. Induction on $|\text{supp } \pi|$. If $\text{supp } \pi = \emptyset$ then $\pi = 1$ is the empty product, otherwise

pick $a_1 \in \text{supp } \pi$ and inductively define $a_{i+1} = \pi(a_i)$. Eventually we must have a repeat

$a_i = a_j$, and the first such repeat must be of the form $a_i = a_{k+1}$ (apply $\pi^{i-1}$ to $a_i = a_j$).

Let $\sigma = (a_1, \ldots, a_k)$. Then $\text{supp } \sigma^{-1} = \text{supp } \pi \setminus \text{supp } \sigma$, so $\sigma^{-1} \pi = \sigma_1 \cdots \sigma_r$, and thus

$\pi = \sigma \sigma_1 \cdots \sigma_r$. Also $\text{supp } \sigma$ is disjoint from each $\text{supp } \sigma_i \subseteq \text{supp } \pi \setminus \text{supp } \sigma$. \hfill \Box

A permutation $\pi$ has cycle type $(k_1)^{a_1} \cdots (k_r)^{a_r}$ if $\pi$ is the product of disjoint cycles $\sigma_i$

of length $k_i$.

Exercise: The order of a permutation of type $(k_1)^{a_1} \cdots (k_r)^{a_r}$ is $\text{lcm}\{k_1, \ldots, k_r\}$.

Lemma 4.3 Any permutation can be written as a product of transpositions, i.e, the set

of transpositions generates $S_n$.

Proof. Any cycle is a product of transpositions, since we can write $(a_1, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_2)$, and the set of all cycles generate $S_n$ by Lemma 4.2 \hfill \Box
Note: The transpositions in Lemma 4.3 are not in general disjoint, nor is the representation unique.

**Lemma 4.4** There exists a group homomorphism \( \text{sgn}: S_n \rightarrow \{ \pm 1 \} \) which sends every transposition to \(-1\). (\( \{ \pm 1 \} \) is group under multiplication.)

One definition of \( \text{sgn} \) is \( \text{sgn} \pi = (-1)^n \) where \( n \) is the number of transpositions used to express \( \pi \) in Lemma 3. This is clearly a homomorphism, but it requires proof that it is well defined. Another is \( \text{sgn} \pi = \prod_{i<j} \frac{\pi(i) - \pi(j)}{i-j} \). This is clearly well defined, but it requires proof that it is a homomorphism.

The Alternating group \( A_n \) is the kernel of \( \text{sgn} \). A permutation \( \pi \) is called even if \( \text{sgn} \pi = 1 \) and odd if \( \text{sgn} \pi = -1 \). \( A_n \) is therefore the set of even permutations.

Note: A \( k \)-cycle is even iff \( k \) is odd.

**Lemma 4.5** The group \( A_n \) is generated by 3-cycles.

**Proof.** The product of two transpositions is always a product of 3-cycles.

Two elements \( x, y \) in a group \( G \) are conjugate if \( x = zyz^{-1} \) for some \( z \in G \). Conjugacy is an equivalence relation on \( G \) and the equivalence classes \( C_x, x \in G \), are called conjugacy classes.

Note: A subgroup is normal iff it is the union of conjugacy classes.

**Lemma 4.6** \( \pi(a_1, \ldots, a_r)(b_1, \ldots, b_s) \ldots \pi^{-1} = (\pi(a_1), \ldots, \pi(a_r))(\pi(b_1), \ldots, \pi(b_s)) \ldots \). In particular two permutations are conjugate in \( S_n \) iff they have the same cycle type.

**Definition** A group \( G \) is called simple if \( |G| > 1 \) and the only normal subgroups of \( G \) are \( \{1\} \) and \( G \).

**Theorem 4.7** \( A_n \) is simple for \( n \geq 5 \).

**Proof.** Assume \( 1 < H \trianglelefteq G \). First show that \( H \) contains a 3-cycle. Pick \( \sigma \in H, \sigma \neq 1 \). If \( \sigma = (123)(456) \cdots \in H \), then \( (124)(124)^{-1}\sigma^{-1} = (124)(235)^{-1} = (12534) \in H \). If \( \sigma = (12 \ldots k)(\ldots) \cdots \in H \) with \( k \geq 4 \) then \( (123)\sigma(123)^{-1}\sigma^{-1} = (124) \in H \). Hence we may assume \( \sigma \) is of type \((2)^r\) or \((3)(2)^r\). But since \( \sigma \in A_n, r \) is even.

If \( \sigma = (12)(34) \cdots \in H \) then \( (123)\sigma(123)^{-1}\sigma^{-1} = (13)(24) \in H \).

If \( \sigma = (12)(34) \in H \) then \( (125)\sigma(125)^{-1}\sigma^{-1} = (152) \in H \).

Once we have one 3-cycle, say \( (123) \), we get all the others by conjugation \( \pi(123)\pi^{-1} \) (or \( (\pi(45))(123)(\pi(45))^{-1} \) if \( \pi \) odd). Then \( H = A_n \) since \( A_n \) is generated by 3-cycles.

Note: The subgroup \( V = \{ 1, (12)(34), (13)(24), (14)(23) \} \) is a normal subgroup of \( A_4 \).
The direct product $G_1 \times G_2$ of groups $G_1$ and $G_2$ is the cartesian product of the sets with product defined componentwise $(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$. Similarly for direct products $\prod_{i \in I} G_i$ of a collection of groups $G_i$, $i \in I$.

