Equivalence Relations

In this section we will define and give some of the properties of equivalence relations. Our main usage will first come in the next section where we construct quotient spaces. However, as in all parts of mathematics, equivalence relations will play a significant role in linear algebra for the construction of new objects and as a way of interpreting certain ideas. In particular, they not only give a method to construct quotients spaces, but also fields of fractions (see Exercise 11), quotients rings which include fields (see Exercise 12), quotient modules, and tensor products, among others.

Definition 1. Let X be a non-empty set. A subset $\mathcal{E} \subseteq X \times X$ is called an *equivalence relation* on X if it satisfies the following three properties:

1. *Reflexive:*
   For all $x \in X$, $(x, x) \in \mathcal{E}$.
2. *Symmetric:*
   If $(x, y) \in \mathcal{E}$, then $(y, x) \in \mathcal{E}$.
3. *Transitive:*
   If $(x, y), (y, z) \in \mathcal{E}$, then $(x, z) \in \mathcal{E}$.

One typically denotes the relation by some symbol, such as $\sim$, so that $x \sim y$ means the same thing as $(x, y) \in \mathcal{E}$. The three conditions above then mean that $\sim$ has the same properties as an equals sign.

Some examples of equivalence relations are

1. Let X be any non-empty set and $\mathcal{E} = \{ (x, x) \mid x \in X \}$. The relation is just ordinary equality of elements of X.
2. Let $\mathcal{L}$ denote the set of lines in the plane. We write $L_1 \parallel L_2$ if the lines L_1 and L_2 are parallel. This gives an equivalence relation on $\mathcal{L}$.
3. Let T denote the set of triangles in the plane. Similarity gives an equivalence on T.
4. Let T denote the set of triangles in the plane. Congruence gives an equivalence on T.
5. Let $n \in \mathbb{Z}$ be a non-zero integer. We say that two integers $a, b \in \mathbb{Z}$ are *congruent modulo* n, and write $a \equiv b \mod n$ if there exists $c \in \mathbb{Z}$ so that $a - b = cn$. That is, n divides $a - b$ exactly (with 0 remainder).
6. Let $\mathbb{C}^*$ be the set of non-zero complex numbers. For $w, z \in \mathbb{C}^*$ define $w \sim z$ if there exists a positive real number r so that $w = rz$. w, z are said to have the same *argument* if they satisfy this relation.

7. Let $m, n, m, n' \in \mathbb{Z}$ be integers with n, n' non-zero. The definition of equality in $\mathbb{Q}$

$$\tfrac{m}{n} = \tfrac{m'}{n'} \text{ if and only if } mn' = m'n$$

is really just an equivalence relation on certain pairs of integers.

Given an equivalence relation $\mathcal{E}$ on X, we define the *equivalence class* of $x \in X$ as

$$\operatorname{class}(x) = \{\, z \in X \mid z \sim x \,\} \ .$$

Lemma 2. *Let $\mathcal{E}$ be an equivalence relation on the non-empty set X.*

1. *Each subset* $\operatorname{class}(x)$ *is non-empty.*
2. *For $x, y \in X$, then* $\operatorname{class}(x) \cap \operatorname{class}(y)$ *is either empty or* $\operatorname{class}(x) = \operatorname{class}(y)$.
3. *X is the union of the subsets* $\operatorname{class}(x)$.

Proof. The first part is clear as $x \in \operatorname{class}(x)$ by the reflexive property. For the second part, suppose $z \in \operatorname{class}(x) \cap \operatorname{class}(y)$. Then $z \sim x$ and $z \sim y$, so $x \sim z$ by symmetry, and finally by transitivity, $x \sim y$. Thus $x \in \operatorname{class}(y)$. Hence if $w \sim x$ by transitivity $w \in \operatorname{class}(y)$ as well; that is $\operatorname{class}(x) \subseteq \operatorname{class}(y)$. In an analogous manner one sees $\operatorname{class}(y) \subseteq \operatorname{class}(x)$ and the two are equal.

Finally, as $x \in \operatorname{class}(x)$, every element of X lies in one of the equivalence classes, yielding the final statement. □

The lemma simply states that an equivalence relation on a set breaks the set into a disjoint union of subsets. Given a set X and a collection of subsets $\{\, X_i \mid i \in I \,\}$ for some index set I which satisfy:

1. Each subset X_i is non-empty.
2. $X_i \cap X_j$ is empty for $i \neq j$.
3. X is the union of the subsets X_i.

We say that the collection forms a *partition* of X. We write

$$X = \dot{\bigcup_{i \in I}} X_i$$

which is read as "X is the disjoint union of the X_i". By Exercise 1 below, any such partition determines a unique equivalence relation on X. Other symbols, such as $\sqcup$, are sometimes used to denote disjoint union.

