Modern Algebra 1 — Lecture notes
MAT 513/613, Fall 2024 — D. Ivanšić

0 Preliminaries

We recall some basic facts about divisibility of numbers.

Definition. A nonzero integer n *divides* an integer m if there exists an integer q such that $m = q \cdot n$. We write $n \mid m$ and say: n *divides* m, n *is a divisor of* m, or m *is a multiple of* n. Note that 0 does not divide any integer.

Definition. A *prime* or a *prime number* is a positive integer greater than 1 whose only positive divisors are 1 and itself.

Definition. Let $n \in \mathbf{N}$, $a, b \in \mathbf{Z}$. We say a *is congruent to* b *modulo* n if $n \mid a - b$.
We write $a \equiv b \pmod{n}$.

Theorem. Let a and b be integers, $n \in \mathbf{N}$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a + c \equiv b + d \pmod{n} \text{ and } ac \equiv bd \pmod{n}$$

Division Algorithm Theorem 0.1. Let $n \in \mathbf{N}$. For every integer a, there exist unique integers q and r, $0 \leq r < n$ such that $a = q \cdot n + r$.

Definition. The *greatest common divisor* of two nonzero integers a and b is the largest of all common divisors of a and b. We say a and b are *relatively prime* if their greatest common divisor is 1.

Notation. Greatest common divisor of a and $b = \gcd(a, b)$ Note that $\gcd(a, b) \geq 1$.

Theorem 0.2. For any nonzero integers a and b there exist integers s and t such that $\gcd(a, b) = as + bt$. Also, $\gcd(a, b)$ is the smallest positive integer in the set $\{as + bt \mid s, t \in \mathbf{Z}\}$.

Proof.

Example. Verify Theorem 0.2 for $\gcd(18, 30)$ and $\gcd(4, 7)$.

Corollary. Nonzero integers a and b are relatively prime if and only if there exist integers s and t such that $as + bt = 1$.

Proof.

Euclid's Lemma. Let a and b be integers. If a prime number p divides ab, then p divides a or p divides b.

Proof.

Fundamental Theorem of Arithmetic 0.3. Every integer greater than 1 is a prime or a product of primes. This product is unique except for the order in which the primes appear.

2 Groups

In our experience with mathematics so far, the word "algebra" generally means "arithmetic," in other words, computation with various objects. In school, we start with addition and multiplication of numbers, and expand from there. Both of those operations take two numbers and combine them to create another number.

Try to think of all examples in mathematics you have encountered so far where you take two objects and combine them to get another object of the same kind. (These are examples of binary operations on some set G, essentially functions that send pairs of objects in G to objects in G, in effect, functions $G \times G \to G$).

Examples.

Set, operation Label Properties

Set, operation Label Properties

Set, operation Label Properties

Definition. Let G be a nonempty set. A *binary operation* on G is a function $m : G \times G \to G$ that assigns to each ordered pair in G an element of G. Generally, for brevity, we do not write $m(a, b)$, but ab or $a \cdot b$. Any of $m(a, b)$, ab, $a \cdot b$ is called the *product* of a and b.

Above, we have described some binary operations for various sets G.

Definition. A set G with a binary operation $\cdot$ is said to be a *group* under this operation if the following three properties are satisfied:

1) *Associativity.* For all $a, b, c \in G$, $(ab)c = a(bc)$
2) *Identity.* There exists an element $e \in G$, called the *identity*, such that $ae = ea = a$ for every $a \in G$.
3) *Inverses.* For every element $a \in G$, there is an element $b \in G$, called the *inverse of* a, such that $ab = ba = e$, where e is the identity from 2).

Notation. As various binary operation may be in play on the same set, it is customary to write that $(G, \cdot)$ is a group, which emphasizes the operation under consideration.

Note. Written in function m notation

1) associativity is $m(m(a, b), c) = m(a, m(b, c))$
2) identity element has the property $m(a, e) = m(e, a) = a$
3) the inverse has the property $m(a, b) = m(b, a) = e$

You can see why we don't write it this way.

Definition. If the operation on G further satisfies

Commutativity. For all $a, b \in G$, $ab = ba$.

the group $(G, \cdot)$ is said to be *abelian*. A group is said to be *non-abelian* if the opposite holds, that is, there exist $a, b \in G$ such that $ab \neq ba$. Clearly, abelian groups, having an additional property, are easier to deal with.

