Equivalence Relations

Equivalence Relations

Definition: Given a set X, we define an *equivalence relation on* X to be a binary relation $\sim$ satisfying:

(i) Reflexivity: for all $x \in X$, $x \sim x$.
(ii) Symmetry: $x \sim y \implies y \sim x$.
(iii) Transitivity: $x \sim y$ and $y \sim z \implies x \sim z$.

Examples of Equivalence Relations

1. Equality "=" is an equivalence relation on any set.
2. Let S be the set of undergraduate students enrolled at UofT. We say two students are "peers" if they have been enrolled in university for the same number of years. This is an equivalence relation on S.
3. For any $n \in \mathbb{N}$, congruence modulo n is an equivalence relation on $\mathbb{Z}$.
4. We can define an equivalence relation on $\mathbb{R}$ which I'll call a "quotient by $\mathbb{Q}$". For $x, y \in \mathbb{R}$ let, $x \sim y$ exactly when $x - y \in \mathbb{Q}$.

Partitions

Definition: A *partition* of a set X, is a collection of subsets of X which are disjoint and union to give all of X. I.e. it is any way to split up X into pieces.

Fundamental Theorem of Equivalence Relations

Proposition: Every equivalence relation $\sim$ on X defines a partition of X into *equivalence classes* $[m] = \{x \in X : x \sim m\}$. Conversely, every partition of X into subsets X_i arises from an equivalence relation $x \sim y$ if and only if $x, y \in X_i$ for some i.

Examples of Corresponding Partitions

1. For equality $(=)$ the equivalence classes are just each individual element.
2. For the peers relation, the equivalence classes are the set of freshmen, sophomores, juniors, etc..

3. For modular congruence, the equivalence classes are what we have called the congruence classes of integers mod n. E.g. for the equivalence relation $\equiv \pmod 4$, there are four equivalence classes $[0], [1], [2], [3]$. Recall we showed in class we can still "do math" on these equivalence classes, i.e. add and multiply congruency classes together; this is because the equivalence classes form a *quotient group* and *quotient ring*. More general examples of these kind of arithmetic features are studied in abstract algebra.

4. For our quotient by $\mathbb{Q}$, the equivalence classes are copies of $\mathbb{Q}$ translated by irrational numbers; for example one class would be $[\pi] = \{\pi + p : p \in \mathbb{Q}\}$. Define a set V by picking exactly one element lying in $[0, 1]$ from each equivalence class. This is an example of a *Vitali Set*, and it is a set for which there is no reasonable way to define its length[1]!

5. To consider an example going the other way, recall that scientists commonly partition the set of living things on Earth into 6 kingdoms: bacteria, archaea, protists, plants, animals, and fungi. This induces an equivalence relation on the set of all living organisms. Under this equivalence relation:

   $$\text{Alicia Keys} \sim \text{Koala Bear} \quad \text{but} \quad \text{Sea Sponge} \nsim \text{Shiitake Mushroom} \nsim \text{Seaweed}.$$

[1] By "reasonable way to define length", I mean some function μ which takes in a subset of $\mathbb{R}$ and returns its (possibly infinite) length. Any such μ which assigns the usual length $b-a$ to intervals $[a, b]$, which is invariant under shifting a set left or right, and which is additive so the length of disjoint sets together is the sum of their lengths individually, cannot be defined on V to give an answer consistent with the fact $\mu([0, 1]) = 1$. That is, not every subset of $\mathbb{R}$ has a length in the ordinary sense.

Problems on the Euler Totient Function

Some of the following are taken from the quite good book *Elementary Number Theory* by Gareth and J. Mary Jones.

1. For any $\varepsilon > 0$, can you find n so that $\frac{\varphi(n)}{n} > 1 - \varepsilon$?

2. Show that $\varphi(mn) \geq \varphi(n)\varphi(m)$ with equality only if m and n are coprime.

3. * Use the above question to show that for any integer m there are only finitely many n such that $\varphi(n) = m$ [Hint: for every prime p, show $\varphi(p^k) > m$ for some k]. (In fact, $\varphi(n) \geq \sqrt{n/2}$ for all n; you can look up the proof online).

4. * Show that the value of $\varphi(n)/n$ is uniquely determined by the set of prime numbers which divide n [Hint: use contradiction and the explicit formula for $\varphi(n)$].

