Math 3121, A Summary of Sections 0,1,2,4,5,6,7,8,9

Section 0. Sets and Relations

Basic concepts

Subset of a set, $B \subseteq A$, $B \subset A$ (Definition 0.1). Cartesian product of sets $A \times B$ (Defintion 0.4). Relation (Defintion 0.7). Function, map, mapping (all the three words have the same meaning) (Definition 0.10). One-to-one, onto (Definition 0.12). Cardinality (Definition 0.13). Partition (Definition 0.16). Equivalence relation (Definition 0.18).

Theorems

Theorem 0.22. Each equivalence relation on a set S gives a partition of the set S. Conversely, each partition of S gives an equivalence relation on S. (the concepts "euqivalence" and "partition" are essentially same).

Conventions. $\mathbb{Z}$ = the set of integers, $\mathbb{Q}$ = the set of rational numbers, $\mathbb{R}$ = the set of real numbers, $\mathbb{C}$ = the set of complex numbers.

Problem

(1). If A and B are finite sets with $|A| = m$ and $|B| = n$, find $|A \times B|$.
(2). If A and B are finite sets with $|A| = m$ and $|B| = n$, and denote $\mathrm{Map}(A, B)$ the set of all maps from A to B, find $|\mathrm{Map}(A, B)|$.
(3). If A, B are finte sets, and there exists a map $f : A \to B$ which is onto (one-to-one, repectively), what can you say about the relation of $|A|$ and $|B|$?

Section 1 and Section 2

Basic concepts

Each complex number can be written as

$$a + bi$$

where a, b are real numbers. Examples of complex numbers $2+5i, 2-4i$, 5 ($a=5, b=0$), $31i$ ($a=0, b=31$).
Addition (the rule is that we add the real parts and imginary parts respectively):

$$(a+bi)+(a'+b'i) = (a+a')+(b+b')i.$$

Multiplication (the rule is that we use the the disributive law and $i^2=-1$):

$$(a+bi)(c+di) = a(c+di)+bi(c+di) = ac+adi+bci+bdi^2 = (ac-bd)+(bc+ad)i.$$

Euler's formula $e^{i\theta} = \cos\theta + \sin\theta$, $e^{i(\theta_1+\theta_2)} = e^{i\theta_1}e^{i\theta_2}$ (page 13). n-th roots of unity,
$U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ (page 18).

Definition 2.1 A **binary operation** $*$ on a set S is a map from $S \times S$ to S. For each $(a,b) \in S \times S$, we will denote its image by $a * b$.

The usual addition on $\mathbb{R}$ is a binary operation. The addition $+$ is a assigns each element $(a,b) \in \mathbb{R} \times \mathbb{R}$ an element $a+b \in \mathbb{R}$.

A binary operation $*$ on S is called a **commutative binary operation** if $a*b = b*a$ for all $a, b \in S$ (Definition 2.11).
A binary operation $*$ on S is called an **associative binary operation** if $(a*b)*c = a*(b*c)$ for all $a, b, c \in S$ (Definition 2.13).

Let S be a set, let $Map(S,S)$ be the set of all maps from S to S itself. Because for two maps $f, g : S \to S$, we may take their composition $f \circ g$ ($f \circ g$ maps each $a \in S$ to $f(g(a))$), so the composition $\circ$ is a binary operation on $Map(S,S)$). The composition is associative (Theorem 2.13).

Problems

(1). Suppose S is a finite set with cardinality $|S| = n$, how many binary operations on S are there? how many commutative binary operations are there?

Section 4. Groups

Basic concepts

Group, identity element, inverse (Definition 4.1). Abelian group (Definition 4.3).

Important examples

$(\mathbb{Z}, +)$, the set of integers is a group under addition.
$(\mathbb{Q}, +)$, the set of rational numbers is a group under addition.
$(\mathbb{R}, +)$, the set of real numbers is a group under addition.
$(\mathbb{C}, +)$, the set of complex numbers is a group under addition.
$(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ the sets of nonzero rational numers, the set of non-zero real numbers, the set of non-zero complext numbers are groups under multiplication $\cdot$.
$GL(n, \mathbb{R})$, the set of **invertible** $n \times n$ matrices, is a group under matrix multiplication.
Every vector space is a group under the addition.

