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:

- $S = \{\text{Notation for elements in } S | \text{ properties specifying being in } S\}$
  Ex: $\{x \in \mathbb{Z} | 2 \text{ divides } x\}$, $\{1, 2, 3, \ldots, \}$, $\{1, 2, 3\}$
- 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 $a, b \in \mathbb{Z}\setminus\{0\}$ 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 $a = q_0 b + r_0$, $b = q_1 r_0 + r_1$, $r_0 = q_2 r_1 + r_2$, $\ldots$, $r_{n-2} = q_n r_{n-1} + r_n$, $r_{n-1} = q_{n+1} r_n$ 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 $a_1a_2 = (b_1+sm)(b_2+tm) = b_1b_2+(b_1t+b_2s+stm)m$ so $a_1a_2 \equiv b_1b_2 \mod m$ □

- $[0] \in \mathbb{Z}/m\mathbb{Z}$ 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 $au \equiv 1 \mod m$ $\square$

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 $c = b^{-1} * a^{-1}$.

$\square$

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 $\square$

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 $|x| = \infty$.

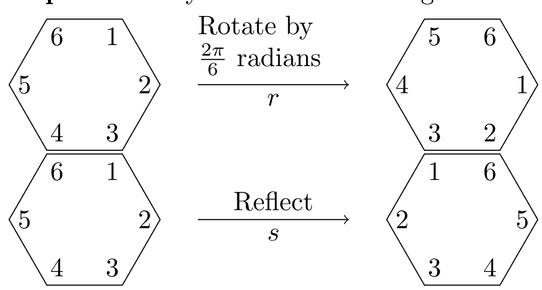
Example 3.12.

- 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

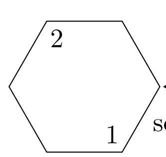
- The elements are symmetries of geometric objects
- Consider regular $n - gons$ for $n \geq 3$

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 j used to be.
eg: $r(1) = 2$, $s(3) = 5$
Note that not every such function gives you a symmetry



$\leftarrow$ 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 $t_1 t_2$ 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 $2n$.

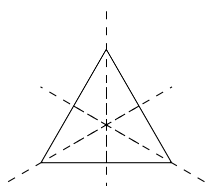
Why is $|D_{2n}| = 2n$?
For any vertex i, there is a symmetry that sends 1 to the vertex i. The vertex 2 (next to 1) must go either to the vertex $i+1$ or $i-1$. So you have n choices for where to send the vertex "$1''$" and 2 choices for where to send to vertex "$2''$". So there are $n \cdot 2$ choices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

4 1/27/2022

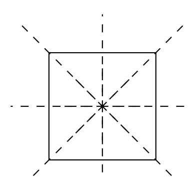
4.1 Dihedral Groups

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 $n!$

5 2/1/2022

5.1 “Maps” between groups

Definition 5.1. Let $(G, *)$ and $(H, \Diamond)$ be groups. A map $\varphi : G \to H$ such that

$$\varphi(x * y) = \varphi(x) \Diamond \varphi(Y),$$

is called a homomorphism.

Remark 5.2. When the group operations are not explicitly written

$$\underbrace{\varphi(xy)}_{\text{“multiplication”in } G} = \underbrace{\varphi(x)\varphi(y)}_{\text{“multiplication in” } H}$$

Think: a map of sets that respects the group structure (is compatible with the group operations.)

Definition 5.3. The map $\varphi : G \to H$ is called an isomorphism (G, H are isomomorphic, denoted $G \cong H$) if:

1) $\varphi(xy) = \varphi(x)\varphi(y) \quad \forall x, y \in G$

2) φ is a bijection

Definition 5.4. A homomorphism from a group to itself is called an endomorphism. Further, if an if an endomorphism is an isomorphism then it is called an automorphism.

Example 5.5.

(1) $\varphi : (\mathbb{Z}, +) \to (\mathbb{Q}, +)$ by $x \mapsto x$ is a homomorphism since $\varphi(x+y) = x+y = \varphi(x) + \varphi(y)$. It is injective but not surjective so not an isomorphism.

(2) $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}/m\mathbb{Z}, +)$ by $x \mapsto [x]$ is a homomorphism since $\varphi(x + y) = [x + y] = [x] + [y] = \varphi(x) + \varphi(y)$. It is surjective but not injective so not an isomorphism.

(3) For any group G, the identity map $\varphi : G \to G$ by $x \mapsto x$ is an isomorphism (also an automorphism.)

(4) Let $\mathbb{R} := \{x \in \mathbb{R} | x > 0\}$. The exponential map, exp: $(\mathbb{R}, +) \to (\mathbb{R}^+, \times)$ by $x \mapsto e^x$ is an isomorphism since $\exp(x+y) = e^{x+y} = e^x e^y = \exp(x)\exp(y)$. Also $\log_e e^x = x$ is an inverse.

