UMASS AMHERST MATH 411 SECTION 2, FALL 2009, F. HAJIR

PROBLEM SET 5

Let us recap a bit what we have been doing lately. Our focus has been not on a group G alone, but on the more refined structure $H \leq G$ where G is a group and H is a subgroup of G. We have proved the Theorem of Lagrange, to the effect that $|H|$ divides $|G|$ (assuming the latter is finite of course!), by introducing an associated set G/H called the set of left cosets of H in G. We have shown that the left cosets of H in G [which are simply the "translates" of H by elements of G, i.e. subsets of G of the form gH where $g \in G$[1]] give a non-overlapping covering of G, i.e. a partition. Since the left cosets of H all have the same size as H, this means that G breaks up into $|G/H|$ subsets each of size $|H|$, giving us the fundamental identity

$$|G/H| = \frac{|G|}{|H|}, \qquad \text{or} \qquad |G| = |G/H||H|.$$

Recall that the notions of equivalence relation on a set and a partition of that set are essentially the same notion. Since the left cosets of H give a partition of G, they are simply the equivalence classes under an equivalence relation on G called *left-coset-H equivalence* given as follows: If $a, b \in G$, we write $a \sim_H b$ if and only if $aH = bH$. There are a number of equivalent ways of writing $aH = bH$ and all of them are useful depending on the situation you happen to be working in. I find it best to get familiar with all the different ways of expressing the equality of two cosets and one of the problems in this homework set will help you do that.

The process of going from a set G with an equivalence relation $\sim$ on it to a new set $G/\sim$, the set of equivalence classes of elements of G is an extremely important one in mathematics.

You might recall my phrase that "You must worship the definitions." You may also have noticed how much time we have already spent on defining what a group is, what a subgroup is, the kernel, the image, homomorphism, etc. All of these ideas crystallize and come into play now when we define a "Quotient Group." In mathematics, the objects we study are not as crucial as the *mappings between the objects.* This is one of the important themes that emerged in twentieth century mathematics. Given an object (say a vector space – if you recall what that is from M235 – or a group G), a major question is: What are the objects Γ of the same type (vector space, group, etc.) that are related to our given G in the sense that there is a non-trivial map (or "morphism") from G to Γ or from Γ to G? Here, the term "morphism" expresses the need that the "relations" we are looking for have to respect the internal structure of the objects in questions. For instance, if we are working with vector spaces, we would want this map to preserve the vector space operations, i.e. we want it to be a "linear transformation," (it is then given by some matrix once we choose bases for the source and target). If we are working with groups, then we want the map to be a group homomorphism.

[1]Recall that $gH = \{gh | h \in H\}$.

For example, suppose G is a group, and we ask: What are the groups J that admit an injective homomorphism $\phi : J \hookrightarrow G$? Recall that the image of a homomorphism is always a subgroup of the target group, so $\phi(J)$ is a subgroup of G and it is isomorphic to J. (Why is J isomorphic to $\phi(J)$?) Thus, an injective homomorphism $\phi : J \hookrightarrow G$ gives rise to a subgroup $\phi(J) \leq G$. On the other hand, if $H \leq G$ is a subgroup, then the identity map gives an injective homomorphism from H to G! (Make sure you understand the latter statement). In other words, the knowledge of all subgroups of G is tantamount to the knowledge of all injective homomorphisms $J \hookrightarrow G$. Clearly, if we want to understand a group G, then understanding its subgroups is very important, in the same way that if you want to understand the architecture of a building then you need to become familiar with the design of each of its floors.

Note that focussing on a subgroup H of a group G isolates certain elements of the group (those in H); in a sense, one does it by becoming blind to the elements of G not in H. As we said above, this process is like entering the building and trying to understand it from within. Accompanying this process of restricting attention to a subgroup H of a group G , there is a "dual" and equally important process for understanding a group G; it is to ignore completely what is happening inside H and try to see the structure of what is happending "outside H" so to speak. Going back to the building analogy, this process is akin to leaving the building and going outside to look at the shadows it throws on the ground. The shadow of a building can be highly revealing: for instance you might learn how many floors the building has from its shadow, whereas if you are studying the design of a particular floor, you wouldn't necessarily know how many such floors there are in the building.