Theorems

Theorem 4.15(Cancellation Law). If G is a group with binary operation $*$. Then $a * b = a * c$ implies $b = c$, and $b * a = c * a$ implies $b = c$.
Corollary 4.18

Problems

Suppose a group $(G, *)$ has exactly three elements e, a, b with e as the identity element. Prove that $a * b = b * a = e, a * a = b, b * b = a$,

Section 5. Subgroups

Conventions

When we deal with a unspecified group G, we always denote the binary operation by $*$, and we often write $a * b$ as ab, $a * \cdots * a$ (n copies of a) as a^n, the inverse of a as a^{-1}, $a^{-1} * \cdots * a^{-1}$ (n copies of a^{-1}) as a^{-n}, and a^0 means the identity element e. We state general theorems about groups using the above conventions.

Basic concepts

Order $|G|$ of a group G (Definition 5.3). Subgroup (Definition 5.4). Cyclic subgroup generated by a (Definition 5.18). Cyclic group (Definition 5.19).

Theorems

Theorem 5.14. A subset H of a group G is a subgroup if and only if
1. H is closed under the binary operation of G,
2. the identity element e of G is in H.
3. for all $a \in H$, it is true that $a^{-1} \in H$ also.

Theorem 5.17. Let G be a group and let $a \in G$. Then $H = \{a^n \,|\, n \in \mathbb{Z}\}$ is a subgroup of G and is the smallest subgroup of G that contains a, that is,every subgroup containing a contains H.

Important example

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, each $\subset$ gives a subgroup relation.
$\mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$, each $\subset$ gives a subgroup relation.
For each positive integer $U_n = \{z \,|\, z^n = 1\}$ is a subgroup of $\mathbb{C}^*$.
$2 \in \mathbb{R}^*$, the cyclic subgroup of $\mathbb{R}^*$ generated by 2 is $\{2^n \,|\, n \in \mathbb{Z}\}$.
$2 \in \mathbb{R}$, the cyclic subgroup of $\mathbb{R}^*$ generated by 2 is $\{2n \,|\, n \in \mathbb{Z}\}$.

Problem (1). Claim: $\mathbb{R}^*$ is a subgroup of $\mathbb{C}$ because (1) both $\mathbb{R}^*$ and $\mathbb{C}$ are groups; (2) $\mathbb{R}^*$ is a subset of $\mathbb{C}$. What is wrong about the above argument?
(2). Let G be a finite group, suppose H is a non-empty subset of G that is closed under the binary operation of G. Prove that H is a subgroup of G.

Section 6. Cyclic Groups

Basic concepts

A group G is called a **cyclic group** if there is $a \in G$ such that $G = \langle a \rangle = \{a^n \,|\, n \in \mathbb{Z}\}$, that is, every element in G can be written as a power of a. By our convention, if the binary operation of G is $*$, G is cyclic iff there is $a \in G$ such that every element $x \in G$ is $x = a * \cdots * a$(n copies of a) or $x = e$ or $x = a' * \cdots * a'$ (n copies of a', a' is the inverse of a). Such element a is called a generator of the cyclic group G. A cyclic group may have more than 1 generators.

Let $a \in G$, the **order** of a is $|\langle a \rangle|$. The order of a is the smallest positve integer m such that $a^m = e$. If there is no positive integer m such that $a^m = e$, the order of a is infinite.
Example. $i \in \mathbb{C}^*$ has order 4, $4 \in \mathbb{C}^*$ has order infinite. $4 \in \mathbb{Z}_6$ has order 3.

Greatest common divisor (Definition 6.8). **Relatively prime**.

Important Examples

$\mathbb{Z}$ is a cyclic group, because $\langle 1 \rangle = \mathbb{Z}$.
$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ is a group under $+$ induced from $+$ in $\mathbb{Z}$, it is a cyclic group, because $\langle 1 \rangle = \mathbb{Z}_n$.
U_n is a cyclic group, because $\langle e^{\frac{2\pi i}{n}} \rangle = U_n$.

Theorems

Theorem 6.1. Every cyclic group is abelian.

