Definitions

Tuesday, May 8, 2018 12:23 AM

Notations

- ":=" means "equals, by definition"
- $\mathbb{Z} \coloneqq \{0, \pm 1, \pm 2, \pm 3, \dots\}$ the set of integers
- $\mathbb{Q} \coloneqq \left\{\frac{a}{b} \middle| a, b \in \mathbb{Z}, b \neq 0\right\}$ the set of rational numbers
- $\mathbb{R} \coloneqq$ the set of all real numbers
- $\mathbb{C} \coloneqq \{a + bi | a, b \in \mathbb{R}, i^2 = -1\}$ the set of complex numbers
- $\mathbb{Z}_{\geq 0} \coloneqq \{a \in \mathbb{Z} | a \geq 0\}$ the set of non-negative integers
- $\mathrm{S} \setminus \{x\} \coloneqq \{s \in S | s \neq x\}$
- Denote a function f from a set A to a set B by $f: A \to B$
- Denote the image of f by $\mathrm{im}(f) \coloneqq \{b \in B | \exists a \in A \text{ s.t. } f(a) = b\}$

Injective, Surjective and Bijective

- Let $f: A \to B$ be a function, then
- f is injective if $\forall a, a' \in A, a \neq a' \Rightarrow f(a) \neq f(a')$
- f is surjective if $\forall b \in B, \exists a \in A$ s.t. $f(a) = b$ (i.e. $\mathrm{im}(f) = B$)
- f is bijective if f is both injective and surjective

Divides

- If $x, y \in \mathbb{Z}$, and $x \neq 0$
- We say x divides y and write $x|y$, if $\exists q \in \mathbb{Z}$ s.t. $xq = y$

Cartesian Product

- If A and B are sets, then the Cartesian product of A and B is
- $A \times B \coloneqq \{(a, b) | a \in \mathrm{A}, b \in \mathrm{B}\}$

Relations

- A relation on a set A is a subset R of $A \times A$
- We write $a \sim a'$ if $(a, a') \in R$

Equivalence Relations

- A relation R on A is an equivalence relation if R is
- Reflexive
  - If $a \in A$, then $a \sim a$
  - i.e. $(a, a) \in R$
- Symmetric
  - If $a \sim a'$, then $a' \sim a$

- i.e. $(a, a') \in R \Rightarrow (a', a) \in R$
- Transitive
  - If $a \sim a', a' \sim a''$, then $a \sim a''$
  - i.e. If $(a, a') \in R$ and $(a', a'') \in R$, then $(a, a'') \in R$

Greatest Common Divisor

- Let $a, b \in \mathbb{Z}$, where either $a \neq 0$ or $b \neq 0$
- A greatest common divisor of a and b is a positive integer d s.t.
  - $d|a$ and $d|b$
  - If $e \in \mathbb{Z}$ s.t. $e|a$ and $e|b$ then $e|d$
- We write the greatest common divisor of a and b, if it exists, as (a, b)
- As a convention $(0,0) \coloneqq 0$

Equivalence Class

- Let X be a set, and let $\sim$ be an equivalence relation on X
- If $x \in X$, then the equivalence class represented by x is the set
- $[x] = \{x' \in X | x \sim x'\} \subseteq X$

Integers Modulo n

- Let $n \in \mathbb{Z}_{>0}$
- The relation on $\mathbb{Z}$ given by $a \sim b \Leftrightarrow n|(a - b)$ is an equivalence relation
- The set of equivalence classes under $\sim$ is denoted as $\mathbb{Z}/n\mathbb{Z}$
- We call this set integers modulo n (or integers mod n)
- We can check that there are n elements in $\mathbb{Z}/n\mathbb{Z}$
- We use $\bar{a}$ to denote the equivalence class in $\mathbb{Z}/n\mathbb{Z}$
- Then $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$

Group

- If G is a set equipped with a binary operation
  - $G \times G \to G$
  - $(g, h) \mapsto g \cdot h$
- that satisfies
  - Associativity: $\forall g, h, k \in G, g \cdot (h \cdot k) = (g \cdot h) \cdot k$
  - Identity: $\exists 1 \in G$ s.t. $\forall g \in G, 1 \cdot g = g \cdot 1 = g$
  - Inverses: $\forall g \in G, \exists g^{-1} \in G$ s.t. $gg^{-1} = g^{-1}g = 1$
- Then we say G is a group under this operation

Abelian Group

- We say a group G is abelian, if $ab = ba, \forall a, b \in G$

Order of Group Element

- If G is a group, and $g \in G$
- The order of g is the smallest positive integer n s.t. $g^n = 1$
- If n is the order of g, write $|g| = n$
- If no such integer exists, write $|g| = \infty$
- i.e. $|g| \coloneqq \inf\{n \in \mathbb{Z}_{>0} | g^n = 1\}$

Symmetric Group

- Let $n \in \mathbb{Z}_{>0}$ be fixed
- Let $S_n \coloneqq \left\{\text{bijective functions } \{1, \dots, n\} \to \{1, \dots, n\}\right\}$
- (i.e. S_n is the set of all permutations of $\{1, \dots, n\}$)
- Then S_n is a group with operation given by function composition
- We call this group symmetric group of degree n

Cycle

- Let $n \in \mathbb{Z}_{>0}$ be fixed
- Let $a_1, \dots, a_t \in \{1, \dots, n\}$
- The element of S_n given by
    - $a_i \mapsto a_{i+1}$ for $1 \le i \le t-1$
    - $a_t \mapsto a_1$
    - $j \mapsto j$ if $j \notin \{a_1, \dots a_t\}$
- is denoted by $(a_1, a_2, \dots, a_t)$ and is called a cycle of length t

Disjoint Cycles

- Two cycles $(a_1, \dots a_t)$ and $(b_1, \dots, b_k)$ are disjoint if
- $\{a_1, \dots a_t\} \cap \{b_1, \dots, b_k\} = \emptyset$

Homomorphism

- Let G, H be groups
- A function $f: G \to H$ is a homomorphism if
    - $f(g_1 g_2) = f(g_1) f(g_2), \forall g_1, g_2 \in G$
- One says f "respects", or "preserves" the group operation

Isomorphism

- Let G, H be groups
- A homomorphism $\alpha: G \to H$ is a isomorphism if
- there is a homomorphism $\beta: H \to G$ s.t.
    - $\alpha\beta = id_H$, and
    - $\beta\alpha = id_G$
- In this case, we say G and H are isomorphic

Subgroup

- Let G be a group, and let $H \subseteq G$
- H is a subgroup if
  - $H \neq \emptyset$ (nonempty)
  - If $h, h' \in H$, then $hh' \in H$ (closed under the operation)
  - If $h \in H$, then $h^{-1} \in H$ (closed under inverse)
- If H is a subgroup of G, we write $H \leq G$

Regular n-gon

- A regular $n -$ gon is a polygon with all sides and angles equal

Symmetry

- A symmetry of a regular n-gon is a way of
  - picking up a copy of it
  - moving it around in 3d
  - setting it back down
- so that it exactly covers the original

Dihedral Groups

- $D_{2n} \coloneqq \{\text{symmetries of the } n\text{-gon}\}$ is called n-th dihedral groups

Cyclic Group

- A group G is cyclic if $\exists g \in G$ s.t. $\langle g \rangle = G$

Least Common Multiple

- Let $a, b \in \mathbb{Z}$ where one of a, b is nonzero.
- A least common multiple of a and b is a positive integer m s.t.
  - $a|m$ and $b|m$
  - If $a|m'$ and $b|m'$, then $m|m'$
- We denote the least common multiple of a and b by $[a, b]$
- Define $[0,0] \coloneqq 0$

Subgroups Generated by Subsets of a Group

- Let G be a group and $A \subseteq G$
- The subgroup generated by A is
- the intersection of every subgroup of G containing A
- $\langle A \rangle \coloneqq \bigcap_{\substack{H \leq G \\ A \subseteq H}} H$

Finitely Generated Group

- A group G is finitely generated if
- There is a finite subset A of G s.t. $\langle A \rangle = G$

Coset

- If G is a group, $H \le G$, and $g \in G$
- $gH \coloneqq \{gh | h \in H\}$ is called a left coset
- $Hg \coloneqq \{hg | h \in H\}$ is called a right coset
- An element of a coset is called a representative of the coset

Normal Subgroup

- Let G be a group, $N \le G$
- N is a normal subgroup if $gng^{-1} \in N, \forall n \in N, \forall g \in G$
- In other words, N is closed under conjugation
- If $N \le G$ is normal, we write $N \trianglelefteq G$

Quotient Group

- Let G be a group, $N \trianglelefteq G$
- The set of left costs of N is a group under the operation
    - $(g_1 N)(g_2 N) = g_1 g_2 N$
- This group is denoted as G/N (say "G mod N")
- We call this group quotient group or factor group

Index of a Subgroup

- If G is a group, and $H \le G$, then
- The index of H is the number of distinct left cosets of H in G
- Denote the index by $[G: H]$

Product of Subgroups

- Let G be a group and $H, K \le G$
- Define $HK \coloneqq \{hk | h \in H, k \in K\}$

Transposition

- Fix n to be a positive integer
- A $2-$cycle $(i\ j)$ in S_n is a transposition

Sign of Permutation ϵ (Transposition Definition)

- Let $\epsilon: S_n \to \mathbb{Z}/2\mathbb{Z}$

$$\sigma \mapsto \begin{cases} \bar{0} & \sigma \text{ is a product of even number of transposition} \\ \bar{1} & \sigma \text{ is a product of odd number of transposition} \end{cases}$$

Sign of Permutation ϵ' (Auxiliary Polynomial Definition)

- Let $\epsilon': S_n \to \mathbb{Z}/2\mathbb{Z}$

$$\sigma \mapsto \begin{cases} \bar{0} & \sigma(\Delta) = \Delta \\ \bar{1} & \sigma(\Delta) = -\Delta \end{cases}$$

- $\epsilon'(\sigma)$ is the sign of σ, often denoted as $\operatorname{sgn}\sigma$
- σ is even if $\epsilon'(\sigma) = \bar{0}$
- σ is odd if $\epsilon'(\sigma) = \bar{1}$

Alternating Group

- The alternative group, denoted as A_n is the kernel of ϵ
- That is, A_n contains of all even permutations in S_n

Group Action

- An action of G on X is a function $G \times X \to X, (g, x) \mapsto gx$ s.t.
  - $1_G x = x, \forall x \in X$
  - $g(hx) = (gh)x, \forall g, h \in G, x \in X$

Orbit and Stabilizer

- Suppose a group G acts on a set X
- Let $x \in X$
- The orbit of x, denoted $\operatorname{orb}(x)$, is $\{g \cdot x | g \in G\} \subseteq X$
- The stabilizer of x, denoted $\operatorname{stab}(x)$, is $\{g \in G | g \cdot x = x\} \subseteq G$

Centralizer

- Let G be a group, and let G act on itself by conjugation
- If $h \in G$, then $\operatorname{stab}(h) = \{g \in G | ghg^{-1} = h\} = \{g \in G | gh = hg\}$
- This set is called the centralizer of h, denoted as $C_G(h)$
- $C_G(h)$ is the set of elements in G that commute with the element h

Center

- $\bigcup_{h \in G} C_G(h) = Z(G)$ is called the center of G
- $Z(G)$ is the set of elements that commute with every element of G

Normalizer

- Let X be the set of subgroups of a group G
- Let G acts on X by $g \cdot H = gHg^{-1}$
- If $H \leq G$, then
  - $\operatorname{stab}(H) = \{g \in G | gHg^{-1} = H\} = \{g \in G | gH = Hg\}$
- This set is called the normalizer of H in G, denoted $N_G(H)$
- $N_G(H)$ is the set of elements in G that commute with the set H
- Note: $N_G(H) = G \Leftrightarrow H \trianglelefteq G$

Conjugacy Class

- If G is a group, G acts on itself by conjugation: $g \cdot h = ghg^{-1}$
- The orbits under this action are called conjugacy classes

- Denote a conjugate class represented by some element $g \in G$ by $\text{conj}(g)$

Partition

- A partition of $n \in \mathbb{Z}_{>0}$ is a way of writing n as a sum of positive integers
- Example: 3 has 3 partitions: $3, 2+1, 1+1+1$

Ring

- A ring is a set R equipped with two operations $+$ and $\cdot$ s.t.
- $(R, +)$ is an abelian group
- $\cdot$ is associative
- $\exists 1 \in R$ s.t. $1 \cdot r = r = r \cdot 1$
- Distributive property:
    - $\forall a, b, c \in R$
    - $a \cdot (b + c) = a \cdot b + a \cdot c$
    - $(a + b) \cdot c = a \cdot c + b \cdot c$

Zero-Divisor and Unit

- Let R be a ring
- A nonzero element $r \in R$ is called a zero-divisor if
    - $\exists s \in R \setminus \{0\}$ s.t. $rs = 0$ or $sr = 0$
- Assume $1 \neq 0$, $u \in R$ is called a unit if
    - $\exists v \in R$ s.t. $uv = 1 = vu$

Group of Unites

- $R^{\times} \coloneqq \{u \in R | u \text{ is a unit}\}$

Field

- A communitive ring R is called a field if
- Every nonzero element of R is a unit
- i.e. Every nonzero element of R have a multiplicative inverse

Product Ring

- Let R_1, R_2 be rings
- The product ring $R_1 \times R_2$ has the following ring structure
- For addition, it's just the product as groups
- For multiplication, $(r_1, r_2)(r_1', r_2') = (r_1 r_1', r_2 r_2')$ with identity $\left(1_{R_1}, 1_{R_2}\right)$

Integral Domain

- A communicative ring R is an integral domain (or just domain) if
- R contains no zero-divisors

Subring

- A subring of a ring R is a additive subgroup S of R s.t.
- S is closed under multiplication
- S contains 1

Polynomials over a ring

- Let R be a commutative ring
- A polynomial over R is the sum
  - $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where
  - x is a variable, and $a_i \in R$

Degree

- If $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial over R
- The degree of f, denoted $\deg(g)$, is $\sup\{n \geq 0 | a_n \neq 0\}$
- Note: $\deg(0) = -\infty$

Leading Term and Leading Coefficient

- If $\deg(f) = n \geq 0$
- The leading term of f is $a_n x^n$
- The leading coefficient of f is a_n

Polynomial ring

- Let $R[x] \coloneqq \{\text{Polynomials over a commutative ring } R\}$
- Then $R[x]$ is a commutative ring with
- ordinary addition and multiplication of polynomials

Ideal

- Let I be a subset of ring R, and let $r \in R$
- Define $rI \coloneqq \{rx | x \in I\}$
- I is a left ideal of R if
  - I is an additive subgroup of R
  - $rI = I, \forall r \in R$
- Right ideal is defined similarly
- I is an ideal if I is both a left and right ideal

Principal Ideal

- Let R is a commutative ring, and let $r \in R$, then
- $(r) \coloneqq \{ar | a \in R\}$ is called the principal ideal generated by r

Quotient Ring

- Let R be a ring
- If $I \subseteq R$ is an ideal, then the quotient group R/I is a ring with multiplication
    - $(r + I)(r' + I) = rr' + I$

- Conversely, if
  - $J \subseteq R$ is an additive subgroup
  - R/J is a ring with multiplication defined above
- Then J is an ideal

Ideal Generated by Subset

- Let R be a commutative ring
- If A is a subset of R, then the ideal generated by A is
- $(A) \coloneqq \{r_1 a_1 + \cdots + r_n a_n | n \in \mathbb{Z}_{\geq 1}, r_i \in R, a_i \in A\} \subseteq R$
- If A is finite, then we write (A) as $(a_1, \dots, a_n)$

Maximal Ideal

- An ideal M in a ring R is maximal if
- $M \neq R$, and the only ideals containing M are M and R

Prime Ideal

- Let R be a commutative ring
- An ideal $P \subsetneq R$ is prime if
- $a, b \in R$, and $ab \in P \Rightarrow a \in P$ or $b \in P$

Euclidean Domain

- Let R be a domain
- A norm on R is a function $N: R \to \mathbb{Z}_{\geq 0}$ s.t. $N(0) = 0$
- R is called a Euclidean domain if R is equipped with a norm N s.t.
- $\forall a, b \in R$ with $b \neq 0$, $\exists q, r \in R$ s.t.
  - $a = qb + r$, and
  - either $r = 0$ or $N(r) < N(b)$

Principal Ideal Domain

- A domain in which every ideal is principal is called a principal ideal domain

Propositions

Wednesday, April 4, 2018 2:18 PM

Proposition 1: Well-ordering of $\mathbb{Z}$

- Every nonempty set S of $\mathbb{Z}_{\geq 0}$ has a unique minimum element
- $\exists!\, m \in \mathrm{S}$ s.t. $m \leq s, \forall s \in \mathrm{S}$

Proposition 2: The Division Algorithm

- Let $a, b \in \mathbb{Z}$, where $b > 0$
- Then $\exists!\, q, r \in \mathbb{Z}$ s.t. $a = qb + r$, and $0 \leq r < b$

Proposition 3: Uniqueness of Greatest Common Divisor

- Let $a, b \in \mathbb{Z}$, where either $a \neq 0$ or $b \neq 0$
- Suppose $\exists d, d' \in \mathbb{Z}_{>0}$ s.t.
  (1) d and d' both divide a and b
  (2) If $e \in \mathbb{Z}$ s.t. $e|a$ and $e|b$, then $e|d$ and $e|d'$
- Then $d = d'$

Proposition 4: Lemma for Euclidean Algorithm

- Suppose $a, b \in \mathbb{Z}$, where $b \neq 0$
- Choose $q, r \in \mathbb{Z}$ s.t. $a = qb + r$, and $0 \leq r < |b|$
- If (b, r) exists, then (a, b) exists and $(a, b) = (b, r)$

Proposition 5: $(a, 0) = |a|$

- $(a, 0) = |a|, \forall a \in \mathbb{Z}$

Proposition 6: Existence of GCD

- If $a, b \in \mathbb{Z}$, then (a, b) exists

Proposition 7: Bézout's Identity

- If $a, b \in \mathbb{Z}$, then $\exists x, y \in \mathbb{Z}$ s.t. $(a, b) = ax + by$

Proposition 8: Equivalence Classes Partition the Set

- Let X be a set with equivalence relationship $\sim$
- If $x, x' \in X$, then $[x]$ and $[x']$ are either equal or disjoint

Proposition 9: Addition and Multiplication in $\mathbb{Z}/n\mathbb{Z}$

- Let $n \in \mathbb{Z}_{>0}$, and let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$
- If $\overline{a_1} = \overline{b_1}$, and $\overline{a_2} = \overline{b_2}$ in $\mathbb{Z}/n\mathbb{Z}$
- Then $\overline{a_1 + a_2} = \overline{b_1 + b_2}$, and $\overline{a_1 a_2} = \overline{b_1 b_2}$

Corollary 10: Integers Modulo n

- For $n \in \mathbb{Z}_{>0}$, $\mathbb{Z}/n\mathbb{Z}$ is a group under the operation
  - $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$
  - $(\bar{a}, \bar{b}) \mapsto \overline{a+b}$
- We will denote this operation by $+$
- So $\bar{a} + \bar{b} = \overline{a+b}$

Proposition 11: $(\mathbb{Z}/n\mathbb{Z})^{\times}$

- $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is a group with operation given by multiplication

Proposition 12: Properties of Group

- Let G be a group, then G has the following properties
- The identity of G is unique
- Each $g \in G$ has a unique inverse
- The Generalized Associative Law
- $(gh)^{-1} = h^{-1}g^{-1}, \forall g, h \in G$

Proposition 13: Cancellation Law

- Let G be a group, and let $a, b, u, v \in G$
- If $au = av$, then $u = v$
- If $ua = va$, then $u = v$

Corollary 14: Cancellation Law and Identity

- Let G be a group, and let $g, h \in G$
- If $gh = g$, then $h = 1$
- If $gh = 1$, then $h = g^{-1}$

Proposition 15: Order of Symmetric Group

- $|S_n| = n!$

Proposition 16: Isomorphism Preserves Commutativity

- Let $f: G \to H$ be an isomorphism
- G is abelian if and only if H is abelian

Proposition 16: Injective Homomorphism Preserves Order

- Let $f: G \to H$ be an injective homomorphism
- Then $\forall g \in G, |g| = |f(g)|$

Proposition 17: The Subgroup Criterion

- A subset H of a group G is a subgroup iff
- $H \neq \emptyset$ and $\forall x, y \in H, xy^{-1} \in H$

Proposition 18: Isomorphism of Cyclic Group

- Let G be a cyclic group

- If $|G| = n < \infty$, then $G \cong \mathbb{Z}/n\mathbb{Z}$
- If $|G| = \infty$, then $G \cong \mathbb{Z}$

Proposition 19: Order of g^a

- If $G = \langle g \rangle$ is cyclic, and $|G| = n < \infty$, then $|g^a| = \dfrac{n}{(a,n)}$

Theorem 20: Subgroup of Cyclic Group is Cyclic

- Let $G = \langle g \rangle$ be a cyclic group
- Then every subgroup of G is cyclic
- More precisely, if $H \leq G$, then either $H = \{1\}$ or $H = \langle g^d \rangle$, where
  - d is the smallest positive integer s.t. $g^d \in H$

Theorem 20: Subgroup of Finite Cyclic Group is Determined by Order

- Let $G = \langle g \rangle$ be a finite cyclic group of order n
- For all positive integers a dividing n, $\exists!$ subgroup $H \leq G$ of order a
- Moreover, this subgroup is $\langle g^d \rangle$, where $d = \dfrac{n}{a}$

Proposition 21: Construction of $\langle A \rangle$

- If $A \subseteq G$, then $\langle A \rangle = \left\{ a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n} \middle| n \in \mathbb{Z}_{>0}, a_i \in A, \varepsilon \in \{\pm 1\} \right\}$

Proposition 22: Properties of Coset

- Let G be a group and $H \leq G$
- If $g_1, g_2 \in G$, then $g_1 H = g_2 H \Leftrightarrow g_2^{-1} g_1 \in H$
- The relation $\sim$ on G given by $g_1 \sim g_2$ iff $g_1 \in g_2 H$ is an equivalence relation
- In particular, left/right cosets are either equal or disjoint

Proposition 23

- Let N be a subgroup of a group G
- $N \trianglelefteq G$ iff $gN = Ng, \forall g \in G$

Proposition 24: Quotient Group

- If G is a group, and $N \trianglelefteq G$, then
- the set of left costs of N, denoted as G/N (say "G mod N")
- is a group under the operation $(g_1 N)(g_2 N) = g_1 g_2 N$
- We call this group quotient group or factor group

Theorem 25: Lagrange's Theorem

- If G is finite group, and $H \leq G$, then $|G| = |H| \cdot [G:H]$
- In particular, $|H| \big| |G|$

Corollary 26: Group of Prime Order is Cyclic

- If G is a group, and $|G|$ is prime, then G is cyclic, hence, $G \cong \mathbb{Z}/p\mathbb{Z}$

Corollary 27: $g^{|G|} = 1$

- If G is a finite group, and $g \in G$, then $g^{|G|} = 1$

Corollary 28: The Fundamental Theorem of Cyclic Groups

- If G is a finite cyclic group, then there is a bijection
- {positive divisors of $|G|$} $\longleftrightarrow$ {subgroups of G}

Proposition 29: Order of Product of Subgroups

- If H, K are finite subgroups of a group G, then $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$

Proposition 30: Permutable Subgroups

- If $H, K \leq G$, then $HK \leq G$ iff $HK = KH$

Corollary 31: Product of Subgroup and Normal Subgroup

- If $H, K \leq G$, and either H or K is normal in G, then $HK \leq G$

Theorem 32: The First Isomorphism Theorem

- If $f: G \to H$ is a homomorphism, then f induces an isomorphism
  - $\bar{f}: {}^{G}/_{\ker f} \xrightarrow{\cong} \operatorname{im}(f)$
  - $\bar{f}(g \ker f) = f(g)$

Corollary 33: Order of Kernel and Image

- $[G: \ker f] = |\operatorname{im} f|$

Theorem 34: The Second Isomorphism Theorem

- Let $A, B \leq G$, and assume $B \trianglelefteq G$
- Then $A \cap B \trianglelefteq A$, and ${}^{AB}/_{B} \cong {}^{A}/_{A \cap B}$

Theorem 35: The Third Isomorphism Theorem

- Let G be a group, and $H, K \trianglelefteq G$, where $H \leq K$
- Then $K/H \trianglelefteq G/H$, and ${}^{G/H}/_{K/H} \cong G/K$

Proposition 36: Criterion for Defining Homomorphism on Quotient

- Let G, H be groups, and $N \trianglelefteq G$
- A homomorphism $\alpha: G \to H$ induces a homomorphism
  - $\bar{\alpha}: G/N \to H$ given by $gN \mapsto \alpha(g)$
- If and only if $N \leq \ker \alpha$

Theorem 37: The Correspondence Theorem

- Let G be a group, and let $N \trianglelefteq G$, then there is a bijection
- {subgroups of G/N}$\underset{F'}{\overset{F}{\rightleftarrows}}${subgroups of G containing N}

Proposition 38: Transposition Decomposition of Permutation

- Every $\sigma \in S_n$ can be written as a product of transposition

Proposition 39: ϵ' is a Group Homomorphism

- ϵ' is a group homomorphism

Proposition 40: Sign of Transposition

- Let $n \in \mathbb{Z}_{>0}$
- If $\tau \in S_n$ is transposition, then $\epsilon'(\tau) = \overline{1}$

Corollary 41: Equivalence of Two Definitions of Sign

- ϵ is well-defined, and $\epsilon = \epsilon'$

Corollary 42: Surjectivity of ϵ

- If $n \geq 2$, then ϵ is surjective

Proposition 43: Subgroup of Index 2 is Normal

- If G is a group, $H \leq G$, and $[G:H] = 2$, then $H \trianglelefteq G$

Proposition 44: Conjugate Cycle

- If $(a_1 \dots a_t), (a_1{}' \dots a_t{}')$ are t-cycles in S_n
- Then $\exists \sigma \in S_n$ s.t. $\sigma(a_1 \dots a_t)\sigma^{-1} = (a_1{}' \dots a_t{}')$

Theorem 45: A_4 Have No Subgroup of Order 6

- A_4 have no subgroup of order 6

Proposition 46: Stabilizer is a Subgroup

- If G acts on X, and $x \in X$, then $\text{stab}(x) \leq G$

Proposition 47: Orbits Equivalence

- Let G act on a set X
- The relation $x \sim x'$ iff $\exists g \in G$ s.t. $gx = x'$ is an equivalence relation on X

Proposition 48: Orbit-Stabilizer Theorem

- If G acts on X, and $x \in X$, then $|\text{orb}(x)| = [G: \text{stab}(x)]$

Proposition 49: Permutation Representation of Group Action

- Let G be a group acting on a finite set $X = \{x_1, \dots, x_n\}$
- Then each $g \in G$ determines a permutation $\sigma_g \in S_n$ by
  - $\sigma_g(i) = j \Leftrightarrow g \cdot x_i = x_j$

Proposition 49: Induced Homomorphism of Group Action

- The map $\Phi: G \to S_n$, given by $g \mapsto \sigma_g$ is a homomorphism

Theorem 50: Cayley's Theorem

- Every finite group is isomorphic to a subgroup of the symmetric group

Theorem 51: The Class Equation

- Let G be a finite group
- Let $g_1, \dots g_r \in G \setminus Z(G)$ be representatives of the conjugacy classes of G
- Then $|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)]$

Corollary 52: Center of p-Group is Non-Trivial

- If p is a prime, and P is a group of order p^α $(\alpha > 1)$, then $|Z(P)| > 1$

Corollary 53: Group of Order Prime Squared is Abelian

- If p is a prime, and P is a group of order p^2, then P is abelian.
- In fact, either $P \cong \mathbb{Z}/p^2\mathbb{Z}$ or $P \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Theorem 54: Cauchy's Theorem

- If G is a finite group, and p is a prime divisor of $|G|$, then $\exists H \leq G$ of order p

Lemma 55: Recognizing Direct Products

- Let G be a group with normal subgroups N_1, N_2
- The map $N_1 \times N_2 \xrightarrow{\alpha} G$ given by $(n_1, n_2) \mapsto n_1 n_2$ is an isomorphism
- if and only if $N_1 N_2 = G$ and $N_1 \cap N_2 = \{1\}$

Lemma 56: Coprime Decomposition of Finite Abelian Group

- Let G be a finite abelian group of order mn, where $(m, n) = 1$
- If $M = \{x \in G | x^m = 1\}, N = \{x \in G | x^n = 1\}$, then
- $M, N \leq G$ and the map $\alpha: M \times N \to G$ given by $(g, h) = gh$ is an isomorphism
- Moreover, if $m, n \neq 1$, then M and N are nontrivial

Corollary 57: p-Group Decomposition of Finite Abelian Group

- Let G be a finite abelian group, and p be a prime divisor of $|G|$
- Choose $m \in \mathbb{Z}_{>0}$ s.t. $|G| = p^m n$ and $p \nmid n$
- Then $G \cong P \times T$, where $P, T \leq G$, $|P| = p^m$, and $p \nmid |T|$

Lemma 58: Prime Decomposition of Abelian p-Group

- If G is an abelian group of order p^n, where p is a prime
- Let $a \in G$ has maximal order among all the elements of G
- Then $G \cong A \times Q$, where $A = \langle a \rangle, Q \leq G$

Theorem 59: Fundamental Theorem of Finite Abelian Groups

- Every finite abelian group G is a product of cyclic groups

Corollary 60: Number of Finite Abelian Groups of Order n

- If $n = p_1^{e_1} \cdots p_n^{e_m}$, where p_i are distinct primes
- Then the number of finite abelian groups of order n is
- $\prod_{i=1}^{m}$ number of partitions of e_i

Proposition 61: Properties of Ring

- Let R be a ring, then
- $0a = 0 = a0, \forall a \in R$
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$
- $(-a)(-b) = ab, \forall a, b \in R$
- The multiplicative identity 1 is unique
- $-a = (-1)a, \forall a \in R$

Proposition 62: Criterion for Trivial Ring

- A ring R is trivial (i.e. have only one element) iff $1 = 0$

Proposition 63: One-Sided Zero Divisor and Unit

- Let R be a ring, then
- $r \in R, s \in R \setminus \{0\}$, and $sr = 0 \nRightarrow \exists t \in R \setminus \{0\}$ s.t. $rt = 0$
- $u \in R$, and $\exists v \in R$ s.t. $uv = 1 \nRightarrow \exists w \in R$ s.t. $wu = 1$

Proposition 64: Units and Zero-Divisors of $\mathbb{Z}/n\mathbb{Z}$

- Let $n > 0$
- Every nonzero element in $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero-divisor

Proposition 65: Criterion for Product Ring to be Domain

- If R_1 and R_2 are rings, then $R_1 \times R_2$ is a domain iff
- one of the R_1 or R_2 is a domain, and the other is trivial

Proposition 66: Finite Domain is a Field

- A finite domain R is a field

Proposition 67: Polynomial Rings over a Domain

- Let R be a domain
- Let $p, q \in R[x] \setminus \{0\}$, then
- $\deg(pq) = \deg(p) + \deg(q)$
- $(R[x])^\times = R^\times$
- $R[x]$ is a domain