Definition 3. Let $\mathcal{E}$ be an equivalence relation on X. A subset $\mathcal{R} \subseteq X$ is called a *set of representatives* if $\mathcal{R} \cap X_i$ contains exactly one element for each $i \in I$.

Note that this implies that $\mathcal{R}$ and I have exactly the same number of elements; that is, they have the same cardinality: $|I| = |\mathcal{R}|$. The function $\varphi : I \longrightarrow \mathcal{R}$ given by $\varphi(i) = \mathcal{R} \cap X_i$ is the required one-to-one, onto function. Sometimes (but not always) it is possible to find very "nice" sets of representatives for equivalence relations. For example, if $n \in \mathbb{Z}$ is a positive integer, it is easy to show that $\{0, 1, \ldots, n-1\}$ is a set of representatives for congruence modulo n. Another example is the set of fractions in $\mathbb{Q}$ written as fractions in lowest terms (no non-trivial common integer factors of the numerator and denominator). See the exercises at the end for further examples of sets of representatives.

Definition 4. Given an equivalence relation $\mathcal{E}$ (denoted by $\sim$) on a set X, the *quotient set* $X/\mathcal{E}$ or $X/\sim$ is defined to be the set whose elements are the equivalence classes (the subsets in the corresponding partition).

That is, if X is the disjoint union of the equivalence classes $X_i, i \in I$, then

$$X/\mathcal{E} = X/\sim = \{ X_i \mid i \in I \} .$$

Hence the quotient set has exactly the same number of elements as a set of representatives $\mathcal{R}$ which is the same as I:

$$|X/\mathcal{E}| = |X/\sim| = |\mathcal{R}| = |I| .$$

In this situation there is a natural (sometimes referred to as "canonical") function from X to the quotient:

$$p : X \longrightarrow X/\mathcal{E}$$

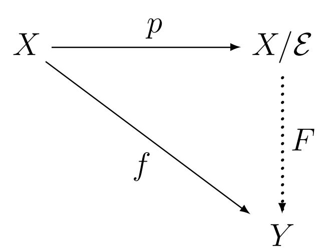
defined by $p(x) = \text{class}(x)$. If we use the partition X_i, $i \in I$, this is the same as $p(x) = X_i$ if $x \in X_i$. Either way, the description of p is very simple: it sends each element of X to the equivalence class which contains it. It should be clear that the function p is onto and that $p(x) = p(y)$ if and only if $x \sim y$. Sometimes this is described as "p is onto with fibers the equivalence classes". Given a function $h : X \longrightarrow Y$, for $y \in Y$ the subset of X

$$h^{-1}(y) = \{ x \in X \mid f(x) = y \}$$

is called the *fiber of* h *over* y. The fibers of h are all such subsets of X. Note that the collection of all non-empty fibers of h is a partition of X (see Exericse 3 below), and hence determines an equivalence relation on X.

The quotient construction is used frequently in mathematics, and in particular, in this course. If the equivalence relation $\mathcal{E}$ behaves "nicely" with respect to the structure of X, then $X/\mathcal{E}$ will have the same sort of structure, and the function p will preserve it. At this point, this is quite vague, but should give you an idea of the philosophy behind the use of the construction. It will be used in the construction of quotient spaces, quotient rings, fields of fractions, tensor products, and others. It gives a method for the construction of "universal" objects via the following simple result.

Proposition 5. *Let $\mathcal{E}$ be an equivalence relation on the set X . If $f : X \longrightarrow Y$ is a function which is constant on the fibers of $p : X \longrightarrow X/\mathcal{E}$, then there exists a unique function $F : X/\mathcal{E} \longrightarrow Y$ such that the diagram*



commutes, that is, $f = F \circ p$.

By "constant on the fibers" we mean $f(x) = f(x')$ whenever $p(x) = p(x')$; that is, $x \sim x'$ for $x \in X$ (i.e., when $(x, x') \in \mathcal{E}$). It is now clear that defining $F(\text{class}(x)) = p(y)$ for any $y \in \text{class}(x)$ makes sense ("F is well-defined").

The basic idea introduced in Proposition 5 will be used many times later in the course. See the section on "Universal Mapping Properties".

Remark 6. One can view the previous proposition as saying that defining a function from $X/\mathcal{E}$ to some set Y *is the same thing* as defining a function from X to Y that is constant on the equivalence classes of $\mathcal{E}$. Often times in this course, we will want to define a function from a quotient set, and we will have to spend time proving that our function is 'well-defined'. To do this, we will show that the function is indeed constant on the equivalence classes of $\mathcal{E}$.