Theorem 6.3. Division Algorithm. (Examples: if $m = 3, n = 20$, then $20 = 3 \cdot 6 + 2$ so $q = 6, r = 2$. If $m = 3, n = -20$, then $-20 = 3 \cdot (-7) + 1$, so $q = -7, r = 1$.

Thmorem 6.6. A subgroup of a cyclic group is cyclic.

Corollary 6.7. The subgroups of $\mathbb{Z}$ are precisely $n\mathbb{Z}$ for $n \in \mathbb{Z}$.

Problems

1. Compute the orders
(a). -1, $e^{\frac{2\pi i}{111}}$, $2006 \in \mathbb{C}^*$.
(b). 1, 2, 3, 4, 5, $6 \in \mathbb{Z}_{30}$.
2. Prove that an infinite cyclic group has exactly two generators.

Section 7. Generating Sets

Basic concepts

The intersection of a collection of sets (Definition 7.3). Subgroup generated by a subset $\{a_i \,|\, i \in I\}$, generators of G, finitely generated (Definition 7.5).

Theorems

Theorem 7.6.

Problems

1. Which of the following statements is correct?
(1). 1 generates $\mathbb{Z}$.
(2). -1 generates $\mathbb{Z}$.
(3). $\{2, 5\}$ generates $\mathbb{Z}$.
(4). $\{2, 4, 6\}$ generates $\mathbb{Z}$.
2. Prove that the $n \times n$ elementary matrices generate $GL_n(\mathbb{R})$.

Section 8. Groups of Permutations

Basic concepts

Permutation of a set (Definition 8.3). Symmetric group on n letters S_n (Definition 8.6). An element $\sigma \in S_n$ can be written as a two-row matrix with the first row always as $(1, 2, \ldots, n)$ and the i-th entry of 2nd row is $\sigma(i)$. For example,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

is the permutation of $\{1, 2, 3, 4, 5, \}$ with $\sigma(1) = 4, \sigma(2) = 2, \sigma(3) = 5, \sigma(4) = 3, \sigma(5) = 1$.

Theorems

Theorem 8.5. Let S_A be the set of all permutations of a non-empty set A. Then S_A is a group under permutation multiplication.

Problems

(1). What is order of S_n?
(2). Is S_n an abelian group?
(3). Which element in S_{10} have the largest order?

Section 9. Orbits, Cycles, and Alternating Groups

Basic concepts

Orbits of a permutation (**Definition 9.1**). Cycle, length of a cycle (**Definition 9.6**). Transposition (**Definition 9.11**). Disjoint cycles (page 89). Even and odd permutations (**Definition 9.18**). Alternating group A_n on n letters (**Definition 9.21**).
For example, $\sigma \in S_5$ given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$$

has two orbits $\{1, 2, 4\}$ and $\{3, 5\}$ (because $1 \mapsto 4 \mapsto 2 \mapsto 1;\; 3 \mapsto 5 \mapsto 3$). And σ is a product of two disjoint cycles:

$$\sigma = (1, 4, 2)(3, 5).$$

To write σ as a product of transpositions, we only need to write the cycles $(1, 4, 2)$ and $(3, 5)$ as products of transpositions: $(1, 4, 2) = (1, 2)(1, 4)$, $(3, 5)$ itself is a transposition. So

$$\sigma = (1, 2)(1, 4)(3, 5),$$

it is a product of 3 transpositions, σ is an odd permutation.

Theorems

Theorem 9.8. Every permutation $\sigma \in S_n$ is a product of disjoint cycles
Corollary 9.12. If $n \geq 2$, any $\sigma \in S_n$ is a product of transpositions.
Proof. By Theorem 9.8, σ is a product of disjoint cycles, it suffices to prove each cycle is a product of transpositions, which is proved by the following formula:

$$(a_1, a_2, \ldots a_k) = (a_1, a_k)(a_1, a_{k-1}) \ldots (a_1, a_2).$$

Theorem 9.15. No permutation in S_n can expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.
Theorem 9.20. For $n \geq 2$, $|A_n| = \frac{n!}{2}$.

Problems.

Prove that the transpositions $(12), (23), \ldots, (n-1, n)$ generate S_n.