MATH 113 Notes

Jad Damaj

Spring 2022

Contents

1 1/18/2022

1.1 What is Algebra?

High School Algebra: Solve equations (over real and complex numbers), precalculus material

Abstract Algebra: Study algebraic structures more general than the real or complex numbers

- The abstract encapsulation of our intuition for composition

Summary of first 6-7 years of math education:

- The notion of unity, eg. 1
- The natural numbers $\mathbb{N} := \{1, 2, 3, \ldots\}$ with $+, \times$
- the integers $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ with $+, \times$, additive inverses exist
- the rational numbers $\mathbb{Q} := \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$ with $+, \times$, additive and multiplicative inverses exist
- $\mathbb{R}$, real numbers
- $\mathbb{C}$, complex numbers

Adding structure at each step: $(\mathbb{Z}, +)$- Group, $(\mathbb{Z}, +, \times)$-Ring, $(\mathbb{Q}, +, \times)$-Field

Goal of this class: define larger class of objects like this

1.2 Set Theory

Definition 1.1. A set is a collection of elements
Ex: Numbers, symbols shapes, turkeys

Notation: P, Q are two statements

- $P \to Q$ means if P is true then Q is true, "P implies Q"
- $P \leftrightarrow Q$ "P is true if and only if Q is true"
- $\forall$ "for all"
- $\exists$ "there exists", $\exists!$ "there exists unique"

Let S and T be two sets

- if s is an object in S we say s is an element of S or a member of S. Write $s \in S$ if s is in S, $s \notin S$ if s is not in S

- If S has finitely many elements we say it is a finite set. $|S| = \#$ of elements in S (cardinality)

Set notation:

- $S = \{$Notation for elements in $S|$ properties specifying being in $S\}$
  Ex: $\{x \in \mathbb{Z} | 2 \text{ divides } x\}$, $\{1, 2, 3, \dots, \}$, $\{1, 2, 3\}$
- If every object in S is also an object in T we say "S is contained in T ", $S \subset T$. If S is not contained in T, $S \not\subset T$
- If $S \subset T$ and $T \subset S$, then $S = T$
- The set of objects contained in both S and T is called the intersection, $S \cap T$
- The set of objects contained in either S or T is called the union, $S \cup T$. (If S and T are disjoint $S \sqcup T$)
- $S \times T = \{(a, b) | a \in S, b \in T\}$ - Cartesian product of S and T
- The set that contains no objects is called the empty set, $\emptyset$

1.3 Maps/Functions

- $f : A \to B$ or $A \xrightarrow[f]{B}$ is a map or function. The value of f at a is denoted $f(a)$
- If specifying a function on elements, $f : a \mapsto b$ or $a \mapsto b$
- A is called the domain of f. B is called the codomain of f.
  Ex: $S = \mathbb{N}, T = \mathbb{N} \quad f : \mathbb{N} \to \mathbb{N} \quad a \mapsto a^2$
- We say f is well defined if $a_1 = a_2 \to f(a_1) = f(a_2)$ $\forall a_1, a_2 \in A$
- The set $f(A) = \{b \in B | b = f(a) \text{ for some } a \in A\}$ is a subset of B called the range or image of f
- The set $f^{-1}(C) = \{a \in A | f(a) \in C\}$ is called the preimage of C under f $(C \subset B)$
- We say f is injective if $f(x) = f(y) \to x = y$ $\forall x, y \in A$
- We say f is surjective if given $b \in B$ $\exists a \in A$ such that $f(a) = b$
- We say f is bijective if it is both injective and surjective
- We say that f is the identity map if $A = B$ and $f(a) = a$ $\forall a \in A$. In this case we write $f = \mathrm{Id}_A$
- if $f : A \to B$ and $g : B \to C$, the composite map $f\dot{g} : A \to C$ is defined by $(g\dot{f})(a) = g(f(a))$