Note: $G_1 \times G_2$ has normal subgroups $G'_1 = G_1 \times \{1\}$ and $G'_2 = \{1\} \times G_2$ isomorphic to $G_1$ and $G_2$ respectively. This can be seen by considering the kernel of the projection homomorphism $\pi_i: G \to G_i$ obtained by taking the $i$'th coordinate of an element of $G$. Elements of $G'_1$ commute with elements of $G'_2$.

**Lemma 5.1** If $H_i \leq G$, $i = 1, \ldots, n$, are subgroups such that $h_i h_j = h_j h_i$ for all $h_i \in H_i$, $h_j \in H_j$, and if $\langle \cup H_i \rangle = G$ and $H_i \cap \langle \cup_{j \neq i} H_j \rangle = 1$ for all $i$, then $G \cong \prod H_i$.

**Proof.** Define $f: \prod H_i \to G$ by $f(h_1, \ldots, h_n) = h_1h_2\ldots h_n$. Since elements of $H_i$ commute with those of $H_j$ for $j \neq i$ it can be shown that $f$ is a homomorphism. Let $(h_1, \ldots, h_n) \in \text{Ker } f$. Then $h_i = (\prod_{j \neq i} h_j)^{-1} \in H_i \cap \langle \cup_{j \neq i} H_j \rangle = 1$ so $h_i = 1$ and $f$ is injective. The image contains each $H_i$ so contains $\langle \cup H_i \rangle = G$. Hence $f$ is surjective. Therefore $f$ is an isomorphism. \qed

**Lemma 5.2** If $H_i \trianglelefteq G$, $i = 1, \ldots, n$, are normal subgroups such that $\langle \cup H_i \rangle = G$ and $H_i \cap \langle \cup_{j \neq i} H_j \rangle = 1$ for all $i$, then $G \cong \prod H_i$.

**Proof.** If $h_i \in H_i$ and $h_j \in H_j$ then $(h_i h_j h_i^{-1})h_j^{-1} = h_i(h_j h_i^{-1} h_j^{-1}) \in H_i \cap H_j = \{1\}$, so $h_i h_j = h_j h_i$. Now apply Lemma 5.1. \qed

**Theorem (Chinese Remainder Theorem)** If $\gcd(n, m) = 1$ then $C_{nm} \cong C_n \times C_m$.

**Proof.** Let $C_{nm} = \langle a \rangle$ and consider the (cyclic) subgroups $\langle a^m \rangle$ and $\langle a^n \rangle$. \qed

**Universal property of direct products.**

If $H$ is any group and $f_i: H \to G_i$ are homomorphisms then there exists a unique homomorphism $f: H \to G$ such that $\pi_i \circ f = f_i$. Conversely, if $f$ and $\pi_i: G \to G_i$ have this property then $G \cong \prod G_i$.

The direct sum $\bigoplus G_i$ of abelian groups $G_i$ is the subgroup of $\prod G_i$ consisting of the elements $(g_i)$ with all but finitely many $g_i$ equal to the identity. Note this it the same as the direct product if there are only finitely many $G_i$. Let $i_j: G_i \to G$ be the map which sends $g_i$ to $(1, \ldots, 1, g_i, 1, \ldots, 1) \in G$.

**Universal property of direct sums.**

If $H$ and $G_j$ are abelian groups and $f_j: G_j \to H$ are homomorphisms then there exists a unique homomorphism $f: G \to H$ such that $f \circ i_j = f_j$. Conversely, if $f$ and $i_j: G_j \to G$ have this property then $G \cong \bigoplus G_j$. 

\[ H \xrightarrow{f_j} G_j \xleftarrow{i_j} G \]
Theorem (Classification of Finite Abelian Groups) Any finite abelian group is a product of cyclic groups $C_{d_1} \times \cdots \times C_{d_r}$ with $d_{i+1} \mid d_i$, $d_i > 1$. Moreover, this representation is unique.

Note: In the representation $C_{d_1} \times \cdots \times C_{d_r}$, the subgroups corresponding to the factors $C_{d_i}$ are not unique in general.

Proof. Let $C = \langle x \rangle$ be a cyclic subgroup of $G$ of maximal order $|C| = d$. Let $H$ be a maximal subgroup of $G$ such that $H \cap C = 1$. Such subgroups exist (e.g., $1 \cap C = 1$) and $G$ is finite so there must be at least one $H$ of maximal size. We wish to show $G \cong C \times H$.

Since $H, C \leq G$ and $H \cap C = 1$, it only remains to prove $HC = G$. Assume otherwise and let $y \notin HC$. Let $s$ be the order of $yHC$ in $G/HC$, so $y^s \in HC$ and $y^s \notin HC$ for $0 < i < s$. Write $y^n = hx^r$, $h \in H$. By replacing $y$ by $yx^{-r}$ we can assume $0 \leq r < s$.

