MA 274: EQUIVALENCE RELATIONS

1. EQUIVALENCE RELATIONS

Definition 1.1. Let A be a set. An **equivalence relation** on A is a relation $\sim$ such that:

(1) $\sim$ is **reflexive**. That is,

$$\forall x \in A, x \sim x.$$

(2) $\sim$ is **symmetric**. That is,

$$(x \sim y) \Rightarrow (y \sim x)$$

(3) $\sim$ is **transitive**. That is, if $(x \sim y)$ and if $(y \sim z)$ then $(x \sim z)$.

Example 1.2. (1) The relation "$=$" is an equivalence relation.

(2) For integers a, b define $a \sim b$ if and only if $a - b$ is even. Then $\sim$ is an equivalence relation.

(3) For integers, a, b define $a \sim b$ if and only if $a - b$ is a multiple of 3. Then $\sim$ is an equivalence relation.

(4) Let k be an integer. Define $a \sim b$ if and only if $a - b$ is a multiple of k. Then $\sim$ is an equivalence relation.

(5) For real numbers x and y, define $x \sim y$ if and only if $x - y$ is an integer multiple of 2π. Then $\sim$ is an equivalence relation.

(6) For real numbers x and y, define $x \sim y$ if and only if $x - y$ is a rational number. Then $\sim$ is an equivalence relation.

(7) Let A be a set and let $U \subset A$ be a subset. Define $x \sim y$ if and only if either both x and y are elements of U or both x and y are not elements of U. Then $\sim$ is an equivalence relation.

(8) Let A and B be finite subsets of a common universal set. Define $A \sim B$ if and only if A and B have the same number of elements.

Date: March 31, 2014.

(9) Let f and g be continuous functions on the interval $[0,1] \subset \mathbb{R}$. Define $f \sim g$ if and only if
$$\int_0^1 f\,dx = \int_0^1 g\,dx$$
Then $\sim$ is an equivalence relation.

(10) Let f and g be differentiable functions on the interval $(0,1) \subset \mathbb{R}$. Define $f \sim g$ if and only if
$$\forall x \in (0,1), f'(x) = g'(x)$$

(11) Let S be the set of all sequences in $[0,1] \subset \mathbb{R}$ that converge in $[0,1]$. For (s_n) and (t_n) in S, define
$$(s_n) \sim (t_n)$$
if and only if (s_n) and (t_n) have the same limit. Then $\sim$ is an equivalence relation on S.

Exercise 1.3. For each of the following relations determine whether they are reflexive, symmetric, or transitive and state whether or not they are an equivalence relation. Write your answers in "good-proof" style.

(1) Let a and b be non-zero integers. Define $a \sim b$ if and only if b is divisible by a.
(2) Let a and b be points in $\mathbb{R}^2$. Define $a \sim b$ if and only if $d(a,b) \leq 1$. (Here $d(a,b)$ is the distance from a to b.)
(3) Let a and b be real numbers. Define $a \sim b$ if and only if $d(a,b) \geq 1$. (Here $d(a,b)$ is the distance from a to b.)

Definition 1.4. Let A be a set and let $\sim$ be an equivalence relation on A. For each $x \in A$ define **the equivalence class of** x to be:
$$[x] = \{y \in A : x \sim y\}.$$

Example 1.5. Let $\sim$ be the equivalence relation on the integers defined by $x \sim y$ if and only if $x - y$ is even. Then there are precisely two equivalence classes: the even integers and the odd integers.

Example 1.6. Let A be a set and let $B \subset A$. Let $\sim$ be the equivalence relation on A defined by $x \sim y$ if and only if either both x and y are in B or both x and y are not in B. There are precisely two equivalence classes: B and $A \backslash B$.

Theorem 1.7. Suppose that $\sim$ is an equivalence relation on a set A. Then:

(1) If $x \in A$, then $x \in [x]$.

(2) If $x, y \in A$ and $x \in [y]$, then $[x] \subset [y]$.

(3) If $x, y \in A$ and $x \in [y]$, then $[x] = [y]$

(4) If $x, y \in A$ and if there exists $z \in [x] \cap [y]$, then $[x] = [y]$.

(Remark: the third conclusion of the previous theorem is extremely important. The others are just steps leading up to it.)