1.4 Equivalence Relations

Let A be a nonempty set. A binary relation on as set A is a subset R of $A \times A$ and we write $a \equiv b$ if $(a, b) \in R$

We say $\sim$ is an equivalence relation if $\sim$ is:

- reflexive: $a \sim a \; \forall a \in A$
- symmetric: $a \sim b \to b \sim a \; \forall a, b \in A$
- transitive: $a \sim b$ and $b \sim c \to a \sim c \; \forall a, b, c \in A$

If $\sim$ defines an equivalence relation on A, then the equivalence class of $a \in A$ is defined to be $[a] = \{x \in A | x \sim a\}$

Example 1.2. Consider the binary relation on $\mathbb{Z} \times \mathbb{Z}$ given by $(x, y) \in R$ if $2|x - y$. We will show $\sim$ is an equivalence relation:
reflexiveness: $x - x = 0$ so $2|0 = x - x$ for all $x \in \mathbb{Z}$
symmetricness: Suppose $2|x-y$. Since $(x-y) = -(y-x)$, $2|y-x$ for all $x, y \in \mathbb{Z}$
transitivity: If $2|x - y$ and $2|y - z$ then $2|x - y + y - z$ so $2|x - z$
So $\sim$ is an equivalence relation

Remark 1.3. The reflexive property, implies that $x \in [x]$ so equivalence classes are nonempty and their union is A

What are the equivalence classes for "$x \sim y$ if and only if $2|x - y$"

$[x] = \{y \in \mathbb{Z} | 2|x - y\}$

- If x is even, $x = 2n$ for some $n \in \mathbb{Z}$ then $2|y - 2n \to y$ is even so $y = 2m$ for some $m \in \mathbb{Z}$
- If x is odd, $x = 2n + 1$ for some $n \in \mathbb{Z}$ then $2|y - 2n - 1 \to y$ is odd so $y = 2n + 1$ for some $m \in \mathbb{Z}$

Remark 1.4. The symmetric and transitive properties imply that $y \in [x]$ if and only if $[y] = [x]$ so two equivalence classes are either equal or disjoint

1.5 Properties of the Integers ($\mathbb{Z}$)

- If $a, b \in \mathbb{Z}$, $a \neq 0$ we say a divides b if there is an element $c \in \mathbb{Z}$ such that $b = ac$. Write $a|b$ (if a does not divide b, write $a \not| b$)
- If $a, b \in \mathbb{Z} \setminus \{0\}$ there is a unique positive integer d, called the greatest common divisor $\gcd(a, b)$, satisfying:
  1. $d|a$ and $d|b$
  2. If $e|a$ and $e|b$, then $e|d$

- If $a, b \in \mathbb{Z}\backslash\{0\}$ there is a unique positive integer l, called the least common divisor satisfying:
  1. $a|l$ and $b|l$
  2. If $a|m$ and $b|m$, then $l|m$

2 1/20/2022

2.1 Properties of the Integers ($\mathbb{Z}$)

The division algorithm: If $a, b \in \mathbb{Z}$ and $b \neq 0$ then there exists unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$.

- q is the quotient, r is the remainder

Example 2.1. For $a = 23, b = 7$ $23 = 7 * 3 + 2$. Here $q = 3, r = 2$

The Euclidean Algorithm: an important procedure which produces the greatest common divisor of two integers a and b by iterating the division algorithm.

If $a, b \in \mathbb{Z} \setminus \{0\}$, we obtain $a = q_0 b + r_0$, $b = q_1 r_0 + r_1$, $r_0 = q_2 r_1 + r_2$, ..., $r_{n-2} = q_n r_{n-1} + r_n$, $r_{n-1} = q_{n+1} r_n$ where r_n is the last nonzero remainder, $r_n = \gcd(a, b)$

Because of division algorithm, $|b| > |r_0| > |r_1| > \cdots > |r_n|$ is a deceasing sequence of strictly positive integers so this cannot continue indefinitely, so r_n exists.