Definition. A set G with a binary operation $\cdot$ is said to be a *monoid* under this operation if only properties of associativity and identity are satisfied (inverses need not exist). Clearly, every group is a monoid.

Examples. For all the examples that we started with, state if the set with the operation is a binary operation, a monoid or a group, or none.

While a group only has three properties, they are strong enough that they have many consequences.

Theorem 2.1. In a group G there is only one identity element.

Proof.

Note. We actually proved this stronger statement: if a binary operation has a left identity e ($ea = a$ for all $a \in G$) and a right identity f ($af = a$ for all $a \in G$), they are equal.

Cancellation Theorem 2.2. In a group G, the left and right cancellation laws hold, that is

$$ab = ac \text{ implies } b = c \qquad ab = ac \text{ implies } b = c$$

Proof.

Uniqueness of Inverses Theorem 2.3. For each element a in a group G, there is a unique element $b \in B$ such that $ab = ba = e$.

Proof.

Definition. The unique inverse of a in a group is denoted a^{-1}.

Theorem 2.4. For every a, b in a group G, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof.

Example. Given elements a, b in a group G, show that the equations $ax = b$ and $xa = b$ always have a solution.

Due to associativity, a product of any finite number of group elements $a_1 a_2 \dots a_n$ is uniquely determined, regardless of which product of a pair is computed first, for example

$$abcd = (ab)(cd) = ((ab)c)d = (a(bc))d = a((bc)d)$$

Note. In general, we cannot reorder the group elements in the expression unless the group is abelian.

Definition. For an integer n and a group element g, we define:

$$g^0 = e \qquad \text{if } n > 0, \quad g^n = \overbrace{gg\dots g}^{n \text{ factors}} \qquad \text{if } n < 0, \quad g^n = (g^{-1})^{|n|} = \overbrace{g^{-1}g^{-1}\dots g^{-1}}^{|n| \text{ factors}}$$

Example. Write out the product: $a^3 b^{-4} c^2 =$

Power Rules Proposition. For a group element g and any $m, n \in \mathbf{Z}$,

$$g^m g^n = g^{m+n} \quad \text{and} \quad (g^m)^n = g^{mn}$$

Note. In general $(ab)^n \neq a^n b^n$, but it does hold in an abelian group. Why?

Notation. Often the operation in the group is denoted + (usually this is for an abelian group). In keeping with usual way of writing addition of numbers, we write powers and inverses a little differently in this situation.

	Multiplicative notation	Additive notation
operation	ab or $a \cdot b$	$a + b$
identity	e or 1	0
inverse	a^{-1}	$-a$
powers	a^n	na
quotient	ab^{-1}	$a - b$ (difference)

Example. Show that the set $(\mathbf{R}^2 \setminus \{(0,0)\}, \cdot)$ is a group, where the operation is given by $(a,b) \cdot (c,d) = (ac + 2bd, ad + bc)$. (Note that a similar multiplication $(a,b) \cdot (c,d) = (ac - bd, ad + bc)$ is the product in $\mathbf{C} = \mathbf{R}^2$.)

Example. Let $\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$. On this set we can define addition and multiplication modulo n. For any integer k, let $k \bmod n$ denote the remainder of division of k by n, a number in $\mathbf{Z}_n$. Note that $k \bmod n \equiv k \pmod{n}$.

1) $a + b = (a + b) \bmod n$ — show that $\mathbf{Z}_n$ is a group under this operation.
2) $ab = (ab) \bmod n$ — show that $\mathbf{Z}_n$ is a monoid under this operation. Consider Z_{12} and determine which elements have an inverse under multiplication.
3) Let $U(n)$ = set of all elements of $\mathbf{Z}_n$ that are relatively prime to n. Show that $U(n)$ is a group under multiplication modulo n. Write the Cayley table (of multiplication) for $U(15)$.

Example. Consider the regular n-gon P_n, $n \geq 3$, and the all the bijections $P_n \to P_n$ that preserve distance between points (isometries, symmetries). Such bijections send vertices to vertices and edges to edges and form a group D_n, the dihedral group.

Useful fact. Isometries $\mathbf{R}^2 \to \mathbf{R}^2$ are determined by their action on three noncollinear points. More precisely, if $f, g : \mathbf{R}^2 \to \mathbf{R}^2$ are isometries such that $f(P_i) = g(P_i)$, for three points P_1, P_2, P_3 not all on the same line, then $f(P) = g(P)$ for all $P \in \mathbf{R}^2$.