(5) For any group G and any group H, the map $\varphi : G \to H$ by $g \mapsto e_H$ is called the trivial homomorphism since $\varphi(g_1 g_2) = e_H = e_H e_H = \varphi(g_1)\varphi(g_2)$

Proposition 5.6. Let $(G, *), (H, \circ), (M, \Box)$ be three groups. Let $f : G \to H$ and $g : H \to M$ be homomorphisms. Then $g \circ f : G \to M$ is a homomorphism.

Proof. $g(f(x * y)) = g(f(x) \circ f(y)) = g(f(x))\Box g(f(y))$ $\Box$

Proposition 5.7. If $\varphi : G \to H$ is an isomorphism,

(1) $|G| = |H|$

(2) G is abelian iff H is abelian

(3) $\forall x \in G$, $|x| = |\varphi(x)|$

Proof of (1) and (2).

(1) This is true since a bijection between two sets means they have the same cardinality.

(2) $\rightarrow$) Assume G is abelian. Let $x, y \in H$ be arbitrary. Since φ is an isomorphism, there exists $x', y' \in G$ such that $\varphi(x') = x$ and $\varphi(y') = y$. Then $xy = \varphi(x')\varphi(y') = \varphi(x'y')$. Since G is abelian $x'y' = y'x'$ so $xy = \varphi(y'x') = \varphi(y')\varphi(x') = yx$ so H is ableian.
$\leftarrow$) Assume H is abelian. Let x, y in G be arbitrary. Consider $\varphi(xy) = \varphi(x)\varphi(y)$. Since H is ableian, $\varphi(xy) = \varphi(y)\varphi(x) = \varphi(yx)$. Since φ is an isomorphism, it is injective so it follows that $xy = yx$. Thus, G is abelian.

$\square$

Lemma 5.8. Let $\varphi : G \to H$ be a homomorphism then $\varphi(x^n) = \varphi(x)^n \ \forall n \in \mathbb{Z}$.

Proof. To show this for all nonegative integers we will proceed by induction.
Basis: $\varphi(x^0) = \varphi(e_G) = e_H = \varphi(x)^0$. We will show this below.
Induction: Assume $\varphi(x^n) = \varphi(x)^n$. Then, $\varphi(x^{n+1}) = \varphi(x^n)\varphi(x) = \varphi(x)^n\varphi(x) = \varphi(x)^{n+1}$.
To show this for negative integers we claim that $\varphi(x^{-1}) = \varphi(x)^{-1}$. To see this observe that

$$\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e_G) = e_H = \varphi(e_G) = \varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x)$$

Also note that $(x^n)^{-1} = x^{-n}$ so by the above induction we have $\varphi(x^{-n})\varphi(x)^n = \varphi(x^{-n}x^n) = e_H = \varphi(x^n x^{-n}) = \varphi(x)^n\varphi(x^{-n})$ so $\varphi(x^{-n}) = (\varphi(x)^n)^{-1} = \varphi(x)^{-n}$. $\square$

Fact: If $\varphi : G \to H$ is an homomorphism, $\varphi(e_G) = e_H$.

Proof. $e_G e_G = e_G$ so $\varphi(e_G e_G) = \varphi(e_G)$ so $\varphi(e_G)\varphi(e_G) = \varphi(e_G)$. Multiplying both sides by $\varphi(e_G)^{-1}$ yields $\varphi(e_G)^{-1}\varphi(e_G)\varphi(e_G) = \varphi(e_G)^{-1}\varphi(e_G)$ so $e_H\varphi(e_G) = e_H$ so $\varphi(e_G) = e_H$. $\square$

Proof of (3). Suppose $|\varphi(x)| = \infty$, $|x| = n < \infty$, then $\varphi(x)^n = \varphi(x^n) = \varphi(e_G) = e_H$ so $|\varphi(x)| \le n < \infty$ which is a contradiction.
Similarly if $|x| = \infty$, $|\varphi(x)| = n < \infty$, then $\varphi(x^n) = \varphi(x)^n = e_H = \varphi(e_G)$. Since φ is an isomorphism, φ is injective so $x^n = e_G$ so $|x| \le n < \infty$ which is a contradiction.
This implies that $|x|$ and $|\varphi(x)|$ must both be finite or infinite. If they are both infinite we are done so suppose $|x| = n$, $|\varphi(x)| = m$.
Then $\varphi(x)^n = \varphi(x^n) = \varphi(e_G) = e_H$ so $m \le n$.
Also, $\varphi(e_G) = e_H = \varphi(x)^m = \varphi(x^m)$ so $e_H = x^m$ and $m \le n$.
Thus $m = n$ $\square$

Example 5.9.

- Consider S_3 and $\mathbb{Z}/6\mathbb{Z}$. These groups are not isomorphic since S_3 is non-abelian and $\mathbb{Z}/6\mathbb{Z}$ is.

- $D_6 \cong S_3$. $D_5 = \{r, s, | r^3 = s^2 = 1, rs = sr^{-1}\}$ so sending $a = (1\,2\,3) \mapsto r$ and $b = (1\,2) \mapsto s$, we see that $a^3 = b^2 = 1$ and $ba = a^{-1}b$ so the group generated by a and b is isomorphic to D_6. Finally, since a and b generate S_3, $S_3 \cong D_6$.

