Group Theory II

UW Math Circle – Advanced Group

Session 15 (30 January 2014)

Let G be a group. We will no longer write $*$ for the operation, but write ab for $a * b$.

For an element $a \in G$, consider the set $\langle a \rangle$ generated by a:

$$\langle a \rangle = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}.$$

If $\langle a \rangle$ is a finite set, then its cardinality $|\langle a \rangle|$ is called the *order* of a in G, written $|a|$. Otherwise, a has *infinite order.*

Theorem 3 (Elements with finite order)**.** *Let G be a group.*

1. *The order of an element $a \in G$ is the least integer $k > 0$ such that $a^k = 1$. If such k does not exist, then x has infinite order.*
2. *If G is a finite group, then every element of G has finite order.*

Note that the converse of (b) is not true: infinite groups can contain elements of finite order. (In fact, in any group, $|1| = 1$.)

A subset $H \subseteq G$ is a *subgroup* of G if H forms a group with the operation of G. We write $H < G$.

Theorem 4. *H is a subgroup of G if and only if*

1. *If $a, b \in H$, then $ab \in H$,*
2. *$1_G \in H$, and*
3. *If $a \in H$, then $a^{-1} \in H$.*

Trivially, if $H < G$, then $1_H = 1_G$.

The set $\langle a \rangle$ forms a group with operation of G. We call it the *subgroup generated by a*. If $|a| = k$, then $\langle a \rangle$ is a *cyclic subgroup of order k*. It is identical to $\mathbb{Z}_k$, the group of integers modulo k with addition.

Next, we classify the subgroups of $\mathbb{Z}$.

Lemma 5 (Bézout)**.** *Let $a, b \in \mathbb{Z}$. There exist $m, n \in \mathbb{Z}$ such that $am + bn = \gcd(a, b)$.*

Theorem 6. *Every subgroup of $\mathbb{Z}$ is generated by one element – that is, it has the form $\langle n \rangle = \{\dots, -2n, -n, 0, n, 2n, \dots\}$.*

The subgroup $\langle n \rangle$ of $\mathbb{Z}$ can also be denoted by $n\mathbb{Z}$.

We can list all the subgroups of $\mathbb{Z}$: they are $\{0\}, \mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, \dots$.