Fill in the blanks as we finish our first pass on prerequisites of group theory.

1. **Subgroups, cosets**

Let $G$ be a group. Recall that a subgroup $H \leq G$ is a subset that is a group under the binary operation of $G$. The **subgroup criterion** says that $H \subseteq G$ is a subgroup if and only if $H$ is closed under the operation of $G$. It shows that if $\phi : G \to G'$ is a group homomorphism, then $\phi(H) \leq G'$ is a subgroup: $\phi(H)$ is a subgroup if and only if $\phi(H)$ is closed under the operation of $G'$.

Let $H \leq G$ be a subgroup. Define an equivalence relation on $G$ by $a \sim b$ if and only if $a^{-1}b \in H$. This is an equivalence relation because $\sim$ is reflexive, symmetric, and transitive. The equivalence classes are $aH = \{ah : h \in H\}$ for $a \in G$; note $aH = bH$ if and only if $H = a^{-1}bH$. Let $G/H$ be the set of equivalence classes.

We similarly define equivalence on the other side, with classes $Ha$ for $a \in G$, and write $H \setminus G$ for the set of equivalence classes.

**Lagrange’s theorem** states: $|G/H| = |G|/|H|$. It implies **Fermat’s little theorem**: $a^{p-1} \equiv 1 \pmod{p}$ because $a^{p-1} = (a^{p-1})^{\phi(p)} = 1^{\phi(p)} = 1$.

*Date:* Wednesday, 14 September 2016.
2. **Centralizer, normalizer, stabilizer**

Let $A \subseteq G$ be a subset. The **centralizer** of $A$ in $G$ is $C_A(G) =$ 

consisting of the elements of $G$ 

The centralizer $C_A(G) \leq G$ is a subgroup: 

The **center** of $G$ is $Z(G) = C_G(G)$. 

Similarly, the **normalizer** of $A$ in $G$ is $N_A(G) =$ 

Note that $C_G(A) \leq N_G(A)$. The normalizer $N_A(G) \leq G$ is a subgroup.

Let $G \circlearrowright X$ act on a set $X$. Let $x \in X$. The **stabilizer** of $x \in G$ is the set $\text{Stab}_G(x) = G_x = \{g \in G : gx = x\}$. We verify that $G_x \leq G$ is a subgroup. Recall that the kernel of the action is the subgroup 

(1) Let $G \circlearrowright X = G$ act on itself by conjugation, so that 

Then the centralizer of $A$ in terms of the group action is 

(2) Let $X = \mathcal{P}(G)$ be the **power set** of $G$, consisting of 

Then $G \circlearrowright X$ acts on $X$ by conjugation via $(g, A) \mapsto gAg^{-1} = \{gag^{-1} : a \in A\}$. Under this action, $N_G(A)$ is 

(3) Let the group $N_G(A) \circlearrowright A$ act on $A$ by conjugation. Then $C_G(A) \leq N_G(A)$ is 


3. Cyclic groups

A group $G$ is cyclic if $\ldots$, and we write $\ldots$. In this case, we have an isomorphism $\ldots$ Consequently, any two cyclic groups of the same order are isomorphic.

**Lemma.** Let $G$ be a cyclic group, generated by $x$, and let $a \in \mathbb{Z}$.

(a) If $x$ has infinite order, then $G = \langle x^a \rangle$ if and only if $\ldots$.

(b) If $x$ has order $n < \infty$, then $G = \langle x^a \rangle$ if and only if $\ldots$; in particular, the number of generators of $G$ is $\ldots$.

Every subgroup of a cyclic group is cyclic: $\ldots$

In fact, the subgroups of a finite cyclic group correspond bijectively with $\ldots$ via $\ldots$.
4. Generating subgroups

Let $G$ be a group. Given any nonempty collection $\{H_i\}_{i \in I}$ of subgroups of $G$, the intersection $\bigcap_{i \in I} H_i \leq G$ is a subgroup.

Let $A \subseteq G$. The subgroup generated by $A$, written $\langle A \rangle \subseteq G$, is

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

The subgroup generated by $A$ is the smallest subgroup of $G$ containing $A$ in the sense that

A more concrete way of thinking about $\langle A \rangle$ is that it consists of all elements of $G$ that can be written as words in elements of $A \cup A^{-1}$, where $A^{-1} = \{a^{-1} : a \in A\}$: this means

A subgroup $H \leq G$ is finitely generated if

Example. The subgroup of $\text{GL}_2(\mathbb{C})$ generated by

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

is

Example. The subgroup of $\text{GL}_2(\mathbb{Q})$ generated by

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

is infinite even though $S, T$ have orders

because

4
5. Kernels, normal subgroups, quotient groups

Let $\phi : G \to G'$ be a group homomorphism. The kernel of $\phi$ is the subgroup

$$\ker \phi = \{ g \in G : \phi(g) = e \} \leq G.$$ 

**Lemma.** $\phi$ is injective if and only if $\ker \phi = \{1\}$.

**Proof.** Proves itself. □

**Lemma.** Let $K \leq G$ be a subgroup. Then the following conditions are equivalent:

(i) For all $a \in G$, we have $aK = Ka$;

(ii) For all $a \in G$, we have $aKa^{-1} \subseteq K$; and

(iii) For all $a \in G$, we have $aKa^{-1} = K$.

**Proof.** Proves itself. □

A subgroup $K \leq G$ is normal if the equivalent conditions (i)–(iii) hold, and we write $K \trianglelefteq G$.

**Example.** Every subgroup of an abelian group is normal.

**Proposition.** If $K \leq G$, then $G/K$ is a group under $(aK)(bK) = abK$ if and only if $K \trianglelefteq G$.

**Proof.** Proves itself. □
If $K \trianglelefteq G$, then the group $G/K$ is the quotient group. Kernels of surjective group homomorphisms are the same as normal subgroups in the sense that 

In general, if $\phi : G \to G'$ is a group homomorphism, then it factors:

**Theorem** (First isomorphism theorem).

There are also three more isomorphism theorems, concerning intersections, quotients, and lattices.

*Example.* The group $\mathbb{Q}/\mathbb{Z}$ looks like 

. 
A (finite or infinite) group is simple if $\#G > 1$ and $\frac{N_{i+1}}{N_i}$ is a simple group for all $0 \leq i \leq k - 1$; we then call the set of groups $N_{i+1}/N_i$ the composition factors.

**Example.** A composition series for $S_3$ is:

**Example.** A composition series for $D_8$ is:

**Example.** A composition series for $A_4$ is:

**Example.** Let $F$ be a field with $\#F = p$. A composition series for the Heisenberg group $H(F)$ is:

**Theorem** (Jordan–Hölder). Every nontrivial finite group has a composition series and the composition factors in any composition series are unique (up to reordering).

To classify all finite groups, we classify all finite simple groups and then try to “put them back together” to get all finite groups.
Theorem. Every finite simple group is isomorphic to either one in a list of 18 infinite families of simple groups or one of 26 sporadic simple groups.

Examples of simple groups include:

• _________________________________

• _________________________________

• _________________________________