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

HOMEWORK 3: DUE OCT. 8 2009

READINGS: These notes are intended as a SUPPLEMENT TO THE TEXTBOOK, NOT A REPLACEMENT FOR IT.

This homework has two sections. The first section covers material from Math 300; I am not requiring you to do the first section, but I am including it for those students who need a reminder about partitions and equivalence classes.

**** ONLY HAND IN SECTION 2 **** But feel free to solve the problems in section 1 as well if you wish. Please also note that almost everything in section 2 is material that we have already covered in detail in class. By asking you write up the solutions to these problems, I am emphasizing the importance of this material and hope that this will help you gain a solid understanding of the concepts related to the proof of Lagrange's theorem.

1. Equivalence Relations

Definition 1.1. Suppose X is a set. Let R be a subset of $X \times X$. We say that R determines a *relation* $\sim_R$ on X in the following way: if $a, b \in X$, then $a \sim_R b$ if and only if $(a, b) \in R$. We usually drop the subscript from $\sim_R$ and just write $\sim$ instead of $\sim_R$.

Suppose R satisfies the following three properties: (1) for all $x \in X$, $(x, x) \in R$, i.e. the "diagonal" is in R; (2) if $(a, b) \in R$, then $(b, a) \in R$ also. (3) If $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$. When these conditions hold, we say that R is an *equivalence relation.* In other words, a relation $\sim$ is an equivalence relation if and only if it is (1) reflexive: $a \sim a$ for all $a \in X$; (2) symmetric: $a \sim b$ implies $b \sim a$, and (3) transitive: if $a \sim b$ and $b \sim c$, then $a \sim c$.

For example, consider the set $\mathbb{Z}$ of all integers. Let us write $a \sim b$ whenever a and b have the same parity. In other words, $a \sim b$ means that a and b are both odd or they are both even. Another way to say this is that $a - b$ is even. Let us check that this defines an equivalence relation on $\mathbb{Z}$: first, $a - a$ is always 0 hence always even. If $a - b$ is even, then $b - a = -(a - b)$ is also even. If $a - b$ and $b - c$ are even, then $a - c$ is even, because $a - c = (a - b) + (b - c)$. Thus, this defines an equivalence relation on $\mathbb{Z}$.

PROBLEM 1. Consider the following relation on $\mathbb{Z}$: if $a, b \in \mathbb{Z}$, then $a \sim b$ if and only if $a \cdot b$ is even. Prove or Disprove: $\sim$ defines an equivalence relation on $\mathbb{Z}$.

Now suppose X is a set and $\sim$ is an equivalence relation on X. Then $\sim$ *partitions* the set. You might say, it polarizes the set into non-overlapping "cliques" of equivalent elements. If $x \in X$, then all the elements of X that are equivalent to x form the "clique" (technical term: equivalence class) of x. We might write

$$\mathrm{Eq}(x) = \{y \in X | x \sim y\}$$

for the equivalence class of x. Note that every element is equivalent to herself, so $\mathrm{Eq}(x)$ is never empty (because $x \in \mathrm{Eq}(x)$). On the other hand, if x and z and two elements of X, then their equivalence classes $\mathrm{Eq}(x)$ and $\mathrm{Eq}(z)$ are either identical or disjoint (two sets are called disjoint if their intersection is the empty set $\emptyset$).

PROBLEM 2. Suppose X is a set and $\sim$ is an equivalence relation on X. Suppose $x, z \in X$. Prove that either $\mathrm{Eq}(x) = \mathrm{Eq}(z)$ or else $\mathrm{Eq}(x) \cap \mathrm{Eq}(z) = \emptyset$.

