Group Theory I

UW Math Circle – Advanced Group

Session 14 (23 January 2014)

A binary operation $*$ on a set S is called *commutative* if $a * b = b * a$ for all $a, b \in S$ and *associative* if $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$.

A *group* is a **nonempty** set G with a **associative** binary operation $*$ on G such that the following axioms are satisfied:

G1. (Identity element) There exists an element $1 \in G$ such that for all $a \in G$, $a * 1 = 1 * a = a$.

G2. (Inverse elements) For every $a \in G$ there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = 1$.

If the operation $*$ is **commutative**, then the group is called *commutative* or *abelian.*

Theorem 1 (Elementary properties of groups I)**.** *Let G be a group.*

1. *(Unique identity) A group contains exactly one identity element.*
2. *(Unique inverses) Every element of a group has exactly one inverse.*
3. *(Cancellation) If $a, b, c \in G$ and $a * c = b * c$ or $c * a = c * b$, then $a = b$.*

The notation a^n, where n is a positive integer, denotes $\underbrace{a * a * \cdots * a}_{n}$. If n is a negative integer, $a^n = \left(a^{-1}\right)^{-n}$. Also, $a^0 = 1$.

Theorem 2 (Elementary properties of groups II)**.** *Let G be a group. Below we assume $a, b, c, d \in G$ and m, n are integers.*

1. $a^m * a^n = a^{m+n}$.
2. $(a^m)^n = a^{mn}$.
3. $(a * b)^{-1} = b^{-1} * a^{-1}$.
4. $(a^n)^{-1} = \left(a^{-1}\right)^n$.