Definition 1.8. Let $\sim$ be an equivalence relation on a set A. Define the **quotient set** $A/\!\sim\, \subset \mathscr{P}(A)$ by

$$A/\!\sim\, = \{[x] \in \mathscr{P}(A) : x \in A\}$$

Theorem 1.9. If $[x]$ and $[y]$ are elements of a quotient set $A/\!\sim$ then either $[x] \cap [y] = \varnothing$ or $[x] = [y]$.

(Hint: You have done all the hard work for this theorem already in Theorem 1.7. Just figure out how to make use of that work here.)

2. Partitions

Partitions and Equivalence Relations are, at heart, the same concept. Sometimes, however, the language of equivalence relations is more useful and sometimes the language of partitions is more useful.

Definition 2.1. Let X be a set and let $\mathscr{U} \subset \mathscr{P}(X)$. Then $\mathscr{U}$ is a **partition** of X if and only if the following hold:

(1) (disjointness) If $U_1, U_2 \in \mathscr{U}$ then either $U_1 \cap U_2 = \varnothing$ or $U_1 = U_2$.

(2) (covering) For all $x \in X$, there exists $U \in \mathscr{U}$ such that $x \in U$.

That is, the sets in a partition of X are pairwise disjoint and they cover X.

Example 2.2. Here are some partitions of the real numbers:

(1) $\{\mathbb{R}\}$
(2) $\Big\{\{x\} : x \in \mathbb{R}\Big\}$
(3) $\{(-\infty, 0], (0, \infty)\}$
(4) $\Big\{(n, n+1] : n \in \mathbb{Z}\Big\}$.

Exercise 2.3. Let X be a non-empty set. Prove the following:

(1) $\{X\}$ is a partition of X.

(2) $\Big\{\{x\} : x \in X\Big\}$ is a partition of X.

Exercise 2.4. In each of the following exercises, find a partition of $\mathbb{N}$ satisfying the requirement.

(1) All the sets in partition have exactly two elements.
(2) There are exactly three sets in the partition
(3) There are infinitely many sets in the partition and each set in the partition has infinitely many elements.

Theorem 2.5. If A is a set and if $\sim$ is an equivalence relation on A, then $A/\sim$ is a partition of A.

Theorem 2.6. Let X be a set and let $\mathscr{U}$ be a partition of X. For $x, y \in X$, define $x \sim y$ if and only if there exists $U \in \mathscr{U}$ such that $x \in U$ and $y \in U$.

The previous two theorems together show that equivalence relations and partitions are nearly the same concept.

3. The meaning of equivalence relations

The purpose of this section is to give some idea as two why the notions of equivalence relations, partitions, and quotient sets are important.

Example 3.1. Define the following equivalence relation on $\mathbb{Z} \times (\mathbb{Z} \backslash \{0\})$:

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc.$$

Then $(\mathbb{Z} \times \mathbb{Z})/\sim$ "is" the rational numbers. More about this later.

Example 3.2. Let $\sim$ be the equivalence relation on $\mathbb{R}$ defined by $x \sim y$ if and only if $x - y$ is an integer multiple of 2π. Then $\mathbb{R}/\sim$ "is" the set of angles (measured in radians).

Example 3.3. Let $X = [0,1] \subset \mathbb{R}$ and define $x \sim y$ if and only if either both x and y are in $\{0,1\}$ or neither x nor y are in $\{0,1\}$. Then $X/\sim$ "is" a circle.

In the past few examples, the word "is" has been in quotes, since we have discussed only the definition of a particular set (the quotient set). To be the rational numbers, angle measurements, or a circle the set must also have an underlying algebraic (eg. the ability to add), topological (eg. connectedness), or geometric (eg. notion of distance) structure and we have not yet discussed how to endow quotient sets with these properties. In fact, we won't discuss this much since that is a major component of courses in real analysis, abstract algebra, topology, and geometry. The few sections, though, give some idea of how to do this in a few particular cases.

4. ANGLES

We know from trigonometry that an angle of 0 radians is the same angle as the angle of 2π radians is the same angle as -2π radians, etc. Similarly, π radians is the same as 3π radians and so on. Indeed, an angle of θ radians and an angle of $\theta + 2\pi k$ radians are the same whenever $k \in \mathbb{Z}$. Equivalence relations give us a natural way of making this idea mathematically precise.

