THEORY OF GROUPS

NOTES FOR THE SENIOR SEMINAR IN ALGEBRA
HAMILTON COLLEGE, FALL 2015.

1. Abstract groups

"Abstraction is real, probably more real than nature."
- Josef Albers

1.1. **The definition.**

Definition 1.1. Let G be a set with a binary operation $*$. The structure $\mathbb{G} = (G, *)$ is called a ***group*** if the following axioms hold:

(1) for all $x, y, z \in G$, we have $(x * y) * z = x * (y * z)$,
(2) there exists an element $e \in G$ such that for all $x \in G$, $x * e = x = e * x$, and
(3) for all $x \in G$, there exists a w such that $x * w = e = w * x$.

We often write xy in place of $x * y$.

Theorem 1.2. *Let G be a group. If $e_1, e_2 \in G$ and for all $x \in G$, $xe_1 = x = e_1x$ and $xe_2 = x = e_2x$, then $e_1 = e_2$. In other words, G has a unique "identity" element.*

Notation 1.3. The previous theorem states that every group has a *unique* element e satisfying axiom (2) from Definition 1.1. This element will be called the ***identity*** or ***trivial*** element of the group. For groups whose binary operation is denote by $*$ or $\cdot$, the default symbol for the identity (in these notes) will be 1. However, if the binary operation is denote by $+$, the default symbol for the identity will be 0.

Theorem 1.4. *Let G be a group, and let $x \in G$. If $w_1, w_2 \in G$ with $xw_1 = 1 = w_1x$ and $xw_2 = 1 = w_2x$, then $w_1 = w_2$. In other words, every element of G has a unique "inverse."*

Notation 1.5. Theorem 1.4 states that for every element x of a group there is a *unique* element w satisfying axiom (3) from Definition 1.1 This element will be called the ***inverse*** of x. For groups whose binary operation is denote by $*$ or $\cdot$, the default notation for the inverse of x will be x^{-1}; however, if the binary operation is denote by $+$, the inverse of x will be denoted by $-x$.

Problem 1.6. Give examples of groups with the following properties by *explicitly* defining the binary operation and noting the identity and inverses:

(1) a group with 4 elements,
(2) a group with 4 elements for which multiplication is *truly different* than the previous example, and
(3) an infinite group.

1.2. **Basic arithmetic.**

Notation 1.7. Let G be a group. If $g, h \in G$, then we call gh the ***product*** of g and h. Also, for $n \in \mathbb{N}$, g^n denotes the product of g with itself n-times, and g^{-n} denotes $\left(g^{-1}\right)^n$.

Theorem 1.8. *Let G be a group. If $g \in G$ and $m, n \in \mathbb{Z}$, then*

(1) $1^n = 1$,
(2) $g^{-n} = (g^n)^{-1}$,
(3) $g^m g^n = g^{m+n}$, *and*
(4) $(g^m)^n = g^{mn}$.

Theorem 1.9. *Let G be a group. If $g, h \in G$, then $(gh)^{-1} = h^{-1}g^{-1}$.*

1.3. **Orders of elements.**

Definition 1.10. Let G be a group, and let $g \in G$. If $g^n = 1$ for some positive $n \in \mathbb{N}$, then we define the ***order*** of g, denoted $|g|$, to be the smallest such n. Otherwise, we say that g has ***infinite order*** and write $|g| = \infty$. The ***order*** of G is defined to be the cardinality of G, denoted $|G|$.

Fact 1.11 (Division Algorithm)**.** Let n be an integer and m a positive integer. There are **unique** integers q (the quotient) and r (the remainder) for which $n = qm+r$ and $0 \leq r < m$.

Theorem 1.12. *Let G be a group and $n \in \mathbb{Z}$. If $g \in G$, then $g^n = 1$ if and only if $|g|$ divides n.*

Definition 1.13. Let G be a group. If $g, h \in G$, then we say that g and h ***commute*** if $gh = hg$. More generally, $g_1, \ldots, g_r \in G$ are said to ***commute*** if $g_i g_j = g_j g_i$ for all $1 \leq i, j \leq r$.

Theorem 1.14. *If $g_1, \ldots, g_r$ are commuting elements of a group, then $|g_1 \cdots g_r|$ must divide* $\operatorname{lcm}(|g_1|, \ldots, |g_r|)$.

Problem 1.15. Determine if the conclusion of the previous theorem can be improved to read "…then $|g_1 \cdots g_r| = \operatorname{lcm}(|g_1|, \ldots, |g_r|)$."

Definition 1.16. We call a group G ***abelian*** (or ***commutative***) if $gh = hg$ for all $g, h \in G$.

Theorem 1.17. *If every nontrivial element of a group has order* 2*, then the group is abelian.*

Problem 1.18. Do you think that there is something special about the number 2 that makes the previous theorem work? If so, what might it be. If not, state a more general theorem that you believe to be true.