# Abstract Algebra I

**George Voutsadakis**[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 341

Subsection 1

# Definition and Examples

# Subgroups

- Basic methods for studying the structure of groups include
  - studying subsets of a group which also satisfy the group axioms, called subgroups;
  - studying quotients of groups, created by collapsing one group onto a smaller group.

## Definition (Subgroup)

Let $G$ be a group. The subset $H$ of $G$ is a **subgroup** of $G$ if $H$ is nonempty and $H$ is closed under products and inverses, i.e., $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$. If $H$ is a subgroup of $G$, we write $H \leq G$.

- Subgroups of $G$ are just subsets of $G$ which are themselves groups with respect to the operation defined in $G$, i.e., the binary operation on $G$ restricts to give a binary operation on $H$ which is:
  - associative,
  - has an identity in $H$,
  - has inverses in $H$, for all the elements of $H$.

# The Operation of a Subgroup

- $H$ being a subgroup of $G$ means that the operation for the group $H$ is the operation on $G$ restricted to $H$.
- Care is needed because, in general, it is possible that the subset $H$ has the structure of a group with respect to some operation other than the operation on $G$ restricted to $H$.
- The operation for $G$ and the operation for the subgroup $H$ will be denoted by the same symbol.
- If $H \leq G$ and $H \neq G$, we write $H < G$.

# Identities and Inverses in Subgroups

- If $H$ is a subgroup of $G$ then, since the operation for $H$ is the operation for $G$ restricted to $H$, any equation in the subgroup $H$ may also be viewed as an equation in the group $G$.
  - Claim: The identity for $H$ is the same as the identity of $G$.
    $H \neq \emptyset$ by definition. Suppose $g \in H$. Since $H$ is a subgroup, $g^{-1} \in H$.
    Therefore, again since $H$ is a subgroup, $1 = gg^{-1} \in H$.
    Thus, every subgroup must contain 1, the identity of $G$.
  - Claim: The inverse of an $x$ in $H$ is the same as the inverse of $x$ in $G$, whence the notation $x^{-1}$ is unambiguous.
    Suppose that $y$ is the inverse of $x$ in $H$ and $x^{-1}$ its inverse in $G$. Then, since 1 is the identity in both $G$ and $H$, we have $xy = 1 = xx^{-1}$.
    Canceling $x$ on the left in $G$, we get $y = x^{-1}$. Thus, the inverse of $x$ in $H$ is the same as the inverse of $x$ in $G$.

# Examples of Subgroups

(1) $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ with the operation of addition.

(2) Any group $G$ has two subgroups: $H = G$ and $H = \{1\}$; the latter is called the **trivial subgroup** and is denoted by 1.

(3) If $G = D_{2n}$ is the dihedral group of order $2n$, let

$$H = \{1, r, r^2, \ldots, r^{n-1}\},$$

the set of all rotations in $G$. Since the product of two rotations is again a rotation and the inverse of a rotation is also a rotation, $H$ is a subgroup of $D_{2n}$ of order $n$.

(4) The set of even integers is a subgroup of the group of all integers under addition.

# Examples of Subset Groups that are Not Subgroups

(1) $\mathbb{Q} - \{0\}$ under multiplication is not a subgroup of $\mathbb{R}$ under addition even though both are groups and $\mathbb{Q} - \{0\}$ is a subset of $\mathbb{R}$. The operation of multiplication on $\mathbb{Q} - \{0\}$ is not the restriction of the operation of addition on $\mathbb{R}$.

(2) $\mathbb{Z}^+$ under addition is not a subgroup of $\mathbb{Z}$ under addition because:

- although $\mathbb{Z}^+$ is closed under $+$, it does not contain the identity 0 of $\mathbb{Z}$;
- although each $x \in \mathbb{Z}^+$ has an additive inverse, $-x$ in $\mathbb{Z}$, $-x \notin \mathbb{Z}^+$, i.e., $\mathbb{Z}^+$ is not closed under the operation of taking inverses.

(3) For analogous reasons, $(\mathbb{Z} - \{0\}, \times)$ is not a subgroup of $(\mathbb{Q} - \{0\}, \times)$.

(4) $D_6$ is not a subgroup of $D_8$ since the former is not even a subset of the latter.

# Transitivity of the "is a subgroup of" Relation

Claim: The relation "is a subgroup of", i.e., $\leq$, is transitive:
If $H$ is a subgroup of a group $G$ and $K$ is a subgroup of $H$, then $K$ is also a subgroup of $G$. In symbols,

$$H \leq G \quad \text{and} \quad K \leq H \quad \text{imply} \quad K \leq G.$$

Suppose $H \leq G$ and $K \leq H$.

Let $k \in K$. Then the inverse of $k$ in $H$ is in $K$, since $K \leq H$. But this same element is also the inverse of $k$ in $G$, since $H \leq G$.

Let $k_1, k_2 \in K$. Then the product $k_1 \cdot_H k_2 \in K$, since $K \leq H$. But the operation $\cdot_H$ is the same as the operation $\cdot$ in $G$, since $H \leq G$. Therefore, $k_1 \cdot k_2 \in K$.

Since $K$ is closed under inverses and multiplication in $G$, we get that $K \leq G$.

# The Subgroup Criterion

**Proposition (The Subgroup Criterion)**

A subset $H$ of a group $G$ is a subgroup if and only if

(1) $H \neq \emptyset$;

(2) For all $x, y \in H$, $xy^{-1} \in H$.

Furthermore, if $H$ is finite, then it suffices to check that $H$ is nonempty and closed under multiplication.

- Suppose $H$ is a subgroup of $G$.
  (1) Since $H$ contains the identity of $G$, $H \neq \emptyset$.
  (2) If $x, y \in H$, by the subgroup property, $y^{-1} \in H$. Since $x, y^{-1} \in H$, by the subgroup property $xy^{-1} \in H$.

# The Proof of the Subgroup Criterion

- We show, conversely, that if $H$ satisfies (1) and (2), then $H \leq G$:
  - Let $x$ be any element in $H \neq \emptyset$. Let $y = x$ and apply Property (2) to get $1 = xx^{-1} \in H$. So $H$ contains the identity of $G$.
  - Then, again by (2), since $H$ contains 1 and $x$, $H$ contains the element $1x^{-1} = x^{-1}$, i.e., $H$ is closed under taking inverses.
  - Finally, if $x$ and $y$ are any two elements of $H$, then $H$ contains $x$ and $y^{-1}$, whence, by (2), $H$ also contains $x(y^{-1})^{-1} = xy$. Hence $H$ is also closed under multiplication.

  Thus, $H$ is a subgroup of $G$.
- Suppose now that $H$ is finite and closed under multiplication. Let $x$ be any element in $H$. Then there are only finitely many distinct elements among $x, x^2, x^3, \ldots$. So $x^a = x^b$, for some integers $a, b$ with $b > a$. If $n = b - a$, then $x^n = 1$. In particular, every element $x \in H$ is of finite order. Then $x^{n-1} = x^{-1}$ is an element of $H$, and $H$ is automatically also closed under inverses.

# Orbits of an Action

## Theorem

Let $H$ be a group acting on a set $A$. The relation $\sim$ on $A$ defined by

$$a \sim b \quad \text{iff} \quad a = hb, \text{ for some } h \in H,$$

is an equivalence relation.

- Reflexivity: $1 \in H$ and $a = 1a$, for all $a \in A$, whence $a \sim a$.
- Symmetry: Assume $a \sim b$. Then, there exists $h \in H$, such that $a = hb$. Since $H$ is a group, $h^{-1} \in H$. We have $b = 1b = (h^{-1}h)b = h^{-1}(hb) = h^{-1}a$. Therefore, $b \sim a$.
- Transitivity: Assume $a \sim b$ and $b \sim c$. Then, there exist $h_1, h_2 \in H$, such that $a = h_1 b$ and $b = h_2 c$. Since $H$ is a group, $h_1 h_2 \in H$. We have $a = h_1 b = h_1(h_2 c) = (h_1 h_2)c$. Thus, $a \sim c$.
- The equivalence class of $x \in A$ under $\sim$ is called the **orbit** of $x$.

## Corollary

The orbits under the action of $H$ form a partition of $A$.

# Lagrange's Theorem

## Proposition

Let $H$ be a subgroup of a finite group $G$. Let $H$ act on $G$ by left multiplication. If $x \in G$ and $\mathcal{O}_x$ is the orbit of $x$ under the action of $H$, then the map $f_x : H \to \mathcal{O}_x$ defined by $f_x(h) = hx$, for all $h \in H$, is a bijection.

- If $y \in \mathcal{O}_x$, then, there exists an $h \in H$, such that $y = hx = f_x(h)$. Thus, $f_x$ is surjective. If $f_x(h_1) = f_x(h_2)$, then $h_1x = h_2x$. By right-cancelation in $G$, $h_1 = h_2$. Thus, $f_x$ is also injective.

