COSETS, THEOREMS AND S_n

L. MARIZZA A BAILEY

1. Review

To review before we continue, below are some of the definitions we have already studied. If you would like examples illuminating each definition, look at the last two set of notes.

Definition 1. A *group* is a set G together with a binary operation $\cdot : G \times G \to G$ satisfying:

- **(G1)** $g_1(g_2g_3) = (g_1g_2)g_3$ for all $g_1, g_2, g_3 \in G$ (associativity);
- **(G2)** there exists $e \in G$ such that $e \cdot g = g \cdot e = g$ for all $g \in G$ (existence of an identity);
- **(G3)** for every $g \in G$ there exists $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$ (existence of inverses).

Definition 2 (Abelian)**.** A group is called *abelian* if its operation is commutative.

$$g * h = h * g$$

for all $g, h \in G$.

Definition 3. The *order* of a group, G, is denoted $|G|$ and is defined to be the cardinality of the set G.

Definition 4. A *subgroup*, H, of a group, $(G, *)$, is a subset of G such that $(H, *)$ is a group under the restriction of the binary operation on G.
If $H \subseteq G$ is a subgroup, we use the notation $H \leq G$.

Date: November 09, 2014.

2. Theorems

Proposition 1. *A subset $H \subseteq G$ of a group, G, is a subgroup of G if and only if:*

(H1) *H is nonempty*
(H2) *closure: For all $h_1, h_2 \in H$, then $h_1 * h_2 \in H$.*
(H3) *inverse: For all $h \in H$, $h^{-1} \in H$.*

Proof. We would like to show that if H satisfies the properties above, then H is a group under the operation of G. To show that H is a group, it must satisfy the properties of a group.
The property of **associativity** is inherited from the group G. For example, if $g, h, k \in H$, then by definition of subset, $g, h, k \in G$. By (G2), for all $g, h, k \in G$, then $(g * h) * k = g * (h * k)$.
If $h_1, h_2 \in H$ implies $h_1 * h_2 \in H$ then the function, $*$, on $G \times G$ restricts to a function on $H \times H$ into H. This makes $* : H \times H \to H$.
The third property of a group (inverses) is (H3), so there is no need for proof.
Finally, to show $1 \in H$, we need to use all (H1), (H3) and (H2).
Since H is nonempty, there exists $h \in H$.
If $h \in H$ then $h^{-1} \in H$ by (H3)
If $h, h^{-1} \in H$ then $h * h^{-1} = 1 \in H$ by (H2). □

We still have three properties we need to show, but, at least, we don't have to show associativity.
If you would like to show $H \leq G$ in two properties, there is a shorter method.

Corollary 1. *If G is a group, and $H \subseteq G$, then $H \leq G$ if and only if*

(A) *$H \neq \varnothing$*
(B) *If $h, k \in H$, then $hk^{-1} \in H$.*

We leave the proof as an exercise to the reader.

Corollary 2. *Let G be a group and H is a non-empty, finite subset of G. Then H is a subgroup of G if and only if*

$$h, k \in H \implies hk \in H$$

Proof. We will show that the assumption of the property implies that $H \leq G$.
Let $h \in H$.
Since H is closed, $h \in H$ implies $h^k \in H$ for all $k \in \mathbb{N}$ and $H \subseteq G$ implies H is finite.
Theref ore, $h^n = h^m$ for some $m \in \mathbb{N}$ where $m > n$.
Since $m > n$, then we can rewrite the equation above as $h^n = h^n h^{m-n}$.
This implies, by uniqueness of identity, $h^{m-n} = 1$.
We have already noted that $h \in H$ implies all powers of h, $h^k \in H$.
Therefore, $h^{m-n} = 1 \in H$.
By multiplying both sides by h, we get $h * h^{n-m} = h$ implies $h * h^{n-m-1} = 1$.
Thus $h^{n-m-1} = h^{-1}$ and is in H. □

Proposition 2. *If H and K are subgroups of G, then $H \cap K$ is a subgroup.*

Proof. Let H and K be subgroups of G.
To show $H \cap K$ is a subgroup, we must show it satisfies the three subgroup properties:
(H1) Nonempty
(H2) Closure
(H3) Inverse