Why is $r_n = \gcd(a, b)$?
Claim: $\gcd(a, b) = \gcd(b, r_0)$

Proof. $r_0 = a - q_0 b$ so if $d|b$ and $d|a$, $d|a - q_0 b = r_0$
Also $r_0 + q_0 b = a$ so if $d|b$ and $d|r_0$, $d|r_0 + q_0 b = a$ □

Iterate this to get $r_n = \gcd(r_{n=1}, r_n) = \cdots = \gcd(a, b)$

Example 2.2. Calculate $\gcd(35, 20)$
$25 = 20 \cdot 1 + 5$, $20 = 15 \cdot 1 + 5$, $15 = 5 \cdot 3 + 0$ so $\gcd(35, 20) = \gcd(15, 5) = 3$

Theorem 2.3. Given any $a, b \in \mathbb{Z}$, $\exists u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a, b)$.

Proof. Work backwards through Euclidean Algorithm □

Example 2.4. Write gcd from example 2 in terms of 20 and 35.
$20 = 15 \cdot 1 + 5$ so $5 = 20 - 15 \cdot 1$
$15 = 35 - 20 \cdot 1$ so $5 = 20 - (35 - 20)$ so $5 = 20 \cdot 2 - 35 \cdot 1$

2.2 Primes

Definition 2.5. An integer $p > 1$ is prime if its only positive divisors are 1 and p itself

Lemma 2.6. Euclid's Lemma $a, b \in \mathbb{Z}, p$ is primes. If $p|ab$ then $p|a$ or $p|b$.

Remark 2.7. Primality is important. $15|3 \cdot 5$ but $15 \not| 3, 15 \not| 5$

Proof. If $p \not| a$ then $\gcd(p, a) = 1$, thus there exists $u, v \in \mathbb{Z}$ such that $au + pv = 1$ but then $b = b(au + pv) = bau = bpv$. By assumption $p|ab$ so $p|bau$ and $p|p$ so $p|bpv$ so $p|bau + pbv$ so $p|b$. □

The fundamental Theorem of Arithmetic: if $n \in \mathbb{Z}, n > 1$ then n can be factored uniquely into the product of primes. In other words, there are distinct primes $p_1, \ldots, p_s$ and positive integers $d_1, \ldots, d_s$ such that $n = p_1^{d_1} p_2^{d_2} \cdots p_s^{d_s}$. Such a factorization is unique up to ordering.

Theorem 2.8. There are infinitely many primes

Proof. Suppose not, then there are finitely many primes, $p_1, \ldots, p_n$. Consider $p_1 \cdots p_n + 1$ by FTA there is a prime factorization so at least one prime divides it. Can't be $p_1, \ldots, p_r$ so must be prime not listed. □

2.3 Congruences

Fix $m \in \mathbb{N}$, by division algorithm , for $a \in \mathbb{Z}$, there exists unique q, r such that $a = qm + r$ and $0 \leq r < m$. We call r the remainder of a modulo m.

This gives a natural equivalence relation on $\mathbb{Z}$: $a \sim b \leftrightarrow a$ and b have the same remainder modulo $m \leftrightarrow m|(a - b)$

Definition 2.9. a and b are congruent modulo $m \leftrightarrow m|(a-b)$. We write $a \equiv b \mod m$.

Remark 2.10. The equivalence classes of $\mathbb{Z}$ under this relation are indexed by the possible remainders modulo m. We call these residue clasess: $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$

- We have a natural surjective map $[\ ] : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \quad a \mapsto [a]$

Definition 2.11. We define addition and multiplication on $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ by $[a] \times [b] = [a \times b]\ \forall a, b \in \mathbb{Z}$ and $[a] + [b] = [a + b]\ \forall a, b \in \mathbb{Z}$