Proposition 68: Ideal Containing 1 is the Whole Ring

- If $I \subseteq R$ is an ideal, then $I = R \Leftrightarrow 1 \in I$

Proposition 69: Quotient Ring

- Let R be a ring
- If $I \subseteq R$ is an ideal, then the quotient group R/I is a ring with multiplication
    - $(r + I)(r' + I) = rr' + I$
- Conversely, if
    - $J \subseteq R$ is an additive subgroup
    - R/J is a ring with multiplication defined above
- Then J is an ideal

Theorem 70: The First Isomorphism Theorem for Rings

- If $f: R \to S$ is a ring homomorphism, then there is an induced isomorphism
- $\bar{f}: R/\ker f \to \mathrm{im}(f)$, given by $r + \ker f \mapsto f(r)$

Proposition 71: Criterion for Maximal Ideal

- If R is a commutative ring, and $M \subseteq R$ is an ideal
- Then M is maximal $\Longleftrightarrow$ R/M is a field

Proposition 72: Prime Ideas of $\mathbb{Z}$

- The prime ideals of $\mathbb{Z}$ are ideals of the form (n), where n is prime or $n = 0$

Proposition 73: Criterion for Prime Ideal

- Let R be a commutative ring, $P \subseteq R$ an ideal, then
- P is prime $\Leftrightarrow$ R/P is a domain
- In particular, R is a domain $\Leftrightarrow$ 0 ideal is prime

Corollary 74: Maximal Ideal is Prime

- If R is a commutative ring, and $M \subseteq R$ is maximal, then M is prime

Proposition 75: Euclidean Domain is a Principal Ideal Domain

- Every ideal in a Euclidean domain R is principal
- More precisely, if $I \subseteq R$ is an ideal, then $I = (d)$, where
- d is an element of I with minimum norm

Theorem 76: Polynomial Division

- Let F be a field
- Then $F[x]$ is a Euclidean domain
- More specifically, if $a, b \in F[x]$ where $b \neq 0$, then
- $\exists!\, q, r \in F[x]$ s.t. $a = bq + r$ and $\deg r < \deg b$

Notations, Divides, Equivalence Relations

Wednesday, January 24, 2018 9:46 AM

Notations

- ":=" means "equals, by definition"
- $\mathbb{Z} \coloneqq \{0, \pm 1, \pm 2, \pm 3, \dots\}$ the set of integers
- $\mathbb{Q} \coloneqq \left\{\frac{a}{b} \middle| a, b \in \mathbb{Z}, b \neq 0\right\}$ the set of rational numbers
- $\mathbb{R} \coloneqq$ the set of all real numbers
- $\mathbb{C} \coloneqq \{a + bi | a, b \in \mathbb{R}, i^2 = -1\}$ the set of complex numbers
- $\mathbb{Z}_{\geq 0} \coloneqq \{a \in \mathbb{Z} | a \geq 0\}$ the set of non-negative integers
- $\mathrm{S} \setminus \{x\} \coloneqq \{s \in S | s \neq x\}$
- Denote a **function** f from a set A to a set B by $f: A \to B$
- Denote the **image** of f by $\mathrm{im}(f) \coloneqq \{b \in B | \exists a \in A \text{ s.t. } f(a) = b\}$

Injective, Surjective and Bijective

- Definition
  - Let $f: A \to B$ be a function, then
  - f is **injective** if $\forall a, a' \in A, a \neq a' \Rightarrow f(a) \neq f(a')$
  - f is **surjective** if $\forall b \in B, \exists a \in A$ s.t. $f(a) = b$ (i.e. $\mathrm{im}(f) = B$)
  - f is **bijective** if f is both injective and surjective
- Example 1
  - For $f: \mathbb{Z} \to \mathbb{Z}, f(a) = 2a$
  - f is injective
    - Let $a, a' \in \mathbb{Z}$
    - Suppose $f(a) = f(a')$
    - $\Rightarrow 2a = 2a'$
    - $\Rightarrow 2a - 2a' = 0$
    - $\Rightarrow 2(a - a') = 0$
    - $\Rightarrow a - a' = 0$
    - $\Rightarrow a = a'$
    - Therefore f is injective
  - f is not surjective
    - Because the image of f does not contain any odd integers
    - $\mathrm{im}(f) = \{\text{even integer}\} \neq \mathbb{Z}$
- Example 2
  - Let $f: \mathbb{Q} \to \mathbb{Q}$ be given by $f(a) = 2a$

- f is injective
  - Let $a, a' \in \mathbb{Z}$, then
  - $f(a) = f(a') \Rightarrow 2a = 2a' \Rightarrow a = a$
- f is surjective
  - Let $b \in \mathbb{Q}$, then $\frac{b}{2} \in \mathbb{Q}$
  - $f\left(\frac{b}{2}\right) = 2\left(\frac{b}{2}\right) = b \in \mathbb{Q}$
  - Therefore f is surjective
- f is bijective
  - Because f is both injective and surjective

Divides

- Definition
  - If $x, y \in \mathbb{Z}$, and $x \neq 0$
  - We say x **divides** y and write $x|y$, if $\exists q \in \mathbb{Z}$ s.t. $xq = y$
- Examples
  - $\forall x \in \mathbb{Z}\backslash\{0\}, x|0$, since $x \cdot 0 = 0$
  - $\forall x \in \mathbb{Z}, 1|x$, since $1 \cdot x = x$
  - $\forall x \in \mathbb{Z}, -1|x$, since $(-1) \cdot (-x) = x$

Equivalence Relations

- Cartesian Product
  - If A and B are sets, then the **Cartesian product** of A and B is
  - $A \times B \coloneqq \{(a, b)|a \in A, b \in B\}$
- Relations
  - A **relation** on a set A is a subset R of $A \times A$
  - We write $a \sim a'$ if $(a, a') \in R$
- Equivalence Relations
  - A relation R on A is an **equivalence relation** if R is
  - **Reflexive**
    - If $a \in A$, then $a \sim a$
    - i.e. $(a, a) \in R$
  - **Symmetric**
    - If $a \sim a'$, then $a' \sim a$
    - i.e. $(a, a') \in R \Rightarrow (a', a) \in R$
  - **Transitive**
    - If $a \sim a', a' \sim a''$, then $a \sim a''$
    - i.e. If $(a, a') \in R$ and $(a', a'') \in R$, then $(a, a'') \in R$

- Example 1
  - Let R be a relation on set A such that $R \coloneqq \{(a,a)|a \in A\}$
  - Then R is an equivalence relation ($a{\sim}a' \Leftrightarrow a = a'$)
  - Reflexive
    - If $a \in \mathrm{A}$, then $(a,a) \in R$ by definition
  - Symmetric
    - If $a{\sim}a'$, then $a = a'$
    - Thus $a' = a$, hence $a'{\sim}a$
  - Transitive
    - If $a{\sim}a', a'{\sim}a''$ then $a = a'$ and $a = a''$
    - Thus $a = a''$, hence $a{\sim}a''$
- Example 2
  - Let n be a positive integer
  - $R \coloneqq \{(a,b) \in \mathbb{Z} \times \mathbb{Z} | n|(a-b)\}$ is an equivalence relation
  - Reflexive
    - $n|(a-a), \forall a \in \mathbb{Z}$, since $n|0$
    - It follows that $a{\sim}a, \forall a \in \mathbb{Z}$
  - Symmetric
    - Let $a, b \in \mathbb{Z}$
    - Suppose $a{\sim}b$, then $n|(a-b)$
    - Choose $q \in \mathbb{Z}$ s.t. $nq = a - b$
    - Then $n(-q) = -(a-b) = b - a$
    - Thus, $n|(b-a)$, and so $b{\sim}a$
  - Transitive
    - Suppose $a, b, c \in \mathbb{Z}$, and we have $a{\sim}b, b{\sim}c$
    - Then $n|(a-b)$ and $n|(b-c)$
    - Choose $q, q' \in \mathbb{Z}$ s.t. $nq = a - b, nq' = b - c$
    - Then $n(q + q') = (a-b) + (b-c) = a - c$
    - Thus, $n|(a-c)$, and so $a{\sim}c$

Induction, Well-Ordering of $\mathbb{Z}$

Friday, January 26, 2018 10:05 AM

Induction

- Prove $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}, \forall n \geq 1$
- Base case
  - When $n = 1, \sum_{i=1}^{i} i = 1 = \frac{1 \times 2}{2}$
- Induction step
  - For $n > 1$
  - Assume $\forall k \text{ s.t. } 1 \leq k < n, \sum_{i=1}^{k} i = \frac{k(k+1)}{2}$
  - Then $\sum_{i=1}^{n} i = \left(\sum_{i=1}^{n-1} i\right) + n = \frac{(n-1)n}{2} + n = \frac{n(n+1)}{2}$

Proposition 1: Well-Ordering of $\mathbb{Z}$

- Statement
  - Every **nonempty** subset S of $\mathbb{Z}_{\geq 0}$ has a **unique minimum element**
  - That is, $\exists! \boldsymbol{m} \in \boldsymbol{S} \textbf{ s.t. } \boldsymbol{m} \leq \boldsymbol{s}, \forall \boldsymbol{s} \in \boldsymbol{S}$
- Proof (Existence)
  - Assume S is finite
    - We argue by induction on $|S|$
    - Base case
      - When $|S| = 1$, this is clear
    - Inductive step
      - Assume $|S| > 1$
      - Choose $x \in S$, then $|S \setminus \{x\}| = |S| - 1$
      - By induction $S \setminus \{x\}$ has a minimum value: call it m
      - Case 1: $x < m$, then x is a minimum value of S
      - Case 2: $m < x$, then m is a minimum value of S
  - When S is infinite
    - Choose $x \in S$
    - Let $S' \coloneqq \{s \in S | s \leq x\}$
    - Then $|S'| \leq x + 1 < \infty$ i.e. S' is finite

        - So we can choose a minimum element of S': call it m
        - Let $s \in S$
            - If $s \in S'$, then $m \leq s$
            - If $s \notin S'$, then $m \leq x < s$
        - In either case, $m \leq s$, so m is a minimum element of S
    - This proves existence
- Proof (Uniqueness)
    - Suppose m and m' are both minimum elements of S
    - $m \leq m'$, and $m' \leq m$
    - Thus, $m = m'$
    - This proves uniqueness

Division Algorithm, Greatest Common Divisor

Monday, January 29, 2018 9:47 AM

Proposition 2: The Division Algorithm

- Statement
    - Let $a, b \in \mathbb{Z}$, where $b > 0$
    - Then $\exists!\, \boldsymbol{q}, \boldsymbol{r} \in \mathbb{Z}$ **s.t.** $\boldsymbol{a} = \boldsymbol{qb} + \boldsymbol{r}$, and $\boldsymbol{0} \leq \boldsymbol{r} < \boldsymbol{b}$
- Proof (Existence)
    - Let $S \coloneqq \{a - bq | q \in \mathbb{Z}, a - bq \geq 0\} \subseteq \mathbb{Z}_{\geq 0}$
    - S is not empty
        - Let $q \in \mathbb{Z}$ s.t. $q \leq \frac{a}{b}$
        - Then $bq \leq a$
        - $\Rightarrow 0 \leq a - bq$
        - i.e. $a - bq \in S$
    - Thus, S contains a unique minimum element: call it r
    - Choose $q \in \mathbb{Z}$ s.t.
        - $a - bq = r$
        - $\Rightarrow a = bq + r$
    - We still need to show that $0 \leq r < b$
        - Since $r \in$ S, we know $0 \leq r$
        - So we just need to show that $r < b$
        - If $r \geq b$, then $a - b(q+1) = a - bq - b = r - b \geq 0$
        - Then $a - b(q+1) \in S$, and it is less than r
        - This is impossible, since r is the minimum element of S
        - Thus, $r < b$
    - Therefore we've proven the existence of q and r
- Proof (Uniqueness)
    - Suppose $\exists q, q', r, r' \in \mathbb{Z}$ s.t.
        - $a = bq + r$, where $0 \leq r < b$
        - $a = bq' + r'$, where $0 \leq r' < b$
    - We must show that $q = q'$ and $r = r'$
    - Suppose $r \neq r'$
        - Without loss of generality, assume $r' > r$
        - Then $0 < r' - r = (a - bq') - (a - bq) = b(q - q')$
        - Thus, $b|(r' - r)$, but $0 < r' - r \leq r' < b$.
        - This is impossible, thus $r = r'$

- We have $bq + r = bq' + r \Rightarrow q = q'$
- Therefore we've proven the uniqueness of q and r

- Note we can prove the following stronger statement
  - If $a, b \in \mathbb{Z}$, and $\boldsymbol{b \neq 0}$, then $\exists!\, \boldsymbol{q}, \boldsymbol{r} \in \mathbb{Z}$ s.t.
  - $\boldsymbol{a = bq + r}$ **and** $\boldsymbol{0 \leq r < |b|}$
- Proof (Existence)
  - Assume $b < 0$
  - Choose $q, r \in \mathbb{Z}$ s.t. $a = (-b)q + r$, and $0 \leq r < -b$
  - Then $a = b(-q) + r$, and $0 \leq r < |b|$
  - This proves existence
- Proof (Uniqueness)
  - Assume $b < 0$
  - Suppose $\exists q, q', r, r' \in \mathbb{Z}$ s.t.
    - $a = bq + r$, where $0 \leq r < b$
    - $a = bq' + r'$, where $0 \leq r' < b$
  - Then
    - $a = (-b)(-q) + r$, where $0 \leq r < |b| = -b$
    - $a = (-b)(-q') + r'$, where $0 \leq r' < |b| = -b$
  - Since $-b > 0$, our previous result implies $-q = -q'$
  - Therefore $q = q'$ and $r = r'$

Greatest Common Divisor

- Let $a, b \in \mathbb{Z}$, where either $a \neq 0$ or $b \neq 0$
- A **greatest common divisor** of a and b is a **positive integer** d s.t.
  - $\boldsymbol{d|a}$ **and** $\boldsymbol{d|b}$
  - **If** $\boldsymbol{e} \in \mathbb{Z}$ **s.t.** $\boldsymbol{e|a}$ **and** $\boldsymbol{e|b}$ **then** $\boldsymbol{e|d}$
- We write the greatest common divisor of a and b, if it exists, as (a, b)
- As a convention $(0,0) \coloneqq 0$

Proposition 3: Uniqueness of Greatest Common Divisor

- Statement
  - Let $a, b \in \mathbb{Z}$, where either $a \neq 0$ or $b \neq 0$
  - Suppose $\exists d, d' \in \mathbb{Z}_{>0}$ s.t.
    (1) d and d' both divide a and b
    (2) If $e \in \mathbb{Z}$ s.t. $e|a$ and $e|b$, then $e|d$ and $e|d'$
  - Then $d = d'$
- Proof
  - Combining properties (1) and (2), we have $d|d'$ and $d'|d$

- Choose $q, q' \in \mathbb{Z}$ s.t. $dq = d'$ and $d'q' = d$
- By substitution, we get $dqq' = d$
- Then $qq' = 1 \Rightarrow q = q' = \pm 1$
- If $q = q' = -1$, then $d = -d' < 0$.
- This is impossible since d and d' are both positive
- Therefore $q = q' = 1$ and $d = d'$

Proposition 4: Lemma for Euclidean Algorithm

- Statement
  - Suppose $a, b \in \mathbb{Z}$, where $b \neq 0$
  - Choose $q, r \in \mathbb{Z}$ s.t. $\boldsymbol{a = qb + r}$, and $\boldsymbol{0 \leq r < |b|}$
  - If (b, r) exists, then (a, b) exists and $\boldsymbol{(a, b) = (b, r)}$
- Proof
  - Set $d \coloneqq (b, r)$
  - $d|a$ and $d|b$
    - Choose $q_1, q_2 \in \mathbb{Z}$ s.t. $dq_1 = b$ and $dq_2 = r$
    - Then $a = qb + r = qq_1d + q_2d = d(qq_1 + q_2)$, so $d|a$
    - And we already know $d|b$, since $(b, r)|b$
  - If $e \in \mathbb{Z}$ s.t. $e|a$ and $e|b$, then $e|d$
    - Let $e \in \mathbb{Z}$ s.t. $e|a$ and $e|b$
    - Choose $q_3, q_4 \in \mathbb{Z}$ s.t. $eq_3 = a$ and $eq_4 = b$
    - $a = qb + r$
    - $\Rightarrow a - qb = r$
    - $\Rightarrow eq_3 - qeq_4 = r$
    - $\Rightarrow e(q_3 - qq_4) = r$
    - Thus $e|r$
    - Since $e|b$ and $d = (b, r)$
    - We can conclude that $e|d$
  - By Proposition 3, $(a, b) = (b, r)$

Proposition 5: $(a, 0) = |a|$

- Statement
  - $\boldsymbol{(a, 0) = |a|, \forall a \in \mathbb{Z}}$
- Proof
  - If $a = 0$
    - This is true by our convention
  - If $a \neq 0$
    - Certainly $|a|\big|a$, and $|a|\big|0$

- If $e \in \mathbb{Z}$ s.t. $e|a$ and $e|0$, then $e\big||a|$
- Therefore $(a, 0) = |a|$

Euclidean Algorithm, Bézout's Identity

Wednesday, January 31, 2018 9:56 AM

Proposition 6: Existence of GCD

- Statement
  - If $a, b \in \mathbb{Z}$, then (a, b) exists
- Proof
  - By Proposition 5, we may assume that $b \neq 0$
  - Choose $q, r \in \mathbb{Z}$ s.t. $a = bq + r$, where $0 \leq r < |b|$
  - We argue by induction on r
  - Base case
    - Suppose $r = 0$, then $a = bq$
    - We have $|b| \big| a$ and $|b| \big| b$
    - If $e \in \mathbb{Z}$ s.t. $e|a$ and $e|b$, then $e \big| |b|$
    - Therefore (a, b) exists, and equals $|b|$
  - Inductive hypothesis
    - If $a', b' \in \mathbb{Z}$ s.t. $b' \neq 0$, and $a' = b'q' + r'$, where $0 \leq r' < r$
    - Then (a', b') exists
  - Inductive step
    - Suppose $r > 0$
    - Choose $q', r' \in \mathbb{Z}$ s.t. $b = q'r + r'$, where $0 \leq r' < r$
    - By inductive hypothesis, (b, r) exists
    - By Proposition 4, (a, b) exists, and equals (b, r)

The Euclidean Algorithm

- Input
  - $a, b \in \mathbb{Z}$ with $|b| \leq |a|$
- Output
  - (a, b)
- Algorithm

  (0) If $b = 0$, output $|a|$

  Else, proceed to step (1)

  (1) Since $b \neq 0$, we can find $q, r \in \mathbb{Z}$ s.t. $a = bq + r$, where $0 \leq r < |b|$

  (2) If $r = 0$, output $|b|$

  Otherwise, repeat step (1) with b and r playing the roles of a and b
- Note
  - The algorithm terminates

- Since the remainder decreases at each application of step (1)
- By Proposition 4, the output will be (a, b)

- Example: use the Euclidean Algorithm to compute $(4148, 2057)$
  - Take $a = 4148, b = 2057$
  - $\underbrace{4148}_{a} = \underbrace{2057}_{b} \times \underbrace{2}_{q} + \underbrace{34}_{r}$
  - $\underbrace{2057}_{a} = \underbrace{34}_{b} \times \underbrace{60}_{q} + \underbrace{17}_{r}$
  - $\underbrace{34}_{a} = \underbrace{17}_{b} \times \underbrace{2}_{q} + \underbrace{0}_{r}$
  - Here $r = 0$, so the algorithm terminates
  - Thus, $(4148, 2057) = 17$

Proposition 7: Bézout's Identity

- Statement
  - If $a, b \in \mathbb{Z}$, then $\exists x, y \in \mathbb{Z}$ s.t. $(a, b) = ax + by$
- Note
  - x, y need not to be unique
- Proof
  - If $a = b = 0$
    - We can take $x = y = 0$
    - In fact, any pair of (x, y) works
  - If $a = 0$ or $b = 0$
    - Without loss of generality, assume $b = 0$
    - Then $(a, b) = |a| = \pm a + b$
    - We can take $x = \pm 1, y = 1$
  - If $a \neq 0$ and $b \neq 0$
    - Without loss of generality, assume $|a| \geq |b|$
    - Choose $q, r \in \mathbb{Z}$ s.t. $a = qb + r$, where $0 \leq r < |b|$
    - We argue by induction on r
    - Base case
      - When $r = 0$
      - $(a, b) = |b| = 0 \cdot a + (\pm 1) \cdot b$
      - So we can take $x = 0, y = \pm 1$
    - Inductive step
      - Suppose $r > 0$
      - Choose $q', r' \in \mathbb{Z}$ s.t. $b = q'r + r'$, where $0 \leq r' < r$
      - By induction, $\exists x', y' \in \mathbb{Z}$ s.t. $(b, r) = bx' + ry'$
      - Thus, by Proposition 4

        - $(a,b) = (b,r) = bx' + ry' = bx' + (a - bq)y' = ay' + b(x' - qy')$
        - So we can take $x = y'$ and $y = x' - qy'$
- Example: Express $(4148, 2057)$ as $4148x + 2057y$ where $x, y \in \mathbb{Z}$
    - Recall when we computed $(4148, 2057)$, we had
        - $4148 = 2057 \times 2 + 34$
        - $2057 = 34 \times 60 + 17$
        - $34 = 17 \times 2 + 0$
    - Let's now find $x, y \in \mathbb{Z}$ s.t. $(4148, 2057) = 17 = 4148x + 2057y$
    - Start with the second to last equation, and "back-fill"
        - $17 = 2057 - 34 \times 60$
        - $= 2057 - (4148 - 2 \times 2057) \times 60$
        - $= 4148 \times (-60) + 2057 \times 121$
    - Therefore $x = -60, y = 121$

Equivalence Class, $\mathbb{Z}/n\mathbb{Z}$, Group

Friday, February 2, 2018 10:06 AM

Homework 1 (a): Injective Function Has a Left Inverse

- Let A and B be two nonempty sets
- Let $f: A \to B$ be a injective function
- Prove that f has a left inverse
- Since f is injective, $\forall b \in \text{im}(f), \exists!\, a \in A \text{ s.t. } f(a) = b$
- Define $g: B \to A$ in the following way
  - Choose $a_0 \in A$
  - If $b \in \text{im}(f)$
    - Choose $a \in A$ s.t. $f(a) = b$
    - Define $g(b) = a$
  - If $b \notin \text{im}(f)$
    - Define $g(b) = a_0$
- Check that g is a left inverse
  - If $a \in A, (g \circ f)(a) = g\big(f(a)\big) = a$
  - Thus, $g \circ f = id_A$

Example of The Euclidean Algorithm

- Let $a = 97, b = 20$
- Use the Euclidean Algorithm to find (a, b)
  - $97 = 20 \times 4 + 17$
  - $20 = 17 \times 1 + 3$
  - $17 = 3 \times 5 + 2$
  - $3 = 2 \times 1 + 1$
  - Therefore $(a, b) = 1$
- Find $x, y \in \mathbb{Z}$ s.t. $(a, b) = ax + by$
  - $(a, b) = 1 = 3 - 2 \times 1$
  - $= 3 - (17 - 3 \times 5) \times 1$
  - $= 3 \times 6 - 17 \times 1$
  - $= (20 - 17 \times 1) \times 6 - 17$
  - $= 20 \times 6 - 17 \times 7$
  - $= 20 \times 6 - (97 - 20 \times 4) \times 7$
  - $= 97 \times (-7) + 20 \times 34$
  - So we can take $x = -7, y = 34$

Equivalence Class

- Let X be a set, and let $\sim$ be an equivalence relation on X
- If $x \in X$, then the **equivalence class** represented by x is the set
- $[x] = \{x' \in X | x \sim x'\} \subseteq X$

Proposition 8: Equivalence Classes Partition the Set

- Statement
    - Let X be a set with equivalence relationship $\sim$
    - If $x, x' \in X$, then $[x]$ and $[x']$ are **either equal or disjoint**
- Proof
    - Suppose $\exists y \in [x] \cap [x']$
    - It suffices to show that if $z \in X$, then $x \sim z \Leftrightarrow x' \sim z$
    - $x \sim z \Rightarrow x' \sim z$
        - Suppose $x \sim z$
        - $\Rightarrow z \sim x$ (Symmetry)
        - $\Rightarrow z \sim y$ (Transitivity)
        - $\Rightarrow y \sim z$ (Symmetry)
        - $\Rightarrow x' \sim z$ (Transitivity)
    - $x \sim z \Leftarrow x' \sim z$
        - Suppose $x' \sim z$
        - $\Rightarrow z \sim x'$ (Symmetry)
        - $\Rightarrow z \sim y$ (Transitivity)
        - $\Rightarrow y \sim z$ (Symmetry)
        - $\Rightarrow x \sim z$ (Transitivity)

Integers Modulo n

- Let $n \in \mathbb{Z}_{>0}$
- The relation on $\mathbb{Z}$ given by $a \sim b \Leftrightarrow n | (a - b)$ is an equivalence relation
- The set of equivalence classes under $\sim$ is denoted as $\mathbb{Z}/n\mathbb{Z}$
- We call this set **integers modulo n** (or integers mod n)
- We can check that there are n elements in $\mathbb{Z}/n\mathbb{Z}$
- We use $\bar{a}$ to denote the equivalence class in $\mathbb{Z}/n\mathbb{Z}$
- Then $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$

Group

- Definition
    - If G is a **set** equipped with a **binary operation**
        - $G \times G \to G$
        - $(g, h) \mapsto g \cdot h$

    - that satisfies
        - **Associativity**: $\forall g, h, k \in G, g \cdot (h \cdot k) = (g \cdot h) \cdot k$
        - **Identity**: $\exists 1 \in G$ s.t. $\forall g \in G, 1 \cdot g = g \cdot 1 = g$
        - **Inverses**: $\forall g \in G, \exists g^{-1} \in G$ s.t. $gg^{-1} = g^{-1}g = 1$
    - Then we say G is a **group** under this operation
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups with operation $+$
    - If $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$ (Similarly for $\mathbb{Q}, \mathbb{R}, \mathbb{C}$)
    - $+$ is certainly associative in all 4 sets
    - 0 is the identity in each case
    - If $a \in \mathbb{Z}$ (or $\mathbb{Q}, \mathbb{R}, \mathbb{C}$), then the inverse of a is $-a$

Examples of Groups, Well-definedness, $\mathbb{Z}/n\mathbb{Z}$

Monday, February 5, 2018 9:55 AM

Examples of Groups

- Is $\mathbb{Z}$ a group under multiplication?
  - No, because there is no inverses for 2
  - Let $x \in \mathbb{Z} \setminus \{\pm 1\}$, then the multiplicative inverse of x is not an integer
- Are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ groups under multiplication?
  - No, because 0 still has no multiplicative inverse
- Multiplicative group of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
  - Let $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ and $\mathbb{R}^\times, \mathbb{C}^\times$ similarly
  - Then $\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times$ are groups with operation given by multiplication
  - We argue this for $\mathbb{Q}^\times$; the same proof works for $\mathbb{R}^\times$ and $\mathbb{C}^\times$
  - Multiplication is an operation on $\mathbb{Q}^\times$
    - If $a, b \in \mathbb{Q}^\times$, then $ab \in \mathbb{Q}^\times$
  - Associativity
    - This is clear
  - Identity
    - $1 \in \mathbb{Q}^\times$ is the identity
  - Inverses
    - $\forall a \in \mathbb{Q}^*, \dfrac{1}{a} \in \mathbb{Q}^\times$ is the inverse of a
- Is $\mathbb{Z}$ a group with operation given by subtraction?
  - No, because subtraction is not associative
  - $(1-2)-3=-4$
  - $1-(2-3)=2$
- General Linear Group
  - Let $n \in \mathbb{Z}_{>0}$
  - $GL_n(\mathbb{R}) := \{\text{invertible } n \times n \text{ matrices with entries in } \mathbb{R}\}$
  - $GL_n(\mathbb{R})$ is a group under matrix multiplication
  - Matrix multiplication is an operation on $\mathrm{GL}_n(\mathbb{R})$
    - If $A, B \in GL_n(\mathbb{R})$
    - Then, $AB \in GL_n(\mathrm{R})$, since $(AB)^{-1} = B^{-1}A^{-1}$
  - Associativity
    - This is clear
  - Identity

        - The $n \times n$ identity matrix I_n is the identity
    - Inverses
        - If $A \in GL_n(\mathbb{R})$, its inverse is A^{-1}
    - Note
        - When $n > 1$, the operation in $GL_n(\mathbb{R})$ is not commutative

Abelian Group

- We say a group G is **abelian**, if $ab = ba, \forall a, b \in G$

Proposition 9: Addition and Multiplication in $\mathbb{Z}/n\mathbb{Z}$

- Statement
    - Let $n \in \mathbb{Z}_{>0}$, and let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$
    - If $\overline{a_1} = \overline{b_1}$, and $\overline{a_2} = \overline{b_2}$ in $\mathbb{Z}/n\mathbb{Z}$
    - Then $\overline{a_1 + a_2} = \overline{b_1 + b_2}$, and $\overline{a_1 a_2} = \overline{b_1 b_2}$
- Proof: $\overline{a_1 + a_2} = \overline{b_1 + b_2}$
    - Choose $c_1, c_2 \in \mathbb{Z}$ s.t. $c_1 n = a_1 - b_1$ and $c_2 n = a_2 - b_2$
    - Then $(c_1 + c_2)n = a_1 - b_1 + a_2 - b_2 = (a_1 + a_2) - (b_1 + b_2)$
    - Thus, $n \big| \big((a_1 + a_2) - (b_1 + b_2)\big)$
    - So, $\overline{a_1 + a_2} = \overline{b_1 + b_2}$
- Proof: $\overline{a_1 a_2} = \overline{b_1 b_2}$
    - Choose $c_1, c_2 \in \mathbb{Z}$ s.t. $c_1 n = a_1 - b_1$ and $c_2 n = a_2 - b_2$
    - Then
        - $a_1 a_2 - b_1 b_2$
        - $= a_1 a_2 + (a_1 b_2 - a_1 b_2) - b_1 b_2$
        - $= a_1(a_2 - b_2) + (a_1 - b_1) b_2$
        - $= a_1 c_2 n + b_2 c_1 n$
        - $= (a_1 c_2 + b_2 c_1) n$
    - Thus, $n | (a_1 c_2 + b_2 c_1)$
    - So, $\overline{a_1 a_2} = \overline{b_1 b_2}$

Well-definedness

- Example
    - Say we want to "define" a map
        - $f: \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$
        - $f(\bar{a}) = a$
    - Note that f is not a function
        - $\bar{1} = \bar{3}$ in $\mathbb{Z}/2\mathbb{Z}$
        - But $f(\bar{1}) = 1 \neq f(\bar{3}) = 3$

- So we say that f is not well defined
- How to check well-definedness
  - To check that a purported function $f: A \to B$ is well-defined,
  - One needs to check that $a = a' \Rightarrow f(a) = f(a')$

