Visual Algebra

Lecture 3.1: Subgroups

Dr. Matthew Macauley

School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

Definitions and notation

Recall the definition of a subgroup.

Definition

A subgroup of G is a subset $H \subseteq G$ that is also a group. We denote this by $H \leq G$.

Writing $C_2 \leq D_3$ means *there is a copy of C_2 sitting inside of D_3 as a subgroup*.

We must be careful, because there might be multiple copies:

$$C_2 \cong \langle f \rangle = \{1, f\} \leq D_3, \qquad C_2 \cong \langle rf \rangle = \{1, rf\} \leq D_3.$$

Some books will write things like

$$\mathbb{Z}_3 \leq D_3 \qquad \text{and} \qquad C_3 \leq S_3,$$

but we will try to avoid this, because $\mathbb{Z}_3 \not\subseteq D_3$ and $C_3 \not\subseteq S_3$. Instead, we can write

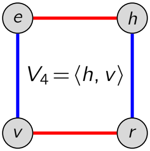
$$\mathbb{Z}_3 \cong \langle r \rangle \leq D_3 \qquad \text{and} \qquad C_3 \cong \langle (123) \rangle \leq S_3.$$

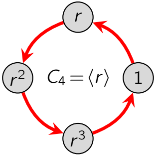
Remark

It is often prefered to express a subgroup by its generator(s).

The two groups of order 4

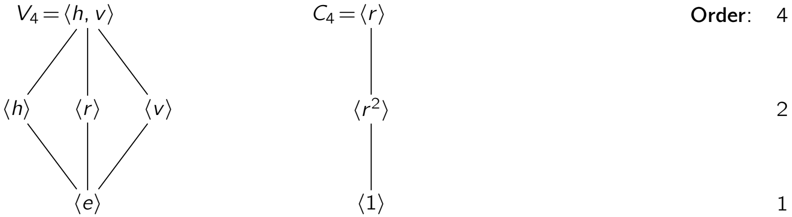
Let's start by considering the subgroup of the two groups of order 4.





- Proper subgroups of V_4: $\langle h \rangle = \{e, h\}$, $\langle v \rangle = \{e, v\}$, $\langle r \rangle = \{e, r\}$, $\langle e \rangle = \{e\}$.
- Subgroups of C_4: $\langle r \rangle = \{1, r, r^2, r^3\} = \langle r^3 \rangle$, $\langle r^2 \rangle = \{1, r^2\}$, $\langle 1 \rangle = \{1\}$.

It is illustrative to arrange these in a subgroup lattice:

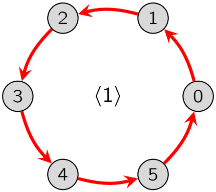


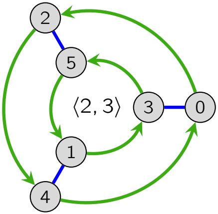
The subgroup lattice of $\mathbb{Z}_6$

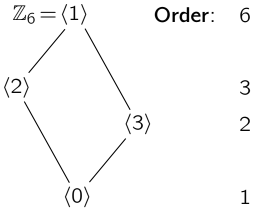
Consider the group $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Its subgroups are

$$\langle 0 \rangle = \{0\}, \qquad \langle 1 \rangle = \mathbb{Z}_6 = \langle 5 \rangle, \qquad \langle 2 \rangle = \{0, 2, 4\} = \langle 4 \rangle, \qquad \langle 3 \rangle = \{0, 3\}.$$

Different choices of Cayley graphs can highlight different subgroups.







Tip

It will be *essential* to learn the subgroup lattices of our standard examples of groups.

The subgroup lattice of D_3

Let's construct the subgroup lattice of $G = D_3$.

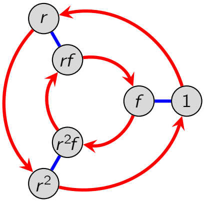
In any group G, every element $g \in D_3$ generates a cyclic subgroup, $\langle g \rangle \leq G$.

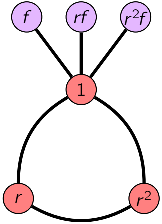
For small groups like D_3, these are the only proper subgroups.

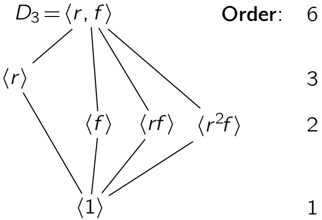
Here are the non-trivial proper subgroups of D_3:

$$\langle r \rangle = \{1, r, r^2\} = \langle r^2 \rangle, \quad \langle f \rangle = \{1, f\}, \quad \langle rf \rangle = \{1, rf\}, \quad \langle r^2 f \rangle = \{1, r^2 f\}, \quad \langle 1 \rangle = \{1\}.$$

Note that some subgroups are visually apparent in the Cayley graph and/or cycle graph, whereas others aren't.







Intersections of subgroups

Proposition (exercise)

For any collection $\{H_\alpha \mid \alpha \in A\}$ of subgroups of G, the intersection $\displaystyle\bigcap_{\alpha\in A} H_\alpha$ is a subgroup.

Every subset $S \subseteq G$, not necessarily finite, generates a subgroup, denoted

$$\langle S\rangle = \left\{s_1^{e_1}s_2^{e_2}\cdots s_k^{e_k} \mid s_i \in S,\ e_i = \{1,-1\}\right\}.$$

That is, $\langle S\rangle$ consists finite words built from elements in S and their inverses.

