Abstract Algebra Theorems and Definitions

MTH 411 - Fall 2023

0 Preliminaries

- **Axiom** **Well Ordering Principle:** Every nonempty set of positive integers contains a smallest element.
- **Definition** **Equivalence Relation:** An *equivalence relation* on a set S is a set R of ordered pairs of elements of S such that
  1. $(a, a) \in R \ \forall a \in S$ (reflexive property).
  2. $(a, b) \in R$ implies $(b, a) \in R$ (symmetric property).
  3. $(a, b) \in R$ and $(b, c) \in R$ imply that $(a, c) \in R$ (transitive property).
- **Definition** **Function (mapping):** A *function* ϕ from a set A to a set B is a rule that assigns to each element a of A exactly one element b of B. The set A is called the *domain* of ϕ, and B is called the *range* of ϕ. If ϕ assigns b to a, then b is called the *image of a under ϕ*. The subset of B comprising all the images of elements of A is called the *image of A under ϕ*.
- **Definition** **Composition of Functions:** Let $\phi : A \mapsto B$ and $\psi B \mapsto C$. The *composition* $\psi\phi$ is the mapping from A to C defined by
$$(\psi\phi)(a) = \psi(\phi(a)), \ \forall a \in A.$$
- **Definition** **One-to-One Functions (injection):** A function ϕ from a set A is called *one-to-one* if for every $a_1, a_2 \in A$, $\phi(a_1) = \phi(a_2)$ implies $a_1 = a_2$.
- **Definition** **Onto Functions (surjection):** A function ϕ from a set A to a set B is said to be *onto* if each element of B is the image of at least one element of A. In symbols, $\phi : A \mapsto B$ is onto if for each $b \in B$ there is at least one $a \in A$ such that $\phi(a) = b$.
- **Theorem** **Division Algorithm:** Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique integers q, r with the property that $a = bq + r$, where $0 \leq r < b$.
- **Theorem** **GCD is a Linear Combination:** For any nonzero integers a and b, there exist integers s and t such that $\texttt{gcd}(a, b)$ is the smallest positive integer of the form $as + bt$.
- **Theorem** **Euclid's Lemma:** Let p be a prime, and let a, b be integers. If $p|ab$ then $p|a$ or $p|b$.

- **Theorem Fundamental Theorem of Arithmetic:** Every integer greater than 1 is a prime or product of primes. This product is unique, except for the order in which the factors appear. That is, if $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$, where the p's and q's are primes, then $r = s$ and, after renumbering the q's, we have $p_i = q_i$ for all i.
- **Theorem First Principle of Mathematical Induction:** Let S be a set of integers containing a. Suppose S has the property that whenever some integer $n \geq a$ belongs to S, then the integer $n+1$ also belongs to S. Then, S contains every integer greater than or equal to a.
- **Theorem Second Principle of Mathematical Induction:** Let S be a set of integers containing a. Suppose S has the property that n belongs to S whenever every integer less than n and greater than or equal to a belongs to S. Then, S contains every integer greater than or equal to a.
- **Theorem DeMoivre's Theorem:** For every positive integer n and every real number θ, $(\cos(\theta) + i\sin(\theta))^n = \cos n\theta + i \sin n\theta$.

1 Introduction to Groups

- **Other?** D_4 **(Symmetries of a Square):** $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$.
- **Other?** D_n **(Dihedral Groups):** $D_n = \{R_0, R_{\cdot\frac{360}{n}}, \ldots, R_{(n-1)\cdot\frac{360}{n}}\} + n$ other flips across lines.

2 Groups

- **Definition Binary Operation:** Let G be a set. A *binary operation* on G is a function that assigns each ordered pair of elements of G an element of G.
- **Definition Group:** Let G be a set together with binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab. We say G is a *group* under this operation if the following three properties are satisfied.
  1. *Associativity.* The operation is associative; that is, $(ab)c = a(bc)$ for all $a, b, c \in G$.
  2. *Identity.* There is an element e (called the *identity*) in G such that $ae = ea = a$ for all $a \in G$.
  3. *Inverses.* For each element a in G, there is an element b in G (called an *inverse* of a) such that $ab = ba = e$.
- **Theorem Uniqueness of Identity:** In a group G, there is only one identity element.
- **Theorem Uniqueness of Inverses:** For each element a in a group G, there is a unique element $b \in G$ such that $ab = ba = e$.
- **Theorem Cancellation:** In a group G, the right and left cancellation laws hold; that is, $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

- **Theorem Socks-Shoes:** For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.