Corollary 10: Addition Group of $\mathbb{Z}/n\mathbb{Z}$

- Statement
  - Let $n \in \mathbb{Z}_{>0}$ be fixed
  - $\mathbb{Z}/n\mathbb{Z}$ is a group under the operation
    - $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$
    - $(\bar{a}, \bar{b}) \mapsto \overline{a+b}$
  - We will denote this operation by $+$
  - So $\bar{a} + \bar{\mathrm{b}} = \overline{a+b}$
- Proof
  - Well-definedness
    - By proposition 9, the operation $\bar{a} + \bar{b} = \overline{a+b}$ is well-defined
  - Associative
    - Associativity is inherited from the associativity of addition for $\mathbb{Z}$
  - Identity
    - The identity is $\bar{0}$
    - $\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z}, \bar{a} + \bar{0} = \overline{a+0} = \bar{a} = \overline{0+a} = \bar{0} + \bar{a}$
  - Inverses
    - $\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z}$, the inverse of $\bar{a}$ is $\overline{-a}$
    - $\bar{a} + \overline{-a} = \overline{a-a} = \bar{0} = \overline{-a+a} = \overline{-a} + \bar{a}$

$(\mathbb{Z}/n\mathbb{Z})^{\times}$, Properties of Group

Wednesday, February 7, 2018 9:56 AM

$\mathbb{Z}/n\mathbb{Z}$ is Not a Group Under Multiplication

- Let $n \in \mathbb{Z}_{>0}$ be fixed
- Proposition 9 implies that there is a well-defined function
  - $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$
  - $(\bar{a}, \bar{b}) \to \overline{ab}$
- Check group property
  - Identity: $\bar{1} \cdot \bar{a} = \overline{1 \cdot a} = \bar{1}$
  - This operation is associative
  - $\bar{1}$ is a reasonable candidate for an identity, but there is **no inverse**
  - Example in $\mathbb{Z}/4\mathbb{Z}$
    - $\bar{2} \cdot \bar{0} = \bar{0}$
    - $\bar{2} \cdot \bar{1} = \bar{2}$
    - $\bar{2} \cdot \bar{2} = \bar{0}$
    - $\bar{2} \cdot \bar{3} = \bar{2}$

Proposition 11: $(\mathbb{Z}/n\mathbb{Z})^{\times}$

- Definition
  - Define $(\mathbb{Z}/n\mathbb{Z})^{\times} := \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} | (a, n) = 1\}$
  - By HW 2 #2,
    - $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^{\times} \Leftrightarrow \exists \bar{c} \in \mathbb{Z}/n\mathbb{Z}$ s.t. $\overline{ac} = \bar{1}$
- Statement
  - $(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})^{\times}$ **is a group** with operation given by **multiplication**
- Proof
  - Closure: If $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, then $\overline{ab} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ as well
  - Associativity: Clear, from associativity of multiplication of integers
  - Identity: $\bar{1}$
  - Inverses: Built in HW 2 #2

List of Groups

Set	Operation
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	$+$
$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$	$\cdot$
$GL_n(\mathbb{R}), n > 0$	Matrix multiplication
$\mathbb{Z}/n\mathbb{Z}, n > 0$	$+$

$\mathbb{Z}/n\mathbb{Z}^*, n > 0$	$\cdot$

Proposition 12: Properties of Group

- Let G be a group, then G has the following properties
- The **identity** of G is **unique**
  - In other word
    - If $\exists 1, 1' \in G$ s.t.
    - $\forall g \in G, 1g = g1 = g$ and $1'g = g1' = g$
    - Then $1 = 1'$
  - Proof
    - $1 = 1 \cdot 1' = 1'$
- Each $g \in G$ has a **unique inverse**
  - In other word
    - If $g \in G$ and $\exists h, h' \in G$ s.t.
    - $hg = gh = 1$ and $h'g = gh' = 1$
    - Then $h = h'$
  - Proof
    - Let $g \in G$, and suppose $h, h' \in G$ are both inverses of g
    - Then $h = h \cdot 1 = h(gh') = (hg)h' = 1 \cdot h' = h'$
- $\boldsymbol{(g^{-1})^{-1} = g, \forall g \in G}$
  - Let $g \in G$, then $gg^{-1} = 1 = g^{-1}g$
  - Since the inverse is unique, $g = (g^{-1})^{-1}$
- **The Generalized Associative Law**
  - i.e. If $g_1, \dots, g_n \in G$, then $g_1 \dots g_n$ is independent of how it is bracketed
  - First show the result is true for $n = 1,2,3$
  - Assume for any $k < n$ any bracketing of a product of k elements
  - $b_1 b_2 \cdots b_k$ can be reduced to an expression of the form $b_1\big(b_2(b_3 \cdots b_k)\big)$
  - Then any bracketing of the product $a_1 a_2 \cdots a_n$ must break into
  - 2 sub-products, say $(a_1 a_2 \cdots a_k)(a_{k+1} a_{k+2} \cdots a_n)$
  - where each sub-product is bracketed in some fashion
  - Apply the induction assumption to each of these two sub-products
  - Reduce the result to the form $a_1\big(a_2(a_3 \dots a_n)\big)$ to complete the induction
- $\boldsymbol{(gh)^{-1} = h^{-1}g^{-1}, \forall g, h \in G}$
  - By the generalized associative law
  - $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = gg^{-1} = 1$
  - $(h^{-1}g^{-1})(gh) = h(gg^{-1})h^{-1} = hh^{-1} = 1$
- Notation

- We will apply the Generalized Associative Law without mentioning it
- In particular, if G is a group and $n \in \mathbb{Z}_{>0}$, we will write
  - $g^n = \underbrace{g \dots g}_{n \text{ copies}}$
  - $g^{-n} = \underbrace{g^{-1} \dots g^{-1}}_{n \text{ copies}}$
  - $g^0 = 1$

Proposition 13: Cancellation Law

- Statement
  - Let G be a group, and let $a, b, u, v \in G$
  - **If $au = av$, then $u = v$**
  - **If $ua = va$, then $u = v$**
- Proof
  - $au = av \Rightarrow a^{-1}au = a^{-1}av \Rightarrow u = v$
  - $ua = va \Rightarrow uaa^{-1} = vaa^{-1} \Rightarrow u = v$
- Warning
  - $ua = av \nRightarrow u = v$
  - This holds in abelian groups, but not in general

Corollary 14: Cancellation Law and Identity

- Let G be a group, and let $g, h \in G$
- **If $gh = g$, then $h = 1$**
  - $gh = g$
  - $\Rightarrow gh = g1$
  - $\Rightarrow h = 1$
- **If $gh = 1$, then $h = g^{-1}$**
  - $gh = 1$
  - $\Rightarrow gh = gg^{-1}$
  - $\Rightarrow h = g^{-1}$

Order, Definition of S_n

Friday, February 9, 2018 10:07 AM

Order

- Definition
  - If G is a group, and $g \in G$
  - The **order** of g is the **smallest positive integer n** s.t. $\boldsymbol{g^n = 1}$
  - If n is the order of g, write $|g| = n$
  - If no such integer exists, write $|g| = \infty$
  - i.e. $\boldsymbol{|g| \coloneqq \inf\{n \in \mathbb{Z}_{>0} | g^n = 1\}}$
- Note
  - The order of the identity is 1
- Example 1
  - Let $A \coloneqq \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in GL_2(\mathbb{R})$
  - $A^3 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^3 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$
  - Therefore, $|A| = 3$
- Example 2
  - In $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, every nonzero element has infinite order
  - The identity 0 has order of 1
- Example 3
  - In $\mathbb{Q}^*$ and $\mathbb{R}^*$, the elements of finite order are
    - $|1| = 1$
    - $|-1| = 2$
  - In $\mathbb{C}^*$, there are lots more
    - Elements of order n in $\mathbb{C}$ are called n^{th} roots of unity
    - i is the fourth root of unity
    - i.e. $i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$
- Example 4
  - What are the orders of the elements in $\mathbb{Z}/6\mathbb{Z}$?

Elements	Order	Note
$\overline{0}$	1	$\overline{0}$ is the identity
$\overline{1}$	6	$\overline{1} \cdot 6 = \overline{6} = \overline{0}$
$\overline{2}$	3	$\overline{2} \cdot 3 = \overline{6} = \overline{0}$
$\overline{3}$	2	$\overline{3} \cdot 2 = \overline{6} = \overline{0}$
$\overline{4}$	3	$\overline{4} \cdot 3 = \overline{12} = \overline{0}$

$\bar{5}$	6	$\bar{5} \cdot 6 = \overline{30} = \bar{0}$

- In general, if $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, then the "$n^{\text{th}}$ power" of $\bar{a}$ is $\overline{na}$
- Note that all the orders are divisors of 6 (Lagrange Theorem)

- Example 5
  - What are the orders of the elements in $(\mathbb{Z}/5\mathbb{Z})^{\times}$?
  - $(\mathbb{Z}/5\mathbb{Z})^{\times} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

Elements	Order	Note
$\bar{1}$	1	$\bar{1}$ is the identity
$\bar{2}$	4	$\bar{2}^4 = \overline{16} = \bar{1}$
$\bar{3}$	4	$\bar{3}^4 = 8\bar{1} = \bar{1}$
$\bar{4}$	2	$\bar{4}^2 = \overline{16} = \bar{1}$

  - Note: $(0,5) = 0 \neq 1$, so $\bar{0} \notin \mathbb{Z}/5\mathbb{Z}^{\times}$

Symmetric Group (Section 1.3)

- Definition
  - Let $n \in \mathbb{Z}_{>0}$ be fixed
  - Let $\boldsymbol{S_n} \coloneqq \{\textbf{bijective functions } \{\mathbf{1}, \dots, \boldsymbol{n}\} \to \{\mathbf{1}, \dots, \boldsymbol{n}\}\}$
  - (i.e. S_n is the **set of all permutations** of $\{1, \dots, n\}$)
  - Then S_n is a group with operation given by **function composition**
  - We call this group **symmetric group of degree $\boldsymbol{n}$**
- Proof
  - Function composition is an operation on S_n
    - The composition of bijective functions is still bijective
    - Therefore, function composition is an operation on S_n
  - Associativity
    - Suppose $f: X \to Y, g: Y \to Z, h: Z \to W$
    - $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h\left(g(f(x))\right)$
    - $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h\left(g(f(x))\right)$
    - Thus $(h \circ g) \circ f = h \circ (g \circ f)$
  - Identity
    - The identity map is the identity
  - Inverses
    - Bijective functions all have inverse functions

Properties of S_n, Properties of Cycles

Monday, February 12, 2018 9:53 AM

Proposition 15: Order of Symmetric Group

- Statement
  - $|\boldsymbol{S_n}| = \boldsymbol{n}!$
- Proof
  - First, we prove that
    - If X and Y are sets of order n
    - Then there are $n!$ injective functions from X to Y
  - We argue by induction on n
    - When $n = 1$, this is clear
    - For $n > 1$
    - Suppose $f: X \to Y$ is injective
    - Let $x \in X$, then there are n possibilities for $f(x)$
    - f restricts to an injective function $X \setminus \{x\} \to Y \setminus \{f(x)\}$
    - There are $(n-1)!$ such functions, by induction
    - Thus, there are $n(n-1)! = n!$ injective functions $X \to Y$
  - Now, take $X = \{1, \dots, n\} = Y$
    - Since injection between finite sets of the same order is bijective
    - We can conclude that $|S_n| = n!$
  - Note
    - The sets must be finite
    - Counterexample: $f: \mathbb{Z} \to \mathbb{Z}, n \mapsto 2n$ is not bijective

Cycle

- Definition
  - Let $n \in \mathbb{Z}_{>0}$ be fixed
  - Let $a_1, \dots, a_t \in \{1, \dots, n\}$
  - The element of S_n given by
    - $a_i \mapsto a_{i+1}$ for $1 \leq i \leq t-1$
    - $a_t \mapsto a_1$
    - $j \mapsto j$ if $j \notin \{a_1, \dots a_t\}$
  - is denoted by $(\boldsymbol{a_1}, \boldsymbol{a_2}, \dots, \boldsymbol{a_t})$ and is called a **cycle of length $\boldsymbol{t}$**
- Example
  - Let $\sigma = (1\ 3\ 2) \in S_4$, then

- $\begin{pmatrix} i & 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \sigma(i) & 3 & 1 & 2 & 4 \end{pmatrix}$
- Notice: $(1\ 3\ 2) = (3\ 2\ 1) = (2\ 1\ 3)$

Disjoint Cycles

- Definition
  - Two cycles $(a_1, \ldots a_t)$ and $(b_1, \ldots, b_k)$ are **disjoint** if
  - $\{\boldsymbol{a_1}, \ldots \boldsymbol{a_t}\} \cap \{\boldsymbol{b_1}, \ldots, \boldsymbol{b_k}\} = \emptyset$
- Example
  - $(1\ 2), (3\ 4) \in S_4$ are disjoint
- Fact
  - Every **element of S_n** can be written as a **product of disjoint cycles**
  - $S_1 = \{(1)\}$
  - $S_2 = \{(1), (1\ 2)\}$
  - $S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$
  - $S_4 = \{(1), (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4)\}$
  - Note: We write the identity of S_n as (1)

Cycle Decomposition for Permutations

- Algorithm

Step	Example
Let $a := \min\{x \in \mathbb{N} \mid x \text{ not appeared in previous cycles}\}$ Begin the new cycle: $(a$	$(1$
Let $b := \sigma(a)$ If $b = a$ • close the cycle with a right parenthesis • return to step 1 If $b \neq a$ • write b next to a in this cycle: $(a\ b$	$\sigma(1) = 12 = b$ $12 \neq 1$ So write $(1\ 12$
Let $c := \sigma(b)$ If $c = a$ • close the cycle with a right parenthesis • return to step 1 If $c \neq a$ • write c next to in this cycle: $(a\ b\ c$ $b := c$ and repeat this step until the cycle closes	$\sigma(12) = 8$ $8 \neq 1$ So continue the cycle as: $(1\ 12\ 8$
Naturally this process stops when all the numbers from	$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)$

$\{1,2,\ldots,n\}$ have appeared in some cycle.	(3)(5 1 1 7)(6 9)
Remove all cycles of length 1	σ = (1 1 2 8 10 4)(2 1 3)(5 1 1 7)(6 9)

- Example
  - Take $\sigma \in S_{13}$ to be the following
  - $\begin{pmatrix} i & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \sigma(i) & 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 3 \end{pmatrix}$
  - Start with 1, $\sigma(1) = 12$, so write 12 after 1.
  - Keep going until you cycle back to 1
  - Start with the smallest number which hasn't yet appeared, and repeat.
  - Repeat this step until $1, \ldots, 13$ have all appeared.

Product of Cycles

- Reminder
  - **Read from right to left**
- Example
  - Write $\sigma = (1\ 2\ 3)(1\ 2)(3\ 4)$ as a product of disjoint cycles
  - What is $\sigma(1)$?
    - $(3\ 4)$ maps 1 to 1
    - $(1\ 2)$ maps 1 to 2
    - $(1\ 2\ 3)$ maps 2 to 3
    - Thus $\sigma(1) = 3$
  - Similarly $\sigma(3) = 4, \sigma(4) = 1$
  - Thus we close the cycle $(1\ 3\ 4)$
  - We won't write down (2), since it is the identity
  - Thus $\sigma = (1\ 3\ 4)(2) = (1\ 3\ 4)$
  - Note: $\sigma \in S_4$, but it make sense to think of $\sigma \in S_n$ for $n > 4$
- Commutativity of S_n
  - $(1\ 2)(1\ 2\ 3) = (2\ 3)$
  - $(1\ 2\ 3)(1\ 2) = (3\ 1)$
  - In particular S_3 is not abelian
  - Therefore $\boldsymbol{S_n}$ is **not abelian** for $n \geq 3$

Homomorphism, Isomorphism

Wednesday, February 14, 2018 9:39 AM

Homomorphism

- Definition
  - Let G, H be groups
  - A function $f: G \to H$ is a **homomorphism** if
    - $f(g_1 g_2) = f(g_1) f(g_2), \forall g_1, g_2 \in G$
  - One says f "respects", or "preserves" the group operation
- Trivial Examples
  - Let G be a group
  - The identity map $f: G \to G$ given by $g \mapsto g$ is a homomorphism
    - $f(g_1) f(g_2) = 1 \cdot 1 = 1 = f(g_1 g_2)$
  - The map $f: G \to G$ given by $g \mapsto 1$ is a homomorphism
    - This only works if we send every element of G to 1
    - If $x \in G \setminus \{1\}$, and $f: G \to G$ is given by $g \mapsto x, \forall g$
    - $f(g_1 g_2) = f(g_1)(g_2) \Rightarrow x = x^2$
    - Thus $x = 1$
    - This is impossible since $x \in G \setminus \{1\}$
- Example 1
  - Let $f: \mathbb{R} \to \mathbb{R}^{\times}$ be given by $f(x) = e^x$
  - Then f is a homomorphism
  - $f(x_1 + x_2) = e^{x_1 + x_2} = e^{x_1} e^{x_2} = f(x_1) f(x_2)$
- Example 2
  - Let G be a group, and let $x \in G$
  - The map $f: G \to G, g \mapsto x g x^{-1}$ is a homomorphism
  - $f(g_1 g_2) = x g_1 g_2 x^{-1} = x g_1 x^{-1} x g_2 x^{-1} = f(g_1) f(g_2)$
  - This homomorphism is called **conjugation by $\boldsymbol{x}$**
- Example 3
  - Let $n \in \mathbb{Z}$ be fixed
  - Is $f: \mathbb{Z} \to \mathbb{Z}, x \mapsto x + n$ a homomorphism?
  - Only when $n = 0$
  - $f(0) + f(0) = f(0) \Rightarrow n + n = n \Rightarrow n = 0$
- Example 4
  - Let $n \in \mathbb{Z}_{>0}$ be fixed
  - Is $\alpha: \mathbb{Z} \to \mathbb{Z}, x \mapsto x^n$ a homomorphism?

        - Only when $n = 1$
        - When $n = 0$
            - $\alpha(x) = x^0 = 1, \forall x \setminus \{0\}$
            - Only constant mapping to identity is a homomorphism
            - But 1 is not the identity (0 is)
            - So this doesn't work
        - For $n \geq 2$
            - $\alpha(x_1 + x_2) = \alpha(x_1) + \alpha(x_2) \Leftrightarrow (x_1 + x_2)^n = x_1^n + x_2^n$
            - But this is not always true
            - For instance, when $x_1 = x_2 = 1$, $2^n \neq 2$ for $n \geq 2$
- Example 5
    - Let $n \in \mathbb{Z}$ be fixed
    - $\beta: \mathbb{Z} \to \mathbb{Z}, x \mapsto nx$ is a homomorphism
    - $\beta(x_1 + x_2) = n(x_1 + x_2) = nx_1 + nx_2 = \beta(x_1) + \beta(x_2)$
- Example 6
    - The previous examples is a special case of the following:
    - Let G be a group, and $n \in \mathbb{Z}$
    - Define $\beta: G \to G, g \mapsto g^n$, then
    - β is a **homomorphism** $\forall n \in \mathbb{Z} \Leftrightarrow G$ is **abelian**
    - Proof: homomorphism $\Rightarrow$ abelian
        - Say $n = -1$
        - Let $g_1, g_2 \in G$
        - Since β is a homomorphism
        - $\beta(g_1, g_2) = \beta(g_1)\beta(g_2)$
        - $(g_1 g_2)^{-1} = g_1^{-1} g_2^{-1}$
        - $g_2^{-1} g_1^{-1} = g_1^{-1} g_2^{-1}$
        - $(g_2^{-1} g_1^{-1})^{-1} = (g_1^{-1} g_2^{-1})^{-1}$
        - $(g_1^{-1})^{-1}(g_2^{-1})^{-1} = (g_2^{-1})^{-1}(g_1^{-1})^{-1}$
        - $g_1 g_2 = g_2 g_1$
        - Thus G is abelian
    - Proof: abelian $\Rightarrow$ homomorphism
        - Let $g, h \in G$
        - First, suppose $n \geq 0$
            - We argue by induction on n
            - If $n = 0$, this is obvious
            - Suppose $n > 0$, then
            - $\beta(gh) = (gh)^n = gh(gh)^{n-1} = ghg^{n-1}h^{n-1}$

        - $= gg^{n-1}hh^{n-1} = g^n h^n = \beta(g)\beta(h)$
      - Now suppose $n < 0$
        - Then $x \mapsto x^{-n}$ is a homomorphism, by the above argument
        - So $(ab)^{-m} = a^{-m}b^{-m}, \forall a, b \in G$
        - Now, take $a = g^{-1}$ and $b = h^{-1}$ to obtain the result

Isomorphism

- Definition
  - Let G, H be groups
  - A homomorphism $\alpha: G \to H$ is a **isomorphism** if
  - there is a homomorphism $\beta: H \to G$ s.t.
    - $\boldsymbol{\alpha\beta = id_H}$, and
    - $\boldsymbol{\beta\alpha = id_G}$
  - In this case, we say G and H are **isomorphic**
- Fact
  - $\alpha: G \to H$ is an **isomorphism** $\Leftrightarrow$ α is a **bijective homomorphism**
  - Proof: isomorphism $\Rightarrow$ bijective homomorphism
    - This is clear
  - Proof: bijective homomorphism $\Rightarrow$ isomorphism
    - We need to show that α^{-1} is a homomorphism
    - Let $h_1, h_2 \in H$
    - Choose $g_1, g_2 \in G$ s.t. $\alpha(g_1) = h_1$ and $\alpha(g_2) = h_2$
    - Then
      - $\alpha^{-1}(h_1h_2)$
      - $= \alpha^{-1}\big(\alpha(g_1)\alpha(g_2)\big)$
      - $= \alpha^{-1}\big(\alpha(g_1g_2)\big)$
      - $= g_1g_2$
      - $= \alpha^{-1}(h_1)f^{-1}(h_2)$
- Example
  - $\mathbb{R}_{>0} \coloneqq \{r \in \mathbb{R} | r > 0\}$ is a group under multiplication
  - Define $f: \mathbb{R} \to \mathbb{R}_{>0}$ where $f(x) = e^x$
  - Then f is a homomorphism
  - Moreover, f is an isomorphism
  - The inverse of f is ln
- Observation
  - If G, H are **isomorphic groups**, then $\boldsymbol{|G| = |H|}$

Homomorphism, Isomorphism, Subgroup

Friday, February 16, 2018 10:05 AM

Proposition 16: Isomorphism Preserves Commutativity

- Statement
  - Let $f: G \to H$ be an **isomorphism**
  - $\boldsymbol{G}$ **is abelian** if and only if $\boldsymbol{H}$ **is abelian**
- Proof
  - $(\Longrightarrow)$ Suppose G is abelian
  - Let $h, h' \in H$
  - Choose $g, g' \in G$ s.t. $f(g) = h, f(g') = h'$
  - Then $hh' = f(g)f(g') = f(gg') = f(g'g) = f(g')f(g) = h'h$
  - $(\Longleftarrow)$ Apply the same argument with $f^{-1}: H \to G$

Proposition 16: Injective Homomorphism Preserves Order

- Statement
  - Let $f: G \to H$ be an **injective homomorphism**
  - Then $\forall \boldsymbol{g} \in \boldsymbol{G}, |\boldsymbol{g}| = |\boldsymbol{f}(\boldsymbol{g})|$
- Proof
  - $f(1_G) = 1_H$
    - Let $g \in G$, then
    - $f(g) = f(1_G \cdot g) = f(1_G) \cdot f(g)$
    - By Cancellation Law, $f(1_G) = 1_H$
  - When $|g| < \infty$
    - Let $n := |g|$, then
    - $1_H = f(1_G) = f(g^n) = f(g)^n$
    - (This last equality follows from an induction argument)
    - Therefore, $|f(g)| \leq n$
    - Now, apply this same argument with f replaced by f^{-1}
    - So we can conclude that $|f(g)| = n$
  - When $|g| = \infty$
    - If $|f(g)| < \infty$
    - The above argument shows $|g| < \infty$
    - This is impossible
    - Thus, $|f(g)| = \infty$

Groups with Same Order is Not Necessarily Isomorphic

- G, H are groups, and $|G| = |H|$, is it the case that $G \cong H$? No
- Example 1: $\mathbb{Z} \ncong \mathbb{Q}$
    - In fact, any homomorphism $f: \mathbb{Z} \to \mathbb{Q}$ is not surjective
    - Let $f: \mathbb{Z} \to \mathbb{Q}$ be a homomorphism
    - If $f(a) = 0, \forall a \in \mathbb{Z}$
        - Obviously f is not surjective
    - Assume otherwise
        - By induction, $f(a) = f\underbrace{(1 + 1 + \cdots + 1)}_{n \text{ copies}} = a \cdot f(1)$
        - By assumption, $f(1) \neq 0$, since otherwise $f = 0$
        - We know that $\dfrac{f(1)}{2} \in \mathbb{Q}$
        - But $\nexists a \in \mathbb{Z}$ s.t. $\dfrac{f(1)}{2} = af(1)$
        - i.e. $\dfrac{f(1)}{2} \notin \operatorname{im}(f)$
        - Thus f is not surjective
- Example 2: $\mathbb{Z}/6\mathbb{Z} \ncong S_3$
    - $|\mathbb{Z}/6\mathbb{Z}| = |S_3|$, but $\mathbb{Z}/6\mathbb{Z} \ncong S_3$
    - Because $\mathbb{Z}/6\mathbb{Z}$ is abelian, but S_3 is not
    - Also $|\bar{1}| = 6$ in $\mathbb{Z}/6\mathbb{Z}$, but S_3 have no element of order 6

Orders of Elements in S_n

- Let $\sigma \in S_n$
- If $\sigma = \sigma_1 \cdots \sigma_m$, where $\sigma_1 \cdots \sigma_m$ are **disjoint** cycles, then $|\sigma| = \operatorname{lcm}(|\sigma_1|, \dots, |\sigma_m|)$
- If σ is a t-cycle, then $|\sigma| = t$

Subgroup

- Definition
    - Let G be a group, and let $H \subseteq G$
    - H is a subgroup if
        - $H \neq \emptyset$ (**nonempty**)
        - If $h, h' \in H$, then $hh' \in H$ (**closed under the operation**)
        - If $h \in H$, then $h^{-1} \in H$ (**closed under inverse**)
    - If H is a subgroup of G, we write $H \leq G$
- Note
    - Subgroups of a group are also groups
- Example 1
    - If G is a group, then $\boldsymbol{G \leq G}$ and $\{\mathbf{1}\} \leq \boldsymbol{G}$
- Example 2

- If $m, n \in \mathbb{Z}_{>0}$, and $\boldsymbol{n} \leq \boldsymbol{m}$, then $\boldsymbol{S_n} \leq \boldsymbol{S_m}$

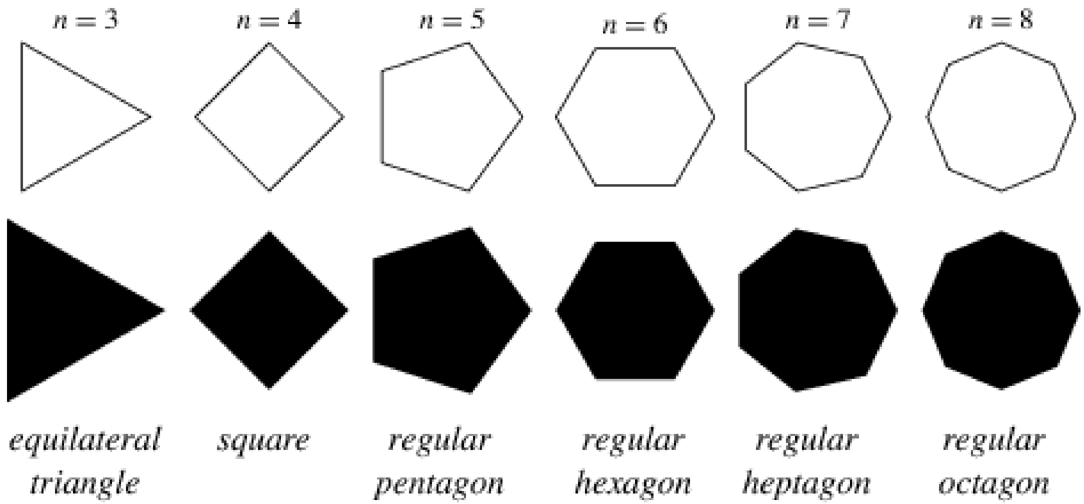
- Example 3
  - Let G be a group, and let $g \in G$
  - Then $\langle \boldsymbol{g} \rangle \coloneqq \{\boldsymbol{g^n} | \boldsymbol{n} \in \mathbb{Z}\} \leq \boldsymbol{G}$
  - $\langle g \rangle$ is called the **cyclic subgroup generated by $\boldsymbol{g}$**
  - $\langle g \rangle \neq \emptyset$, since $g \in \langle g \rangle$
  - Let $g^i, g^j \in \langle g \rangle$, then $g^i g^j = g^{ij} \in \langle g \rangle$
  - If $g^i \in \langle g \rangle$, then $\left(g^i\right)^{-1} = g^{-i} \in \langle g \rangle$

D_{2n}, Subgroup Criterion, Special Subgroups

Monday, February 19, 2018 9:58 AM

Regular n-gon

- A **regular n-gon** is a polygon with all sides and angles equal



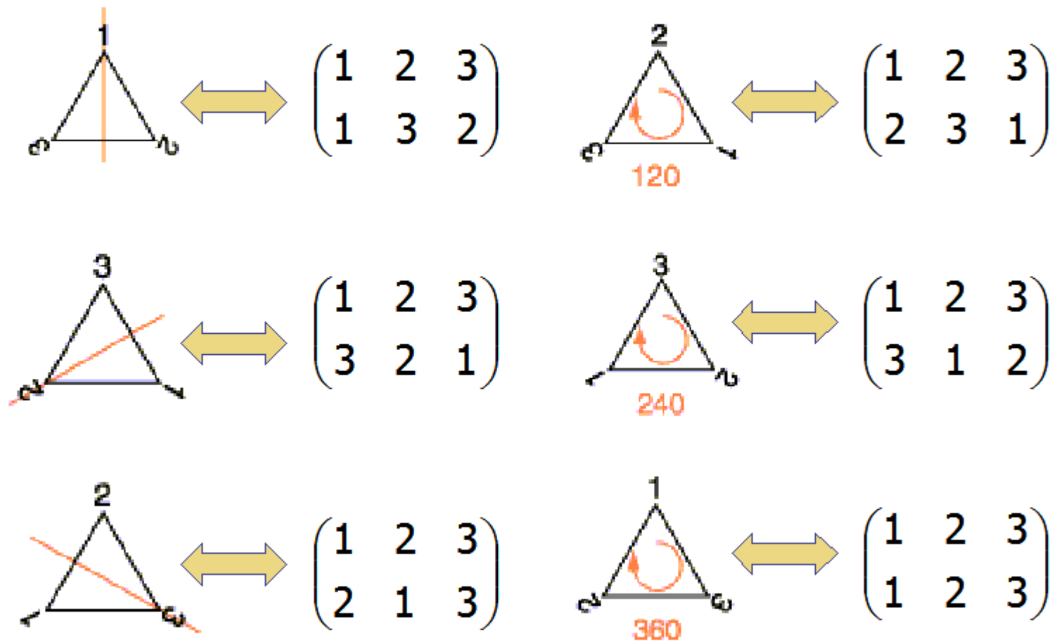
Symmetry

- Definition
  - A **symmetry** of a regular n-gon is a way of
    - picking up a copy of it
    - moving it around in 3d
    - setting it back down
  - so that it **exactly covers the original**
- Examples
  - Rotations
  - Reflection