Definition 4.1. An **angle** is an element of $\mathbb{R}/\sim$ where $x \sim y$ if and only if $x = y + 2\pi k$ for some $k \in \mathbb{Z}$. We say that the equivalence class $[x] \in \mathbb{R}/\sim$ is an angle of x **radians**.

We know from experience that the idea of adding two angles makes sense. For example, if we add π radians to π radians we get 2π radians and if we add 3π radians to π radians we still get 2π radians (which is the same angle as 4π radians). To make this notion of angle addition mathematically precise, we do the following:

Definition 4.2. Suppose that $[x], [y] \in \mathbb{R}/\sim$ are angles. We define their sum by

$$[x] + [y] = [x + y].$$

Just because we declare a definition, doesn't mean that it makes sense. The next lemma guarantees that angle addition makes sense.

Lemma 4.3. Suppose that $[x] = [a]$ and $[y] = [b]$. Then $[x] + [y] = [a] + [b]$.

Proof. By definition $[x] + [y] = [x + y]$ and $[a] + [b] = [a + b]$. We desire to show that $[x + y] = [a + b]$. By Theorem 2.5, it suffices to show that $[x + y]$ and $[a + b]$ have an element in common. That is, we will show that there exists $c \in \mathbb{R}$ such that $c \in [x + y]$ and $c \in [a + b]$.

Let $c = a + b$. By Theorem 2.5, $c \in [a + b]$. We must show that $c \in [x + y]$. To do this, we must show that $x + y \sim c$. By the definition of $\sim$, we must show that there exists $k \in Z$ such that $c = (x + y) + 2\pi k$.

Since $[x] = [a]$, $a \sim x$. Hence, there exists $k_1 \in \mathbb{Z}$ such that $x = a + 2\pi k_1$. Similarly, since $[y] = [b]$, there exists $k_2 \in \mathbb{Z}$ such that $y = b + 2\pi k_2$. Consequently,

$$x + y = (a + 2\pi k_1) + (b + 2\pi k_2) = (a + b) + 2\pi(k_1 + k_2).$$

Let $k = (k_1 + k_2)$. Since $c = a + b$, we have shown that there exists $k \in \mathbb{Z}$ such that $x + y = (a + b) + 2\pi k$. Consequently, $[x + y] = [a + b]$. $\square$

We also need to show that addition has all the usual properties: that is, angles with $+$ form a group.

Lemma 4.4. Let A be the set of angles and let $+$ be defined as above. Then $(A,+)$ is a commutative group.

Proof. We must show that $+$ is commutative and associative and that there is an identity and that each element has an inverse.

Claim 1: Angle addition is associative.

The proof is based on the fact that addition of real numbers is associative. Let $[x]$, $[y]$, and $[z]$ be angles. We must show that

$$([x]+[y])+[z]=[x]+([y]+[z]).$$

By the definition of $+$, $([x]+[y])=[x+y]$. Hence,

$$([x]+[y])+[z]=[(x+y)]+[z]=[(x+y)+z].$$

Similarly,

$$[x]+([y]+[z])=[x]+([y+z])=[x+(y+z)].$$

Since addition of real numbers is associative, $x+(y+z)=(x+y)+z$. Consequently,

$$[(x+y)+z]=[x+(y+z)].$$

And so,

$$([x]+[y])+[z]=[x]+([y]+[z])$$

Claim 2: Angle addition is commutative

This is very similar to Claim 1 and we leave the proof for the reader.

Claim 3: The element $[0]\in A$ is the identity for $(A,+)$.

Let $[x]\in A$. We must show that $[x]+[0]=[0]+[x]=[x]$. Since $+$ is commutative (Claim 2), it suffices to show that $[x]+[0]=[x]$.

By the definition of $+$, $[x]+[0]=[x+0]$. Since 0 is the identity for $(\mathbb{R},+)$, $x+0=x$. Hence,

$$[x]+[0]=[x+0]=[x].$$

We conclude that $[0]$ is the additive identity for $(A,+)$.

Claim 4: Each element of A has an inverse in $(A,+)$.

