Abstract Algebra

Rohan Jain

Contents

Chapter 1

1.1 Introductory Notes

1.1.1 Things to Remember

Note:

- Definitions will usually be stated as "if" even though they mean "if and only if".
- Any form of proof is valid. Avoid proofs by contradiction because of disbelief in the law of excluded middle.
- When you define an object, you can *only* utilize its definition to prove anything about it.

1.1.2 Set Review

Definition 1.1.1: Set

In mathematics, a set is an undefined term. Basically, "everyone knows what it is." A few examples of sets are:

- The empty set is the set with no elements. It is denoted by ϕ or $\emptyset$.
- $\mathbb{N}$ is the set of natural numbers.
- $\mathbb{Z}$ is the set of integers.
- $\mathbb{Q}$ is the set of rational numbers.
- $\mathbb{R}$ is the set of real numbers.
- $\mathbb{C}$ is the set of complex numbers.

Note:

- A set is a well-defined collection of objects. The objects in a set are called elements of the set.
- A set is generally defined as a capital letter.
- $(A = B) \iff (\forall x : x \in A \iff x \in B)$
- $(A \subset B) \iff (\forall x \in A : x \in B)$
- A is a proper subset of B if $A \subset B$ and $A \neq B$.

Theorem 1.1.1

$A = B \iff A \subset B \land B \subset A$

Note:

- $A \cup B = x : x \in A \lor x \in B$
- $A \cap B = x : x \in A \land x \in B$
- $A \backslash B = x : x \in A \land x \notin B$
- $C \backslash (A \cup B) = (C \backslash A) \cap (C \backslash B)$

1.1.3 Cartesian Products and Functions

Note:

- $A \times B = \{(a, b) : a \in A \land b \in B\}$

Example 1.1.1 (Cartesian Product of two sets)

Let $A = \{1, 2, \Delta\}$ and $B = \{0, \pi\}$

- $(1, 0)$
- $(2, 0)$
- $(\Delta, 0)$
- $(1, \pi)$
- $(2, \pi)$
- (Δ, π)

Note:

Relations are subsets of Cartesian Products. For example, we can say that $<$ is a relation on the subset of $\mathbb{R} \times \mathbb{R}$ consisting of all ordered pairs of real numbers such that the first element is less than the second.

Definition 1.1.2: Function

A function f from a set A to a set B is a subset of $A \times B$ such that for every $a \in A$, there is exactly one $b \in B$ such that $(a, b) \in f$.

Note:

Let R be a relation from A to B.

- A is the domain
- B is the codomain
- $\{b : aRb\}$ is the image
- R is injective (one-to-one) if $a_1Rb \land a_2Rb \implies a_1 = a_2$
- R is surjective (onto) if $\forall b \in B : \exists a \in A : aRb$. Basically if the image is the entire codomain.
- R is bijective if it is injective and surjective

Note:

$A \xrightarrow{\text{R}} B$
$B \xrightarrow{\text{S}} C$
Define the composition as $S \circ R = \{(a, c) : \text{there is some } b \text{ such that } (a, b) \in R \text{ and } (b, c) \in S\}$

Theorem 1.1.2

Let $f : A \longrightarrow B$, $g : B \longrightarrow C$, and $h : C \longrightarrow D$. Then

- $h \circ (g \circ f) = (h \circ g) \circ f$
- If f and g are injective, so is $g \circ f$
- If f and g are surjective, so is $g \circ f$
- If f and g are bijective, so is $g \circ f$

1.1.4 Equivalence Relations

Definition 1.1.3: Equivalence Relation

An equivalence relation is a relation that has the following special properties:

- Reflexivity: aRa for all $a \in A$
- Symmetry: $aRb \implies bRa$
- Transitivity: $aRb \wedge bRc \implies aRc$

Definition 1.1.4: Partition

Given a set S, a partition of S is a collection of subsets of S such that their union is S.

Note:

Equivalence relations go hand in hand with partitions.

Note:

If $\sim$ is an equivalence relation $a \sim b$, then $\sim$ partiations a set X into chunks. $X/\sim$ is the set of chunks.
Addition is *well-defined* as an operation on $\mathbb{Z}/x\mathbb{Z}$ for $x \in \mathbb{Z}$.