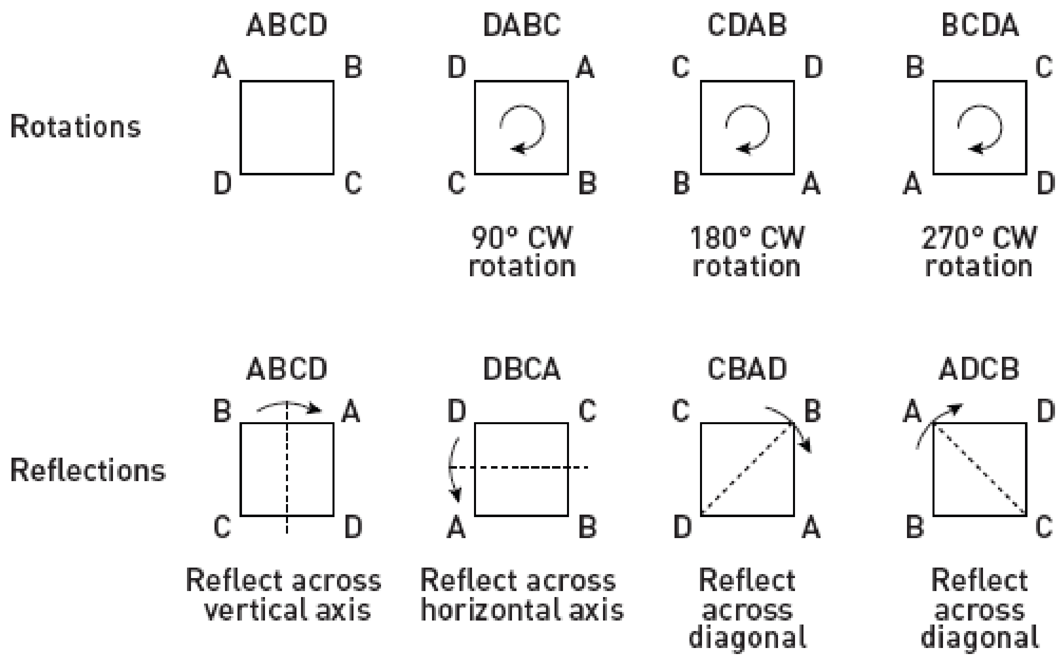
Dihedral Groups (Section 1.2)

- Definition
  - $D_{2n} :=$ {symmetries of the n-gon} is called ***n*-th dihedral groups**
- Note
  - $|D_{2n}| = 2n$ (proof on page 24)
  - There are ***n* rotations** and ***n* reflections**
  - Symmetries of n-gons are determined by
  - **the permutations of the vertices they induce**
- Example: $n = 3$
  - Rotations

        - $120°$: $(1\ 2\ 3)$
        - $240°$: $(1\ 3\ 2)$
        - $360°$: (1)
    - Reflections
        - $(2\ 3)$
        - $(1\ 3)$
        - $(1\ 2)$
    - $D_6 \cong \{(1), (2\ 3), (1\ 3), (1\ 2), (1\ 3\ 2), (1\ 2\ 3)\} = S_3$



- Example: $n = 4$
    - Rotations
        - $90°$: $(1\ 2\ 3\ 4)$
        - $180°$: $(1\ 3)(2\ 4)$
        - $270°$: $(1\ 4\ 3\ 2)$
        - $360°$: (1)
    - Reflections
        - $(2\ 4)$
        - $(1\ 3)$
        - $(1\ 4)(2\ 3)$
        - $(1\ 2)(3\ 4)$
    - $D_8 \cong \{(1), (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 3), (2\ 4), (1\ 4)(2\ 3), (1\ 2)(3\ 4)\} \leq S_4$



- Fact
  - In general D_{2n} is **isomorphic** to a **subgroup of $\boldsymbol{S_n}$**
  - **Every finite group is isomorphic to a subgroup of a symmetric group**

Proposition 17: The Subgroup Criterion

- Statement
  - A subset H of a group G is a subgroup iff
  - $\boldsymbol{H} \neq \emptyset$ and $\forall x, y \in H, \boldsymbol{xy^{-1}} \in \boldsymbol{H}$
- Recall the original definition
  - A subset H of a group G is a subgroup iff
  - $\boldsymbol{H} \neq \emptyset$
  - $\forall \boldsymbol{h}, \boldsymbol{h}' \in \boldsymbol{H}, \boldsymbol{hh}' \in \boldsymbol{H}$
  - $\forall \boldsymbol{h} \in \boldsymbol{H}, \boldsymbol{h}^{-1} \in \boldsymbol{H}$
- Proof ($\Longrightarrow$)
  - This is Clear
- Proof ($\Longleftarrow$)
  - Closed under multiplication
    - Let $x \in H$
    - $1 \cdot x^{-1} \in H$
    - Thus, $x^{-1} \in H$
  - Closed under inversion
    - Let $x, y \in H$, then $y^{-1} \in H$
    - So $x(y^{-1})^{-1} \in H$
    - Thus, $xy \in H$

Examples of Subgroups

- Example 1
  - $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$
- Example 2
  - Definition
    - Fix $n \in \mathbb{Z}_{>0}$
    - $\mathrm{SL}_n(\mathbb{R}) \coloneqq \{A \in \mathrm{GL}_n(\mathbb{R}) | \det A = 1\}$ is called the **special linear group**
  - Claim
    - $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$
  - Proof
    - $\mathrm{SL}_n(\mathbb{R}) \neq \emptyset$, since $I_n \in \mathrm{SL}_n(\mathbb{R})$
    - Let $A, B \in \mathrm{SL}_n(\mathbb{R})$
    - $\det(AB^{-1}) = \det A \cdot \det B^{-1} = \dfrac{\det A}{\det B} = \dfrac{1}{1} = 1$
- Example 3
  - Definition
    - If G is a group
    - $Z(G) \coloneqq \{a \in G | ag = ga, \forall g \in G\}$ is called the **center** or G
  - Claim
    - $Z(G) \leq G$
  - Proof
    - $Z(G) \neq \emptyset$, since $1 \in Z(G)$
    - Let $a, b \in Z(G)$
    - If $g \in G, abg = agb = gab$
    - so $Z(G)$ is closed under multiplication
    - Also $a^{-1}g = (g^{-1}a)^{-1} = (ag^{-1})^{-1} = ga^{-1}$
    - so $Z(G)$ is closed under inversion

Properties of Cyclic Group, Order of g^a

Wednesday, February 21, 2018 9:56 AM

Cyclic Group

- Definition
  - A group G is **cyclic** if $\exists \boldsymbol{g} \in \boldsymbol{G}$ **s.t.** $\langle \boldsymbol{g} \rangle = \boldsymbol{G}$
- Note
  - **A finite group $\boldsymbol{G}$ of order $\boldsymbol{n}$ is cyclic iff $\exists \boldsymbol{g} \in \boldsymbol{G}$ s.t. $|\boldsymbol{g}| = \boldsymbol{n}$**
- Example 1: $\mathbb{Z}$ is cyclic
  - $\mathbb{Z} = \langle 1 \rangle$
  - $\mathbb{Z} = \langle -1 \rangle$
- Example 2: $\mathbb{Z}/n\mathbb{Z}$ is cyclic
  - If $(a, n) = 1$, then $\mathbb{Z}/n\mathbb{Z} = \langle \bar{a} \rangle$
- Example 3: S_3 is not cyclic
  - Note: If $(a_1, \dots, a_t) \in S_n$ is a t-cycle, then $|(a_1, \dots, a_t)| = t$
  - $S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$
  - Every element in S_3 have order 1,2, or 3
  - So S_3 cannot be cyclic

Proposition 18: Isomorphism of Cyclic Group

- Let G be a cyclic group
- **If $|\boldsymbol{G}| = \boldsymbol{n} < \infty$, then $\boldsymbol{G} \cong \mathbb{Z}/\boldsymbol{n}\mathbb{Z}$**
  - Choose $g \in G$ s.t. $G = \langle g \rangle$
  - Define a map $f: \mathbb{Z}/n\mathbb{Z} \to G$ given by $\bar{a} \mapsto g^a$
  - Well-definedness
    - We need to check that f is well-defined.
    - That is we must show that if $\bar{a} = \bar{b}$ in $\mathbb{Z}/n\mathbb{Z}$, then $f(\bar{a}) = f(\bar{b})$
    - Let $a, b \in \mathbb{Z}$, suppose $\bar{a} = \bar{b}$ in $\mathbb{Z}/n\mathbb{Z}$
    - Choose $q \in \mathbb{Z}$ s,t, $nq = a - b$
    - $f(\bar{a}) = g^a = g^{nq+b} = g^{nq} g^b = g^b = f(\bar{b})$
    - Thus, f is well-defined
  - Homomorphism
    - $f(\bar{a} + \bar{b}) = g^{a+b} = g^a g^b = f(\bar{a}) f(\bar{b})$
    - Thus, f is a homomorphism
  - Surjectivity
    - Surjectivity is clear by definition

        - Injectivity
            - If $f(\bar{a}) = f(\bar{b})$
            - $g^a = g^b$
            - $g^{a-b} = 1$
            - $|g| \big| (a-b)$
            - $n|(a-b)$
            - $\bar{a} = \bar{b}$
            - Thus f is injective
- **If $|G| = \infty$, then $G \cong \mathbb{Z}$**
    - Choose $g \in G$ s.t. $G = \langle g \rangle$
    - Define a map $f: \mathbb{Z} \to G$ given by $n \mapsto g^n$
    - Homomorphism
        - If $n_1, n_2 \in \mathbb{Z}$
        - then $f(n_1 + n_2) = g^{n_1+n_2} = g^{n_1}g^{n_2} = f(n_1)f(n_2)$
        - Thus, f is a homomorphism
    - Surjectivity
        - Surjectivity is clear
    - Injectivity
        - Suppose $f(n_1) = f(n_2)$
        - Then $g^{n_1} = g^{n_2}$
        - Without loss of generality, assume $n_1 \geq n_2$
        - Then $g^{n_1-n_2} = 1$
        - Since $|g| = \infty$
        - $n_1 - n_2 = 0$
        - i.e. $n_1 = n_2$
        - Thus f is injective

Least Common Multiple

- Definition
    - Let $a, b \in \mathbb{Z}$ where one of a, b is nonzero.
    - A **least common multiple** of a and b is a **positive integer** m s.t.
        - $\boldsymbol{a|m}$ **and** $\boldsymbol{b|m}$
        - **If $\boldsymbol{a|m'}$ and $\boldsymbol{b|m'}$, then $\boldsymbol{m|m'}$**
    - We denote the least common multiple of a and b by $[a, b]$
    - Define $[0,0] \coloneqq 0$
- Uniqueness
    - Similar to the proof of uniqueness of greatest common divisor

- Existence: If $a, b \in \mathbb{Z}$, and one of a, b is nonzero, then $[\boldsymbol{a}, \boldsymbol{b}] = \dfrac{\boldsymbol{ab}}{(\boldsymbol{a}, \boldsymbol{b})}$
  - Let $m := \dfrac{ab}{(a, b)}$
  - $a|m$ and $b|m$
    - This is true since $\dfrac{ab}{(a, b)}$ is a multiple of a and b
  - Suppose $a|m'$ and $b|m'$
    - Choose $q, q' \in \mathbb{Z}$ s.t. $aq = m'$ and $bq' = m'$
    - Choose $x, y \in \mathbb{Z}$ s.t. $ax + by = (a, b)$, then
      - $m'(a, b)$
      - $= m'(ax + by)$
      - $= m'ax + m'by$
      - $= bq'ax + aqby$
      - $= ab(q'x + qy)$
    - Thus $ab\big|\big(m'(a, b)\big)$
    - Therefore $\left.\dfrac{ab}{(a, b)}\right| m' \Rightarrow m|m'$

Proposition 19: Order of g^a

- Statement
  - If $\boldsymbol{G} = \langle \boldsymbol{g} \rangle$ **is cyclic**, and $|G| = n < \infty$, then $|\boldsymbol{g}^{\boldsymbol{a}}| = \dfrac{\boldsymbol{n}}{(\boldsymbol{a}, \boldsymbol{n})}$
- Proof
  - Let $a \in \mathbb{Z}$
  - When $a = 0$, this is clear, since $|g^0| = \dfrac{n}{(0, n)} = \dfrac{n}{n} = 1$
  - So assume $a \neq 0$
  - $|g^a| \left| \dfrac{n}{(a, n)} \right.$
    - $(g^a)^{\frac{n}{(a,n)}} = g^{\frac{an}{(a,n)}} = g^{[a,n]} = g^{kn}$ for some integer k
    - Thus, $(g^a)^{\frac{n}{(a,n)}} = (g^n)^k = 1$, since $n = |g|$
  - $\left.\dfrac{n}{(a, n)}\right| |g^a|$
    - Let $t = |g^a|$, then $(g^a)^t = 1$
    - By HW3 #1, $g^{at} = 1 \Rightarrow n|at$
    - Thus, at is a common multiple of n and a
    - $[a, n]|at \Rightarrow \left.\dfrac{an}{(a, n)}\right| at \Rightarrow \left.\dfrac{n}{(a, n)}\right| t \Rightarrow \left.\dfrac{n}{(a, n)}\right| |g^a|$

- Therefore $\frac{n}{(a,n)} = |g^a|$

Subgroups of Cyclic Groups, $\langle A \rangle$

Friday, February 23, 2018 10:07 AM

Theorem 20: Subgroup of Cyclic Group is Cyclic

- Statement
  - Let $G = \langle g \rangle$ be a cyclic group
  - Then every **subgroup of $\boldsymbol{G}$ is cyclic**
  - More precisely, if $H \leq G$, then either $\boldsymbol{H} = \{\mathbf{1}\}$ or $\boldsymbol{H} = \langle \boldsymbol{g^d} \rangle$, where
    - **$\boldsymbol{d}$ is the smallest positive integer s.t. $\boldsymbol{g^d} \in \boldsymbol{H}$**
- Proof
  - Assume $H \neq \{1\}$
  - Let $S \coloneqq \{b \in \mathbb{Z}_{>0} | g^b \in H\}$
  - $\langle g^d \rangle \subseteq H$
    - Choose $a \in \mathbb{Z} \setminus \{0\}$ s.t. $g^a \in H$, then $(g^a)^{-1} = g^{-a} \in H$
    - Thus, H contains some positive power of g, and so $S \neq \emptyset$
    - By the Well-Ordering Principle, S contains a minimum element d
    - Therefore, $\langle g^d \rangle \subseteq H$
  - $H \subseteq \langle g^d \rangle$
    - Let $h \in H$, then $h = g^a$ for some $a \in \mathbb{Z}$
    - Choose $q, r \in \mathbb{Z}$ s.t. $a = qd + r, 0 \leq r < d$
    - $g^d \in H \Rightarrow g^{a-qd} \in H \Rightarrow g^r \in H$
    - If $r > 0$, then $r \in S$, which is impossible since $r < d$
    - The minimality of d forces $r = 0$
    - So $h = g^a = g^{qd} \in \langle g^d \rangle, \forall h \in H$
    - Therefore $H \subseteq \langle g^d \rangle$
  - Therefore $H = \langle g^d \rangle$

Theorem 20: Subgroup of Finite Cyclic Group is Determined by Order

- Statement
  - Let $G = \langle g \rangle$ be a finite cyclic group of order n
  - For **all positive integers $\boldsymbol{a}$ dividing $\boldsymbol{n}$**, $\exists!$ **subgroup $\boldsymbol{H} \leq \boldsymbol{G}$ of order $\boldsymbol{a}$**
  - Moreover, this subgroup is $\langle \boldsymbol{g^d} \rangle$, where $\boldsymbol{d} = \dfrac{\boldsymbol{n}}{\boldsymbol{a}}$
- Proof
  - Let a be a positive divisor of n, and let $d \coloneqq \dfrac{n}{a}$
  - Existence

        - $|\langle g^d \rangle| = \dfrac{n}{(d,n)} = \dfrac{n}{d} = a$ by Proposition 19
    - Uniqueness
        - Suppose $H \leq G$ and $|H| = a$
        - Then, $H = \langle g^b \rangle$, where b is the smallest positive integer s.t. $g^b \in H$
        - We have $\dfrac{n}{d} = a = |H| = |\langle g^b \rangle| = \dfrac{n}{(n,b)}$ by Proposition 19
        - Thus $d = (n,b)$ i.e. $d|b$
        - So $g^b \in \langle g^d \rangle \Rightarrow H = \langle g^b \rangle \leq \langle g^d \rangle$
        - Since $|H| = |\langle g^d \rangle| = a$, we have $H = \langle g^d \rangle$

Lemma: Intersection of Subgroups is Again a Subgroup

- Statement
    - If $\{H_i\}_{i \in I}$ is a **family of subgroups** of G, then $\boldsymbol{\bigcap_{i \in I} H_i \leq G}$
- Proof
    - Let $H := \bigcap_{i \in I} H_i$
    - $H \neq \emptyset$
        - Since $1 \in H_i, \forall i \in I$
    - Let $h_1, h_2 \in H$
        - Then $h_1, h_2 \in H_i, \forall i \in I$
        - $\Rightarrow h_1 h_2^{-1} \in H_i, \forall i \in I$
        - $\Rightarrow h_1 h_2^{-1} \in H$

Subgroups Generated by Subsets of a Group (Section 2.4)

- Definition
    - Let G be a group and $A \subseteq G$
    - The **subgroup generated by $\boldsymbol{A}$** is
    - the intersection of every subgroup of G containing A
    - $\langle A \rangle := \bigcap_{\substack{H \leq G \\ A \subseteq H}} H$
- Example
    - If $A = \emptyset$, then $\langle A \rangle = \{1\}$
    - If $A = \{1\}$, then $\langle A \rangle = \{1\}$

$\langle A \rangle$, Finitely Generated Group

Monday, February 26, 2018 10:01 AM

Proposition 21: Construction of $\langle A \rangle$

- Statement
  - If $A \subseteq G$, then $\langle \boldsymbol{A} \rangle = \left\{ \boldsymbol{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n}} \middle| \boldsymbol{n} \in \mathbb{Z}_{>\mathbf{0}}, \boldsymbol{a_i} \in \boldsymbol{A}, \boldsymbol{\varepsilon} \in \{\pm \mathbf{1}\} \right\}$
  - Note: When $n = 0$, we get 1
- Proof
  - Denote the right hand side by $\bar{A}$
  - $\bar{A} \leq \mathrm{G}$
    - $\bar{A} \neq \emptyset$, since $1 \in \bar{A}$ (take $n = 0$)
    - If $a = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n}, b = b_1^{\delta_1} b_2^{\delta_2} \dots b_m^{\delta_m} \in \bar{A}$
    - Then $ab^{-1} = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n} b_m^{-\delta_1} b_{m-1}^{-\delta_2} \dots b_1^{-\delta_m} \in \bar{A}$
    - Therefore $\bar{A} \leq \mathrm{G}$
  - $\langle A \rangle \subseteq \bar{A}$
    - Because $A \subseteq \bar{A}$, and $\langle A \rangle$ is the smallest subgroup of G containing A
  - $\bar{A} \subseteq \langle A \rangle$
    - Because every subgroup of G containing A (i.e. $\langle A \rangle$) must contain
    - every finite product of elements of A and their inverses.
  - Therefore $\langle A \rangle = \bar{A} = \left\{ a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n} \middle| n \in \mathbb{Z}_{>0}, a_i \in A, \varepsilon \in \{\pm 1\} \right\}$
- Example
  - If G is a group, and $g \in G$, then $\langle \{g\} \rangle = \langle g \rangle$
- Note
  - When G is **abelian** and $A \subseteq G$, then we have
  - $\langle \boldsymbol{A} \rangle = \left\{ \boldsymbol{a_1^{n_1} \dots a_m^{n_m}} \middle| \boldsymbol{n_i} \in \mathbb{Z}, \boldsymbol{a_i} \in \boldsymbol{A}, \boldsymbol{m} \in \mathbb{Z}_{\geq \mathbf{0}} \right\}$

Finitely Generated Group

- Definition
  - A group G is **finitely generated** if
  - There is a **finite subset** A of G s.t. $\langle \boldsymbol{A} \rangle = \boldsymbol{G}$
- Example 1
  - Cyclic groups are finitely generated
- Example 2
  - Finite groups are finitely generated
- Example 3
  - **If $\boldsymbol{G}, \boldsymbol{H}$ are finitely generated, then $\boldsymbol{G} \times \boldsymbol{H}$ is also finitely generated**

- For instance, $\mathbb{Z} \times \mathbb{Z}$ is finitely generated by $A = \{(1,0), (0,1)\}$
- In particular, **products of cyclic groups are finitely generated**
- Every finitely generated abelian group is a product of cyclic groups
- (This is called the Fundamental Theorem of Finite Abelian Groups)

- Example 4
  - **Every finitely generated subgroup of $\mathbb{Q}$ is cyclic.**
  - It follows that $\mathbb{Q}$ is not finitely generated, since $\mathbb{Q}$ is not cyclic ($\mathbb{Q} \ncong \mathbb{Z}$)
  - Suppose $H \leq \mathbb{Q}$, and $H = \left\langle \frac{a_1}{b_1}, \frac{a_2}{b_2}, \dots, \frac{a_n}{b_n} \right\rangle$ where $a_i, b_i \in \mathbb{Z}$ and $b_i \neq 0$
  - Without loss of generality, assume $a_i \neq 0$
  - Let $S \coloneqq \left\{ x \in \mathbb{Z}_{>0} \middle| \frac{x}{b_1 b_2 \dots b_n} \in H \right\}$
    - $S \neq \emptyset$, since $\pm \frac{a_1 a_2 \dots a_n}{b_1 b_2 \dots b_n} \in H$
    - Applying the Well-Ordering Principle
    - We can choose a minimum element $e \in S$
  - Claim: $H = \left\langle \frac{e}{b_1 b_2 \dots b_n} \right\rangle$
    - Notice that $H = \left\{ c_1 \frac{a_1}{b_1} + c_2 \frac{a_2}{b_2} + \dots + c_n \frac{a_n}{b_n} \middle| c_i \in \mathbb{Z} \right\}$
    - So we only need to check that $\frac{a_i}{b_i} \in \left\langle \frac{e}{b_1 b_2 \dots b_n} \right\rangle \ \forall i$
    - Let i be fixed
    - Set $z \coloneqq b_1 \dots b_{i-1} a_i b_{i+1} \dots b_n$
    - So $\frac{a_i}{b_i} = \frac{z}{b_1 b_2 \dots b_n}$
    - Choose $q, r \in \mathbb{Z}$ s.t $z = qe + r, 0 \leq r < e$
    - $\frac{z}{b_1 b_2 \dots b_n} - q \left(\frac{e}{b_1 b_2 \dots b_n} \right) = \frac{z - qe}{b_1 b_2 \dots b_n} \in H \Rightarrow \frac{r}{b_1 b_2 \dots b_n} \in H$
    - The minimality of e forces $r = 0$
    - This shows $e | z$
    - So $\frac{a_i}{b_i} = \frac{z}{b_1 b_2 \dots b_n} \in \left\langle \frac{e}{b_1 b_2 \dots b_n} \right\rangle$
    - Therefore $H = \left\langle \frac{e}{b_1 b_2 \dots b_n} \right\rangle$
  - So H is cyclic

Coset, Normal Subgroup

Wednesday, February 28, 2018 9:59 AM

Coset

- If G is a group, $H \leq G$, and $g \in G$
- $gH \coloneqq \{gh | h \in H\}$ is called a **left coset**
- $Hg \coloneqq \{hg | h \in H\}$ is called a **right coset**
- An element of a coset is called a **representative** of the coset

Proposition 22: Properties of Coset

- Let G be a group and $H \leq G$, then
- For $g_1, g_2 \in G$, $\boldsymbol{g_1 H = g_2 H \Leftrightarrow g_2^{-1} g_1 \in H}$
    - ($\Longrightarrow$) Choose $h \in H$ s.t. $g_1 = g_2 h$ (since $g_1 = g_1 \cdot 1 \in g_1 H = g_2 H$)
    - Therefore $g_2^{-1} g_1 = h \in H$
    - ($\Longleftarrow$) Choose $h \in H$ s.t. $g_1 = g_2 h$
    - $\forall h' \in H, g_1 h' = g_2 \underbrace{hh'}_{\in H} \in g_2 H \Rightarrow g_1 H \subseteq g_2 H$
    - $\forall h' \in H, g_2 h' = g_1 \underbrace{h^{-1} h'}_{\in H} \in g_1 H \Rightarrow g_2 H \subseteq g_1 H$
    - Therefore $g_1 H = g_2 H$
- The relation $\sim$ on G given by $g_1 \sim g_2$ iff $g_1 \in g_2 H$ is an equivalence relation
    - Reflexive
        - If $g \in G$, then $g = g \cdot 1 \in gH$
        - So $g \sim g$
    - Symmetric
        - If $g_1, g_2 \in G$, and $g_1 \sim g_2$ i.e. $g_1 \in g_2 H$, then
        - $g_1 = g_2 h$ for some $h \in H$
        - Thus $g_1 h^{-1} = g_2$
        - So $g_2 \in g_1 H$, which means $g_2 \sim g_1$
    - Transitive
        - Suppose $g_1 \sim g_2$ and $g_2 \sim g_3$
        - This means $g_1 \in g_2 H$ and $g_2 \in g_3 H$
        - Choose $h_1, h_2 \in H$ s.t. $g_1 = g_2 h$, and $g_2 = g_3 h$
        - Then $g_1 = g_3 h_2 h_1 \in g_3 H$
        - So $g_1 \sim g_2$
- In particular, left/right cosets are either equal or disjoint
    - Suppose $g_1, g_2 \in G$, and $z \in g_1 H \cap g_2 H$
    - Suppose $x \in g_1 H$, then $x \sim g_1 \sim z \sim g_2$

- So $x \in g_2H$
- This implies that $g_1H \subseteq g_2H$
- To get $g_2H \subseteq g_1H$, exchange the roles of g_1 and g_2
- Therefore $g_1H = g_2H$

- Example 1
  - Let G be a group, $H \leq G$
  - **If $\boldsymbol{h \in H}$, then $\boldsymbol{hH = H}$**
  - Let $h' \in H$, then $h' = h(h^{-1}h') \in hH$
  - Thus $H \subseteq hH$
  - By closure under the operation, $hH \subseteq H$
  - Therefore $hH = H$
- Example 2
  - Let $G = \mathbb{Z}/6\mathbb{Z}$, and $H =$ unique subgroup of $\mathbb{Z}/6\mathbb{Z}$ of order 2
  - $H = \{\bar{0}, \bar{3}\} \leq \mathbb{Z}/6\mathbb{Z}$
  - Left cosets of H in G
    - $\bar{0} + \{\bar{0}, \bar{3}\} = \{\bar{0}, \bar{3}\}$
    - $\bar{1} + \{\bar{0}, \bar{3}\} = \{\bar{1}, \bar{4}\}$
    - $\bar{2} + \{\bar{0}, \bar{3}\} = \{\bar{2}, \bar{5}\}$
    - $\bar{3} + \{\bar{0}, \bar{3}\} = \{\bar{0}, \bar{3}\}$
    - $\bar{4} + \{\bar{0}, \bar{3}\} = \{\bar{1}, \bar{4}\}$
    - $\bar{5} + \{\bar{0}, \bar{3}\} = \{\bar{2}, \bar{5}\}$
  - Note
    - $|G| = 6$, $|H| = 2$, and H has 3 distinct cosets $(2 \cdot 3 = 6)$
    - If G is a finite group, and $H \leq G$, then $|H| \big| |G|$, and
    - H has $\dfrac{|G|}{|H|}$ distinct left (or right) cosets in G
    - This is called the Lagrange's Theorem

Normal Subgroup

- Definition
  - Let G be a group, $N \leq G$
  - N is a **normal subgroup** if $\boldsymbol{gng^{-1} \in N, \forall n \in N, \forall g \in G}$
  - In other words, **$\boldsymbol{N}$ is closed under conjugation**
  - If $N \leq G$ is normal, we write $N \trianglelefteq G$
- Example 1
  - **If $\boldsymbol{G}$ is abelian, every subgroup of $\boldsymbol{G}$ is normal**
  - Suppose $H \leq G$

- Let $h \in H$ and $g \in G$
- Then $ghg^{-1} = hgg^{-1} = h \in H$

- Example 2
  - Let $G = S_3, H = \langle(1\ 2)\rangle$
  - Suppose $g = (1\ 2\ 3) \in G$, and $h = (1\ 2) \in H$
  - Then $ghg^{-1} = (1\ 2\ 3)(1\ 2)(1\ 2\ 3)^{-1} = (1\ 2\ 3)(1\ 2)(1\ 3\ 2) = (2\ 3) \notin H$
  - Therefore $H \ntrianglelefteq G$
- Example 3
  - $\langle(1\ 2\ 3)\rangle$ in S_3 is normal
- Note
  - In $GL_n(\mathbb{R})$, conjugation amounts to changing basis
  - Let $G = GL_n(\mathbb{R})$
  - Let $P, A \in G$, then PAP^{-1} is change of basis matrix
- Example 4
  - Let $f: G \to H$ be a **homomorphism**, then **ker** $\boldsymbol{f \trianglelefteq G}$
  - $\ker f \leq G$
    - $\ker f \neq \emptyset$, since $f(1_G) = 1_H$
    - If $k_1, k_2 \in \ker f$
    - $f(k_1 k_2^{-1}) = f(k_1) f(k_2)^{-1} = 1_H$
    - Thus $k_1 k_2^{-1} \in \ker f$
    - Therefore $\ker f \leq G$
  - $\ker f$ is normal
    - Let $g \in G, k \in \ker f$
    - $f(gkg^{-1}) = f(g)f(k)f(g)^{-1} = f(g)f(g)^{-1} = 1_H$
    - $\Rightarrow gkg^{-1} \in \ker f$

Proposition 23: Criteria for a Subgroup to be Normal

- Statement
  - Let N be a subgroup of a group G
  - $\boldsymbol{N \trianglelefteq G \Leftrightarrow gN = Ng, \forall g \in G}$
- Proof ($\Longrightarrow$)
  - Suppose $N \trianglelefteq G$
  - Let $g \in G, n \in N$
  - $gn = gn(g^{-1}g) = \underbrace{gng^{-1}}_{\in N} g \in Ng \Rightarrow gN \subseteq Ng$
  - $ng = (gg^{-1})ng = g\, \underbrace{g^{-1}ng}_{\in N} \in gN \Rightarrow Ng \subseteq gN$
  - Therefore $gN = Ng$

- Proof ($\Longleftarrow$)
    - Suppose $gN = Ng, \forall g \in G$
    - Let $g \in G, n \in N$
    - We must show that $gng^{-1} \in N$
    - Choose $n' \in N$ s.t. $gn = n'g$
    - Then $gng^{-1} = n' \in N$
    - Therefore $N \trianglelefteq G$

