0. PRELIMINARIES

0.1. BASICS [SET THY].

Remark.
- assume basic set theory: sets, $\cap$, $\cup$, $\in$, etc
- ntn: subset of A: $\{x \in A | ...(\text{condition on } x)...\}$
- should know how to test whether $x \in A$ lies in $B \subseteq A$

Definition.
- order ("cardinality") of set A, $|A|$
  for finite: # elements
- cartesian product $A \times B = \{(a,b) | a \in A, b \in B\}$
  ie the set of ordered pairs from A, B
- common sets:
  $\mathbb{Z}$
  $\mathbb{Q} = \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$
  $\mathbb{R}$ = {all decimal expansions $\pm d_1 d_2 ... d_n . a_1 a_2 a_3 ...$}
  $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}, i^2 = -1\}$
  $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ are positive (nonzero)

FUNCTIONS

Definition.
- function ("map") $f : A \to B$ ("$A \xrightarrow{f} B$") from domain A to codomain B st value $f(a) \in B$ for each $a \in A$
  ntn: "function specified on elements" $f : a \mapsto b$
  ntn: drop "f" if understood or not needed
- well defined means unambiguously determined
- range ("image") of f is $f(A) = \{b \in B | \exists a f(a) = b\}$
- preimage ("inverse image") of $C \subseteq B$ under f is $f^{-1}(C) = \{a \in A | f(a) \in C\}$
- the fiber of f over $b \in B$ is $f^{-1}(\{b\})$ (note: a set)
- composite map $g \circ f : A \to C$ where $f : A \to B$, $g : B \to C$, is $(g \circ f)(a) = g(f(a))$

*JECTIVES AND INVERSES

Definition. let $f : A \to B$
- injective: $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$
- surjective: $\forall b \in B \exists a \in A f(a) = b$ ie $f(A) = B$
- bijective: both injective and surjective
- left inverse of f is $g : B \to A$ st $g \circ f : A \to A$ is the identity map of A
  right inverse is analogous
  inverse ("two-sided inverse") is $g : B \to A$ st $f \circ g$ and $g \circ f$ are identity maps on B and A

Proposition. *(1) let $f : A \to B$*
(1) injective iff has left inverse
(2) surjective iff has right inverse
(3) bijective iff $\exists$ inverse $g : B \to A$
(4) let A, B finite and $|A| = |B|$
f bijective iff f injective iff f surjective

EXTRA FUNCTIONS STUFF

Definition.
- a permutation of set A is a bijection of A to itself
- the restriction of $f : A \to B$ to $C \subset A$ is $f|_C : C \to B$, $c \mapsto f(c)$ $\forall c \in C$
- an extension of $g : A \to C$ to $B \supset A$ is $f : B \to C$ st $f|_A = g$

RELATIONS

Definition.
- a binary relation on A is a subset $R \subseteq A \times A$
- types of binary relations:
  reflexive: $\forall a \in A$ $a \sim a$
  symmetric: $\forall a, b \in A$ $a \sim b \Rightarrow b \sim a$
  transitive: $\forall a, b, c \in A$ $a \sim b, b \sim c \Rightarrow a \sim c$

EQUIV REL $\Leftrightarrow$ PARTITION

Definition.
- equivalence relation: reflexive, symmetric, transitive
- the equivalence class of $a \in A$ wrt some equiv rel $\sim$ is $\{x \in A | x \sim a\}$
  x equivalent to a means in same equivalence class
  a representative of an equivalence class C is any element of C
- a partition of A is a collection $\{A_i | i \in I\}$, I index set, of nonempty subsets st $A = \cup_{i \in I} A_i$ and for $i, j \in A$ nonequal, $A_i \cap A_j = \emptyset$
  ie A is a disjoint union of the sets in the partition

Proposition. *(2)*
Let A nonempty set.
(1) $\sim$ is an equivalence relation on A
$\Rightarrow$ the set of equiv classes of $\sim$ form a partition of A
(2) $\{a_i\}$ is a partition of A
$\Rightarrow \exists$ equiv rel on A whose equivalence classes are precisely $\{A_i\}$

Remark. finally, we assume familiarity with proofs by induction

0.2. PROPERTIES OF THE INTEGERS.

Remark.
- this section is needed in Part I: Group Thy
  but will prove a generalization in Part II: Ring Thy (without needing this section or Part I)
- this section is 10 properties of integers

(1)

Claim. (well ordering of $\mathbb{Z}$)
$A \subseteq \mathbb{Z}^+$ nonempty $\Rightarrow \exists m \in A$ minimal element of A (ie $\forall a \in A$, $m \leq a$)

(2)

Definition. $a \in \mathbb{Z} \setminus \{0\}$ divides $b \in \mathbb{Z}$, $a \mid b$, means $\exists c \in \mathbb{Z}$ st $b = ac$
otherwise $a \nmid b$

(3)

Claim. let $a, b \in \mathbb{Z} \setminus \{0\}$
$\exists!$ greatest common divisor $d \in \mathbb{Z}$ (d is a divisor ($d \mid a$, $d \mid b$) and the greatest such divisor ($e \mid a, e \mid b \Rightarrow e \mid d$))
ntn $d = (a, b)$

Definition. a, b relatively prime means $(a, b) = 1$

(4)

Claim. let $a, b \in \mathbb{Z} \setminus \{0\}$
- $\exists!$ least common multiple $l \in \mathbb{Z}^+$ (l is a multiple ($a \mid l$, $b \mid l$) and the least such multiple ($a \mid m, b \mid m \Rightarrow l \mid m$))
- $dl = ab$

(5)

Claim. let $a, b \in \mathbb{Z} \setminus \{0\}$
$\exists! r, q \in \mathbb{Z}$ st $a = qb + r$ st $0 \leq r \leq |b|$
ntn: q is "quotient" and r is "remainder"

(6)

Claim. Euclidean algorithm for gcd of $a, b \in \mathbb{Z} \setminus \{0\}$
obtain sequence $r_0, r_1, ..., r_n$ of remainders
$a = q_0 b + r_0$
$b = q_1 r_0 + r_1$
$r_0 = q_2 r_1 + r_2$
$\vdots$
$r_{n-2} = q_n r_{n-1} + r_n$
$r_{n-1} = q_n r_n + 0$
r_n is gcd of a, b

Proof. exists since sequence $|b| > |r_0| > |r_1| > ... > |r_n|$ positive decreasing integers

Example. Euclidean algorithm with $a = 57970$ and $b = 10353$

(7)

Claim. $\forall a, b \in \mathbb{Z} \setminus \{0\}$ $\exists x, y \in \mathbb{Z}$ st $(a, b) = ax + by$
ie (a, b) is a $\mathbb{Z}$-linear combination of a and b

Proof. perform Euclidean algorithm on a, b
take second to last line $r_n = r_{n-2} - q_n r_{n-1}$
plug earlier lines for $r_{n-1}, r_{n-2}, ...$ until left with $ax + by$ for some x, y

Example. demonstrate using example from (6)

Remark. note: x, y but may not be unique
see exercise for general formula for x, y

(8)

Definition. prime $p \in \mathbb{Z}^+$ (positive for now), $p > 1$ means its only positive divisors are 1 and p
composite otherwise

Claim. let p prime, $a, b \in \mathbb{Z}$
$p \mid ab \Rightarrow p \mid a$ or $p \mid b$
(note: this characterization can be used to define the primes, see ex 3)

