MATH 101: ALGEBRA I
WORKSHEET, DAY #1

We review the prerequisites for the course in set theory and beginning a first pass on group theory. Fill in the blanks as we go along.

1. Sets

A set is a "collection of objects". (Our set theory is naive, and we do not go into super important foundational issues. Please take a logic class, it is amazingly cool!)

Basic sets:

- $\emptyset$, the empty set containing no elements;
- $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$, the integers;
- $\mathbb{Z}_{\geq 0} = \{x \in \mathbb{Z} : x \geq 0\}$, the nonnegative integers; similarly, positive integers, etc.;
- $\mathbb{N} =$ __________________________, the natural numbers;
- $\mathbb{Q}$, the rational numbers;
- $\mathbb{R}$, the real numbers;
- $\mathbb{C}$, the complex numbers.

A set X is a subset of a set Y if $x \in X$ implies $x \in Y$, and we write $X \subseteq Y$. (Some write $X \subset Y$.) Two sets are equal, and we write $X = Y$, if they contain precisely the same elements, which can also be written ____.

Operations on two sets X, Y:

- $X \cup Y$, union: we have $x \in X \cup Y$ if and only if $x \in X$ or $x \in Y$;

Date: Monday, 12 September 2016.

- $X \cap Y$, intersection: we have $x \in X \cap Y$ if and only if ________________________;

- $X \setminus Y$, set minus: we have $x \in X \setminus Y$ if and only if ________________________;

- $X \sqcup Y$, disjoint union: we write disjoint union instead of union when

  ____.

- $X \times Y = \{(x, y) : x \in X, y \in Y\}$, the Cartesian product.

A relation R on a set X is ____. For example, equality is a relation on any set, defined by ______________________________. An equivalence relation is a relation $\sim$ that is:

- reflexive, ______________________________,

- ____________, ____, and

- ____________, ____.

An equivalence relation $\sim$ partitions X into a disjoint union of equivalence classes, where the equivalence class of $x \in X$ is ____. The set of equivalence classes $X/\sim$ is the quotient of X by $\sim$, and we have a projection map

$$\pi : X \to X/\sim$$

$$x \mapsto [x]$$

Let $n \in \mathbb{Z}_{>0}$. We define an equivalence relation on $\mathbb{Z}$ by $x \equiv y \pmod{n}$ if $n \mid (x - y)$. The set of equivalence classes is denoted $\mathbb{Z}/n\mathbb{Z}$.

2. Functions

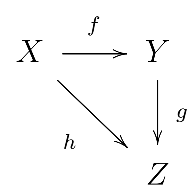
A function or map from a set X to Y is denoted $f : X \to Y$: the precise definition is via its graph $\{(x, f(x)) : x \in X\} \subseteq X \times Y$.

The collection of all functions from X to Y is denoted Y^X, and this is sensible notation because

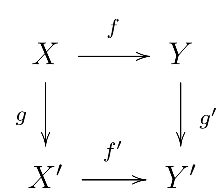
____.

Let $f : X \to Y$ be a function. Then X is the domain and Y is the ____________. We write $f(X) = \operatorname{img} f$ for the image of f. The identity map on X is denoted $\mathrm{id}_X : X \to X$ and defined by ________________________.

Given another function $g : Y \to Z$, we can compose to get $g \circ f : X \to Z$ defined by $(g \circ f)(x) = g(f(x))$. Sometimes we will have more elaborate diagrams:



We say a diagram like the above is commutative if we start from one set and travel to any other, we get the same answer regardless of the path chosen: in the above example, this reads ________________________. Similarly, the diagram



is commutative if and only if ________________________.

We say that f factors through a map $g : X \to Z$ if there exists a map $h : Z \to Y$ such that ____, i.e. the diagram commutes.

The function f is:

- injective (or one-to-one) if ______________________________, and if so we write $X \hookrightarrow Y$;
- surjective (or onto) if ______________________________, and if so we write $X \twoheadrightarrow Y$; and
- bijective (or a one-to-one correspondence), if f is both injective and surjective, and we write $X \xrightarrow{\sim} Y$.

