Elementary Number Theory
Math 17500, Section 30
Autumn Quarter 2008

John Boller, e-mail: `boller@math.uchicago.edu`
website: `http://www.math.uchicago.edu/~boller/M175`

# Some Algebraic Definitions

**Definition 0.0.1** A *ring* is a set $R$ with two binary operations $+$ and $\cdot$ satisfying rules E1–E3, A1–A5, M1–M2, and D from the definition of the integers. In addition (and independent of each other), the ring is said to be:

- *commutative* if it also satisfies M3
- *with identity* if it also satisfies M4
- *ordered* if it also satisfies O1–O4

A *field* is a set $F$ with two binary operations $+$ and $\cdot$ satisfying rules E1–E3, A1–A5, M1–M4, and D from the definition of the integers as well as:

**M5. (Multiplicative Inverses)**

For any $a \in F$ with $a \neq 0$, there is an element $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$ and $a^{-1} \cdot a = 1$.

**Definition 0.0.2** A *group* is a set $G$ with a binary operation $*$ satisfying:

**E1. (Reflexivity, Symmetry, and Transitivity of Equality)**

| | |
|---|---|
| Reflexivity of Equality | If $a \in G$, then $a = a$. |
| Symmetry of Equality | If $a, b \in G$ and $a = b$, then $b = a$. |
| Transitivity of Equality | If $a, b, c \in G$ and $a = b$ and $b = c$, then $a = c$. |

**E2. (Equality and the Group Law)**

If $a, b, c \in G$ and $a = b$, then $a * c = b * c$.

**G1. (Closure)**

If $a, b \in G$, then $a * b \in G$.

**G2. (Associativity)**

If $a, b, c \in G$, then $(a * b) * c = a * (b * c)$.

**G3. (Identity)**

There is an element $e \in G$ such that $a * e = a$ and $e * a = a$ for every $a \in G$.

**G4. (Inverses)**

For any $g \in G$, there is an element $g^{-1} \in F$ such that $g \cdot g^{-1} = 1$ and $g^{-1} \cdot g = 1$.