Note that $yHC = yx^{-r}HC$ so the value of $s$ above is the same for $y$ as for $yx^{-r}$. Now the order of $y$ is divisible by $s$ (since $y^n = 1$ implies $(yHC)^n = 1$ in $G/HC$). Thus if $y^n = 1$ then $y^n = h^{n/s}x^{rn/s} = 1$ and $x^{rn/s} = h^{-n/s} \in H \cap C = 1$. But then $rn/s$ is a multiple of $d$ and $r < s$ so either $r = 0$ or $rn/s \geq d$ which gives $n > d$, contradicting the choice of $C$.

Hence $r = 0$ and $y^n = h$. Now consider $H' = \langle y, H \rangle$. If $z \in H' \cap C$ then $y^ih' = z = x^i$ for some $i, j \in \mathbb{Z}$, $h \in H$. But then $y^i \in HC$, so $s \mid i$, $z = y^ih' = h^{i/s}h' \in H \cap C = 1$.

Thus $H' \cap C = 1$ and $H' > H$ contradicting the choice of $H$.

Hence $HC = G$ and $G \cong C \times H$. Since $H \cap C = 1$, if $h \in H$ is of order $d'$ then the order of $xh$ is lcm$(d,d')$. But by the choice of $C$ this is $\leq d$. Hence $d' \mid d$, and so all elements of $H$ have orders dividing $d$. By induction on $|G|$ we can write $H \cong C_{d_2} \times \cdots \times C_{d_r}$, so $G \cong C_{d_1} \times \cdots \times C_{d_r}$ with $d_1 = d$ and $d_{i+1} \mid d_i$ for $i > 1$. But $H$ has an element of order $d_2$ so $d_2 \mid d_1$ as well.

For uniqueness, assume $G \cong C_{d_1} \times \cdots \times C_{d_r} \cong C_1 \times \cdots \times C_{d_r}$. By dropping the requirement that $d_i > 1$ and including $C_1$ factors, we may assume $r = s$. Let $i$ be the smallest integer such that $d_i \neq d_i'$. Consider the subgroup $G^{d_i} = \{g^{d_i} : g \in G\}$. (This is a subgroup since $G$ is abelian.) Now $C_{d_i} \cong C_{d/d_i}$ for $d_i \mid d$ and $C_{d_i} \cong 1$ if $d \nmid d_i$, so $G^{d_i} \cong C_{d_i/d_1} \times \cdots \times C_{d_{i-1}/d_1}$. But $d_j = d_i'$ for $j < i$, so $G^{d_i} \cong C_{d_1/d_i} \times \cdots \times C_{d_{i-1}/d_1} \times H$, where $H = (C_{d_i'/d_i} \times \cdots \times C_{d_r'/d_r})^{d_i}$. By comparing orders, $|H| = 1$, so in particular $d_i' \mid d_i$.

Similarly $d_i \mid d_i'$, so $d_i = d_i'$, contradicting the choice of $i$.

Note that the requirement that $d_{i+1} \mid d_i$ is important for uniqueness. Indeed, $C_r \times C_s \cong C_{rs}$ if gcd$(r, s) = 1$. As a consequence of this, if $d_i = p_1^{a_{i,1}} \cdots p_s^{a_{i,s}}$ is the prime factorization of $d_i$, then $C_{d_i} \cong C_{p_1^{a_{i,1}}} \times \cdots \times C_{p_s^{a_{i,s}}}$. Hence we may write any finite abelian group as

$$G \cong (C_{p_1^{a_{1,1}}} \times C_{p_1^{a_{1,2}}} \times \cdots) \times (C_{p_2^{a_{2,1}}} \times C_{p_2^{a_{2,2}}} \times \cdots) \times \cdots$$

where $a_{i,1} \geq a_{i,2} \geq \cdots \geq 1$ and $p_i$ are distinct primes. This representation is unique up to rearrangement of the $p_i$.

Example: $C_{360} \times C_{24} \times C_2 \cong (C_8 \times C_8 \times C_2) \times (C_9 \times C_3) \times (C_5)$. 

10
A group $F$ is **free** on a subset $S \subseteq F$ if for any group $G$ and any function $\phi: S \rightarrow G$, there exists a unique homomorphism $f: F \rightarrow G$ with $f|_S = \phi$.

**Example:** $(\mathbb{Z}, +)$ is a free group on $S = \{1\}$ with $f(n) = (\phi(1))^n$.

Idea: Existence of $f$ implies that there are no relations between the elements of $S$ which hold in $F$ but do not hold in a general group $G$. Uniqueness of $f$ implies that $F$ is generated by $S$.

The universal property states that any map on $S$ can be extended uniquely to a homomorphism on $F$. Compare this with a basis in a vector space — any map on the basis can be extended uniquely to a linear map on the space.

**Construction:** Let $S$ be a set of symbols and let $T$ be the set of ‘terms’ $\{x, x^{-1} \mid x \in S\}$. Let $W_S = \bigcup_{n=0}^{\infty} T^n$ be the set of all finite ‘words’ or ‘strings’ made up from elements of $T$. We can define multiplication $\star$ on $W_S$ by concatenation. This makes $W_S$ into a monoid with identity equal to the empty string ‘$\varepsilon$’ in $T^0$. However, $W_S$ is not a group since there are no inverses. Somehow we must modify the construction so that ‘$xx^{-1} = 1$’. To do this, define an equivalence relation $\sim$ on $W_S$ as the smallest equivalence relation that makes $sx^a x^{-at}$ equivalent to $st$ for any $s, t \in W_S$, $x \in S$, $a \in \{\pm 1\}$. We check that $s \sim s'$ and $t \sim t'$ imply $s \star t \sim s' \star t'$ so that $\star$ is well defined on $F_S = W_S/\sim$. Since $W_S/\sim$ has inverses, it is a group. Now check the universal property.

