Group Theory

Lecture 4, Sunday November 13, 2022
Ari Feiglin

Definition 4.0.1:

If G is a group and $H \leq G$ is a subgroup of G, we define the following:

- A **right coset** of H is a set $Ha = \{ha \mid h \in H\}$ where $a \in G$.
- A **left coset** of H is a set $aH = \{ah \mid h \in H\}$ where $a \in G$.

Notice that if G is an abelian group, then the left and right cosets of a subgroup H are the same. Also notice that if $h \in H$ then $hH = H = Hh$, since $h^{-1} \in H$ so if $h' \in H$ then $h\big(h^{-1}h'\big) = h' \in hH$.
The principle property of cosets is that they form a partition of the group G. This is an important property which we will prove.

Proposition 4.0.2:

If H is a subgroup of G, then $\{gH \mid g \in G\}$ and $\{Hg \mid g \in G\}$ form partitions of G.

Proof:

We will show this for the left cosets of H. So we must show that if $gH \cap g'H \neq \varnothing$ then $gH = g'H$. Suppose $x \in gH \cap g'H$, so $x = gh = g'h'$ and therefore $g' = ghh'^{-1}$ and similarly $g = g'h'h^{-1}$. And so if $y \in g'H$ then $y = g'h'' = ghh'^{-1}h'' \in gH$ since H is subgroup, so $g'H \subseteq gH$. And similarly $gH \subseteq g'H$, so $gH = g'H$ as required.
And we will show that $\bigcup gH = G$. This is trivial since if $g \in G$ then since $e \in H$, $g \in gH$ so g is in the union. And every coset is a subset of G, so the union is equal to G.
Therefore the union of $\{gH \mid g \in G\}$ is G and the elements in the set are disjoint, therefore it is a partition as required.

■

Lemma 4.0.3:

If H is a subgroup of G and $g \in G$ then $|gH| = |Hg| = |H|$.

Proof:

We define a function $f\colon H \longrightarrow gH$ by $h \mapsto gh$. This is trivially surjective by definition, and it is injective since if $f(h) = f(h')$ then $gh = gh'$, so $h = h'$. And so f is a bijection and therefore $|H| = |gH|$. A similar proof is valid for right cosets.

■

Definition 4.0.4:

If H is a subgroup of the group G, we define its **index** to be the size of the partition its cosets form:

$$[G : H] = |\{gH \mid g \in G\}| = |\{Hg \mid g \in G\}|$$

And the set of left cosets is denoted G/H, so $[G : H] = |G/H|$.

Since the set of cosets of H forms a partition of G, and the cardinality of every gH is equal to the cardinality of H, we have that

$$|G| = |H| \cdot |\{gH \mid g \in G\}| = |H| \cdot [G : H]$$

Theorem 4.0.5 (Lagrange's Theorem):

If G is a finite group and H is a subgroup of G's, then $|H| \mid |G|$.

Therefore if $g \in G$, then the order of g divides the order of G (which is the cardinality of G), since $o(g) = |\langle g \rangle|$ and $\langle g \rangle$ is a subgroup of G.

Theorem 4.0.6 (Fermat's Little Theorem):

Suppose p is prime, then if a is coprime with p then $a^{p-1} \equiv 1 \pmod{p}$.

Proof:

Notice that the order of $\text{Euler}(p)$ is $p-1$ since it is equal to $\{1, \ldots, p-1\}$. Since a is coprime with p, its equivalence class is in $\text{Euler}(p)$, and the order of it divides $p-1$. That is $o(a) \mid p-1$, and therefore $a^{p-1} \equiv 1 \pmod{p}$ (since if $o(a) \mid n$ then $a^n = e$).

■

Definition 4.0.7:

Euler's Totient Function is a function $\varphi\colon \mathbb{N} \longrightarrow \mathbb{N}$ defined by:

$$\varphi(n) = |\text{Euler}(n)|$$

Notice that we know $a \in \text{Euler}(b)$ if and only if they are coprime, so we can rewrite the definition of the Euler Totient function as:

$$\varphi(n) = |\{1 \leq m < n \mid \gcd(n, m) = 1\}|$$

Theorem 4.0.8 (Euler's Totient Theorem):

If a is disjoint from n then:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Proof:

By the definition of the Euler Totient function, the order of $\text{Euler}(n)$ is $\varphi(n)$. Then since a is coprime from n it is in $\text{Euler}(n)$, and $o(a) \mid \varphi(n)$, $a^{\varphi(n)} \equiv 1 \pmod{n}$ as required. The reason for this is identical to the reason given in our proof of **Fermat's Little Theorem**.