5.2 Subgroups

Definition 5.10. Let $(G, *)$ be a group. A subgroup H of G is a subset $H \subseteq G$ such that:

1. $e \in H$
2. if $x, y \in H$, $x * y \in H$
3. if $x \in H$, $x^{-1} \in H$

Think: A subgroup H of $(G, *)$ is a subset of G that is a group under the same operation.

Example 5.11.

1) $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$
2) $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$
3) $(\mathbb{Q} \setminus \{0\}, \times)$ is a subgroup of $(\mathbb{R} \setminus \{0\}, \times)$
4) If G is a group then $H = G$ and $H = \{e\}$ are both subgroups of G.
5) If $m \in \mathbb{Z}$, the subset $m\mathbb{Z} = \{ma | a \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$

6 2/3/2022

6.1 Subgroups

Example 6.1 (Non-Example)**.**

1) $(\mathbb{Z}, +)$ is not a subgroup of $(\mathbb{Z}, +)$. For $x \in \mathbb{Z}^+$, $x \notin \mathbb{Z}^+$ no inverses. Also $0 \notin \mathbb{Z}^+$ so no identity.
2) $(\mathbb{Z} \setminus \{0\}, \times)$ is not a subgroup of $(\mathbb{Q} \setminus \{0\}, \times)$ since in general $x \in \mathbb{Z} \setminus \{0\}$ but $\frac{1}{x} \notin \mathbb{Z} \setminus \{0\}$ so inverses fail.

Remark 6.2. The relation "is a subgroup of" is transitive so if $H \leq G$ and $k \leq H$, then $k \leq G$.

Proposition 6.3. Let H, K be subgroups of G, then $H \cap K \leq G$.

Proof. $e \in H$, $e \in K$ so $e \in H \cap K$. If $x \in H \cap K$, then $x^{-1} \in H, x^{-1} \in K$ so $x^{-1} \in H \cap K$. If $x, y \in H \cap K$, then $x, y \in H \cap K$, then $xy \in H$, $xy \in K$ so $xy \in H \cap K$. $\square$

Proposition 6.4 (The Subgroup Criterion)**.** A subset H of a group G is a subgroup if

1. $H \neq \emptyset$
2. if $x, y \in H$, then $xy^{-1} \in H$

Proof. If H is a subgroup then $e \in H$ so $H \neq 0$ and if $x, y \in H$, then $x, y^{-1} \in H$ so $xy^{-1} \in H$ so (1) and (2) hold.
Now, suppose (1) and (2) hold. Let $x \in H$ (we know there is such an x since $H \neq \emptyset$). Apply (2) to x so $xx^{-1} = e \in H$. Apply (2) to e and x so $ex^{-1} = x^{-1} \in H$. If $x, y \in H$, apply (2) to x and y^{-1} so $x(y^{-1})^{-1} = xy \in H$. Thus H is a subgroup. □

6.2 Centralizers, Normalizers, and Center

- An important Class of Subgroups
- Let A be a nonempty subset of G

Definition 6.5. $C_G(A) = \{g \in G | gag^{-1} = a \, \forall a \in A\}$. $C_G(A)$ is called the centralizer of A. It consists of the set of elements in G that comute with all elements of A.

- $C_G(A) \subseteq G$

Proposition 6.6. $C_G(A)$ is a subgroup of G.

Proof. $eae^{-1} = a \ \forall a in A$ so $e \in C_G(A)$.
If $x, y \in C_G(A)$, $xax^{-1} = a$ and $yay^{-1} = a \ \forall a \in A$
so $y^{-1}yay^{-1}y = y^{-1}ay$ so $a = y^{-1}ay$ so $y^{-1} \in C_G(A)$. Also, $xya(xy)^{-1} = xyax^{-1}x^{-1} = x(yay^{-1})x^{-1} = xax^{-1} = a$ so $xy \in C_G(A)$. □

Definition 6.7. $Z(G) = \{g \in G | gx = xg \, \forall x \in G\}$ is called the center of G and is the set of elements commuting with all elements of G.

Note: $Z(G) = C_G(G)$ so $Z(G) \leq G$.

Definition 6.8. $gAg^{-1} = \{gag^{-1} | a \in A\}$

Definition 6.9. $N_G(A) = \{g \in G | gag^{-1} = a\}$ is the normalizer of A in G.

Note: If $g \in C_G(A)$, $g \in N_G(A)$. Also $C_G(A) \leq N_G(A)$ and $N_G(A) \leq G$.

Example 6.10. If G is abelian, $Z(G) = C_G(A) = N_G(A) = G$ since $gag^{-1} = gg^{-1}a = a \ \forall a \in A, g \in G$.

Example 6.11. Let $G = D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$. Let $A = \{1, r, r^2, r^3\}$. Claim: $C_{D_8}(A) = A$.

