MATH H113: Honors Introduction to Abstract Algebra

2016-02-24

For Friday: Read Sect. 3.1

- Subsets generated by subsets of a group
- Lattice diagrams of subgroups
- Start quotient groups

Last Time

Subgroups of cyclic groups $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$

The book defines Z_n ($n \in \mathbb{Z}_{>0}$) to be the cyclic group of order n, written multiplicatively. The same facts about $\mathbb{Z}/n\mathbb{Z}$ are true also (thm. 7 on p. 58) for Z_n, via $Z_n \cong \mathbb{Z}/n\mathbb{Z}$.

Subgroups Generated by Subsets

Main idea: Given a group G and a subset $A \subseteq G$, there is always a subgroup H of G, such that:

i. $H \supseteq A$, and
ii. A is a generating set for H (top of p. 26).

We'll write $H = \langle A \rangle$ (this is similar to the subspace of a vector space spanned by some set, except here there is no scalar multiplication).

Definition: Let A be a subset of a group G. Then we define $\bar{A} = \{a_1^{\epsilon_1}, a_2^{\epsilon_2}, \dots, a_n^{\epsilon_n} : n \in \mathbb{N}; a_1, \dots, a_n \in A; \epsilon_1, \epsilon_2, \dots \epsilon_n \in \{\pm 1\}\} = \{a_1^{\alpha_1}, a_2^{\alpha_2}, \dots, a_n^{\alpha_n} : n \in \mathbb{N}; a_1, \dots, a_n \in A; \alpha_1, \alpha_2, \dots \alpha_n \in \mathbb{Z}\} \subseteq G$
They're equal because:

- 1st $\subseteq$ 2nd ($\Sigma_i \in \mathbb{Z}\ \forall i$)
- 2nd $\subseteq$ 1st eliminate factors $a_i^{\alpha_i}$ if $\alpha_i = 0$ replace all other $a_i^{\alpha_i}$ with $|\alpha_i|$ copies of $a_i^{\pm 1}$

Proposition: $\bar{A} \leq G$
Proof: $\bar{A} \neq \emptyset$ because it contains 1 (take $n = 0$ if $A = \emptyset$).

Let $a, b \in \bar{A}$. Write $a = a_1^{\alpha_1} \dots a_n^{\alpha_n}$ and $b = b_1^{\beta_1} \dots b_m^{\beta_m}$. Then $ab^{-1} = a_1^{\alpha_1} \dots a_n^{\alpha_n} b_m^{-\beta_m} b_{m-1}^{-\beta_{m-1}} \dots b_1^{-\beta_1} \in \bar{A}$. $\therefore$ $\bar{A}$ is a subgroup.

Definition: $\langle A \rangle$ is the intersection of all subgroups of G that contain A:
$\langle A \rangle = \bigcap_{H \leq G, H \supseteq A} H$ Obviously $\langle A \rangle \leq G$

Proposition: $\bar{A} = \langle A \rangle$

Proof:

- $\langle A \rangle \subseteq \bar{A}$:
  $\bar{A}$ is a subgroup of G and contains A, so it occurs among the subgroups in the intersection $\bigcap_{H \leq G, H \supseteq A} H$. $\therefore$ $\langle A \rangle = \bigcap_{H \leq G, H \supseteq A} H \subseteq \bar{A}$.
- $\bar{A} \subseteq \langle A \rangle$
  Let H be a subgroup of G containing A. Then H must contain all products $a_1^{\alpha_1} \dots a_n^{\alpha_n}$ as in the definition of $\bar{A}$, so $H \supseteq \bar{A}$.
  So, in the intersetion, all H contain $\bar{A}$, $\therefore$ $\bigcap_{H \leq G, H \supseteq A} H \supseteq \bar{A}$.

Definition: $\langle A \rangle = \bar{A}$ is the subgroup of G generated by A (compare with the subspace of a vector space spanned by some subset: can describe it as either).

1. the set of linear combinations of elements of A, or
2. by a set of linear equations in some coordinate system $= \bigcap$ of all linear subspaces containing A.