1) Think of all possible symmetries of P_4 and P_5.
2) How many elements does D_n have?
3) D_2 is interpreted as all symmetries of the "di-gon." How many elements does D_2 have?
4) D_1 is interpreted as all symmetries of two points. How many elements does D_1 have?

3 Finite Groups and Subgroups

Definition. The number of elements in a group G (finite or infinite) is called the *order of the group* G and denoted $|G|$.

Example. $|\mathbf{Z}_n| = n$, $|U(n)| \leq n$ since $U(n) \subseteq \mathbf{Z}_n$

Find $|U(10)| =$

Definition. The *order of an element* g *in a group* G is the smallest positive integer n such that $g^n = e$. We say g has infinite order if no such integer exists. The order of g is denoted $|g|$.

Example. Find the orders of all elements of $(Z_{10}, +)$ and $U(10)$. What happens if you try to apply the same idea to $(Z_{10}, \cdot)$?

Example. What is the order of any nonzero element in $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$, $(\mathbf{C}, +)$?

Example. We know that $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R}$, and each is a group with the same (inherited) operation, addition. This is essentially because $\mathbf{Z}$ and $\mathbf{Q}$ are closed under addition and taking of inverses. This is a common occurrence, so it gets a name: subgroup.

Definition. If a subset H of a group G is a group under the operation of G, we say that H is a subgroup of G.

Notation. H is a subgroup of G: $H \leq G$
H is a proper subgroup of G (that is, $H \neq G$): $H < G$

Note. The set $\{e\}$ and all of G are always subgroups of G.

To show that H is a subgroup, we have to show (associativity is inherited):

— H is closed under the operation of G.

— $e \in H$.

— For every $a \in H$, $a^{-1} \in H$.

Two-Step Subgroup Test Theorem 3.2. Let G be a group and H a nonempty subset of G. If H satisfies the following two conditions, H is a subgroup of G.

1) For every $a, b \in H$, $ab \in H$.
2) For every $a \in H$, $a^{-1} \in H$.

Proof.

Example. $GL(n, \mathbf{R}) = \{A \in M_n(\mathbf{R}) \mid \det A \neq 0\}$, $SL(n, \mathbf{R}) = \{A \in M_n(\mathbf{R}) \mid \det A = 1\}$. Show that $SL(n, \mathbf{R})$ is a subgroup of $GL(n, \mathbf{R})$.

Proposition. Every subgroup of $(\mathbf{Z}, +)$ is of form $n\mathbf{Z}$ for some $n \in \mathbf{N}$, where $n\mathbf{Z} = \{nk \mid k \in \mathbf{Z}\} = \{\dots, -2n, -n, 0, n, 2n, 3n, \dots\}$.

Test 3.2 can be shortened:

One-Step Subgroup Test Theorem 3.1. Let G be a group and H a nonempty subset of G. If H satisfies that for every a, b in H, ab^{-1} is also in H, then H is a subgroup of G.

Finite Subgroup Test Theorem 3.3. Let H be a nonempty finite subset of G. If H is closed under the operation of G, then H is a subgroup of G.

Proof.

Definition. Let $\langle a \rangle = \{a^n \mid n \in \mathbf{Z}\} = \{\ldots, a^{-2}, a^{-1}, a^0, a, a^2, \ldots\}$.

Theorem 3.4. For any element a of a group G, $\langle a \rangle$ is a subgroup of G and $|\langle a \rangle| = |a|$.

Proof.

Definition. The subgroup $\langle a \rangle$ is called the *cyclic subgroup of G generated by a*. Note that $\langle a \rangle$ is finite if $|a|$ is finite, and infinite otherwise.

Example. Consider the example above, $(Z_{10}, +)$ and $U(10)$, and write the elements of all of their cyclic subgroups.

Example. In the dihedral group D_n, let H denote the subset of rotations. Then H is a cyclic subgroup of D_n generated by the rotation by $\frac{2\pi}{n}$.

Note. The group of rotations is a good visualization of any cyclic group generated by an element of order n. (That's why it's called cyclic!)

