Algebra 1 Jan 6.

<u>Remark</u>: This course will consist almost entirely of proofs. As much as possible, we will ground ourselves by doing sample calculations and examples, but this is a theoretical course. It is targeted at students who intend to pursue a degree in math. Please review the textbook to be sure this is the course for you.

<u>Sets</u>

A <u>set</u> is a collection of things. It could be a collection of numbers:

$$A = \{x \mid x \text{ is an even integer and } x > 2\}$$
$$= \{4, 6, 8, 10, \dots\}$$

or something very abstract:

$$A = \{\text{people in MATH 2020} \mid \text{they have been to Tim Horton's in the last 72 hours}\}.$$

The things in a set are <u>elements/members</u>: Our notation for some important sets will be: $\emptyset$ = empty set.

$\mathbb{N}$ = natural numbers = $\{1, 2, 3, \dots\}$

$\mathbb{Z}$ = integers $\{\dots, -1, 0, 1, \dots\}$

$\mathbb{Q}$ = rational numbers $\{\frac{p}{q} \mid p, q \in \mathbb{Z} \text{ and } q \neq 0\}$

$\mathbb{R}$ = real numbers

$\mathbb{C}$ = complex numbers.

We write <u>subsets</u> as: $A \subset B$. This means every element of A is also in B. Sets are equal, written $A = B$, if $A \subset B$ and $B \subset A$.

We can take intersections and unions:

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\} \quad \text{or} \quad \bigcap_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ for all } i\}$$

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\} \quad \text{or} \quad \bigcup_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ for some } i\}$$

<u>Disjoint</u> sets are sets with $A \cap B = \emptyset$.

The <u>difference</u> of two sets is

$$A \setminus B = \{x \mid x \in A \text{ but not } x \in B\}.$$

i.e. $x \notin B$, or A' if we want complement.

<u>Theorem</u>: (De Morgan's Laws).

Let A and B be sets. Then

(1) $(A \cup B)' = A' \cap B'$

(2) $(A \cap B)' = A' \cup B'$.

<u>Proof</u>: Equality of sets means there are two containments to show, so we need to do $(A \cup B)' \subset A' \cup B'$ and $A' \cup B' \subset (A \cup B)'$ to show (1).

So first assume $x \in (A \cup B)'$. Then $x \notin A \cup B$, meaning x is neither in A nor in B.

By definition of A' and B', this means $x \in A'$ and $x \in B'$. So $x \in A' \cap B'$. Therefore $(A \cup B)' \subset A' \cap B'$.

To show the reverse inclusion, let $x \in A' \cap B'$. Then $x \notin A$ and $x \notin B$. Therefore $x \notin A \cup B$, so ~~###~~ $x \in (A \cup B)'$. Thus $A' \cap B' \subset (A \cup B)'$.

We conclude that $A' \cap B' = (A \cup B)'$.

To prove the statement (2), we proceed similarly.

== Relations, functions, products ==

The <u>product</u> of two sets A and B is

$$A \times B = \{(a,b) \mid a \in A \text{ and } b \in B\}.$$

<u>Example</u>: If $A = \{0,1,2\}$ and $B = \{a, b\}$, then $A \times B$ has $3 \times 2 = 6$ elements, they are:

$$A \times B = \{(0,a),(0,b),(1,a),(1,b),(2,a),(2,b)\}.$$

We can also that a product of many sets:

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i \text{ for all } i\}.$$

<u>Example</u>: $\mathbb{R}^n = \underbrace{\mathbb{R} \times \mathbb{R} \times \dots \times \mathbb{R}}_{n \text{ times}}.$

Definition: A *relation* is a subset of $A \times B$, where A and B are arbitrary sets.

