Math 425: Abstract Algebra I
Theorems from the Textbook - Sections 2.1-2.4

Theorems

Theorem 2.1.1. *If a binary operation $*$ on a set S has an identity, then it is unique.*

Theorem 2.1.4. *If $(G, *)$ is a group and $g \in G$, then the inverse of G is unique.*

Theorem 2.2.1. *If $(M, *)$ is a monoid, then the set of all unit $M^\times$ is a group using the operation $*$, called the* unit group*.*

Theorem 2.2.2. *If $G_1, G_2, \ldots, G_n$ are groups with respective operations $*_1, *_2, \ldots, *_n$, then*

$$G_1 \times G_2 \times \cdots \times G_n$$

is a group under component-wise operation

$$(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots, g_n *_n h_n).$$

Theorem 2.2.3. *Let $g, h, g_1, g_2, \ldots, g_{n-1}, g_n$ be elements of a group G ($n \in \mathbb{Z}_{\geq 1}$).*

1. $e^{-1} = e$.
2. $(g^{-1})^{-1} = g$.
3. $(gh)^{-1} = h^{-1}g^{-1}$.
4. $(g_1 g_2 \cdots g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} \cdots g_2^{-1} g_1^{-1}$.
5. $(g^m)^{-1} = (g^{-1})^m$ *for all* $m \geq 0$.

Theorem 2.2.4 (Exponent Laws)**.** *Let G be a group and $g, h \in G$.*

1. $g^n g^m = g^{n+m}$ *for all* $m, n \in \mathbb{Z}$
2. $(g^n)^m = g^{n \cdot m}$ *for all* $m, n \in \mathbb{Z}$
3. *If* $gh = hg$, *then* $(gh)^n = g^n h^n$ *for all* $n \in \mathbb{Z}$

Theorem 2.2.5 (Cancellation Laws)**.** *Let G be a group and $g, h, f \in G$.*

1. *If* $gh = gf$ *then* $h = f$ *(*left cancellation*)*
2. *If* $hg = fg$ *then* $h = f$ *(*right cancellation*)*

Theorem 2.2.6. *Let G be a group and $g, h \in G$.*

1. *The equation $gx = h$ has a unique solution $x = g^{-1}h$ in G.*
2. *The equation $xg = h$ has a unique solution $x = hg^{-1}$ in G.*

Theorem 2.3.1 (Subgoup Test)**.** *A subset H of a group G is a subgroup of G if and only if the following conditions are satisfied.*

1. $1_G \in H$*, where* 1_G *is the identity element of* G*.*

2. *If* $h \in H$ *and* $h_1 \in H$*, then* $hh_1 \in H$*.*

3. *If* $h \in H$*, then* $h^{-1} \in H$*, where* $h^{-1} \in G$ *denotes the inverse of* h *in* G*.*

Note that implicit in these statements, if $H \leq G$ then H and G have the same unity and inverses persist.

Theorem 2.3.3. *If G is any group, then $Z(G)$ is a subgroup of G. Moreover, $Z(G)$ is always abelian.*

Theorem 2.4.1. *Let g be an element of a group G, and write*

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}.$$

Then $\langle g \rangle$ is a subgroup of G, and $\langle g \rangle \subseteq H$ for every subgroup H of G with $g \in H$.

Theorem 2.4.2. *Let $g \in G$ with $o(g) = n$. Then*

1. $g^k = 1$ *if and only if* $n|k$*.*

2. $g^k = g^m$ *if and only if* $k \equiv m \pmod{n}$

3. $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ *where* $1, g, g^2, \ldots, g^{n-1}$ *are all distinct.*

Theorem 2.4.3. *Let G be a group and let $g \in G$ satisfy $o(g) = \infty$. Then*

1. $g^k = 1$ *if and only if* $k = 0$*.*

2. $g^k = g^m$ *if and only if* $k = m$*.*

3. $\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots\}$ *where the* g^i *are distinct.*

Corollary. *For all g in a group G, $|g| = |\langle g \rangle|$.*

Theorem (Order in $\mathbb{Z}_n$)**.** *Given $\overline{a} \in (\mathbb{Z}_n, +)$, with $1 \leq a \leq n-1$,*

$$|\overline{a}| = \frac{n}{\gcd(a, n)}.$$

Theorem . *If $\gamma = (k_1\ k_2\ \ldots\ k_r)$ is an r-cycle in S_n, then $|\gamma| = r$.*