Theorem. *(Fundamental Thm of Arithmetic)*
if $n \in \mathbb{Z}$, $n > 1$
then n can be factored uniquely into primes
ie $\exists!$ distinct primes to positive integer powers st $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$

Claim. $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$ where powers can be 0
then $(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_s^{\min(\alpha_s, \beta_s)}$
and lcm is similar but with max

Example. apply to a, b from example from (6)
note: euclidean algorithm is faster for gcd, then lcm from dl=ab

(10)

Definition. Euler totient function ϕ (note "ϕ" can be used for other things)
$\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$, $\phi(n) =$# positive integers $a \leq n$ with $(a, n) = 1$ ie relatively prime

Example. $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$,

Claim.
- for p prime, $\phi(p) = p - 1$ and $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ where $\alpha \geq 1$
- if $(a, b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$ ie "multiplicative"
- cor: $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$
  $\phi(n) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_s^{\alpha_s}) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_s^{\alpha_s - 1}(p_s - 1)$

Example. $\phi(12) = 4$

0.3. $\mathbb{Z}/n\mathbb{Z}$: THE INTEGERS MODULO n.

Definition. [congruence relation] for $n \in \mathbb{Z}^+$ $a \sim b$ iff $n \mid (b - a)$
ntn: $a \equiv b \mod n$ read "a is congruent to b modulo n"

Claim. congruence relation is an equiv rel

Definition.
- congruence class ("residue class") of $a \mod n$ is equivalence class $\overline{a} = \{a + kn | k \in \mathbb{Z}\}$
  intuition: each congruence class has numbers with same remainder when divided by n
  ntn: before using overline, make sure n is fixed
  ntn: if understood, can drop overline, but do not accidently mistake equiv class for integer
- reduce $a \mod n$ means finding the least residue of a modulo n (smallest nonnegative integer congruent to $a \mod n$)
- the integers modulo n, $\mathbb{Z}/n\mathbb{Z}$, is the set of congruence classes
  ntn: "$\mathbb{Z}/n\mathbb{Z}$" motivated by quotient groups and quotient rings

Claim. there are n congruence classes modulo n: $\overline{0}, \overline{1}, ..., \overline{n-1}$

MODULAR ARITHMETIC

Theorem. *(3) (modular arithmetic)*
$\overline{a} + \overline{b} := \overline{a+b}$ *and* $\overline{a}\,\overline{b} := \overline{ab}$
where rhs uses any representatives

Proof. well defined:
Let a_1, b_1 congruent and a_2, b_2 congruent
(ie $\overline{a_1} = \overline{b_1}$ and $\overline{a_2} = \overline{b_2}$)
(ie $a_1 \equiv b_1 \mod n$ and $a_2 \equiv b_2 \mod n$)
(ie $a_1 = b_1 + sn$ and $a_2 = b_2 + tn$ for some $s, t \in \mathbb{Z}$)
want to show that modular arithmetic is indep of representative chosen
(ie $\overline{a_1 + a_2} = \overline{b_1 + b_2}$ and $\overline{a_1 a_2} = \overline{b_1 b_2}$)
(ie $a_1 + a_2 \equiv b_1 + b_2 \mod n$ and $a_1 a_2 \equiv b_1 b_2 \mod n$)
(ie $a_1 + a_2 = b_1 + b_2 + pn$ and $a_1 a_2 = b_1 b_2 + qn$)
this is true since $a_1 + a_2 = b_1 + b_2 + (s+t)n$ and $a_1 a_2 = (b_1 + sn)(b_2 + tn) = b_1 b_2 + (b_1 t + b_2 s + tsn)n$

Example. $n = 12$: $\overline{5} + \overline{8}$ and $\overline{5}\,\overline{8}$ can be computed with any representatives

Remark.
- these idea are common:
  - rational number addition also adds equiv classes by adding any representatives
  - modular arithmetic is used when adding or subtracting hours, then reducing mod 12
- will later generalize this to "quotients" where we also add equiv classes by adding any representatives

Example. application of modular arithmetic to finding last digits of some big power
find: last 2 digits of 2^{1000}
soln: find congruence class of $2^{1000} \mod 100$
$2^{10} = 1024 \equiv 24 \mod 100$
$2^{20} = (2^{10})^2 \equiv 24^2 = 576 \equiv 76 \mod 100$
$2^{40} = (2^{20})^2 \equiv 76^2 = 5776 \equiv 76 \mod 100$
$2^{80} \equiv 2^{160} \equiv 2^{320} \equiv 2^{640} \equiv 76 \mod 100$
$2^{1000} = 2^{640} 2^{320} 2^{20} \equiv 76 \cdot 76 \cdot 76 \equiv 76 \mod 100$
so last two digits are 76

MULTIPLICATION INVERSES OF CONGRUENCE CLASSES

Definition. $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} | \exists \overline{c} \in \mathbb{Z}/n\mathbb{Z} \text{ st } \overline{a} \cdot \overline{c} = \overline{1}\}$
ie the collection of residue classes with a multiplication inverse in $\mathbb{Z}/n\mathbb{Z}$

Proposition. *(4)*
$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} | (a,n) = 1\}$
ie the collection of residue classes whose representatives are relatively prime to n
note: well defined since if a representative a is relatively prime to n then its whole class is

Example. $(\mathbb{Z}/9\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$ (with respective inverses $\overline{1}, \overline{5}, \overline{7}, \overline{2}, \overline{4}, \overline{8}$)

Remark. can efficiently compute multiplicative inverse of $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$:
use method above to find x, y st $ax + ny = (a, n)$ $(= 1$ since prop 4$)$
note $ax \equiv 1 \mod n$ so $\overline{x}$ is multiplicative inverse of $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$

Example. Let: $n = 60$
find: multiplicative inverse of $a = 17$ (note $(60, 17) = 1$ so $\overline{17} \in (\mathbb{Z}/n\mathbb{Z})^\times$)
soln: euclidean algorithm gives $1 = (2)60 + (-7)17$
so $\overline{-7} = \overline{53}$ is multiplicative inverse of $\overline{17}$ in $\mathbb{Z}/60\mathbb{Z}$

PART I: GROUP THEORY

Remark.
- given def of group, want to know the structure of such objects
- result for abstract group applies to all examples of groups
- historically, similar techniques were used in algebraic eqns, number thy, and geometry, and people wondered about the scope of these methods, which motivated their def (1882) and study of groups in their own right
  (ie want to isolate specific characteristics and study structure of objects with these characteristics)
- the structure of an algebraic object (made precise by isomorphism between objects with same structure) is a recurring theme of this book

Example. some uses of groups before their definition
- in number thy, Euler's thm used group properties of integers, and were a special case of Lagrange's thm
- (diophantine eqns, elliptic integral)
  finding integer or rational slns to diophantine eqn $y^2 = x^3 - 2x$ can find a new soln geometrically by connecting two existing solns with a straight line and finding intersection with curve $y^2 = x^3 - 2x$. Euler solved elliptic integral $\int \frac{dx}{\sqrt{1-x^4}}$ to get arc length of an ellipse using a "multiplication formula" which took two elliptic integrals and gave rise to a third; this began the theory of elliptic functions in analysis
  Jacobi noticed connections between solving diophantine eqn and solving elliptic integrals and used above geometric operation to give a group structure to points on elliptic curve
- Abel and Galois showed that there is no formula for the roots of a quintic, using permutations of roots and groups of substitutions
  geometers Cayley, Jordan, Klein studied structure of 3-space and 4-space with groups of transformations (translations, reflections, etc)
  the same group is used in rigid motions of icosohedron, solving quintic, and study of elliptic functions