Exercises

EqRel 1. Show that any partitition of a non-empty set X determines a unique equivalence relation on X for which the equivalence classes are precisely the elements of the partition. Hence there is a one-to-one correspondence between equivalence classes of the set X and partitions of the set X.

EqRel 2. Show that the function $\varphi :\ I \longrightarrow \mathcal{R}$ defined in the discussion about sets of representatives is one-to-one and onto.

EqRel 3. Let X and Y be non-empty sets and let $h :\ X \longrightarrow Y$ be a function. Show that the collection of non-empty fibers of h forms a partition of X.

EqRel 4. Let $f :\ X \longrightarrow Y$ be an onto function, and denote by $\sim$ the equivalence relation given by the fibers of f (see the previous exercise). Show that there is a bijection between $X/\sim$ and Y. (This fact is sometimes referred to as the 'First Isomorphism Theorem'.)

EqRel 5. Prove Proposition 5: First prove that F is unique given the required condition. Then define F via the formula just derived. (Compare the partition given by the fibers of f to the partition given by the fibers of p.)

EqRel 6. Show that in the situation of Proposition 5 we must have

$$\{\, f :\ X \longrightarrow Y \mid f \text{ is constant on equivalence classes of } \mathcal{E}\,\} =$$

$$\{\, f :\ X \longrightarrow Y \mid f \text{ is constant on fibers of } p\,\}$$

and that there is a natural bijection with set of all functions

$$\{\, F :\ X/\mathcal{E} \longrightarrow Y \,\} \ .$$

EqRel 7. Let R be a ring (with identity). Let $U(R)$ denote the set of all elements of R which have multiplicative inverses. This is called the *group of units* of R. [The examples are needed in the next exercise.]

1. Verify that $U(R)$ is a group under multiplication.
2. Compute $U(R)$ for $R = \mathbb{Z}$ and for $R = F[x]$ (F a field).
3. Compute $U(R)$ for $R = F^{m\times m}$ for F a field and $m > 1$.
4. Compute $U(R)$ when $R = F[[x]]$, F a field. [Hint: First determine a (simple) necessary condition in order that $f \in F[[x]]$ has a multiplicative inverse. Then show that in fact the condition you found is also sufficient.]

EqRel 8. Let R be a ring (with identity) with group of units $U(R)$.

1. Define elements $r, s \in R$ to be *left associate* if there exists a $u \in U(R)$ such that $s = ur$. Show that this gives an equivalence relation on R. One defines *right associate* analogously.

2. Define elements $r, s \in R$ to be *associate* if there exist $u, v \in U(R)$ such that $s = urv$. Show that this gives an equivalence relation on R.

3. Define elements $r, s \in R$ to be *conjugate* if there exists $u \in U(R)$ such that $s = uru^{-1}$. Show that this gives an equivalence relation on R.

4. Explicitly determine the equivalence classes of the four equivlence relations given above for each of the rings listed below and give a system of unique representatives in each case:

   a. $\mathbb{Z}$.

   b. $F[x]$ for F a field.

   c. $F^{m \times m}$ for F a field and $m > 1$.

   d. $F[[x]]$ for F a field.

EqRel 9. Let $\mathbb{Z}$ be the integers and $n \neq 0$ an integer. Show that the equivalence relation mod n (the 5th example in our original list) is indeed an equivalence relation. Give a natural set of representatives of this equivalence relation, with a proof. Define addition and multiplication on the set of equivalence classes (see the next exercise) and prove that the set of equivalence classes becomes a commutative ring with identity. Show that no non-trivial products are 0 in this ring if and only if n is a prime. This ring will be denoted by $\mathbb{Z}_n$; in case $n = p > 0$ is a prime, it will also be denoted $\mathbb{F}_p$ (as discussed in the section on "Fields").

EqRel 10. Let R be an equivalence relation on $\mathbb{Z}$ such that the operation on the quotient set $\mathbb{Z}/R$ given by the rule $[a]_R + [b]_R = [a + b]_R$ is well-defined. Show that R must either be the identity relation ($a \equiv_R b \Leftrightarrow a = b$) or the relation "mod n" for some n. (Hint: Consider the smallest difference that occurs between elements of the same equivalence class).

(Remarks: Here, $[c]_R$ denotes the equivalence class of c. By a well-defined rule, we mean that the rule is independent of the choice of representative for the equivalence class. In this case, it means that for any a and a' such that $[a]_R = [a']_R$ and for any b and b' such that $[b]_R = [b']_R$, we must have $[a + b]_R = [a' + b']_R$.)