**Group presentations:** The group presentation $(S \mid t_i = 1, \; i \in I)$ where $S$ is a set of symbols and $t_i$ are words in $W_S$, is the group $F_S/K$ where $K$ is the smallest normal subgroup of $F_S$ containing (the equivalence classes of) $t_i$ for all $i \in I$. More specifically

$$K = \langle \{zt_i z^{-1} \mid i \in I, \; z \in F_S\} \rangle$$

The group $F_S/K$ is a group generated by $S$ in which the equations $t_i = 1$ hold, and is the largest group for which this is true, as the following lemma shows.

**Lemma 7.1** Let $F_S/K = \langle S \mid t_i = 1, \; i \in I \rangle$ be a group presentation and $G$ a group generated by $S$ in which the equations $t_i = 1$ hold. Then $G$ is isomorphic to a quotient of $F_S/K$.

**Proof.** Define $f: F_S \rightarrow G$ by sending each $x \in S$ to $x \in G$ and extending to a homomorphism by the universal property. Now $f(zt_i z^{-1}) = f(z)f(t_i)f(z)^{-1} = 1$ since $f(t_i) = 1$. Thus ker $f$ contains all $zt_i z^{-1}$, and hence contains $K$. Thus $f$ induces a map $\tilde{f}: F_S/K \rightarrow G$ but $\text{Im } \tilde{f} = \text{Im } f = G$ since $G$ is generated by $S$ and $S \subseteq \text{Im } f$. Thus $G$ is isomorphic to quotient $(F_S/K)/\ker \tilde{f}$.

To show that a group presentation is isomorphic to a given finite group, it is enough to show (a) $G$ is generated by $S$, (b) the equations $t_i = 1$ hold in $G$ and (c) $|F_S/K| \leq |G|$. For (c) one usually shows that every element of $F_S/K$ can be written in one of $|G|$ forms.
An action of a group $G$ on a set $X$ is a binary operation $\cdot : G \times X \to X$ such that

A1. For all $x \in X$, \quad $1 \cdot x = x$,
A2. For all $g, h \in G$, $x \in X$, \quad $(gh) \cdot x = g \cdot (h \cdot x)$.

**Lemma 8.1** An action on $G$ on $X$ defines a homomorphism $\phi : G \to S_X$. Conversely any such homomorphism corresponds to an action of $G$ on $X$.

**Proof.** Let $\phi(g)$ be the map $X \to X$ defined by $\phi(g)(x) = g \cdot x$. A2 implies $\phi(gh) = \phi(g) \circ \phi(h)$ and A1 implies that $\phi(1) = 1_X$ is the identity map on $X$. Hence $\phi(g) \phi(g^{-1}) = \phi(g^{-1}) \phi(g) = \phi(1) = 1_X$ and so $\phi(g^{-1})$ is a two sided inverse for $\phi(g)$. Therefore $\phi(g) \in S_X$ is a permutation and $\phi$ is a homomorphism $G \to S_X$ since $\phi(gh) = \phi(g) \phi(h)$.

Conversely, if $\phi : G \to S_X$ is a homomorphism, define $g \cdot x = \phi(g)x$. Conditions A1 and A2 follow since $1 \cdot x = \phi(1)x = 1_X(x) = x$ and $(gh) \cdot x = \phi(gh)x = \phi(g(\phi(h)(x))) = g \cdot (h \cdot x)$.

An action is called faithful or effective if for all $g \neq 1$ there exists and $x$ with $g \cdot x \neq x$. Equivalently, $\phi$ is injective.

**Examples**

1. $S_n$ acts naturally on $\{1, \ldots, n\}$. In this case $\phi$ is the identity.
2. Matrix groups $GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$, etc., act on the set of vectors $\mathbb{R}^n$ by matrix multiplication.
3. $G$ acts on $X = G$ by left multiplication $g \cdot x = gx$. [Recall the proof of Cayley’s Theorem from Section 4.]
4. $G$ acts on $X = \{\text{subsets of } G\}$ by left multiplication $g \cdot S = gS$. If $H \leq G$ then $G$ acts on the set of left cosets $X = G/H$ by $g \cdot xH = gxH$.
5. $G$ acts on $X = G$ by conjugation $g \cdot x = gxg^{-1}$ [Note: it is important here to use $gxg^{-1}$, not $g^{-1}xg$.]
6. $G$ acts on $X = \{\text{subsets of } G\}$ by conjugation $g \cdot S = gSg^{-1}$. If $H \leq G$ then $G$ acts on $X = \{\text{conjugates } xHx^{-1} \text{ of } H\}$ by $g \cdot xHx^{-1} = (gx)H(gx)^{-1}$.

The orbit of $x \in X$ under the action of $G$ is the set of elements $x$ is mapped to, i.e., $\text{Orb}_G(x) = \{g \cdot x : g \in G\}$. The Stabilizer of $x \in X$ is the subset of $G$ that fixes $x$, $\text{Stab}_G(x) = \{g \in G : g \cdot x = x\}$.