Quotient Group, Index, Lagrange's Theorem

Monday, March 5, 2018 9:41 AM

Proposition 24: Quotient Group

- Statement
    - Let G be a group, $N \trianglelefteq G$
    - The **set of left costs of N** is a group under the operation
        - $(\boldsymbol{g_1 N})(\boldsymbol{g_2 N}) = \boldsymbol{g_1 g_2 N}$
    - This group is denoted as $\boldsymbol{G/N}$ (say "G mod N")
    - We call this group **quotient group** or factor group
- Proof
    - Check $G/N \times G/N \to G/N$, given by $(g_1 N, g_2 N) \mapsto g_1 g_2 N$ is well-defined
        - Suppose $g_1 N = g_1' N$, and $g_2 N = g_2' N$
            - $g_1 N = g_1' N \Leftrightarrow (g_1{}')^{-1} g_1 \in N$
            - $g_2 N = g_2' N \Leftrightarrow (g_2{}')^{-1} g_2 \in N$
        - $(g_1' g_2')^{-1} g_1 g_2 \in N$
            - $(g_1' g_2')^{-1} g_1 g_2$
            - $= (g_2')^{-1} (g_1')^{-1} g_1 g_2$
            - $= (g_2')^{-1} (g_1')^{-1} g_1 [g_2' (g_2')^{-1}] g_2$
            - $= (g_2')^{-1} \underbrace{(g_1')^{-1} g_1}_{\in N} g_2' \underbrace{(g_2')^{-1} g_2}_{\in N}$
            - $= \underbrace{(g_2')^{-1} (g_1')^{-1} g_1 g_2'}_{\in N} \underbrace{(g_2')^{-1} g_2}_{\in N} \in N$
        - Therefore $g_1 g_2 N = g_1' g_2' N$
        - So the operation is well-defined
    - Identity
        - $1 \cdot N = N$
    - Inverse
        - $(gN)^{-1} = g^{-1} N$
        - Since $(gN)(g^{-1} N) = g g^{-1} N = N$
    - Associativity
        - $(g_1 N g_2 N)(g_3 N)$
        - $= (g_1 g_2 N)(g_3 N)$
        - $= g_1 g_2 g_3 N$
        - $= g_1 N (g_2 g_3 N)$
        - $= g_1 N (g_2 N g_3 N)$
- Note

- If $N \trianglelefteq G$, then there is a surjective homomorphism
    - $f: G \to G/N$ given by $g \mapsto gN$ with $\ker f = N$
    - Since $f(g) = 1_{G/N} \Leftrightarrow gN = N \Leftrightarrow g \in N$
- This shows that, if $H \leq G$, then
    - $H \trianglelefteq G \Leftrightarrow H$ is the kernel of a homomorphism from G to some other group
- Example 1
    - Let H be a subgroup of $\mathbb{Z}$
    - Then $H \trianglelefteq \mathbb{Z}$ since $\mathbb{Z}$ is abelian
    - Since $\mathbb{Z}$ is cyclic, H is also cyclic
    - So we can write $H = \langle n \rangle$
    - There is isomorphism
        - $\mathbb{Z}/\langle n \rangle \to \mathbb{Z}/n\mathbb{Z}$
        - $a + \langle n \rangle \to \bar{a}$
- Example 2
    - If G is a group, then $\{1_G\} \trianglelefteq G$ and $G \trianglelefteq G$
        - $G/\{1_G\} \cong G$
        - $G/G \cong *$, where $*$ is the trivial group of order 1
    - Intuition: The bigger the subgroup, the smaller the quotient

Index of a Subgroup

- Definition
    - If G is a group, and $H \leq G$, then
    - The **index** of H is the **number of distinct left cosets** of H in G
    - Denote the index by $[G: H]$
- Note
    - If $N \trianglelefteq G$, then $[G: N] = |G/N|$
- Example
    - $[\mathbb{Z}: \langle n \rangle] = |\mathbb{Z}/n\mathbb{Z}| = n$

Theorem 25: Lagrange's Theorem

- Statement
    - If G is finite group, and $H \leq G$, then $\boldsymbol{|G| = |H| \cdot [G: H]}$
    - In particular, $\boldsymbol{|H| \,\big|\, |G|}$
- Notice
    - If in the setting of Lagrange's Theorem, $H \trianglelefteq G$, then
    - $|G| = |H| \cdot |G/H| \Rightarrow |G/H| = \dfrac{|G|}{|H|}$
- Proof

- Let $n \coloneqq |H|$, and $k \coloneqq [G: H]$
- Cosets partition G
  - Let $g_1, \dots, g_k$ be the representatives of the distinct cosets of H in G
  - (In other words: if $g \in G$, then $gH \in \{g_1 H, g_2 H, \dots, g_k H\}$)
  - By proposition 22, left costs are either equal or disjoint
  - So, $G = g_1 H \cup g_2 H \cup \cdots \cup g_k H$
- Cosets have the same size
  - Let $g \in G$, then there is a function $f: H \to gH$ given by $h \mapsto gh$
  - f is certainly surjective
  - f is also injective since if $gh_1 = gh_2$, then $h_1 = h_2$
  - Thus, $|gH| = |H|$
- Therefore $|G| = |g_1 H| + \cdots + |g_k H| = \underbrace{n + n + \cdots + n}_{k \text{ copies}} = kn = |H| \cdot [G: H]$

Lagrange's Theorem, Product of Subgroups

Wednesday, March 7, 2018 9:56 AM

Corollary 26: Group of Prime Order is Cyclic

- Statement
  - If G is a group, and $|\boldsymbol{G}|$ **is prime,** then G is **cyclic**
  - Hence, $G \cong \mathbb{Z}/p\mathbb{Z}$
- Proof
  - If $g \in G$, then $|g| = |\langle g \rangle|$
  - By Lagrange's Theorem, $|\langle g \rangle| \big| |G|$
  - Thus, $|g| \in \{1, |G|\}$
  - It follows that if $g \in G \setminus \{1\}$, then $|g| = |G|$
  - Therefore $\langle g \rangle = G$
  - i.e. G is cyclic

Groups of Small Order

Order	Property
2	Cyclic
3	Cyclic
4	Cyclic or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
5	Cyclic
6	Cyclic or S_3

Corollary 27: $g^{|G|} = 1$

- Statement
  - If G is a finite group, and $g \in G$, then $\boldsymbol{g^{|G|} = 1}$
- Proof
  - By Lagrange's Theorem, $|\langle g \rangle| \big| |G|$
  - Since $|g| = |\langle g \rangle|$, we have $|g| \big| |G|$
  - Thus, $g^{|G|} = g^{|g|m}$ for some integer m
  - Therefore $g^{|G|} = \left(g^{|g|}\right)^m = 1$

Corollary 28: The Fundamental Theorem of Cyclic Groups

- Statement
  - If G is a **finite cyclic group**, then there is a **bijection**
  - $\{$**positive divisors of** $|\boldsymbol{G}|\} \leftrightarrow \{$**subgroups of G**$\}$
- Proof

- ($\Longrightarrow$) Divisor m of $|G| \mapsto$ the unique subgroup G with order m
- ($\Longleftarrow$) Subgroup H of $G \mapsto |H|$

Product of Subgroups

- Let G be a group and $H, K \leq G$
- Define $\boldsymbol{HK} \coloneqq \{\boldsymbol{hk} | \boldsymbol{h} \in \boldsymbol{H}, \boldsymbol{k} \in \boldsymbol{K}\}$

Proposition 29: Order of Product of Subgroups

- Statement
  - If H, K are **finite subgroups** of a group G, then $|\boldsymbol{HK}| = \dfrac{|\boldsymbol{H}| \cdot |\boldsymbol{K}|}{|\boldsymbol{H} \cap \boldsymbol{K}|}$
- Proof
  - Notice that HK is the union of left cosets of K
    - $HK = \bigcup_{h \in H} hK$
  - In the proof of Lagrange's Theorem, we know that $|hK| = |K|$
  - We want to show that there are $\dfrac{|H|}{|H \cap K|}$ cosets of the form hK, where $h \in H$
  - Let $h_1, h_2 \in H$
    - $h_1 K = h_2 K$
    - $\Leftrightarrow h_2^{-1} h_1 \in K$
    - $\Leftrightarrow h_2^{-1} h_1 \in H \cap K$
    - $\Leftrightarrow h_1 (H \cap K) = h_2 (H \cap K)$
  - By Lanrange′s Theorem, the number of distinct cosets of the form $hK, h \in H$ is
    - $[H : H \cap K] = \dfrac{|H|}{|H \cap K|}$
  - Thus HK consists of $\dfrac{|H|}{|H \cap K|}$ distinct cosets of K
  - Therefore, $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$
- Note: ***HK* is not always a subgroup**
  - Let $G = S_3, H = \langle (1\ 2) \rangle, K = \langle (1\ 3) \rangle$
  - $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|} = \dfrac{2 \times 2}{1} = 4$
  - But $|HK|$ is not a divisor of S_3
  - By Lagrange's Theorem, HK is not a subgroup of S_3

Proposition 30: Permutable Subgroups

- Statement
  - If $H, K \leq G$, then $\boldsymbol{HK} \leq \boldsymbol{G} \Leftrightarrow \boldsymbol{HK} = \boldsymbol{KH}$
- Note

  - $\boldsymbol{HK = KH}$ **is not equivalent to** $\boldsymbol{hk = kh, \forall h \in H, k \in K}$
  - It implies that every product hk is of the form $k'h'$ and conversely
- Proof ($\Longrightarrow$)
  - $KH \subseteq HK$
    - This is true because $H \leq HK, K \leq HK$
  - $HK \subseteq KH$
    - Let $hk \in HK$
    - Set $a \coloneqq (hk)^{-1}$, then $a \in HK$
    - So, $a = h'k'$ for some $h' \in H, k' \in K$
    - Then $hk = a^{-1} = (h'k')^{-1} = (k')^{-1}(h')^{-1} \in KH$
- Proof ($\Longleftarrow$)
  - $HK \neq \emptyset$, since $1 \cdot 1 = 1 \in HK$
  - Let $hk, h'k' \in HK$
  - We must show that $hk(h'k')^{-1} \in HK$
  - $hk(h'k')^{-1} = h\,\underbrace{k(k')^{-1}(h')^{-1}}_{\in KH}$
  - Choose $h'' \in H, k'' \in K$ s. t. $\underbrace{k(k')^{-1}(h')^{-1}}_{\in KH} = \underbrace{h''k''}_{\in HK}$
  - Then $hk(h'k')^{-1} = h\,\underbrace{h''k''}_{\in HK} = \underbrace{hh''}_{\in H}\,\underbrace{k''}_{\in K} \in HK$
  - Therefore $HK \leq G$
- Example
  - Let $G = S_3, H = \langle(1\ 2)\rangle, K = \langle(1\ 3)\rangle$
  - $HK = \{(1), (1\ 2), (1\ 3), (1\ 3\ 2)\}$
  - $KH = \{(1), (1\ 2), (1\ 3), (1\ 2\ 3)\}$
  - Thus $HK \neq KH$
  - Therefore HK is not a subgroup of S_3

Corollary 31: Product of Subgroup and Normal Subgroup

- Statement
  - If $H, K \leq G$, and either $\boldsymbol{H}$ **or** $\boldsymbol{K}$ **is normal in** $\boldsymbol{G}$, then $\boldsymbol{HK \leq G}$
- Proof
  - Without loss of generality, assume $K \trianglelefteq G$
  - Let $h \in H, k \in K$
  - $hk = hk(h^{-1}h) = \underbrace{hkh^{-1}}_{\in K}\,h \in KH \Rightarrow HK \leq KH$
  - $kh = (hh^{-1})kh = h\,\underbrace{h^{-1}kh}_{\in K} \in HK \Rightarrow KH \leq HK$
  - Therefore $HK = KH$

The First & Second Isomorphism Theorems

Friday, March 9, 2018 10:06 AM

Theorem 32: The First Isomorphism Theorem

- Statement
  - If $f: G \to H$ is a **homomorphism**, then f induces an isomorphism
    - $\boldsymbol{\bar{f}: {}^{G}\!/_{\ker f} \xrightarrow{\cong} \operatorname{im}(f)}$
    - $g \ker f \mapsto f(g)$
- Intuition
  - This is an analogue of the Rank-Nullity Theorem in Linear Algebra
  - Given vector space V, W and a linear transformation $A: V \to W$
  - ${}^{V}\!/_{\ker A} \cong \operatorname{im}(A)$
  - $\Rightarrow \dim\left({}^{V}\!/_{\ker A}\right) = \dim\big(\operatorname{im}(A)\big)$
  - $\Rightarrow \dim V - \text{nullity } A = \text{rank } A$
- Proof
  - $\bar{f}$ is well-defined and injective
    - Let $g_1, g_2 \in G$
    - $g_1 \ker f = g_2 \ker f$
    - $\Leftrightarrow g_2^{-1} g_1 \in \ker f$
    - $\Leftrightarrow f(g_2^{-1} g_1) = 1$
    - $\Leftrightarrow f(g_2)^{-1} f(g_1) = 1$
    - $\Leftrightarrow f(g_1) = f(g_2)$
    - $\Leftrightarrow \bar{f}(g_1 \ker f) = \bar{f}(g_2 \ker f)$
    - Thus f is well-defined and injective
  - $\bar{f}$ is surjective
    - Let $h \in \operatorname{im} f$
    - Choose $g \in G$ s.t. $f(g) = h$
    - Then $\bar{f}(g \ker f) = h$
  - $\bar{f}$ is a homomorphism
    - If $g_1 \ker f, g_2 \ker f \in {}^{G}\!/_{\ker f}$
    - $\bar{f}(g_1 \ker f \cdot g_2 \ker f)$
    - $= \bar{f}(g_1 g_2 \ker f)$
    - $= f(g_1 g_2)$
    - $= f(g_1) f(g_2)$

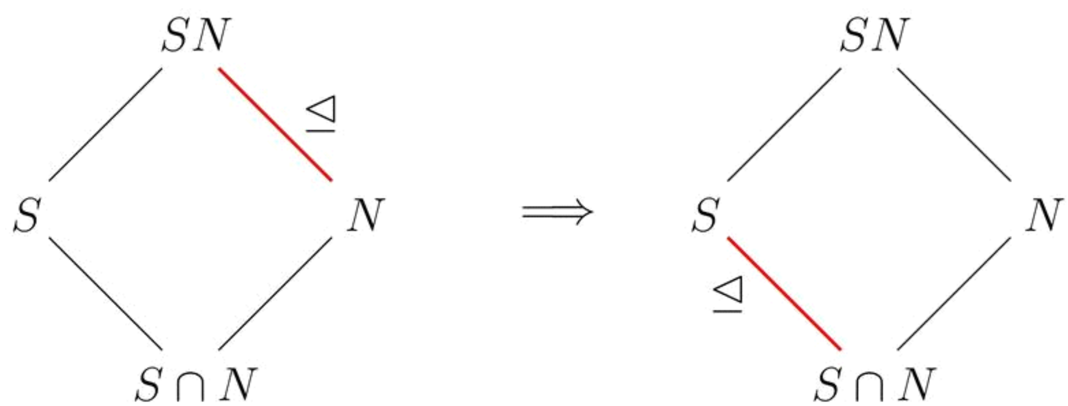
        - $= \bar{f}(g_1 \ker f)\bar{f}(g_2 \ker f)$

Corollary 33: Order of Kernel and Image

- Statement
  - $[\boldsymbol{G}: \mathbf{ker}\, \boldsymbol{f}] = |\mathbf{im}\, \boldsymbol{f}|$
- Example
  - Let $m, n \in \mathbb{Z}$ be coprimes
  - Then any homomorphism $f: \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is trivial
  - i.e. $f(\bar{n}) = \bar{0}, \forall \bar{n} \in \mathbb{Z}/m\mathbb{Z}$
- Proof
  - Let f be such a homomorphism
  - By the First Isomorphism Theorem, $\left| {}^{\mathbb{Z}/n\mathbb{Z}}\!/_{ker\, f} \right| = |\mathrm{im}\, f|$
  - So $\dfrac{n}{|\ker f|} = |\mathrm{im}\, f|$, where
    - $\dfrac{n}{|\ker f|}$ is a divisor of n, and
    - $|\mathrm{im}\, f|$ is a divisor of m, by Lagrange's Theorem
  - Thus, $|\mathrm{im}\, f| = 1$, so $\mathrm{im}\, f = \{\bar{0}\}$
- Note
  - The same proof tells us that
  - If G, H are finite groups such that $(|\boldsymbol{G}|, |\boldsymbol{H}|) = \mathbf{1}$, then
  - All **homomorphism** between them are **trivial**

Theorem 34: The Second Isomorphism Theorem

- Statement
  - If $\boldsymbol{A} \leq \boldsymbol{G}$, and $\boldsymbol{B} \trianglelefteq \boldsymbol{G}$
  - Then $\boldsymbol{A} \cap \boldsymbol{B} \trianglelefteq \boldsymbol{A}$, and ${}^{\boldsymbol{AB}}\!/_{\boldsymbol{B}} \cong {}^{\boldsymbol{A}}\!/_{\boldsymbol{A} \cap \boldsymbol{B}}$
- Intuition



$$\frac{SN}{N} \cong \frac{S}{S \cap N}$$

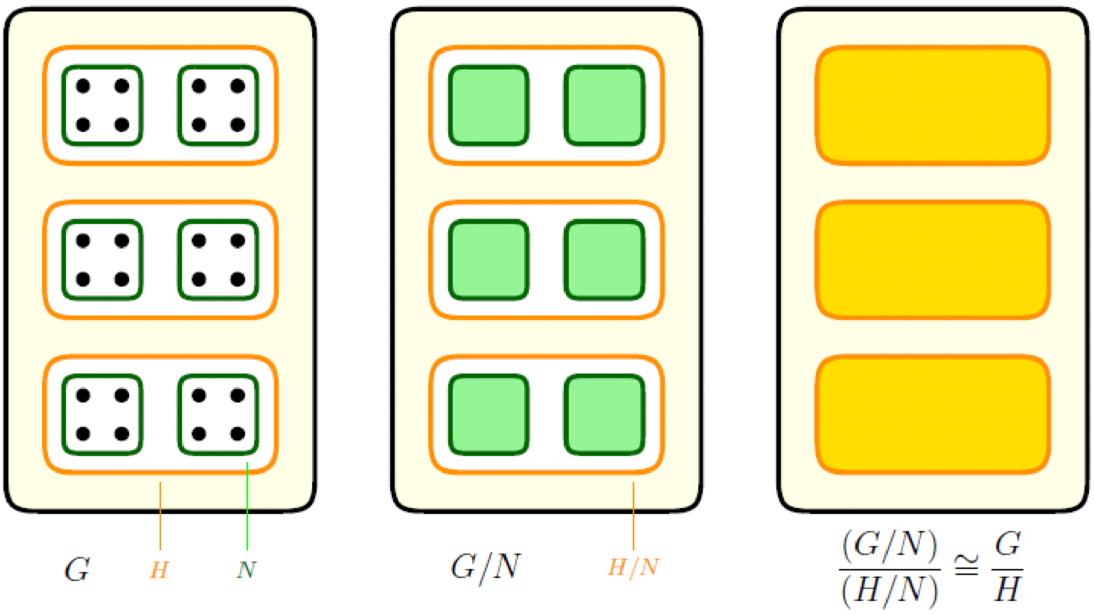
- Note
  - $B \trianglelefteq AB \leq G$ by Corollary 31
  - So, ${}^{AB}/_{B}$ make sense
- Proof
  - We have homomorphisms
    - $\alpha: A \to AB$ given by $a \mapsto a$
    - $\beta: AB \to {}^{AB}/_{B}$ given by $x \mapsto xB$
  - Let $f \coloneqq \beta \circ \alpha$, then
    - $f: A \to {}^{AB}/_{B}$, where $a \mapsto aB$
  - f is certainly surjective
  - Compute $\ker f$
    - Let $a \in A$
    - $f(a) = 1_{{}^{AB}/_{B}} \Leftrightarrow aB = B \Leftrightarrow a \in B$
    - Thus, $\ker f = A \cap B \trianglelefteq A$
  - The First Isomorphism Theorem gives an isomorphism
    - $\bar{f}: {}^{A}/_{A \cap B} \xrightarrow{\cong} {}^{AB}/_{B}$

The Third & Fourth Isomorphism Theorem

Monday, March 12, 2018 9:57 AM

Theorem 35: The Third Isomorphism Theorem

- Statement
  - Let G be a group, and $\boldsymbol{H, K \trianglelefteq G}$, where $\boldsymbol{H \leq K}$
  - Then $\boldsymbol{K/H \trianglelefteq G/H}$, and $\boldsymbol{{}^{G/H}\!/_{K/H} \cong G/K}$
- Note
  - $K/H \coloneqq \{gH \in G/H | g \in K\}$
  - Also, $H \trianglelefteq G \Rightarrow H \trianglelefteq K$, and so K/H makes sense
- Intuition



- Proof
  - $K/H \leq G/H$
    - Certainly $K/H \neq \emptyset$ since $K \neq \emptyset$
    - Let $k_1H, k_2H \in K/H$
    - Then $k_1H(k_2H)^{-1} = k_1Hk_2^{-1}H = k_1k_2^{-1}H \in K/H$
  - $K/H \trianglelefteq G/H$
    - Let $kH \in K/H$ and $gH \in G/H$
    - Then $gHkH(gH)^{-1} = \underbrace{gkg^{-1}}_{\in K}H \in K/H$
  - Define a homomorphism $\alpha: G/H \to G/K$ given by $gH \mapsto gK$
  - α is well-defined
    - Suppose $g_1H = g_2H$

        - Then $g_2^{-1}g_1 \in H$
        - Since $H \leq K$, we have $g_2^{-1}g_1 \in K$
        - So $g_1K = g_2K$
        - i.e. $\alpha(g_1H) = \alpha(g_1H)$
    - α is surjective
        - If $gK \in G/K$, then $\alpha(gH) = gK$
    - Compute $\ker \alpha$
        - $\ker \alpha = \{gH \in G/H | gK = K\} = \{gH \in G/H | g \in K\} = K/H$
    - By First Isomorphism Theorem
        - ${}^{G/H}\!/_{K/H} = {}^{G/H}\!/_{\ker \alpha} \cong \operatorname{im} \alpha = G/K$
- Example
    - Let $G = \mathbb{Z}, K = \mathbb{Z}/2\mathbb{Z}, H = \mathbb{Z}/4\mathbb{Z}$
    - Then the Third Isomorphism Theorem tells us that
    - The map $f: \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ given by $\bar{a} \to \bar{a}$ is well-defined and surjective
    - $\ker f = 2\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{2}\} \subseteq \mathbb{Z}/4\mathbb{Z}$
    - Therefore, ${}^{\mathbb{Z}/4\mathbb{Z}}\!/_{2\mathbb{Z}/4\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z}$

Proposition 36: Criterion for Defining Homomorphism on Quotient

- Statement
    - Let G, H be groups, and $N \trianglelefteq G$
    - A homomorphism $\alpha: G \to H$ **induces a homomorphism**
        - $\bar{\alpha}: G/N \to H$ given by $gN \mapsto \alpha(g)$
    - If and only if $\boldsymbol{N \leq \ker \alpha}$
- Proof ($\Longrightarrow$)
    - Let $n \in N$, then
        - $\bar{\alpha}(nN) = 1_H$ since homomorphisms preserve identities
        - $\bar{\alpha}(nN) = \alpha(n)$, by definition of $\bar{\alpha}$
    - Thus, $\alpha(n) = 1_H$
    - i.e. $N \subseteq \ker \alpha$
    - And N certainly meets the Subgroup Criteria
    - Therefore $N \leq \ker \alpha$
- Proof ($\Longleftarrow$)
    - $\bar{\alpha}: G/N \to H, gN \mapsto \alpha(g)$ is well-defined
        - Suppose $g_1N = g_2N$, we must check that $\alpha(g_1) = \alpha(g_2)$
        - $g_1N = g_2N$
        - $\Leftrightarrow g_2^{-1}g_1 \in N$
        - $\Rightarrow \alpha(g_2^{-1}g_1) = 1_H$ (since $N \leq \ker \alpha$)

        - $\Leftrightarrow \alpha(g_2)^{-1}\alpha(g_1) = 1_H$
        - $\Leftrightarrow \alpha(g_2) = \alpha(g_1)$
    - $\bar{\alpha}$ is a homomorphism
        - $\bar{\alpha}(g_1Hg_2H) = \bar{\alpha}(g_1g_2H) = \alpha(g_1g_2) = \alpha(g_1)\alpha(g_2) = \bar{\alpha}(g_1H)\bar{\alpha}(g_2H)$

Theorem 37: The Correspondence Theorem

- Statement
    - Let G be a group, and let $N \trianglelefteq G$, then there is a bijection
    - $\{\textbf{subgroups of } \boldsymbol{G/N}\} \underset{F'}{\overset{F}{\rightleftarrows}} \{\textbf{subgroups of } \boldsymbol{G} \textbf{ containing } \boldsymbol{N}\}$
- Proof
    - Define
        - $F(H) = \{g \in G | gN \in H\}$
        - $F'(K) = K/N \coloneqq \{gN \in G/N | g \in K\}$
    - $F(H)$ is a subgroup of G containing N
        - If $n \in N$, then $nN = id_{G/N} \in H$
        - Thus, $N \subseteq F(H)$
        - This also shows that $F(H) \neq \emptyset$
        - If $g_1, g_2 \in F(H)$, then
            - $g_1N, g_2N \in H$
            - $\Rightarrow g_1N(g_2N)^{-1} = g_1g_2^{-1}N \in H$
            - $\Rightarrow g_1g_2^{-1} \in F(H)$
    - $F \circ F'$ and $F' \circ F$ are the identity maps
        - $(F \circ F')(K) = F(K/N) = \{g \in G | gN \in K/N\} = K$
        - $(F' \circ F)(H) = F'(\{g | gN \in H\}) = {}^{\{g|gN \in H\}}/_{N} = H$

Transposition, Sign of Permutation

Wednesday, March 14, 2018 9:56 AM

Transposition

- Fix n to be a positive integer
- A 2-cycle $(i\ j)$ in S_n is a **transposition**

Proposition 38: Transposition Decomposition of Permutation

- Statement
    - Every $\boldsymbol{\sigma} \in \boldsymbol{S_n}$ can be written as a **product of transposition**
- Example
    - $(1\ 5\ 3\ 2\ 4) = (1\ 4)(1\ 2)(1\ 3)(1\ 5)$
    - $(3\ 5) = (1\ 5)(1\ 3)(1\ 5)$
- Proof
    - Fix $\sigma \in S_n$
    - We may assume that σ is a cycle $\sigma = (a_1\ a_2\ \dots\ a_t)$
    - By induction on t, we claim
        - $(a_1\ a_2\ \dots\ a_t) = (a_1\ a_t)(a_1\ a_{t-1}) \dots (a_1\ a_2)$
    - Base case: $t = 2$
        - $(a_1\ a_2) = (a_1\ a_2)$
    - Inductive step: $t > 2$
        - $(a_1\ a_t)(a_1\ a_{t-1}) \dots (a_1\ a_2)$
        - $= (a_1\ a_t)(a_1\ a_2\ \dots\ a_{t-1})$
        - $= (a_1\ a_2\ \dots\ a_{t-1}\ a_t)$
- Note
    - S_n is generated by $\{(1\ 2), (1\ 3), \dots, (1\ n)\}$

Sign of Permutation ϵ (Transposition Definition)

- Intuition
    - The **numbers of transposition** used to write some $\sigma \in S_n$
    - is not well-defined, but it is **always either even or odd**
- Definition
    - Let $\epsilon: S_n \to \mathbb{Z}/2\mathbb{Z}$

$$\sigma \mapsto \begin{cases} \bar{0} & \sigma \text{ is a product of even number of transposition} \\ \bar{1} & \sigma \text{ is a product of odd number of transposition} \end{cases}$$

    - Then ϵ is a group homomorphism
    - $A_n \coloneqq \ker \epsilon$ is the **alternating group of degree $\boldsymbol{n}$**

Sign of Permutation ϵ' (Auxiliary Polynomial Definition)

- Auxiliary Polynomial Δ
  - $\Delta \coloneqq \prod_{1\le i<j\le n} (x_i - x_j)$
  - For $\sigma \in S_n$, define $\sigma(\Delta) \coloneqq \prod_{1\le i<j\le n} (x_{\sigma(i)} - x_{\sigma(j)})$
  - Then $\sigma(\Delta)$ is always either Δ or $-\Delta$
- Example
  - Let $n = 4$ and $\sigma = (1\ 2\ 3\ 4)$
  - $\Delta = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$
  - $\sigma(\Delta) = (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_4 - x_1) = -\Delta$
- Definition
  - Let $\epsilon' : S_n \to \mathbb{Z}/2\mathbb{Z}$

$$\sigma \mapsto \begin{cases} \bar{0} & \sigma(\Delta) = \Delta \\ \bar{1} & \sigma(\Delta) = -\Delta \end{cases}$$

  - $\epsilon'(\sigma)$ is the **sign** of σ, often denoted as $\operatorname{sgn} \sigma$
  - σ is **even** if $\epsilon'(\sigma) = \bar{0}$
  - σ is **odd** if $\epsilon'(\sigma) = \bar{1}$

Proposition 39: ϵ' is a Group Homomorphism

- Statement
  - $\boldsymbol{\epsilon'}$ is a group **homomorphism**
- Example
  - Let $\sigma = (1\ 2), \tau = (1\ 2\ 3) \Rightarrow \tau\sigma = (1\ 3)$
  - Let $\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$
    - $\sigma(\Delta) = (x_2 - x_1)(x_1 - x_3)(x_2 - x_3) = -\Delta$
    - $\tau(\Delta) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = (-1)^2\Delta = \Delta$
    - $(\tau\sigma)(\Delta) = (x_3 - x_2)(x_3 - x_1)(x_2 - x_1) = (-1)^3\Delta = -\Delta$
  - $\epsilon'(\tau\sigma) = \epsilon'(\tau)\epsilon'(\sigma)$, since
    - $\epsilon'(\tau\sigma) = \bar{1}$
    - $\epsilon'(\tau)\epsilon'(\sigma) = \bar{0} + \bar{1} = \bar{1}$
- Proof
  - Fix $\sigma, \tau \in S_n$
  - Let $\Delta \coloneqq \prod_{1\le i<j\le n} (x_i - x_j)$, then
    - $\tau(\Delta) = \prod_{1\le i<j\le n} (x_{\tau(i)} - x_{\tau(j)})$

    - $\sigma(\Delta) = \prod_{1 \le i < j \le n} \left(x_{\sigma(i)} - x_{\sigma(j)}\right)$
    - $(\tau\sigma)(\Delta) = \prod_{1 \le i < j \le n} \left(x_{(\tau\sigma)(i)} - x_{(\tau\sigma)(j)}\right)$
  - Suppose $\sigma(\Delta)$ has k "reversed factor" (i.e. factors $\left(x_j - x_i\right)$, where $i < j$), then
    - $(\tau\sigma)(\Delta)$
    - $= \prod_{1 \le i < j \le n} \left(x_{\tau(\sigma(i))} - x_{\tau(\sigma(j))}\right)$
    - $= (-1)^k \prod_{1 \le i < j \le n} \left(x_{\tau(i)} - x_{\tau(j)}\right)$
    - $= (-1)^k \tau(\Delta)$
    - $= \sigma(\Delta)\tau(\Delta)$
  - Therefore $\epsilon'(\tau\sigma) = \epsilon'(\tau)\epsilon'(\sigma)$