3 Finite Groups; Subgroups

- **Definition Order of a Group:** The number of elements of a group (finite or infinite) is called its *order*. We will use $|G|$ to denote the order of G.

- **Definition Order of an Element:** The order of an element g is a group G is the smallest integer n such that $g^n = e$ (in additive notation, this would be $ng = 0$). If no such integer exists, we say that g was *infinite order*. The order of an element g is denoted $|g|$.

- **Definition Subgroup:** If a subset H of a group G is itself a group under the operation of G, we say that H is a *subgroup* of G.

- **Definition Center of a Group:** The *center*, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. In symbols,
$$Z(G) = \{a \in G | ax = xa,\ a \in G\}.$$

- **Definition Centralizer of a in G:** Let a be a fixed element of a group G. The *centralizer of a in G, $C(G)$*, is the set of all elements in G that commute with a. In symbols, $C(a) = \{g \in G | ga = ag\}$.

- **Theorem One-Step Subgroup Test:** Let G be a group and H a nonempty subset of G. If ab^{-1} is in H whenever a, b are in H, then H is a subgroup of G (in additive notation, if $a - b$ is in H whenever a, b are in H, then H is a subgroup of G).

- **Theorem Two-Step Subgroup Test:** Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a, b are in H (H is closed under the operation), and a^{-1} is in H whenever a is in H (H is closed under taking inverses), then H is a subgroup of G.

- **Theorem Finite Subgroup Test:** Let H be a nonempty finite subset of a group G. If H is closed under the operation G, then H is a subgroup of G.

- **Theorem Center of a Subgroup:** The center of a group G is a subgroup of G.

- **Theorem C(a) is a Subgroup:** For each a in a group G, the centralizer of a is a subgroup of G.

4 Cyclic Groups

- **Definition Euler $\varphi-$Function:** Let $\phi(1) = 1$, and for any integer $n > 1$, let $\phi(n)$ denote the number of positive integers less than n and relatively prime to n.

- Theorem **Criterion for $a^i = a^j$:** Let G be a group, and let $a \in G$. If a has infinite order, then $a^i = a^j$ if and only if $i = j$. If a has finite order, say n, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ if and only if $n | i - j$.
- Corollary **$|a| = \langle a \rangle$:** For any group element a, $|a| = \langle a \rangle$.
- Corollary **$a^k = e$ Implies That $|a|$ divides k:** Let G be a group and let a be an element of order n in G. If $a^k = e$, then n divides k.
- Corollary **Relationship Between $|ab|$ and $|a||b|$:** If a and b belong to a finite group and $ab = ba$, then $|ab|$ divides $|a||b|$.
- Theorem **$\langle a^k \rangle = \langle a^{\mathsf{gcd}(n,k)} \rangle$ and $|a^k| = n/\mathsf{gcd}(n,k)$:** Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\mathsf{gcd}(n,k)} \rangle$ and $|a^k| = n/\mathsf{gcd}(n,k)$.
- Corollary **Orders of Elements in Finite Cyclic Groups:** In a finite cyclic group, the order of an element divides the order of a group.
- Corollary **Criterion for $\langle a^i \rangle = \langle a^j \rangle$ and $|a^i| = |a^j|$:** Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\mathsf{gcd}(n,i) = \mathsf{gcd}(n,j)$, and $|a^i| = |a^j|$ if and only if $\mathsf{gcd}(n,i) = \mathsf{gcd}(n,j)$.
- Corollary **Generators of Finite Cyclic Groups:** Let $|a| = n$. Then $\langle a \rangle = \langle a^j \rangle$ if and only if $\mathsf{gcd}(n,j) = 1$, and $|a| = |\langle a^j \rangle|$ if and only if $\mathsf{gcd}(n,j) = 1$.
- Corollary **Generators of $\mathbb{Z}_n$:** An integer $k \in Z_n$ is a generator of Z_n if and only if $\mathsf{gcd}(n,k) = 1$.
- Theorem **The Fundamental Theorem of Cyclic Groups:** Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k–namely, $\langle a^{n/k} \rangle$.
- Corollary **Subgroups of $\mathbb{Z}_n$:** For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of Z_n of order k; moreover, these are the only subgroups of Z_n.
- Theorem **Number of Elements of Each Order in a Cyclic Group:** If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.