## Theorem (Lagrange's Theorem)

If $G$ is a finite group and $H \leq G$, then $|H| \mid |G|$.

- By the preceding corollary, $\{\mathcal{O}_x : x \in G\}$ is a partition of $G$. By the preceding proposition $|\mathcal{O}_x| = |H|$, for all $x \in G$. Thus, $G = |\{\mathcal{O}_x : x \in G\}| \cdot |H|$ and, therefore, $|H| \mid |G|$.

Subsection 2

# Centralizers, Normalizers, Stabilizers and Kernels

# Centralizers

- Let $A$ be any nonempty subset of a group $G$.

## Definition (Centralizer)

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

Claim: $C_G(A)$ is a subgroup of $G$.

- Since $1a = a1 = a$, for all $a \in G$, we have $1 \in C_G(A)$. So, $C_G(A) \neq \emptyset$.
- Assume $x \in C_G(A)$. Then, for all $a \in A$, $xax^{-1} = a$. By multiplying on the left by $x^{-1}$, then on the right by $x$, we get $a = x^{-1}ax$, i.e., $x^{-1} \in C_G(A)$. Thus, $C_G(A)$ is closed under taking inverses.
- Assume $x, y \in C_G(A)$. Then, for all $a \in A$, $xax^{-1} = a$ and $yay^{-1} = a$. Now $(xy)a(xy)^{-1} = (xy)a(y^{-1}x^{-1}) = x(yay^{-1})x^{-1} = xax^{-1} = a$, whence $xy \in C_G(A)$ and $C_G(A)$ is closed under products.

Thus $C_G(A) \leq G$.

- If $A = \{a\}$, we write simply $C_G(a)$ instead of $C_G(\{a\})$.

# The Center of a Group

## Definition (The Center)

Define the **center** of a group $G$ to be the set

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

So $Z(G)$ is the set of elements commuting with all the elements of $G$.

- Note that $Z(G) = C_G(G)$.

  So the argument in the preceding slide proves $Z(G) \leq G$ as a special case.

# Normalizers

## Definition (Normalizer)

Define $gAg^{-1} = \{gag^{-1} : a \in A\}$. The **normalizer** of $A$ in $G$ is the set

$$N_G(A) = \{g \in G : gAg^{-1} = A\}.$$

Claim: The normalizer $N_G(A)$ of $A \subseteq G$ is a subgroup of $G$.

- Since $1A1^{-1} = \{1a1^{-1} : a \in A\} = \{a : a \in A\} = A$, we have $1 \in N_G(A)$. So, $N_G(A) \neq \emptyset$.
- Assume $x \in N_G(A)$. Then, $xAx^{-1} = A$. By multiplying on the left by $x^{-1}$, then on the right by $x$, we get $A = x^{-1}Ax$, i.e., $x^{-1} \in N_G(A)$. Thus, $N_G(A)$ is closed under taking inverses.
- Assume $x, y \in N_G(A)$. Then, $xAx^{-1} = A$ and $yAy^{-1} = A$. Now $(xy)A(xy)^{-1} = (xy)A(y^{-1}x^{-1}) = x(yAy^{-1})x^{-1} = xAx^{-1} = A$, whence $xy \in N_G(A)$ and $N_G(A)$ is closed under products.

Thus $N_G(A) \leq G$.

- Notice that, if $g \in C_G(A)$, then $gag^{-1} = a \in A$, for all $a \in A$, so $C_G(A) \leq N_G(A)$.

# Examples I

(1) If $G$ is abelian then all the elements of $G$ commute, so $Z(G) = G$. Similarly, $C_G(A) = N_G(A) = G$, for any subset $A$ of $G$, since $gag^{-1} = gg^{-1}a = a$, for every $g \in G$ and every $a \in A$.

(2) Let $G = D_8$ be the dihedral group of order 8 with the usual generators $r$ and $s$ and let $A = \{1, r, r^2, r^3\}$ be the subgroup of rotations in $D_8$. We show that $C_{D_8}(A) = A$.

- Since all powers of $r$ commute with each other, $A \subseteq C_{D_8}(A)$.
- Since $sr = r^{-1}s \neq rs$, the element $s$ does not commute with all members of $A$, i.e., $s \notin C_{D_8}(A)$. Finally, the elements of $D_8$ that are not in $A$ are all of the form $sr^i$, for some $i \in \{0, 1, 2, 3\}$. If the element $sr^i$ were in $C_{D_8}(A)$, then, since $C_{D_8}(A)$ is a subgroup which contains $r$, we would also have the element $s = (sr^i)(r^{-i})$ in $C_{D_8}(A)$, a contradiction.

This shows $C_{D_8}(A) = A$.

# Examples II

(3) Let again $G = D_8$ and let $A = \{1, r, r^2, r^3\}$. We show that $N_{D_8}(A) = D_8$.

Since, in general, the centralizer of a subset is contained in its normalizer, $A \subseteq N_{D_8}(A)$. Next compute

$$sAs^{-1} = \{s1s^{-1}, srs^{-1}, sr^2s^{-1}sr^3s^{-1}\} = \{1, r^3, r^2, r\} = A,$$

so that $s \in N_{D_8}(A)$.

Note that the set $sAs^{-1}$ equals the set $A$ even though the elements in these two sets appear in different orders, indicating that $s$ is in the normalizer of $A$ but not in the centralizer of $A$.

Since both $r$ and $s$ belong to the subgroup $N_{D_8}(A)$, $s^i r^j \in N_{D_8}(A)$, for all integers $i$ and $j$, so, since $r$ and $s$ generate $D_8$, every element of $D_8$ is in $N_{D_8}(A)$. Since $D_8 \leq N_{D_8}(A)$, we have $N_{D_8}(A) = D_8$.

# Examples III

(4) We show that the center of $D_8$ is the subgroup $\{1, r^2\}$.

Since $Z(G) \leq C_G(A)$, for any subset $A$ of $G$, by Example (2), $Z(D_8) \leq C_{D_8}(A) = A$, where $A = \{1, r, r^2, r^3\}$. The calculation in Example (2) shows that $r$ and similarly $r^3$ are not in $Z(D_8)$, so $Z(D_8) \leq \{1, r^2\}$.

Since $r$ commutes with $r^2$ and $s$ also commutes with $r^2$ and they generate $D_8$, every element of $D_8$ commutes with $r^2$ (and 1), hence $\{1, r^2\} \leq Z(D_8)$.

# Examples IV

(5) Let $G = S_3$ and let $A$ be the subgroup $\{1, (1\ 2)\}$. We show that $C_{S_3}(A) = N_{S_3}(A) = A$.

One can compute directly that $C_{S_3}(A) = A$.

Alternatively, since an element commutes with its powers, $A \leq C_{S_3}(A)$. By Lagrange's Theorem, the order of the subgroup $C_{S_3}(A)$ of $S_3$ divides $|S_3| = 6$. Also by Lagrange's Theorem applied to the subgroup $A$ of the group $C_{S_3}(A)$, we have that $2 \mid |C_{S_3}(A)|$. The only possibilities are: $|C_{S_3}(A)| = 2$ or 6. If the latter occurs, $C_{S_3}(A) = S_3$, i.e., $A \leq Z(S_3)$. This is a contradiction because $(1\ 2)$ does not commute with $(1\ 2\ 3)$. Thus $|C_{S_3}(A)| = 2$. So $A = C_{S_3}(A)$.

Next, note that $N_{S_3}(A) = A$ because $\sigma \in N_{S_3}(A)$ if and only if $\{\sigma 1 \sigma^{-1}, \sigma(1\ 2)\sigma^{-1}\} = \{1, (1\ 2)\}$. Since $\sigma 1 \sigma^{-1} = 1$, this equality of sets occurs if and only if $\sigma(1\ 2)\sigma^{-1} = (1\ 2)$ as well, i.e., if and only if $\sigma \in C_{S_3}(A)$.

Finally, $Z(S_3) = \{1\}$, since $Z(S_3) \leq C_{S_3}(A) = A$ and $(1\ 2) \notin Z(S_3)$.

# Stabilizers

- If $G$ is a group acting on a set $S$ and $s$ is some fixed element of $S$, the **stabilizer** of $s$ in $G$ is the set

$$G_s = \{g \in G : g \cdot s = s\}.$$

Claim: $G_s \leq G$.

- First, $1 \in G_s$, since $1 \cdot s = s$.
- If $y \in G_s$, $s = 1 \cdot s = (y^{-1}y) \cdot s = y^{-1} \cdot (y \cdot s) = y^{-1} \cdot s$, so $y^{-1} \in G_s$ as well.
- Finally, if $x, y \in G_s$, then $(xy) \cdot s = x \cdot (y \cdot s) = x \cdot s = s$. So $G_s$ is also closed under multiplication.