Let $[x]\in A$. We must show that there exists $[y]\in A$ such that

$$[x]+[y]=[y]+[x]=[0].$$

Since $+$ is commutative, it suffices to show that there exists $[y] \in A$ such that $[x]+[y]=[0]$.

Let $y=-x$. Then

$$[x]+[y]=[x+y]=[x+(-x)]=[0],$$

as desired. □

5. Groups and Subgroups

Throughout this section, let $(G,\circ)$ be a group and let $H \subset G$ be a group with the same operation $\circ$. (H is called a **subgroup** of G.) Let $\mathbf{1}$ be the identity of G and recall that $\mathbf{1} \in H$ since H is a subgroup.

Define a relation $\sim_H$ on G by

$$(x \sim_H y) \Leftrightarrow (\exists h \in H \text{ s.t. } x = y \circ h.$$

Lemma 5.1. The relation $\sim_H$ is an equivalence relation.

Proof. That $\sim_H$ is reflexive, follows from the observation that $\mathbf{1} \in H$ and $x = x \circ \mathbf{1}$.

We next show that $\sim_H$ is symmetric. Assume $x \sim_H y$. Then there exists $h \in H$ such that $x = y \circ h$. Since H is a group, $h^{-1} \in H$. Hence,

$$x \circ h^{-1} = (y \circ h) \circ h^{-1}.$$

Since H (or G) is a group, $\circ$ is associative, thus

$$(y \circ h) \circ h^{-1} = y \circ (h \circ h^{-1}).$$

By the definition of inverse, $h \circ h^{-1} = \mathbf{1}$. By the definition of $\mathbf{1}$, $y \circ \mathbf{1} = y$. Consequently,

$$x \circ h^{-1} = y.$$

Since $h^{-1} \in H$, $y \sim_H x$ as desired.

Finally, we show that $\sim_H$ is transitive. Assume that $x \sim_H y$ and $y \sim_H z$. There exist $h_1, h_2 \in H$ such that

$$\begin{aligned} x &= y \circ h_1 \\ y &= z \circ h_2. \end{aligned}$$

Hence,

$$x = (z \circ h_2) \circ h_1.$$

Since $\circ$ is associative,

$$x = z \circ (h_2 \circ h_1).$$

Since H is a group, $h_2 \circ h_1 \in H$. Consequently, $x \sim_H z$.

Since $\sim_H$ is symmetric, reflexive, and transitive, $\sim_H$ is an equivalence relation. □

We can now prove the fundamental theorem of finite group theory.

Theorem 5.2 (LaGrange's Theorem)**.** Suppose that $(G, \circ)$ is a group with finitely many elements and that $H \subset G$ is a subgroup. Then the number of elements in G is a multiple of the number of elements in H. In fact,

$$|G| = |G/\!\sim_H| \cdot |H|,$$

where the vertical bars denote the number of elements in the set.

Proof. By Theorem 2.5, the sets in $G/\!\sim_H$ partition G. Thus, it suffices to show that all the sets in $G/\!\sim_H$ have the same number of elements as H.

Claim: If $[x] \in G/\!\sim_H$, then $|[x]| = |H|$.

We prove the claim by showing that there exists a one-to-one and onto function $f\colon H \to [x]$.

Let $h \in H$ and define

$$f(h) = x \circ h.$$

By the definition of $\sim_H$, $f(h) \in [x]$.

We begin by showing that f is one-to-one. Suppose that $f(h_1) = f(h_2)$. Then $x \circ h_1 = x \circ h_2$. Since G is a group, $x^{-1} \in G$. The defining properties of a group can be applied to show:

$$\begin{array}{rcl} x^{-1} \circ (x \circ h_1) &=& x^{-1} \circ (x \circ h_2) \\ (x^{-1} \circ x) \circ h_1) &=& (x^{-1} \circ x) \circ h_2 \\ \mathbf{1} \circ h_1 &=& \mathbf{1} \circ h_2 \\ h_1 &=& h_2. \end{array}$$

Consequently, f is one-to-one.