Proof. $r^i r^j = r^{i+j} = r^{j+i} = r^j r^i$ so $A \subset C_{D_8}(A)$. $rs = sr^{-1} \neq sr$ so $s \notin C_{D_8}(A)$. Suppose that $sr^i \in C_{D_8}(A)$ for $i = 1, 2, 3$. Since $C_{D_8}(A)$ is a group and $r^{-i} \in C_{D_8}(A)$ so $sr^i sr^{-1} = s \in C_{D_8}(A)$ which is a contradiction. $\square$

Claim: $N_{D_8}(A) = D_8$

Proof. Note $r^i = sr^{-1}$. Since $C_{D_8}(A) \subseteq N_{D_8}(A)$, $A \subseteq N_{D_8}(A)$. $sAs^{-1} = \{s1s^{-1}, srs^{-1}, sr^2s^{-1}.sr^3s^{-1}\} = \{1, r^3, r^2, r\} = A$ so $s \in N_{D_8}(A)$. Since $N_{D_8}(A)$ is a group, $sr^i \in N_{D_8}(A)$ for $i = 1, 2, 3$ so $N_{D_8}(A) = D_8$. $\square$

Claim: $Z(D_8) = \{1, r^2\}$

Proof. $Z(D_8) \subset C_{D_8}(A) = A$ so we need to check if $\{1, r, r^2, r^3\}$ are in $Z(D_8)$. $1 \in Z(D_8)$. $rs = sr^{-1} \neq sr$ so $r \notin Z(D_8)$, also $r^3 s = sr^{-3} \neq sr^3$. $r^2 s = sr^{-2} = sr^2$ so r^2 and s commutes. Also $r^2 sr^i = sr^2 r^i = sr^i r^2$ so r^2 commutes with D_8. Thus $Z(D_8) = \{1, r^2\}$. $\square$

7 2/8/2022

7.1 Cyclic Groups

Definition 7.1. A group is cyclic if it is generated by one element. $H =< x >= \{x^n | n \in \mathbb{Z}\}$. x is called a generator for H.

Example 7.2.

1) $\mathbb{Z}$ under addition: $(\mathbb{Z}, +) =< 1 >= \{n \cdot 1 | n \in \mathbb{Z}\} =< -1 >= \{n \cdot -1 | n \in \mathbb{Z}\}$

2) $(\mathbb{Z}/m\mathbb{Z}, +) =< [1] >= \{[1], [2], \ldots, [m-1], [0]\}$

Remark 7.3. Generators need not be unique.

Cyclic groups are abelian.

Proof. if $a, b \in H =< x >$. $a = x^\alpha, y = x^\beta$ for $\alpha, \beta \in \mathbb{Z}$ so
$ab = x^\alpha x^\beta = x^{\alpha+\beta} = x^{\beta+\alpha} = x^\beta x^\alpha = ba$ $\square$

Proposition 7.4. Let $H =< x >$, then $|x| = |H|$. (the order of a group is the same as the order of its generator)

Proof. If $|x| = n$, $\{1, x, \ldots, x^{n-1}\}$ are all distinct so H has at least n elements. Suppose $x^t \in H$, then by the division algorithm $t = nq + r$ for $0 \leq r < n$. So $x^t = x^{nq+r} = (x^n)^q x^r = 1^q x^r = x^r \in \{1, x, \ldots, x^{n=1}\}$.
If $|x| = \infty$, then there is no positive integer such that $x^n = 1$. If $x^a = x^b$ for $a < b$, then $x^{b-a} = 1$ which contradicts our assumption so all x^n must be distinct. $\square$

Proposition 7.5. If $|x| = n$, $x^a = 1$ iff $n|a$.

Proof. If $x^a = 1$, and $n \not| a$, then $\gcd(n,a) = d$ for some $0 < d \leq n$. By euclidean algorithm, $\exists u, v$ such that $nu + av = d$. $x^d = x^{nu}x^{av} = (x^n)^u(x^a)^v = 1^u 1^v$ so $x^d = 1$. Thus, by the minimality of n we must have $d = n$ so $n|a$.
Suppose $n|a$, then $a = bn$ for $b \in \mathbb{Z}$ so $x^a = x^{bn} = (x^n)^b = 1^b = 1$. □

Theorem 7.6. Let G be a cyclic group.

1. If G is infinte, $G \cong (\mathbb{Z}, +)$
2. If G if finite and $|G| = m$, $G \cong (\mathbb{Z}/m\mathbb{Z}, +)$

Proof.