1. INTRO TO GROUPS

1.1. BASIC AXIOMS AND EXAMPLES.

Definition.
- binary opertation $\star : G \times G \to G$
  ntn: infix or prefix
- associative: $(a \star b) \star c = a \star (b \star c)$
  commutative: $a \star b = b \star a$

Example.
- $+$ on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ is commutative, associative
- $\times$ on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ is commutative and associative
- $-$ on $\mathbb{Z}$ is not commutative or associative
- vector cross product is binary operation $\mathbb{R}^k \times \mathbb{R}^k \to \mathbb{R}^k$ but not commutative or associative

Definition.
- $\star : G \times G \to G$ is closed under $H \subset G$ means $a \star b \in H \ \forall a, b \in H$
  then $\star|_H$ is also a binary operation

Claim. consider $\star : G \times G \to G$ closed under $H \subseteq G$
if $\star$ associative (commutative), then so is $\star|_H$
ie associativity and commutativity are preserved for "closed under"

Definition.
- a group is a set G and a binary operation $\star : G \times G \to G$ st
  (i) $\star$ associative
  (ii) $\exists e \in G$ identity $(\forall a \in G \ a \star e = e \star a = a)$
  note: implies nonempty
  (iii) $\forall a \in G \ \exists a^{-1} \in G$ inverse $(a \star a^{-1} = a^{-1} \star a = e)$
- abelian group is also commutative
- finite group has G finite

Remark. ntn: G instead of $(G, \star)$
ntn: ab instead of $a \star b$

Example.
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ with $e = 0$ and $a^{-1} = -a \ \forall a$
  pf: associativity of $\mathbb{N}$ implies that of $\mathbb{Z}$, which implies that of $\mathbb{Q}$ ... $\mathbb{R}$ ... $\mathbb{C}$
  note: we will not construct $\mathbb{R}$ from $\mathbb{Q}$
- $(\mathbb{Q}^+, \times)$, $(\mathbb{R}^+, \times)$, $(\mathbb{Q} \setminus \{0\}, \times)$, $(\mathbb{R} \setminus \{0\}, \times)$, $(\mathbb{C} \setminus \{0\}, \times)$ with $e = 1$ and $a^{-1} = \frac{1}{a} \ \forall a$
  pf: similar to above
  note: $\{\mathbb{Z} \setminus \{0\}, \times\}$ is associative, but no inverse for eg 2
- vector space V with addition is an abelian group
  pf: see axioms for vector spaces
- $\mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{Z}^+$ is an abelian group with modular addition, identity $\overline{0}$, inverse of $\overline{a}$ is $\overline{-a}$
  pf: see ch 3 for pf of well defined and associative
- $(\mathbb{Z}/n\mathbb{Z})^\times$ for $n \in \mathbb{Z}^+$ with modular multiplication, identity $\overline{1}$, inverse by definition, is an abelian group
- let groups $(A, \diamond)$, $(B, \star)$
  the direct product group is set $A \times B$ and operation $(a1, b1)(a2, b2) = (a_1 \diamond a_2, b_1 \star b_2)$
  pf: later
  eg $A = B = \mathbb{R}$ euclidean plane

Proposition. *(1)*
let group $(G, \star)$
1) identity is unique
2) each inverse is uniquely determined
3) $(a^{-1})^{-1} = a \ \forall a \in G$
4) $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$
5) (generalized associative law) $a_1 \star a_2 \star ... \star a_n$ *is indep of how bracketed*

Proof.
1) assume identities f, g
   then $f \star g = f$ and $f \star g = g$
   thus $f = g$
2) assume b, c are both inverses of a and e identity
   then $c = c \star e = c \star (a \star b) = (c \star a) \star b = e \star b = b$
3) by def of inverse
4) $(a \star b) \star (a \star b)^{-1} = e$
   left multiply both sides by a^{-1} then b^{-1}
   $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$
5) exercise. first show for $1, 2, 3$
   next assume true for $k < n$, $b_1 \star (b_2 \star (b_3 \star (... \star b_k))...)$
   any bracketing breaks product into two $(a_1 \star a_2 \star ... \star a_k) \star (a_{k+1} \star a_{k+2} \star ... \star a_n)$.
   apply induction hypothesis to both parts
   rearrange to finally get $a_1 \star (a_2 \star (a_3 \star (... \star a_k))...)$

Remark.
ntn: associative can omit parentheses
ntn: multiplicative identity 1, $x^n := xx \cdots x$, $x^{-n} := x^{-1} x^{-1} \cdots x^{-1}$
ntn: additive 0, na, and $-na$

Proposition. *(2)*
Let group G, $a, b \in G$
equations $ax = b$ *and* $ya = b$ *have unique solns for* $x, y \in G$
in particular, left and right cancellation laws hold
ie $au = av \Rightarrow u = v$ *and* $ub = vb \Rightarrow u = v$

Proof. multiply both sides by inverse

Claim. cor:
$ab = e$ or $ba = e \Rightarrow b = a^{-1}$
$ab = a$ or $ba = a \Rightarrow b = 1$

Definition.
- the order of $x \in G$ is $|x|$ =the smallest positive integer n st $x^n = 1$
  ntn: same as ntn for cardinality

- infinite order means order is infinity

Example.
- order 1 iff identity
- for additive groups $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, every nonidentity element has infinite order
- for multiplicative groups $\mathbb{R}\backslash\{0\}, \mathbb{Q}\backslash\{0\}$, $|-1| = 2$ and every other nonidentity element has infinite order
- for additive group $\mathbb{Z}/9\mathbb{Z}$
  $|\overline{6}| = 3$ since lcm of 6, 9 is $18 = 6 \times 3$
  $|\overline{5}| = 9$ since lcm of 5, 9 is $45 = 9 \times 5$
- multiplicative group $(\mathbb{Z}/7\mathbb{Z})^\times$
  $|\overline{2}| = 3$ since $\overline{2} \times \overline{2} = \overline{4}$ then $\times\overline{2} = \overline{8} = \overline{1}$
  $|\overline{3}| = 6$ since 3^6 is smallest power of 3 that is congruent to 1 mod 7

Definition. the multiplication table ("group table") of group $G = \{g_1, g_2, ..., g_n\}$ is $n \times n$ mx with i, jth entry $g_i g_j$

Remark. we will not focus on group tables, will have other ways to visualize structure of a group

1.2. DIHEDRAL GROUPS [& INTRO TO PRESENTATIONS].

Remark. will revisit 2d case in many examples

Definition.
- lines of symmetry of regular n-gon are
  case n even: $n/2$ pass through opposite vertices, $n/2$ perpendicularly bisect opposite sides
  case n odd: n lines through vertex and midpoint of opposite edge
- some rigid motions of regular n-gon are rotation about point (2d) and reflection about line (3d)
  ntn: r is rotation clockwise about origin, s is reflection about line from vertex 1 through origin
- symmetries of regular n-gon are rigid motions to cover its original position (rotations by $2\pi/n$ about center, reflections about lines of symmetry)
  convention: center is origin
- D_{2n}, integer $n \geq 3$, is the set of symmetries of a regular n-gon