So, getting back to mathematics, what precisely is this "process of completely ignoring what is happening inside H and trying to see the structure of what is happending outside H" that we talked about in the previous paragraph? It is the process of understanding the Quotients of G. I will now proceed with defining what this means.

Definition 0.1. Suppose G is a group. A group Q is called a *homomorphic image* of G if there exists a surjective homomorphism $G \twoheadrightarrow Q$.

Quotients of G are like shadows of it. By studying enough of its shadows, one can learn a great deal about a group. Let us note first that every group G has at least two quotients, namely G itself (use the identity isomorphism) and the trivial quotient $\{e\}$ (use the trivial map). (Are you having dejà vu? If you are not, then you should review your notes about subgroups; hint, hint.) Some groups have no other shadows except for the one-element group and the group itself. You might be tempted to call such groups "prime" groups via analogy with prime numbers (why?). The term that is actually used is "simple," which is pretty funny because understanding simple groups is in fact a very complex task; why? because simple groups are, so-to-speak, "shadowless" groups, so it's hard to understand them.

Definition 0.2. A group G is called *simple* if its only quotients are G and $\{e\}$.

Now I want to remind you how we define a group law on G/H, assuming that H is a normal subgroup of G. For $aH, bH \in G/H$, we define $aH * bH = abH$. The most subtle thing about this operation is its being well-defined. Once you check that, then it is very easy to see that it satisfies the group axioms. To see a conceptual reason why this operation is well-defined, see (6) in Problem 8.

Definition 0.3. If G is a group and H is a normal subgroup of G, then the group $(G/H, *, eH)$ with the operation $aH * bH = abH$ is called a *quotient of* G.

Note that since $H = \{e\}$ and $H = G$ are always normal subgroups of G, G/G and $G/\{e\}$ are always quotients of G.

PROBLEM 1. Suppose H is a subgroup of a group G and $a, b \in H$. Show that the following conditions are all equivalent.
(1) $aH = bH$
(2) $a \in bH$
(3) $b \in aH$
(4) $b^{-1}a \in H$
(5) $a^{-1}b \in H$
Hint: do this by "going in a cycle," 1 implies 2, 2 implies 3, etc. 4 implies 5, and 5 implies 6. Then you are done!
NOTE: A VERY USEFUL FACT which follows from this is that for all $a \in G$,

$$aH = H \Longleftrightarrow a \in H.$$

PROBLEM 2. Suppose G is a group, and H is a normal subgroup of G. Show that the operation $G/H \times G/H \to G/H$ given by $(aH, bH) \mapsto abH$ is a well-defined operation. In other words, prove that if $a, b, a', b' \in G$ satisfy $a'H = aH$, and $b'H = bH$ then $a'b'H = abH$. Now show that this operation turns G/H into a group, and that the map $G \to G/H$ given by $g \mapsto gH$ is a surjective group homomorphims with kernel H.

PROBLEM 3. Suppose $\psi : G \twoheadrightarrow Q$ is a surjective homomorphism, so Q is a homomorphic image of G. Let $H = \ker(\psi)$ be the kernel of this map. Recall that H is a normal subgroup of G [proof: if $g \in G$ and $h \in H$, $\psi(ghg^{-1}) = \psi(g)\psi(h)\psi(g^{-1})$. But $\psi(h) = e$, so $\psi(ghg^{-1}) = \psi(g)\psi(g)^{-1} = e$. Thus, $ghg^{-1} \in H$, proving that H is normal in G.] Since H is normal in G, we can give $(G/H, *, eH)$ a group structure via the operation $aH * bH = abH$ where the identity is the coset $H = eH$. Define a map $\Psi : G/H \to Q$ by $\Psi(gH) = \psi(g)$ for all $g \in G$.
(i) First show that $\Psi : G/H \to Q$ is a well-defined map.
(ii) Show that Ψ is a homomorphism.
(iii) Show that Ψ is bijective, concluding that G/H and Q are isomorphic.
Congratulations. You have just proven The First Isomorphism Theorem of Group Theory.