(1) Let $G =< x >$, $\varphi : G \to \mathbb{Z}$ by $x^n \mapsto n$
Well defined: $x^a = x^b \to a = b$ by previous proposition
Injective: $a = b \to x^a = x^b$
Surjective: By def of G, it contains all integral powers of x so for $n \in \mathbb{Z}$, take x^n.
Homomorphism: $\varphi(x^a x^b) = \varphi(x^{a+b}) = a + b = \varphi(x^a) + \varphi(x^b)$

(2) Let $|G| = m$, $G =< x >$, $\varphi G \to \mathbb{Z}/m\mathbb{Z}$ by $x^n \mapsto [n]$
Homomorphism: $\varphi(x^a x^b) = \varphi(x^{a+b}) = [a + b] = [a] + [b] = \varphi(x^a) + \varphi(x^b)$.
Well defined: WTS $x^r = x^s \to \varphi(x^s) = \varphi(x^r)$ eg. $[r] = [s]$
$x^{r-s} = 1$ so $m|r - s$ so $r - s = tm$ $t \in \mathbb{Z}$ so $\varphi(x^r) = \varphi(x^{tm+s}) = [tm+s] = [s] = \varphi(x^s)$
Surjective: $|G| = m$ so $|x| = m$ so $\{1, x, \ldots, x^{m-1}\}$ are all distinct so $G = \{1, x, \ldots, x^{m-1}\}$ and $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$. SO each element in $\mathbb{Z}/m\mathbb{Z}$ has a preimage.
Injective: WTS $[a] = [b] \to x^a = x^b$. Suppose $x^a \neq x^b$, then $x^{a-b} \neq 1$ so $m \not| a - b$ so $a \not\equiv b \mod m$ so $[a] \neq [b]$ which contradicts our assumption. Thus, they must be equal.

□

Corollary 7.7. Any two cyclic groups of the same order are isomorphic.

Proposition 7.8. Let G be a group $x \in G$, $a \in \mathbb{Z} \setminus \{0\}$. If $|x| = n < \infty$, then $|x^a| = \frac{n}{\gcd(n,a)}$.

Proof. Let $y = x^a$, $\gcd(a, n) = d$, $n = db$, $a = dc$ $b, c \in \mathbb{Z}$. Then $\gcd(b, c) = 1$.
WTS $|y| = b$ ($|x|^a = \frac{n}{\gcd(a,b)} = \frac{db}{d} = b$)
$y^b = x^{ab} = x^{dcb} = x^{nc} = (x^n)^c = 1^c = 1$ so $|y||b$.
Let $k = |y|$, we have $k|b$, WTS $b|k$. $x^{ak} = y^k = 1$ so $n|ak$ so $db|dck$ so $b|ck$.
Since $\gcd(b, c) = 1$, $b|k$. □

$\mathbb{Z}/m\mathbb{Z} = \{[0], [1] \ldots, [5]\}$ and $|[0]| = 1$, $|[1]| = |[5]| = 6$, $|[2]| = |[4]| = 3$, $|[3]| = 2$.

Consider D_{16}. Let $R = \{1, r, \ldots, r^7\}$. Observe $\langle r \rangle = R$. also $\langle r^2 \rangle \{r^2, r^4, r^6, 1\}$, $\langle r^3 \rangle = \{r^3, r^6, r^4, r^7, r^2, r^5, 1\}$. More generally, $R = \langle r \rangle = \langle r^3 \rangle = \langle r^5 \rangle = \langle r^7 \rangle$.

8 2/10/22

8.1 Cyclic Groups

Corollary 8.1. Let $H = \langle x \rangle$. Assume $|x| = n < \infty$, then $H = \langle x^a \rangle$ iff $\gcd(a, n) = 1$

- $\#$ of generators of H is $\varphi(n) = \#$ integers $< n$ relatively prime to n.

Example 8.2. $\mathbb{Z}/12\mathbb{Z} = \{[0], [1], \ldots, [11]\}$.
[1]- generator, $[2] = [1] + [1] =$ "$[1]^2$". For which a is $\gcd(a, \mathbb{Z}) = 1$?
$\varphi(12) = 4$ so $[1], [5], [7], [11]$ are generators of $\mathbb{Z}/12\mathbb{Z}$.

Theorem 8.3. If $H =< x >$ is a cyclic group

(a) Every subgroup of H is cyclic.

(b) If $|H| = n < \infty$, for each positive integer a dividing n, there is a unique subgroup of H of order a.

Proof.

(a) Let $K = \langle x \rangle$. If $K = \{1\}$ we are done.
Otherwise, let $a = \min\{k > 0$ such that $x^k \in H\}$. Claim: $K = \langle x^a \rangle$
Suppose not (suppose $\exists\ x^b \in K$ with $a \not| b$). The division algorithm gives us $bq + r$ with $0 < r < a$. Then since $x^b, x^a \in K$, $x^{b-aq} = x^r \in K$. This contradicts the minimality of a so $a|b\ \forall b$ with $x^b \in K$.

(b) $|H| = n < \infty$, $a|n$. $x^{n/a}$ has order a so $< x^{n/a} >$ has order a since $\gcd(n/a, n) = n/a$. Suppose there is another k such that $\gcd(k, n) = n/a$, then there exists u, v such that $ku + nv = n/a$ so $x^{ku} = x^{ku+nv} = x^{a/n} \in \langle x^k \rangle$. Since a/n is the smallest element with $\gcd(b, n) = a/n$, $\langle x^k \rangle = \langle x^{a/n} \rangle$.