Examples:

0. If $A = \emptyset$ then $\langle A \rangle = \{1\}$
1. If $A = \{x\}$ then $\langle A \rangle = \langle x \rangle$
2. If $G = \mathbb{Z}$ and $A = \{a, b\}$, then $\langle A \rangle = \langle a, b \rangle = \{xa + yb : x, y \in \mathbb{Z}\}$ (as was done last time). (= set of multiples of $\gcd(a, b)$ (unless $a = b = 0$))
3. Let $G = S_5$ and $A = \{\rho, \sigma\}$ where $\rho = (1\ 2\ 3\ 4\ 5)$ and $\sigma = (1\ 2)$. Then $\langle A \rangle = S_5$.
   For $i = 1, 2, 3, 4$: $\rho^{i-1} \sigma \rho^{1-i} = (i\ (i+1))$ (as on the practice midterm).
   So $(1\ 2), (2\ 3), (3\ 4), (4\ 5)$ are all in $\langle A \rangle$ (S_n can be generated by transpositions of adjacent elements).
   In particular, if ρ and σ do not commute, then usually not every element of $\langle \rho, \sigma \rangle$ can be written $\rho^i \sigma^j$ for $i, j \in \mathbb{Z}$.
   In this example $|\rho| = 5$ and $|\sigma| = 2$, so $\{\rho^i \sigma^j : i, j \in \mathbb{Z}\} = \{p^i \sigma^j : i \in \{0, 1, 2, 3, 4\} \wedge j \in \{0, 1\}\}$ (has 10 elements, but $|S_5| = 120$).

The Lattice of Subgroups of a Group

We've seen one example already:

$$\begin{tikzcd}[column sep=small]
 & & S_3 \arrow[dll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\langle x \rangle & \langle y \rangle & & \langle z \rangle & \langle w \rangle \\
 & & \{(1)\} \arrow[ull, dash] \arrow[ul, dash] \arrow[ur, dash] \arrow[urr, dash] & &
\end{tikzcd}$$

The general rule: show all subgroups of the group
a line between two such subgroups means: the lower of the two is a proper subgroup of the higher of the two, and there are no other subgroups in between.

Other Examples:

$$\begin{tikzcd}
\mathbb{Z}/4\mathbb{Z} = \langle \bar{1} \rangle \arrow[d, dash] \\
\langle \bar{2} \rangle \arrow[d, dash] \\
\langle \bar{4} \rangle = \langle \bar{0} \rangle = \{0\}
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbb{Z}/9\mathbb{Z} = \langle \bar{1} \rangle \arrow[d, dash] \\
\langle \bar{3} \rangle \arrow[d, dash] \\
\langle \bar{9} \rangle = \langle \bar{0} \rangle = \{0\}
\end{tikzcd}
\qquad
\begin{tikzcd}
 & (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \bar{0}, \bar{1} \rangle = (\mathbb{Z}/2\mathbb{Z}) \times 0 & 0 \times (\mathbb{Z}/2\mathbb{Z}) & \langle \bar{1}, \bar{1} \rangle \\
 & \{0\} \arrow[ul, dash] \arrow[u, dash] \arrow[ur, dash] &
\end{tikzcd}$$

($\therefore V_4 \not\cong \mathbb{Z}/4\mathbb{Z}$, because their lattices of subgroups are different (though if the lattices are the same, it does *not* guarantee they are isomorphic))

$$\begin{tikzcd}[column sep=small]
 & & \mathbb{Z}/12\mathbb{Z} \arrow[dl, dash] \arrow[dr, dash] & \\
 & \langle \bar{2} \rangle \arrow[dl, dash] \arrow[dr, dash] & & \langle \bar{3} \rangle \arrow[dl, dash] \\
\langle \bar{4} \rangle & & \langle \bar{6} \rangle & \\
 & \langle \overline{12} \rangle = \{0\} \arrow[ul, dash] \arrow[ur, dash] & &
\end{tikzcd}$$

One use for these diagrams:
To find $H \cap K$ (when $H, K \leq G$):
find the largest subgroup *below* (defined by going down lines at each step) both of them
Similarly, $\langle H, K \rangle = \langle H \cup K \rangle$ can be found by going up from H and K.

Section 3.1

The key questions are are, given a group G:

1. Which groups can occur as images of homomorphism from G? (i.e. for which groups H is there a surjective homomorphism $G \to H$?)
2. Which groups can occur as kernels of homomorphisms from G?

3. How are the kernel and image of a homomorphism (from G) related to each other?