- This doesn't depend on choice of representatives for the class

  Proof. Suppose $a_1 \equiv b_1 \mod m$, then $m|a1 - b - 1$ so $a_1 = b_1 + sm$ for $s \in \mathbb{Z}$
  Also $a_2 \equiv b_2 \mod m$ so $a_2 = b_2 + tm$ for $t \in \mathbb{Z}$
  $(a_1 + a_2) = b_1 + b_2 + (s + t)m$ so $a_1 + a_2 \equiv b_1 + b_2 \mod m$ also $a_1 a_2 = (b_1 + sm)(b_2 + tm) = b_1 b_2 + (b_1 t + b_2 s + stm)m$ so $a_1 a_2 \equiv b_1 b_2 \mod m$ □

- $[0] \in \mathbb{Z}/m\mathbb{Z}$ behaves like 0 in $\mathbb{Z} : [0] + [a] = [a]$ for $[a] \in \mathbb{Z}/m\mathbb{Z}$
- $[1] \in \mathbb{Z}\ m\mathbb{Z}$ behaves like 1 in $\mathbb{Z} : [1] \times [a] = [a]$ for $[a] \in \mathbb{Z}/m\mathbb{Z}$
  but $\underbrace{[1] + \cdots + [1]}_{m \text{ times}} = [0]$ and $[r][s] = [rs] = [m] = [0]$ for some r, s

Proposition 2.12. For every $m \in \mathbb{N}, a \in \mathbb{Z}$ the congruence $ax \equiv 1 \mod m$ has a solution in $\mathbb{Z}$ if and only if a and m are coprime.

Proof. If a and m are coprime, $\gcd(a, m) = 1$ so $\exists u, v \in \mathbb{Z}$ such that $au + mv = 1$ so $au \equiv 1 \mod m$ □

2.4 Groups

Definition 2.13. Let G be a set. A binary operation is a map of sets $* : G \times G \to G$. Write $a * b$ for $*(a, b)$ for $a, b \in G$ or ab when $*$ is clear.

Definition 2.14. A group is a set G with a binary operation $*$ such that the following hold:

1. (Associativity): $(a * b) * c = a * (b * c)\ \forall a, b, c, \in G$
2. (Identity): $\exists e \in G$ such that $a * e = e * a = a\ \forall a \in G$
3. (Inverses): Given $a \in G$, $\exists b \in G$ such that $a * b = b * a = e$

3 1/25/2022

3.1 Groups

Example 3.1.

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$ under $+$, $e = 0, [0]$, for $a \in G$, $a^{-1} = -a$
- $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$, under $\times$, $e = 1$, $a^{-1} = \frac{1}{a}$

Example 3.2 (Non-Example)**.**
$(\mathbb{Z} \setminus \{0\}, \times)$ not group since no inverses.

Example 3.3. $\mathbb{Z}/n\mathbb{Z}^\times :=$ elements in $\mathbb{Z}/n\mathbb{Z}$ that have inverses ($[a]$ such that $\gcd(a, n) = 1$). $\mathbb{Z}/n\mathbb{Z}^\times$ is a group.

Example 3.4.

- If $(A, *)$ and $(B, \Diamond)$ are groups. We can from the group $(A \times B, (*, \Diamond))$ where $A \times B = \{(a, b) | a \in A, b \in B\}$ whose operation is defined componentwise $(a_1, b_1)(*, \Diamond)(a_2, b_2) = (a_1 * a_2, b_1 \Diamond b_2)$
- The trivial group: a set with a single element e, $e * e = e$ is the definition of the binary operation. No choice but to be associative. e is the identity and its own inverse.

A set with a binary operation $*$ is called a moniod if the first two properties of a group hold (no need for inverses.)

Example 3.5. $(\mathbb{Z}, \times)$ is a monoid.

- All groups are monoids but not all monoids are groups.

Definition 3.6. A group $(G, *)$ is called abelian if it satisfies

$$a * b = b * a \, \forall a, b \in G \, (\text{commutative}).$$

Example 3.7. $(\mathbb{Z}, +)$ is an abelian group.