Note: Both $\text{Stab}_G(x)$ and $\text{Orb}_G(x)$ depend very much on $x \in X$ (for a good example, consider the action of $D_3$, as a subgroup of $GL_2(\mathbb{R})$, acting on the plane $\mathbb{R}^2$.)
Lemma 8.2 The orbits of any action of $G$ on $X$ form a partition of $X$.

Proof. Define a relation $x \sim y$ iff $\exists g : g \cdot x = y$. It can be checked that this is an equivalence relation and the orbits are precisely the equivalence classes. \qed

An action is transitive iff $\text{Orb}_G(x) = X$ for some (and hence all) $x \in X$.

Theorem (Orbit-Stabilizer Theorem) For any action of $G$ on $X$, $\text{Stab}_G(x)$ is a subgroup of $G$ and $|G : \text{Stab}_G(x)| = |\text{Orb}_G(x)|$.

Proof. Proof that $H = \text{Stab}_G(x) \leq G$ is standard. For the second part consider the map $\phi : G \to \text{Orb}_G(x)$ given by $\phi(g) = g \cdot x$. By definition of $\text{Orb}_G(x)$, $\phi$ is surjective. Also $\phi(g) = \phi(h)$ holds iff $g \cdot x = h \cdot x$ which holds iff $\exists h^{-1}g \cdot x = x$ or $h^{-1}g \in H$. Thus $\phi(g) = \phi(h)$ iff $gH = hH$. Thus there is a bijection between the left cosets of $H$ and $\text{Orb}_G(x)$. \qed

Examples

1. If $G$ acts on $X$ by conjugation $g \cdot x = gxg^{-1}$ then $\text{Orb}_G(x)$ is the conjugacy class $C_x$ of $x$ and $\text{Stab}_G(x)$ is the centralizer of $x$, $C_G(x)$. In particular $|C_x| = |G : G_G(x)|$, so the size of any conjugacy class divides $|G|$.

2. If $G$ acts on the conjugates of $H \leq G$ by conjugation, then the stabilizer of $H$ is $N_G(H)$ and the action is transitive. Hence the number of conjugates of $H$ in $G$ is $[G : N_G(H)]$. In particular it is a factor of $[G:H]$.

Lemma 8.3 If $p$ is a prime and $p | |G|$ then $G$ contains an element of order $p$.

Proof. Let $X = \{(g_1, \ldots, g_p) \mid g_1g_2\cdots g_p = 1\} \subseteq G^p$ and let $\mathbb{Z}/p\mathbb{Z}$ act on $X$ by cyclically permuting the coordinates: $i \cdot (g_1, \ldots, g_p) = (g_{i+1}, \ldots, g_p, g_1)$. It is easy to see that the result still lies in $X$ and gives an action of $\mathbb{Z}/p\mathbb{Z}$ on $X$. The orbits are all of size $p$ or 1, with 1 occurring when $g_1 = g_2 = \cdots = g$ with $g^p = 1$. But $|X| = |G|^{p-1}$ since for any choice of $g_1, \ldots, g_{p-1}$ there is a unique $g_p$ with $(g_1, \ldots, g_p) \in X$. Thus $p \mid |X|$, so the number of elements $g$ with $g^p = 1$ is also divisible by $p$. Since $1^p = 1$, there is at least $p$ such elements, and hence some elements of order $p$. \qed

Note that this does not hold in general if $p$ is not prime. Eg., $D_3$ has no element of order 6, $A_3$ has no element of order 30.

Lemma 8.4 If $G$ is a group of order $p^n$, $p$ prime, $n > 0$, then $Z(G) \neq 1$.

Proof. Write $G$ as a union of conjugacy classes $C_x$. Each $|C_x|$ divides $|G|$ so is a power of $p$. Also $|C_x| = 1$ iff $xz^{-1} = x$ for all $z \in G$, which is just the statement that $x \in Z(G)$. Thus $|G| = |Z(G)| + \sum_{|C_x| > 1} |C_x|$ and so $0 \equiv |G| \equiv |Z(G)| + \sum 0 \mod p$. So $p \mid |Z(G)|$ and thus $Z(G) \neq 1$. \qed
Throughout this section, assume $G$ is a finite group.

**Theorem (Sylow 1)** If $p$ is prime and $p^k \mid |G|$ then $G$ contains a subgroup of order $p^k$.

*Proof.* Induction on $|G|$. If $k = 0$ then the result is clear, hence we may assume $p \mid |G|$ and the result holds for smaller groups. Use the action of $G$ on $G$ by conjugation to write $|G| = \sum |\text{Orb}_G(x)| = |Z(G)| + \sum_{|C_x| > 1} |C_x|$. Since $|G| \equiv 0 \mod p$, either $p \mid |Z(G)|$ or $p \nmid |C_x|$ for some $x \notin Z(G)$. In the second case $|C_x| = [G:C_G(x)] = |G|/|C_G(x)|$, so $p^k \mid |C_G(x)|$. But $C_G(x) \lhd G$ since $x \notin Z(G)$, so by induction there is a subgroup $H \leq C_G(x)$ with order $p^k$. In the first case $p \mid |Z(G)|$. Now $Z(G)$ has an element of order $p$, thus there exists a normal subgroup $C \leq G$ with $|C| = p$ (normal since $C \leq Z(G)$). Now by induction $G/C$ contains a subgroup $H/C$ of order $p^{k-1}$, which corresponds by the 2nd isomorphism theorem to a subgroup $H \leq G$ of order $p^k$. □

A $p$-**group** is a group in which every element has order a power of $p$. For a finite group this is equivalent to $|G| = p^k$ for some $k$. A $p$-**Sylow subgroup** of a finite group $G$ is a $p$-subgroup $P \leq G$ with $p \nmid |G:P|$. Equivalently, $|P| = p^k$ with $p^k$ being the largest power of $p$ dividing $|G|$.