Theorem 2.4.4. *If $\gamma = \sigma_1\sigma_2 \ldots \sigma_r$ where σ_i are disjoint cycles, then*

$$|\gamma| = \operatorname{lcm}(|\sigma_1|, |\sigma_2|, \ldots, |\sigma_r|).$$

Theorem 2.4.6. *Every cyclic group is abelian, but the converse does not hold.*

Theorem 2.4.7. *Every subgroup of a cyclic group is cyclic.*

Theorem 2.4.8. *Let $G = \langle g \rangle$ be a cyclic group, where $o(g) = n$. Then $G = \langle g^k \rangle$ if and only if $\gcd(k, n) = 1$.*

Theorem 2.4.9 (The Fundamental Theorem of Finite Cyclic Groups)**.** *Let $G = \langle g \rangle$ be a cyclic group of order n.*

1. *If H is a subgroup of G, then $H = \langle g^d \rangle$ for some $d|n$. Hence $|H|$ divides n.*

2. *Conversely if $k|n$, then $\langle g^{n/k} \rangle$ is the unique subgroup of G of order k.*

Definitions

Definition. A *binary operation*, $*$ on a set S is a function that associates to each ordered pair $(a, b) \in S \times S$ an element of S which we call $a * b$.

Since we know that $a * b \in S$ for all $a, b \in S$, we say that the binary operation is *closed under* $*$.

Definition. A binary operation $*$ on S is *associative* if

$$a * (b * c) = (a * b) * c,$$

for all $a, b, c \in S$.

Definition. A binary operation $*$ on S is *commutative* if

$$a * b = b * a,$$

for all $a, b \in S$.

Definition. An element $e \in S$ is called an *identity* (or *unity*) for the binary operation $*$ if

$$a * e = e * a = a,$$

for all $a \in S$.

Definition. A set S along with a binary operation $*$ is called an *monoid* if $*$ is associate and has an identity.

If $(S, *)$ is also commutative, then we say S is a *commutative monoid*.

Definition. Let $(M, *)$ be a monoid.

If $x \in M$, we call $y \in M$ an *inverse of* x if

$$xy = e = yx.$$

An element that has an inverse is called a *unit*.

Definition. Suppose that

1. G is a set and $*$ is a binary operation on G,
2. $*$ is associative,
3. there is some $e \in G$ such that
$$g * e = e * g = g,$$
for all $g \in G$, and
4. for all $g \in G$, the is an $h \in G$ such that $g * h = e = h * g$.

Then $(G, *)$ is a *GROUP*.

Definition. The *nth roots of unity* are the complex numbers that are the roots of

$$x^n - 1.$$

Denote the set of roots as $\mathcal{U}_n$

Definition. If the operation of a group G is commutative, we call G an *abelian group.*

Definition. A *Cayley table* is essentially a multiplication table for a given binary operation.

Definition. We call $C_n = \{1, a, a^2, \ldots, a^{n-1}\}$ the cyclic group of order n. Multiplication is defined by $a^x a^y = a^{x+y}$ and $a^n = a^0 = 1$.

Definition. A subsets H of a group G is call a *subgroup* of G if H is also a group using the same operation as G. We denote subgroups using the notation $H \leq G$.

If $H \leq G$ and $H \neq G$, we call H a *proper subgroup of G.*

Definition. The *subset of G generated by $g \in G$* in multiplicative notation is

$$\langle g \rangle = \{g^k | k \in Z\} = \{\ldots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^2, \ldots\}.$$

The *subset of G generated by $g \in G$* in additive notation is

$$\begin{aligned}\langle g \rangle &= \{kg | k \in Z\} \\ &= \{\ldots, -g-g-g, -g-g, -g, 0, g, g+g, g+g+g, \ldots\}.\end{aligned}$$

Definition. The *subgroup lattice* of a group G is a schematic picture of the subgroups of G. A line going up from one group to another indicates that the bottom group is a subgroup of the top one.

Definition. The *center* of the group G is the set

$$Z(G) = \{z \in G | zg = gz \ \forall g \in G\}.$$

Definition. A group G is *cyclic* if there is some $g \in G$ for which $G = \langle g \rangle$.

Definition. If G is a finite group, the *order of a group G* is denoted $|G|$ and is the cardinality of the set G.

The *order of an element $g \in G$* is denoted $|g|$ or $o(g)$ and equals the smallest positive integer n such that $g^n = e$.

Definition. In general, if X is a nonempty subset of a group G, then the *subgroup of G generated by X* is defined as

$$\begin{aligned}\langle X \rangle &= \{\text{products of powers (not nec. distinct) of elements of X}\} \\ &= \{x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m} \mid x_i \in X,\ k_i \in \mathbb{Z},\ m \geq 1\}\end{aligned}$$

We will always have $\langle X \rangle \leq G$.