Claim.
- symmetry t characterized by corresponding permutation σ of enumerated vertices
  convention: vertices labeled 1 to n in clockwise manner
- D_{2n} with composition of symmetries is a group called dihedral group
  pf: if $s, r \in D_{2n}$, sr is first applying r, then s (characterized by function composition of corresponding permuataitons $\sigma \circ \tau$); associative since function composition is associative; identity 1 leaves vertices fixed; inverse reverses rigid motion and corresponds to inverse permutation
- $|D_{2n}| = 2n$
  (this is why it is called "dihedral")
  pf1: for every vertex i, there is a symmetry sending 1 to i, and vertex 2 to either $i+1$ or $i-1$ (where $n+1$ is 1 and $1-1$ is n ie mod n), and all other vertices follow since rigid
  pf2: n rotations about origin and n reflections about lines of symmetry

Claim. claims about s and r
- $|r| = n$
  pf: $1, r, r^2, ..., r^{n-1}$ are distinct and $r^n = 1$
- $|s| = 2$
- $s \neq r^i$ for all i
  pf: show what each side does to vertices 1,2
- $sr^i \neq sr^j$ for $0 \leq i, j \leq n-1$ with $i \neq j$
- cor: $D_{2n} = \{1, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\}$
  ie each element can be written uniquiely $s^k r^i$ for $k = 1, 2$ and $i = 0, 1, ..., n-1$
- $rs = sr^{-1}$
  pf: show what each side does to vertices 1,2
- cor: not commutative
- $r^i s = sr^{-i}$ for all $0 \leq i \leq n$
  ie can commute s with powers of r
  pf: induction on i, note $r^{i+1}s = r(r^i s)$

Example. for $n = 12$, reduce $(sr^9)(sr^6)$ (using above and reducing exponents mod n)
$(sr^9)(sr^6) = s(r^9 s)r^6 = s(sr^{-9})r^6 = s^2 r^{-9+6} = r^{-3} = r^9$

GENERATORS AND RELATIONS

Remark.
- want way to succinctly describe a group
- this section is informal, will rigorously discuss generators in §2.4, and generators and relations in §6.3 with "free groups"

Definition. a set of generators $S \subset G$ means every element of group G can be written as a finite product of elements of S and their inverses
note: S implicitly includes inverses of elements
ntn: $G = \langle S \rangle$; "S generates G"
ntn: list the generators $\langle a, b, c \rangle$

Example.
- $D_{2n} = \langle r, s \rangle$
  pf: see earlier claims
- $(\mathbb{Z}, +) = \langle 1 \rangle$
  pf: see def of generator

Definition.
- relation is any equation that generators satisfy
- a presentation of G is a collection of relations $R_1, R_2, ..., R_m$, using elements of generator S and identity, st any relation among elements of S can be deduced from these
  ie can determine exactly when two group elements are equal using these relations
  ntn: $G = \langle S | R_1, R_2, ..., R_m \rangle$
- commutation relation $xy = yx^p$ determines how to move y from right to left

Example.
- $D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$ is one presentation of D_{2n}
- clm: $|D_{2n}| = 2n$
  pf2: ($|D_{2n}| \geq 2n$): showed earlier geometricly
  ($|D_{2n}| \leq 2n$): use similar method as neighboring example for X_{2n}
- warning: may be difficult (or impossible[?]) to determine when two elements (expressed in terms of generators) are equal
- warning: presentations may implicitly give relations that are consequences of the explicitly given ones, and thus difficult to determine upper bound or lower bound (since "collapsing") for size of group
  - group $\langle x_1, y_1 | x_1^2 = y_1^2 = (x_1 y_1)^2 = 1 \rangle$ has order 4
  - group $\langle x_2, y_2 | x_2^3 = y_2^3 = (x_2 y_2)^3 = 1 \rangle$ has infinite order
  - group $X_{2n} = \langle x, y | x^n = y^2 = 1, xy = yx^2 \rangle$ has order at most 6
    pf: (note: looks like D_{2n}, every element can be written $y^k x^i$ by using commutation relation)
    $x = xy^2 = (xy)y = (yx^2)y = (yx)(xy) = (yx)(yx^2) = y(xy)x^2 = y(yx^2)x^2 = y^2 x^4 = x^4$ so $x = x^4$ so $x^3 = 1$, so X_{2n} has order at most 6 $\forall n$
  - group $Y = \langle u, v | u^4 = v^3 = 1, uv = v^2 u^2 \rangle$ has order 1 ie trivial group
    pf: can show $u = 1 = v$

1.3. SYMMETRIC GROUPS [& THEIR CYCLE DECOMPOSITIONS].

Definition.
- a permutation of set Ω is bijection $\Omega \to \Omega$
- $S_\Omega = \{$all permutations of set $\Omega\}$
  for finite ($\Omega = \{1, 2, ..., n\}$), $S_n := S_\Omega$ called "symmetric group of degree n"

Claim.
- S_Ω is a group (symmetric group) with composition of permutations, and identity map 1
  pf: composition of bijections is bijection; composition is associative; $\exists!$ inverse since bijection
- $|S_n| = n!$
  pf: n ways to pick $\sigma(1)$, $n-1$ ways to pick $\sigma(2)$,...

Remark. will see in section 6 that all symmetric groups of degree n have identical structure

CYCLE DECOMPOSITIONS

Definition.
- a cycle is string of integers $(a_1 a_2 ... a_m)$ representing permutation which sends a_i to a_{i+1} except sends a_m to a_1.
  represents permutations which fixes all other integers
- the length of a cycle is the number of integers appearing in it
  ntn: t-cycle has length t
- disjoint cycles if have no members in common

Example. (2 1 3) sends 2 to 1, 1 to 3, 3 to 2

Claim.
- each permutation $\sigma \in S_n$ can be decomposed uniquely into k disjoint cycles whose product is σ:
  $(a_1 a_2 ... a_{m_1})(a_{m_1+1} a_{m_1+2} ... a_{m_2}) ... (a_{m_{k-1}+1} a_{m_{k-1}}$
  pf: uniqueness etc in ch4
- given cycle decomposition of σ, its inverse σ^{-1} is each individial cycle written in reverse
- products of permutations using cycle decomposition is just following permutations right-to-left
- S_n ($n \geq 3$) nonabelian, but disjoint cycles commute
  so can rearrange order of cycles in our decomposition ntn
- given cycle $(a_1\ a_2\ ...a_m)$, can shift starting position $(a_i\ a_{i+1} ... a_m\ a_1 ... a_{i-1})$
- the order of a permutation is the lcm of the lengths of the cycles in its cycle decomposition
  pf: exercise

Remark.
- ntn: leftmost chain starts with smallest number not visited yet, eg first chain starts with 1
- ntn: omit chains of length 1, it is understood that $i \mapsto i$
- identity is (1)(2)...(n) and written 1
- this ntn is convenient because a cycle (2 3 1) makes sense wrt any S_n where $n \geq 3$

Example.
- see book for long example from S_{13}
- $S_3 = \{1, (2\ 3), (1\ 3), (1\ 2), (1\ 2\ 3), (1\ 3\ 2)\} = \{((1)(2)(3), (1)(2\ 3), (1\ 3)(2), (1\ 2)(3), (1\ 2\ 3), (1\ 3\ 2)$
- eg (1 2)(3 4) has inverse (2 1)(4 3)
- (1 2 3)∘(1 2)(3 4) maps 1 to 2 to 3; 2 to 1 to 2, 3 to 4 to 4, 4 to 3 to 1
  so equals (3 4 1)=(1 3 4)
- can compare equality of two permutations by putting both into ntn above

1.4. MATRIX GROUPS [& INTRO TO FIELDS].

Remark.
- matrix groups will be used as an example in part I, and will be studied rigorously in the chapters on vector spaces
- will use coefs from fields $\mathbb{Q}, \mathbb{R}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for p prime, but results hold for arbitrary fields

Definition.

