MATH 514: EUCLIDEAN GEOMETRY

1. Some math terms

The following is a quick "dictionary" of terms commonly used in mathematical writing. Note that the distinction between some of these terms is very important, and the distinction between others is merely semantic.

The following terms describe things that are *assumed* to hold true. They usually do not follow logically from other principles. A specific example in which the axioms hold is considered a **model**.

- **Axiom** - usually the foundation of a part of mathematics
- **Definition** - not as foundational as axioms, and the statements often involve previous definitions or consequences of the axioms
- **Postulate** - historically interchangeable with axiom, though not commonly used now

The following things are all *logical consequences* of axioms and definitions. That is, they can be *proven* using only the axioms, definitions, logic, and previously proven propositions. The difference between the following items is semantic, not mathematical.

- **Proposition** - a generic term for a logical consequence of average importance
- **Theorem** - an extremely fundamental, important proposition
- **Corollary** - follows almost immediately from a Theorem (requires very little extra work)
- **Lemma** - a seemingly minor/unimportant proposition that is used to prove a larger proposition/theorem

Here are a couple of other terms you may encounter.

- **Conjecture** - an unproven statement which is believed to be true, but no proof has been found. Usually, disproving the conjecture is equally as interesting.
- **Proof** - the actual series of logical steps used to establish a proposition.

We say that an axiom is **independent** of other axioms if it is not a logical consequence of the other axioms. While it is not required that all axioms are independent of one another, this is usually the case. To show that an axiom (A) is independent of the others, it suffices to construct a model where the other axioms hold, but (A) does not hold.

Date: March 5, 2014.

2. Isomorphisms of groups

Most mathematical objects are defined as sets with some extra structure. In these cases, one usually studies maps between sets that preserve this extra structure. An **isomorphism** will be a bijection that preserves this structure. Here is a particular example.

In an abstract algebra course, one studies groups. These are sets equipped with a multiplication structure that is associative, and has inverses and an identity. One studies functions between groups that are compatible with the product structure.

Definition 2.1. A *group* $(G, *)$ is a set G equipped with a binary operation $G \times G \xrightarrow{*} G$ (called multiplication) satisfying the following axioms:

- (Identity) Exists $e \in G$ satisfying $e * g = g * e = g$ for all $g \in G$.
- (Inverse) For all $g \in G$, exists $g^{-1} \in G$ satisfying $g^{-1} * g = e = g * g^{-1}$.
- (Associativity) For all $g_1, g_2, g_3 \in G$, $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$.

Definition 2.2. Let G, H be groups. A function $G \xrightarrow{f} H$ is a *group homomorphism* if it satisfies

$$f(g_1 * g_2) = f(g_1) * f(g_2)$$

for all $g_1, g_2 \in G$. An *isomorphism* is a group homomorphism that is a bijection. We say that two groups G_1 and G_2 are isomorphic $G_1 \cong G_2$ if there exists an isomorphism $G_1 \to G_2$.

An *automorphism* of a group G is a group isomorphism $G \to G$.

Example 2.3. Define $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \cdots, n-1\}$, where the "product" is defined $a * b := (a + b \mod n)$. This is an example of an *abelian group*, meaning that the product structure is also commutative. (The product in an abelian group is often denoted $+$.)

Example 2.4. Consider $H = \{1, x, x^2\}$ with the multiplication induced by $x^i * x^j = x^{i+j}$ and the relation $x^3 = 1$. One can readily check this is a group.

Example 2.5. There is a natural function $\mathbb{Z}/3\mathbb{Z} \xrightarrow{f} H$ given by

$$f(0) = 1, \quad f(1) = x, \quad f(2) = x^2;$$

which can be written concisely as $f(n) = x^n$. One can check that f is a *homomorphism* (compatible with the products), and that f is a bijection. Hence, we say that $\mathbb{Z}/3\mathbb{Z} \cong H$; i.e. the group $\mathbb{Z}/3\mathbb{Z}$ is isomorphic to H.

Example 2.6. Can there be an isomorphism $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} H$ for any other $n \neq 3$? Suppose that $f : \mathbb{Z}/n\mathbb{Z} \to H$ is an isomorphism. This implies that f is a bijection of sets, *and* that f is compatible with the group structure. In general, a bijection between two sets exists if and only if they have the *same cardinality.* A simple counting argument shows that

$$|\mathbb{Z}/n\mathbb{Z}| = n, \quad |\{1, x, x^2\}| = 3.$$

Hence, there cannot exist an isomorphism $\mathbb{Z}/n\mathbb{Z} \cong H$ when $n \neq 3$.

Example 2.7. Let $G = \{1, -1, i, -i\}$ denote the group with commutative multiplication defined by

$$1g = g, \quad -1 * -1 = 1, -1 * i = -i, -1 * -i = i, i^2 = -1.$$

Show that $G \cong \mathbb{Z}/4\mathbb{Z}$.

Example 2.8. The group D_3 is given by the set $D_3 = \{1, x, x^2, y, xy, x^2y\}$, with multiplication induced by the usual laws of exponents combined with the following relations:

$$x^3 = 1, \quad y^2 = 1, \quad yx = x^2y.$$

The groups D_3 and $\mathbb{Z}/6\mathbb{Z}$ both have 6 elements. However, they are not isomorphic, because one cannot construct a bijection that is also a group homomorphism. Why not? Bonus HW problem: Show that if G_1 is an abelian group, and G_2 is not abelian, then $G_1 \ncong G_2$.