Homework 6

Friday, March 16, 2018 9:51 AM

Homework 6 Question 1

- Statement
  - Suppose $A, B \trianglelefteq H, AB = H$
  - Then there is an **isomorphism** $\boldsymbol{H/_{A \cap B}} \xrightarrow{\cong} \boldsymbol{(H/_A) \times (H/_B)}$
- Proof
  - Define a map
    - $f: H \to (H/_A) \times (H/_B)$
      $h \mapsto (hA, hB)$
  - Check f is a homomorphism
    - $f(h_1 h_2)$
    - $= (h_1 h_2 A, h_1 h_2 B)$
    - $= (h_1 A h_2 A, h_1 B h_2 B)$
    - $= (h_1 A, h_1 B)(h_2 A, h_2 B)$
    - $= f(h_1) f(h_2)$
  - Compute $\ker f$
    - Let $h \in \ker f$
    - $\Leftrightarrow f(h) = (1_{H/A}, 1_{H/B}) = (A, B)$
    - $\Leftrightarrow h \in A$ and $h \in B$
    - $\Leftrightarrow h \in A \cap B$
    - Therefore $\ker f = A \cap B$
  - Prove surjectivity
    - Let $(h_1 A, h_2 B) \in (H/_A) \times (H/_B)$
    - Choose $a_1, a_2 \in A, b_1, b_2 \in B$ s.t.
      - $h_1 = a_1 b_1$
      - $h_2 = a_2 b_2$
    - Then
      - $h_1 A = A h_1 = A a_1 b_1 = A b_1$
      - $h_2 B = a_2 b_2 B = a_2 B$
    - $f(a_2 b_1) = (h_1 A, h_2 B)$
      - $f(a_2 b_1)$
      - $= (a_2 b_1 A, a_2 b_1 B)$
      - $= (A a_2 b_1, a_2 B)$

- $= (Ab_1, a_2B)$
- $= (h_1A, h_2B)$
   - Therefore f is surjective
  - By the First Isomorphism theorem, there is an isomorphism
    - $\bar{f}: {}^{H}/_{\ker f} \to \operatorname{im} f$
    - $\Rightarrow \bar{f}: {}^{H}/_{A \cap B} \to \left({}^{H}/_{A}\right) \times \left({}^{H}/_{B}\right)$
- Note
  - Given two homomorphism $f_1: G \to H_1, f_2: G \to H_2$
  - Then their direct product
    - $f: G \to H_1 \times H_2$ given by $g \to \big(f_1(g), f_2(g)\big)$
  - is also a homomorphism

Homework 6 Question 2

- Statement
  - $\boldsymbol{G}$ **is abelian** $\Leftrightarrow$ $\boldsymbol{G/Z(G)}$ **is cyclic**
- Proof ($\Longrightarrow$)
  - Suppose G is abelian, then $G = Z(G)$
  - So $G/Z(G)$ is the trivial group
  - Therefore $G/Z(G)$ is cyclic
- Proof ($\Longleftarrow$)
  - Suppose $G/Z(G)$ is cyclic
  - Choose $gZ(G) \in G/Z(G)$ s.t. $\langle gZ(G)\rangle = G/Z(G)$
  - Let $x \in G$, then
    - $xZ(G) = g^kZ(G)$ for some $k \in \mathbb{Z}$, and $g^{-k}x \in Z(G)$
  - Let $a, b \in G$
  - Choose $k_1, k_2 \in \mathbb{Z}$ and $z_1, z_2 \in Z(G)$ s.t
    - $g^{-k_1}a = z_1$ and $g^{-k_2}b = z_2$
  - So, $a = g^{k_1}z_1, b = g^{k_2}z_2$
  - Then $ab = g^{k_1}z_1g^{k_2}z_2 = g^{k_2}z_2g^{k_1}z_1 = ba$

Homework 6 Question 4

- Statement
  - $G = \langle g\rangle$ is cyclic of order $n, d|n, d > 0$
  - Then ${}^{G}/_{\langle g^d\rangle}$ is cyclic of order d
- Proof: If H is a cyclic group and $A \leq H$, then H/A is also cyclic
  - Choose a generator $h \in H$
  - Then hA is a generator of H/A

- If $h'A \in H/A$
- Choose $k \in \mathbb{Z}$ s.t. $h' = h^k$
- Therefore $h'A = h^k A = (hA)^k$

- Proof
  - $\left|\langle g^d \rangle\right| = \frac{n}{(n,d)} = \frac{n}{d}$
  - By Lagrange's Theorem
  - $n = |G| = \left|\langle g^d \rangle\right| \cdot \left[G : \langle g^d \rangle\right] = \frac{n}{d}\left|{}^{G}/_{\langle g^d \rangle}\right|$
  - $\Rightarrow \left|{}^{G}/_{\langle g^d \rangle}\right| = d$

Sign of Permutation, A_n

Monday, March 19, 2018 9:50 AM

Recall

- $\epsilon: S_n \to \mathbb{Z}/2\mathbb{Z}$

$$\sigma \mapsto \begin{cases} \bar{0} & \sigma \text{ is a product of } \textbf{even} \text{ number of transposition} \\ \bar{1} & \sigma \text{ is a product of } \textbf{odd} \text{ number of transposition} \end{cases}$$

- $\epsilon': S_n \to \mathbb{Z}/2\mathbb{Z}$

$$\sigma \mapsto \begin{cases} \bar{0} & \sigma(\Delta) = \Delta \\ \bar{1} & \sigma(\Delta) = -\Delta \end{cases}$$

- $\Delta \coloneqq \prod_{1 \le i < j \le n} (x_i - x_j), \sigma(\Delta) \coloneqq \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)})$

Proposition 40: Sign of Transposition

- Statement
  - Let $n \in \mathbb{Z}_{>0}$
  - If $\tau \in S_n$ is **transposition**, then $\boldsymbol{\epsilon'(\tau) = \bar{1}}$
- Example
  - Suppose $n = 4, \tau = (1\ 2)$
  - $\Delta = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$
  - $\tau(\Delta) = (x_2 - x_1)(x_2 - x_3)(x_2 - x_4)(x_1 - x_3)(x_1 - x_4)(x_3 - x_4)$
  - $\tau(\Delta) = -\Delta \Rightarrow \epsilon'(\tau) = \bar{1}$
- Proof
  - Suppose $\tau = (1\ 2)$
    - Say $(x_i - x_j)$ is a factor of Δ
    - Then $\tau(i) > \tau(j) \Leftrightarrow i = 1, j = 2$
    - Thus $\tau(\Delta) = -\Delta$
    - So $\epsilon'(\tau) = \bar{1}$
  - Suppose $\tau = (i\ j), 1 \le i < j \le n$
    - Let $\lambda \in S_n$ denote the following permutation
      - $\lambda(1) = i$
      - $\lambda(2) = j$
      - $\lambda(i) = 1$
      - $\lambda(j) = 2$
      - $\lambda(k) = k, k \notin \{1,2,i,j\}$
    - $(i\ j) = \lambda(1\ 2)\lambda$

- $[\lambda(1\ 2)\lambda](i) = [\lambda(1\ 2)](1) = \lambda(2) = j$
- $[\lambda(1\ 2)\lambda](j) = [\lambda(1\ 2)](2) = \lambda(1) = i$
- Without loss of generality, assume $i, j \notin \{1,2\}$
- $[\lambda(1\ 2)\lambda](1) = [\lambda(1\ 2)](i) = \lambda(i) = 1$
- $[\lambda(1\ 2)\lambda](2) = [\lambda(1\ 2)](j) = \lambda(j) = 2$
- For $k \notin \{1,2,i,j\}$
- $[\lambda(1\ 2)\lambda](k) = [\lambda(1\ 2)](k) = \lambda(k) = k$

- We know ϵ' is a homomorphism, so
  - $\epsilon'(i\ j) = \epsilon'(\lambda(1\ 2)\lambda)$
  - $= \epsilon'(\lambda) + \epsilon'(1\ 2) + \epsilon'(\lambda)$
  - $= 2\epsilon'(\lambda) + \bar{1}$
  - $= \bar{0} + \bar{1} = \bar{1}$

Corollary 41: Equivalence of Two Definitions of Sign

- Statement
  - **ϵ is well-defined**, and **$\epsilon = \epsilon'$**
- Proof
  - Let $\sigma \in S_n$
  - Say $\sigma = \tau_1 \cdots \tau_k$ where τ_i is a transposition, then
  - $\epsilon'(\sigma) = \epsilon'(\tau_1) + \cdots + \epsilon'(\tau_k) = \underbrace{\bar{1} + \cdots + \bar{1}}_{k \text{ copies}} = \bar{k}$
  - If k is odd, then
    - σ cannot be written as a product of an even number of transpositions
  - So $\epsilon(\sigma) = \epsilon'(\sigma) = \bar{0}$ for σ with odd k, and vice verse
  - This shows ϵ is well-defined, and $\epsilon = \epsilon'$

Corollary 42: Surjectivity of ϵ

- Statement
  - If $n \geq 2$, then ϵ is **surjective**
- Proof
  - $\epsilon(1) = \bar{0}$, and $\epsilon(1\ 2) = \bar{1}$
  - Since $\mathbb{Z}/2\mathbb{Z}$ has only 2 elements, ϵ is surjective

Alternating Group

- Definition
  - The alternative group, denoted as A_n is the kernel of ϵ
  - That is, A_n contains of all **even permutations** in S_n
- Order of A_n
  - By the First Isomorphism Theorem

- We have an isomorphism $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$
- By Lagrange's Theorem, $|A_n|[S_n : A_n] = |S_n|$
- $\Rightarrow |\boldsymbol{A_n}| = \dfrac{|S_n|}{[S_n : A_n]} = \dfrac{\boldsymbol{n}!}{\mathbf{2}}$

- Note
  - We showed earlier that, if $(a_1 \dots a_t) \in S_n$,
  - $(a_1 \dots a_t) = \underbrace{(a_1\ a_t)(a_1\ a_{t-1}) \cdots (a_1\ a_2)}_{t-1 \text{ terms}}$
  - t-cycle is even when t is odd, and vise versa
  - Thus, $(\boldsymbol{a_1} \dots \boldsymbol{a_t}) \in \boldsymbol{A_n} \Leftrightarrow \boldsymbol{t}$ **is odd**
- Examples
  - $A_2 =$ trivial group
  - $A_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\} = \langle(1\ 2\ 3)\rangle$
  - $A_4 = \{(1), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$
- Subgroups of A_4

Order	Subgroup
1	$\{(1)\}$
2	$\{(1), (1\ 2)(3\ 4)\}$ $\{(1), (1\ 3)(2\ 4)\}$ $\{(1), (1\ 4)(2\ 3)\}$
3	$\{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ $\{(1), (1\ 2\ 4), (1\ 4\ 2)\}$ $\{(1), (1\ 3\ 4), (1\ 4\ 3)\}$ $\{(1), (2\ 3\ 4), (2\ 4\ 3)\}$
4	$\{(1), (12)(34), (13)(24), (14)(23)\}$
6	None
12	A_4

Converse of Lagrange's Theorem

- A_4 has no subgroup of order 6
- This shows that the converse of Lagrange's Theorem is false
  - If $d||G|$, there is not necessarily a subgroup of G with order d
- But the **converse** does **hold** for **finite cyclic groups**
- Cauchy's Theorem
  - If p is a **prime**, and $p||G|$, then G contains a subgroup of order p
- Sylow's Theorem
  - If $|G| = p^\alpha m$, where p is prime and $(p, m) = 1$
  - Then G contains a subgroup of order $\boldsymbol{p^\alpha}$

Subgroups of A_4, Group Action, Orbit, Stabilizer

Wednesday, March 21, 2018 9:57 AM

Proposition 43: Subgroup of Index 2 is Normal

- Statement
  - If G is a group, $\boldsymbol{H \leq G}$**, and** $\boldsymbol{[G:H] = 2}$, then $\boldsymbol{H \trianglelefteq G}$
- Proof
  - If $g \in H$, then $gH = H = Hg$
  - If $g \notin H$, then $gH = G \setminus H = Hg$
  - Therefore $gH = Hg, \forall g \in G$
  - So $H \trianglelefteq G$
- Corollary (See HW8 #2)
  - Let p be the smallest prime dividing $|G|$
  - If $[G:H] = p$, then $H \trianglelefteq G$

Proposition 44: Conjugate Cycle

- Statement
  - If $(a_1 \dots a_t), (a_1{}' \dots a_t{}')$ are t-cycles in S_n
  - Then $\boldsymbol{\exists \sigma \in S_n}$ **s.t.** $\boldsymbol{\sigma(a_1 \dots a_t)\sigma^{-1} = (a_1{}' \dots a_t{}')}$
- Proof
  - Choose $\sigma \in S_n$ s.t. $\sigma(a_i) = a_i', \forall i \in \{1, \dots, t\}$
  - By HW 7 #1, $\sigma(a_1 \dots a_t)\sigma^{-1} = \big(\sigma(a_1) \dots \sigma(a_t)\big) = (a_1{}' \dots a_t{}')$

Theorem 45: A_4 Have No Subgroup of Order 6

- Statement
  - $\boldsymbol{A_4}$ have **no subgroup** of **order 6**
- Proof
  - By way of contradiction, suppose $H \leq G$, and $|H| = 6$
  - Then $[A_4 : H] = 2$ and thus $H \trianglelefteq A_4$
  - Since A_4 contains eight 3-cycles, H must contain some 3-cycle α
  - Write $\alpha = (a\ b\ c)$, then
    - $(a\ b\ d)(a\ b\ c)(a\ b\ d)^{-1} = (b\ d\ c) \in H$
    - $(b\ c\ d)(a\ b\ c)(b\ c\ d)^{-1} = (a\ c\ d) \in H$
    - $(b\ d\ c)(a\ b\ c)(b\ d\ c)^{-1} = (a\ d\ b) \in H$
  - So far, we have $(1), (a\ b\ c), (b\ d\ c), (a\ c\ d), (a\ d\ b) \in H$
  - Also, since H is closed under inverses, $(a\ c\ b), (b\ c\ d) \in H$
  - Thus, $|H| \geq 7$, which makes a contradiction

- Therefore A_4 have no subgroup of order 6

Group Action

- Definition
    - An **action** of G on X is a function $G \times X \to X, (g, x) \mapsto gx$ s.t.
        - $\boldsymbol{1_G x = x, \forall x \in X}$
        - $\boldsymbol{g(hx) = (gh)x, \forall g, h \in G, x \in X}$
- Examples

Set	Group	Action
$\mathbb{R}^n$	$GL_n(\mathbb{R})$	$(A, v) \mapsto Av$
$\{1, \dots, n\}$	S_n	$(\sigma, i) \mapsto \sigma(i)$
Group G	Group G	$(g, h) \mapsto gh$
Group G	Group G	$(g, h) \mapsto ghg^{-1}$
Set of cosets of $H \leq G$	Group G	$(g, g'H) \mapsto gg'H$
Set of all subgroups of group G	Group G	$(g, H) \mapsto gHg^{-1}$

- Proof: Conjugation on subgroup is a group action
    - If $H \leq G$, and $g \in G$, then $gHg^{-1} = \{ghg^{-1} | h \in H\} \leq G$
    - $gHg^{-1} \neq \emptyset$, since $g1g^{-1} = 1 \in gHg^{-1}$
    - If $ghg^{-1}, gh'g^{-1} \in gHg^{-1}$, then
    - $ghg^{-1}(gh'g^{-1})^{-1} = ghg^{-1}g(h')^{-1}g^{-1} = gh(h')^{-1} \in gHg^{-1}$

Orbit and Stabilizer

- Suppose a group G acts on a set X
- Let $x \in X$
- The **orbit** of x, denoted $\text{orb}(x)$, is $\{g \cdot x | g \in G\} \subseteq X$
- The **stabilizer** of x, denoted $\text{stab}(x)$, is $\{g \in G | g \cdot x = x\} \subseteq G$

Proposition 46: Stabilizer is a Subgroup

- Statement
    - If G acts on X, and $x \in X$, then $\text{stab}(x) \leq G$
- Proof
    - $\text{stab}(x) \neq \emptyset$, because $1x = x$
    - Let $g, h \in \text{stab}(x)$
    - $(gh)x = g(hx) = gx = x \Rightarrow gh \in \text{stab}(x)$
    - $x = 1 \cdot x = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x \Rightarrow g^{-1} \in \text{stab}(x)$

Centralizer

- Let G be a group, and let G **act on itself by conjugation**
- If $h \in G$, then $\text{stab}(h) = \{g \in G | ghg^{-1} = h\} = \{g \in G | gh = hg\}$
- This set is called the **centralizer** of h, denoted as $C_G(h)$

- $C_G(h)$ is the set of **elements in G** that **commute with the element h**

Center

- Intersections of subgroups are subgroup
- Thus if G acts on a set X, $\bigcup_{x \in X} \text{stab}(x) \leq G$
- In the example above, $\bigcup_{h \in G} C_G(h) = Z(G)$ is called the **center** of G
- $Z(G)$ is the set of elements that **commute with every element** of G

Normalizer

- Let X be the set of subgroups of a group G
- Let G acts on X by $g \cdot H = gHg^{-1}$
- If $H \leq G$, then
  - $\text{stab}(H) = \{g \in G | gHg^{-1} = H\} = \{g \in G | gH = Hg\}$
- This set is called the **normalizer** of H in G, denoted $N_G(H)$
- $N_G(H)$ is the set of **elements in G** that **commute with the set H**
- Note: $N_G(H) = G \Leftrightarrow H \trianglelefteq G$

Orbit, Stabilizer, Cayley's Theorem

Friday, March 23, 2018 10:07 AM

Proposition 47: Orbits Equivalence

- Statement
  - Let G act on a set X
  - The relation $x \sim x' \Leftrightarrow \exists \boldsymbol{g} \in \boldsymbol{G}$ **s.t.** $\boldsymbol{gx} = \boldsymbol{x'}$ is an **equivalence relation**
- Proof
  - Reflexive
    - $1 \cdot x = x$
  - Symmetric
    - Suppose $x \sim x'$, then $\exists g \in G$ s.t. $gx = x' \Rightarrow x = g^{-1}x'$
  - Transitive
    - Suppose $x \sim x'$ and $x' \sim x''$
    - Choose $g, h \in G$ s.t. $gx = x'$ and $hx' = x''$
    - Then $ghx = hx' = x''$
- Note
  - The **equivalence classes** are the **orbits** of the group action
  - Thus, the orbits partition X

Proposition 48: Orbit-Stabilizer Theorem

- Statement
  - If G acts on X, and $x \in X$, then $|\mathbf{orb}(\boldsymbol{x})| = [\boldsymbol{G}: \mathbf{stab}(\boldsymbol{x})]$
- Proof
  - Define a function
    - $F: \mathrm{orb}(x) \to \{\text{left costs of stab}(x)\}$
    - $gx \mapsto g\ \mathrm{stab}(x)$
  - F is injective
    - $g\ \mathrm{stab}(x) = g'\ \mathrm{stab}(x)$
    - $\Leftrightarrow (g')^{-1}g \in \mathrm{stab}(x)$
    - $\Leftrightarrow (g')^{-1}gx = x$
    - $\Leftrightarrow gx = g'x$
  - F is surjective
    - This is clear
  - So $\mathrm{orb}(x) \cong \{\text{left costs of stab}(x)\}$
  - Therefore $|\mathrm{orb}(x)| = [G: \mathrm{stab}(x)]$

Proposition 49: Permutation Representation of Group Action

- Statement
  - Let G be a group acting on a finite set $X = \{x_1, \dots, x_n\}$
  - Then **each $\boldsymbol{g} \in \boldsymbol{G}$ determines a permutation** $\sigma_g \in S_n$ by
    - $\sigma_g(i) = j \Leftrightarrow g \cdot x_i = x_j$
- Proof
  - The map $f: X \to X$, given by $x \mapsto g \cdot x$ is bijection $\forall g \in G$
    - Injectivity: $g \cdot x = g \cdot x' \Rightarrow (g^{-1}g) \cdot x = (g^{-1}g) \cdot x' \Rightarrow x = x'$
    - Surjectivity: $f(g^{-1} \cdot x) = (gg^{-1}) \cdot x = x$
  - So each $g \in G$ determines a permutation $\sigma_g \in S_n$ where
    - $\sigma_g(i) = j \Leftrightarrow g \cdot x_i = x_j$

Proposition 49: Induced Homomorphism of Group Action

- Statement
  - The map **$\boldsymbol{\Phi}: \boldsymbol{G} \to \boldsymbol{S_n}$, given by $\boldsymbol{g} \mapsto \boldsymbol{\sigma_g}$** is a **homomorphism**
- Proof
  - Let $g, h \in G, i \in \{1, \dots, n\}$
  - Suppose $\sigma_{gh}(i) = j$ for some j
  - Then $(gh)x_i = x_j$
  - Write $hx_i = x_k$ for some k, then $\sigma_h(i) = k$
  - $(gh)x_i = x_j \Leftrightarrow gx_k = x_j \Leftrightarrow \sigma_g(k) = j \Leftrightarrow \sigma_g\big(\sigma_h(i)\big) = j$
  - Therefore $\sigma_{gh}(i) = \sigma_g\sigma_h(i), \forall i \in \{1, \dots, n\}$

Theorem 50: Cayley's Theorem

- Statement
  - Every **finite group** is isomorphic to a **subgroup** of the **symmetric group**
- Proof
  - Let $G = \{g_1, \dots, g_n\}$ act on itself by left multiplication $g \cdot h = gh$
  - Then this action determines a homomorphism
    - $\Phi: G \to S_n$
    - $g \mapsto \sigma_g$, where $\sigma_g(i) = j \Leftrightarrow g \cdot g_i = g_j$
  - Φ is injective
    - $\Phi(g) = \Phi(h) \Leftrightarrow \sigma_g = \sigma_h \Leftrightarrow ggi = hgi, \forall i \Leftrightarrow g = h$
  - Thus $G \cong \mathrm{im}(\Phi) \leq S_n$
- Example
  - Klein 4 group $K = \{1, a, b, c\}$
  - where $a^2 = b^2 = c^2 = 1 \Leftrightarrow ab = c, bc = a, ac = b$

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

- Label the group elements with 1, 2, 3, 4
- $1 \mapsto \sigma_1 = (1)$ since
  - $\sigma_1(1) = 1$
  - $\sigma_2(2) = 2$
  - $\sigma_3(3) = 3$
  - $\sigma_4(4) = 5$
- $a \mapsto \sigma_a = (1\ 2)(3\ 4)$ since
  - $\sigma_a(1) = 2$
  - $\sigma_a(2) = 1$
  - $\sigma_a(3) = 4$
  - $\sigma_a(4) = 3$
- $b \mapsto \sigma_b = (1\ 3)(2\ 4)$ since
  - $\sigma_b(1) = 3$
  - $\sigma_b(2) = 4$
  - $\sigma_b(3) = 1$
  - $\sigma_b(4) = 2$
- $c \mapsto \sigma_c = (1\ 4)(2\ 3)$ since
  - $\sigma_c(1) = 4$
  - $\sigma_c(2) = 3$
  - $\sigma_c(3) = 2$
  - $\sigma_c(4) = 1$
- Therefore $K \cong \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \leq S_4$

Conjugacy Class, The Class Equation

Monday, April 2, 2018 9:57 AM

Conjugacy Class

- Definition
  - If G is a group, G **acts on itself by conjugation**: $g \cdot h = ghg^{-1}$
  - The orbits under this action are called **conjugacy classes**
  - Denote a conjugate class represented by some element $g \in G$ by $\mathbf{conj}(\boldsymbol{g})$
- Example 1
  - If $g \in G$, and $g \in Z(G)$, then $\mathrm{conj}(g) = \{g\}$
  - Since $hgh^{-1} = hh^{-1}g = g, \forall h \in G$
  - The converse is also true: If $\mathrm{conj}(g) = \{g\}$, then $g \in Z(G)$
- Example 2
  - Let $G = S_n$
  - If $\sigma \in S_n$, then $\mathbf{conj}(\boldsymbol{g}) = \{$**all permutations of the same cycle type as** $\boldsymbol{\sigma}\}$
  - For instance
    - If σ is a t-cycle, then $\mathrm{conj}(\sigma) = \{\text{all } t\text{-cycles}\}$
  - More generally
    - Let $\sigma = \left(a_1^{(1)} \dots a_{t_1}^{(1)}\right) \cdots \left(a_1^{(m)} \dots a_{t_m}^{(m)}\right)$ be a product of disjoint cycles
    - Then $\mathrm{conj}(\sigma) = \{\text{all products of disjoint cycles of length } t_1, \dots, t_m\}$

Theorem 51: The Class Equation

- Statement
  - Let G be a finite group
  - Let $g_1, \dots g_r \in G$ be
    - **representatives of the conjugacy classes** of G that are
    - **not contained in the center** $\boldsymbol{Z}(\boldsymbol{G})$
  - Then $|\boldsymbol{G}| = |\boldsymbol{Z}(\boldsymbol{G})| + \sum_{\boldsymbol{i}=\mathbf{1}}^{\boldsymbol{r}} [\boldsymbol{G}: \boldsymbol{C}_{\boldsymbol{G}}(\boldsymbol{g}_{\boldsymbol{i}})]$
- Recall: $C_G(g_i) = \{g \in G \mid gg_i = g_i g\}$
- Proof
  - G is the disjoint union of its disjoint conjugate classes
  - Then $G = Z(G) \cup \bigcup_{i=1}^{r} \mathrm{conj}(g_i)$
  - $\Rightarrow |G| = |Z(G)| + \sum_{i=1}^{r} |\mathrm{conj}(g_i)|$

- $\Rightarrow |G| = |Z(G)| + \sum_{i=1}^{r} |\mathrm{orb}(g_i)|$ (under conjugacy action)
- $\Rightarrow |G| = |Z(G)| + \sum_{i=1}^{r} [G:\mathrm{stab}(g_i)]$ by Proposition 48
- $\Rightarrow |G| = |Z(G)| + \sum_{i=1}^{r} [G:C_G(g_i)]$

Corollary 52: Center of p-Group is Non-Trivial

- Statement
  - If p is a prime, and P is a **group of order $\boldsymbol{p^\alpha}$** ($\alpha > 1$), then $\boldsymbol{|Z(P)| > 1}$
- Note
  - Group of order p^α for prime p is called a ***p*-group**
- Proof
  - By the class equation, $|Z(P)| = |P| - \sum_{i=1}^{r} [P:C_P(p_i)]$, where $p_1, \ldots p_r \in P$ are
  - representatives of the conjugate classes of P not contained in $Z(P)$
  - $g_i \notin Z(P) \Rightarrow C_P(g_i) \neq P \Rightarrow [P:C_P(g_i)] \neq 1$
  - By Lagrange's Theorem, $[P:C_P(g_i)] \big| p^\alpha$
  - Combing previous two results, $p \big| [P:C_P(g_i)]$
  - Thus, $p \left| \left(|P| - \sum_{i=1}^{r} [P:C_P(g_i)] \right) \right. = |Z(P)|$, since $p \big| |P|$
  - $\Rightarrow |Z(P)| \neq 1$

Corollary 53: Group of Order Prime Squared is Abelian

- Statement
  - If p is a prime, and P is a group of **order $\boldsymbol{p^2}$**, then P is **abelian**.
  - In fact, either $\boldsymbol{P \cong \mathbb{Z}/p^2\mathbb{Z}}$ or $\boldsymbol{P \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}}$
- Proof
  - By Corollary 52 and Lagrange's Theorem, $|Z(P)| = p$ or p^2
  - Suppose $|Z(P)| = p$
    - $|P/Z(P)| = [P:Z(P)] = \frac{|P|}{|Z(P)|} = \frac{p^2}{p} = p$
    - By Corollary 26, $P/Z(P)$ is cyclic
    - By HW6 #2, P is abelian
    - In this case $Z(P) = P \Rightarrow |Z(P)| = p^2$
    - Therefore $|Z(P)| = p$ is impossible
  - Suppose $|Z(p)| = p^2$

        - We have $|Z(p)| = |P| \Rightarrow Z(P) = P$
        - So P is abelian
    - If P is cyclic, then clearly $P \cong \mathbb{Z}/p^2\mathbb{Z}$
    - If P is not cyclic, we need to show that $P \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$
        - Let $z \in P \setminus \{1\}$, then $|z| = p$
        - Let $y \in P \setminus \langle z \rangle$
        - Set $H \coloneqq \langle z \rangle, K \coloneqq \langle y \rangle$, then $H \cap K = \{1\}$
            - Since any non-identity element of H or K is a generator
            - For instance, if $1 \neq y^k \in H$ for some k, then $y \in H$
            - This is impossible, so $H \cap K = \{1\}$
        - $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|} = |H| \cdot |K| = p^2 = |P| \Rightarrow HK = P$
        - By HW6 #1, there exists an isomorphism $P \xrightarrow{\cong} P/H \times P/K$
        - $|P/H| = [P : H] = \dfrac{|P|}{|H|} = \dfrac{p^2}{p} = p \Rightarrow P/H \cong \mathbb{Z}/p\mathbb{Z}$
        - Similarly for P/K
        - Therefore $P = HK \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Cauchy's Theorem, Recognizing Direct Products

Wednesday, April 4, 2018 9:48 AM

Theorem 54: Cauchy's Theorem

- Statement
  - If G is a finite group, and **p is a prime divisor of $|G|$**, then $\exists \boldsymbol{H \leq G}$ **of order p**
- Proof
  - Write $|G| = mp$
  - We argue by strong induction on m
  - When $m = 1$, this is trivial, since any non-identity element of G has order p
  - Suppose $m > 1$, and $\forall n \in \{1, \dots, m-1\}$ if $|G'| = np$, then $\exists H' \leq G'$ of order p
  - If G is abelian
    - Let $x \in G \setminus \{1\}$
    - If $\langle x \rangle = G$
      - By the Fundamental Theorem of Cyclic Groups,
      - $G = \langle x \rangle$ contains a (unique) subgroup of order p
    - If $\langle x \rangle \neq G$
      - Set $H \coloneqq \langle x \rangle \trianglelefteq G$
      - By the Lagrange's Theorem, $|G| = |H|[G: H] = |H| \cdot |G/H|$
      - Since $p \big| |G|$, either $p \big| |H|$ or $p \big| |G/H|$
      - If $p \big| |H|$
        - Since H is cyclic, H contains a (unique) subgroup of order p
        - It follows that G contains a subgroup of order p
      - If $p \big| |G/H|$
        - $|G/H| < |G|$, so, by induction, $\exists gH \in G/H$ s.t. $|gH| = p$
        - So we only need to prove $|gH| \big| |g|$
          - If $K \xrightarrow{f} K'$ is a group homomorphism, $|f(k)| \big| |k|, \forall k \in K$
          - Now, take $K = G, K' = G/H, f$ the usual surjection $g \mapsto gH$
        - Therefore $p \big| |g|$
        - Since $\langle g \rangle$ is cyclic, $\langle g \rangle$ contains a (unique) subgroup of order p
        - It follows that G contains a subgroup of order p
  - If G is not abelian
    - By the Lagrange's Theorem, $|G| = |C_G(g_i)| \cdot [G: C_G(g_i)], \forall i \in \{1, \dots, r\}$
    - Since $p \big| |G|$, either $p \big| |C_G(g_i)|$ or $p \big| [G: C_G(g_i)]$
    - If $p \big| |C_G(g_i)|$ for some i