Definition. Let $S \subset G$ be any subset of a group G and let $S^{-1} = \{a^{-1} \mid a \in S\}$. We define the *subgroup generated by* S as

$$\langle S \rangle = \{a_1 a_2 \dots a_n \mid a_1, a_2, \dots, a_n \in S \cup S^{-1}, n \in \mathbf{N}\}$$

Example. Show that

— $\langle S \rangle$ is a subgroup of G.

— If H is any subgroup of G that contains S, then $\langle S \rangle \leq H$. This says that $\langle S \rangle$ is the smallest subgroup of G that contains S, because it is contained in any other subgroup with the same property.

Note. $\langle S \rangle$ can also be defined as $\bigcap_{H \leq G,\ S \subseteq H} H$, the intersection of all subgroups of G that contain S. One gets the same subgroup.

Definition. The *center* $Z(G)$ *of a group* G is the subset of all elements of G that commute with every element of G.

$$Z(G) = \{a \in G \mid ax = xa \text{ for every } x \in G\}$$

Theorem 3.5. The center of a group G is a subgroup of G.

Proof.

Example. Determine the center of $GL(2, \mathbf{R})$. The same method can be used for $GL(n, \mathbf{R})$.

Definition. For an element $a \in G$ we define $C(a)$, the *centralizer of a in G* as all elements in G that commute with a.

$$C(a) = \{g \in G \mid ga = ag\}$$

Theorem 3.5. The centralizer of a in G is a subgroup of G.

Proof. Essentially the same as for the center of a group.

Example. Determine the centralizer of $\begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}$ in $GL(2, \mathbf{R})$. (For a fun related problem, show using Theorem 3.2 that the form of the matrices in the centralizer form a subgroup.)

4 Cyclic Groups

Recall that a group G is cyclic if $G = \langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$.

Example. Not every group is cyclic. Show that $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ and $(U(8), \cdot)$ are not cyclic.

Theorem 4.1. Let G be a group and let $a \in G$. Then

a) If a has infinite order $a^i = a^j$ if and only if $i = j$.

b) If a has finite order n, then $a^i = a^j$ if and only if $i \equiv j \pmod{n}$, so $\langle a \rangle = \{e, a, a^2, \ldots a^{n-1}\}$.

Proof.

Corollary. Let G be a group and let $a, b \in G$.

1) $|a| = |\langle a \rangle|$.
2) If $|a| = n$ and $a^k = e$ for some $k \in \mathbf{Z}$, then n divides k.
3) If $ab = ba$, then $|ab|$ divides $|a||b|$.

Proof.

Theorem 4.2. Let G be a group, $a \in G$ and let $|a| = n$. For any $k \in \mathbf{N}$, $\left\langle a^k \right\rangle = \left\langle a^{\gcd(n,k)} \right\rangle$ and $|a^k| = \dfrac{n}{\gcd(n,k)}$.

Proof.

Example. Apply the theorem to $(\mathbf{Z}_{10}, +)$ to find orders of all elements without going through their powers.

Corollary. Let G be a group and let $a, b \in G$.

1) In a finite cyclic group, the order of every element divides the order of the group.
2) If $|a| = n$, then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\gcd(n, i) = \gcd(n, j)$, and $|a^i| = |a^j|$ if and only if $\gcd(n, i) = \gcd(n, j)$.
3) If $|a| = n$, then $\langle a^j \rangle = \langle a \rangle$ if and only if $\gcd(n, j) = 1$, and $|a^j| = |a|$ if and only if $\gcd(n, j) = 1$.
4) An integer $k \in \mathbf{Z}_n$ generates $\mathbf{Z}_n$ if and only if $\gcd(n, k) = 1$.

Proof.

Fundamental Theorem of Cyclic Groups 4.3. Every subgroup of a cyclic group is cyclic. Furthemore, if $|a| = n$, the order of any subgroup of $\langle a \rangle$ is a divisor of n; and for each divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k, namely $\left\langle a^{\frac{n}{k}} \right\rangle$.

Proof.

Corollary. For each positive divisor k of n, the subgroup $\left\langle \frac{n}{k} \right\rangle$ is the unique subgroup of order k, and these are the only subgroups of $\mathbf{Z}_n$.

Example. Find all the generators of the subgroup of order 4 in $\mathbf{Z}_{20}$.