Example 3.8. Non Abelian group $= GL_n(\mathbb{R}) := \{M \in M_n(\mathbb{R}) | \det(M) \neq 0\}$. A square matrix has a nonzero determinant iff it is invertible so every element has an inverse under matrix multiplication. Matrix multiplication is associative and we have $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ as the identity matrix. So $\{GL_n(\mathbb{R}), \times\}$ is a group and for $n \geq 2$ is non-abelian.

Proposition 3.9. If G is a group under $*$ them,

1) The identity of G is unique.

2) For each $a \in G$, a^{-1} is uniquely determined.

3) $(a^{-1})^{-1} = a$ for all $a \in G$.

4) $(a * b)^{-1} = (b^{-1}) * (a^{-1})$.

Proof. 1) If e_1, e_2 are both identities, by axiom of identity $e_1 * e_2 = e_1$, but also $e_1 * e_2 = e_2$ so $e_1 = e_2$.

2) Assume b and c are both inverses of a. Let e be the identity of G. By inverse axiom, $a * b = e$, and $a * c = e$ so $c = c * e$ by identity axiom so $c = c*(a*b) = (c*a)*b$ by associatvity axiom so $c = e*b = b$ by identity axiom.

3) To show $(a^{-1})^{-1} = a$ we need to show that a is the inverse of a^{-1} (By (2) the inverse is unique.) Since a^{-1} is the inverse of a, we have $a * a^{-1} = a^{-1} * a = e$ but this is the same as $a^{-1} * a = a * a^{-1} = e$ so a is the inverse of a^{-1}.

4) Let $c = (a * b)^{-1}$, then $(a * b) * c = e$. By associativity, $a * (b(c) = e$. "multiply" by a^{-1} to get $a^{-1} * (a * (b * c)) = a^{-1} * e$ so by the associativity and inverse axioms $(a^{-1} * a) * (b * c) = a^{-1}$ so $e * (b * c) = a^{-1}$ so $b * c = a^{-1}$. Now, "multiply" by b^{-1} to get $b^{-1} * (b * c) = b^{-1} * a^{-1}$ so $(b^{-1} * b) * c = b^{-1} * a^{-1}$ so $e * c = b^{-1} * a^{-1}$ so $c = b^{-1} * a^{-1}$.

□

Proposition 3.10. Let G be a group and $a, b \in G$. The equality $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular,

(1) if $au = av$ then $u = v$

(2) if $ub = vb$ then $u = v$

Proof. Existence - multiply by inverses
Uniqueness - because inverses are unique □

Definition 3.11. For G a group and $x \in G$, the order of x is the smallest positive integer n such that $x^n = 1 (:= \underbrace{x * \cdots * x}_{n \text{ times}})$, where 1 is the identity of G. We denote this by $|x|$ and x is said to be of order n. If no positive power of x is 1, then $|x| = \infty$.

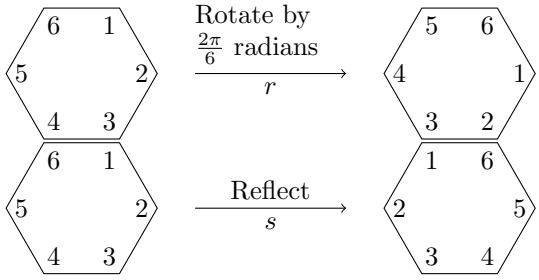
Example 3.12.

- Elements of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ (additive): All nonzero elements have order ∞.
- $(\mathbb{Z}/9\mathbb{Z}, +) = \{[0], \ldots, [8]\}$: $[6] + [6] + [6] = [18] = 0$ so $[6]$ has order 3 in $\mathbb{Z}/9\mathbb{Z}$.