- ▫ Since G is not abelian, $C_G(g_i) \lneqq G$ for all i
- ▫ Apply the induction hypothesis, $C_G(g_i)$ contains a subgroup of order p
- ▫ It follows that G contains a subgroup of order p

- If $p|[G: C_G(g_i)], \forall i$
  - ▫ By the Class Equation, $|G| = |Z(G)| + \sum_{i=1}^{r}[G: C_G(g_i)]$ where $g_1, \dots, g_r \in G$
  - ▫ are the representatives of the conjugate classes not contained in $Z(G)$
  - ▫ It follows that $p \left| \left(|G| - \sum_{i=1}^{r}[G: C_G(g_i)] \right) = |Z(G)| \right.$
  - ▫ G is not abelian, so $Z(G) \lneqq G$
  - ▫ Apply the induction hypothesis, $Z(G)$ contains a subgroup of order p
  - ▫ It follows that G contains a subgroup of order p

Lemma 55: Recognizing Direct Products

- Statement
  - Let G be a group with normal subgroups N_1, N_2
  - The map $\alpha: \boldsymbol{N_1 \times N_2 \to G}$ given by $(n_1, n_2) \mapsto n_1 n_2$ is an **isomorphism**
  - if and only if $\boldsymbol{N_1 N_2 = G}$ and $\boldsymbol{N_1 \cap N_2 = \{1\}}$
- Proof ($\Longrightarrow$)
  - Since α is surjective, $N_1 N_2 = G$
  - Suppose $n \in N_1 \cap N_2$
  - Then $\alpha(n, 1) = n = \alpha(1, n)$
  - Since α is injective, $(1, n) = (n, 1) \Rightarrow n = 1$
  - So $N_1 \cap N_2 = \{1\}$
- Proof ($\Longleftarrow$)
  - α is surjective
    - This is true since $N_1 N_2 = G$
  - α is a homomorphism
    - $\alpha\big((n_1, n_2), (n_1', n_2')\big) = \alpha\big((n_1 n_1', n_2 n_2')\big) = n_1 n_1' n_2 n_2'$
    - $\alpha(n_1, n_2)\alpha(n_1', n_2') = n_1 n_2 n_1' n_2'$
    - We want show that $\alpha\big((n_1, n_2), (n_1', n_2')\big)\big(\alpha(n_1, n_2)\alpha(n_1', n_2')\big)^{-1} = 1$
    - $(n_1 n_1' n_2 n_2')(n_1 n_2 n_1' n_2')^{-1} = n_1 n_1' n_2 n_2' (n_2')^{-1}(n_1')^{-1} n_2^{-1} n_1^{-1}$
    - $= n_1 \underbrace{n_1' n_2 (n_1')^{-1}}_{\in N_2} n_2^{-1} n_1^{-1} = n_1 \underbrace{n_1' n_2 (n_1')^{-1} n_2^{-1}}_{\in N_2} n_1^{-1} \in N_2$
    - $= n_1 n_1' \underbrace{n_2 (n_1')^{-1} n_2^{-1}}_{\in N_1} n_1^{-1} = n_1 \underbrace{n_1' n_2 (n_1')^{-1} n_2^{-1}}_{\in N_1} n_1^{-1} \in N_1$
    - Thus $(n_1 n_1' n_2 n_2')(n_1 n_2 n_1' n_2')^{-1} \in N_1 \cap N_2 = \{1\}$

- Therefore $\alpha\big((n_1, n_2), (n_1', n_2')\big) = \alpha\big((n_1, n_2), (n_1', n_2')\big)$

- α is injective
  - If $(n_1, n_2) = 1$
  - $\Rightarrow n_1 n_2 = 1$
  - $\Rightarrow n_1 = n_2^{-1}$
  - $\Rightarrow n_1 \in N_2, n_2 \in N_1$
  - $\Rightarrow n_1 = n_2 = 1$
  - $\Rightarrow (n_1, n_2) = (1,1)$
  - $\Rightarrow \alpha$ is injective

Homework 8, Properties of Finite Abelian Group

Saturday, April 7, 2018 10:09 PM

Homework 8 Question 3

- Statement
  - If G is a group with $|G| \leq 11$, and $d \big| |G|$, then G has a subgroup of order d
- Proof
  - For $|G| = 2,3,5,7,11$
    - $|G|$ is prime, thus cyclic
  - For $|G| = 4,6,9,10$
    - $|G|$ is product of two primes, so use the Cauchy's Theorem
  - For $|G| = 8$
    - $d \in \{1,2,4,8\}$
    - When $d = 1,2,8$, this is obvious
    - So assume $d = 4$
    - If G contains an element of order 4, then we are done
    - So, we may assume $|g| = 2, \forall g \in G \setminus \{1\}$, then G is abelian
    - Let $a, b \in G \setminus \{1\}$. Let $H \coloneqq \{1, a, b, ab\}$
    - H is closed under inverse
      - The inverse of every element of G is itself
    - H is closed under multiplication by multiplication table below

$\cdot$	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

Lemma 56: Coprime Decomposition of Finite Abelian Group

- Statement
  - Let G be a **finite abelian group of order mn**, where $(\boldsymbol{m}, \boldsymbol{n}) = \mathbf{1}$
  - Let $M = \{x \in G | x^m = 1\}, N = \{x \in G | x^n = 1\}$, then
    - $M, N \leq G$, and
    - The map $\alpha: \boldsymbol{M} \times \boldsymbol{N} \to \boldsymbol{G}$ given by $(g, h) \mapsto gh$ is an **isomorphism**
  - Moreover, if $m, n \neq 1$, then M and N are nontrivial
- Proof
  - $M, N \leq G$
    - It suffices to check $M \leq G$

        - $M \neq \emptyset$, since $1 \in M$
        - If $x, y \in M$, then $(xy^{-1})^m = x^m(y^m)^{-1} = 1$. Thus $xy^{-1} \in M$
    - $MN = G$
        - Choose $r, s \in \mathbb{Z}$ s.t. $mr + ns = 1$
        - Let $g \in G$, then $g = g^{mr+ns} = g^{mr}g^{ns}$
        - $(g^{mr})^n = (g^{mn})^r = \left(g^{|G|}\right)^r = 1$ by Lagrange's Theorem
        - Similarly, $(g^{ns})^m = 1$
        - So, $g^{ns} \in M$, $g^{mr} \in N$, so $g \in MN$
        - Therefore $MN = G$
    - $M \cap N = \{1\}$
        - Let $g \in M \cap N$, then $g^m = 1 = g^n$
        - Then $|g||m$ and $|g||n$
        - Since $(m, n) = 1$, $|g| = 1$
        - Thus $M \cap N = \{1\}$
    - By Lemma 55, $M \cap N = \{1\}$ and $MN = G \Rightarrow \alpha$ is an isomorphism
    - M and N are nontrivial
        - Suppose $m \neq 1$
        - Let p be a prime divisor of m
        - Then G contains an element z of order p, by Cauchy's Theorem
        - $z \in M$, so $M \neq \{1\}$
        - Similarly, if $n \neq 1$, $N \neq \{1\}$

Corollary 57: p-Group Decomposition of Finite Abelian Group

- Statement
    - Let G be a **finite abelian group**, and p be a prime divisor of $|G|$
    - Choose $m \in \mathbb{Z}_{>0}$ s.t. $|G| = p^m n$ and $p \nmid n$
    - Then $\boldsymbol{G} \cong \boldsymbol{P} \times \boldsymbol{T}$, where $P, T \leq G$, $|P| = p^m$, and $p \nmid |T|$
- Intuition
    - If $|G| = p_1^{m_1} p_2^{m_2} \dots p_n^{m_n}$
    - This corollary says $G \cong P_1 \times \cdots \times P_n$, where $|P_i| = p_i^{m_i}$
    - This reduces the Fundamental Theorem of Finite Abelian Groups
    - to the case where the group has order given by a prime power
- Proof
    - Let $P \coloneqq \left\{x \in G \middle| x^{p^m} = 1\right\}, T \coloneqq \{x \in G | x^n = 1\}$
    - By Lemma 56, $G \cong P \times T$
    - $p \nmid |T|$
        - Suppose, by way of contradiction, that $p \big| |T|$

        - By Cauchy's Theorem, $\exists z \in T$ s.t. $|z| = p$
        - Since $z \in T$, $z^n = 1$, so $p|n$
        - This is impossible, thus $p \nmid |T|$
    - $|P| = p^m$
        - Since $|G| = |P| \cdot |T| = p^m n$, $p^m \Big| |T|$
        - Suppose $p^m < |P|$
        - Then, $\exists$ prime q s.t. $p \neq q$ and $q \Big| |P|$
        - By Cauchy's Theorem, $\exists y \in P$ s.t. $|y| = q$
        - This is impossible since $y \in P \Rightarrow y^{p^m} = 1 \Rightarrow q \Big| p^m$
        - Thus $p^m = |P|$

Fundamental Theorem of Finite Abelian Groups

Monday, April 9, 2018 10:26 PM

Lemma 58: Prime Decomposition of Abelian p-Group

- Statement
  - If G is an abelian group of order p^n, where p is a prime
  - Let $a \in G$ has maximal order among all the elements of G
  - Then $\boldsymbol{G \cong A \times Q}$, where $\boldsymbol{A = \langle a \rangle, Q \leq G}$
- Proof
  - We argue by induction on n
  - If $n = 1$, then $G = A$, so we may take $Q = \{1\}$
  - Now suppose $n > 1$
  - Case 1: $\exists b \in G$ s.t. $b \notin A$ and $b^p = 1$
    - Let $B \coloneqq \langle b \rangle \trianglelefteq G$
    - $A \cap B = \{1\}$
      - $|b|$ is prime, since $b^p = 1$
      - Recall: If $(x, n) = 1$, then $\mathbb{Z}/n\mathbb{Z} = \langle \bar{x} \rangle$
      - So every non-identity element of B is a generator
      - Thus, if $x \in A \cap B$, and $x \neq 1$, then $B = \langle x \rangle \subset A \cap B \subset A$
      - Then $b \in A$, which contradicts the assumption
      - Therefore $A \cap B = \{1\}$
    - Let $\bar{G} \coloneqq G/B$, then $|\bar{G}| < |G|$ since $B \neq \{1\}$
    - aB is an element of maximal order in $\bar{G}$
      - $|aB| \big| |a|$
        - $a^{|a|} = 1$
        - $\Rightarrow a^{|a|} \in B$
        - $\Rightarrow (aB)^{|a|} = 1_{\bar{G}}$
        - $\Rightarrow |aB| \big| |a|$
      - $|a| \big| |aB|$
        - $(aB)^{|aB|} = 1_{\bar{G}}$
        - $\Rightarrow a^{|aB|} B = B$
        - $\Rightarrow a^{|aB|} \in B$
        - $\Rightarrow a^{|aB|} \in A \cap B = \{1\}$
        - $\Rightarrow a^{|aB|} = 1$
        - $\Rightarrow |a| \big| |aB|$

- So $|aB| = |a|$
- Therefore aB is an element of maximal order in $\bar{G}$

- By induction, $\exists \bar{Q} \leq \bar{G}$ s.t. $\bar{G} \cong \langle aB \rangle \times \bar{Q}$
- Apply the Correspondence Theorem, choose $Q \leq G$ s.t. $\bar{Q} = Q/B$
- Claim: $G \cong A \times Q$
  - By Lemma 55, we need only show $A \cap Q = \{1\}$ and $AQ = G$
  - $A \cap Q = \{1\}$
    - Let $g \in A \cap Q$, then $g = a^i$ for some i
    - Thus, $a^iB \in \langle aB \rangle \cap \bar{Q} \leq \bar{G}$
    - Since $\bar{G} \cong \langle aB \rangle \times \bar{Q}$, $\langle aB \rangle \cap \bar{Q} = \{1\}$
    - Therefore $a^iB = 1_{\bar{G}}$
    - $\Rightarrow |a| = |aB||i$
    - $\Rightarrow a^i = 1$
    - $\Rightarrow A \cap Q = \{1\}$
  - $AQ = G$
    - Let $g \in G$
    - Since $\bar{G} = \langle aB \rangle \times \bar{Q}$,
    - $gB = a^iByB$ for some $a^iB \in \langle aB \rangle$ and $yB \in \bar{Q}$,
    - Thus $gB = a^iyB \Leftrightarrow g\left(a^iy\right)^{-1} \in B$
    - Choose $b \in B$ s.t. $ga^{-i}y^{-1} = b$
    - Then $g = \underbrace{a^i}_{\in A} \underbrace{yb}_{\in Q}$
    - Therefore $AQ = G$

- Case 2: $\nexists b \in G$ s.t. $b \notin A$ and $|b| = p$
  - In this case, we need to prove $G = A$
  - By way of contradiction, suppose otherwise
  - Choose $x \in G \setminus A$ with the smallest order
  - Recall: If $H = \langle z \rangle$, then $|\langle z^m \rangle| = \dfrac{|z|}{(|z|, m)}$
  - $|x^p| < |x|$, so $x^p \in A$
  - Choose i s.t. $x^p = a^i$
  - Say $|a| = p^s$
  - Since a has maximal order, $x^{p^s} = 1$
  - $\Rightarrow 1 = x^{p^s} = (x^p)^{p^{s-1}} = \left(a^i\right)^{p^{s-1}} = a^{ip^{s-1}}$
  - It follows that $p|i$
  - So $x^p = a^i$, where $p|i$
  - Set $y \coloneqq a^{-i/p}x$, then $y^p = a^{-i}x^p = 1$

- But $y \notin A$, since $ya^{i/p} = x \notin A$
- This contradicts the assumption that $\nexists b \in G$ s.t. $b \notin A$ and $|b| = p$
- So $G \setminus A = \emptyset$
- Therefore $G = A = \langle a \rangle$, and $Q = \{1\}$

Theorem 59: Fundamental Theorem of Finite Abelian Groups

- Statement
  - Every **finite abelian group** G is a **product of cyclic groups**
- Proof
  - Say $|G| = p_1^{m_1} \cdots p_n^{m_n}$, where p_i are distinct primes
  - By Corollary 57, and induction $G \cong P_1 \times \cdots \times P_n$ where
  - $P_i = \left\{ x \in G \middle| x^{p_i^{m_i}} = 1 \right\}$ and $|P_i| = p_i^{m_i}$
  - So, it suffices to show each P_i is a product of cyclic groups
  - By Lemma 58, $P_i \cong A_i \times Q_i$, where A_i is cyclic
  - The result immediately follows by induction on m_i
- Example
  - How may abelian groups of order 8 are there up to isomorphism
  - There are 3 abelian groups of order 8: $\mathbb{Z}/_{8\mathbb{Z}}, \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}}, \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$

Partition

- A **partition** of $n \in \mathbb{Z}_{>0}$ is a way of writing n as a sum of positive integers
- Example: 3 has 3 partitions: $3, 2 + 1, 1 + 1 + 1$

Corollary 60: Number of Finite Abelian Groups of Order n

- Statement
  - If $n = p_1^{e_1} \cdots p_n^{e_m}$, where p_i are distinct primes
  - Then the **number of finite abelian groups** of order n is
  - $\displaystyle\prod_{i=1}^{m} \textbf{number of partitions of } \boldsymbol{e_i}$
- Note
  - If $(\lambda^1, \dots, \lambda^m)$ are partitions of $e_1, \dots, e_m$, where $\lambda_i = \{\lambda_i^1, \dots, \lambda_i^{s_i}\}$
  - Then this list of partitions corresponds to the abelian group
  - $\left(\mathbb{Z}/_{p_1^{\lambda_1^1}\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{p_1^{\lambda_1^{s_1}}\mathbb{Z}} \right) \times \cdots \times \left(\mathbb{Z}/_{p_1^{\lambda_m^1}\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{p_1^{\lambda_m^{s_m}}\mathbb{Z}} \right)$
- Example
  - When $n = 72 = 2^3 \cdot 3^2$
  - $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}} \cong \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{6\mathbb{Z}} \times \mathbb{Z}/_{6\mathbb{Z}}$
  - $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{9\mathbb{Z}}$

- $\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}$
- $\mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{9\mathbb{Z}}$
- $\mathbb{Z}/_{8\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}$
- $\mathbb{Z}/_{8\mathbb{Z}} \times \mathbb{Z}/_{9\mathbb{Z}}$

Definition of Ring

Wednesday, April 11, 2018 9:58 AM

Ring

- Definition
  - A **ring** is a set R equipped with two operations $+$ and $\cdot$ s.t.
  - $(R, +)$ is an abelian group
  - $\cdot$ is associative
  - $\exists 1 \in R$ s.t. $1 \cdot r = r = r \cdot 1$
  - Distributive property:
    - $\forall a, b, c \in R$
    - $a \cdot (b + c) = a \cdot b + a \cdot c$
    - $(a + b) \cdot c = a \cdot c + b \cdot c$
- Note
  - 1 is called the **multiplicative identity**
  - Dummit-Foote don't require the multiplicative identity
  - $\cdot$ is not necessarily commutative
  - R is not a group under $\cdot$, because inverses may not exist
  - We will typically denote multiplication of $r, s \in R$ by rs
  - Typically 1 will denote the multiplicative identity
  - And 0 will denote the identity of $(R, +)$

Properties of Ring, Zero-Divisor, Unit

Monday, April 16, 2018 9:57 AM

Examples of Ring

- Example 1
  - The trivial group, equipped with the trivial multiplication, is a ring
  - It's called the trivial ring
- Example 2
  - $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all rings with usual addition and multiplication
- Example 3
  - For $n > 0$, $\mathbb{Z}/n\mathbb{Z}$ is a ring with modular addition and multiplication
- Example 4
  - For $n > 0$, define $\mathrm{Mat}_{n\times n}(\mathbb{R}) \coloneqq \{n \times n \text{ matrices with entries in } \mathbb{R}\}$
  - Then $\mathrm{Mat}_{n\times n}(\mathbb{R})$ is a ring with matrix addition and multiplication
  - Note: when $n > 1$, $\mathrm{Mat}_{n\times n}(\mathbb{R})$ is not commutative
- Example 5
  - $\mathrm{GL}_n(\mathbb{R})$ is not a ring under the usual matrix addition and multiplication
  - Because $\mathrm{GL}_n(\mathbb{R})$ is not a group under addition: $0 \notin \mathrm{GL}_n(\mathbb{R})$

Proposition 61: Properties of Ring

- Let R be a ring, then
- $\boldsymbol{0a = 0 = a0, \forall a \in R}$
  - $0a = (0+0)a = 0a + 0a \Rightarrow 0a = 0$
  - $a0 = a(0+0) = a0 + a0 \Rightarrow a0 = 0$
- $\boldsymbol{(-a)b = a(-b) = -(ab), \forall a, b \in R}$
  - $(-a)b + ab = (-a+a)b = 0b = 0 \Rightarrow (-a)b = -(ab)$
  - $a(-b) + ab = a(-b+b) = a0 = 0 \Rightarrow a(-b) = -(ab)$
- $\boldsymbol{(-a)(-b) = ab, \forall a, b \in R}$
  - $(-a)(-b) = -\big(a(-b)\big) = -(-ab) = ab$
- **The multiplicative identity 1 is unique**
  - Suppose $1, 1' \in R$ satisfy $1r = r = r1$ and $1'r = r = r1', \forall r \in R$
  - Then $1 = 1 \cdot 1' = 1'$
- $\boldsymbol{-a = (-1)a, \forall a \in R}$
  - $(-1)a + a = (-1)a + 1 \cdot a = (-1+1)a = 0a = a \Rightarrow -a = (-1)a$

Proposition 62: Criterion for Trivial Ring

- Statement

- A ring R is **trivial** (i.e. have only one element) iff $\mathbf{1 = 0}$
- Proof
  - $(\Longrightarrow)$ Clear
  - $(\Longleftarrow)$ Let $r \in R$, then $r = 1 \cdot r = 0 \cdot r = 0$
- Note
  - Often, instead of saying "R is nontrivial", one says "$1 \neq 0$"

Zero-Divisor and Unit

- Definition
  - Let R be a ring
  - A nonzero element $r \in R$ is called a **zero-divisor** if
    - $\exists s \in R \setminus \{0\}$ s.t. $\boldsymbol{rs = 0}$ **or** $\boldsymbol{sr = 0}$
  - Assume $1 \neq 0$, then $u \in R$ is called a **unit** if
    - $\exists v \in R$ s.t. $\boldsymbol{uv = 1 = vu}$
- Note
  - If R is a ring, and $1 \neq 0$, then 0 and zero-divisors are not units
  - Let $z \in R$ be a zero-divisor
  - By way of contradiction
  - Choose $v \in R$ s.t. $zv = 1 = vz$
  - Choose $s \in R \setminus \{0\}$ s.t. $zs = 0$
  - Then $s = (vz)s = v(0) = 0$, contradiction
- Example 1
  - What are the units in $\mathbb{Z}/6\mathbb{Z}$?
    - $\overline{1}, \overline{5}$, since $\overline{1} \cdot \overline{1} = \overline{1}$ and $\overline{5} \cdot \overline{5} = \overline{25} = \overline{1}$
  - What are the zero-divisors in $\mathbb{Z}/6\mathbb{Z}$?
    - $\overline{2}, \overline{3}, \overline{4}$, since $\overline{2} \cdot \overline{3} = \overline{3} \cdot \overline{4} = \overline{0}$
- Example 2
  - If r, s are elements of a ring, and $rs = 0$, we can't conclude $sr = 0$
  - $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$
  - $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Proposition 63: One-Sided Zero Divisor and Unit

- Statement
  - Let R be a ring, then
  - $\boldsymbol{r \in R}, s \in R \setminus \{0\}$, and $\boldsymbol{sr = 0} \nRightarrow \exists t \in R \setminus \{0\}$ s.t. $\boldsymbol{rt = 0}$
  - $\boldsymbol{u \in R}$, and $\exists v \in R$ s.t. $\boldsymbol{uv = 1} \nRightarrow \exists w \in R$ s.t. $\boldsymbol{wu = 1}$
- Proof

- Let V be a vector space over $\mathbb{R}$ with countably infinite dimension
- Fix a basis $\{e_1, e_2, \dots\}$ of V
- Let $R \coloneqq \{\text{linear transformation } V \to V\}$ is a ring given by
  - $(f+g)(v) = f(v) + g(v), \forall f, g \in R$
  - $(fg)(v) = f\big(g(v)\big), \forall f, g \in R$
- Check R is a ring
  - $id_V \in R$, so $R \neq \emptyset$
  - $(R, +)$ is an abelian group
    - Addition is associative
    - The zero map is the additive identity
    - Let $f, g \in R$ and $v \in V$
    - $(-f)(v) = -f(v)$ is the additive inverse of f
    - $(f+g)(v) = f(v) + g(v) = g(v) + f(v) = (g+f)(v)$
  - Multiplication
    - Associativity of multiplication is clear
    - id_V is the multiplicative identity
  - Distributive property
    - Let $f, g, h \in R$ and $v \in V$
    - $\big(h \circ (f+g)\big)(v) = h\big(f(v) + g(v)\big) = (hf)(v) + (hg)(v)$
    - $\big((f+g) \circ h\big)(v) = (f+g)\big(h(v)\big) = (fh)(v) + (gh)(v)$
    - So $h(f+g) = hf + hg$ and $(f+g)h = fh + gh$
- Define
  - $\alpha: V \to V$ by $e_i \mapsto e_{i+1}, \forall i \geq 1$
  - $\beta: V \to V$ by $e_1 \mapsto 0$, and $e_i \mapsto e_{i-1}, \forall i \geq 2$
  - $\gamma: V \to V$ by $e_1 \mapsto e_1$, and $e_i \mapsto 0, \forall i \geq 2$
- $\beta\alpha = id_V$
  - Since $e_i \overset{\alpha}{\mapsto} e_{i+1} \overset{\beta}{\mapsto} e_{(i+1)-1} = e_i, \forall i \geq 1$
- $\alpha\beta \neq id_V$
  - Suppose $\alpha\beta = id_V$, then $\gamma\alpha\beta = \gamma$
  - But $(\gamma\alpha\beta)(e_1) = 0 \neq \gamma(e_1) = e_1$
- $\gamma\alpha = 0$
  - Since $e_i \overset{\alpha}{\mapsto} e_{i+1} \overset{\gamma}{\mapsto} 0, \forall i \geq 1$
  - Notice: neither α nor γ is 0
- $\alpha\delta \neq 0, \forall \delta \in R \setminus \{0\}$
  - If $\exists \delta \in R \setminus \{0\}$ s.t. $\alpha\delta = 0$, then
  - $0 = \beta\alpha\delta = \delta \neq 0$, which is impossible

- Note
    - If $V = \mathbb{P}(\mathbb{R})$, the set of all polynomials over $\mathbb{R}$, then
    - α is analogous to integration
    - β is analogous to differentiation
    - γ is analogous to evaluation at 0

Group of Unites

- Definition
  - $R^\times := \{u \in R | u \text{ is a unit}\}$
- Note
  - $R^\times$ is a group under multiplication
- Example
  - $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} | (a, n) = 1\} = \{\text{units in } \mathbb{Z}/n\mathbb{Z}\}$

Field, Product Ring, Integral Domain

Wednesday, April 18, 2018 10:42 AM

Proposition 64: Units and Zero-Divisors of $\mathbb{Z}/n\mathbb{Z}$

- Statement
  - Let $n > 0$
  - Every **nonzero element in** $\mathbb{Z}/\boldsymbol{n}\mathbb{Z}$ is either a **unit** or a **zero-divisor**
- Note
  - We don't have this property in $\mathbb{Z}$
  - In $\mathbb{Z}$, the units are ± 1, there are no zero-divisor
  - In particular, $2 \in \mathbb{Z}$ is not 0 or unit or zero-divisor
- Proof
  - Suppose $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is nonzero and not a unit
  - Let $d := (a, n)$, then $d > 1$
  - Write $cd = a, md = n$, then
  - $\bar{a}\bar{m} = \bar{c}\bar{d}\bar{m} = \bar{c}\bar{n} = \bar{0}$
  - Since $md = n$, where $1 \leq m \leq n$ and $d > 1$
  - m cannot be a multiple of n
  - So $\bar{a}\bar{m} = \bar{0}$ with $\bar{m} \neq \bar{0}$
  - Therefore $\bar{a}$ is a zero-divisor

Field

- Definition
  - A communitive ring R is called a **field** if
  - Every **nonzero** element of R is a **unit**
  - i.e. Every nonzero element of R have a **multiplicative inverse**
- Example 1
  - $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- Example 2
  - $\mathbb{Z}/p\mathbb{Z}$, where p is a prime
  - $1 \leq a \leq p - 1, (a, p) = 1 \Rightarrow \bar{a} \in \mathbb{Z}/p\mathbb{Z}$
  - Note: $\mathbb{Z}/n\mathbb{Z}$ is a field $\Leftrightarrow n$ is prime
- Example 3
  - $\mathbb{R}^2$ is not a field with multiplication defined as $(r_1, r_2)(r_1', r_2') = (r_1 r_1', r_2 r_2')$

Product Ring

- Let R_1, R_2 be rings

- The product ring $\boldsymbol{R_1} \times \boldsymbol{R_2}$ has the following ring structure
- For addition, it's just the **product as groups**
- For multiplication, $(\boldsymbol{r_1}, \boldsymbol{r_2})(\boldsymbol{r'_1}, \boldsymbol{r'_2}) = (\boldsymbol{r_1 r'_1}, \boldsymbol{r_2 r'_2})$ with identity $\left(1_{R_1}, 1_{R_2}\right)$

Integral Domain

- Definition
  - A communicative ring R is an **integral domain** (or just **domain**) if
  - R contains no **zero-divisors**
- Example
  - Unites are not zero-divisors, so all fields are domains
  - $\mathbb{Z}$ is a domain, but not a field
  - $\mathbb{Z}/n\mathbb{Z}$ is a domain $\Leftrightarrow$ it is a field $\Leftrightarrow$ n is prime
  - $R_1 \times R_2$ is a domain $\Leftrightarrow$ one of them is trivial, and the other is a domain

Product Ring, Finite Domain and Field, Subring

Friday, April 20, 2018 10:08 AM

Proposition 65: Criterion for Product Ring to be a Domain

- Statement
  - If R_1 and R_2 are rings, then $\boldsymbol{R_1 \times R_2}$ **is a domain** iff
  - One of the R_1 or R_2 is a **domain**, and the other is **trivial**
- Proof ($\Longleftarrow$)
  - Without loss of generality, assume R_1 is a domain and R_2 is trivial
  - Let $(r_1, r_2), (r_1', r_2') \in R_1 \times R_2 \setminus \{(0,0)\}$
  - Then $r_1 \neq 0$ and $r_1' \neq 0$
  - Since R_1 is a domain, $r_1 r_1' \neq 0$
  - Thus, $(r_1, r_2)(r_1', r_2') = (r_1 r_1', r_2 r_2') \neq 0$
- Proof ($\Longrightarrow$)
  - $(1_{R_1}, 0)(0, 1_{R_2}) = (0,0)$
  - Since $R_1 \times R_2$ is a domain, either $(1_{R_1}, 0)$ or $(0, 1_{R_2})$ is $(0,0)$
  - This means either 1_{R_1} or 1_{R_2} is 0, and thus R_1 or R_2 is trivial
  - Without loss of generality, suppose R_2 is trivial
  - We want to show that R_1 is a domain
  - Let $r_1, r_1' \in R_1 \setminus \{0\}$
  - Then $(r_1, 0), (r_1', 0) \in R_1 \times R_2 \setminus \{(0,0)\}$
  - So $(r_1, 0)(r_1', 0) = (r_1 r_1', 0) \neq (0,0)$ i.e. $r_1 r_1' \neq 0$

Proposition 66: Finite Domain is a Field

- Statement
  - **A finite domain $\boldsymbol{R}$ is a field**
- Proof
  - Let $a \in R \setminus \{0\}$
  - We want to show that a has a multiplicative inverse
  - Define a function $F: R \to R$ given by $r \mapsto ar$
  - F is injective
    - Suppose $F(r_1) = F(r_2)$
    - Then $ar_1 = ar_2$
    - So $a(r_1 - r_2) = 0$
    - Since R is a domain, $r_1 - r_2 = 0$
    - Thus, $r_1 = r_2$

- F is surjective since R is finite
- Choose $b \in R$ s.t. $F(b) = 1$, then $ab = 1$
- So b is the inverse of a

Subring

- Definition
  - A **subring** of a ring R is a **additive subgroup** S of R s.t.
  - S is **closed under multiplication**
  - S **contains 1**
- Note
  - A subring of a ring is also a ring
- Example 1
  - A ring is always a subring of itself
- Example 2
  - $\{n \times n \text{ scalar matrix}\} \subseteq \{n \times n \text{ diagonal matrix}\} \subseteq \mathrm{Mat}_{n \times n}(\mathbb{R})$
- Example 3
  - $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$
- Example 4
  - Let $R \coloneqq \{\text{continuous function from } \mathbb{R}^n \text{ to } \mathbb{R} \text{ for some } n \geq 1\}$
  - Define addition and multiplication as
    - $(f + g)(v) = f(v) + g(v)$
    - $(fg)(v) = f(v)g(v)$
    - $f = 1$ is the multiplicative identity
  - Then {polynomial functions with n variables} is a subring of R
- Example 5
  - If $f: R \to S$ is a **ring homomorphism** i.e.
    - f is a homomorphism of abelian groups under addition
    - $\boldsymbol{f(r_1 r_2) = f(r_1)f(r_2), \forall r_1, r_2 \in R}$
    - $\boldsymbol{f(1_R) = 1_S}$
  - Then $\mathrm{im}(f)$ is a subring of S
  - Proof
    - By group theory, $\mathrm{im}(f)$ is an additive subgroup of S
    - $1 \in \mathrm{im}(f)$ by assumption
    - If $f(r_1), f(r_2) \in \mathrm{im}(f)$, then $f(r_1)f(r_2) = f(r_1 r_2) \in \mathrm{im}(f)$
- Example 6
  - By HW9 #1, $\exists!$ Ring homomorphism $f: \mathbb{Z} \to R$ for any ring R
  - $\mathrm{im}(f)$ is the smallest subring of R