$\square$

Example 8.4. $\mathbb{Z}/12\mathbb{Z} = \langle [1] \rangle = \langle [5] \rangle = \langle [7] \rangle = \langle [11] \rangle$ order 12
$\langle [2] \rangle = \langle [6] \rangle$ order 6, $\langle [3] \rangle = \langle [9] \rangle$ order 4, $\langle [4] \rangle = \langle [8] \rangle$ order 3, $\langle [6] \rangle$ order 2, $\langle [0] \rangle$ order 1.
Inclusion between subgroups: $\langle [a] \rangle \subseteq \langle [b] \rangle$ iff $\gcd(b, 12) | \gcd(a, 12)$.

8.2 Subgroups Generated by Subsets of a Group

- Cyclic subgroups $\{x\}$, take one element, take all possible products (close under multiplication and taking inverses)
- This is the smallest subgroup of G containing x
- Want to generalize this to the setting where your generating set has more than one element

Proposition 8.5. For any nonempty collection of subgroups of G, the intersection of all their members is also a subgroup of G.

Definition 8.6. If A is any subset of the group G,

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq H}}$$

called the subgroup of G generated by A. "intersection of all subgroups of G containing A"

- $\langle A \rangle$ is the minimal subgroup of G containing A
- Let's see a more concrete definition

Another way to define $\langle A \rangle$ is in terms of generators.

$$\overline{A} = \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} | n \in \mathbb{Z}, n \geq 0, \varepsilon_i = \pm 1\}$$

$\overline{A} = \{1\}$ of $A = \emptyset$

Proposition 8.7. $\overline{A} = \langle A \rangle$

Proof. Using the subgroup criterion we will show $\overline{A}$ is a subgroup.
$\overline{A} \neg \emptyset$ since $A = \emptyset \rightarrow \overline{A} = \{1\}$. If $a, b \in \overline{A}$. $a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}, b = b_1^{\delta_1} b_2^{\delta_2} \cdots b_m^{\delta_m}$ then $ab^{-1} = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} b_m^{-\delta_m} \cdots b_1^{-\delta_1}$ so ab^{-1} is of the form we wanted (elements of A raised to ± 1) so $\overline{A} \leq G$. Now, since $a \in A$ can be written as a^1, $A \subseteq \overline{A}$ so $\langle A \rangle \subseteq \overline{A}$ because $\langle A \rangle$ was minimal among subgroups containing A.
Now, $\langle A \rangle$ contains $\overline{A}$ because it contains A and is closed under multiplication and taking inverses. $\square$

Example 8.8. $\langle (1\,2), (1\,3)(2\,4) \rangle \leq S_4$ is isomorphic to D_8.

8.3 Quotient Groups

Definition 8.9. If $\varphi : G \rightarrow H$ is a homomorphism, the kernel of φ is the set $\ker \varphi = \{g \in G : \varphi(g) = e_H\}$. The image of φ is the set $\text{im}(\varphi) = \{\varphi(x) | x \in G\}$

Proposition 8.10. Let H, G be groups, $\varphi : G \rightarrow H$ a homomorphism, the kernel of φ is a subgroup of G and $\text{im}\varphi$ is a subgroup of H.

Proof (Kernel). Since e_G is such that $\varphi(e_G) = e_H$, $e_G \in \ker \varphi$ so $\ker \varphi \neq \emptyset$.
Now, let $x, y \in \ker \varphi$ so that $\varphi(x) = \varphi(y) = e_H$. Then $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = e_H e_H^{-1}$ so $xy^{-1} \in \ker \varphi$ so $\ker \varphi \leq G$. $\square$

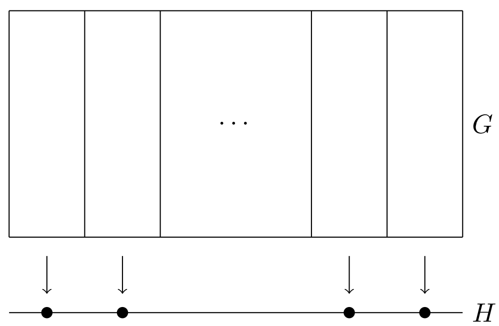
Proof (Image). $\varphi(e_G) = e_H \in \text{im}\varphi$ so $\text{im}\varphi \neq \emptyset$.
If $x, y \in \text{im}\varphi$, say $x = \varphi(a)$, $y = \varphi(b)$ $a, b \in G$ then $y^{-1} = (\varphi(b))^{-1} = \varphi(b^{-1})$, so $xy^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$ so $xy^{-1} \in \text{im}\varphi$ so $\text{im}\varphi \leq H$. $\square$

9 2/15/2022

9.1 Quotient Groups

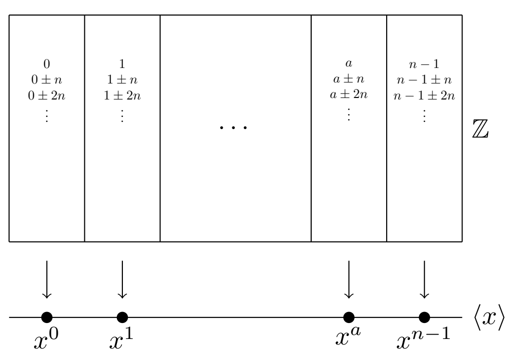
Another way to make a (smaller) group out of a given group.

