Math 113, Fall 2019

Lecture 8, Tuesday, 9/24/2019

Topics Today:

- Finish cyclic groups
- Generating sets
- Cayley digraphs (quickly)
- Permutation groups

Assigned readings: §8 and 9.

We open with two clicker questions on Cayley digraphs.

1 Review from last lecture

Let G be a cyclic group generated by a, and let $n := |G|, s \in \mathbb{Z}, b := a^s$, and let $H = \langle b \rangle$. Then

$$\{k \in \mathbb{Z} \mid a^k \in H\} = \{in + js \mid i, j \in \mathbb{Z}\}$$

This is a nontrivial subgroup of $\mathbb{Z}$, equal to $d\mathbb{Z}$, where d is its smallest positive element. Then

$$d := \gcd(s, n),$$

and H contains $\{a^d, a^{2d}, \ldots, a^{\frac{n}{d}d} = 1\}$, so $H \supseteq \left\langle a^d \right\rangle$, which has $\frac{n}{d}$ elements. Now from an earlier proof (of Theorem 6.6), $H = \left\langle a^d \right\rangle$, and $|H| = \frac{n}{d}$. So we've shown part of the following theorem:

Theorem 1.1. Let G, a, and n be as above. Let $b \in G$, and pick $s \in \mathbb{Z}$ such that $b = a^s$.
Let $d := \gcd(s, n)$. Then $|B| = \frac{n}{d}$ and $\langle b \rangle = \left\langle a^d \right\rangle$. Also, for all $t \in \mathbb{Z}$,

$$\langle a^s \rangle = \left\langle a^t \right\rangle \iff \gcd(s, n) = \gcd(t, n)$$

Proof. We've computed $|b| = \frac{n}{d}$, and showed $\langle b \rangle = \langle a \rangle$. Also, $\gcd(s, n) = \gcd(t, n) \implies \langle a^s \rangle = \langle a^t \rangle$, since both equal $\left\langle a^d \right\rangle$, where $d = \gcd(s, n) = \gcd(t, n)$.
Conversely, if $\langle a^s \rangle = \langle a^t \rangle$, then $\gcd(s, n) = \frac{n}{|\langle a^s \rangle|} = \frac{n}{|\langle a^t \rangle|} = \gcd(t, n)$. □

As a corollary, we have the additional homework problem (on HW4).

Example: We showed that the subgroups of U_6 are U_1, U_2, U_3, and U_6, and $1, 2, 3, 6$ are the positive divisors of 6.
As another corollary, the cyclic generators of G are

$$\{a^s \mid \gcd(s, n) = 1\} = \{b \in G \mid \langle b \rangle = G\}.$$

2 Generating Sets

Recall that for all $a \in G$, we have:

$$\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}.$$

We also said (or Vojta notes perhaps the book said) that $\langle a \rangle$ is the smallest subgroup of G containing a.
Let's look in more detail. Suppose we have a nonempty collection of subgroups of a group G, and let

$$K := \bigcap_{i \in I} H_i.$$

Then K is a subgroup of G.

Proof. Notice $e \in H_i$ for all i, so $e \in \cap H_i = K$. In particular, $K \neq \{\}$. Let x, y be arbitrary elements of K. Then $x, y \in H_i, \forall_i$. Therefore, $xy^{-1} \in H_i, \forall_i$, which implies $xy^{-1} \in K$, and hence $K \leq G$. □

Further, consider that $\langle a \rangle$ is the **intersection of all subgroups** of G containing a.

Proof. Let $\{H_i\}_{i \in I}$ be all subgroups of G containing a. This is a nonempty collection because it contains G. Let $K := \cap_{i \in I} H_i$. Then $\langle a \rangle \subseteq K$ because all of the H_i contain a. Hence they all contain $\langle a \rangle$. Also, $K \subseteq \langle a \rangle$ because $\langle a \rangle$ is one of the H_i. □

Vojta notes that we now have two characterizations of cyclic groups. That is, $\langle a \rangle$ is
(1) $\{a^n \mid n \in \mathbb{Z}\}$, and
(2) The intersection of all subgroups containing a.
Vojta gives the analogy that the first is the '3d printing method' , building it up piece by piece, whereas the second is the 'sculpture method', chipping away piece by piece.
Now, instead of a single element a, consider a subset of G.