This proves $G_s$ is a subgroup of $G$.

# Kernels of Actions

- The **kernel** of the action of $G$ on $S$ is defined as

$$\{g \in G : g \cdot s = s, \text{ for all } s \in S\}.$$

Claim: The kernel of an action is also a subgroup.

Set $K = \{g \in G : g \cdot s = s, \text{ for all } s \in S\}$.

- First, $1 \in K$, since, for all $s \in S$, $1 \cdot s = s$.
- If $y \in K$, then, for all $s \in S$,
  $s = 1 \cdot s = (y^{-1}y) \cdot s = y^{-1} \cdot (y \cdot s) = y^{-1} \cdot s$, so $y^{-1} \in K$ as well.
- Finally, if $x, y \in K$, then, for all $s \in S$, $(xy) \cdot s = x \cdot (y \cdot s) = x \cdot s = s$.
  So $K$ is also closed under multiplication.

This proves $K$ is a subgroup of $G$.

# Examples

(1) The group $G = D_8$ acts on the set $A$ of four vertices of a square.
- The stabilizer of any vertex $a$ is the subgroup $\{1, t\}$ of $D_8$, where $t$ is the reflection about the line of symmetry passing through vertex $a$ and the center of the square.
- The kernel of this action is the identity subgroup since only the identity symmetry fixes every vertex.

(2) The group $G = D_8$ also acts on the set $A$ whose elements are the two unordered pairs of opposite vertices.
- The kernel of the action of $D_8$ on this set $A$ is the subgroup $\{1, s, r^2, sr^2\}$.
- For either element $a \in A$, the stabilizer of $a$ in $D_8$ equals the kernel of the action.

# Special Subgroups as Stabilizers and Kernels of Actions

- Centralizers, normalizers and kernels can be viewed as special cases stabilizers and kernels of actions:
- Let $S = \mathcal{P}(G)$, the collection of all subsets of $G$, and let $G$ act on $S$ by **conjugation**, i.e., for every $g \in G$ and every $B \subseteq G$, let

$$g : B \mapsto gBg^{-1}, \text{ where } gBg^{-1} = \{gbg^{-1} : b \in B\}.$$

  - $N_G(A)$ is precisely the stabilizer of $A$ in $G$, i.e., $N_G(A) = G_s$, where $s = A \in \mathcal{P}(G)$. Thus, $N_G(A)$ is a subgroup of $G$.
- Next, let the group $N_G(A)$ act on the set $S = A$ by conjugation, i.e., for all $g \in N_G(A)$ and all $a \in A$, $g : a \mapsto gag^{-1}$. This does map $A$ to $A$ by the definition of $N_G(A)$. So, it gives an action on $A$.
  - It is easy to check that $C_G(A)$ is precisely the kernel of this action. Thus, $C_G(A) \leq N_G(A)$ By transitivity of the relation "$\leq$", $C_G(A) \leq G$.
- Finally, $Z(G)$ is the kernel of $G$ acting on $S = G$ by conjugation. Hence $Z(G) \leq G$.

Subsection 3

# Cyclic Groups and Cyclic Subgroups

# Cyclic Groups

- Let $G$ be any group and let $x$ be any element of $G$. One way of forming a subgroup $H$ of $G$ is by letting $H$ be the set of all integer powers of $x$.

**Definition (Cyclic Group)**

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

- In additive notation, $H$ is cyclic if $H = \{nx : n \in \mathbb{Z}\}$.
- In both cases we shall write $H = \langle x \rangle$ and say $H$ is **generated** by x and $x$ is a **generator** of $H$.

# Remarks

- A cyclic group may have more than one generator.
  Example: If $H = \langle x \rangle$, then also $H = \langle x^{-1} \rangle$.
  Since $(x^{-1})^n = x^{-n}$, we get

$$\{x^n : n \in \mathbb{Z}\} = \{(x^{-1})^n : n \in \mathbb{Z}\}.$$

- The elements of $\langle x \rangle$ are powers of $x$ (or multiples of $x$, in groups written additively) and not integers.
- It is not necessarily true that all powers of $x$ are distinct.
  Example: Consider $\mathbb{Z}/3\mathbb{Z} = \langle \overline{1} \rangle$. Clearly, $2 \cdot \overline{1} = \overline{2} = 5 \cdot \overline{1}$.
  Claim: Cyclic groups are abelian.
  Let $H = \langle x \rangle$. Suppose $g_1, g_2 \in H$. Then, there exist $m, n \in \mathbb{Z}$, such that $g_1 = x^m$ and $g_2 = x^n$. Then, we have

$$g_1 g_2 = x^m x^n = x^{m+n} = x^n x^m = g_2 g_1,$$

  showing that $H$ is abelian.

# Example

- Example: Let $G = D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$, $n \geq 3$, and let $H$ be the subgroup of all rotations of the $n$-gon. Thus, $H = \langle r \rangle$ and the distinct elements of $H$ are $1, r, r^2, \ldots, r^{n-1}$, all the distinct powers of $r$. So $|H| = n$ and the generator $r$ of $H$ has order $n$.

  The powers of $r$ "cycle" (forward and backward) with period $n$, i.e., $r^n = 1,\ r^{n+1} = r,\ r^{n+2} = r^2,\ \ldots,\ r^{n-1} = r^{-1},\ r^{n-2} = r^{-2},\ \ldots$

  In general, to write any power of $r$, say $r^t$, in the form $r^k$, for some $k$ between 0 and $n-1$:

  - We use the Division Algorithm to write $t = nq + k$, where $0 \leq k < n$;
  - Then, $r^t = r^{nq+k} = (r^n)^q r^k = 1^q r^k = r^k$.

  In $D_8$, $r^4 = 1$. So $r^{105} = (r^4)^{26} r^1 = r$ and $r^{-42} = (r^4)^{-11} r^2 = r^2$.

  $D_{2n}$ itself is not a cyclic group since it is non-abelian.

# The Cyclic Group $\mathbb{Z}$

- Let $H = \mathbb{Z}$ with operation $+$.
  - Thus $H = \langle 1 \rangle$, where 1 is the integer 1 and the identity of $H$ is 0.
  - Each element in $H$ can be written uniquely in the form $n \cdot 1$, for some $n \in \mathbb{Z}$.
  - In contrast to the preceding example, multiples of the generator are all distinct and we need to take both positive, negative and zero multiples of the generator to obtain all elements of $H$.
  - In this example $|H|$ and the order of the generator 1 are both $\infty$.
  - Note also that $H = \langle -1 \rangle$ since each integer $x$ can be written (uniquely) as $(-x)(-1)$.

# Order of Cyclic Groups and Order of Generators

## Proposition

If $H = \langle x \rangle$, then $|H| = |x|$, where, if one side of this equality is infinite, so is the other. More specifically:

(1) If $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all the distinct elements of $H$.

(2) If $|H| = \infty$, then $x^n \neq 1$, for all $n \neq 0$, and $x^a \neq x^b$, $a \neq b$ in $\mathbb{Z}$.

- Let $|x| = n$ and consider, first, the case when $n < \infty$.
  - The elements $1, x, x^2, \ldots, x^{n-1}$ are distinct: If $x^a = x^b$, with, $0 \leq a < b < n$, then $x^{b-a} = x^0 = 1$, contrary to $n$ being the smallest positive power of $x$ giving the identity. Thus, $H$ has at least $n$ elements.
  - To see that these are all of them, let $x^t$ be any power of $x$. Use the Division Algorithm to write $t = nq + k$, where $0 \leq k < n$. Then $x^t = x^{nq+k} = (x^n)^q x^k = 1^q x^k = x^k \in \{1, x, x^2, \ldots, x^{n-1}\}$.
- Next, suppose $|x| = \infty$, so no positive power of $x$ is the identity.
  - If $x^a = x^b$, for some $a < b$, then $x^{b-a} = 1$, a contradiction. Distinct powers of $x$ yields distinct elements of $H$ and $|H| = \infty$.

# Powers yielding the Identity

## Proposition

Let $G$ be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$.

- If $x^n = 1$ and $x^m = 1$, then $x^d = 1$, where $d = (m, n)$.
- In particular, if $x^m = 1$, for some $m \in \mathbb{Z}$, then $|x|$ divides $m$.

- By the Euclidean Algorithm, there exist integers $r$ and $s$, such that $d = mr + ns$, where $d$ is the g.c.d. of $m$ and $n$. Thus, $x^d = x^{mr+ns} = (x^m)^r(x^n)^s = 1^r 1^s = 1$. This proves the first assertion.
- Suppose $x^m = 1$ and let $n = |x|$. If $m = 0$, certainly $n \mid m$. So we may assume $m \neq 0$. Since some nonzero power of $x$ is the identity, $n < \infty$. Let $d = (m, n)$. By the preceding result, $x^d = 1$. Since $0 < d \leq n$ and $n$ is the smallest positive power of $x$ which gives the identity, we must have $d = n$, i.e., $n \mid m$, as asserted.