3.2 Dihedral Groups

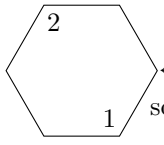
- The elements are symmetries of geometric objects
- Consider regular $n - gons$ for $n \geq 3$

Example 3.13. Symmetries of a hexagon:



- We describe these symmetries by labeling the vertices

Observe: A symmetry of a hexagon gives you a function $\{1, \ldots, 6\} \to \{1, \ldots, 6\}$. if σ is a symmetry, $\sigma(i) = j$ means σ sends i to the place where i used to be.
eg: $r(1) = 2$, $s(3) = 5$
Note that not every such function gives you a symmetry



← No way to do this without breaking the hexagon
so $\sigma(1) = 3, \sigma(2) = 6$ is not one of the symmetries

Let D_{2n} be the set of symmetries of the n-gon. Define t_1t_2 to be the symmetry reached by applying t_2 then applying t_1 for t_1, t_2 symmetries of the n-gon ($t_1, t_2 \in D_{2n}$). This operation is associative because composition of functions is associative. The identity symmetry is do nothing, denoted by 1. The inverse of a symmetry is to undo the symmetry. Under these operations, D_{2n} is the dihedral group of order $2n$.

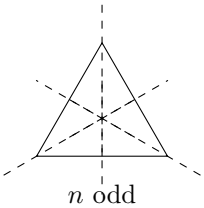
Why is $|D_{2n}| = 2n$?
For any vertex i, there is a symmetry that sends 1 to the vertex i. The vertex 2 (next to 1) must go either to the vertex $i+1$ or $i-1$. So you have n choices for where to send the vertex "1" and 2 choices for where to send to vertex "2". So there are $n \cdot 2$ choices for symmetries of an n-gon. So $|D_{2n}| = 2n$.

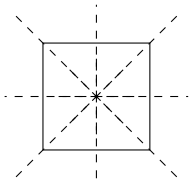
4 1/27/2022

4.1 Dihedral Groups

Explicitly, what are these symmetries?

- n rotations about the center through $2\pi/n$ radians (clockwise)
- n reflections through n lines of symmetry


n odd


n even

  - If n odd: symmetry lines pass through the vertex, midpoint of opposite side.
  - if n even: $n/2$ symmetry lines pass through opposite edges.
    $n/2$ symmetry lines pass through opposite vertices.

Fix Notation:

- r- rotation clockwise about the origin through $2\pi/n$ radians
- s- reflection (through 1 and the origin)

Example 4.1. D_{12} $\quad 2n = 12$ so $n = 6$

(i) $1, r(\frac{2\pi}{6}), r^2(\frac{4\pi}{6}), r^3(\pi), r^4(\frac{8\pi}{6}), r^5(\frac{10\pi}{6}), r^6(2\pi) = 1$
$1, r, \ldots, r^5$ all distinct so $|r| = 6$

(ii) $s^2 = 1$ so $|s| = 2$

(iii) $s \neq r^i$ for any i

(iv) $sr^i \neq sr^j$ $0 \leq i, j < 6$

(v) $r^i \neq sr^j$ for any i, j

Thus, $D_{12} = \{1, r, r^2, r^3, r^4, r^5, s, sr, sr^2, sr^3, sr^4, sr^5\}$ all distinct, and there are 12 so this is all the elements.
$D_{12} = \{r^i s^j | i = 0, \ldots, n-1\, j = 0, 1\}$ or equivalently $D_1 2 = \{r, s | r^n = s^2 = 1, rs = sr^{-1}\}$

4.2 Symmetric Groups

- Let Ω be a nonempty set and let S_Ω be the set of bijections from Ω to itself (ie. permutations.)
- Let σ, τ be elements of S_Ω, $\sigma : \Omega \to \Omega$, $\tau : \Omega \to \Omega$, then $\sigma \circ \tau$ is a bijection $\Omega \to \Omega$.
- The identity of S_Ω is the permutation 1 defined by $1(a) = a \, \forall a \in \Omega$.
- Every permutation has an inverse $\sigma^{-1} : \Omega \to \Omega$ such that $\sigma^{-1} \dot{\sigma} = \sigma \circ \sigma^{-1} = 1$.
- Composition of functions is associative so $\circ$ is associative.
- Thus, $(S_\Omega, \circ)$ is a group called the symmetric group of S_Ω
- Often we will use $\Omega = \{1, \ldots, n\}$- will write S_n instead of S_Ω