3 Generating Sets

We now consider generating sets as opposed to the cyclic group generated by a single cyclic generator. We emphasize here that we take a generic subset (in fact, it's most interesting when our subset is NOT a subgroup).
Let G be a group, and let $S \subseteq G$ be a sub**set**. Let $\{H_i\}_{i \in I}$ be the set of all subgroups of G containing S.
Again, G itself is one of these subgroups, so $I \neq \{\}$.
Then we can let $K := \cap_{i \in I} H_i$. This is a subgroup of G, and it contains S. In fact, it si the smallest subgroup of G containing S. That is,

$$K \subseteq H_i, \forall_i,$$

and $K \in \{H_i\}_{i \in I}$.

Definition: Subgroup generated by a set -

$K := \cap_{i \in I} H_i$ as above is the **subgroup** of G **generated by** S, and is denoted $\langle S \rangle$.

Remark: If $S = \{a_1, \ldots, a_n$, then we also write:

$$\langle a_1, \ldots, a_n \rangle = \langle S \rangle .$$

and if $S = \{a_1, a_2, \ldots\}$, we write:

$$\langle a_1, a_2, \ldots \rangle = \langle S \rangle .$$

On the other hand, if we take the 3d-printing method, we have:

$$\langle S \rangle = \{s_1^{n_1}, \ldots, s_m^{n_m} \mid m \in \mathbb{N}, s_1, \ldots, s_m \in S, n_1, \ldots, n_m \in \mathbb{Z}\}$$

The right hand side is a subgroup of G, because take $m = 0$ and $e \in rhs$. Then rhs is closed under the group operation (concatenate the formulas). Also, the rhs is closed under the inverse, namely

$$\left((s_1^{n_1} \cdots s_m^{n_m})^{-1} = s_m^{-n_m} \cdots s_1^{-n_1}\right) .$$

Also, the rhs contains S, because $\forall_{s \in S}$, take $m = n_1 = 1$ and $s_1 = s$. Also, all H_i contain the rhs (the H_i contains S and are closed under taking integer powers and taking products). Then we get the desired equality.

Example:

- Let G be any group. Then $S = \{\}$ implies $\langle S \rangle = \{e\}$.
- $G = \mathbb{R}$ (or $\mathbb{Q}$ or $\mathbb{C}$) and $S = \{1\}$ imply $\langle S \rangle = \langle 1 \rangle = \mathbb{Z}$.
- $G = \mathbb{R}$ (or $\mathbb{C}$), and $S = \{\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\}$. These imply that $\langle S \rangle = \mathbb{Q}$.

Definition: Generating set -

A **generating set** for a group G is a subset S of G such that $\langle S \rangle = G$. If so, then we also say that S **generates** G.

Often we'll use the word "generator" to mean an element of some **specific** generating set (otherwise it has no meaning, because always $G = \langle G \rangle$).

4 Cayley Digraphs

Vojta notes that he will hold us responsible for Cayley digraphs as discussed in the text, except the examples 7.10 and 7.12. All others are fair game.

5 Clicker Questions

3. For which of these pairs G, S is $G \neq \langle S \rangle$?
(a) $G := \mathbb{Z}, S = \{-1\}$
(b) $G = \mathbb{R}, S = (0, 1) \cup \mathbb{Z}$
(c) $G = \mathbb{C}^*, S = \mathbb{R}^* \cup U$
(d) None of the above (all S above generate the given G)
(e) $G \neq \langle S \rangle$ for more than one of the above three.

4. For which pairs σ, A is σ **NOT** in S_A?

Lecture ends here.