# Isomorphic Cyclic Groups

## Theorem

Any two cyclic groups of the same order are isomorphic. More specifically:

(1) If $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order $n$, then the map $\varphi : \langle x \rangle \to \langle y \rangle$, with $x^k \mapsto y^k$, is well defined and is an isomorphism.

(2) If $\langle x \rangle$ is an infinite cyclic group, the map $\varphi : \mathbb{Z} \to \langle x \rangle$, with $k \mapsto x^k$, is well defined and is an isomorphism.

- Suppose $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order $n$. Let $\varphi : \langle x \rangle \to \langle y \rangle$ be defined by $\varphi(x^k) = y^k$.
  - We first show $\varphi$ is well defined, i.e., if $x^r = x^s$, then $\varphi(x^r) = \varphi(x^s)$. Since $x^{r-s} = 1$, we have $n \mid r - s$. Write $r = tn + s$. Then, $\varphi(x^r) = \varphi(x^{tn+s}) = y^{tn+s} = (y^n)^t y^s = y^s = \varphi(x^s)$. This proves $\varphi$ is well defined.
  - By the laws of exponents $\varphi(x^a x^b) = \varphi(x^a)\varphi(x^b)$, i.e., $\varphi$ is a homomorphism.

# Isomorphic Cyclic Groups (Cont'd)

- Continuing with the finite order case:
  - Since the element $y^k$ of $\langle y \rangle$ is the image of $x^k$ under $\varphi$, this map is surjective.
  - Since both groups have the same finite order, any surjection from one to the other is a bijection, so $\varphi$ is an isomorphism.
- If $\langle x \rangle$ is an infinite cyclic group, let $\varphi : \mathbb{Z} \to \langle x \rangle$ be defined by $\varphi(k) = x^k$.
  - This map is already well defined since there is no ambiguity in the representation of elements in the domain.
  - Since $x^a \neq x^b$, for all distinct $a, b \in \mathbb{Z}$, $\varphi$ is injective.
  - By definition of a cyclic group, $\varphi$ is surjective.
  - As in the finite order case, the laws of exponents ensure $\varphi$ is a homomorphism.

  Hence $\varphi$ is an isomorphism.
- For each $n \in \mathbb{Z}^+$, let $Z_n$ be the cyclic group of order $n$ written multiplicatively. Up to isomorphism, $Z_n$ is the unique cyclic group of order $n$ and $Z_n \cong \mathbb{Z}/n\mathbb{Z}$.

# Orders of Powers

- We determine precisely which powers of $x$ generate the group $\langle x \rangle$.

**Proposition**

Let $G$ be a group, let $x \in G$ and let $a \in \mathbb{Z} - \{0\}$.

(1) If $|x| = \infty$, then $|x^a| = \infty$.

(2) If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$. So, if $a > 0$ and $a \mid n$, then $|x^a| = \frac{n}{a}$.

(1) By way of contradiction assume $|x| = \infty$ but $|x^a| = m < \infty$. By definition of order $1 = (x^a)^m = x^{am}$ and $x^{-am} = (x^{am})^{-1} = 1^{-1} = 1$. One of $am$ or $-am$ is positive (since neither $a$ nor $m$ is 0). So some positive power of $x$ is the identity. This contradicts $|x| = \infty$. So the assumption $|x^a| < \infty$ must be false.

# Orders of Powers (Cont'd)

(2) Let $y = x^a$, $(n, a) = d$ and write $n = db$, $a = dc$, for suitable $b, c \in \mathbb{Z}$, with $b > 0$. Since $d$ is the greatest common divisor of $n$ and $a$, the integers $b$ and $c$ are relatively prime: $(b, c) = 1$. We must now show $|y| = b$. First note that

$$y^b = x^{ab} = x^{dcb} = (x^{db})^c = (x^n)^c = 1^c = 1.$$

Thus, $|y|$ divides $b$.

Let $k = |y|$. Then $x^{ak} = y^k = 1$. Hence $n \mid ak$, i.e., $db \mid dck$. Thus, $b \mid ck$. Since $b$ and $c$ have no factors in common, $b$ must divide $k$.

Since $b$ and $k$ are positive integers which divide each other, $b = k$.

# Subgroups Generated By Powers

## Proposition

Let $H = \langle x \rangle$.

(1) Assume $|x| = \infty$. Then $H = \langle x^a \rangle$ if and only if $a = \pm 1$.

(2) Assume $|x| = n < \infty$. Then $H = \langle x^a \rangle$ if and only if $(a, n) = 1$. Thus, the number of generators of $H$ is $\varphi(n)$, where $\varphi$ is Euler's $\varphi$-function.

(1) Clearly, if $a = \pm 1$, then $\langle x \rangle = \langle x^{-1} \rangle = H$.

Suppose, conversely, that $\langle x^a \rangle = \langle x \rangle = H$. Then, since $x \in \langle x^a \rangle$, there exists $b \in \mathbb{Z}$, such that $(x^a)^b = x$. This gives $x^{ab} = x$. By cancelation, we get $x^{ab-1} = 1$. Since $|x| = \infty$, we must have $ab - 1 = 0$. This yields $ab = 1$. Since $a, b \in \mathbb{Z}$, we must have $a = \pm 1$.

# Subgroups Generated By Powers (Cont'd)

(2) If $|x| = n < \infty$, then $x^a$ generates a subgroup of $H$ of order $|x^a|$. This subgroup equals all of $H$ if and only if $|x^a| = |x|$. By the preceding proposition, $|x^a| = |x|$ if and only if $\frac{n}{(a,n)} = n$, i.e., if and only if $(a, n) = 1$.

Since $\varphi(n)$ is, by definition, the number of $a \in \{1, 2, \ldots, n\}$, such that $(a, n) = 1$, this is the number of generators of $H$.

Example: The residue classes $\overline{a}$ mod $n$ that generate $\mathbb{Z}/n\mathbb{Z}$ are precisely those, such that $(a, n) = 1$.
E.g., if $n = 12$,

- the generators of $\mathbb{Z}/12\mathbb{Z}$ are $\overline{1}, \overline{5}, \overline{7}$ and $\overline{11}$;
- $\varphi(12) = 4$.

# The Subgroup Structure of a Cyclic Group (Cyclicity)

## Theorem

Let $H = \langle x \rangle$ be a cyclic group. Every subgroup of $H$ is cyclic. More precisely, if $K \leq H$, then either $K = \{1\}$ or $K = \langle x^d \rangle$, where $d$ is the smallest positive integer such that $x^d \in K$.

- Let $K \leq H$. If $K = \{1\}$, the proposition is true. So, assume $K \neq \{1\}$. Thus, there exists some $a \neq 0$, such that $x^a \in K$. If $a < 0$, then, since $K$ is a group, also $x^{-a} = (x^a)^{-1} \in K$. Hence $K$ always contains some positive power of $x$. Let $\mathcal{P} = \{b : b \in \mathbb{Z}^+ \text{ and } x^b \in K\}$. By the above, $\mathcal{P}$ is a nonempty set of positive integers. By the Well Ordering Principle, $\mathcal{P}$ has a minimum element $d$.
  - Since $K$ is a subgroup and $x^d \in K$, $\langle x^d \rangle \leq K$.
  - Since $K$ is a subgroup of $H$, any element of $K$ is of the form $x^a$, for some integer $a$. By the Division Algorithm, write $a = qd + r$, $0 \leq r < d$. Then $x^r = x^{(a-qd)} = x^a(x^d)^{-q}$ is an element of $K$, since both $x^a$ and $x^d$ are elements of $K$. By the minimality of $d$, it follows that $r = 0$, i.e., $a = qd$, whence $x^a = (x^d)^q \in \langle x^d \rangle$. So $K \leq \langle x^d \rangle$.

# The Subgroup Structure of a Cyclic Group (Infinite Order)

## Theorem

Let $H = \langle x \rangle$ be a cyclic group. If $|H| = \infty$, then for any nonnegative integers $a \neq b$, $\langle x^a \rangle \neq \langle x^b \rangle$. Further, for every integer $m$, $\langle x^m \rangle = \langle x^{|m|} \rangle$, where $|m|$ is the absolute value of $m$, so that the nontrivial subgroups of $H$ correspond bijectively with the integers $1, 2, 3, \ldots$.

