Intro to Logic

A *group* is a triple $\langle G, \circ, e \rangle$ such that

- (G1) For all x, y, z: $(x \circ y) \circ z = x \circ (y \circ z)$.
- (G2) For all x: $x \circ e = x$.
- (G3) For all x there is a y such that: $x \circ y = e$.

The following are groups: $\langle \mathbb{Z}, +, 0 \rangle$ and $\langle \mathbb{R}, +, 0 \rangle$.

The following are not: $\langle \mathbb{N}, +, 0 \rangle$ and $\langle \mathbb{R}, \cdot, 1 \rangle$.

The axioms mention right inverses; below we claim that left inverses exist.

Theorem 1 *For every x, there is a y such that:* $y \circ x = e$.

In mathematics, we study the properties of various objects, *e.g.*, groups. The properties that these objects enjoy are captured with "non-logical" axioms, *e.g.*, in the case of group theory, (G1)-(G3). The theory of groups consists of all theorems that are derivable from the "non-logical axioms" *via logical reasoning alone*.

This reasoning cannot appeal to intuition or "obvious truths" about groups. So, what exactly is a "proof", then? This question naturally leads to computer science and historically that is what happened, as a proof has to be machine-checkable.

Proofs and Logic

When we prove theorems about groups, then the results apply to every instance of a group, a structure satisfying $G = \{(G1), (G2), (G3)\}$.

If some formula φ holds in every group (denoted $G \models \varphi$), then does there necessarily exist a proof (denoted $G \vdash \varphi$)?

Note that proofs are finite, but there are many groups; how many?

Some of the results we prove will answer these questions in a very general way.

Preview: There are so many groups, that they do not even form a set. Also, we will present a simple proof theory. Then, we will see that for any set of sentences Φ and any sentence φ, $\Phi \models \varphi$ iff $\Phi \vdash \varphi$. This is Gödel's completeness theorem, perhaps the most important result in logic, as it relates syntax with semantics.

Alphabets

An *alphabet* $\mathcal{A}$ is a nonempty set of *symbols*. $\mathcal{A}^*$ is the set of finite strings over $\mathcal{A}$.

Lemma 1 *If* $|\mathcal{A}| \leq \omega$ *then* $|\mathcal{A}^*| = \omega$