Next we show that f is onto. Let $w \in [x]$. Then there exists $h \in H$ such that $x = w \circ h$. Thus, $f(h) = x$. Consequently, f is both injective and surjective and is, therefore, a bijection. If there exists a bijection between two finite sets, they have the same number of elements. Hence, H and $[x]$ have the same number of elements for each $[x] \in G/\!\sim_H$. □

Corollary 5.3. If a finite group G has a prime number of elements then its only subgroups are $\{\mathbf{1}\}$ and G itself.

Example 5.4. The collection of symmetries of any given object form a group. For example, the symmetry group of a regular hexagon has 12 symmetries: 6 rotations and 6 reflections. If you decorate the hexagon and require the symmetries to preserve the decoration, the new symmetry group is a subgroup of the old symmetry group. Thus, for example, LaGrange's theorem implies that it is impossible to decorate a hexagon so that it has exactly 5 symmetries since 12 is not a multiple of 5.

6. Construction the Rationals

Recall from our work in appendix A that set theory forms the basis for almost all of modern mathematics. This means that (almost) any idea in mathematics can be expressed in terms of sets. We've seen that the set $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ can be defined purely in set theoretic terms and that even the notion of $\leq$ or $+$ for $\mathbb{N}_0$ can be defined in terms of set theory. Using equivalence relations it is possible to define the integers $\mathbb{Z}$ and the rational numbers $\mathbb{Q}$ along with their additional algebraic structure (the ability to add and multiply) and order structure (the notion of $\leq$).

To make the main points most evident, we'll assume that we have already constructed the $\mathbb{Z}$ and that it is possible to add, subtract, and multiply these numbers and that these operations work they way we learned they do in elementary school. We also assume that $\leq$ is defined on $\mathbb{Z}$ and that it works the way we expect it to. We must prove that these operations are defined on $\mathbb{Q}$ and that they work the way we expect them to.

Definition 6.1. The rational numbers $\mathbb{Q}$ are defined to be the quotient set $(\mathbb{Z} \times (\mathbb{Z} \backslash \{0\})/\sim$ where

$$(a,b) \sim (c,d)$$

if and only if $ad = bc$. We will sometimes write $\frac{a}{b}$ instead of $[(a,b)]$.

Definition 6.2. We define the following operations on $\mathbb{Q}$:

- Addition is defined by

$$[(a,b)] + [(c,d)] = [(ad+bc,bd)]$$

- Negation is defined by

$$-[(a,b)] = [(-a,b)]$$

- Multiplication is defined by

$$[(a,b)] \cdot [(c,d)] = [(ac,bd)]$$

Also we say that

$$[(0,1)] \leq [(a,b)]$$

if and only $ab \in \mathbb{N}_0$.

If r and q are rational numbers, we define $r-q$ to be equal to $r+(-q)$. We say that $q \leq r$ if and only if $[(0,0)] \leq r-q$.

Lemma 6.3. The previous definitions of $-$, $+$, $\cdot$, and $\leq$ are well-defined. That is, they do not depend on the particular members of the equivalence classes used in the definitions.

Proof. We prove only that $+$ is well-defined and we leave the others as exercises.

Suppose that $[(a,b)] = [(a',b')]$ and that $[(c,d)] = [(c',d')]$. Then,

$$[(a,b)] + [(c,d)] = [(ad+bc,bd)]$$

and

$$[(a',b')] + [(c',d')] = [(a'd'+b'c',b'd')]$$

We must show that

$$[(ad+bc,bd)] = [(a'd'+b'c',b'd')]$$

Since equivalence classes are a partition, it suffices to show that

$$(ad+bc,bd) \sim (a'd'+b'c',b'd')$$

Claim: $(ad+bc,bd) \sim (a'd'+b'c',b'd')$

Since $[(a,b)] = [(a',b')]$, we have $(a,b) \sim (a',b')$. Thus, $ab' = a'b$. Similarly, $cd' = c'd$. Thus,

$$(ad+bc)(b'd') = adb'd' + bcb'd' = (ab')(dd') + (cd')(bb') = (a'b)(dd') + (c'd)(bb').$$

We also have

$$(a'd'+b'c')(bd) = a'd'bd + b'c'bd = (a'b)(dd') + (c'd)(bb').$$

Consequently,

$$(ad+bc)(b'd') = (a'd'+b'c')(bd).$$

Hence,

$$(ad+bc,bd) \sim (a'd'+b'c',b'd')$$

as desired. □