Group Theory Exercises 4

Jason Sass

July 17, 2023

Cosets/Lagrange Theorem

Exercise 1. Let H and K be finite subgroups of a group G.
If the orders of H and K are relatively prime, then $H \cap K = \{e\}$.

Proof. Suppose the orders of H and K are relatively prime.
Let $m = |H|$ and $n = |K|$.
Then $\gcd(m, n) = 1$.
The intersection of any two groups is a subgroup, so $H \cap K < G$.

Suppose $H \cap K \neq \{e\}$.
Then there exists $g \in H \cap K$ such that $g \neq e$.
Hence, $g \in H$ and $g \in K$.
Let $s = |g|$.
Then by Lagrange, s divides m and s divides n, since H and K are finite groups.
Hence, s is a common divisor of m and n, so s divides $\gcd(m, n)$.
Hence, s divides 1, so $s = 1$.
Thus, $e = g^s = g^1 = g$, so $g = e$.
Therefore, we have $g = e$ and $g \neq e$, a contradiction.
Hence, $H \cap K = \{e\}$. ∎

Proposition 2. *Let H be a subgroup of G such that $[G : H] = 2$.*
If a and b are not in H, then $ab \in H$.

Solution. We must prove $(\forall a, b \in G)(a \notin H \land b \notin H \to ab \in H)$. ∎

Proof. Let $a, b \in G$ such that $a \notin H$ and $b \notin H$.
Since $[G : H] = 2$, then there are two distinct left cosets of H in G.
Since $e \in G$, then $eH = H$.
Thus, one of the left cosets is H.
Since $a \in aH$ and $a \notin H$, then $aH \neq H$.
Since aH is a left coset and $aH \neq H$ and there are exactly two left cosets of H in G, then aH is the other left coset.

Let L_H be the collection of all left cosets of H in G.
Then L_H is a partition of G and $L_H = \{H, aH\}$.
Since $a, b \in G$ and G is a group, then $ab \in G$.

Suppose $ab \notin H$.
Every element of G exists in exactly one left coset of H in G.
Hence, every element of G is in either H or in aH.
Since $ab \notin H$, then this implies $ab \in aH$.
Thus, there exists $h \in H$ such that $ab = ah$.
By the left cancellation law we obtain $b = h$.
Since $b = h$ and $h \in H$, then $b \in H$.
Thus, we have $b \notin H$ and $b \in H$, a contradiction.
Therefore, $ab \in H$. $\square$

Exercise 3. Let p, q be prime.
Let G be a group of order pq.
Then every proper subgroup of G is cyclic.

Proof. The smallest prime is 2.
Since p and q are prime, then the smallest value of the product pq is $2*2 = 4$.
Hence, $pq \geq 4$, so G cannot be the trivial group.
Let H be an arbitrary proper subgroup of G.
Since G is a finite group, then by LaGrange's theorem, the order of H divides the order of G.
Let n be the order of H.
Then $n \in \mathbb{Z}^+$ and $n|pq$.
Hence, either $n = 1$ or $n = p$ or $n = q$ or $n = pq$.

Any proper subgroup of G has order that is greater than 1 and less than pq.
Thus, $n > 1$ and $n < pq$, so $n \neq 1$ and $n \neq pq$.
Hence, either $n = p$ or $n = q$.
Therefore, H is a group of prime order.
Every group of prime order is cyclic, so H must be cyclic. $\square$

Exercise 4. Let G be a group with different subgroups H_1 and H_2.
If $|H_1| = |H_2| = 3$, then $H_1 \cap H_2 = \{e\}$.
G has an even number of elements of order 3.
The number of elements of order 5 is a multiple of 4.

Proof. Suppose $|H_1| = |H_2| = 3$.
Then H_1 and H_2 are groups of order 3.
Since 3 is prime, then H_1 and H_2 are cyclic.
Observe that $H_1 \cap H_2 \subset H_1$ and $H_1 \cap H_2 \subset H_2$.
Since H_1 and H_2 are finite, then $H_1 \cap H_2$ is finite.
Let e be the identity of G.
Since $H_1 < G$, then $e \in H_1$.
Since $H_2 < G$, then $e \in H_2$.

