Math 444 Review

Leslie Rodriguez

June 17, 2015

Chapters 1 and 2.

Equivalence Relations.

Let X be a nonempy set. A *relation* on X is a subset of $X \times X$, where $X \times X$ is the set of ordered pairs $\{(x, y) : x, y \in X\}$. We write $x \sim y$ if and only if (x, y) is a member of this relation. A relation on X that satisfies the following properties:

- *Reflexivity.* For each $x \in X$, we have that $x \sim x$.
- *Symmetry.* If $x \sim y$ for some $x, y \in X$, then it follows that $y \sim x$.
- *Transitivity.* If $x \sim y$ and $y \sim z$ for some $x, y, z \in X$, then it follows that $x \sim z$.

is said to be an *equivalence relation*. If we have an equivalence relation, then for $x \in X$, we let $[x]$ denote the set of all elements of X that are related to x; that is, $[x] = \{y \in X : y \sim x\}$. The set $[x]$ is also referred to as the *equivalence class* of x.

Exercise 1.

Prove that if n is a natural number, then

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{1}$$

Proof. We shall proceed by induction on n.

Base Case. $n = 1$. Since $1 = \dfrac{1(1+1)(2 \cdot 1 + 1)}{6}$, it follows that (1) holds whenever n is 1.

Inductive Hypothesis. Suppose that (1) holds for some positive integer k. That is,

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}. \tag{2}$$

To complete the proof, we must now show that (1) holds for $k+1$. Thus

$$\begin{aligned}
1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 && \text{[From (2)]} \\
&= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\
&= \frac{(k+1)[k(2k+1) + 6(k+1)]}{6} \\
&= \frac{(k+1)(2k^2+7k+6)}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} \\
&= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6},
\end{aligned}$$

so that (1) holds for $k+1$; thus it follows by Mathematical Induction that (1) holds for all natural numbers. □

Functions.

Let $f : X \to Y$ be a function. Then f is

- *injective (or one-to-one)* if $f(x_1) = f(x_2)$, with $x_1, x_2 \in X$, then $x_1 = x_2$.
- *surjective (or onto)* if for every $y \in Y$, there exists an $x \in X$ such that $f(x) = y$.
- *well defined* if $x_1 = x_2$, with $x_1, x_2 \in X$, then $f(x_1) = f(x_2)$.

A function $h : S \to T$ is called an *identity* on S if $h(s) = s$ for all $s \in S$. Now consider the functions $f : X \to Y$ and $g : Y \to X$. The function g is an inverse function of f if $f \circ g$ is an identity on Y and if $g \circ f$ is an identity on X.

Integers mod n.

Let n be a positive integer. Define a relation on $\mathbb{Z}$ as follows:

$$x \sim y \text{ if and only if there exists } k \in \mathbb{Z} \text{ such that } x = y + kn.$$

Now we shall show that this is an equivalence relation on $\mathbb{Z}$.
Proof. Let x, y, and z be integers. We have

- *Reflexivity.* Clearly $x \sim x$ since $x = x + 0 \cdot n$; so this relation is reflexive.
- *Symmetry.* Suppose that $x \sim y$. Then it follows by definition that $x = y + kn$ for some integer k. That is, $y = x + (-k)n$, so that $y \sim x$. Thus this relation is symmetric.
- *Transitivity.* Suppose that $x \sim y$ and $y \sim z$. By definition, we have that $x = y + k_1 n$ and $y = z + k_2 n$ for some integers k_1 and k_2. Thus $x = (z + k_2 n) + k_1 n = z + (k_1 + k_2)n$, so that $x \sim z$. We have thus shown that this relation is transitive.

Since the relation is reflexive, symmetric, and transitive, it follows by definition that it is an equivalence relation. $\square$

To emphasize the dependence of this relation on n, we usually write $x \equiv y \pmod{n}$ instead of $x \sim y$. Also the equivalence class of an integer y is denoted $[y]_n$.

Example. $[2]_{11} = \{\ldots, 2, 13, 24, 35, \ldots\}$.

Exercise 2.

Proof that addition mod n is well-defined; i.e.,

$$[a]_n + [b]_n = [a+b]_n.$$

Proof. Let $x \in [a]_n$ and $y \in [b]_n$. Then $x \equiv a \pmod{n}$ and $y \equiv b \pmod{n}$. By definition, $n \mid x - a$ and $n \mid y - b$. So, by definition, $x - a = np$ and $y - b = nq$ for some integers p and q. Then we have:

$$\begin{aligned} (x-a) + (y-b) &= np + nq && \Rightarrow \\ (x+y) - (a+b) &= n(p+q) && \Rightarrow, \end{aligned}$$

so $n \mid (x+y) - (a+b)$. Therefore, by definition, $x + y \equiv a + b \pmod{n}$, as desired. $\square$

Chapter 3.

Groups.

A group is a set G together with a binary operation $*$ that satisfies the following:

1. *Associativity.* For all $x, y, z \in G$, we have that $x * (y * z) = (x * y) * z$.
2. *Identity.* There exists an element e in G such that $e * x = x = x * e$ for all $x \in G$.
3. *Inverses.* For all $g \in G$, there exists $g^{-1} \in G$ such that $g * g^{-1} = e = g^{-1} * g$.

Subset and Subgroups.

Let $(G, *)$ be a group and let H be a subset of G. Then H is called a subgroup of G if:

1. *Closure.* For all $h_1, h_2 \in H$, we have that $h_1 * h_2 \in H$.
2. *Identity.* $e \in H$, where e is the identity of G.
3. *Inverses.* For all $h \in H$, there exists $h^{-1} \in H$ such that $h * h^{-1} = e = h^{-1} * h$.

or, equivalently, if

1. H is not empty, and
2. H is closed under $*$; that is $h_1 * h_2 \in H$ for all $h_1, h_2 \in H$.

Some Notations.

$$M_n(\mathbb{R}) := \text{the set of all } n \times n \text{ matrices with real entries}$$
$$GL_n(\mathbb{R}) := \text{the set of all } n \times n \text{ invertible matrices with real entries}$$
$$SL_n(\mathbb{R}) := \text{the set of all } n \times n \text{ matrices with real entries and determinant} = 1$$

When are the three sets defined above groups?

	Binary Operation		
Set	Addition	Multiplication	Is abelian?
$M_n(\mathbb{R})$	Yes	No	Yes
$GL_n(\mathbb{R})$	No	Yes	No
$SL_n(\mathbb{R})$	No	Yes	No

Theorem 3.4.

Let G be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. We have $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. By uniqueness, $(ab)^{-1} = b^{-1}a^{-1}$. $\square$