Think: $H \leq G$, $H \hookrightarrow G$ (injective homomorphism), then the quotient group $G \twoheadrightarrow H$ (surjective homomorphism).



$\varphi : G \to H$ is surjective
Regions in G are fibers
of the points in H

Example 9.1. $G = \mathbb{Z}$, $H = \langle x \rangle$, $|x| = m$. $\varphi : \mathbb{Z} \to \langle x \rangle$ by $a \mapsto x^a$.
$\varphi(a + b) = x^{a+b} = x^a x^b = \varphi(a)\varphi(b)$ so homomorphism.
Can see φ is surjective since $\{n, 1, \ldots, n-1\} \to \{1, x^1, \ldots, x^{n-1}\}$
The fiber of φ over x^a: $\varphi^{-1}(a) = \{m \in \mathbb{Z} | x^m = a\} = \{m \in \mathbb{Z} | x^{m-a} = 1\} = \{m \in \mathbb{Z} | n | m - a\} = \{m \in \mathbb{Z} | m \equiv a \mod n\} = [a]$



Multiplication in $\langle x \rangle$:
$x^a x^b = x^{a+b}$. Fibers over $[a], [b], [a+b]$. Operation should be $[a] * [b] = [a+b]$.
So the group is $(\mathbb{Z}/n\mathbb{Z}, +)$.
Identity of the group is $[0]$ $(0 + n\mathbb{Z})$.
The equivalence classes are $a + n\mathbb{Z}$.

Definition 9.2. Let $\varphi : G \to H$ be a homomorphism with kernel K. Then the quotient group "G mod K" is the group whose elements are the fibers of φ. The group operation is inherited from H.

Remark 9.3. This requires knowing the map explicitly.

Proposition 9.4. Let $\varphi : G \to H$ be a homomorphism with kernel K, let $X \in G/K$ be the fiber above $a \in H$ ($X = \varphi^{-1}(a)$). For any $u \in X$, $X = \{uk|k \in K\}$ ($X = \{ku|k \in K\}$).

Proof. Let $u \in X$ be such that $\varphi(u) = a$. Let $uK = \{uk|k \in K\}$. Want to show $X = uK$. First show $uK \subseteq X$.
For $uk \in uK$, $\varphi(uk) = \varphi(u)\varphi(k) = ae = a$ so $uk \in X$.
Want to show $X \subseteq uK$. Let $g \in X$, let $k \in u^{-1}g$. $\varphi(k) = \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}a = a^{-1}a = e$ so $k \in \ker\varphi$. Since $k = u^{-1}g$, $g = uk \in uK$. □

Definition 9.5. For any $N \leq G$ and $g \in G$, $gN = \{gn|n \in N\}$ is called the left coset of N in G. ($Ng = \{ng|n \in N\}$ is called the right coset of N in G)

The proposition says the fibers of a homomorphism are cosets of the kernel.
$X \in G/K \to X = gK$.
We can define multiplication by choosing coset representatives.

Theorem 9.6. $\varphi : G \to H$ is a homomorphism with kernel K. The set of cosets of K in G (gK) with the operation $uKvK = uvK$ forms a group (the quotient group G/K).

Multiplication does not depend on representative.

Proof. Let $X, Y \in G/K$, $Z = XY \in G/K$. $X = \varphi^{-1}(a), Y = \varphi^{-1}(b)$ for some $a, b \in H$. Then $Z = \varphi^{-1}(ab)$. Let u, v be representatives of X and Y. Want to show $uv \in Z$. $\varphi(u) = a, \varphi(v) = b$, $X = uK, Y = vK$ so $uv \in Z \iff uv \in \varphi^{-1}(ab) \iff \varphi(uv) = ab \iff \varphi(u)\varphi(v) = ab$. Last statement is true so $uv \in Z$, $Z = uvK$. □

Question: Can you define a quotient group G/N for any subgroup N in this way?
A: No.

10 2/17/2022

10.1 Quotient Groups

Two views of quotient groups:

- Fibers of homomorphism with group structure seen in target space
- Cosets of the kernel of $\varphi : G \to H$ uK, vK with $uKvK = uvK$

Can we generalize quotient groups to any subgroup N?

Claim: If $\varphi : G \to H$ is a homomorphism with kernel K then $gKg^{-1} \subseteq K$ $\forall g \in G$.

