Algebra I
Fall 2011

Prof. Rami Grossberg
notes by Brendan W. Sullivan

September 1, 2011

1 Groups

Definition 1.1. *A* semigroup *is a nonempty set S with a binary operation $\cdot$ that is associative; i.e.*

$$\forall x, y, z \in S \; [x \cdot (y \cdot z) = (x \cdot y) \cdot z]$$

Definition 1.2. *A* monoid *is a semigroup $(S, \cdot)$ with a two-sided identity; i.e.*

$$\exists e \in S . \forall x \in S \; [x \cdot e = e \cdot x = x]$$

Definition 1.3. *A group is a monoid $(G, \cdot)$ with two-sided inverses; i.e.*

$$\forall x \in G . \exists y \in G \; [x \cdot y = y \cdot x = e]$$

Remark 1.4. In a group $(G, \cdot)$, inverses are unique, because

$$x \cdot y_1 = y_1 \cdot x = x \cdot y_2 = y_2 \cdot x = e \Rightarrow y_1 = (y_2 x) y_1 = y_2$$

Definition 1.5. *A group $(G, \cdot)$ is* abelian *(equivalently,* commutative*)* $\iff \forall x, y \in G [x \cdot y = y \cdot x]$.

Definition 1.6. *A* field $(F, +, \cdot, 0, 1)$ *is a nonempty set F with elemens $0 \neq 1 \in F$ such that $(F, +, 0)$ is an abelian group and $(F - \{0\}, \cdot, 1)$ is an abelian group (sometimes denoted $F^\star$, or called the multiplicative group of F) and the distributive property holds:*

$$\forall x, y, z \in F [x \cdot (y + z) = x \cdot y + x \cdot z]$$