Non-empty Since $1 \in H$ and $1 \in K$ then $1 \in H \cap K$. Therefore it isn't empty.
Closure Let $g_1, g_2 \in H \cap K$. Then $g_1, g_2 \in H$ and $g_1, g_2 \in K$.
By the closure property of subgroups H and K, $g_1 * g_2 \in H$ and $g_1 * g_2 \in K$.
Inverse Let $g \in H \cap K$.
Then $g \in H$ implies $g^{-1} \in G$ by inverse property of H.
Similarly, $g \in K$ implies $g^{-1} \in K$.
Therefore, $g^{-1} \in H \cap K$. □

Proposition 3. *Let G be a cyclic group. Then G is abelian.*

The proof of this is just a direct consequence of the exponential property, $g^k g^m = g^{k+m} = g^m g^k$.

Proposition 4. *Let G be a cyclic group and let $H \leq G$. Then H is cyclic.*

Proof. Let g be a generator for G. Then every element in G is of the form g^k for some $k \in \mathbb{Z}$.

If H is trivial, then $H = \langle 1 \rangle$ is cyclic. Suppose that H is nontrivial and let $h \in H \setminus \{1\}$. Then $h = g^k$ for some $k \in \mathbb{Z}$. If $k < 0$, then $h^{-1} = g^{-k} \in H$; thus H contains an element of the form g^k where k is a positive integer.

Let k be the smallest positive integer such that $g^k \in H$. Let $h \in H$; then $h = g^l$ for some $l \in \mathbb{Z}$. There exist unique $q, r \in \mathbb{Z}$ such that $l = kq + r$ where $0 \leq r < k$. Then

$$h = g^l = g^{kq+r} = (g^k)^q g^r.$$

Since $g^k \in H$, we have $g^r \in H$. But r is nonnegative and less then k, so we must have $r = 0$. Thus $h = (g^k)^q$, which proves that $H = \langle g^k \rangle$. □

Proposition 5. *Let G be a group and let $g \in G$ with $ord(g) = n < \infty$. Then*

- **(a)** *$i, j \in \{0, \ldots, n-1\}$ and $g^i = g^j \Rightarrow i = j$;*
- **(b)** *$\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$;*
- **(c)** *$|\langle g \rangle| = ord(g)$;*
- **(d)** *$|G| = ord(g)$ if and only if $G = \langle g \rangle$.*

The proofs of these statements will be left as an exercise to the reader.

2.1. **Exercises.**

Exercise 1. Show that $S \subseteq \mathbb{Z}_{15}$ defined by $S = \{n \in \mathbb{Z}_{15}^{+} \mid \text{ord}(n) = 3\}$ is a subgroup of $\mathbb{Z}_{15}$.

Exercise 2. Let G be an abelian group. Show $S = \{g \in G \mid \text{ord}(g) = m\}$ is a subgroup of G.
Find an example of a non-abelian group for which this is not true.

Exercise 3. Prove Corollary 1

Exercise 4. Let G and H be groups. How can we define an operation on $G \times H$ so that it is also a group.

Exercise 5. Prove Proposition 5

Exercise 6. Let

$$Z(G) = \{g \in G \mid ga = ag \forall a \in G\}$$

be the set of all elements which commute with everything in G.
Show this is a subgroup of G
It is called the center of G.

Exercise 7. Show that $\{e, \rho^2\}$ is the center of D_4.

Exercise 8. Find all generators for:

- **(a)** $\mathbb{Z}_6$
- **(b)** $\mathbb{Z}_{10}$
- **(c)** $\mathbb{Z}_{15}$
- **(d)** $\mathbb{Z}_7$

Make a conjecture about the relationship between the generators and $\mathbb{Z}_n$

3. Cosets

Now we will see how structured any group is by studying the relationship between the $|H|$ and $|G|$ whenever $H \leq G$.
Let $H \leq G$ be a subgroup.
Then a set defined by

$$gH = \{gh \mid h \in H\}$$

is called a left coset of H in G.
Similarly, a right coset of H in G is defined to be a set of the form

$$Hg = \{hg \mid h \in H\}$$

Lemma 1. *Let $f : H \to gH$ defined by $f(x) = gx$. Then f is a bijective function.*