Definition. The *Euler phi function* is the function $\phi : \mathbf{N} \to \mathbf{N}$ given by: $\phi(1) = 1$, and

$\phi(n) =$ number of positive integers less than n and relatively prime with n, if $n > 1$

Clearly, $\phi(n) = |U(n)|$.

Theorem 4.4. If $d > 0$ divides n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

Proof.

Note. The number of elements of order d does not depend on n: for example, $\mathbf{Z}_6$, $\mathbf{Z}_{30}$ and $\mathbf{Z}_{150}$ all have $\phi(6) = 2$ elements of order 6.

Corollary. In a finite group, the number of elements of order d is a multiple of $\phi(d)$.

Proof.

One can draw the *lattice* of subgroups of a group G: a picture where all the subgroups are listed and it is shown which one is contained in which. For cyclic groups, this can be done easily based on the statements we had in this chapter.

Example. Draw the lattice of subgroups of $\mathbf{Z}_{24}$.

5 Permutation Groups

Definition. Let A be a set. Any bijection $f : A \to A$ is called a *permutation of A*. The set of all bijections of A with the operation of composition is a group, called the *permutation group of A*.

The permutation group of the finite set $A = \{1, 2, \ldots, n\}$ is called the *symmetric group of degree n* and is denoted S_n. (This is the permutation group we study in this section.)

Any element of S_n can be given by a table of values. For example, a permutation $\alpha \in S_5$ can be written as

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{bmatrix} \text{ which denotes that } \alpha(1) = 3, \alpha(2) = 4, \text{etc.}$$

The name "permutation" comes from the fact that the bottom row in this notation is simply a permutation of the numbers $1, 2, \ldots, n$, of which there are $n!$.

Proposition. $|S_n| = n!$

Note. In keeping with the usual convention of order of composition — for $f \circ g$, it is g that acts first — permutation products are computed so that the rightmost permutation acts first, and then the next one to the left, thus:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{bmatrix} \text{ and NOT } \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{bmatrix}$$

For the permutation α above, note the following:

$$1 \overset{\alpha}{\longmapsto} 4 \overset{\alpha}{\longmapsto} 3 \overset{\alpha}{\longmapsto} 1, \quad 2 \overset{\alpha}{\longmapsto} 5 \overset{\alpha}{\longmapsto} 2$$

In other words, we can form cycles of values that completely describe the permutation, written as $\alpha = (143)(25)$, and this notation can be interpreted as the composite of the permutation that cycles 2 and 5 (and leaves 1, 4 and 3 fixed) and another permutation that cycles 1, 4 and 3 (and leaves 2 and 5 fixed).

Definition. Let α be a permutation of the set $\{1, 2 \ldots, n\}$. A *cycle of values of a number* $a \in \{1, 2, \ldots, n\}$ is the set $[a] = \{\alpha^k(a) \mid k \in \mathbf{Z}\}$ (images of a by all powers of α). The *length of a cycle of values* $[a]$ is the number of elements in $[a]$, that is $|[a]|$.

Note. The length of a cycle of values is ≥ 1.

Example. State the cycles of values and their lengths for the permutation α above.

Proposition. For a permutation $\alpha \in S_n$ and $a, b \in \{1, 2, \ldots, n\}$ we have:

1) $[a] = \{\alpha^k(a) \mid k \in \mathbf{Z}\} = \{\alpha^k(a) \mid k \in \mathbf{Z}, k \geq 0\}$
2) Cycles of values are either disjoint or equal, that is, either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.
3) $[a] = \{a_1, a_2, \ldots, a_m\}$, where $\alpha(a_1) = a_2, \alpha(a_2) = a_3, \ldots, \alpha(a_m) = a_1$ (may take $a_1 = a$), where $a_1, a_2, \ldots, a_m$ are distinct numbers and m is the smallest $k \geq 1$ such that $\alpha^k(a_1) = a_1$.

Definition. A *cycle* α is a permutation in S_n for which there exist distinct numbers $a_1, a_2, \ldots, a_m \in \{1, 2, \ldots, n\}$ so that $\alpha(a_1) = a_2, \alpha(a_2) = a_3, \ldots, \alpha(a_m) = a_1$ and $\alpha(a) = a$ for any $a \notin \{a_1, a_2, \ldots, a_m\}$. This cycle is denoted $(a_1, a_2, \ldots, a_m)$ (order matters). The length of a cycle is the number of elements m in $\{a_1, a_2, \ldots, a_m\}$. A cycle of length m is called an *m-cycle*.