- a field is set F and binary operations $+, \cdot$ st $(F,+)$ is abelian group with identity 0 and $(F \setminus \{0\}, \cdot)$ is also an abelian group, and distributive laws $a \cdot (b+c) = (a \cdot b) + (a \cdot c)\ \forall a,b,c \in F$
- for $n \in \mathbb{Z}^+$, define $GL_n(F) = \{A | A \text{ is } n \times n \text{ matrix whose entries come from } F \text{ and with } \det \neq 0\}$ (where formula for det is same as for $F = \mathbb{R}$)
- given field F, let $F^\times = F \setminus \{0\}$

Claim. $GL_n(F)$ is a group under mx multiplication with identity mx I
ntn general linear group of degree n
- product of $n \times n$ mxs (product uses same formula as $F = \mathbb{R}$) is associative
- $\det(AB) = \det(A)\det(B)$
- $GL_n(F)$ is closed under mx multiplication
  pf: $\det A \neq 0$ and $\det B \neq 0 \Rightarrow \det AB \neq 0$
- $\det A \neq 0$ iff A has mx inverse (computed using same adjoint method as $F = \mathbb{R}$)
  so each $A \in GL_n(F)$ has inverse st $AA^{-1} = A^{-1}A = I$ where I identity mx

Claim.
- field F st $|F| < \infty \Rightarrow |F| = p^m$ for p prime, m integer
  pf: part III
- $|F| = q < \infty \Rightarrow |GL_n(F)| = (q^n-1)(q^n-q)(q^n-q^2)...(q^n-q^{n-1})$
  pf: part III

1.5. THE QUATERNION GROUP.

Definition. the quaternion group $Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$ with product $\cdot$ st
$1 \cdot a = a \cdot 1 = a\ \forall a \in Q_8$
$(-1)\cdot(-1) = 1,\ (-1)\cdot a = a \cdot (-1) = -a\ \forall a \in Q_8$
$i \cdot i = j \cdot j = k \cdot k = -1$
$i \cdot j = k \quad j \cdot i = -k$
$j \cdot k = i \quad k \cdot j = -i$
$k \cdot i = j \quad i \cdot k = -j$

Claim.
- it is actually a group
  pf: tedious to check associative law, will prove later by less computational means
  other axioms are easily checked
- Q_8 nonabelian
- $|Q_8| = 8$

1.6. HOMOMORPHISMS AND ISOMORPHISMS [& INTRO TO CLASSIFICATION & PRESENTATIONS].

Remark. this section: what it means for groups to have same structure
will later generalize these ideas to rings, fields, vector spaces, etc

Definition.
- a homomorphism between groups $(G,\star),(H,\diamond)$ is map $\phi : G \to H$ st $\phi(x \star y) = \phi(x) \diamond \phi(y)\ \forall x,y \in G$
  ntn: $\phi(xy) = \phi(x)\phi(y)$
- an isomorphism is a homomorphism and bijection
  ntn: $G \cong H$; G, H isomorphic
  intuition: preserves group "structure"

Claim. relation $\cong$ is an equivalence relation (so partitions a collection of groups into isomorphism classes)

Example.
- identity map is a trivial isomorphism from group to itself
- exponential map $\exp : \mathbb{R} \to \mathbb{R}^+$, $\exp(x) = e^x$, is an isomorphism from $(\mathbb{R},+)$ to $(\mathbb{R}^+,\times)$
  pf: bijection since inverse log
  homomorphism since $e^{x+y} = e^x e^y$

CLASSIFICATION THMS

Remark. it may be difficult to find the actual bijection
classification thms allow checking whether isomorphic without finding the bijective map

Claim. (classification thms)
- any non-abelian group of order 6 is isomorphic to S_3
  ie can classify based on properties: size 6, commutativity
  cor: $D_6 \cong S_3$ and $GL_2(\mathbb{F}_2) \cong S_3$ without having to find isomorphism
- there are two isomorphism classes for groups of order 6: S_3 and $\mathbb{Z}/6\mathbb{Z}$
- (structure of S_Ω depends only on $|\Omega|$)
  let sets Δ, Ω nonempty.
  $S_\Delta \cong S_\Omega$ iff $|\Delta| = |\Omega|$
  pf: ($\Leftarrow$) $\exists \theta : \Delta \to \Omega$ bijection since same size.
  define homomorphsim $\phi : S_\Delta \to S_\Omega$: for $\sigma \in S_\Delta$, for $x,y \in \Delta$, $\sigma(x) = y \Rightarrow \phi(\sigma)(\theta(x)) = \theta(y)$
  ϕ is invertable using inverse of θ
  see exercise for more arguments
  ($\Rightarrow$) (will only prove finite case, see ch4 exercise for infinite case)
  isomorphic so $|S_\Delta| = |S_\Omega|$
  and $|S_\Delta| = n! = |S_\Omega|$
  so $|\Delta| = n = |\Omega|$

Claim. (trick to show groups non-isomorphic, use contrapositive of the following thm)
- $\phi : G \to H$ isomorphism $\Rightarrow$
  (a) $|G| = |H|$
  (b) G is abelian iff H abelian
  (c) $\forall x \in G$, $|x| = |\phi(x)|$
- S_3 and $\mathbb{Z}/6\mathbb{Z}$ not isomorphic since one is abelian and other is not
- $(\mathbb{R}\setminus\{0\},\times)$ and $(\mathbb{R},+)$ not isomorphic since first group has element $|-1| = 2$ and second has no element of order 2

HOMO/ISOMORPHISMS BASED ON GENERATORS/RELATIONS

Remark. there is a way to construct homomorphisms based on generators/relations, and sometimes they are also isomorphisms

Claim. Let G finite group of order n with presentation with generators $\{s_1, s_2, ..., s_m\}$
Let H finite group with some elements $\{r_1, r_2, ..., r_m\}$
- If every relation of G also satisfied in H with r_i instead of s_i
  then $\exists!$ homomoprhism $\phi : G \to H$ which satisifies $\phi(s_i) = r_i$
- if, in addition, H is generated by $\{r_1, r_2, ..., r_m\}$, then ϕ is surjective
- if, in addition, H is the same (finite) order as G, then ϕ is injective (thus bijective thus isomorphism)