Proof. WTS $\varphi(gkg^{-1}) = e$ $\forall k \in K$, $\forall g \in G$.
Observe $\varphi(gKg^{-1}) = \varphi(g)e\varphi(g^{-1}) = \varphi(g)e\varphi(g)^{-1} = e$ □

If we have a subgroup N of G such that $gNg^{-1} \subseteq N \ \forall g \in G$ then we can show multiplication of G/N is well defined (doesn't depend on representative)
eg. If $x_1N = x_2, y_1N = y_2N$, then $x_1y_1N = x_2y_2N$

Proof. We know $x_1^{-1}x_2$, $y_1^{-1}y_2 \in N$. Let $u = (x_1y_1)^{-1}(x_2y_2) = y_1^{-1}x_2^{-1}x_2y_2$. $uy_2^{-1}y_1 = y_1^{-1}x_1x_2y_1$ and since $y_1 \in G$, $gNg^{-1} \subseteq N$ then $ux_1^{-1}x \in N$. Since $y_2^{-1}, y_1 \in N$, $uy_2^{-1}y_1y_1^{-1}y_2 = u \in N$ so $x_1y_1N = x_2y_2N$. $\square$

Definition 10.1. A subgroup $N \leq G$ is called normal if for all $g \in G$, $gNg^{-1} = \{gng^{-1} | n \in N\} = N$. We write $H \trianglelefteq G$.

Claim: If $gNg^{-1} \subseteq N \ \forall g \in G$, then $gNg^{-1} = N$

Proof. WTS: $N \subseteq gNg^{-1}$. Let $n \in N$ be arbitrary. Since by assumption $g^{-1}ng \in N$, we see that $g(g^{-1}ng)g^{-1} = n$ is an element of $gNg6{-}1$, as desired. $\square$

Remark 10.2.

(a) Same as saying every element of G normalizes N. ($N_G(N) = G$)

(b) We are not saying $gng^{-1} = n$, just that $gng^{-1} \in N$

(c) If G is abelian, every subgroup of G is normal (because $gng^{-1} = n \forall g, n \in G$)

Claim from before implies that for $\varphi : G \to H$, $\ker(\varphi) \trianglelefteq G$.

Any normal subgroup can be realized as the kernel of a homomorphism.

Proposition 10.3. For $H \trianglelefteq G$, the map $\varphi : G \to G/H$ by $x \mapsto xH$ is a homomorphism with $\ker(\varphi) = H$.

Proof. $\varphi(xy) = xyH = xHyH = \varphi(x)\varphi(y)$ so φ is a homomorphism.
The identity of G/H is H. If $x \in \ker(\varphi)$, $\varphi(x) = xH = H \iff x \in H$ so $\ker\varphi = H$. $\square$

Remark 10.4. 3 perspectives on quotient groups:

- Groups of fibers of a homomorphism.
- Groups of cosets of a normal subgroup.
- Image of a surjective homomorphism (the image of the quotient map)

Theorem 10.5 (Lagrange)**.** If G is a finite group and H is a subgroup of G. then $|H| \mid |G|$ and the number of cosets of H in G is $\frac{|G|}{|H|}$.

Proof. Let $|H| = n$, let the number of cosets of H in G be k. The set of cosets partitions G and the map $H \to gH$ by $h \mapsto gh$ is a bijection so $|H| = |gH| = n$. Thus, $|G| = nk$ so $|H| \mid |G|$ and $k = \frac{|G|}{n} = \frac{|G|}{|H|}$. $\square$

Definition 10.6. The number of cosets if H in G is called the index of H in G, $[G : H]$.

Corollary 10.7. If G is a finite group and $x \in G$, then $|x| \mid |G|$ and $x^{|G|} = 1$.

Proof. $|x| = |\langle x \rangle|$. Since $|\langle x \rangle|$ is a subgroup of G, by Lagrange, $|\langle x \rangle| \mid |G|$ so $|x| \mid |G|$. $x^{|G|} = 1$ since $x^{|a|} = 1$ iff $|x| \mid a$. $\square$

Corollary 10.8. Every group of prime order is cyclic.

Proof. Let $x \in G$, $x \neq 1$. Then $|\langle x \rangle| = |x| > 1$ and $|\langle x \rangle| \mid |G|$ so $|\langle x \rangle| = p = |G|$ so $G = \langle x \rangle$ so G is cylic. $\square$

Proposition 10.9. Every subgroup of index 2 is normal. eg. If $H \leq G$, $[G : H] = 2$, then $H \trianglelefteq G$.

Proof. Let $g \in G \setminus H$. The two left cosets of H in G are gH and $eH = H$. Similarly, the right cosets of H in G are Hg and $He = H$. So $gH = Hg$ so $gHg^{-1} = H \, \forall g \in G$ so H is normal. $\square$

Remark 10.10. The full converse of Lagrange's theorem is false, $n \mid |G|$ then G need not have a subgroup of order n.

Note: If $p \mid |G|$ then G has an element of order p.

Slyow's Thm: If $|G| = p^\alpha m$, $p \nmid m$ then G has a subgroup of order p^α.