Note. The order of a cycle $|\alpha|$ is equal to the length of the cycle.

Theorem 5.1. Every permutation of a finite set is a cycle or a product of disjoint cycles.

Proof.

Theorem 5.2. If cycles $\alpha = (a_1, a_2, \ldots, a_l)$ and $\beta = (b_1, b_2, \ldots, b_m)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Proof.

Theorem 5.3. The order of a permutation written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Proof.

Example. Find the order of the permutation $\alpha \in S_9$ if $\alpha = (7,3,1,4)(5,8)(6,9)$.

Theorem 5.4. Every permutation in S_n is a product of 2-cycles (non-disjoint).

Proof.

Lemma. If $\varepsilon = \beta_1\beta_2 \ldots \beta_r$, where β_i's are 2-cycles, then r is even (ε = identity).

Proof.

Theorem 5.5. If a permutation α is a product of 2-cycles, then the number of 2-cycles always has the same parity (odd or even). That is, if $\beta_1\beta_2 \ldots \beta_r = \alpha = \gamma_1\gamma_2 \ldots \gamma_s$, where the β_i's and γ_j's are 2-cycles, then r and s are both even or both odd.

Proof.

Definition. A permutation in S_n is *even* if it is a product of an even number of 2-cycles, *odd* if it is a product of an odd number of 2-cycles. We can define a function sign : $S_n \to \{-1, 1\}$ as

$$\text{sign}(\alpha) = \begin{cases} 1 = (-1)^{\text{even}}, & \text{if } \alpha \text{ is even} \\ -1 = (-1)^{\text{odd}}, & \text{if } \alpha \text{ is odd} \end{cases}$$

Theorem 5.6. The set of even permutations forms a subgroup of S_n.

Proof.

Definition. The group of even permutations of n elements is denoted A_n and called the *alternating group of degree* n.

Theorem 5.7. For $n > 1$, the order of A_n is $\dfrac{n!}{2}$.

Proof.

Permutations play an essential role in the definition of the determinant.

Definition. The *determinant* of an $n \times n$ matrix is given as

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \sum_{\alpha \in S_n} \operatorname{sign}(\alpha)\, a_{1\alpha(1)} a_{2\alpha(2)} \dots a_{n\alpha(n)} \quad (\text{has } n! \text{ terms})$$

Example. For 2×2 and 3×3 matrices, show that the above definition is the same as you learned before.

6, 10 Group Homomorphisms and Isomorphisms

Definition. A *homomorphism* from group G to group $\overline{G}$ is a map $\phi : G \to \overline{G}$ that preserves the group operation, that is

$$\text{for every } a, b \in G, \quad \phi(ab) = \phi(a)\phi(b)$$

Example. Verify that the following maps are homomorphisms.

$\phi : (\mathbf{R}, +) \to (\mathbf{R}, +)$
$\phi(x) = cx$ for some $c \in \mathbf{R}$

$\phi : (\mathbf{C} - \{0\}, \cdot) \to (\mathbf{R}^+, \cdot)$
$\phi(z) = |z|$

$\det : (GL(n, \mathbf{R}), \cdot) \to (\mathbf{R}, \cdot)$

$\phi : (\mathbf{R} - \{0\}, \cdot) \to (\mathbf{R} - \{0\}, \cdot)$
$\phi(x) = x^n$

What if $\phi : (\mathbf{R} - \{0\}, +) \to (\mathbf{R} - \{0\}, +)$?

$\phi : (G, \cdot) \to (G, \cdot)$
where G is abelian
$\phi(a) = a^n$

$\phi : (\mathbf{Z}, +) \to (\mathbf{Z}_n, +)$
$\phi(k) = k \bmod n$

Definition. The *kernel* of a homomorphism $\phi : G \to \overline{G}$ is the set

$$\ker \phi = \{x \in G \mid \phi(x) = \overline{e}\} = \phi^{-1}(\{\overline{e}\}) \quad \text{(inverse image of } \{\overline{e}\})$$

Example. Determine the kernels of the above homomorphisms.