Problems on the Euclidean Algorithm

1. (The Chicken Nugget Theorem) Let n, m be coprime and positive. Show that any number N can be written as $N = xn + ym$ for x, y *non-negative* as long as,
$$N > mn - m - n.$$
(Hint: For a given N, find the smallest non-negative y that satisfies the given linear Diophantine equation and see what happens if x is negative).

   To see the role of chicken nuggets, consider this everyday scenario. An avant-garde fast food restaurant McEuclid's has just opened up and sells only boxes of 13 and 19 nuggets. In an attempt to carve a niche in the number-theorist demographic, McEuclid's will fail to deliver my order if I request a number that can't be made from boxes of 13 and/or 19 nuggets (but they'll still charge me for the food!). After a long day of proof writing, my friend Gauss is desperate for in excess of 200 nuggets and asks me to pick a large amount. Gauss may also add a few extra nuggets to the total if they are in the mood for more food, but I'm definitely not in the mood to perform more extended Euclidean algorithm computations. At least how many nuggets should I order so that, even if Gauss adds some more, we will never be requesting an impossible amount of nuggets and hence surely get our food?

2. (The Euclidean Algorithm for Polynomials) The Euclidean algorithm can be applied on more general algebraic structures called *Euclidean domains*. An example of a Euclidean domain you have seen before is the set of polynomials with real coefficients. We can apply the Euclidean algorithm to polynomials just like we do to integers, replacing integer division with remainders by polynomial division with remainders. Perform the Euclidean algorithm to find the gcd of:
$$x^3 - 9x^2 + 23x - 15 \quad \text{and} \quad x^3 - x^2 + 4x - 4.$$
What do you think gcd means in this context? Factor the two polynomials to check your intuition.

Problems on the Rational Numbers

1. We know there are infinitely many rational numbers between any two rational numbers. The same is true for reals; between any two real numbers there are infinitely many rationals. This property is called the *density* of the rationals in the reals. Prove that $\mathbb{Q}$ is dense in $\mathbb{R}$.

2. A *dyadic rational* is a rational number whose denominator is a power of two. Show that these dyadics are closed under addition and multiplication. Use this to show that dyadic rationals are precisely the numbers with finite binary expansions. For this reason the dyadic rationals are important in computer science. They also appear in music theory, where time signatures and note lengths are usually given as dyadic rationals.

3. Remember in a previous tutorial we defined equivalence relations. Find an equivalence relation on pairs of integers (a, b) for $b \neq 0$ that defines a set equivalent to the rationals. Because of this construction, $\mathbb{Q}$ can be called the *field of fractions* of $\mathbb{Z}$.

More Problems on the Rational Numbers

1. For $p \geq 2$, $x^p - 1$ has a rational root $x = 1$. Use it to factor the polynomial. When p odd, how can you factor further? What does the factorization look like when we allow for complex roots?

2. A number is *algebraic* if it is the root of some polynomial with integer coefficients. Show that $\sqrt{p} + \sqrt{q}$ is algebraic for all $p, q \in \mathbb{Q}$. Numbers which are not algebraic are called *transcendental*. Providing any example (with proof) that a number is transcendental is very difficult, (look up Liouville's constant), but we will find a non-constructive proof of the existence of infinitely many transcendental numbers once we discuss set theory.

3. An *infinitely nested radical* is an expression of the form,

$$\sqrt{n + \sqrt{n + \sqrt{n + \sqrt{n + \cdots}}}}$$

With some algebraic manipulation, evaluate this expression and show that sometimes it may have rational solutions for $n \in \mathbb{N}$. What if you replace the square roots with higher order radicals, can you find any rational solutions then? Show that, for $k, n \in \mathbb{N}$, that if

$$\sqrt[k]{n + \sqrt[k]{n + \sqrt[k]{n + \sqrt[k]{n + \cdots}}}} \in \mathbb{Q}$$

then the expression is in $\mathbb{N}$.