Thus, $e \in H_1 \cap H_2$, so $\{e\} \subset H_1 \cap H_2$.

Suppose for the sake of contradiction that there exists $x \in H_1 \cap H_2$ such that $x \neq e$.

Then $x \in H_1$ and $x \in H_2$.

Since $x \in H_1$ and $x \neq e$ and H_1 is a group of prime order, then x is a generator of H_1.

Let K_1 be the cyclic subgroup of H_1 generated by x.

Then $K_1 = H_1$.

Since $x \in H_2$ and $x \neq e$ and H_2 is a group of prime order, then x is a generator of H_2.

Let K_2 be the cyclic subgroup of H_2 generated by x.

Then $K_2 = H_2$.

The cyclic subgroup containing x is the smallest subgroup that contains x, so any subgroup that contains x must contain the cyclic subgroup generated by x.

In particular, $H_1 \cap H_2$ contains x, so $H_1 \cap H_2$ must contain K_1 and K_2.

Hence, $K_1 \subset H_1 \cap H_2$ and $K_2 \subset H_1 \cap H_2$.

Thus, $H_1 \subset H_1 \cap H_2$ and $H_2 \subset H_1 \cap H_2$.

Since $H_1 \cap H_2 \subset H_1$ and $H_1 \subset H_1 \cap H_2$, then $H_1 \cap H_2 = H_1$.

Since $H_1 \cap H_2 \subset H_2$ and $H_2 \subset H_1 \cap H_2$, then $H_1 \cap H_2 = H_2$.

Thus, $H_1 = H_2$.

Since H_1 and H_2 are different groups, then $H_1 \neq H_2$.

Hence, we have $H_1 = H_2$ and $H_1 \neq H_2$, a contradiction.

Therefore, there is no nonidentity element in $H_1 \cap H_2$.

Let $x \in H_1 \cap H_2$.

Then $x = e$.

Thus, $x \in H_1 \cap H_2$ implies $x \in \{e\}$.

Hence, $H_1 \cap H_2 \subset \{e\}$.

Since $H_1 \cap H_2 \subset \{e\}$ and $\{e\} \subset H_1 \cap H_2$, then $H_1 \cap H_2 = \{e\}$.

We prove G has an even number of elements of order 3.

Let $a \in G$ be an element of order 3.

Then a generates a cyclic subgroup of G of order 3.

Thus, $\langle a \rangle = \{e, a, a^2\}$.

Both a and a^2, the inverse of a, are elements of order 3 and $a \neq a^2$.

Thus, elements of order 3 occur in pairs, the element a and its inverse a^{-1}.

Thus, if G has k cyclic subgroups of order 3, then there must be $2k$ elements of order 3.

We prove the number of elements of order 5 is a multiple of 4.

Let $h \in G$ have order 5.

Then h generates a cyclic subgroup of G of order 5.

Thus, $\langle h \rangle = \{e, h, h^2, h^3, h^4\}$.

Hence, the generators of $\langle h \rangle$ are elements h^k such that $\gcd(k, 5) = 1$.

Thus the number of such generators is $\phi(5) = 5 - 1 = 4$.

Thus, there are 4 elements in the cyclic group generated by h that have order 5, namely, h, h^2, h^3, h^4.

Hence, $|e| = 1$ and $|h| = 5$ and $|h^2| = \frac{5}{\gcd(2,5)} = 5$ and $|h^3| = \frac{5}{\gcd(3,5)} = 5$ and $|h^4| = \frac{5}{\gcd(4,5)} = 5$. Therefore, $\langle h \rangle$ contains 4 elements of order 5.

Hence, each cyclic subgroup of order 5 has 4 elements of order 5.

Thus, if G has m cyclic subgroups of order 5, then there must be $4m$ elements of order 5. $\square$