Subgroups Generated by Sets

Recall: Let G be a group and $a \in G$. Then

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

is the cyclic subgroup of G generated by a.

We first provide an alternate formulation for cyclic subgroups.

Thm: Let G be a group and $a \in G$. Then

$$\bigcap_{a \in H \leq G} H = \langle a \rangle.$$

Proof. Clearly $a \in \langle a \rangle$ and we proved that $\langle a \rangle \leq G$, so $\langle a \rangle$ is one of the subgroups being intersected and hence

$$\bigcap_{a \in H \leq G} H \subseteq \langle a \rangle.$$

Now, suppose $H \leq G$ and $a \in H$. Then, since H is closed under the operation of G and contains the inverses of its elements, we must have $a^n \in H$ for all $n \in \mathbb{Z}$. Hence $\langle a \rangle \subseteq H$. It follows that $\langle a \rangle$ is a subset of every subgroup being intersected and so

$$\langle a \rangle \subseteq \bigcap_{a \in H \leq G} H.$$

Therefore,

$$\bigcap_{a \in H \leq G} H = \langle a \rangle.$$

$\square$

In this sense, $\langle a \rangle$ can be thought of as the "smallest subgroup of G containing a": If $a \in H \leq G$, then $\langle a \rangle \leq H$. This notion of $\langle a \rangle$ as the intersection of subgroups containing a easily generalizes to arbitrary subsets of G. The following theorem is left as a homework exercise.

Thm: Let G be a group and $A \subseteq G$. Then $\displaystyle\bigcap_{A \subseteq H \leq G} H$ is a subgroup of G.

In the theorem, the intersection is taken over all subgroups of G that contain A. It can be proven in a similar fashion to Exercise 54 from Section 6 in the book (*A First Course In Abstract Algebra* by John B. Fraleigh). In light of the theorem, the following definition very naturally generalizes that of the cyclic subgroup.

Def: Let G be a group and $A \subseteq G$. We write

$$\langle A \rangle := \bigcap_{A \subseteq H \leq G} H$$

and call $\langle A \rangle$ the subgroup of G generated by A.

We emphasize that $\langle A \rangle$ as defined above should be thought of as the "smallest subgroup of G containing A" in the following sense: If $A \subseteq K \leq G$, then $\langle A \rangle \leq K$. This is left as a homework exercise.

Ex: $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not cyclic, but $\langle (0,1), (1,0) \rangle = \mathbb{Z}_3 \times \mathbb{Z}_3$ since $(m,n) = m(1,0) + n(0,1)$ for $0 \leq m, n < 3$. We say that "$\mathbb{Z}_3 \times \mathbb{Z}_3$ is generated by $(1,0)$ and $(0,1)$."

We can easily see that, in fact, any direct product of some $\mathbb{Z}_n$'s is generated by a similar set of elements.

Prop: Given $m_1, m_2, \ldots, m_n \geq 2$, $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is generated by the set of elements of the form $(0, 0, \ldots, 1, \ldots, 0)$, namely, n-tuples with exactly one 1 and all other entries 0. Explicitly,

$$(k_1, k_2, \ldots, k_n) = k_1(1, 0, \ldots, 0) + k_2(0, 1, 0, \ldots, 0) + \cdots + k_n(0, \ldots, 0, 1)$$

for $0 \leq k_i < m_i$, $i = 1, \ldots, n$.

We can generalize the notion of cyclic group to that of being generated by a finite set.

Def: We say a group G is finitely generated if there exists some finite subset $A \subseteq G$ such that $\langle A \rangle = G$.

Of course, any finite group G is finitely generated, since it is obvious that $\langle G \rangle = G$. It is more interesting to consider groups which are of infinite cardinality, but still finitely generated. We will consider some of these during the next class.