Proof. later when we discuss "free" groups

Example.
- corresponding statement for vector spaces:
  if V n dimesnional vector space with basis S
  if W another vector space
  define linear transformation $T : V \to W$ by mapping elements in S to W
  (note: no relations to satisfy)
  if W also dimension n and the vectors mapped from S span W
  then this linear transformation is invertable
- $D_{2n} = \langle r, s | r^n = s^2 = 1, sr = r^{-1}s \rangle$
  let group H containing elements a, b st $a^n = b^2 = 1$ and $ba = a^{-1}b$
  note: a, b need not have order $n, 2$
  then $\exists!$ homomorphsim $D_{2n} \to H$ with $r \mapsto a$ and $s \mapsto b$
- consider D_{2n} and D_{2k} with $k \geq 3$ dividing n ie $n = km$
  define $\phi : D_{2n} \to D_{2k}$ st r, s mapped to corresponding elements r_1, s_1 of D_{2k}
  relations satisfied since $r_1^n = (r_1^k)^m = 1^m = 1$
  thus homomorphism
  surjective since $\{r_1, s_1\}$ generates D_{2k}
  but not isomorphism since $k < n$
- consider D_6 and S_3
  S_3 elements $a = (1\ 2\ 3)$, $b = (1\ 2)$ satisfy $a^3 = b^2 = 1$, $ba = ab^{-1}$
  thus $\exists!$ homomorphism $D_6 \to S_3$ st $r \mapsto a, s \mapsto b$.
  this homomorphism is surjective since a, b generate S_3
  this homomorphism is bijective since $|D_6| = |S_3| = 6$
  so isomorphism

1.7. GROUP ACTIONS [& THEIR PERMUTATION REPRESENTATION].

Remark. "group actions" are a useful tool for proving general thms and for studying structure of specific examples
later, will generalize the idea of using "actions" to study algebraic objects by seeing how they acts on other structures

Definition. a group action of group G on set A is map $\cdot : G \times A \to A$ (note: not technically a binary operation), st
(1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a\ \forall g_1, g_2 \in G\ a \in A$ where $g_1 g_2$ is multiplication in G
(2) $1 \cdot a = a\ \forall a \in A$
ntn: repace $g\cdot$ with $\sigma_g : A \to A$, $\sigma_g(a) = g \cdot a$
ntn: can omit the $\cdot$
ntn: could have called it "left group action", since can define similarly for right

Claim. (group action G on A, each $g\cdot$ permutes A in a manner consistent with structure of G)
- (group action permute A)
  each group action has a permutation representation $\phi : G \to S_A$, $\phi(g) = \sigma_g \in S_A$
  ie each $g \in G$ permutes A
- (characterize group action with homomorphisms)
  Let $\phi : G \to S_A$
  permutation representation iff homomorphism
  ie {all actions of G on A} bijective corresponds with {all homomorphisms $\phi : G \to S_A$}

Proof.
- suffices to show σ_g has 2-sided inverse (prop 0.1.1)

$(\sigma_{g^{-1}} \circ \sigma_g)(a) =$

$= \sigma_{g^{-1}}(\sigma_g(a))$	def of function composition
$= g^{-1} \cdot (g \cdot a)$	def of $\sigma_{g^{-1}}$ and σ_g
$= (g^{-1}g) \cdot a$	property 1 of action
$= 1 \cdot a = a$	property 2 of action

  similarly for $\sigma_g \circ \sigma_{g^{-1}}$
  so $\sigma_{g^{-1}}$ is two sided inverse of σ_g
- ("$\Rightarrow$") (the permutation representation is a homomorphism)
  to show ϕ homomorphism, need $\phi(g_1 g_2) = \phi(g_1) \circ \phi(g_2)$ (where S_A group under $\circ$)

$\phi(g_1 g_2)(a) =$

$= \sigma_{g_1 g_2}(a)$	def of ϕ
$= g_1 g_2 \cdot a$	def of $\sigma_{g_1 g_2}$
$= g_1 \cdot (g_2 \cdot a)$	property (1) of action
$= \sigma_{g_1}(\sigma_{g_2}(a))$	def of $\sigma_{g_1}, \sigma_{g_2}$
$= (\phi(g_1) \circ \phi(g_2))(a)$	def of ϕ

  (converse) let $\phi : G \to S_A$ is any homomorphism
  define map $G \times A \to A$, $g \cdot a = \phi(g)(a)\ \forall g \in G$, $a \in A$

this is a group action of G on A since $g_1 \cdot (g_2 \cdot a) = \phi(g_1)(\phi(g_2)(a)) = (\phi(g_1) \circ \phi(g_2))(a) = \phi(g_1 g_2)(a) = ((g_1 g_2) \cdot a)$

Definition. let group G and nonempty set A.
- trivial action is $ga = a \ \forall g \in G, \forall a \in A$.
  ntn: G "acts trivially" on A
  intuition: all elements induce the identity permutation on A ie the permutation representation $G \to S_A$ is the trivial homomorphism $g \mapsto$identity
- faithful action means distinct elements of G induce distinct permutations of A.
  ie permutation representation is injective
- the kernel of action G on A is $\{g \in G | g \cdot a = a \ \forall a \in A\}$
  ie the elements of G which identity permute elements of A
- the left regular action is G acting on itself (ie $A = G$) st $G \times A \to A$, $g \cdot a = ga \ \forall g \in G, a \in A$
  where ga is group multiplication.
  intuition: g permutes the elements of G by left multiplication $g : a \mapsto ga$
- [conjugation action of G on subset $A \subseteq G$ is $g \cdot a = gag^{-1}$
  conjugation action of G on power set $P(G)$ is $g \cdot B := gBg^{-1} := \{gbg^{-1} | b \in B\}$ where $B \in P(G)$ (see §1.7 exercise 16))]

Claim.
- trivial action has kernel G and is not faithful when $|G| > 1$
- faithful action has kernel $\{1\}$
- left regular action is faithful

Example.
let group G and nonempty set A. Proving the following are group actions is an exercise.
- the axioms of vector space V over field F include two axioms that the multiplicative group $F^\times$ acts on V
  special case $V = R^n$, $F = \mathbb{R}$: action is $\alpha(r_1, r_2, ..., r_n) = (\alpha r_1, \alpha r_2, ..., \alpha r_n) \ \forall \alpha \in \mathbb{R}, (r_1, r_2, ..., r_n) \in \mathbb{R}^n$, and αr_i is just real multiplication
- the action of symmetry group S_A on A by $\sigma \cdot a = \sigma(a) \ \forall \sigma \in S_A, a \in A$
  the permutation representation is the identity map from S_A to itself
- recall element of D_{2n} permutes vertices
  group action of D_{2n} on $\{1, 2, ..., n\}$ defined $D_{2n} \times \{1, 2, ..., n\} \to \{1, 2, ..., n\}$, $(\alpha, i) \mapsto \sigma_\alpha(i)$
  ntn: αi instead of $\sigma_\alpha(i)$
  this action is faithful
  for $n = 3$, injective homomorphism from D_6 to S_3
  this map is surjective since these groups have same order
  so it is an isomorphism
  geomertic intuition: permutations of the vertices of a triangle is a symmetry
  this is not true for $n \geq 4$ since group sizes are different

2. SUBGROUPS

2.1. DEFINITION AND EXAMPLES.

Remark.
- this chapter: study structure of a group by studying subset satisfying same axioms
- next chapter: study structure of a group by studying quotients, which, roughly speaking, collapses object to smaller object
- these themes will recur when we study subrings and quotient rings, subspaces and quotient spaces of a vector space, etc

Definition. subgroup of group G is nonempty $H \subset G$ closed under products and inverses (ie $x, y \in H \Rightarrow x^{-1}, xy \in H$)
ntn: $H \leq G$ and proper containment $H < G$
ntn: use same binary operation symbol, without restriction $|_H$

Claim.
- [subgroup is a group
  pf: associative since G, identity since has inverses and $x^{-1}x = 1$, and inverse by def]
- any group has at least two subgroups, itself and the trivial subgroup $\{1\}$ (written "1")
- subgroup relation is transitive