- Since $|H| = \langle x \rangle = \infty$, we get $|x| = \infty$. Suppose that $\langle x^a \rangle = \langle x^b \rangle$ for positive integers $a, b$. Since $|x| = \infty$, we get $|x^b| = \infty$. Since $x^a \in \langle x^b \rangle$ and $\langle x^a \rangle = \langle x^b \rangle$, we get, by a previous lemma, that $a = \pm b$. Since both $a$ and $b$ are positive, we get $a = b$.
  It is clear that $\langle x^{-m} \rangle = \langle x^m \rangle$. Therefore, $\langle x^m \rangle = \langle x^{|m|} \rangle$.
  Finally, let $f$ be the map from the set of nonidentity subgroups of $H$ to the set $\{1, 2, 3, \ldots\}$, with $K \mapsto d$, where $d$ is the smallest positive integer, such that $x^d \in K$.
  - $f$ is injective by the previous part.
  - $f$ is surjective by the preceding theorem.

# The Subgroup Structure of a Cyclic Group (Finite Order)

## Theorem

Let $H = \langle x \rangle$ be a cyclic group. If $|H| = n < \infty$, then for each positive integer $a$ dividing $n$ there is a unique subgroup of $H$ of order $a$. This subgroup is the cyclic group $\langle x^d \rangle$, where $d = \frac{n}{a}$. In addition, for every integer $m$, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so that the subgroups of $H$ correspond bijectively with the positive divisors of $n$.

- Assume $|H| = n < \infty$ and $a \mid n$. Let $d = \frac{n}{a}$. We know that $\langle x^d \rangle$ is a subgroup of order $a$. Thus, there exists a subgroup of order $a$.
  To show uniqueness, suppose $K$ is any subgroup of $H$ of order $a$. By a previous theorem, we have $K = \langle x^b \rangle$, where $b$ is the smallest positive integer such that $x^b \in K$. But, then, by a previous proposition, $\frac{n}{d} = a = |K| = |x^b| = \frac{n}{(n,b)}$. In particular, $d \mid b$. Since $b$ is a multiple of $d$, $x^b \in \langle x^d \rangle$, Hence $K = \langle x^b \rangle \leq \langle x^d \rangle$. Since $|\langle x^d \rangle| = a = |K|$, we have $K = \langle x^d \rangle$.

# The Subgroup Structure of a Cyclic Group (Finite Order)

- To see that, for every integer $m$, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, note that:
  - $\langle x^m \rangle$ is a subgroup of $\langle x^{(n,m)} \rangle$;
  - $|\langle x^m \rangle| = \dfrac{n}{(n,m)} = |\langle x^{(n,m)} \rangle|$.

  Since $(n, m)$ is certainly a divisor of $n$, this shows that every subgroup of $H$ arises from a divisor of $n$, completing the proof.

# Examples

- We can use the last proposition and the last theorem to list all the subgroups of $\mathbb{Z}/n\mathbb{Z}$ for any given $n$.

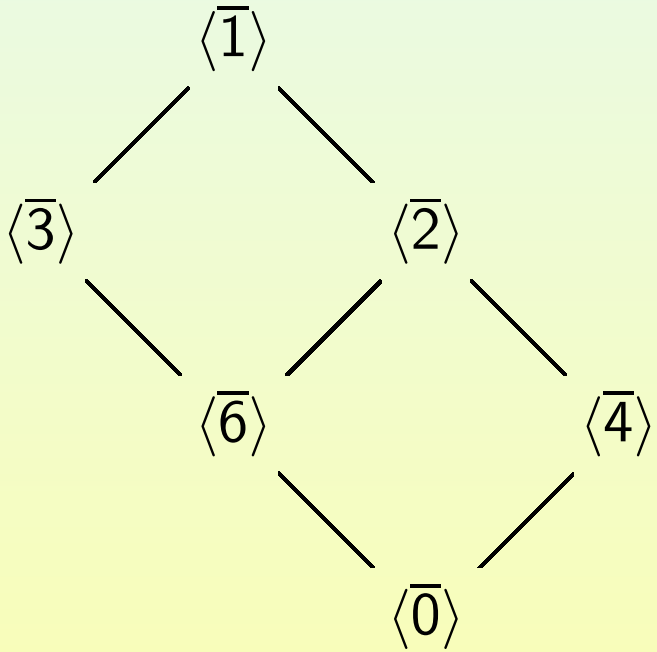
  Example: The subgroups of $\mathbb{Z}/12\mathbb{Z}$ are:

  (a) $\mathbb{Z}/12\mathbb{Z} = \langle\overline{1}\rangle = \langle\overline{5}) = \langle\overline{7}\rangle = \langle\overline{11}\rangle$ (order 12);
  (b) $\langle\overline{2}\rangle = \langle\overline{10}\rangle$ (order 6);
  (c) $\langle\overline{3}\rangle = \langle\overline{9}\rangle$ (order 4);
  (d) $\langle\overline{4}\rangle = \langle\overline{8}\rangle$ (order 3);
  (e) $\langle\overline{6}\rangle$ (order 2);
  (f) $\langle\overline{0}\rangle$ (order 1).

  The inclusions between them are given by

$$\langle\overline{a}\rangle \leq \langle\overline{b}\rangle \quad \text{if and only if} \quad (b, 12) \mid (a, 12),\ 1 \leq a, b \leq 12.$$

# Subgroup Structure of $\mathbb{Z}/12\mathbb{Z}$



# Centralizers of Cyclic Subgroups

Claim: Let $G$ be a group and $x \in G$. Then $C_G(\langle x \rangle) = C_G(x)$.

It suffices to show that an element $g \in G$ commutes with $x$ if and only if it commutes with all powers of $x$.

The "if" part is obvious.

For the "only if", suppose that $g$ commutes with $x$, i.e., $gx = xg$. We show by induction on $n$ that $gx^n = x^n g$, for all $n \geq 0$.

- For $n = 0$, we have $gx^0 = g1 = g = 1g = x^0 g$.
- Assume that $gx^n = x^n g$.
- Then we have $gx^{n+1} = g(x^n x) = (gx^n)x \overset{\text{IH}}{=} (x^n g)x = x^n(gx) \overset{\text{Hyp.}}{=} x^n(xg) = (x^n x)g = x^{n+1}g$.

# Normalizers of Cyclic Subgroups

Claim: Let $G$ be a group and $x \in G$. Then $\langle x \rangle \leq N_G(\langle x \rangle)$, but equality need not hold.

Since $\langle x \rangle \leq G$, it suffices to show that $\langle x \rangle \subseteq N_G(\langle x \rangle)$. For this, in turn, it suffices to show that $x \in N_G(\langle x \rangle)$, since $\langle x \rangle$ is the smallest subgroup of $G$ including $x$. We have

$$\begin{aligned} x\langle x \rangle x^{-1} &= x\{x^a : a \in \mathbb{Z}\}x^{-1} \\ &= \{xx^a x^{-1} : a \in \mathbb{Z}\} \\ &= \{x^{1+a-1} : a \in \mathbb{Z}\} \\ &= \{x^a : a \in \mathbb{Z}\} \\ &= \langle x \rangle. \end{aligned}$$

Note, however, that for $G = Q_8$ and $x = i$,

- $\langle i \rangle = \{\pm 1, \pm i\}$;
- $N_{Q_8}(\langle i \rangle) = Q_8$.

So $\langle i \rangle \lneq N_{Q_8}(\langle i \rangle)$.

Subsection 4

# Subgroups Generated by Subsets of a Group

# Intersection of a Collection of Subgroups

**Proposition**

If $\mathcal{A}$ is any nonempty collection of subgroups of $G$, then the intersection of all members of $\mathcal{A}$ is also a subgroup of $G$.

- We apply the subgroup criterion. Let

$$K = \bigcap_{H \in \mathcal{A}} H.$$

  - Since each $H \in \mathcal{A}$ is a subgroup, $1 \in H$, so $1 \in K$, i.e., $K \neq \emptyset$.
  - If $a, b \in K$, then $a, b \in H$, for all $H \in A$. Since each $H$ is a group, $ab^{-1} \in H$, for all $H$, whence $ab^{-1} \in K$.

  The criterion gives that $K \leq G$.

# Subgroup Generated by a Set of Elements

## Definition

If $A$ is any subset of the group G define $\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H$. This is called the **subgroup of $G$ generated by $A$.**

- $\langle A \rangle$ is a subgroup of $G$ containing $A$:
  - It is a subgroup of $G$ by the preceding proposition applied to $\mathcal{A} = \{H \leq G : A \subseteq H\}$. Note that $\mathcal{A} \neq \emptyset$ since $G \in \mathcal{A}$.
  - Since $A$ lies in each $H \in \mathcal{A}$, $A$ is a subset of their intersection $\langle A \rangle$.
- $\langle A \rangle$ is the unique minimal element of $\mathcal{A}$:
  - $\langle A \rangle$ is a subgroup of $G$ containing $A$, so $\langle A \rangle \in \mathcal{A}$;
  - Any element of $\mathcal{A}$ contains the intersection of all elements in $A$, i.e., contains $\langle A \rangle$.
- If $A$ is the finite set $\{a_1, a_2, \ldots, a_n\}$, we write $\langle a_1, a_2, \ldots, a_n \rangle$, for the group generated by $a_1, a_2, \ldots, a_n$ instead of $\langle \{a_1, a_2, \ldots, a_n\} \rangle$.
- If $A$ and $B$ are two subsets of $G$, we write $\langle A, B \rangle$ in place of $\langle A \cup B \rangle$.