Theorem 10.1. Let $\phi : G \to \overline{G}$ be a homomorphism, and $a, b \in G$. Then

1) $\phi(e) = \overline{e}$, where $e, \overline{e}$ are identities in $G, \overline{G}$.
2) $\phi(a^n) = (\phi(a))^n$ for all $n \in \mathbf{Z}$. In particular, $\phi(a^{-1}) = (\phi(a))^{-1}$.
3) If $|a|$ is finite, then $|\phi(a)|$ divides $|a|$.
4) $\ker \phi$ is a subgroup of G.
5) $\phi(a) = \phi(b)$ if and only if $ab^{-1} \in \ker \phi$. In particular, ϕ is injective if and only if $\ker \phi = \{e\}$.
6) If $\phi(a) = c$, then $\phi^{-1}(c) = a \ker \phi$. In other words, the inverse image of c is (particular element sent to c)$\ker \phi$.

Proof.

Theorem 10.2. Let $\phi : G \to \overline{G}$ be a homomorphism, and let H be a subgroup of G and $\overline{K}$ a subgroup of $\overline{G}$. Then

1) $\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of $\overline{G}$.
2) If H is cyclic, so is $\phi(H)$.
3) If H is abelian, so is $\phi(H)$.
4) If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$.
5) If $|\ker \phi| = n$, then ϕ is an n-to-1 mapping from G onto $\phi(G)$
6) If $|H| = n$, then $|\phi(H)|$ divides n.
7) $\phi^{-1}(\overline{K}) = \{x \in G \mid \phi(x) \in \overline{K}\}$ is a subgroup of G.
8) If $\overline{K}$ is a normal subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K})$ is a normal subgroup of G.
9) If ϕ is onto and $\ker \phi = \{e\}$, then ϕ is a bijection.

Proof.

Definition. An *isomorphism* from a group G to a group $\overline{G}$ is a map $\phi : G \to \overline{G}$ that preserves the group operation and is bijective. Thus, $\phi : G \to \overline{G}$ is an isomorphism if

$$1)\ \phi \text{ is a homomorphism: } \phi(ab) = \phi(a)\phi(b) \qquad 2)\ \phi \text{ is a bijection}$$

If there is an isomorphism $\phi : G \to \overline{G}$, we say that G and $\overline{G}$ are *isomorphic* and write $G \approx \overline{G}$.

An isomorphism between groups tells us that they are essentially the same set with the same operation, merely taking different guises.

Example. Let $\langle a \rangle$ be a cyclic group.
If $|a|$ is not finite, $\phi : \mathbf{Z} \to \langle a \rangle$, $\phi(k) = a^k$ is an isomorphism.
If $|a| = n$, $\phi : \mathbf{Z}_n \to \langle a \rangle$, $\phi(k) = a^k$ is an isomorphism.

Note. The subgroup H of rotations in D_n is cyclic of order n so it is isomorphic to $(\mathbf{Z}_n, +)$.

Example. The map $\phi(x) = e^x$ is an isomorphism between $(\mathbf{R}, +)$ and $(\mathbf{R}^+, \cdot)$.

Note. This tells us that multiplication of positive real numbers and addition of real numbers are essentially the same operation. This was exploited since the 17th century with logarithmic tables, which helped turn multiplication and division of numbers (hard) into addition and subtraction (much easier).

There is a good reason we study groups of permutations: every group can be viewed as a subgroup of the group of bijections on some set A.

Example. Every symmetry in D_n permutes the vertices of a regular n-gon in a unique way (why?), so it can be viewed as a permutation of the set $\{1, 2, \ldots, n\}$. However, not every permutation of $\{1, 2, \ldots, n\}$ is realizable by a symmetry: give an example of a permutation of $\{1, \ldots, 4\}$ that is not the result of a symmetry.

Cayley's Theorem 6.1. Every group is isomorphic to a subgroup of the group of permutations on some set A.

Proof.

Example. Follow the proof above to see what subgroup of permutations of $\mathbf{R}$ is $(\mathbf{R}, +)$ isomorphic to.

Note. The theorem allows us to view every group as a more concrete object, permutations of some set A. The proof of the theorem has every group G as a subgroup of permutations of $A = G$. In practice, this is not very efficient or useful, as we generally strive for the set A to be "small."

For example, associating elements of D_n with permutations of $\{1, 2, \ldots, n\}$ (n elements) is an improvement of the default association of D_n with permutation of D_n, which has $2n$ elements.