Definition 1.2. Suppose X is a set and $\{X_\alpha | \alpha \in A\}$ is a collection of subsets of X. We say that $\{X_\alpha\}$ is a *partition* of X if (1) for all $\alpha, \beta \in A$, $X_\alpha \cap X_\beta = \emptyset$; (2) $\cup_{\alpha \in A} X_\alpha = X$. In other words, the subests X_α are non-overlapping and together entirely cover X. Equivalently, $\{X_\alpha | \alpha \in A\}$ is a partition of X means that for every $x \in X$ there exists a unique $\alpha \in A$ such that $x \in X_\alpha$.

For example, let $X = \mathbb{Z}$, let $A = \{0, 1\}$, let X_0 bet the set of even integers, and let X_1 be the set of odd integers. Then $\{X_0, X_1\}$ is a partition of $\mathbb{Z}$ because every integer is either odd or even (and no integer is both odd and even). You may note that this partition is mandated by the parity equivalence relation we discussed earlier. If we impose the parity relation on the integers and then order all the integers to band together into the corresponding cliques, we will have exactly two cliques, the evens and the odds, i.e. X_0 and X_1.

PROBLEM 3. In this problem, you will show that the two concepts of "equivalence relation on a set X" and "partition of X" are really the same concept.

(a) Suppose X is a set equipped with an equivalence relation $\sim$. Show the the set of equivalence classes of X under $\sim$ is a partition of X.

(b) Conversely, suppose $\{X_\alpha | \alpha \in A\}$ is a partition of a set X. Now define a relation on X as follows: if $x, y \in X$, then $x \sim y$ if and only if there exists $\alpha \in A$ such that $x, y \in X_\alpha$. Prove that $\sim$ is an equivalence relation on X.

Definition 1.3. If X is a set and $\sim$ is an equivalence relation on X, then X breaks up (is partitioned into) non-overlapping spanning equivalence classes. The set of these equivalence classes is denoted $X/\sim$ and called "X modulo $\sim$."

For example, for $\mathbb{Z}$ under the parity equivlance, the set $\mathbb{Z}/\sim$ is the set $\{X_0, X_1\}$ consisting of two elements. Note that the elements of $\mathbb{Z}/\sim$ are themselves sets: X_0 is the set of even integers and X_1 is the set of odd integers, but as elements of the set $\mathbb{Z}/\sim$, we just think of them as "the even equivalence class" and the "the odd equivalence class." One psychological technique is to say that the equivalence relation gloms all odds together into one object and all the evens together into another object (it "forgets" or erases the distinguishing features of the integers and remembers only their parity).

PROBLEM 4. Suppose $X = \mathbb{Z}$ is the set of integers, and let n be a positive integer. Define an equivalence relation on X as follows. For $a, b \in \mathbb{Z}$, we write $a \sim_n b$ if and only if n divides $a - b$. The more common notation is $a \equiv b \bmod n$.

(i) Show that this really is an equivalence relation.

(ii) Show that if $n = 1$, then all integers are equivalent to each other.

(iii) Show that if $n = 2$, then the resulting equivalence relation is the parity equivalence relation discussed above.

(iv) Show that under $\sim_n$, $\mathbb{Z}$ breaks up into n equivalence relations corresponding to the n possible remainders $0, 1, 2, \cdots, n-1$ for division by n.

(v) By (iv), we can write $\mathbb{Z}/\sim_n$ be the set $\{X_0, X_1, \cdots, X_{n-1}\}$ where

$$X_j = \{a \in \mathbb{Z} | \text{ the remainder of } a \text{ divided by } n \text{ is } j\}.$$

(vi) We define a group law on $\mathbb{Z}/\sim_n$ as follows: $X_j + X_k = X_l$ where l is the remainder of $j + k$ divided by n. Show that this makes $\mathbb{Z}/\sim_n$ into a commutative group.

(vii) Show that the map $(\mathbb{Z}, +, 0) \to (\mathbb{Z}/\sim_n, +, X_0)$ given by $a \mapsto X_r$ where r is the remainder of a divided by n is a surjective group homomorphism with kernel $n\mathbb{Z}$.