Lemma. *Define the relation $\sim$ on X by $x \sim x'$ if $f(x) = f(x')$. Then the following hold.*

(a) *$\sim$ is an equivalence relation.*

(b) *f factors uniquely through the projection $\pi : X \to X/\sim$. If f is surjective, then the map $(X/\sim) \to Y$ is bijective.*

In a picture:

Proof. First, part (a). ______________________________

____

Next, part (b). ______________________________

____

____

____

____ □

Example. If I is a set, and for each $i \in I$ we have a set X_i, we can form the product $X_I = \prod_{i \in I} X_i$. The set X_i has projection maps $\pi_i : X_I \to X_i$ for $i \in I$. The product X_I is uniquely determined up to bijection by the following property: for any set Y and maps $f_i : Y \to X_i$, there is a unique map $f : Y \to \prod_{i \in I} X_i$ such that $\pi_i \circ f = f_i$. In a diagram:

A left inverse to f is a function $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$, and similarly a right inverse. The function f has a left inverse if and only if ______________________________.
In a picture:

Similarly, f has a right inverse if and only if ______________________________.

If $y \in Y$, we will write $f^{-1}(y) = \{x \in X : f(x) = y\}$ for the fiber of y, and if this fiber consists of one element, we will abuse notation and also write this for the single element.

An inverse to f is a common left and right inverse. The function f has an inverse if and only if ________________________; if this inverse exists, it is unique, denoted $f^{-1} : Y \to X$ in line with the above.

The cardinality of a set X is either:

- finite, if there is a bijection $X \xrightarrow{\sim} \{1, \ldots, n\}$ for some $n \in \mathbb{Z}_{\geq 0}$, and in this case we write $\#X = n$;
- countable, if there is a bijection $X \xrightarrow{\sim} \mathbb{Z}$; or
- uncountable, otherwise.

If X is finite, we sometimes write $\#X < \infty$ and in the latter two cases, we write $\#X = \infty$.

(This is just the beginning of a more advanced theory of cardinal numbers.)

3. Groups

Let X be a set. A binary operation on X is ____.

Let $*$ be a binary operation on X. The definition is still too general, and some binary operations are better than others!

- $*$ is associative if ____.
- $*$ has an identity if ____.

Lemma. *A binary operation can have at most one identity element.*

Proof. ____ □

Definition. A monoid is a set X equipped with an associative binary operation $*$ that has an identity. (We will never use them, but a semigroup is a nonempty set with an associative binary operation.)

Example. The set of positive integers $\mathbb{Z}_{>0}$ is a monoid under multiplication.

The set of nonnegative integers $\mathbb{Z}_{\geq 0}$ is a monoid under addition.

Monoids exist everywhere in mathematics, but they are still too general to study: their structure theory combines all the complications of combinatorics with algebra.

Let X be a monoid. An element $x \in X$ is invertible if there exists $y \in X$ such that ____; the element y is unique if it exists because

____

so it is denoted x^{-1} and is called the inverse of x.

Definition. A group is a monoid in which every element is invertible.

The group axioms for a group G can be recovered from the requirement that $a * x = b$ has a unique solution $x \in G$ for every $a, b \in G$.

Example. The smallest group is ______________________________, with the binary operation ________________________. Examples of groups include:

- ____
- ____
- ____

Example. My favorite group is the quaternion group of order 8, defined by

____

Example. Let $n \in \mathbb{Z}_{>0}$. The dihedral group of order $2n$, denoted D_{2n} (or sometimes D_n) is

____

____

In a group, the (left or right) cancellation law holds:

____

A group is:

- abelian (or commutative) if ______________________________.
- finite if ________________________.
- dihedral if ________________________.

From now on, let G be a group.

Lemma. *If $x^2 = 1$ for all $x \in G$, then G is abelian.*

Proof. ____. □

The order of an element $x \in G$ is ____, and is denoted ______________.

Example. Important examples are matrix groups. Let F be a field, a set with ____.

We write $F^\times = F \smallsetminus \{0\}$. For $n \in \mathbb{Z}_{\geq 1}$, let

$$\mathrm{GL}_n(F) = \{A \in \mathrm{M}_n(F) : \det(A) \neq 0\}$$

be the general linear group (of rank n) over F. Then $\mathrm{GL}_n(F)$ is a group.

A homomorphism of groups $\phi : G \to G'$ is a map such that ____________________________.

Let $\phi : G \to G'$ be a group homomorphism. Then we say ϕ is a(n):

- isomorphism if ____________________________;
- automorphism if ____________________________;
- endomorphism if ____________________________;
- monomorphism if ____________________________;
- epimorphism if ____________________________.

A subgroup $H \leq G$ is a subset that is a group under the binary operation of G (closed under the binary operation and inverses).