Math 412. Quotient groups

Fix an arbitrary group $(G, \circ)$.

DEFINITION: A subgroup N of G is **normal** if for all $g \in G$, the left and right N-cosets gN and Ng are the *same* subsets of G.

NOTATION: If $H \subseteq G$ is *any subgroup*, then G/H denotes the set of left cosets of H in G. Its elements are *sets* denoted gH where $g \in G$. The cardinality of G/H is called the **index** of H in G.

DEFINITION/THEOREM 8.13: Let N be a *normal subgroup* of G. Then there is a well-defined binary operation on the set G/N defined as follows:

$$G/N \times G/N \to G/N \qquad g_1N \star g_2N = (g_1 \circ g_2)N$$

making G/N into a group. We call this the **quotient group** "G modulo N".

Part 1: The essentials.

A. WARMUP: Define the *sign map:*

$$S_n \to \{\pm 1\} \quad \sigma \mapsto 1 \text{ if } \sigma \text{ is even; } \sigma \mapsto -1 \text{ if } \sigma \text{ is odd.}$$

(1) Prove that sign map is a group homomorphism.
(2) Use the sign map to give a different proof that A_n is a normal subgroup of S_n for all n.
(3) Describe the A_n-cosets of S_n. Make a table to describe the quotient group structure S_n/A_n. What is the identity element?

Solution.

(1) By definition, if τ is a transposition then $\tau \mapsto -1$. Given any element $\sigma \in S_n$, if we write σ as a product of transpositions, say $\sigma = \tau_1 \dots \tau_k$, then $\sigma \mapsto (-1)^n$. Now if $\sigma' \in S_n$ is a product of r transpositions, $\sigma\sigma'$ is a product of $k+r$ transpositions, and

$$\sigma\sigma' \mapsto (-1)^{k+r} = (-1)^k(-1)^r.$$

(2) By definition, A_n is the kernel of the sign map, and we have shown that the kernel of a group homomorphism must be a normal subgroup.
(3) There are two cosets: A_n and $S_n \setminus A_n$, the last one being the set of odd permutations. The identity element in S_n/A_n is the coset A_n, and the group S_n/A_n is isomorphic to $\mathbb{Z}_2$.

B. OPERATIONS ON COSETS: Let $(G, \circ)$ be a group and let $N \subseteq G$ be a **normal** subgroup.

(1) Take arbitrary $ng \in Ng$. Prove that there exists $n' \in N$ such that $ng = gn'$.
(2) Take any $x \in g_1N$ and any $y \in g_2N$. Prove that $xy \in g_1g_2N$.
(3) Define a binary operation $\star$ on the set G/N of left N-cosets as follows:

$$G/N \times G/N \to G/N \qquad g_1N \star g_2N = (g_1 \circ g_2)N.$$

Think through the meaning: the elements of G/N are *sets* and the operation $\star$ combines two of these sets into a third set: how? Explain why the binary operation $\star$ is **well-defined.** Where are you using normality of N?
(4) Prove that the operation $\star$ in (4) is associative.
(5) Prove that N is an identity for the operation $\star$ in (4).
(6) Prove that every coset $gN \in G/N$ has an inverse under the operation $\star$ in (4).

(7) Conclude that $(G/N, \star)$ is a group.
(8) Does the set of **right cosets** also have a natural group structure? What is it? Does it differ from G/N?

Solution.

(1) Since N is normal, $Ng = gN$. Given $ng \in Ng = gN$, there exists $n' \in N$ such that $ng = gn'$.
(2) There exist some $n_1, n_2 \in N$ such that $x = g_1 n_1$ and $y = g_2 n_2$. Then
$$xy = g_1 n_1 g_2 n_2 = g_1(n_1 g_2) n_2.$$
We assumed that N is normal, so $n_1 g_2 \in N g_2 = g_2 N$. Let $n \in N$ be such that $n_1 g_2 = g_2 n$. Then
$$xy = g_1(n_1 g_2) n_2 = g_1(g_2 n) n_1 = (g_1 g_2)(n_1 n) \in (g_1 g_2)N.$$
(3) The problem could be that if we can write a coset in two different ways, say $g_1 N = h_1 N$, then when we multiply by another coset, say $g_2 N$, then there could be two different possible answers for $(g_1 N) \cdot (g_2 N)$:
   - One possible answer is $(g_1 g_2)N$;
   - another possible answer is $(h_1 g_2)N$.