Example.
- additive groups $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$
- D_{2n} has subgroup the set of its rotations $\{1, r, r^2, ..., r^{n-1}\}$
- addition of integers has subgroup addition of even integers
- D_6 is not a subgroup of D_8 since not even a subset

Proposition. *(1)(characterize subgroups, easier to check)*
$H \leq G$ iff
1) $H \neq \emptyset$, and
2) $\forall x, y \in H$, $xy^{-1} \in H$
furthermore, if H finite, then suffices to check H nonempty and closed under multiplication

Proof. ($\Rightarrow$) obvious
($\Leftarrow$) assume (1),(2) and let $x \in H$
H contains identity since $xx^{-1} \in H$
H contains inverses since $1 \in H$ so $1y^{-1} \in H$
if $x, y \in H$ then $xy \in H$ since $x(y^{-1})^{-1} \in H$
(finite part) assume finite H closed under multiplication
for each $x \in H$, contains $x^2, x^3, ...$, so $x^n = 1$, so $x^{-1} = x^{n-1}$
so H closed under inverses

2.2. CENTRALIZERS AND NORMALIZERS (OF SUBSET), STABILIZERS AND KERNELS (OF ACTION).

Remark.
- now, introduce some important families of subgroups
- Let A be a nonempty subset of group G

Definition.
- the centralizer of A in G is $C_G(A) = \{g \in G | gag^{-1} = a \ \forall a \in A\}$
  intuition: $ga = ag$ so all elements which commute with every $a \in A$
  [ie kernel of conjugation action of G on $A \subseteq G$]
  ntn: for singleton $\{a\}$, write $C_G(a)$
- center of G is $Z(G) = C_G(G)$
- normalizer of A in G is $N_G(A) = \{g \in G | gAg^{-1} = A\}$
  [ie all $g \in G$ that commute with A "as a whole", "$gA = Ag$"]
  [ie all $g \in G$ that allow some commuting, [??] $\forall b \in A \exists a \in A$ st $ga = bg$]

Claim. $(Z(G) \leq C_G(A) \leq N_G(A) \leq G)$
- $C_G(A)$ is a subgroup of G
  pf: nonempty since $1 \in C_G(A)$
  let $x, y \in C_G(A)$ ie $\forall a \in A$, $xax^{-1} = a$ and $yay^{-1} = a$
  so $a = y^{-1}ay$
  so contains y^{-1}
  contains xy since $(xy)a(xy)^{-1} = x(yay^{-1})x^{-1} = xax^{-1} = a$
- $N_G(A)$ is a subgroup of G
  pf: follows same steps as $C_G(A) \leq G$
- center is contained in all centralizers
- $C_G(A) \leq N_G(A)$
  if $g \in C_G(A)$ then $gag^{-1} = a \ \forall a \in A$
- if G abelian, then $Z(G) = C_G(A) = N_G(A) = G \ \forall A \subset G$, since $gag^{-1} = gg^{-1}a = a \ \forall g \in G, a \in A$

Example.
- consider subgroup $A = \{1, r, r^2, r^3\}$ of D_8
  - $C_{D_8}(A) = A$
    pf: will show exhaustively
    $C_{D_8}(A)$ includes A since all powers of r commute with each other
    $C_{D_8}(A)$ does not include s since does not commute with r since $sr = r^{-1}s \neq rs$
    $C_{D_8}(A)$ does not include sr^1, sr^2, sr^3, (otherwise subgroup would also have $(sr^i)r^{-i}$ which equals s)
  - $Z(D_8) = \{1, r^2\}$
    pf: will show both inclusions
    ($\leq$): $Z(D_8) \leq C_{D_8}(A) = A$ and $r, r^3 \notin Z(D_8)$
    (reverse): r and s both commute with r^2, thus all of D_8 commutes with r^2 since r, s generate D_8
  - $N_{D_8}(A) = D_8$
    pf: will show both containments
    ($\leq$): by big claim
    ($\geq$): $N_{D_8}(A)$ contains A since eqauls $C_{D_8}(A)$
    $N_{D_8}(A)$ contains s since $sAs^{-1} = \{s1s^{-1}, srs^{-1}, sr^2s^{-1}, sr^3s^{-1}\} = \{1, r^3, r^2, r\} = A$
    so $s, r \in N_{D_8}(A)$ thus any $s^i r^j \in N_{D_8}(A)$
- consider subgroup $A = \{1, (1\ 2)\}$ of S_3
  - $C_{S_3}(A) = A$
    pf: $C_{S_3}(A) = A$ since similar method as above
    [?] pf2: alternatively, $A \leq C_{S_3}(A) = A$ since an element commutes with its powers
    and the reverse inclusion by Lagrange's thm (§1.7 exercise 19) $\left|C_{S_3}(A)\right|$ divides $|S_3| = 6$ and $|A| = 2$ divides $\left|C_{S_3}(A)\right|$, so 2 possibilities: $\left|C_{S_3}(A)\right| = 2$ or 6, but the latter implies $C_{S_3}(A) = S_3$ (ie $A \leq Z(S_3)$) which implies (1 2) commutes with (1 2 3) which is a contradiction
    thus $\left|C_{S_3}(A)\right| = 2$ and $A = C_{S_3}(A)$
  - $Z(S_3) =$ identity
    pf: $Z(S_3) \leq C_{S_3}(A) = A$ and $(1\ 2) \notin Z(S_3)$
  - $N_{S_3}(A) = A$
    pf: by def, $\sigma \in N_{S_3}(A)$ iff $\{\sigma 1\sigma^{-1}, \sigma(1\ 2)\sigma^{-1}\} = \{1, (1\ 2)\}$
    $\sigma 1\sigma^{-1} = 1$
    the second equality iff $\sigma \in C_{S_3}(S)$

STABILIZERS AND KERNELS OF GROUP ACTIONS

Remark. the fact that $Z(G), C_G(A), N_G(A) \leq G$ can be deduced as special cases of results on group actions
ie the structure of group is reflected on sets on which it acts
will formalize this

Definition. Let G act on set S.
- The stabilizer of $s \in S$ in G is $G_s = \{g \in G | g \cdot s = s\}$ (see §1.7 exercise 14 [?])
- recall kernel of action is $\{g \in G | g \cdot s = s \ \forall s \in S\}$

Claim.
- [? the kernel is the intersection of all stabilizers ie stabilizes every $s \in S$]
- (stabilizers and kernel are subgroups of G)
  - $G_s \leq G$
    pf: $1 \in G$ by axiom (2) of action
    also if $y \in G_s$ then so is y^{-1} since $s = 1 \cdot s = (y^{-1}y) \cdot s = y^{-1} \cdot (y \cdot s) = y^{-1} \cdot s$
    also if $x, y \in G_s$ then so is xy since $(xy) \cdot s = x \cdot (y \cdot s) = x \cdot s = s$
    note: same as pf above for $C_G(A) \leq G$ with axiom (1) of action replacing the associative law

– more generally, the kernel of an action is a subgroup
pf: similar argument, see §1.7 exercise 1 [?]