Proposition

For any $S \subseteq G$, the subgroup $\langle S\rangle$ is the intersection of all subgroups containing S:

$$\langle S\rangle = \bigcap_{S\subseteq H_\alpha\leq G} H_\alpha\,,$$

That is, the subgroup *generated by S* is the *smallest subgroup containing S*.

- Think of the LHS as the subgroup built "*from the bottom up*"
- Think of the RHS as the subgroup built "*from the top down*"

There are a number of mathematical objects that can be viewed in these two ways.

The defining property of lattices

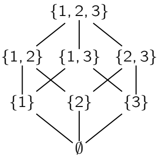
A lattice is a partially ordered set such that every pair of elements x, y has a unique:

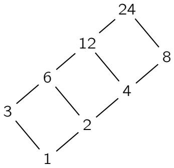
- supremum, or least upper bound, $x \vee y$
- infimum, or greatest lower bound, $x \wedge y$.

Examples that we're familiar with are subset lattices and divisor lattices.

$x \vee y = x \cup y$

$x \wedge y = x \cap y$



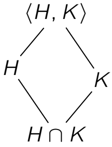


$x \vee y = \mathrm{lcm}(x, y)$

$x \wedge y = \gcd(x, y)$

The intersection $H \cap K$ of two subgroups is the largest subgroup contained in both of them.

Their union $H \cup K$ is not a subgroup (unless one contains the other). But it generates $\langle H, K \rangle$, the smallest subgroup containing both of them.



$H \vee K$: "*smallest subgroup above both H and K*"

$H \wedge K$: "*largest subgroup below both H and K*"

Subgroups of cyclic groups

Proposition

Every subgroup of a cyclic group is cyclic.

Proof

Let $H \leq G = \langle x \rangle$, and $|H| > 1$.

Note that $H = \{x^k \mid k \in \mathbb{Z}\}$. Let x^k be the smallest positive power of x in H.

We'll show that all elements of H have the form $(x^k)^m = x^{km}$ for some $m \in \mathbb{Z}$.

Take any other $x^\ell \in H$, with $\ell > 0$.

Use the division algorithm to write $\ell = qk + r$, for some remainder where $0 \leq r < k$.

We have $x^\ell = x^{qk+r}$, and hence

$$x^r = x^{\ell - qk} = x^\ell x^{-qk} = x^\ell (x^k)^{-q} \in H.$$

Minimality of $k > 0$ forces $r = 0$. $\square$

Corollary

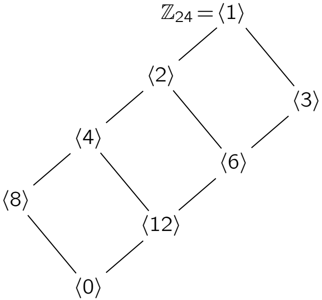
The subgroup of $G = \mathbb{Z}$ generated by $a_1, \ldots, a_k$ is $\langle \gcd(a_1, \ldots, a_k) \rangle \cong \mathbb{Z}$. $\square$

Subgroups of cyclic groups

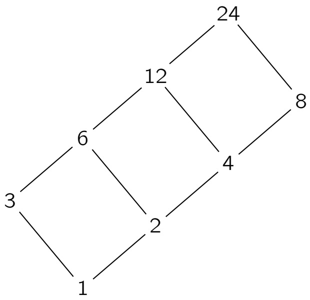
If d divides n, then $\langle d\rangle \leq \mathbb{Z}_n$ has order n/d. Moreover, all cyclic subgroups have this form.

Corollary

The subgroups of $\mathbb{Z}_n$ are of the form $\langle d\rangle$ for every divisor d of n. $\square$



subgroup lattice



divisor lattice

The order of each subgroup can be read off from the divisor lattice of 24.

A useful shortcut

Often, we'll need to verify that some $H \subseteq G$ is a subgroup. This requires checking

1. Identity: $e \in H$.
2. Inverses: If $h \in H$, then $h^{-1} \in H$.
3. Closure: If $h_1, h_2 \in H$, then $h_1 h_2 \in H$.

There is a better way to check whether H is a subgroup.

One-step subgroup test

A subset $H \subseteq G$ is a subgroup if and only if the following condition holds:

$$\textit{If } \; x, y \in H, \; \textit{ then } \; xy^{-1} \in H.$$

Proof

"$\Rightarrow$": Suppose $H \leq G$, and pick $h_1, h_2 \in H$. Then $h_2^{-1} \in H$, and by closure, $h_1 h_2^{-1} \in H$. ✓

"$\Leftarrow$": Suppose Eq. (1) holds, and take any $h \in H$.

- **Identity**: Take $x = y = h$. By Eq. (1), $xy^{-1} = hh^{-1} = e \in H$. ✓
- **Inverses**: Take $x = e$, $y = h$. By Eq. (1), $xy^{-1} = eh^{-1} = h^{-1} \in H$. ✓
- **Closure**: Take $x = h_1$ and $y = h_2^{-1}$. By Eq. (1),

$$xy^{-1} = h_1 (h_2^{-1})^{-1} = h_1 h_2 \in H. \quad ✓$$