Problems on the Complex Numbers

1. Consider a function on the complex plane,

$$\omega(z) = \frac{az+b}{cz+d} \quad \text{such that} \quad a,b,c,d \in \mathbb{C} \quad \text{and} \quad ad-bc \neq 0.$$

   This is called a *fractional linear transformation.* These functions have the special property that they always send circles and lines to circles and lines (i.e. a circle may map to a circle or a line but never an ellipse or a squiggly curve). What is the unit disk $\{|z| \leq 1\}$ mapped to under the following fractional linear transformations?

$$\text{(i)}\ \ \omega(z) = \frac{i}{4}z + \sqrt{2}e^{i\pi/4} \qquad \text{(ii)}\ \ \omega(z) = \frac{1}{z}$$

$$\text{(iii)}\ \ \omega(z) = \frac{z+1}{iz-i} \qquad \text{(iv)}\ \ \omega(z) = \frac{z-i}{iz+1}$$

2. In class, we are proving the Fundamental Theorem of Algebra. A more traditional proof of the theorem uses the following powerful result in complex and harmonic analysis:
   Theorem 1 (Liouville's Theorem)**.** *Every complex differentiable function on all of $\mathbb{C}$ which is bounded, i.e. $|f(z)| < M$ for all $z \in \mathbb{C}$ and some $M > 0$, is constant.*
   You don't need to know what complex differentiable means to solve this problem, just know it includes polynomials, the exponential function, sine, cosine etc. and well-defined algebraic manipulations of these (sums, products, non-singular reciprocals). Use Liouville's Theorem to prove the Fundamental Theorem of Algebra. (Hint: Assume a polynomial $P(z)$ has no complex roots and consider $1/P(z)$).

3. Use DeMoivre's Theorem, Euler's Formula, and the Pythagorean identity to expand $\cos(4\theta)$ and $\sin(4\theta)$ in terms of $\cos\theta$ as the real and imaginary parts of $e^{i4\theta}$. Use the double angle formulas to write out $\sin^4\theta$, $\cos^4\theta$ in terms of $\cos(4\theta)$ and $\cos(2\theta)$. Use this result to find the indefinite integrals,

$$\int \sin^4\theta \, \mathrm{d}\theta \quad \text{and} \quad \int \cos^4\theta \, \mathrm{d}\theta \, .$$

Some Exercises on Quaternions

1. The complex numbers can be viewed as a subset of the *quaternions*, $\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{R}\}$. These are like the complex numbers but with two other imaginary units $\mathbf{j}$ and $\mathbf{k}$. Addition is defined component by component and we can multiply quaternion using associativity, distributivity and the following relations,

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k} \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i} \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

Unlike other numbers you are used to, the quaternions are not in general commutative. Only the real coefficients commute with all of $\mathbb{H}$.

(a) Use associativity, distributivity and the above relations to write explicitly the product,

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(\alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}).$$

(b) We can represent a quaternion $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ as a 2×2 complex matrix,

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}.$$

Show that quaternion addition and multiplication act just like addition and multiplication of these matrices.

(c) Find the multiplicative inverse of any quaternion, $(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})^{-1}$.

(d) Consider quaternions with no scalar part, i.e. of the form $x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$. Show that multiplication of these quaternions behaves just like the cross product of vectors $x\hat{x} + y\hat{y} + z\hat{z}$ in $\mathbb{R}^3$.

(e) (Hard) We say $x = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ is a *unit quaternion* if $a^2 + b^2 + c^2 + d^2 = 1$. As in the previous part, identify a vector $v = (v_1, v_2, v_3) \in \mathbb{R}^3$ with the quaternion $v_1\mathbf{i} + v_2\mathbf{j} + v_3\mathbf{k}$. Show that for any unit quaternion x, xvx^{-1} has no scalar part and amounts to a rotation of v. As an extra challenge, show that any arbitrary rotation is uniquely determined by some unit quaternion x up to a sign ($x, -x$ give the same rotation).

The last problem gives one common use for quaternions in computer graphics: to succinctly represent rotations of vectors in $\mathbb{R}^3$.

Exercises on Cardinality

1. Find the cardinalities of the following sets.
   (a) The set of isosceles triangles up to scaling (i.e. we consider similar triangles as the same).
   (b) The set of algebraic numbers, i.e. the set of all possible real roots of polynomials with rational coefficients.
   (c) The set of open subsets of $\mathbb{R}$. (A subset U is open if every point of U has an open interval around it contained in U). [Hint: use the density of the rationals to show that two open sets with the same rational elements are the same].