PROBLEM 4. Suppose G is a group and H is a normal subgroup of G. Show that there is a surjective homomorphism $G \to G/H$ where the group structure on G/H is given by $aH * bH = abH$.

Note that the conclusion of PROBLEMS 3 and 4 is rather profound: together they say that the quotients of G are precisely the homomorphic images of G.

PROBLEM 5. Show that a group G is simple if and only if its only **normal** subgroups are $\{e\}$ and G.

PROBLEM 6. Suppose G is a finite group and Q is a homomorphic image of G. Show that Q is also a finite group and that its order divides the order of G.

Definition 0.4. Recall that if G is a group and $x \in G$, then

$$\langle x \rangle = \{x^n | n \in \mathbb{Z}\}$$

is the *subgroup generated by* x. A group G is called *cyclic* if there exists $x \in G$ such that $\langle x \rangle = G$. In other words, G is cyclic if it can be generated by one element x, which is then called a generator of G.

PROBLEM 7. Suppose G is a finite group. Show that G is a cyclic group if and only if there exists $x \in G$ such that $\text{ord}_G(x) = |G|$.

PROBLEM 8. Suppose G is a group of prime order p.

(i) Show that G is a cyclic group. [take a non-trivial guy in G and ask him what his order is].

(ii) Show that G is a simple group. [take a non-trivial subgroup H of G and ask her what her order is].

PROBLEM 9. (a) Suppose G is a cyclic group and Q is a homomorphic image of G, i.e. there is a surjective homomorphism $f : G \to Q$. Show that Q is also a cyclic group. Hint: You are looking for a generator of Q, right? Maybe G can "lend" you her generator...but how do you get elements of G over to Q?

(b) Show that $\mathbb{Z}$ is a cyclic group. Hint: dont' work too hard!

(c) Show that if $G = \mathbb{Z}$ and $H = n\mathbb{Z}$ for some positive integer n, then $G/H = \mathbb{Z}/n\mathbb{Z}$ is a cyclic group of order n. Hint: Use (a) and (b) and the canonical surjective homomorphism from a group to its quotient group.

PROBLEM 10. Suppose G is a group and H is a subgroup of G. Show that the following conditions are all equivalent. If any (hence all) of these conditions hold, we say that H is a *normal* subgroup of G.

(1) for all $g \in G$ and $h \in H$, $ghg^{-1} \in H$.

(2) for all $g \in G$, $gHg^{-1} \subseteq H$. [2]

(3) for all $g \in G$, $gHg^{-1} = H$.

(4) for all $g \in G$, $gH = Hg$. (you've already done this one, but just do it again: it doesn't hurt, and it's good to have it here as a reminder and a reference).

(5) for all $a \in G$ and $h_1 \in H$, there exists $h_2 \in H$ such that $ah_1 = h_2a$.

(6) for all $a, b \in G$, $aHbH = abH$ where $aHbH = \{ah_1bh_2 | h_1, h_2 \in H\}$.

(7) there exists a group Q and a surjective homomorphism $\psi : G \to Q$ with kernel $\ker(\psi) = H$.

Hint: You may want to do this by showing

$$(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (5) \Rightarrow (6) \Rightarrow (7) \Rightarrow (1),$$

[2]Recall that $gHg^{-1} = \{ghg^{-1} | h \in H\}$.

instead of (1) if and only if (2) and then (2) if and only if (3) etc. which would require a lot more writing.