Example 4.2. $\Omega = \{1, 2, 3\}$
Let σ be in S_Ω sending $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$.
$\begin{pmatrix} \sigma : & 1 \to 2 \\ & 2 \to 3 \\ & 3 \to 1 \end{pmatrix}$ We write $(1\,2\,3)$ to represent σ.
$\tau \in S_\Omega$ by $\tau(1) = 2$, $\tau(2) = 1$, $\tau(3) = 3$
$\begin{pmatrix} \tau : & 1 \to 2 \\ & 2 \to 1 \\ & 3 \to 3 \end{pmatrix} = (1\,2)(3)$. Often we will leave out 1 element cycles and write $(1\,2)$

- A cycle is a string of integers representing an element of S_n which cyclically permutes the integers
- The length of a cycle is the number of integers that appear in it
- Two cycles are disjoint if they have no numbers in common

Example 4.3. The Group S_3

$\sigma_1(1) = 1, \sigma_1(2) = 2, \sigma_1(3) = 3$	$1 = (1)(2)(3)$
$\sigma_2(1) = 1, \sigma_2(2) = 3, \sigma_2(3) = 2$	$(2\,3)$
$\sigma_3(1) = 3, \sigma_3(2) = 2, \sigma_3(3) = 1$	$(1\,3)$
$\sigma_4(1) = 2, \sigma_4(2) = 1, \sigma_4(3) = 3$	$(1,\,2)$
$\sigma_5(1) = 2, \sigma_5(2) = 3, \sigma_5(3) = 1$	$(1\,2\,3)$
$\sigma_6(1) = 3, \sigma_6(2) = 1, \sigma_6(3) = 2$	$(1\,3\,2)$

- For any $\sigma \in S_n$ the cycle decomposition of σ^{-1} is obtained by writing the number sin each cycle of the decomposition of σ in reverse order.

Example 4.4. $\sigma = (1\,12\,8\,10\,4)(2\,13)(5\,11\,7)(6,\,9) \in S_{13}$
$\sigma^{-1} = (4\,10\,8\,12\,1)(13\,2)(7\,11\,5)(9,\,6)$

Remark 4.5. $(2\,13) = (13\,2)$ since they permute cyclically.
More generally, $(a_1\,a_2\,a_3) = (a_3\,a_1\,a_2) = (a_2\,a_3\,a_1)$
By convention, we put the smallest number first.

4.3 Composing $\sigma \circ \tau$ in S_n

- Go from right to left

Example 4.6. $(1\,2\,3) \circ (1\,2)(3\,4)$
$\tau : 1 \to 2 \quad \sigma : 2 \to 1$ so $\sigma \circ \tau : 1 \to 3$
$\tau : 3 \to 4 \quad \sigma : 4 \to 4$ so $\sigma \circ \tau : 4 \to 4$
$\tau : 4 \to 4 \quad \sigma : 3 \to 1$ so $\sigma \circ \tau : 4 \to 1$
$\tau : 2 \to 1 \quad \sigma : 1 \to 2$ so $\sigma \circ \tau : 2 \to 2$
so $\sigma \circ \tau = (1\,3\,4)$

Remark 4.7.

- S_n is non abelian for $n \geq 3$
  ex: $(1\,2) \circ (1\,3) = (1\,3\,2)$ but $(1\,3) \circ (1\,2) = (1\,2\,3)$
- The order of a permutation is the lcm of the lengths of the cycles in its decomposition
- A transposition is a cycle of length 2
- The order of S_n is $n!$