EqRel 11. Let R be a ring with identity [We'll also assume $1 \in R$, although that is not really necessary here.] An element $a \in R$ with $a \neq 0$ is called a *zero divisor* if there is an element $b \in R$ with $b \neq 0$ and either $ab = 0$ or $ba = 0$. A ring with no zero divisors is called a *domain* (or integral domain). Assume that R is a domain. We will also assume that R is commutative, i.e. $xy = yx$ for all $x, y \in R$, and that R is not the 0 ring. This exercise will generalize the construction of $\mathbb{Q}$ from $\mathbb{Z}$ and will give you more experience with equivalence relations. Let

$$X = \{ (r, s) \mid r, s \in R, s \neq 0 \}.$$

Define an equivalence relation on this set of pairs X as follows:

$$(r, s) \equiv (r', s') \text{ if and only if } rs' = sr'.$$

a. Show that this defines an equivalence relation on X.

b. Let r/s denote the equivalence class of (r,s) under the equivalence relation, and let $F := \{\, r/s \mid r,s \in R,\ s \neq 0 \,\}$ denote the quotient set. Define addition and multiplication on F by

$$\begin{aligned} r/s + r'/s' &= (rs' + sr')/(ss') \\ (r/s)\cdot(r'/s') &= (rr')/(ss') \end{aligned}$$

Show that these rules are well-defined. We claim that F becomes a field under these rules. Verify the commutative law for addition, that F has a 0 and 1, that additive and multiplicative inverses exist, and the distributive law. (Hint: If s' is not 0, prove the useful formula $(rs')/(ss') = r/s$).

c. Define a function $i:\ R \longrightarrow F$ (analogous to the inclusion of $\mathbb{Z}$ into $\mathbb{Q}$). Verify that it is injective and a homomorphism of rings. [See the section "Some Useful Definitions" for the meaning of homomorphism.]

d. Prove that the field you have constructed is the "smallest field containing R". More precisely, prove that if $h:\ R \longrightarrow K$ is any injective homomorphism into a field K, then there is a unique injective homomorphism $H:\ F \longrightarrow K$ such that $H \circ i = h$. This is another example of a Universal Mapping Property.

The field F constructed in this exercise is called the *field of fractions* of R.

EqRel 12. Let F be a field and let $f \in F[y]$ be a polynomial. Since the ideal $I = (f)$ generated by f is a subspace of $F[x]$, we can form the quotient vector space $F[y]/(f)$. (This is the rigorous definition of root adjunction!)

a. For $a, b \in F[y]$, show $a + (f) = b + (f)$ if and only if f divides $a - b$.

b. Show $F[y]/(f)$ has a well-defined multiplication operation given by

$$(a + (f))(b + (f)) := ab + (f).$$

(In other words, if $a + (f) = a' + (f)$ and $b + (f) = b' + (f)$, show that $ab + (f) = a'b' + (f)$). Conclude that $F[y]/(f)$ is an F-algebra, and that there is a natural one-to-one homomorphism $F \longrightarrow F[y]/(f)$ (hence we can consider F as a subring).

c. Prove that $F[y]/(f)$ is a field if and only if f is irreducible.

d. Let f be irreducible and let $K = F[y]/(f)$. Let $h \in F[x]$. For $a \in K$ (or indeed for any F-algebra K), we can evaluate $h(a) \in K$ as usual. Show that there is an $a \in K$ such that $f(a) = 0$. Hence we have constructed a field K which contains F and which contains a root of the irreducible polynomial f.

EqRel 13. Is there a generalization of Exercise 10 to the situation of the previous exercise? If so, state and prove. If not, give a counter-example.

The Notes for the course *Math 4330, Honors Linear Algebra* at Cornell University have been developed over the last ten years or so mainly by the following (in chronological order):

Gerhard O. Michler

R. Keith Dennis

Martin Kassabov

W. Frank Moore

and

Yuri Berest.

Most sections have been revised so many times the original author may no longer recognize it. The intent is to provide a modern treatement of linear algebra using consistent terminology and notation. Some sections are written simply to provide a central source of information such as those on "Useful Definitions", "Subobjects", and "Universal Mapping Properties" rather than as a chapter as one might find in a traditional textbook. Additionally there are sections whose intent is to provide proofs of some results which are not given in the lectures, but rather provide them as part of a more thorough development of a tangential topic (e.g., Zorn's Lemma to develop cardinal numbers and the existence of bases and dimension in the general case).

A large number of challenging exercises from many different sources have been included. Although most should be readily solvable by students who have mastered the material, a few even more challenging ones still remain.

Much still remains to be done. Corrections and suggestions for additional exercises, topics and supplements are always welcome.