# Generating $\langle A \rangle$ "Bottom-Up"

- For a group $G$ and $A \subseteq G$, define

$$\overline{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n} : n \in \mathbb{Z}, n \geq 0 \text{ and } a_i \in A, \epsilon_i = \pm 1 \text{ for all } i\},$$

  where $\overline{A} = \{1\}$ if $A = \emptyset$. So $\overline{A}$ is the set of all finite products, called **words**, of elements of $A$ and inverses of elements of $A$.
- The $a_i$'s need not be distinct, nor is $A$ assumed to be a finite set.

**Proposition**

$\overline{A} = \langle A \rangle$.

- We first prove $A$ is a subgroup:
  - $\overline{A} \neq \emptyset$.
  - Let $a, b \in \overline{A}$, with $a = a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n}$ and $b = b_1^{\delta_1} b_2^{\delta_2} \cdots b_m^{\delta_m}$. Then $ab^{-1} = a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n} b_m^{-\delta_m} b_{m-1}^{-\delta_{m-1}} \cdots b_1^{-\delta_1}$. Thus $ab^{-1}$ is a product of elements of $A$ raised to powers $\pm 1$, whence $ab^{-1} \in A$.

  By the subgroup criterion, $A$ is a subgroup of $G$.

# The Proof of the Proposition (Cont'd)

- Since each $a \in A$ may be written $a^1$, $A \subseteq \overline{A}$. Since $\langle A \rangle$ is the smallest subgroup of $G$ containing $A$, $\langle A \rangle \subseteq \overline{A}$.
- On the other hand, $\langle A \rangle$ is a group containing $A$. Since it is closed under the group operation and the process of taking inverses, $\langle A \rangle$ contains each element of the form $a_1^{\epsilon 1} a_2^{\epsilon 2} \cdots a_n^{\epsilon n}$. Therefore, $\overline{A} \subseteq \langle A \rangle$.

  These two inclusions prove that $\overline{A} = \langle A \rangle$.

# A Reformulation of $\langle A \rangle$

- Since $\langle A \rangle = \overline{A}$, we may use the notation $\langle A \rangle$ in place of $\overline{A}$ as well.
- Note that products of the form $a \cdot a, a \cdot a \cdot a, a \cdot a^{-1}$, etc. could have been simplified to $a^2, a^3, 1$, etc. respectively.
- Thus, another way of writing $\langle A \rangle$ is

$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_n^{\alpha_n} : \text{for all } i, a_i \in A, \alpha_i \in \mathbb{Z}, a_i \neq a_{i+1} \text{ and } n \in \mathbb{Z}^+\}.$$

- If $G$ is abelian, we could commute the $a_i$'s and so collect all powers of a given generator together.

  E.g., if $A$ were the finite subset $\{a_1, a_2, \ldots, a_k\}$ of the abelian group $G$, then $\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_k^{\alpha_k} : \alpha_i \in \mathbb{Z}, \text{ for each } i\}$.
  - If in this situation we further assume that each $a_i$ has finite order $d_i$, for all $i$, then since there are exactly $d_i$ distinct powers of $a_i$, the total number of distinct products of the form $a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_k^{\alpha_k}$ is at most $d_1 d_2 \cdots d_k$, i.e., $|\langle A \rangle| \leq d_1 d_2 \cdots d_k$.

# The Non-Abelian Case: $D_8$

- Let $G = D_8$ and let $r$ and $s$ be the usual generators of $D_8$. Let $a = s$, $b = rs$ and let $A = \{a, b\}$. Since both $s$ and $r$ $(= rs \cdot s)$ belong to $\langle a, b \rangle$, $G = \langle a, b \rangle$, i.e., $G$ is also generated by $a$ and $b$. Both $a$ and $b$ have order 2, but $D_8$ has order 8. Thus, it is not possible to write every element of $D_8$ in the form $a^\alpha b^\beta$, $\alpha, \beta \in \mathbb{Z}$. More specifically, the product $aba$ cannot be simplified to a product of the form $a^\alpha b^\beta$.

# The Non-Abelian Case: $D_{2n}$

- Let $G = D_{2n}$, for any $n > 2$, and let $r, s$ be the usual generators of $D_{2n}$.
  Let $a = s$ and $b = rs$.
  It is still true that $|a| = |b| = 2$, $D_{2n} = \langle a, b \rangle$ and $|D_{2n}| = 2n$.
  This means that for large $n$, long products of the form $abab \cdots ab$ cannot be further simplified.
- This illustrates that, unlike the abelian (or the cyclic) group case, the order of a (finite) group cannot even be bounded once we know the orders of the elements in some generating set.

# The Non-Abelian Case: $S_n$ and $\mathrm{GL}_2(\mathbb{R})$

- Consider
$$S_n = \langle (1\ 2), (1\ 2\ 3 \ldots n) \rangle.$$
Thus $S_n$ is generated by an element of order 2 together with one of order $n$.
However, $|S_n| = n!$.
- Consider $G = \mathrm{GL}_2(\mathbb{R})$, $a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{pmatrix}$.
So $a^2 = b^2 = 1$.
But $ab = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 2 \end{pmatrix}$. The element $ab$ has order $\infty$.
So $\langle a, b \rangle$ is an infinite subgroup of $\mathrm{GL}_2(\mathbb{R})$ which is generated by two elements of order 2.

Subsection 5

# The Lattice of Subgroups of a Group

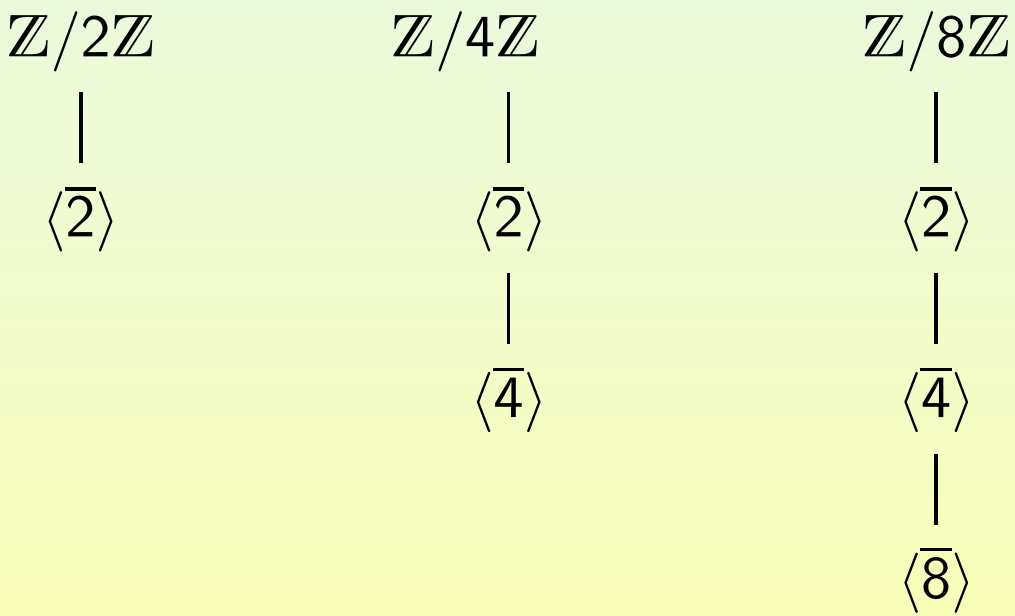
# The Lattice of Subgroups of a Group

- The **lattice of subgroups** of a group is a graph that depicts the relationships among the subgroups of the group.
- The lattice of subgroups of a finite group $G$ is constructed as follows:
  - Plot all subgroups of $G$ starting at the bottom with 1, ending at the top with $G$ and, roughly speaking, with subgroups of larger order positioned higher on the page than those of smaller order.
  - Draw a line upward from subgroup $A$ to subgroup $B$ if $A \leq B$ and there are no subgroups properly between $A$ and $B$.

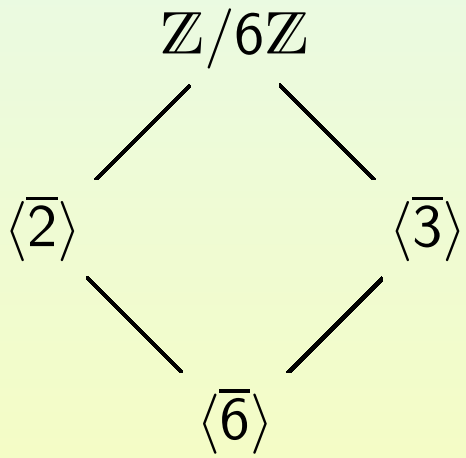
  Thus, if $A \leq B$, there is a path (possibly many paths) upward from $A$ to $B$ passing through a chain of intermediate subgroups.
- For any pair of subgroups $H$ and $K$ of $G$,
  - the unique smallest subgroup $\langle H, K \rangle$ containing both of them, their **join**, may be read off by tracing paths upwards from $H$ and $K$ until a common subgroup $A$ which contains $H$ and $K$ is reached.
  - the largest subgroup of $G$ which is contained in both $H$ and $K$, their **intersection**, can be found similarly.