**Lemma 9.1** If $H$ is a $p$-subgroup of $G$ and $P$ is a $p$-Sylow subgroup of $G$ with $H \leq N_G(P)$, then $H \leq P$.

*Proof.* By assumption $H \leq N_G(P)$ and by definition of $N_G(P)$, $P \leq N_G(P)$. Therefore by the 3rd Isomorphism Theorem, $HP/P \cong H/(H \cap P)$. But $|P|$ is the maximal power of $p$ dividing $|G|$ and $|HP| \mid |G|$, so $p \nmid |HP| / |P| = |HP/P|$. On the other hand $|H/(H \cap P)|$ is a power of $p$ since $H$ (and hence $H/(H \cap P)$ is a $p$-group. Therefore $H/(H \cap P) = 1$ and so $H \leq P$. □

**Theorem (Sylow 2)** If $P$ is a $p$-Sylow subgroup of $G$ and $H$ is any $p$-subgroup of $G$ then $H$ is a subgroup of some conjugate of $P$. In particular, any two $p$-Sylow subgroups are conjugate.

*Proof.* Let $X = \{xp^{-1} \mid x \in G\}$ be the set of conjugates of $P$ and let $G$ act on $X$ by conjugation. The action of $G$ is transitive, so $|X| = |\text{Orb}_G(P)| = [G:\text{Stab}_G(P)] = [G:N_G(P)] = |G|/|N_G(P)|$. But $P \leq N_G(P)$, so $|X|$ divides $|G|/|P|$. Thus $|X| \neq 0 \mod p$. Now restrict the action to one of $H$ on $X$. At least one of the orbits $\text{Orb}_H(P')$, $P' \in X$, must have size not divisible by $p$. But $|\text{Orb}_H(P')| = [H:\text{Stab}_H(P')]$ divides $|H|$ which is a power of $p$. Thus $\text{Orb}_H(P') = \{P'\}$ and so $H \leq N_G(P')$. By Lemma 9.1, $H \leq P'$, where $P' \in X$ is a conjugate of $P$. □

**Theorem (Sylow 3)** The number $n_p$ of $p$-Sylow subgroups of $G$ is equivalent to $1 \mod p$ and divides $|G|/|P|$.

*Proof.* Use the action of $P$ on $X = \{xp^{-1} \mid x \in G\}$ by conjugation. $\text{Orb}_P(P) = \{P\}$ has size 1. But for $P' \neq P$, $P \nleq P'$. Thus by Lemma 9.1, $P \nleq N_G(P')$, so
Orb\(_{p}(P') \neq \{P'\} \). But \(|\text{Orb}_p(P')|\) is a factor of \(|P|\), so is divisible by \(p\). Hence \(n_p = |X| = |\text{Orb}_p(P)| + \sum_{p \neq p} |\text{Orb}_p(P')| \equiv 1 \mod p\). For the last part, \(|X| = |\text{Orb}_G(P)| = [G: \text{Stab}_G(P)] \) divides \(|G|\). But \(|X|\) is relatively prime to \(p\), so \(|X|\) divides \(|G|/p^k\). \(\square\)

**Example** Suppose \(|G| = 28\), then \(n_7 \equiv 1 \mod 7\) and \(n_7 | 28/7 = 4\). Hence \(n_7 = 1\). But then all conjugates of a 7-Sylow subgroup \(P\) are equal to \(P\) and thus \(P \trianglelefteq G\). Hence \(G\) has a normal subgroup of order 7.

**Example** Suppose \(|G| = 56\), then \(n_7 \equiv 1 \mod 7\) and \(n_7 | 56\). Hence \(n_7 \in \{1, 8\}\). If \(n_7 = 8\) then there are 8 7-Sylow subgroups \(P_1, \ldots, P_8\) each of which is cyclic of order 7. But \(P_i \cap P_j < P_i\), so \(P_i \cap P_j = \{1\}\) for \(i \neq j\). Thus the sets \(P_i \setminus \{1\}\) are disjoint and there are a total of (at least) \(8 \times 6 = 48\) elements of \(G\) of order 7. But this gives only 8 remaining elements. Since 2-Sylow subgroups have order 8, there can only be one 2-Sylow subgroup. Hence \(G\) either has a normal subgroup of order 7 (when \(n_7 = 1\)) or it has a normal subgroup of order 8 (when \(n_7 = 8\)). In particular \(G\) is not simple.

