ES.S20: Group Theory

Formula and Notation Sheet

#1: Order of a Group

The order of the group G is the number of elements in the group G. We write $|G|$ to denote the order of the group G.

#2: Order of an Element

The order of an element a in the group G is the least integer r such that $a^r = 1$ in G.

#3: Lagrange's Theorem

We write $H \leq G$ to denote that H is a subgroup of G. (Remember: H is a subgroup of G if and only if H is a subset of G and H is a group in its own right.) If H is a subgroup of G, then order of H divides the order of G — that is, $|H| \, \Big| \, |G|$. The converse of Lagrange's theorem does not hold in general. (For instance, A_4 has no subgroup of order 6.)

#4: Abelian Groups

G is an Abelian group if and only if $ab = ba$ for all $a, b \in G$.

#5: Cyclic Groups

G is a cyclic group if and only if there is an element $a \in G$ such that $o(a) = |G|$. So, $G = \{a, a^2, a^3, \ldots, a^{r-1}, a^r = 1\}$. We write $G = \langle a \rangle$ and say G is generated by a.

#6: Cosets

We write $Hx = \{hx \,|\, \text{for all } h \in H \text{ and } x \in G\}$ to denote the right coset of H with representative x. Note that $|Hx| = |H|$ since $h_1 x = h_2 x$ if and only if $h_1 = h_2$. $Hx = Hy \iff xy^{-1} \in H$.

#7: Normal Subgroups

N is a normal subgroup of G if and only if $x^{-1}Nx = N$ for all $x \in G$. (So, N is a normal subgroup of G if and only if $Nx = xN$, which holds true if and only if $x^{-1}nx \in N$ for all $x \in G$ and all $n \in N$.)

#8: Simple Groups

A group G is called simple if and only if it has no proper normal subgroups N of G. So, if $N \lhd G$ and G is simple, then $N = \{1\}$ or $N = G$.

#9: Isomorphic Groups

Two groups G and H are isomorphic if and only if there is a map $\theta : G \mapsto H$ which is one-to-one and onto.

- **map:** A map θ is a rule which assigns to each element $g \in G$ an element $h \in H$.
- **one-to-one:** $g_1\theta = g_2\theta$ if and only if $g_1 = g_2$.
- **onto:** Given an $h \in H$, there is a $g \in G$ such that $g\theta = h$.

In addition, θ must preserve operations in G and H. That is, $(g_1g_2)\theta = (g_1\theta)(g_2\theta)$.

We write $G \cong H$ to denote that G and H are isomorphic. If G and H are isomorphic, we regard them as the "same group."

#10: Multiplicative Group of Integers Modulo n

$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ is the group with n elements. The n elements are infinite classes of elements corresponding to remainders on division by n.

- $\overline{0} = \{\text{all integers with remainder 0 on division by } n\} = \{0, \pm n, \pm 2n, \ldots\}$
- $\overline{k} = \{\text{all integers with remainder } k \text{ on division by } n\} = \{k, k \pm n, k \pm 2n, \ldots\}$

$\mathbb{Z}_n^* = \{\overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ has $n-1$ elements.
$\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ is a multiplicative group with $p-1$ elements when p is a prime.