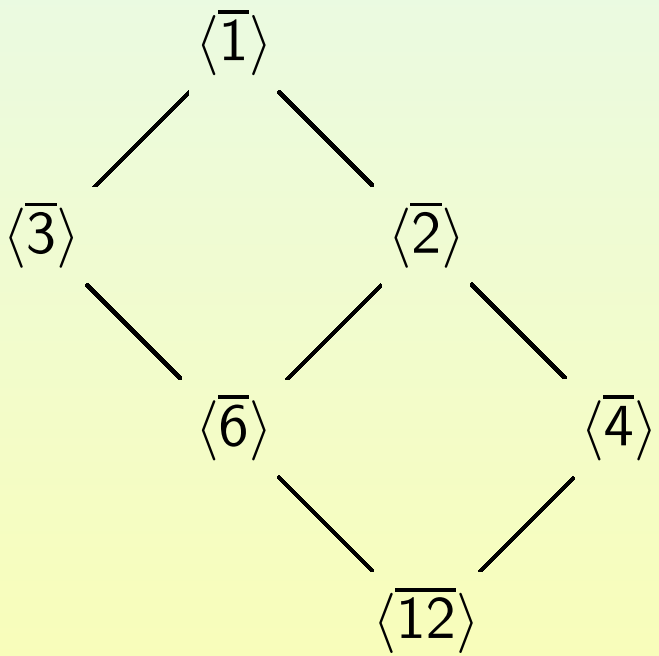
# The Groups $\mathbb{Z}/n\mathbb{Z}$

- For $G = \mathbb{Z}/n\mathbb{Z}$, we proved that the lattice of subgroups is the lattice of divisors of $n$:



# $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$



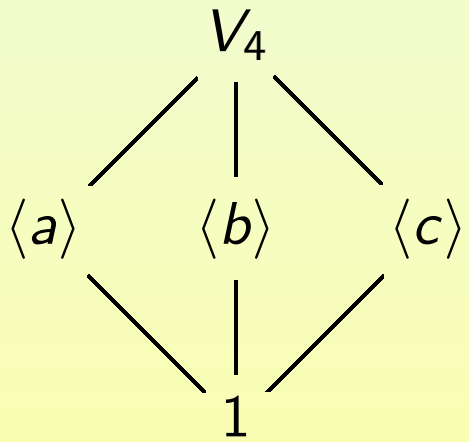



# The Klein 4-group

- The Klein 4-group (Viergruppe) $V_4$ is the group of order 4 with multiplication table

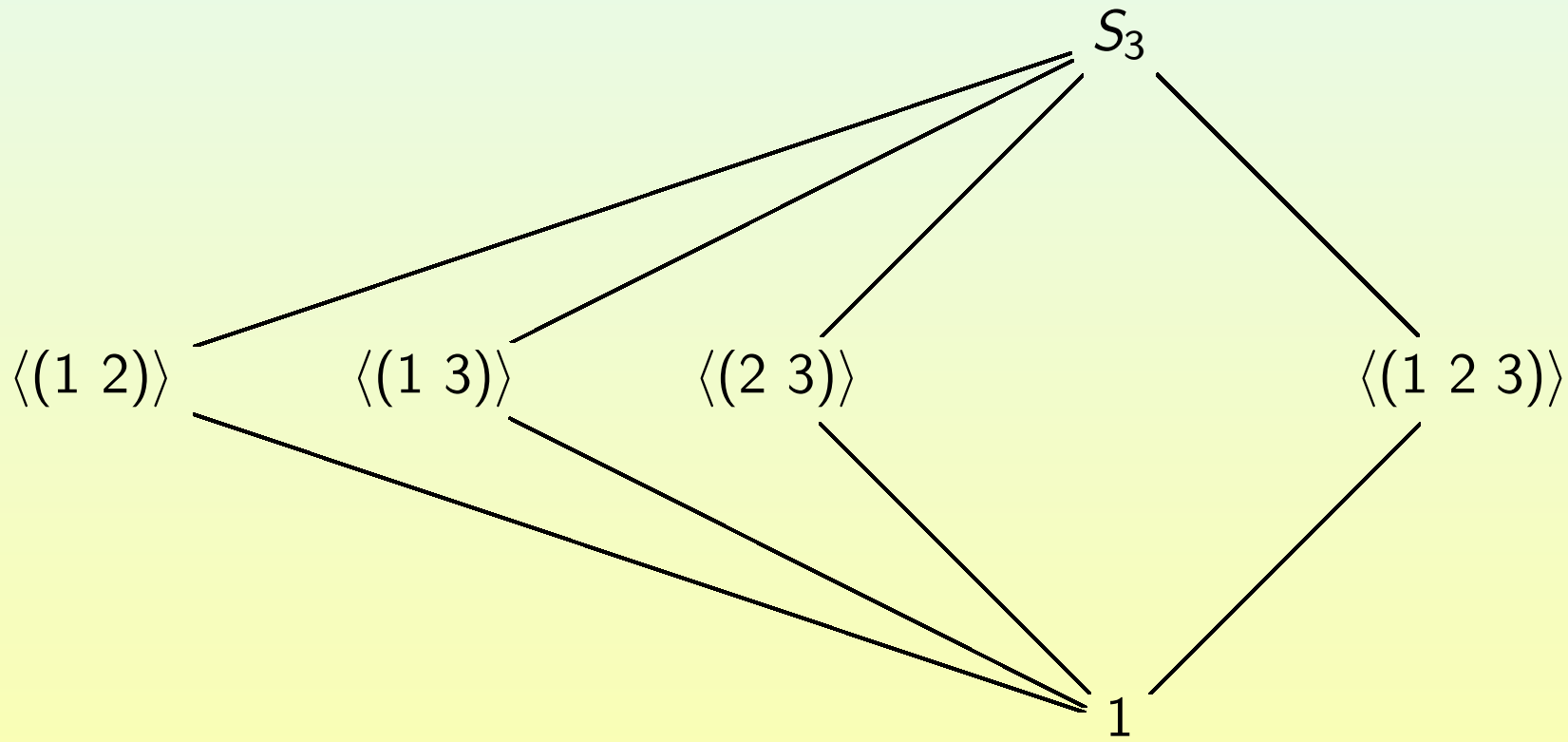
| $\cdot$ | $1$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $1$ | $1$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $1$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $1$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $1$ |