■

Notice that $\varphi(p) = p-1$ for p prime, so by Euler's Totient theorem, if a is coprime from p then $a^{p-1} = a^{\varphi(p)} \equiv 1 \pmod{p}$. So Euler's Totient function is a generalization of Fermat's Little theorem.
In general if G is a finite group and $a \in G$ then $a^{|G|} = e$ since $o(a) \mid |G|$.

Proposition 4.0.9:

If H and K are subgroups of G, then $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.

Proof:

If one is the subset of the other, it is trivial. To prove the converse, suppose for the sake of a contradiction that neither is a subset of the other. Then there is $h \in H \setminus K$ and $k \in K \setminus H$. Then $h, k \in H \cup K$ but if $hk \in H \cup K$ then suppose without loss of generality that $hk \in H$ which means $k = h^{-1}h'$ for some $h' \in H$. And so $k \in H$ in contradiction. So one must be the subset of the other.

■

Definition 4.0.10:

If G is a group and $A, B \subseteq G$ are subsets, we define:

- $A \cdot B = \{ab \mid a \in A, b \in B\}$
- $A^{-1} = \left\{a^{-1} \mid a \in A\right\}$

Proposition 4.0.11:

If H and K are subgroups of G then $H \cdot K$ is a subgroup if and only if $H \cdot K = K \cdot H$.

Proof:

We know that A non empty is a subgroup if and only if it is closed under the operation and inverses, which is equivalent to saying $A \cdot A \subseteq A$ and $A^{-1} \subseteq A$. Also notice this is equivalent to $A \cdot A = A$ and $A^{-1} = A$.
So if $HK = KH$ then:

$$(HK)(HK) = HKHK = HHKK \subseteq HK$$

And

$$(HK)^{-1} = K^{-1}H^{-1} \subseteq KH = HK$$

So HK is a subgroup.
If HK is a subgroup, then since $HK = H^{-1}K^{-1} = (KH)^{-1} = KH$, that is $HK = KH$ as required.

∎

Proposition 4.0.12:

If H is a subgroup of G then the following are equivalent:

- For every $a \in G$ then $aH = Ha$ ($aHa^{-1} = H$).
- Every right coset is a left coset.
- For every $a \in G$, $Ha \subseteq aH$.
- For every $a \in G$, $aH \subseteq Ha$ ($aHa^{-1} \subseteq H$).
- For every $a, b \in G$, $aH \cdot aH = abH$.
- For every $a, b \in G$ there exists a $c \in G$ such that $aH \cdot bH = cH$.

Proof:

- 1 implies 2 trivially, and 2 implies 1 since aH is also a right coset Hb and therefore Hb has a non trivial intersection with Ha so they are equal, so $aH = Hb = Ha$.
- 1 implies 3 trivially.
- 3 implies 4 since if $a \in G$ then $Ha^{-1} \subseteq a^{-1}H$ so $aH \subseteq Ha$, and similarly 4 implies 3.
- And 3 implies 4 and together they imply 1, and 1 implies 3 and 4 trivially. So 1, 2, 3, and 4 are all equivalent.
- 5 implies 6 trivially, and since $ab \in aH \cdot bH = cH$, abH and cH have nontrivial intersection, $cH = abH$, so 6 implies 5.
- 1 implies 5 since $aHbH = abHH = abH$ (since $Hb = bH$).
- If we know 5 then if we choose $a = e$ then for every $b \in G$ we know $H \cdot bH = bH$ so $b \in Hb \subseteq HbH = bH$, so $Hb \subseteq bH$ for every $b \in G$, so 5 implies 3. So everything is equivalent.

Definition 4.0.13:

If any of the above properties hold for a subset H of G, then H is considered a **normal** subset of G and this is denoted $H \trianglelefteq G$.

To prove that a subgroup is normal, it is usually the easiest to prove the fourth property, $aHa^{-1} \subseteq H$.

Proposition 4.0.14:

If $H \trianglelefteq G$ then G/H forms a group under the operation $aH \cdot bH = abH$.

Proof:

We know that this operation is well defined and H is closed under it since H is normal, and H is the identity element since $H \cdot aH = aH \cdot H = aH$. And the inverse of aH is $a^{-1}H$ since $aH \cdot a^{-1}H = a^{-1}H \cdot aH = eH = H$. And it is associative since $(aH \cdot bH) \cdot cH = abH \cdot cH = abcH = aH \cdot (bH \cdot cH)$.

$\blacksquare$