1.1.5 Complex Numbers and Matrices

Definition 1.1.5: Complex Number

A complex number is a number of the form $a + bi$, where a and b are real numbers and i is the imaginary unit. $i^2 = -1$.

Note:

Complex numbers generally take the from $z = a + bi$.
$\bar{z} = a - bi$ is the complex conjugate of z.
Divide complex numbers by multiplying by the complex conjugate of the denominator

Definition 1.1.6: Matrix

A matrix is a rectangular array of numbers. A $m \times n$ matrix is an array of m rows and n columns. Define the group of $m \times n$ matrices over a field $\mathbb{F}$ as $\mathbb{F}^{m \times n}$.

Note:

Multiplication by an $m \times n$ matrix is a function from $\mathbb{F}^n$ to $\mathbb{F}^m$. It is associative because all functions are associative.

Example 1.1.2 (2 × 2 matrix exercise)

Consider $\mathbb{Z}^{2\times 2}$. Define a relation $A \sim B$ if there is an integer matrix P whose determinant is one and $B = P^{-1}AP$. Note that if an integer matrix has a determinant 1 it is invertible and its inverse is also an integer matrix with determinant 1.

1. Show that this is an equivalence relation.
2. Show that two matrices with different determinants cannot be similar.
3. Determine whether $\begin{bmatrix} 6 & 0 \\ 0 & 1 \end{bmatrix}$ is similar to $\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$.
4. Determine whether $\begin{bmatrix} 6 & 0 \\ 0 & 1 \end{bmatrix}$ is similar to $\begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}$.

Solution:

1. Reflexive: $A = P^{-1}AP$ for $P = I_2$.
   Symmetric: $P^{-1}AP = P^{-1}BP$ for some P with determinant 1.
   Transitive: $B = P_1^{-1}AP_1 \wedge C = P_2^{-1}BP_2 \Rightarrow C = P_2^{-1}P_1^{-1}AP_1P_2$
2. Determinants are a multiplicative property. If $B = P^{-1}AP$ and $\det(B) \neq \det(A)$, then $\det(B) \neq 1 * \det(A) * 1$.
3. No, different JCF.
4. Yes, same JCF.

1.1.6 Number Theory

Note:

Know induction, division algorithm, GCD and Bezout's lemma, and Primes and the Fundmental Theorem of Arithmetic.

Example 1.1.3 (Weak Induction)

Prove that $5 | n^5 - n$ for all n.

Proof: Proof by induction.

1. $n = 1$ is true, $5|0$.
2. If it is true then $n = k$, show that it is true when $n = k + 1$.
   $(k+1)^5 - (k+1) = k^5 + 5k^4 + 10k^3 + 10k^3 + 5k + 1 - (k+1) = (k^5 - k) + (5k^4 + 10k^3 + 10k^2 + 5k)$.
   Both quantities are divisible by 5.

Therefore, $5 | n^5 - n$ for all n. 😊

Example 1.1.4 (Strong Induction)

Prove that every integer n can be written as $n = d_1 1! + d_2 2! + \cdots + d_k k!$ for some $d_1, \ldots, d_k \leqslant k \in \mathbb{Z}$ and $k \geqslant 1$.

Proof: Strong induction.
Given n, chose s s.t. $s! \leqslant n < (s+1)!$. Then we can write $n = q \cdot s! + r$.

1. $q \leqslant s$ (if $q \geqslant s + 1$, then $n \geqslant (s+1)!$, which goes against our claim)

2. $r < s!$

Assume that this is true for any $k < n$. Then we can write $n = q \cdot s! + r$ for some $r < s!$. Then we can write r in the same format since it is true for all $k < n$. ☺

Example 1.1.5 (Well-ordering)

Prove that given $a, b, b \neq 0$, there exists unique q, r such that $a = qb + r$ and $0 \leqslant r < |b|$.

Proof: Well-ordering.
Consider all the integeres of the form $a - xb$ for $x \in \mathbb{Z}$. At least one of these is nonnegative. If $a > 0$, choose $x = 0$. If $a \leqslant 0$, then choose $x = -ab|b|$. So let the set of all negative $a - xb$ be nonempty. Let $q = x$ be the smallest. Define $r = a - qb$ so that $a = qb + r$ and $r < |b|$.
To prove uniqueness, consider two sets: qr and $q'r'$. Then $qb + r = q'b + r'$ and $r < |b|$. Or, $(q - q')b = r' - r$. The absolute value of the RHS has to be between $1 - |b|$ and $|b| - 1$. This has to be 0 since its the only multipe of b in that range. So $q - q' = 0$ and $q = q'$ and $r = r'$. ☺

Lemma 1.1.1 Bezout's Lemma

Given integers $a, b \neq 0$, their GCD can be written in the form $ra + sb$ for some r, s.

