The Lecture Title

Scribe: Your Name

Date: Day, Mon, Date Year

1 Theorems About Groups

Let G be a group with identity e. (We use the short hand ab when we really mean $a \cdot b$, where $\cdot$ is the group operation).

Theorem 1.1. *The identity e is unique.*

Proof. Let $x \in G$. Assume that we somehow have e_1, e_2 are identities in G. Notice that $e_1 x = x = e_2 x$, and thus $e_1 x x^{-1} = e_2 x x^{-1}$. Since xx^{-1} is an identity, we must have $e_1 = e_2$.

■

Theorem 1.2. *Each element has a unique inverse.*

Proof. Suppose x has two inverses, a and b. Thus, $xa = xb = e$. If we multiply by a on both sides, we have $axa = axb$, or that $a = b$.

■

Theorem 1.3. $(ab)^{-1} = b^{-1}a^{-1}$

Proof. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Similarly we show that $b^{-1}a^{-1}$ has inverse ab.

■

A corollary - $(a_1 a_2 \dots a_k)^{-1} = a_k^{-1} a_{k-1}^{-1} \dots a_1^{-1}$.

Recall from last lecture that we saw $(\mathbb{Z}_4, +) \cong (\mathbb{Z}_5^*, \times)$, but the symmetry group for the rectangle was different. We also found that $(\mathbb{Z}_1 2, +) \cong (\mathbb{Z}_{13}^*, \times)$.

We define a cyclic group as any group that can be written in the form $\{g, g^2, g^3, \dots g^k = e\}$. g here is the generator of the group. Observe then that $(\mathbb{Z}_n, +)$ is always cyclic, as it is always generated by 1. We write this by saying that $(\mathbb{Z}_n, +) = \langle 1 \rangle$.

Question: is $\mathbb{Z}_n^*$ always cyclic? Is $\mathbb{Z}_p^*$ always cyclic?

The answer is no to the first question: notice that $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$, and each element is its own inverse. This is thus not cyclic and it's actually congruent to the rectangle group.

Theorem 1.4. *$\mathbb{Z}_p^*$ is cyclic.*

Proof omitted for brevity.

2 Euler's Totient

Define $\varphi(n)$ to be the number of integers $1 \leq x \leq n$ such that x is relatively prime to n. Notice that if p is prime, $\varphi(p) = p - 1$.

In general, suppose that $n = p_1^{e_1} \dots p_k^{e_k}$. We will compute this by complementary counting. First, we remove numbers that have a factor of p_i, of which there are $\frac{n}{p_i}$, where we do so for all p_i. This gives us (so far)

$$n - \left(\sum \frac{n}{p_i} \right)$$

However, we have already subtracted off too many - we've subtracted off all numbers that are a product of two primes one too many times, so we have to add them back:

$$n - \left(\sum \frac{n}{p_i} \right) + \left(\sum \frac{n}{p_i p_j} \right)$$

We continue in this fashion, adding and removing numbers from our set until we are left with

$$\varphi(n) = n - \left(\sum \frac{n}{p_i} \right) + \left(\sum \frac{n}{p_i p_j} \right) - \left(\sum \frac{n}{p_i p_j p_k} \right) + \ldots + (-1)^k \left(\sum \frac{n}{p_1 p_2 \dots p_k} \right)$$

If we factor, we actually have

$$\varphi(n) = n \prod \left(1 - \frac{1}{p_i} \right) = n \left(1 - \frac{1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \dots \left(1 - \frac{1}{p_k} \right)$$

This immediately tells us that $\varphi(p^k) = p^k - p^{k-1}$ for p prime. We also have that $\varphi(n)$ is multiplicative (to some extent): if m, n are relatively prime then

$$\varphi(mn) = \varphi(m)\varphi(n)$$

The proof is done by essentially applying the above formula: let m have prime factors p_i and n have prime factors q_j:

$$\varphi(mn) = mn \prod \left(1 - \frac{1}{p_i} \right) \prod \left(1 - \frac{1}{q_j} \right) = \left(m \prod \left(1 - \frac{1}{p_i} \right) \right) \left(n \prod \left(1 - \frac{1}{q_j} \right) \right) = \varphi(m)\varphi(n)$$

3 More Proofs with Groups

We now prove Lagrange's Theorem with this newfound knowledge: If H is a finite subgroup of the finite group G, then $\operatorname{ord}(H) | \operatorname{ord}(G)$, or $|H||G|$.

Proof. Consider all the cosets $\{aH\}$ of H for $a \in G$. We now claim that the distinct cosets partition G and all of them are the same size.

To prove this, we claim that two cosets only intersect if they are actually identical. We prove this by supposing that we have two cosets such that $aH \cap bH \neq \varnothing$. There must be some element c in both cosets such that $c = ah_1 = bh_2$. Let us take some element $z \in aH$ such that $z = ah_3$. Now, notice that $a = ch_1^{-1}$, so $z = ch_1^{-1}h_3 = bh_2h_1^{-1}h_3$. By closure, these h's multiplied together must be some other element in the group H, so $z \in bH$ for all z. Thus, $aH \subseteq bH$ and similarly, $bH \subseteq aH$, so $aH = bH$. Thus, all the distinct cosets will cover G exactly once.

We now prove the second statement. Let $f(h) = aH$ for all $h \in H$. Let $f(h_1) = f(h_2)$. Then, if we multiply by the inverse of a, we must have $h_1 = h_2$, so f is bijective.

With these two claims, each aH is the same size and non-overlapping and corresponds to a subgroup H. Thus, $|aH|||G|$ and thus $|H|||G|$.

■

We use these facts to show Euler's Totient Theorem and Fermat's Little Theorem:

$$a^{\varphi(m)} \equiv 1 \bmod m \quad a^{p-1} \equiv 1 \bmod p$$

Proof. Take the group $\mathbb{Z}_m^*$ which has $\varphi(m)$ elements. We pick some $a \in \mathbb{Z}_m^*$. Note that we must have $\gcd(a, m) = 1$. Now consider the group generated by a, $\langle a \rangle = \{a, a^2, a^3, \ldots a^k = e\}$. This is in fact a group (and we can check all of its properties easily). Thus, $\operatorname{ord}(\langle a \rangle) | \operatorname{ord}(\mathbb{Z}_m^*)$. As $a^k \equiv 1 \bmod m$ as a^k must be the identity, and $kt = \varphi(m)$, so $a^{kt} \equiv 1^t \equiv 1 \bmod m$, so then $a^{\varphi(m)} \equiv 1 \bmod m$.

Letting m be a prime gives Fermat's Little Theorem immediately.

■

Cool-down - find the orbits of each of the elements of $\mathbb{Z}_9^*$.