Definition: A function f from A to B (written $f: A \longrightarrow B$ is a relation $f \subset A \times B$ that satisfies:

(*) For every $a \in A$, there is exactly one pair of the form $(a, b) \in f$

In other words, 'a' occurs as the first entry of exactly one pair. We write $f(a) = b$ instead of $(a,b) \in f$.
The set A is the *domain* of f, and B is the *range* or *image* of f.

Example: If $A = \{0, 1, 2\}$ and $B = \{a, b\}$ and

$$f(0) = a$$
$$f(1) = a$$
$$f(2) = b$$

Then, technically $f = \{(0,a), (1,a), (2,b)\} \subset A \times B$.

Example: If we try to define $f: \mathbb{Q} \longrightarrow \mathbb{R}$ by $f(\frac{p}{q}) = p$, then this is not a function:

$f(\frac{1}{2}) = 1$, but $\frac{2}{4} = \frac{1}{2}$ and $f(\frac{2}{4}) = 2$.

So is $f(\frac{1}{2}) = 1$ or $= 2$? The problem here is that $(\frac{1}{2}, 1) \in f$ and $(\frac{1}{2}, 2) \in f$.

When there are many possible values for f, we say it is *not* *well-defined*.

The words onto, one-to-one will be replaced by *surjective* and *injective*, a function which has both these properties will be called *bijective*.

Example: Suppose that $S = \{1, 2, 3\}$. Define a function $\pi : S \longrightarrow S$ by the rule

$$\pi(1) = 2, \quad \pi(2) = 1, \quad \pi(3) = 3.$$

As a relation, π is the subset

$$\pi = \{(1, 2), (2, 1), (3, 3)\}.$$

The function π is one-to-one and onto, so it's bijective.

A bijection $\pi : S \longrightarrow S$ will be called a *permutation* of S. Permutations are sometimes written:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{array}{l} \longleftarrow \text{the domain} \\ \longleftarrow \text{their images} \end{array}$$

This is *not* ~~to~~ be confused with some other kind of matrix!

There is one special map we need to name. For any set S, you can always define a function f by

$$f(s) = s \quad \text{for all } s \in S.$$

This function will be called the *identity function*, and written $id_S(s) = s$.

A function $g: B \to A$ is the <u>inverse</u> of $f: A \to B$ if $g \circ f = id_A$ and $f \circ g = id_B$. In this case we call f invertible, and write f^{-1} in place of g.

<u>Theorem</u>: A function is invertible if and only if it is one-to-one and onto.

<u>Proof</u>: Suppose first that f has an inverse, call it g. Then if $f: A \to B$, $g \circ f = id_A$. That is, $g \circ f(a) = a$ for all $a \in A$. So, if $f(a_1) = f(a_2)$, then apply g and $g(f(a_1)) = g(f(a_2)) \Rightarrow a_1 = a_2$. So f is injective.

To show f is surjective, choose $b \in B$. Then $f \circ g = id_B$ and we calculate $f(g(b)) = b$. So we plug $g(b)$ into f to get $b \Rightarrow f$ surjective.

On the other hand, if f is bijective then define $g: B \to A$ by letting $g(b)$ be the unique $a \in A$ s.t. $f(a) = b$.

Equivalence relations

<u>Def</u>:

An <u>equivalence</u> <u>relation</u> on a set X is a relation $R \subset X \times X$ satisfying:

(i) $(x, x) \in R$ for all $x \in X$ (reflexive)

(ii) $(x,y)\in R \implies (y,x)\in R$ (symmetric)

(iii) $(x,y)\in R$ and $(y,z)\in R$ implies $(x,z)\in R$ (transitive).

When $(x,y)\in R$, we write $x\sim y$ and say x and y are equivalent.