    - Also, $\text{im}(f) \cong \mathbb{Z}/n\mathbb{Z}$, where $n = \text{char}(R)$
    - Note: A **ring isomorphism** is a ring homomorphism that is **bijective**
- Example 7
    - $\{(r_1, 0) | r_1 \in R_1\} \subseteq R_1 \times R_2$ is not a subring
    - Since it doesn't contain the identity (1,1)

Polynomial Ring, Ideal, Principal Ideal

Monday, April 23, 2018 9:57 AM

Polynomial Ring

- Polynomials over a ring
  - Let R be a **commutative ring**
  - A **polynomial over R** is the sum
    - $\boldsymbol{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0}$, where
    - x is a variable, and $a_i \in R$
- Degree
  - Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial over R
  - The **degree** of f, denoted as $\mathbf{deg}(\boldsymbol{g})$, is $\mathbf{sup}\{\boldsymbol{n} \geq \mathbf{0} | \boldsymbol{a_n} \neq \mathbf{0}\}$
  - Note: $\deg(0) = -\infty$
- Leading term and leading coefficient
  - If $\deg(f) = n \geq 0$
  - The **leading term** of f is $\boldsymbol{a_n x^n}$
  - The **leading coefficient** of f is $\boldsymbol{a_n}$
- Polynomial ring
  - Let $\boldsymbol{R}[\boldsymbol{x}] \coloneqq \{$**Polynomials over a commutative ring $\boldsymbol{R}$**$\}$
  - Then $R[x]$ is a **commutative ring** with
  - ordinary addition and multiplication of polynomials
- **$\boldsymbol{R}$ is a subring of $\boldsymbol{R}[\boldsymbol{x}]$**
  - R is identified with the **constant polynomials**
  - There is a ring homomorphism $i: R \to R[x]$ defined as
  - mapping the ring element $r \in R$ to the constant polynomial r
  - The constant polynomials in $R[x]$ form a subring
  - And i gives an isomorphism between R and the subring
- Polynomial ring with **multiple variables**
  - We define polynomial rings in several variables inductively
  - $R[x_1, x_2] = (R[x_1])[x_2]$
  - $\vdots$
  - $\boldsymbol{R}[\boldsymbol{x_1}, \dots, \boldsymbol{x_n}] = (\boldsymbol{R}[\boldsymbol{x_1}, \dots, \boldsymbol{x_{n-1}}])[\boldsymbol{x_n}]$

Proposition 67: Polynomial Rings over a Domain

- Statement
  - Let R be a **domain**

- Let $p, q \in R[x] \setminus \{0\}$, then

1. $\mathbf{deg}(\boldsymbol{pq}) = \mathbf{deg}(\boldsymbol{p}) + \mathbf{deg}(\boldsymbol{q})$
2. $(\boldsymbol{R}[\boldsymbol{x}])^{\times} = \boldsymbol{R}^{\times}$
3. **$\boldsymbol{R}[\boldsymbol{x}]$ is a domain**

- Proof
  - Write
    - $p = a_n x^n + \cdots + a_1 x + a_0$, where $\deg(p) = n$
    - $q = b_m x^m + \cdots + b_1 x + b_0$, where $\deg(q) = m$
  - Then $a_n \neq 0$ and $b_m \neq 0$
  - Since R is a domain, $a_n m_m \neq 0$
  - So, the leading term of pq is $a_n b_m x^{m+n}$, which verifies (1)
  - Also, $a_n b_m x^{m+n} \neq 0$. This proves (3)
  - For (2), suppose $pq = 1$, then
    - $\deg(p) + \deg(q) = \deg(pq) = 0$ by (1)
    - Thus, $\deg(p) = 0 = \deg(q)$ i.e. $p, q \in R$
    - Since $pq = 1, p, q \in R^{\times}$
    - Thus $(R[x])^{\times} \subseteq R^{\times}$
    - Also, $R^{\times} \subseteq (R[x])^{\times}$
    - Therefore $(R[x])^{\times} = R^{\times}$

Ideal

- Definition
  - Let I be a subset of ring R, and let $r \in R$
  - Define $rI \coloneqq \{rx | x \in I\}$
  - I is a **left ideal** of R if
    - I is an **additive subgroup** of R
    - $\boldsymbol{rI} = \boldsymbol{I}, \forall \boldsymbol{r} \in \boldsymbol{R}$
  - Right ideal is defined similarly
  - I is an **ideal** if I is **both a left and right ideal**
- Intuition
  - Normal subgroups are to groups as ideals are to rings
- Example
  - If R is a ring, then R and $\{0\}$ are both ideals

Proposition 68: Ideal Containing 1 is the Whole Ring

- Statement
  - If $I \subseteq R$ is an ideal, then $\boldsymbol{I} = \boldsymbol{R} \Leftrightarrow \mathbf{1} \in \boldsymbol{I}$
- Proof ($\Longrightarrow$)

    - Trivial
- Proof ($\Longleftarrow$)
    - By definition of ideal, $rI = I, \forall r \in R$
    - So $r = r \cdot 1 \in I$
    - Thus $R = I$
- Corollary
    - Recall that subrings always contain 1
    - If S is a subring of ring R, then
        - $S \subseteq R$ is an ideal $\Leftrightarrow S = R$
    - If $I \subseteq R$ is an ideal, then
        - I is a subring of $R \Leftrightarrow I = R$

Principal Ideal

- Definition
    - Let R is a **commutative ring**, and let $r \in R$, then
    - $(r) \coloneqq \{ar | a \in R\}$ is called the **principal ideal generated by $\boldsymbol{r}$**
- Proof: Principal ideals are ideals
    - $0 = 0 \cdot r \in (r)$, so (r) is not empty
    - Let $ar, br \in (r)$, then
        - $ar - br = (a - b)r \in (r)$
        - Therefore, (r) is an additive subgroup of R
    - Let $a \in R, br \in (r)$, then
        - $a(br) = abr \in (r)$
        - $(br)a = bra = abr \in (r)$
        - So $a(r) = (r)a, \forall a \in R$
- Example
    - If $n \in \mathbb{Z}$, then (n) is just the cyclic subgroup generated by n

Examples of Ideals, Quotient Ring

Wednesday, April 25, 2018 9:56 AM

Examples of Ideals

- $\{(\boldsymbol{n}) | \boldsymbol{n} \in \mathbb{Z}\}$ **is all of the ideals in** $\mathbb{Z}$
  - Let $I \subseteq \mathbb{Z}$ be a nonzero ideal
  - Let d be the smallest positive integer in I
  - $I \supseteq (d)$
    - This is clear
  - $(d) \supseteq I$
    - Suppose $x \in I$
    - Write $x = qd + r$ where $q, r \in \mathbb{Z}$, and $0 \leq r < d$
    - Then we have $r = x - qd$, where $x \in I, qd \in I$
    - So $r \in I$, and the minimality of d forces $r = 0$
    - Therefore $x \in (d)$
- If $f: R \to S$ is a ring homomorphism, then **ker $\boldsymbol{f}$ is an ideal**
  - $\ker f$ is an additive subgroup of R by group theory
  - Let $r \in R$, and $x \in \ker f$
  - Then $f(rx) = f(r)f(x) = 0 = f(x)f(r) = f(xr)$
  - Thus $xr, rx \in \ker f$
- There are **left ideals that are not right ideals**, and vice versa
  - Let $R = \mathrm{Mat}_n(S)$, where S is any ring
  - Let $1 \leq k \leq n$
  - Let $C_k \coloneqq \{\text{matrices with 0 entries except in the } k^{\text{th}} \text{ column}\} \subseteq R$
  - C_k is a left ideal
    - Let $A \in \mathrm{Mat}_n(S)$, and $B \in C_k$
    - The (i, j) entry of AB is the dot product of i-th row and j-th column
    - It's clear that the (i, j) entry of AB is 0 unless $j = k$
  - C_k is not a right ideal
    - $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \in C_2 \subseteq \mathrm{Mat}_2(\mathbb{R})$
    - $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin C_2$
  - Similarly, $R_k \coloneqq \{\text{matrices with 0 entries except in the } k^{\text{th}} \text{ row}\} \subseteq R$
  - Then R_k is a right ideal, but not left ideal

Proposition 69: Quotient Ring

- Statement
    - Let R be a ring
    - If $I \subseteq R$ is an ideal, then the **quotient group R/I** is a ring with multiplication
        - $\boldsymbol{(r+I)(r'+I) = rr'+I}$
    - Conversely, if
        - **$J \subseteq R$ is an additive subgroup**
        - **R/J is a ring with multiplication** defined above
    - Then J is an ideal
- Proof ($\Longrightarrow$)
    - Multiplication is well-defined
        - Let $r_1 + I = r_2 + I$, and $r_1' + I = r_2' + I$
        - We must show that $r_1 r_1' + I = r_2 r_2' + I$
        - $r_1 r_1' - r_2 r_2' = r_1 r_1' + r_1 r_2' - r_1 r_2' - r_2 r_2' = r_1(r_1' - r_2') + (r_1 - r_2) r_2'$
        - $\begin{cases} r_1 + I = r_2 + I \\ r_1' + I = r_2' + I \end{cases} \Rightarrow \begin{cases} r_1 - r_2 \in I \\ r_1' - r_2' \in I \end{cases} \Rightarrow r_1 r_1' - r_2 r_2' \in I$
        - Thus $r_1 r_1' + I = r_2 r_2' + I$
    - $1_{R/I} = 1 + I$
    - Associativity and distributivity of R/I follow from analogous properties of R
- Proof ($\Longleftarrow$)
    - Suppose $J \subseteq R$ is an additive subgroup, and R/J is a ring with above operation
    - Then $f: R \to R/J$ given by $r \mapsto r + J$ is a ring homomorphism with $\ker f = J$
    - Thus, J is an ideal

Isomorphism Theorems for Rings

Friday, April 27, 2018 10:08 AM

Theorem 70: The First Isomorphism Theorem for Rings

- Statement
  - If $f: R \to S$ is a **ring homomorphism**, then there is an induced **isomorphism**
  - $\boldsymbol{\bar{f}: R/\ker f \to \mathrm{im}(f)}$, given by $\boldsymbol{r + \ker f \mapsto f(r)}$
- Proof
  - We need only check $\boldsymbol{\bar{f}\left(1_{R/\ker f}\right) = 1_S}$, and $\boldsymbol{\bar{f}}$ **preserves multiplication**
  - $\bar{f}\left(1_{R/\ker f}\right) = \bar{f}(1 + \ker f) = f(1_R) = 1_S$
  - $\bar{f}\big((r_1 + I)(r_2 + I)\big) = \bar{f}(r_1 r_2 + I) = f(r_1 r_2) = f(r_1)f(r_2) = \bar{f}(r_1 + I)\bar{f}(r_2 + I)$
- Example: $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$
  - Let $F: \mathbb{R}[x] \to \mathbb{C}$ given by $p \mapsto p(i)$
  - F is a ring homomorphism
    - In fact, if R is a subring of some ring S, and $s \in S$, then
    - The function $\boldsymbol{R[x] \to S}$ given by $\boldsymbol{p \mapsto p(s)}$ is a **ring homomorphism**
  - F is surjective
    - If $a + bi \in \mathbb{C}$, then $F(a + bx) = a + bi$
  - $(x^2 + 1) \subseteq \ker f$
    - If $p(x^2 + 1) \in (x^2 + 1)$, then
    - $F\big(p(x^2 + 1)\big) = F(p)F(x^2 + 1) = p(i)p(i^2 + 1) = 0$
  - $\ker f \subseteq (x^2 + 1)$
    - Let $p \in \ker f$
    - Using polynomial division, we can find $q, r \in \mathbb{R}[x]$ s.t.
    - $p = q(x^2 + 1) + r$ where $\deg r < \deg(x^2 + 1) = 2$
    - Write $r = ax + b$ for some $a, b \in \mathbb{R}$
    - Since $p \in \ker f$, $p(i) = 0$
    - $0 = p(i) = q(i) \times (i^2 + 1) + r(i) = r(i) = ai + b$
    - So $a = b = 0$
    - Therefore $p = q(x^2 + 1)$, and $p \in (x^2 + 1)$
  - Therefore, $\ker f = (x^2 + 1)$
  - By the First Isomorphism Theorem of Rings, $\mathbb{R}[\boldsymbol{x}]/\big(\boldsymbol{x^2 + 1}\big) \cong \mathbb{C}$
- Example: $\mathbb{R}[x]/(x - a) \cong \mathbb{R}$, where $a \in \mathbb{R}$
  - Let $F: \mathbb{R}[x] \to \mathbb{R}$ given by $p \mapsto p(a)$
  - F is surjective

        - $F(b) = b, \forall b \in \mathbb{R}$
    - F is a ring homomorphism
    - $(x-a) \subseteq \ker f$
        - If $p(x-a) \in (x-a)$, then
        - $F\big(p(x-a)\big) = F(p)F(x-a) = p(a)p(a-a) = 0$
    - $\ker f \subseteq (x-a)$
        - Let $p \in \ker f$
        - Divide $x-a$ into p to obtain $q, r \in \mathbb{R}[x]$ s.t.
        - $p = q(x-a) + r$, where $\deg r < 1$
        - Since $p \in \ker f$, $0 = p(a) = q(a)(a-a) + r = r$
        - Thus $r = 0$, so $p = q(x-a) \in (x-a)$
    - Therefore, $\ker f = (x-a)$
    - By the First Isomorphism Theorem of Rings, $\mathbb{R}[x]/(x-a) \cong \mathbb{R}$
- Example: $\mathbb{R}[x]/(x^2-1) \cong \mathbb{R} \times \mathbb{R}$
    - Recall: Chinese Remainder Theorem
        - If I, J are ideals in a **commutative ring** R s.t. $\boldsymbol{I + J = R}$
        - Then $\boldsymbol{R/IJ} \cong \boldsymbol{R/I} \times \boldsymbol{R/J}$, where
        - $I + J = \{x + y | x \in I, y \in J\}$
        - $IJ = \{x_1y_1 + \cdots + x_ny_n | n \in \mathbb{Z}_{\geq 1}, x_i \in I, y_i \in J\}$
    - $(x^2-1) \subseteq (x+1)(x-1)$
        - This is obvious, since $x^2 - 1 \in (x+1)(x-1)$
    - $(x+1)(x-1) \subseteq (x^2-1)$
        - Let $p_1q_1 + \cdots + p_nq_n \in (x-1)(x+1)$, where $p_i \in (x-1), q_i \in (x+1)$
        - Each term p_iq_i is of form
            - $f_i(x-1) \cdot g_i(x+1) = f_ig_i(x^2-1)$ for some $f_i, g_i \in \mathbb{R}$
        - Thus $p_iq_i \in (x^2-1) \Rightarrow p_1q_1 + \cdots + p_nq_n \in (x^2-1)$
    - Thus $(x^2-1) = (x+1)(x-1)$
    - $\mathbb{R}[x]/(x+1)(x-1) \cong \mathbb{R} \times \mathbb{R}$
        - $\dfrac{1}{2}(x+1) - \dfrac{1}{2}(x-1) = 1 \in \mathbb{R}[x]$
        - $\Rightarrow (x+1) + (x-1) = \mathbb{R}[x]$
        - $\Rightarrow 1 \in (x+1) + (x-1)$
        - Chinese Remainder Theorem implies $\mathbb{R}[x]/(x+1)(x-1) \cong \mathbb{R} \times \mathbb{R}$
    - Therefore, $\mathbb{R}[x]/(x^2-1) \cong \mathbb{R} \times \mathbb{R}$

Other Isomorphism Theorems for Rings

- The Second Isomorphism Theorem for Rings
    - If I is an ideal of a ring R, and S is a subring of R

- Then $S + I$ is also a subring of R, where
- I is an ideal of $S + I$, and $\boldsymbol{(S + I)/I \cong S/(I \cap S)}$

- The Third Isomorphism Theorem for Rings
  - If $I \subseteq J$ are ideals of a ring R, then $\boldsymbol{{}^{R/I}\!/_{J/I} \cong R/J}$

- Correspondence Theorem
  - If R is a ring, and I is an ideal of R
  - Then there is a bijection $\{\textbf{ideals of } \boldsymbol{R/I}\} \leftrightarrow \{\textbf{ideals of } \boldsymbol{R} \textbf{ containing } \boldsymbol{I}\}$

Ideal Generated by Subset, Maximal Ideal

Monday, April 30, 2018 10:00 AM

Ideal Generated by Subset

- Definition
  - Let R be a **commutative ring**
  - If A is a subset of R, then the **ideal generated by A** is
  - $(\boldsymbol{A}) \coloneqq \{\boldsymbol{r_1 a_1} + \cdots + \boldsymbol{r_n a_n} | \boldsymbol{n} \in \mathbb{Z}_{\geq 1}, \boldsymbol{r_i} \in \boldsymbol{R}, \boldsymbol{a_i} \in \boldsymbol{A}\} \subseteq \boldsymbol{R}$
  - If A is finite, then we write (A) as $(a_1, \dots, a_n)$
- Note
  - When $|A| = 1$, (A) is a principal ideal
- Example: $(2, x) \subseteq \mathbb{Z}[x]$
  - Suppose, by way of contradiction, that $(2, x) = (p)$ for some $p \in \mathbb{Z}[x]$
  - Since $2 \in (p)$
    - $2 = pq$ for some $q \in \mathbb{Z}[x]$
    - $0 = \deg 2 = \deg p + \deg q$
    - $\deg p = \deg q = 0$
  - Since $x \in (p)$
    - Choose $r \in \mathbb{R}[x]$ s.t. $pr = x$, then $\deg r = 1$
    - Write $r = ax + b$, where $a, b \in \mathbb{Z}$
    - Then $pr = p(ax + b) = x$
    - So $pa = 1$, by comparing coefficients
    - Since $p \in \mathbb{Z}[x]$ and $a \in \mathbb{Z}$, $p \in \{\pm 1\}$
  - Therefore $(2, x) = (p) = \mathbb{Z}[x]$
  - So, $1 = 2p' + xq'$, where $p', q' \in \mathbb{Z}[x]$
  - Evaluating both side at 0, we get $1 = 2p'(0) = 0$
  - This is a contradiction, so $(2, x) \subseteq \mathbb{Z}[x]$
- Example: $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/(2)$
  - Define $F: \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$ given by $a_0 x^n + \cdots + a_1 x + a_0 \mapsto \overline{a_0}$
  - F is a ring homomorphism
    - F factors as $\mathbb{Z}[x] \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, where $p \mapsto p(0) \mapsto p\overline{(0)}$
    - Composition of homomorphisms is still a homomorphism
  - F is certainly surjective
  - $(2, x) \subseteq \ker F$
    - Let $p \in (2, x)$
    - Then $p = 2g + xh$ for some $g, h \in \mathbb{Z}[x]$

- Since xh has no constant term, and $2g$ has even constant term
- $F(p) = F(2g) = F(g) = \bar{0} \in \mathbb{Z}/2\mathbb{Z}$
  - $\ker F \subseteq (2, x)$
    - Let $p = a_n x^n + \cdots + a_1 x + a_0 \in \ker F$
    - Write $a_0 = 2b$, where $b \in \mathbb{Z}$
    - Then $p = x(a_n x^{n-1} + \cdots + a_1) + 2b \in (2, x)$
  - Therefore, $\ker F = (2, x)$
  - By the First Isomorphism Theorem of , $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/(2)$
  - Note: $\mathbb{Z}[x]/(x, n) \cong \mathbb{Z}/(n)$

Maximal Ideal

- An ideal M in a ring R is **maximal** if
- $\boldsymbol{M \neq R}$, and **the only ideals containing $\boldsymbol{M}$ are $\boldsymbol{M}$ and $\boldsymbol{R}$**

Proposition 71: Criterion for Maximal Ideal

- Statement
  - If R is a commutative ring, and $M \subseteq R$ is an ideal
  - Then **$\boldsymbol{M}$ is maximal $\Leftrightarrow$ $\boldsymbol{R/M}$ is a field**
- Proof ($\Longrightarrow$)
  - The only ideals containing M are R and M
  - Thus, R/M has exactly 2 idals, by the Correspondence Theorem
  - Namely, the zero ideal, and the entire ring
  - Let $x + M \in R/M$ s.t. $x \notin M$
  - Suppose $x \notin M$ i.e. $x + M \neq 0_{R/M}$
  - Then $(x + M) = R/M$
  - So $1 + M \in (x + M)$
  - Choose $y + M \in R/M$ s.t. $(x + M)(y + M) = 1 + M$
  - This shows $x + M$ is a unit
  - Therefore R/M is a field
- Proof ($\Longleftarrow$)
  - Suppose R/M is a field
  - Then R/M has exactly two ideals, 0 and R/M
  - By the Correspondence Theorem,
  - There are exactly two ideals containing M, that is R and M
  - By definition of maximal ideal, M is maximal

Examples of Maximal Ideals

- What are the maximal ideals in $\mathbb{Z}$?
  - $(n) \in \mathbb{Z}$ is maximal $\Leftrightarrow$ $\mathbb{Z}/(n)$ is a field $\Leftrightarrow$ n is prime

- Is $(x) \subseteq \mathbb{Z}[x]$ maximal?
  - No, $(x) \subsetneq (2, x) \neq \mathbb{Z}[x]$
  - Also, by First Isomorphism Theorem, $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, but $\mathbb{Z}$ is not a field
    - Define a ring map $\mathbb{Z}[x] \to \mathbb{Z}$ given by $p \to p(0)$
    - F is surjective, and $\ker F = (x)$
- Is $(x^2 + 1) \subseteq \mathbb{R}[x]$ maximal?
  - $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ is a field
- Is $(x^2 - 1) \subseteq \mathbb{R}[x]$ maximal
  - $\mathbb{R}[x]/(x^2 - 1) \cong \mathbb{R} \times \mathbb{R}$ is not a field, since $(1,0)$ is not a unit
  - Another way to see $(x^2 - 1)$ is not maximal
    - $(x^2 - 1) \subsetneq (x - 1) \subsetneq \mathbb{R}[x]$
    - $(x^2 - 1) \subsetneq (x + 1) \subsetneq \mathbb{R}[x]$

Prime Ideal, Euclidean Domain

May 2, 2018 10:00 AM

Prime Ideal

- Let R be a commutative ring
- An ideal $P \subsetneq R$ is **prime** if
- $\boldsymbol{a, b \in R}$, and $\boldsymbol{ab \in P \Rightarrow a \in P}$ **or** $\boldsymbol{b \in P}$

Proposition 72: Prime Ideas of $\mathbb{Z}$

- Statement
    - The **prime ideals** of $\mathbb{Z}$ are ideals of the form $(\boldsymbol{n})$, where $\boldsymbol{n}$ **is prime** or $\boldsymbol{n = 0}$
- Proof ($\Longrightarrow$)
    - Let $(n) \subseteq \mathbb{Z}$ be a prime ideal, and $n \neq 0$
    - We want to show that n is prime
    - Choose $a, b \in \mathbb{Z}$ s.t. $n = ab$
    - Then $ab \in (n)$, so either $a \in (n)$ or $b \in (n)$, by definiton of prime ideal
    - Without loss of generality, suppose $a \in (n)$, then $n|a$
    - Choose $q \in \mathbb{Z}$ s.t. $nq = a$
    - $n = ab \Rightarrow n = nqb \Rightarrow 1 = qb \Rightarrow b \in \{\pm 1\}$
    - So n is a prime
- Proof ($\Longleftarrow$)
    - (0) is prime
        - Let $a, b \in \mathbb{Z}$, and $ab \in (0)$
        - Then $ab = 0$
        - $\Rightarrow a = 0$ or $b = 0$
        - $\Rightarrow a \in (0)$ or $b \in (0)$
        - Therefore (0) is prime
    - (p) is prime for $p \in \mathbb{Z}$ prime
        - Let $a, b \in \mathbb{Z}$, and say $ab \in (p)$
        - Then $p|ab$
        - Since p is prime, this means $p|a$ or $p|b$
        - $\Rightarrow a \in (p)$ or $b \in (p)$

Proposition 73: Criterion for Prime Ideal

- Statement
    - Let R be a commutative ring, $P \subseteq R$ an ideal, then
    - $\boldsymbol{P}$ **is prime** $\Leftrightarrow$ $\boldsymbol{R/P}$ **is a domain**

- In particular, R is a domain $\Leftrightarrow$ zero ideal is prime

- Proof ($\Longrightarrow$)
  - Let $a + P, b + P \in (R/P) \setminus \{P\}$
  - Then $(a + P)(b + P) = ab + P = 0$
  - So, $ab \in P$
  - Since P is prime, $a \in P$ or $b \in P$
  - Therefore $a + P = 0$ or $b + P = 0$
  - So R/P is a domain
- Proof ($\Longleftarrow$)
  - Let $a, b \in R$, and suppose $ab \in P$, then
  - $0 = ab + P = (a + P)(b + P)$
  - Since R/P is a domain, $a + P = 0$ or $b + P = 0$
  - So $a \in P$ or $b \in P$
  - Therefore P is prime
- Example
  - $(x^2 - 1) \subseteq \mathbb{R}[x]$ is not prime, since $\mathbb{R}[x]/(x^2 - 1) \cong \mathbb{R} \times \mathbb{R}$ is not a domain
  - Also, $x^2 - 1 \in (x^2 - 1)$, but $x - 1, x + 1 \notin (x^2 - 1)$

Corollary 74: Maximal Ideal is Prime

- Statement
  - If R is a commutative ring, and $\boldsymbol{M \subseteq R}$ **is maximal**, then $\boldsymbol{M}$ **is prime**
- Proof
  - M is maximal $\Rightarrow R/M$ is a field $\Rightarrow R/M$ is a domain $\Rightarrow M$ is prime

Euclidean Domain

- Definition
  - Let R be a domain
  - A **norm** on R is a function $N: R \to \mathbb{Z}_{\geq 0}$ s.t. $N(0) = 0$
  - R is called a **Euclidean domain** if R is equipped with a norm N s.t.
  - $\forall a, b \in R$ with $b \neq 0$, $\exists q, r \in R$ s.t.
    - $a = qb + r$, and
    - either $r = 0$ or $N(r) < N(b)$
- Example 1
  - $\mathbb{Z}$ is a Euclidean domain, $N(a) = |a|$
- Example 2
  - If F is a field, then F is trivially a Euclidean domain
  - Take $N: F \to \mathbb{Z}_{\geq 0}$ to be any function s.t. $N(0) = 0$

- Then, if $a, b \in F$, where $b \neq 0$, take $q = \frac{a}{b}, r = 0$
- Example 3
  - If F is a field, then $F[x]$ is a Euclidean domain, with $N(p) = \deg p$
  - The division algorithm is just polynomial division
  - Note
    - $\deg 0 = -\infty \notin \mathbb{Z}_{\geq 0}$, so this definition isn't quite right
    - To handle this problem, define a norm that sends values not in $\mathbb{Z}_{\geq 0}$, but
    - any total ordered set in order-preserving bijection with $\mathbb{Z}_{\geq 0}$
    - (For instance, $\mathbb{Z}_{\geq 0} \cup \{-\infty\}$)

Principal Ideal Domain

- A domain in which **every ideal is principal** is called a **principal ideal domain**

Proposition 75: Euclidean Domain is a Principal Ideal Domain

- Statement
  - Every **ideal** in a **Euclidean domain** R is **principal**
  - More precisely, if $I \subseteq R$ is an ideal, then $I = (d)$, where
  - d is an element of I with minimum norm
- Proof
  - Let $I \subseteq R$ be an ideal
  - If $I = (0)$, then I is principal, so assume $I \neq (0)$
  - $\{N(a) | a \in I \setminus \{0\}\}$ has a minimal element, by well-ordering principal
  - Choose $d \in I \setminus \{0\}$ s.t. $N(d)$ is minimal
  - Certainly, $(d) \subseteq I$
  - Let $a \in I$, write $a = qd + r$, where
    - $q, r \in R$, and
    - either $r = 0$ or $N(r) < N(d)$
  - Since $r = a - qd \in I$, $N(r)$ can't be smaller than $N(d)$
  - So $r = 0 \Rightarrow a = qd \Rightarrow a \in (d)$
  - Therefore $I \subseteq (d)$
- Example 1
  - We haven't yet proven that $F[x]$ is a Euclidean domain, where F is a field
  - Once we show this, then $F[x]$ has the property that all of its ideals are principal
- Example 2
  - $\mathbb{Z}[x]$ cannot be a Euclidean domain, since $(2, x) \subseteq \mathbb{Z}[x]$ is not principal

Theorem 76: Polynomial Division

- Statement

- Let F be a field, then $\boldsymbol{F[x]}$ **is a Euclidean domain**
- More specifically, if $a, b \in F[x]$ where $b \neq 0$, then
- $\exists!\, q, r \in F[x]$ s.t. $a = bq + r$ and $\deg r < \deg b$

- Proof (Existence)
  - We argue by induction on $\deg a$
  - If $a = 0$, take $q, r = 0$, so assume $a \neq 0$
  - Set $n \coloneqq \deg a\,, m \coloneqq \deg b$
  - If $n < m$, then take $q = 0, r = a$
  - Assume $n \geq m$
  - Write
    - $a = a_n x^n + \cdots + a_1 x + a_0$
    - $b = b_m x^m + \cdots + b_1 x + b_0$
  - Set $a' = a - \frac{a_n}{b_m} x^{n-m} b$
    - Then $\deg a' < \deg a$
    - Since a and $\frac{a_n}{b_m} x^{n-m} b$ have the same leading coefficient
  - By inductive hypothesis
    - $\exists q', r \in F[x]$ with $a' = q'b + r$ and $\deg r < \deg b$
  - Set $q = q' + \frac{a_n}{b_m} x^{n-m} b$, then
    - $a = a' + \frac{a_n}{b_m} x^{n-m} b$
    - $= q'b + r + \frac{a_n}{b_m} x^{n-m} b$
    - $= \left(q' + \frac{a_n}{a_m} x^{n-m}\right) b + r$
    - $= qb + r$
- Proof (Uniqueness)
  - Suppose $bq' + r' = a = bq + r$ where $\deg r < \deg b$, and $\deg r' < \deg b$
  - Then $\deg(a - bq) < \deg b$ and $\deg(a - bq') < \deg b$
  - $\Rightarrow \deg\big((a - bq) - (a - bq')\big) = \deg(bq' - bq) = \deg b + \deg(q' - q) < \deg b$
  - $\Rightarrow \deg(q' - q) < 0 \Rightarrow q' = q$
  - It follows immediately that $r' = r$