Math 418H **Fall 2005**

Lecture: Wed 11/31

1. Subgroups

   - Subgroup: $H \subset G$ closed under multiplication and inverses: if $a, b \in H$, then $ab, a^{-1} \in H$.
   - Informally, if $G = \mathrm{Sym}(X)$ is the symmetries of an object X, then $H = \mathrm{Sym}(\widetilde{X})$ is the symmetries of $\widetilde{X}$, which is X with some"decorations" added to make it less symmetric.

2. Cyclic subgroups

   - Abstract cyclic group: $C_n = \{\iota, x, x^2, \ldots, x^{n-1}\}$ with the relation $x^n = \iota$. An isomorphic group is $(\mathbb{Z}_n, +)$, clock addition modulo n, with the isomorphism $\mathbb{Z}_n \to C_n$, $j \mapsto x^j$.
   - Abstract infinite cyclic group: $C_\infty = \{\ldots, x^{-2}, x^{-1}, \iota, x, x^2, \ldots\}$, with no relations. This is isomorphic to $(\mathbb{Z}, +)$.
   - An element $a \in G$ generates the cyclic subgroup

     $$\langle a \rangle := \{\ldots, a^{-2}, a^{-1}, \iota, a, a^2, \ldots\}.$$

     This group can be finite (if $a^k = \iota$ for some $k \neq 0$) or infinite (if $a^k \neq \iota$ for all $k \neq 0$).
   - Order of an element: $\mathrm{ord}(a) := \min\{k > 0 \mid a^k = \iota\}$; also $\mathrm{ord}(a) := \infty$ if there is no such $k > 0$.
   - *Proposition:* $\langle a \rangle \cong C_m$, where $m = \mathrm{ord}(a)$.

     Proof. Suppose m is finite. I claim $a^j = a^k$ if and only if $j \equiv k \bmod m$. Indeed, if $a^j = a^k$, then $a^{j-k} = \iota$. Taking $j-k = qm+r$ for $0 \le r < m$, we have $\iota = a^{j-k} = a^{qm}a^r = a^r$. Since there cannot be any $0 < r < m$ with $a^r = \iota$, we must have $r = 0$, so $m|(j-k)$, meaining $j \equiv k \bmod m$. The reverse claim is obvious.

     Now consider the map $\langle a \rangle \to C_m$ defined by $a^j \mapsto x^j$. This is well-defined, since if $a^j = a^k$, then $j = qm + k$ and $x^j = x^{qm}x^k = x^k$. It is one-to-one since if $x^j = x^k$, then $j \equiv k \bmod m$, so $a^j = a^k$. It is clearly onto and respects multiplication.

     If m is infinite, then clearly $a^j \neq a^k$ for any $j \neq k$, and the isomorphism is obvious.

3. Product of groups

   - For groups G_1, G_2, the product is the set
   $$G_1 \times G_2 := \{\, (g_1, g_2) \mid g_1 \in G_1\,, g_2 \in G_2 \,\}\,,$$
   with componentwise multiplication: $(a_1, a_2)(b_1, b_2) := (a_1b_1, a_2b_2)\,.$ The identity is $\iota := (\iota_1, \iota_2)\,$, and $(g_1, g_2)^{-1} := (g_1^{-1}, g_2^{-1})\,.$
   - The product group contains copies of its factors: $G_1 \times \iota_2 \cong G_1$ and $\iota_1 \times G_2 \cong G_2\,.$ These copies commute:
   $$(g_1, \iota_2)(\iota_1, g_2) = (g_1, g_2) = (\iota_1, g_2)(g_1, \iota_2)\,.$$
   - *Theorem:* Every abelian (commutative) group G is isomorphic to a product of cyclic groups: $G \cong C_{n_1} \times C_{n_2} \times C_{n_3} \times \cdots$, where n_j are positive integers or ∞.

     This is a difficult theorem which we will not prove.

4. Cosets and Lagrange's Theorem

   - Given $H \subset G$ a subgroup, the H-coset of $g \in G$ is the set $gH := \{\, gh \mid h \in H \,\}\,.$ For example, for any $h \in H$ we have $hH = H$, since hH is a row of the multiplication table of H.
   - $G/H = \{gH \mid g \in G\}$ is the collection of all cosets.
   - *Lemma:* If two cosets overlap, then they are identical. That is, for $a, b \in G$, either $aH \cap bH = \emptyset$ or $aH = bH\,.$

     Proof. Suppose $aH \cap bH \neq \emptyset\,.$ An element in the intersection is of the form $ah_1 = bh_2$, so that $b = ah_1h_2^{-1}$. Thus $bH = ah_1h_2^{-1}H = aH$, since $hH = H$ for any $h \in H\,.$
   - *Lemma:* Any two cosets have the same number of elements: $|aH| = |bH|$ for any $a, b \in G\,.$

     Proof. The map $aH \to bH\,,\ ah \to bh$ is one-to-one, since if $bh_1 = bh_2$ then $h_1 = h_2$ and $ah_1 = ah_2\,.$ The map is obviously onto. Thus it is a bijection, a one-to-one correspondence between the cosets, which must thus have the same size.

5. Lagrange's Theorem

   - *Theorem:* If G is a finite group with $|G| = n$ elements and H is a subgroup with $|H| = m$ elements, then $m|n$: the order of a subgroup evenly divides the order of the group.

     Proof. By the above two lemmas, the cosets partition the n elements of G into disjoint subsets: $G = g_1H \cup \cdots \cup g_\ell H$, with each coset having m elements. Thus, $n = \ell m$ meaning $m|n\,.$ That is:
     $$|G| = |G/H|\ |H|\,.$$
   - *Theorem:* If $|G| = p$ a prime, then $G \cong C_p$ a cyclic group.

     Proof. Let $g \neq \iota \in G$. Then $\mathrm{ord}(g) := k > 1$, and by Lagrange's Theorem, $k|p$, so $k = p$. Thus the cyclic subgroup $\langle g \rangle \cong C_k = C_p$ is *all* of G, and $G \cong C_p\,..$