<u>Example</u>: Consider $\mathbb{Z}\times\mathbb{Z} = X$. Define a subset $R\subset(\mathbb{Z}\times\mathbb{Z})\times(\mathbb{Z}\times\mathbb{Z})$ by $(p,q)\sim(r,s)$ if and only if $ps=qr$, where q and s are nonzero. Then it is easy to check that it's reflexive and symmetric, for example $(p,q)\sim(p,q)$ since $pq=pq$. To check transitivity, let $(p,q)\sim(r,s)$ and $(r,s)\sim(a,b)$ be given. Then $ps=qr$ and $rb=sa$ which implies $\frac{p}{q}=\frac{r}{s}$ and $\frac{r}{s}=\frac{a}{b}$, and so $\frac{p}{q}=\frac{a}{b}$, which implies $pb=qa$. Therefore $(p,q)\sim(a,b)$ and R is an equiv. relation.

<u>Example</u>: Let A, B be ~~real~~ $n\times n$ matrices with real entries. Define $A\sim B$ if there is an invertible $n\times n$ matrix P with real entries such that

$$PAP^{-1}=B.$$

For example, if $n=2$ and $A=\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}$ and $B=\begin{pmatrix} -18 & 33 \\ -11 & 20 \end{pmatrix}$ then $A \sim B$ since $P=\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$ gives $PAP^{-1}=B$ (check!)

To show this is an equivalence relation, we check:

(i) If I is the identity matrix, then $IAI^{-1}=A$. so $A \sim A$ (reflexive).

(ii) If $A \sim B$ then $PAP^{-1}=B$. Set $Q=P^{-1}$, then $P^{-1}BP=A$ becomes $QBQ^{-1}=A$, so $B \sim A$ (symmetric).

(iii) If $A \sim B$ and $B \sim C$, then $PAP^{-1}=B$ and $QBQ^{-1}=C$. Therefore $Q(PAP^{-1})Q^{-1}=C$

$$\Rightarrow (QP)A(QP)^{-1}=C,$$

so $A \sim C$ (transitive).

<u>Definition</u>: A partition P of a nonempty set X is a collection $\{X_i\}_{i\in I}$ of subsets of X such that

(i) $X_i \cap X_j$ when $i \neq j$

(ii) $\bigcup_{i\in I} X_i = X$.

<u>Definition</u>: Let $\sim$ be an equivalence relation on a set X. Then we call, for each $x \in X$,

$[x] = \{y \in X \mid x \sim y\}$

the equivalence class of x.

<u>Theorem</u>: Given an equivalence relation $\sim$ on a set X, the equivalence classes form a partition of X. Conversely, if $\mathcal{P} = \{X_i\}$ is a partition of X then there is an equivalence relation on X whose equivalence classes are $\{X_i\}_{i \in I}$.

<u>Proof</u>: First, suppose $\sim$ is an equivalence relation on X. Then $X = \bigcup_{x \in X} [x]$, so we need only show that when $[x]$ and $[y]$ are distinct, they are disjoint. Suppose, for contradiction, that $[x] \neq [y]$ and $z \in [x] \cap [y]$. Then $x \sim z$ and $y \sim z$, so by transitivity, $x \sim y$. So $[x] \subset [y]$, similarly $[y] \subset [x]$, so $[y] = [x]$. This contradicts $[x] \neq [y]$, so $[x] \cap [y] = \emptyset$.

On the other hand, if $\mathcal{P} = \{X_i\}_{i \in I}$, given $x, y \in X$ declare $x \sim y$ if $x, y \in X_i$ (there's a single set containing them). Then we check that it's reflexive, symmetric & transitive.

Example: For $i = 0, 1, 2, 3, \ldots, n-1$, set

$$X_i = \{ m \in \mathbb{Z} \mid m = i + kn \text{ for some } k \in \mathbb{Z} \}.$$

ie, the remainder of m when you divide by n is i.

Then $\{X_i\}_{i=0}^{n-1}$ is a partition of the integers. The equivalence relation corresponding to this partition is called "congruence modulo n", we write $a \equiv b \mod n$ if $a, b \in X_i$ for some i, equivalently if $a \sim b$.

Recommended Exercises:

4–16, 17, 19, 20–24.