**Lemma 9.2** If \(|G| = 60\) and \(G\) is simple, then \(G \cong A_5\).

*Proof.* Assume first that \(G\) has a subgroup \(H\) of index \(2 \leq m \leq 5\). Then \(G\) acts of the left cosets \(X = \{xH \mid x \in G\}\) by left multiplication. This gives a homomorphism \(\phi: G \to S_m\). Let \(K = \ker \phi\). Then \(K \leq G\), so either \(K = 1\) or \(K = G\). But the action of \(G\) is not trivial (it is transitive on \(X\)), so \(K \neq G\). Hence \(K = 1\) and \(G\) is isomorphic to a subgroup of \(S_m\), \(m \leq 5\). Since \(|G| = 60\), \(m = 5\) and \(G \leq S_5\). But then \(G \cap A_5 \leq G\) and \([G:G \cap A_5] = [GA_5:A_5] \leq 2\), so \(|G \cap A_5| \geq 60/2 > 1\) and so \(G \cap A_5 = G\). Hence \(G \leq A_5\), so \(G = A_5\). Hence we may now assume \(G\) has no proper subgroup of index \(\leq 5\).

Count the number of \(p\)-Sylow subgroups for \(p = 2, 3, 5\).

\[
\begin{align*}
n_2 &\equiv 1 \mod 2, \quad n_2 | 15 \implies n_2 \in \{1, 3, 5, 15\} \\
n_3 &\equiv 1 \mod 3, \quad n_3 | 20 \implies n_3 \in \{1, 4, 10\} \\
n_5 &\equiv 1 \mod 5, \quad n_5 | 12 \implies n_5 \in \{1, 6\}
\end{align*}
\]

If \(n_p = 1\) then the \(p\)-Sylow subgroup \(P\) is normal in \(G\). If \(2 \leq n_p \leq 5\) then \(N_G(P)\) has index \(n_p \leq 5\) in \(G\). Hence we may assume \(n_2 = 15, n_3 = 10, n_5 = 6\).

Using \(n_3 = 6\) we have 6 subgroups \(P_1, \ldots, P_6\), each of order 5 and \(P_i \cap P_j = \{1\}\). Thus there are \(6 \times 4 = 24\) non-identity elements in \(\bigcup P_i\), each of order 5.

Using \(n_3 = 10\), a similar argument gives 10 \(\times 2 = 20\) elements of order 3.

Using \(n_5 = 12\) we must be a bit more careful since \(P_i \cap P_j\) does not have to be trivial. Let \(P_i\) and \(P_j\) be two distinct 2-Sylow subgroups (of order 4) and \(F = \langle P_i, P_j \rangle\). Then \(4 < |F| \leq |G| = 60\), so \(|F| \in \{12, 20, 60\}\). Since we may assume \(G\) has no subgroup of index \(2 \leq [G:F] \leq 5\), we have \(F = G\). Now if \(|P_i \cap P_j| = 2\) then \(P_i \cap P_j\) is normal in both \(P_i\) and \(P_j\) (index 2) and so in \(F\), contradicting simplicity of \(F = G\). Thus \(P_i \cap P_j = 1\) and we get \(15 \times 3 \times 4 = 45\) elements of order 2 or 4.

The total number of elements of \(G\) accounted for so far is \(1 + 24 + 20 + 45 > 60\), a contradiction. Thus \(G \cong A_5\). \(\square\)
A subnormal series of a group $G$ is a sequence of subgroups

$$1 = G_n \trianglelefteq \cdots \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0 = G,$$

with $G_n = 1$, $G_0 = G$ and $G_i \trianglelefteq G_{i-1}$ for all $i$. A normal series is a subnormal series in which each $G_i$ is normal in $G$ (not just in $G_{i-1}$). A composition series is a subnormal series in which each quotient $G_{i-1}/G_i$ is simple, or equivalently (by the 2nd Isomorphism Theorem) it is a subnormal series in which $G_{i-1} \neq G_i$ and which cannot be ‘refined’ by inserting any additional groups: $G_i \triangleleft H \triangleleft G_{i-1}$.

Note: All finite groups must have a composition series (take $G_i$ to be any maximal proper normal subgroup of $G_{i-1}$ and note that eventually $G_n = 1$), however infinite groups do not necessarily have one. For example, $\mathbb{Z}$ has no composition series. Simple groups $G$ have only one composition series: $1 \triangleleft G$.

**Example** 1 $\triangleleft V \triangleleft A_4 \triangleleft S_4$ is a normal series but not a composition series. It can be refined to $1 \triangleleft \{1, (12)(34)\} \triangleleft V \triangleleft A_4 \triangleleft S_4$ which is a composition series, but is not normal.

**Example** 1 $\triangleleft C_2 \triangleleft C_6$ and 1 $\triangleleft C_3 \triangleleft C_6$ are two different composition series. The factor groups are $C_2$ and $C_3$ for both, but occur in a different order. For $S_4$ however, all composition series have factors $C_2, C_2, C_3, C_2$ in that order.

**Theorem (Jordan-Hölder)** All composition series of a finite group $G$ have the same composition factors (up to isomorphism) with the same multiplicities.