   We need to check that we really only get one answer for each possible product; so we need to check that $(g_1 g_2)N = (h_1 g_2)N$. This is what we just did in the previous question!
   A similar problem arises with the second factor. So to check that our operation really is well-defined, we need to take any g_1, h_1, g_2, h_2 such that $g_1 N = h_1 N$ and $g_2 N = h_2 N$, and verify that $(g_1 g_2)N = (h_1 h_2)N$. Again, this is what the previous question says. This is equivalent to proving that $(g_1 g_2)(h_1 h_2)^{-1} \in N$.
(4) Now that we know the operation is well-defined, it is easy to check that properties of the operation on G pass to G/H. In particular, $\star$ is associative because the operation on G also is associative:
$$(gN \star hN) \star kN = (gh)N \star kN = ((gh)k)N = (g(hk))N = gN \star (hk)N = gN \star (hN \star kN).$$
(5) Given any $g \in G$,
$$gN \star eN = (ge)N = gN = (eg)N = eN \star gN.$$
(6) Let $g \in G$. Then
$$g^{-1}N \star gN = (g^{-1}g)N = N = (gg^{-1})N = gN \star g^{-1}N.$$
(7) We have shown that this is a set with an associative operation for which there is an identity and every element has an inverse, so this is a group.

C. FIRST EXAMPLES OF QUOTIENT GROUPS:

(1) In $(\mathbb{Z}, +)$, explain why $n\mathbb{Z}$ is a normal subgroup and describe the corresponding quotient group.
(2) For any group G, explain why G is a normal subgroup of itself. What is the quotient G/G?
(3) For any group G, explain why $\{e\}$ is a normal subgroup of G. What is the quotient $G/\{e\}$?

Solution.

(1) We have shown that every subgroup of an abelian group is normal, so $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. The quotient group is the group $(\mathbb{Z}_n, +)$.

(2) For every $g \in G$, $gGg^{-1} \subseteq G$, because G is closed for products. This means that G is a normal subgroup of G. The quotient G/G is the trivial group (with one element).
(3) For every $g \in G$, $g\{e\} = \{g\} = \{e\}g$, so the trivial subgroup is normal. The quotient group $G/\{e\}$ is isomorphic to G.

D. ANOTHER EXAMPLE. Let $G = \mathbb{Z}_{25}^{\times}$. Let N be the subgroup generated by $[7]$.

(1) Give a one-line proof that N is normal.
(2) List out the elements of G and of N. Compute the order of both. Compute the index of N in G.
(3) List out the elements of G/N; don't forget that each one is a *coset* (in particular, a set whose elements you should list).
(4) Give each coset in G/N a reasonable name. Now make a multiplication table for the group G/N, using these names. Is G/N abelian?

Solution.

(1) G is abelian, so N is a normal subgroup.
(2) $G = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$ and $N = \{1, 7, 24, 18\}$. So $|\mathbb{Z}_{25}^{\times}| = 5^2 - \frac{25}{5} = 20$ and $|\langle 7 \rangle| = 4$. By Lagrange's Theorem $[\mathbb{Z}_{25}^{\times} : \langle 7 \rangle] = \frac{20}{4} = 5$.
(3) $N = \{1, 7, 24, 18\}$, $2N = \{2, 14, 23, 11\}$, $3N = \{3, 21, 22, 4\}$, $6N = \{6, 17, 19, 8\}$, $9N = \{9, 13, 16, 12\}$.
(4) Actually, this is just $\mathbb{Z}_5$: it is a group of order 5. So yes, this is an abelian group, and writing a multiplication table is quite easy. What if we wanted to give an explicit isomorphism to $\mathbb{Z}_5$? Our isomorphism must send N to $[0]_5$. Now which element gets sent to $[1]_5$ does not matter: every element in $\mathbb{Z}_5$ is a generator! But once we pick what element goes to $[1]_5$, the others are completely determined. For example, we can have $2N \mapsto [1]_5$, $3N \mapsto [2]_5$, $6N \mapsto [3]_5$ and $9N \mapsto [4]_5$.

E. THE CANONICAL QUOTIENT MAP: Prove that the map

$$G \to G/N \qquad g \mapsto gN$$

is a group homomorphism. What is its kernel?

Solution. Write ϕ for the canonical map. Given $g, h \in G$, $\phi(gh) = (gh)N = gN \star hN = \phi(g)\phi(h)$. The kernel of the canonical map is N. This shows that given any normal subgroup N, there is always a group homomorphism with kernel N.

F. INDEX TWO. Suppose that H is an index two subgroup of G. Last time, we proved the

THEOREM: *Every subgroup of index two in G is normal.*

(1) Describe the quotient group G/H. What are its elements? What is the table?
(2) Find an example of an index two subgroup of D_n and describe its two cosets explicitly. Make a table for this group and describe the canonical quotient map $G \to G/H$ explicitly.

Solution.

(1) This is a group of order 2, so isomorphic to $\mathbb{Z}_2$. The elements are H and $G \setminus H$.
(2) The group of rotations! It has n elements, the n rotations.

G. PRODUCTS AND QUOTIENT GROUPS: Let K and H be arbitrary groups and let $G = K \times H$.

(1) Find a natural homomorphism $G \to H$ whose kernel K' is $K \times e_H$.
(2) Prove that K' is a normal subgroup of G, whose cosets are all of the form $K \times h$ for $h \in H$.
(3) Prove that G/K' is isomorphic to H.