- Its lattice is

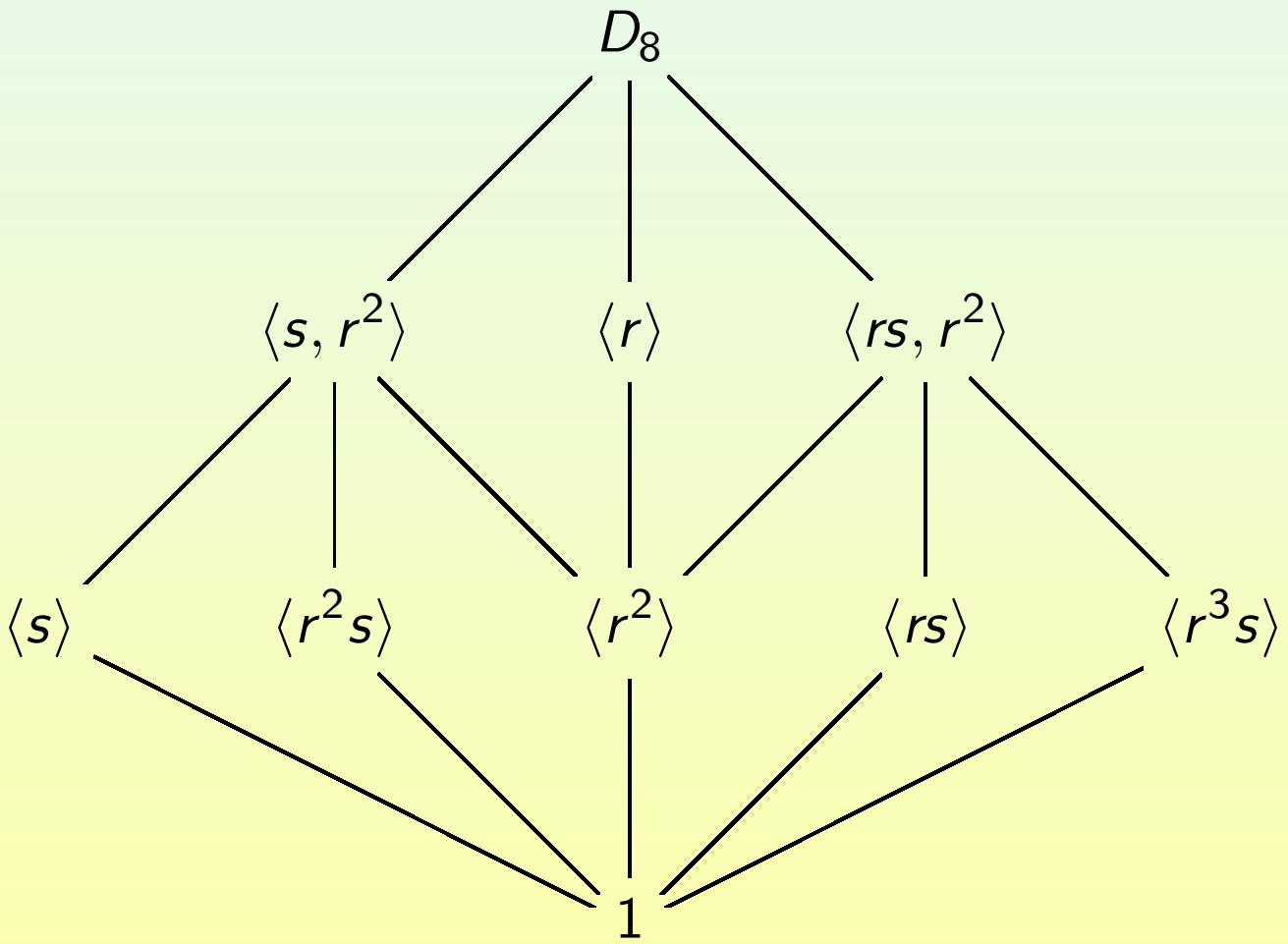



- $V_4$ is abelian and is not isomorphic to $Z_4$.

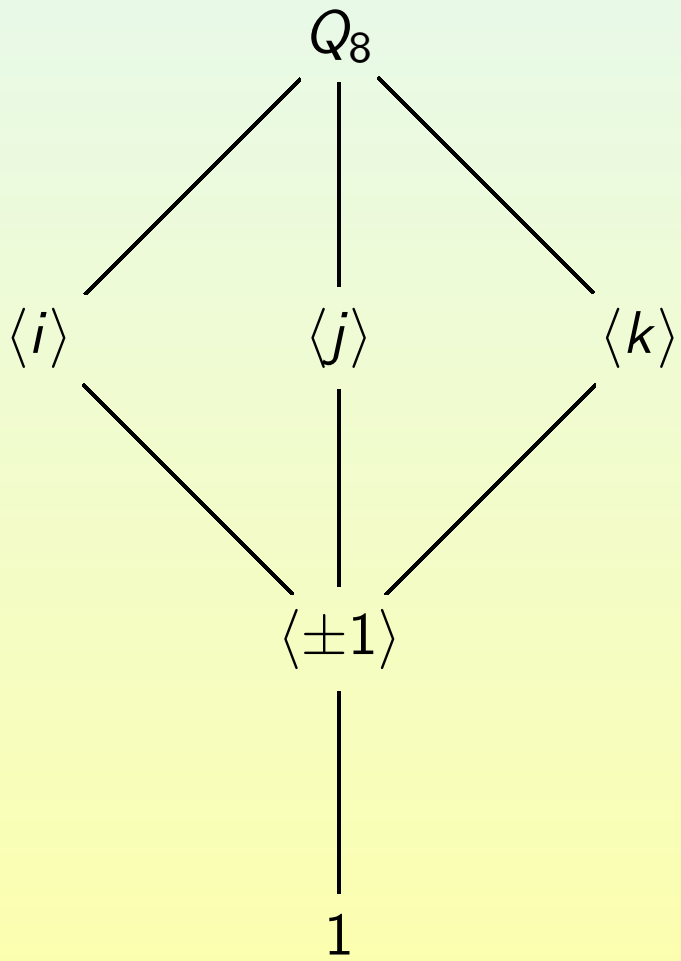
# The lattice of $S_3$



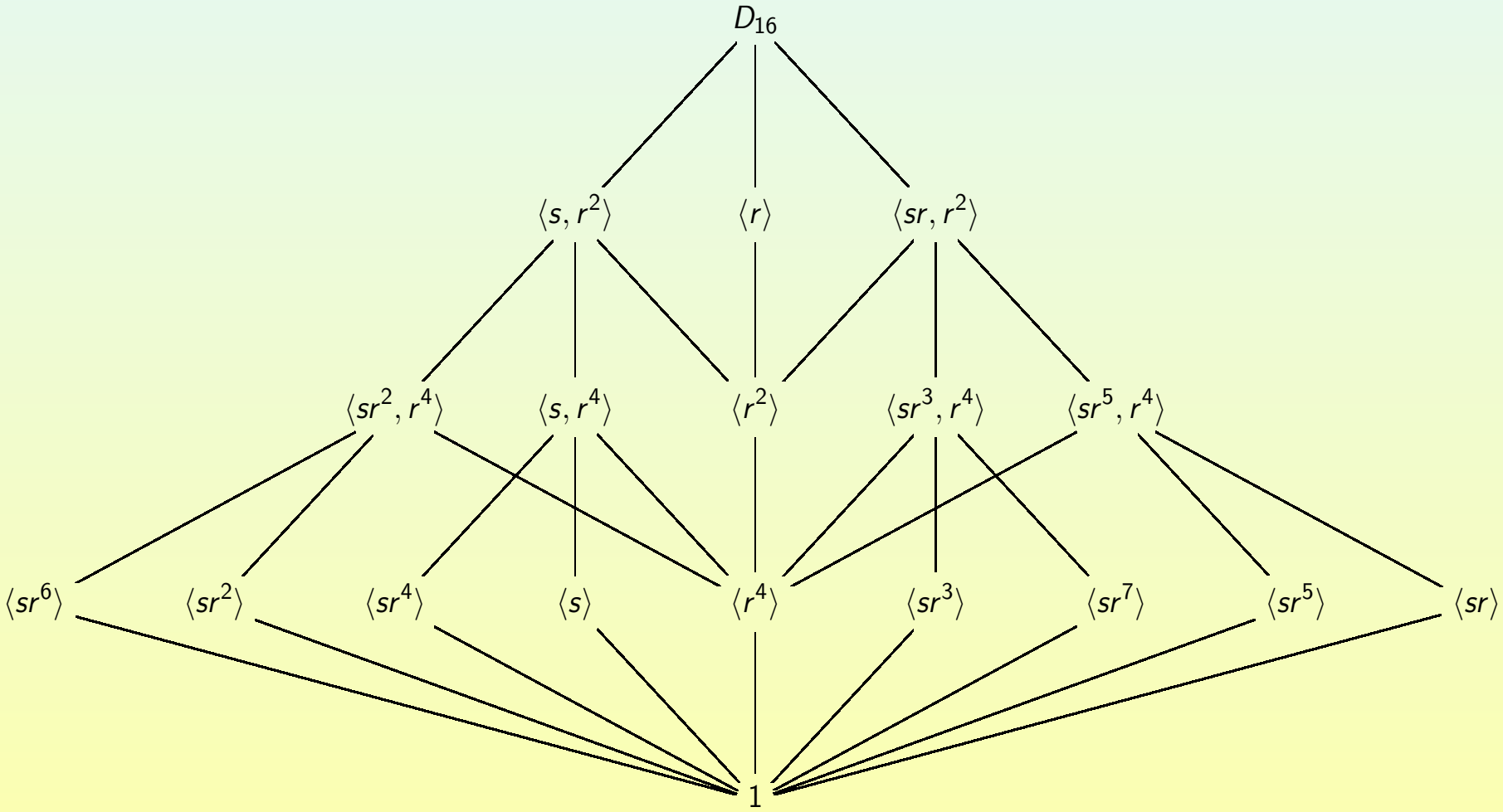
# The lattice of $D_8$



# The lattice of $Q_8$



# The lattice of $D_{16}$



# Mining Information From the Lattices

Example: We show that, in $D_8$, $C_{D_8}(s) = \langle s, r^2 \rangle$:

- We first calculate that $r^2 \in C_{D_8}(s)$. This proves $\langle s, r^2 \rangle \leq C_{D_8}(s)$.
- The only subgroups which contain $\langle s, r^2 \rangle$ are that subgroup itself and all of $D_8$. We cannot have $C_{D_8}(s) = D_8$ because $r$ does not commute with $s$. Thus, necessarily, $C_{D_8}(s) = \langle s, r^2 \rangle$.