**Proof.** We prove the result by induction on $|G|$, $|G| = 1$ being trivial. Suppose we have two composition series $1 \triangleleft \cdots \triangleleft G_1 \triangleleft G$ and $1 \triangleleft \cdots \triangleleft H_1 \triangleleft G$. If $H_1 = G_1$ then we are done by induction (applied to $G_1$). Hence we may assume $H_1 \neq G_1$. Let $1 \triangleleft \cdots \triangleleft K_1 \triangleleft G_1 \cap H_1$ be any composition series of $G_1 \cap H_1$. Now consider the following four series.

$$
1 \triangleleft \ldots \triangleleft G_3 \triangleleft G_2 \triangleleft G_1 \triangleleft G \\
1 \triangleleft \ldots \triangleleft K_1 \triangleleft G_1 \cap H_1 \triangleleft G_1 \triangleleft G \\
1 \triangleleft \ldots \triangleleft K_1 \triangleleft G_1 \cap H_1 \triangleleft H_1 \triangleleft G \\
1 \triangleleft \ldots \triangleleft H_3 \triangleleft H_2 \triangleleft H_1 \triangleleft G
$$

Since $H_1 \neq G_1$ we may assume $H_1 \ntriangleleft G_1$. Now $H_1, G_1 \trianglelefteq G$, so $G_1 \triangleleft H_1G_1 \trianglelefteq G$. Since (1) is a composition series, $H_1G_1 = G$. Thus by the 3rd Isomorphism Theorem $G/G_1 \cong H_1/(G_1 \cap H_1)$ and $G/H_1 \cong G_1/(G_1 \cap H_1)$. Thus both (2) and (3) have all their factors simple, and so are composition series for $G$. Moreover their factors are the same up to isomorphism. Now (1) and (2) have the same factors by induction applied to $G_1$, and (3) and (4) have the same factors by induction applied to $H_1$. Thus (1) and (4) have the same factors. 

**Exercise:** Show that all the composition factors of a finite $p$-group are isomorphic to $C_p$. 

16
A group $G$ is **solvable** if it has a subnormal series $1 \leq G_n \leq \cdots \leq G_1 \leq G_0 = G$ where each quotient $G_{i-1}/G_i$ is an abelian group. We will call this a solvable series.

Any abelian group is solvable even if it is infinite. Another interesting example is $S_4$ which has the solvable series $1 \leq V \leq A_4 \leq S_4$. However $S_5$ is not solvable. Indeed $1 < A_5 < S_5$ is a composition series with an $A_5$ factor. Thus by Jordan-Hölder, every composition series, including one obtained by refining a solvable series would contain an $A_5$ factor, which is impossible since $A_5$ is not abelian. Indeed, for a finite group $G$, $G$ is solvable if and only if all its composition factors are cyclic of prime order. In particular, all finite $p$-groups are solvable.

Recall the commutator subgroup $G' = \langle \{xyx^{-1}y^{-1} : x, y \in G\} \rangle$ of $G$. We note that $G' \trianglelefteq G$ and for any $K \trianglelefteq G$, $G/K$ is abelian iff $K \supseteq G'$. Moreover, it is clear that if $H \leq G$ then $H' \leq G'$.

The $n$’th derived subgroup of $G$ is defined inductively by $G^{(0)} = G$ and $G^{(n+1)} = (G^{(n)})'$. As a result we obtain the **derived** series of $G$:

$$\cdots \leq G^{(2)} \leq G^{(1)} \leq G^{(0)} = G.$$

Note that this series may not reach 1. For example $A_5' = A_5$, so for $G = S_5$ the series is $\cdots \leq A_5 \leq A_5 \leq A_5 \leq S_5$.

**Lemma 11.1** A group $G$ is solvable if and only if $G^{(n)} = 1$ for some $n$.

**Proof.** If $G^{(n)} = 1$ then $1 = G^{(n)} \leq \cdots \leq G^{(1)} \leq G$ is a solvable series for $G$. Conversely, we shall show that if $1 = G_n \leq \cdots \leq G_1 \leq G$ is a solvable series then $G^{(i)} \leq G_i$, so in particular $G^{(n)} \leq G_n = 1$. We prove this by induction on $i$. For $i = 0$, $G^{(0)} = G_0 = G$. For $i > 0$, $G^{(i)} = (G^{(i-1)})' \leq (G_{i-1})'$, but $G_{i-1}' \leq G_i$ since $G_{i-1}/G_i$ is abelian. \hfill \Box

Note that $G^{(n)} \leq G$, so the derived series of a solvable group is in fact a normal series.

**Lemma 11.2** Let $H \leq G$ and $K \trianglelefteq G$.

1. If $G$ is solvable then $H$ is solvable.

2. If $G$ is solvable then $G/K$ is solvable.

3. If $K$ and $G/K$ are both solvable then $G$ is solvable.

**Proof.** 1. $H^{(n)} \leq G^{(n)}$. 2. $(G/K)^{(n)} = G^{(n)}K/K$. 3. Take a solvable series $K/K \leq \cdots \leq G_2/K \leq G_1/K \leq G/K$ for $G/K$ and $1 \leq \cdots \leq K_2 \leq K_1 \leq K$ and put them together to form $1 \leq \cdots \leq K_2 \leq K_1 \leq K \leq \cdots \leq G_2 \leq G_1 \leq G$. This is a solvable series since $G_i/G_{i-1} \cong (G_i/K)/(G_{i-1}/K)$ is abelian. \hfill \Box