Definition 1.1.7

An integer is prime if it only has 1 and itself as positive divisors.

Note:
1 is not a prime.

Lemma 1.1.2

If p is prime and $p|ab$, then either $p|a$ or $p|b$.

Theorem 1.1.3 Fundamental Theorem of Arithmetic

Every integer greater than 1 is either a prime or can be written as a product of primes in a unique way.

1.2 Group Theory

1.2.1 Introduction to Groups

Definition 1.2.1: Binary Operation

Given a set S, a *binary operation* on S is a function $S \times S \longrightarrow S$.

Definition 1.2.2: Group

A *group* is a set G with a binary operation $*$ such that for all $a, b, c \in G$, the following hold:

1. $(a * b) * c = a * (b * c)$ (associativity)
2. $e * a = a * e = a$ (identity)
3. $a * a^{-1} = e$ (inverse)
4. $*$ is closed under G.

Note:

A set that only has associativity and identity is called a *monoid*.

Note:

Examples of groups

- $\mathbb{Z}, \mathbb{R}, \mathbb{R}^{3\times 3}, \mathbb{C}, \mathbb{Q}$ with addition.
- $z \in \mathbb{C} : |z| = 1$ with multiplication.
- $GL(2, \mathbb{R})$ with matrix multiplication. However, this is not abelian.
- D_4 = symmetries of a square.
- D_2 = symmetries of a triangle.
- $U(n)$ with multiplication modulo n.

If we take a random group, say $U(5)$, then we can create a table for how the multiplication works:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

A table like this is called a *Cayley Table*. Notice that this table is actually symmetric. This means that the group is *commutative*, but more properly, *abelian*.

Definition 1.2.3: Abelian Group

An *abelian group*, G, is a group where $a * b = b * a$ for all $a, b \in G$.

1.2.2 Properties of Groups

Theorem 1.2.1

The identity element of a group is unique.

Proof: Let e_1 and e_2 be the identity elements. Then $e_1 * e_2 = e_2 * e_1 = e_1$. So $e_1 = e_2$. 😊

Theorem 1.2.2

Each element has a unique inverse.

Proof: Let a^{-1} and b both be inverses of a then consider the product baa^{-1}. Then $b = be = b(aa^{-1}) = (ba)a^{-1} = ea^{-1} = a^{-1}$. So $b = a^{-1}$. 😊

Corollary 1.2.1

$(ab)^{-1} = b^{-1}a^{-1}$

Proof: $abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$. 😊

Corollary 1.2.2

$(a_1a_2a_3 \dots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}a_{n-2}^{-1} \dots a_1$

Proof: Induction from 1.2.1. ☺

Corollary 1.2.3
$(a^{-1})^{-1} = a$

Proof: $(a^{-1})^{-1}a^{-1} = e = aa^{-1}$, so by uniqueness of inverses... ☺

Theorem 1.2.3
Given any $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solutions, though not necessary equal.

Proof: Let $x = a^{-1}b$ and $y = ba^{-1}$. Then $ax = a(a^{-1}b) = eb = b$ and $ya = ba^{-1}a = be = b$. To show uniqueness, consider $ax_1 = ax_2$ then left multiply by a^{-1}. ☺

Corollary 1.2.4 Cancellation Laws
In any group G, if $ac = bc$, then $a = b$. And if $ca = cb$, then $a = b$.

Proof: Right or left multiply by c^{-1} for appropriate equation. ☺

Note:
Proving that a group is associative from its Cayley digram takes too long. It is easier to show an isomorphism to a well-established group.

Note:
Groups of order n:

- 1: $\mathbb{Z}_1$
- 2: $\mathbb{Z}_2$
- 3: $\mathbb{Z}_3$
- 4: $\mathbb{Z}_4, V$
- 5: $\mathbb{Z}_5$
- 6: $D_3, \mathbb{Z}_6$
- 7: $\mathbb{Z}_7$
- 8: $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4, H$
- 9: $\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$

Note:
A note on notation:
$a \cdot a = a^2, a \cdot a \cdot a = a^3 \ldots$

Definition 1.2.4: Direct Product

Given G_1, G_2 groups, then the direct proudct $G_1 \times G_2$ is the group of ordered pairs (g_1, g_2) where $g_1 \in G_1$ and $g_2 \in G_2$. The operation is $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2)$.