Solution.

(1) Consider the projection onto the second component, meaning the map $\phi : G \longrightarrow H$ given by $\phi(k, h) = h$. Then $(k, h) \in K'$ if and only if $h = e_H$, or equivalently, $(k, h) \in K \times e_H$.
(2) Since K' is the kernel of of a group homomorphism, K' is normal. Now note that for each $h \in H$,
$$K \times h = \{(k, h) : k \in K\} = (e_K, h)\,(K \times e_H)\,.$$
On the other hand, given any left K-coset $(k, h)K'$, $(e_K, h) = (k, h)(k^{-1}, e_H) \in (k, h)K'$, so $(k, h)K' = (e_K, h)\,(K \times e_H)$. So every coset is of the form $K \times h$ for some h. Finally, if $h, h' \in H$, then $K \times h = K \times h'$ if and only if $(e, h^{-1})(e, h') \in K \times \{e\}$, or equivalently, $h^{-1}h' = e$.
(3) By the previous part, we have that $\{K \times h = (e_K, h)K' \ : \ h \in H\}$ is G/K', and no two elements of that list are repeated. Let $\psi : G/K' \to H$ be defined by $\psi(K \times h) = h$.
Let $h_1, h_2 \in H$. We have that $\psi(K \times h_1 \star K \times h_2) = \psi((e_K, h_1)K' \star (e_K, h_2)K') = \psi((e_K, h_1h_2)K') = \psi(K \times (h_1h_2)) = h_1h_2 = \psi(K \times h_1)\psi(K \times h_2)$, so ψ is a group homomorphism.
Let $h \in H$. We have that $\psi(K \times h) = h$, so ψ is surjective. Moreover, $\psi(K \times h) = e_H$ implies that $h = e_H$, so $K \times h = K'$, which is the identity in the group G/K'. Hence, ψ is injective.

H. What goes wrong if we try to define a group structure on the set of right cosets G/H where H is a *non-normal* subgroup of G? Try illustrating the problem with the non-normal subgroup $\langle(1\,2)\rangle$ in S_3.

Solution. The operation $g_1H \star g_2H = (g_1 \circ g_2)H$ from problem B is not well defined anymore, so there is no natural way of endowing G/H with a group structure. They don't usk as to, but we may try to prove this in full generality. Indeed, if H is a subgroup of G that is not normal, that means that there exists $g_2 \in G$ such that $g_2H \neq Hg_2$. Since g_2H and Hg_2 have the same number of elements, there exists $g_1 \in H$ such that $g_1g_2 \notin g_2H$, which implies that $g_1g_2H \neq g_2H$. Note that, since $g_2 \in H$, then $g_2H = H = eH$. But $(e \circ g_2)H \neq (g_1 \circ g_2)H$, so $\star$ is not well defined.

Let's illustrate this with an example. In the cosets adventure sheet, problem E2, we saw that if H is the subgroup of $G = \mathcal{S}_3$ generated by $(1, 2)$, then $(123)H \neq H(123)$, because $(23) = (12)(123) \notin (123)H = \{(123), (1, 3)\}$. Hence, $(12)(123)H \neq e(123)H = (123)H$, even though $(12)H = eH = H$, so the operation $\star$ is not well defined.

Part 2: Foreshadowing.

I. THE FIRST ISOMORPHISM THEOREM. Conjecture and prove **first isomorphism theorem** for groups.

Solution. The First Isomorphism Theorem says the following:

Given a surjective group homomorphism $\phi : G \longrightarrow H$, $H \cong G/\ker(\phi)$.

Here is a proof:

Consider the map $\psi : G/\ker(\phi) \longrightarrow H$ given by $\phi(\ker(\phi)g) = \phi(g)$.

This map ψ is well-defined: given $g, h \in G$ such that $g\ker(\phi) = h\ker(\phi)$, by definition we have $h^{-1}g \in \ker(\phi)$, so $\phi(h^{-1}g) = e$, and thus $\phi(g) = \phi(h)$.

Moreover, this map ψ is a group homomorphism:

$$\psi\left((gh)\ker(\phi)\right) = \phi(gh) = \phi(g)\phi(h) = \psi(g\ker(\phi))\psi(h\ker(\phi)).$$

Let's check that ψ is injective. Suppose that $\psi(g\ker(\phi)) = e_H$. We need to show that $g\ker(\phi) = \ker(\phi)$ (the identity in the quotient group $G/\ker(\phi)$), or equivalently, that $g \in \ker(\phi)$. But $\psi(g\ker(\phi)) = \phi(g) = e_H$, so $g \in \ker(\phi)$, like we wanted to show.

Finally, let's check that ψ is surjective. Let $h \in H$. Since ϕ is surjective by hypothesis, there exists $g \in G$ such that $\phi(g) = h$. By the definition of ψ, we have that $\psi(g\ker(\phi)) = h$. Hence, ψ is surjective.