2. Consider an arbitrary function $f : \mathbb{R} \to \mathbb{R}$. Define a family of functions $f_\tau(x) = f(x) + \tau$. Show that for every f, there is some $\tau \in \mathbb{R}$ such that the graph of f_τ, $\{(x, f_\tau(x)) : x \in \mathbb{R}\} \subset \mathbb{R}^2$, contains no points in $\mathbb{Q}^2 \subset \mathbb{R}^2$.

3. You are a point which lives on the grid $[0,1] \times [0,1]$. At every element of $\mathbb{Q}^2$ in the grid, there is a booby trap which will suck you off the grid (oh no! by the density of the rationals these traps are everywhere!!). Find a continuous path given by two line segments that connects $(0,0)$ to $(1,1)$ which passes through no booby traps. In fact, explain why almost every random path of this form you could choose does not pass through a trap.

4. Take the set of all algebraic numbers, add to that set any mathematical constant you can think of (e.g. π, e, $\sin(1)$, $\log(2)$, the Euler-Mascheroni constant, etc.). Now assemble a panel of expert mathematicians and give them a billion years to list out, one by one, any function they can think of which takes in some finite number of real numbers and outputs a single real number (e.g. $x+y$, xy, $x!$, $\sin(x)$, x^y, $\int_1^x \log(z) \arctan(z)\,\mathrm{d}z$, etc.). Argue (non-rigourously) that there is some real number which can not be computed by applying any of these functions to any of the constants we could think of.

More Exercises on Cardinality

1. Show that a continuous function $f : \mathbb{R} \to \mathbb{R}$ is completely determined by its values on $\mathbb{Q}$. (I.e. if we know $f(x)$ for all $x \in \mathbb{Q}$, then we know it for all $x \in \mathbb{R}$). As a consequence, find the cardinality of the set of continuous functions $\mathbb{R} \to \mathbb{R}$. What is the cardinality of differentiable functions? Smooth functions? Analytic functions?

2. The purpose of this problem is to show the cardinality of Riemann integrable functions is $2^{\mathfrak{c}}$ using an important counter-example in math called the *Cantor Set*.

   (a) The Cantor Set $\mathcal{C}$ can be defined as the set of all real numbers in $[0, 1]$ which contain no 1s in their expansion in base three. I.e.,

   $$0.202020202020... \in \mathcal{C} \quad \text{but} \quad 0.20220200\mathbf{1}020... \notin \mathcal{C}.$$

   Explain why $\mathcal{C}$ is uncountable.

   (b) Show that $\mathbb{R} \setminus \mathcal{C}$ is open, i.e. that every real number not in the Cantor set has an open interval containing it which is disjoint from the Cantor Set.

   (c) A set $A \subset \mathbb{R}$ has *measure zero* if for any $\varepsilon > 0$, there is a collection of closed intervals of combined length less than ε whose union contains A. Let $\mathcal{C}_n$ be the subset of $[0, 1]$ of numbers, when expressed as a decimal in base three, have their first n digits not containing a 1. Look up a picture of the Cantor set and use this as a heuristic to explain why the intervals making up $\mathcal{C}_n$ have combined length $(2/3)^n$. Conclude that $\mathcal{C}$ has measure zero.

2. (d) Consider any subset $A \subset \mathcal{C}$. Define a function, $\chi_A : \mathbb{R} \to \mathbb{R}$ by,

$$\chi_A(x) = \begin{cases} 0 & x \notin A \\ 1 & x \in A \end{cases}.$$

Use (b) to show A is continuous for at least all $x \in \mathbb{R} \setminus \mathcal{C}$.

(e) Note the following theorem, which you may have seen a version of in multivariable calculus:
Theorem 2. *If $f : [a, b] \to \mathbb{R}$ is bounded, then it is Riemann integrable if and only if its set of discontinuities is measure zero.*
Use this along with the previous parts to conclude χ_A is Riemann integrable on $[0, 1]$.

(f) Conclude that the cardinality of Riemann integrable functions $[0, 1] \to \mathbb{R}$ is greater than or equal to $2^{\mathfrak{c}}$. Show this is an equality.

(g) Explain how one can replicate what was done above to show the cardinality of the Riemann integrable functions $[a, b] \to \mathbb{R}$ is $2^{\mathfrak{c}}$ for any $a < b$.