Example 1.2.1
$\{e\} \times G \cong G$

Example 1.2.2
$\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$

Example 1.2.3
$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong Z_6$

Theorem 1.2.4
Let $(G, \circ, e)$ be a set with the binary operation $\circ$ and left identity e. Then assume each $x \in G$ has a left inverse such that $x^{-1} \circ x = e$. Then G is a group.

Proof: what is $xe =$?
Let $y = xe$. Then $x^{-1}y = x^{-1}(xe) = (x^{-1}x)e = e$. So $x^{-1}y = e = x^{-1}x$. Multiply by $x^{-1^{-1}}$ to get $y = x$. Therefore, e is a two-sided identity.
To show that x^{-1}, consider $z = x \circ x^{-1}$. Left multiply by x^{-1} to get $x^{-1} \circ z = x^{-1} \circ (x \circ x^{-1}) = (x^{-1} \circ x) \circ x^{-1} = x^{-1}$. Left multiply both sides by $x^{-1^{-1}}$ to see that $e \circ z = z = e$. Therefore, x^{-1} is a left inverse and G is a group. 😆

Definition 1.2.5: Subgroups

Let $(G, \circ, e)$ be a group and let $H \subset G$. If H is a group under the same operation $\circ$, then H is a *subgroup* of G. This is denoted as $H < G$.

Note:
Having the same operation is critical. For example $GL(2) \subset \mathbb{R}^{2\times 2}$, but $GL(2)$ is not a subgroup of $\mathbb{R}^{2\times 2}$ because the operation is matrix multiplication, not addition.

Lenma 1.2.1
If $H \subset G$ and for any $h_1, h_2 \in H$, $h_1 h_2^{-1} \in H$, then H is a subgroup.

Proof: Following:

- Choose $h_2 = h_1$, then $H \supset h_1 h_1^{-1} = e$.
- Let $h_1 = e, h_2 = h$. Then $eh^{-1} = h^{-1} \in H$.
- $h_1 h_2 = h_1(h_2^{-1})^{-1}$.

😆

Example 1.2.4 (Quarternion Units)
Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. These function such that $i^2 = j^2 = k^2 = ijk = -1$. All the two element subgroups are $\{\pm 1\}$.

Definition 1.2.6: Cyclic Subgroup

Given $a \in G$, the *cyclic subgroup generated by* a, denoted $\langle a \rangle$, is the set $\{a^n : n \in \mathbb{Z}\}$. The element a is called the *generator*.

Example 1.2.5 (Cylic Subgroups)

- $\mathbb{Z} = \langle 1 \rangle$
- $\mathbb{Z}_7 = \langle 1 \rangle, \langle 5 \rangle$
- $\mathbb{Z}_{10} = \langle 1 \rangle, \langle 7 \rangle$

Proposition 1.2.1
Every subgroup of $\mathbb{Z}$ is cyclic.

Addendum: Any subgroup of any cyclic subgroup is itself cyclic. ☺

Note:
Some $U(n)$ groups are cyclic while others are not. They are cyclic if n has primitive roots.

Lenma 1.2.2
Let $a \in G$, order of $a = n$. Then order of $a^k = \frac{n}{\gcd(a,k)}$

Proof: Let $b = a^k$. Order is the smallest number we can find such that $b^s = e$. Note that $b^s = a^{ks}$, so we need $n|ks$. Let $d = \gcd(n,k)$. Then $n = dn'$ and $k = dk'$. Then we need dn' to be a divisor of sdk'. So, $n'|sk'$. Since n' and k' are coprime, $n'|s$. Therefore, the smallest possible s is $n' = n/\gcd(a,k)$. ☺

Theorem 1.2.5
A group has no proper nontrivial subgroups is and only if it is a cyclic group of prime order.

Proof: Let $G = \langle a \rangle$ for any $a \in G$. What is the oder of a? If a isn't prime, $a = xy$ and $y \neq 1$. Then a^x has order y. ☺