Theorem 6.2. Let $\phi : G \to \overline{G}$ be an isomorphism, and $a, b \in G$. Then

1) $\phi(e) = \overline{e}$, where $e, \overline{e}$ are identities in $G, \overline{G}$.
2) $\phi(a^n) = (\phi(a))^n$ for all $n \in \mathbf{Z}$. In particular, $\phi(a^{-1}) = (\phi(a))^{-1}$.
3) a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.
4) $G = \langle a \rangle$ if and only if $\overline{G} = \langle \phi(a) \rangle$.
5) $|a| = |\phi(a)|$
6) For a fixed integer k, the equation $x^k = b$ has the same number of solutions in G as the equation $x^k = \phi(b)$ in $\overline{G}$.
7) If G is finite, then G and $\overline{G}$ have the same number of elements of every order.
8) $\ker \phi = \{e\}$

Proof.

Theorem 6.3. Let $\phi : G \to \overline{G}$ be a isomorphism, and let H be a subgroup of G and $\overline{K}$ a subgroup of $\overline{G}$. Then

1) $\phi^{-1} : \overline{G} \to G$ is an isomorphism.
2) G is abelian if and only if $\overline{G}$ is abelian.
3) G is cyclic if and only if $\overline{G}$ is cyclic.
4) $\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of $\overline{G}$.
5) $\phi^{-1}(\overline{K}) = \{x \in G \mid \phi(x) \in \overline{K}\}$ is a subgroup of G.
6) $\phi(Z(G)) = Z(\phi(G))$

Proof.

Example. $\mathbf{Z}_{12}$, D_6 and A_4 all have order 12. Show they are not isomorphic by considering the largest orders of elements in every group or the number of elements of order 2.

Example. Show $(\mathbf{Q}, +)$ is not isomorphic to $(\mathbf{Q} - \{0\}, \cdot)$ by considering the number of order-2 elements.

Note. As one can glean from theorems 6.2 and 6.3, any property expressed in the language of group theory is true for a group if and only if it is true for an isomorphic group. That is why we think of isomorphic groups as "same."

Definition. An *automorphism* of a group G is any isomorphism from G to G. The set of all automorphisms of a group G is denoted $\mathrm{Aut}(G)$.

Example. For $k = 0, \ldots, 9$, consider the function $\phi : \mathbf{Z}_{10} \to \mathbf{Z}_{10}$, $\phi(n) = kn$.
a) Show ϕ is a homomorphism.
b) Why is it enough to consider $k \in \{0, 1, \ldots, 9\}$, rather than $k \in \mathbf{Z}$?
c) For which k is ϕ an automorphism?

Example. Let $a \in G$, and define $\phi_a : G \to G$, $\phi(x) = axa^{-1}$. Show that phi_a is an isomorphism.

Definition. The automorphism ϕ_a of G is called the *inner automorphism induced by* a. Define $\text{Inn}(G) = \{\phi_a \mid a \in G\}$, the set of all inner automorphisms.

Note. $\phi_a = \varepsilon$ if and only if $a \in Z(G)$, so in an abelian group, all inner isomorphisms are the identity (not very interesting).

Example. Let H be a subgroup of G. Then for every $a \in G$, $\phi_a(H)$ is a subgroup isomorphic to H. When G is not abelian, this may give us a number of subgroups in H that are isomorphic to H, but different from H.
a) When $a \in H$, what is $\phi_a(H)$?
b) Let $G = D_n$, $H = \langle a \rangle$, where a is a reflection. Determine $\phi_a(H)$ for every $a \in G$.

Theorem 6.4. $\text{Aut}(G)$ is a group under the operation of composition, and $\text{Inn}(G)$ is a subgroup of $\text{Inn}(G)$. (Note $\text{Aut}(G)$ is itself a subgroup of the group of permutations of G.)

Proof. Homework!

Example. Determine the group $\text{Aut}(\mathbf{Z}_{10})$.

Theorem 6.5. $\mathrm{Aut}(\mathbf{Z}_n) \approx U(n)$

Example. In most examples we have considered, the isomorphism of the groups was pretty apparent. However, some groups that do not seem "same" are in fact isomorphic. These examples are surprising and require somewhat more advanced techniques to show:
— $(\mathbf{R}, +)$ is isomorphic to $(\mathbf{C}, +)$
— $(\mathbf{C} - \{0\}, \cdot)$ is isomorphic to $(\{z \in \mathbf{C} \mid |z| = 1\}, \cdot)$