Proof. To show f is bijective, we need to show f is surjective and injective.
First, let's prove f is surjective.
Let $k \in gH$.
Then, by definition, $k = gh$ for some $h \in H$.
Therefore, $f(h) = gh = k$.
This shows f is surjective.
To show f is injective, we need to show that $h_1 \neq h_2$ if and only if $f(h_1) \neq f(h_2)$.
Suppose $gh_1 \neq gh_2$, then by multiplying both sides g^{-1}, we get $g^{-1}gh_1 \neq g^{-1}gh_2$ or $h_1 \neq h_2$. □

Showing that f is bijective also shows that $|H| = |gH|$ for all $g \in G$.
Now let us see what happens if we assume that $|G|$ is finite.
If $|G| = n$ then clearly, $|H| \leq n$ and the number of cosets is less than n. We will now show that the collection of cosets of H,

$$S = \{H, g_2H, g_3H, g_4H, \ldots, g_mH\}$$

forms a partition of G.

Lemma 2. *Let G be a group, $H \leq G$, and $g_k, g_j \in G \setminus H$.*
If $g_j \notin g_kH$ then $g_jH \cap g_kH = \varnothing$.

Proof. We will prove this statement by proving the contrapositive.
Suppose $k \in g_jH \cap g_kH$.
Then $k = g_jh_1$ for some $h_1 \in H$ and $k = g_jh_2$ for some $h_2 \in H$.
By transitivity of equality, we know that for $h_1, h_2 \in H$

$$g_jh_1 = g_kh_2$$

Since $H \leq G$, then $h_2 \in H$ implies $h_2^{-1} \in H$.
Therefore $h_1h_2^{-1} \in H$, so multiplying both sides of the equation by h_2^{-1}, we get

$$g_jh_1h_2^{-1} = g_k$$

Since $h_1h_2^{-1} \in H$, then $g_k \in g_jH$.
This means that the only time there exists something in the intersection of $g_jH \cap g_kH$ is when $g_j \in g_kH$.

□

It is also rather easy to show that if $g_j \in g_k H$, then $g_j H = g_k H$.
To see this, note that for all $k \in g_j H$, $k = g_j h$ where $h \in H$.
Since $g_j \in g_k H$ then $g_j = g_k h'$ where $h' \in H$.
By substitution, $k = (g_k h')h = g_k(h'h)$.
Since $h, h' \in h$, then $h'h \in H$ and, therefore $k \in g_k H$.
This shows $g_j H \subseteq g_k H$. A similar argument shows that $g_k H \subseteq g_j H$.
Hence, $g_j H = g_k H$ if and only if $g_j \in g_k H$.

It is just as easy to show that

$$G = \bigcup_{g \in G} gH$$

To see this, not that for all $g \in G$, $g \in gH$, therefore it is in, at least, one coset of H.
Also, since $gH \subseteq G$ for all g, then $\bigcup_{g \in G} gH \subseteq G$.

Therefore, the distinct cosets of H form a partition of G.
Choosing a representative from each coset, we can let denote the cosets by

$$S = \{g_1 H, g_2 H, g_3 H, \ldots, g_m H\}$$

and since these cosets are mutually disjoint and they cover G, then

$$|G| = \sum_{i=1}^{m} |g_i H|$$

We also know that $|g_i H| = |H|$, which means that

$$|G| = \sum_{i=1}^{m} |H| = mH$$

Therefore $|H| \mid |G|$.

Definition 5. Let G be a finite group and $H \leq G$.
Suppose the number of cosets of H in G is m.
We the say **the index of H in G is** m**,** $[G : H] = m$**.**

Theorem 1 (LaGrange's Theorem)**.** *Let G be a finite group, and $H \leq G$.*
Then $|G| = |H|[G : H]$.

3.1. **Exercises.**

Exercise 9. Let G be a finite group of order n, $|G| = n$.
If $g \in G$ then $\text{ord}(g) \mid n$.

Exercise 10. Let G be a finite group and $H \leq G$ and $K \leq H$.
Then $[G : K] = [G : H][H : K]$.

Exercise 11. Let $G =< g >$ be a cyclic group generated by g such that $|G| = n$.
Show that for any $k \mid n$, there exists $h \in G$ such that $\text{ord}(h) = k$.

Exercise 12. Why is it impossible for there to be:

(A) an element of order 7 in Z_{10}.
(B) a subgroup of S_5 of order 14.
(C) a subgroup of S_4 of index 5.

Department of Mathematics, BASIS Scottsdale
E-mail address: marizza.bailey@basisscottsdale.org