2. Cosets

Let $(G, *, e)$ be a group.

Let H be a subgroup of G.

Let us recall what this means:

(1) whenever, elements of H are composed together, the resulting element of G is actually in H, i.e. if $h_1, h_2 \in H$, then $h_1 * h_2 \in H$. In other words, if we banish from our minds the elements of G that are not in H and keep only the elements of H, then the law of composition on G actually becomes a law of composition on H.

That's only the first condition for being a subgroup, however. We also need:

(2) for every element of H, the inverse of it is also in H: $\forall h \in H$, $h^{-1} \in H$.

And finally,

(3) $e \in H$.

If we have these three conditions, then H inherits a composition law from G under which H itself becomes a group.

PROBLEM 5. Obviously condition (3) implies that

(3') H is not the empty set.

Show that a subest H of a group G which satisfies (1), (2) and (3') is automatically a subgroup of G.

Now, whenever G is a group and H is a subgroup of G, we automatically obtain an *equivalence relation* on the set G in the following way.

Definition 2.1. Suppose $(G, *, e)$ is a group and H is a subgroup of H. We then get a corresponding equivalence relation (called **left-coset H-equivalence** on the set G by the following rule: for $a, b \in G$, we write $a \sim b$ if and only if $a^{-1} * b \in H$.

PROBLEM 6. Verify that the definition we have given really does give an equivalence relation on G. In other words, show that this relation is reflexive, symmetric and transitive.

Even after doing the above problem, the definition we just gave seems kind of bogus, in that we seem to have concted it out of thin air. Perhaps it is more illuminating to see what left-coset H-equivalence means in terms of the partition of G which corresponds to it. First of all, let us show that under this equivalence, $\text{Eq}(e) = H$. Well, for $a \in G$, $e \sim a$ if and only if $e^{-1} * a \in H$ i.e. if and only if $a \in H$. Thus, $\mathrm{Eq}(e) = H$. Now let us make a very important definition.

Definition 2.2. If $(G, *, e)$ is a group and H is a subgroup of G, and $a \in G$, then the left coset of G associated to a is the following subset of G:

$$a * H = \{a * h | h \in H\}$$

Note that the left coset of H associated to e is simply H itself. Also, if $a \in H$, then $a * H = H$. Here is why: first $a * H \subseteq H$ because H is a subgroup (composing a with some guy in H produces yet again someone in H). On the other hand, $H \subseteq aH$: if $h \in H$ is any given element of H, then $h = a * (a^{-1} * h)$ by associativity. On the other hand, since $a \in H$, $a^{-1} \in H$ and so $h_1 = a^{-1} * h \in H$ again since H is a subgroup. Thus, $h = a * h_1 \in a * H$. We have shown that $aH \subseteq H$ and $H \subseteq aH$ hence $aH = H$.

PROBLEM 7. Recall G is a group, H is a subgroup of G. We define for $a, b \in G$, $a \sim b$ if and only if $a^{-1}b \in H$, and have shown that this is an equivalence relation in the preceding problem. Now show that the equivalence classes of G under this equivalence relation are precisely the left cosets of H. Thus, the left cosets of H form a partition of G.

PROBLEM 8. Suppose $a, b \in G$ and consider the corresponding left cosets of H, namely $a * H$ and $b * H$. Give a bijection of sets from $a * H$ to $b * H$ (Hint: you can go from a to b via multiplication on the left by c where $c = ba^{-1}$). Supposing that H is finite, therefore, we have $|a * H| = |b * H|$.

PROBLEM 9. Now suppose G is a finite group. Show that $|H|$ divides $|G|$. This is called Lagrange's theorem.

PROBLEM 10. Let $G = S_4$ and H be the subset consisting of those permutations that fix 1. Show that H is a subgroup. Write down the elements of H. How many elements does H have? Now list the left cosets of H. How many of them are there? Could you have predicted that once you had calculated $|H|$?