Example.
- group D_8 acts on set $A = \{4 \text{ vertices of a square}\}$ (see ex 4 of §1.7).
the stabilizer of any vertex a is the subgroup $\{1, t\} \subset D_8$ where t is reflection about the line of symmetry passing through vertex a and the center of the square
the kernel (of action on all vertices) is the identity subgroup, which fixes each vertex
- D_8 acts on $A = \{\text{the 2 diagonal symmetries}\}$ (see from §1.2 figure 2, $A = \{(1,3),(2,4)\}$)
the kernel is $\{1, s, r^2, sr^2\}$
the stabilizer for either element of A equals the kernel

Claim. the fact that centralizers, normalizers, and centers are subgroups is a special case of thms about stabilizers and kernels of actions are subgroups (see ch 4 for more)

Proof.
$(N_G(A))$: Let G act on power set $P(G)$ by conjugation
under this action on $A \in P(G)$, $N_G(A) = G_A$
so it is a subgroup
$(C_G(A))$: let group $N_G(A)$ act on some A by conjugation ($\forall g \in N_G(A)$ and $a \in A$, $g : a \mapsto gag^{-1}$; this is an action on A since maps A to A by def of $N_G(A)$)
$C_G(A)$ is the kernel of this action
thus $C_G(A) \leq N_G(A)$
thus $C_G(A) \leq G$ by transitivity of $\leq$
$(Z(G))$: $Z(G)$ is the kernel of G acting on G by conjugation, so $Z(G) \leq G$

2.3. CYCLIC GROUPS AND CYCLIC SUBGROUPS.

Remark. this section: subgroups generated by one element under all integer powers

Definition. a cyclic group H means $\exists x \in H$ st $H = \{x^n | n \in \mathbb{Z}\}$
ntn: H "generated" by "generator" x
ntn: for additive, $\{nx | n \in \mathbb{Z}\}$
ntn: $H = \langle x \rangle$

Claim.
- $\langle x \rangle$ closed under inverses and products
- generated by x means also generated by x^{-1}
- powers of x need not be distinct
- cyclic groups are abelian
pf: laws of exponents, see §1.1 exercise 19

Example. (motivating examples before props)
- consider $D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$
D_{2n} is not cyclic since not abelian
$\langle r \rangle$ is the cyclic subgroup of all rotations
$|\langle r \rangle| = n$ and r has order n
multiples of the generator are not distinct...
any power can be written (using division algorithm) to power $0 \leq k < n$ since $r^t = r^{nq+k} = (r^n)^q r^k = 1^q r^k = r^k$
eg D_8, $r^{105} = r^{4(26)+1} = r$ since $r^4 = 1$
eg D_8, $r^{-42} = r^{4(-11)+2} = r^2$
- $(\mathbb{Z}, +)$ is $\langle 1 \rangle$ where 1 is integer and 0 is identity
multiples of the generator are all distinct
$|(\mathbb{Z}, +)|$ and order of 1 are both infinite
also generated by -1

Proposition. *(2) ($H = \langle x \rangle \Rightarrow |H| = |x|$)*
1) if $|H| = n < \infty$ then $x^n = 1$ and $1, x, x^2, ..., x^{n-1}$ are all distinct elements of H
2) if $|H| = \infty$ then $x^n \neq 1$ $\forall n \neq 0$ and $x^a \neq x^b$ $\forall a \neq b \in \mathbb{Z}$

Proof. case $|x| = n < \infty$:
$1, x, x^2, ..., x^{n-1}$ are distinct since otherwise, $x^a = x^b$, $0 \leq a < b < n$, then $x^{b-a} = x^0 = 1$, contrary to n being smallest positive power st $x^n = 1$
thus $|H| \geq n$, and want to show equality
for any power $t \notin [0, n)$, can rewrite $r^t = r^{nq+k} = (r^n)^q r^k = 1^q r^k = r^k$ since $r^n = 1$ where $k \in [0, n)$
case $|x| = \infty$:
so no positive power of x is the identity
all distinct, since otherwise, $x^a = x^b \Rightarrow x^{a-b} = 1$
so $|H| = \infty$

Proposition. *(3)*
- *let group G, $x \in G$, $m, n \in \mathbb{Z}$*
if $x^n = 1$ and $x^m = 1$, then $x^d = 1$ where $d = (m, n)$
- *in particular if $|x| = n$ and $x^m = 1$, then $n \mid m$*

Proof.
- by euclidean algorithm, $\exists r, s \in \mathbb{Z}$ st $d = mr + ns$
thus $x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1^r 1^s = 1$
- case $m = 0$: $n \mid m$ trivially
case $m \neq 0$: $n < \infty$ since some nonzero power is identity
$x^d = 1$, where $d = (m, n)$, by previous result
so $d = n$ since $0 < d \leq n$ and n is the smallest positive power which gives identity
so $n \mid m$

Theorem. *(4) (cyclic groups of the same order are isomorphic)*
1) $\langle x \rangle$, $\langle y \rangle$ both order $n \in Z^+$
then map $\phi : \langle x \rangle \to \langle y \rangle$, $x^k \mapsto y^k$ is well-defined and an isomorphism
2) if $\langle x \rangle$ is infinite cyclic group, then map $\phi : \mathbb{Z} \to \langle x \rangle$, $k \mapsto x^k$ is well-defined and an isomorphism

Proof.
1) (well defined) let $x^r = x^s$, then $x^{r-s} = 1$, then $n \mid r - s$, then $r = tn + s$
then $\phi(x^r) = \phi(x^{tn+s}) = y^{tn+s} = (y^n)^t y^s = y^s = \phi(x^s)$
(homomorphism) $\phi(x^a x^b) = y^{a+b} = \phi(x^a)\phi(x^b)$ since laws of exponents
(isomorphism) surjective since $\phi(x^k) = y^k$ and finite so bijection
2) consider $\phi : \mathbb{Z} \to \langle x \rangle$, $\phi(k) = x^k$
(well defined) no ambiguity
(homomorphism) by law of exponents as above
(isomorphism) injective since $b \neq a \Rightarrow x^b \neq x^a$
surjective by def of cyclic group
so bijection

Remark. since cyclic group unique up to isomorphism:
ntn: for finite $n = |\langle x \rangle|$, write Z_n; will occasionally use $\mathbb{Z}/n\mathbb{Z}$ as representative of the isomorphism
ntn: for infinite, will always use $(\mathbb{Z}, +)$ as representative

Proposition. *(5) (which powers of x generate $\langle x \rangle$)*
Let group G, $x \in G$, $a \in \mathbb{Z} \setminus \{0\}$
1) $|x| = \infty \Rightarrow |x^a| = \infty$
2) $|x| = n < \infty \Rightarrow |x^a| = \frac{n}{(n,a)}$
3) special case: $|x| = n < \infty$ and positive $a \mid n \Rightarrow |x^a| = \frac{n}{a}$

Proof.
1) towards contradiction, assume $|x^a| = m$
then $(x^a)^m = x^{am} = 1$ and $x^{-am} = 1$
so $|x| = am$ (or $-am$), which contradicts $|x| = \infty$
2) ntn: $y = x^a$, $d = (n, a)$
let $n = db$, $a = dc$ for suitable $b, c \in \mathbb{Z}$, $b > 0$
sufficient to show $|y| = b$
ntn: $k = |y|$, so want $k = b$
$k \mid b$ since $y^b = x^{ab} = x^{dcb} = x^{nc} = 1^c = 1$ and prop 3.2
$n \mid ak$ since $x^{ak} = y^k = 1$ and prop 3.2
rewrite previous line: $db \mid dck$, thus $b \mid ck$
thus $b \mid k$ since $(b, c) = 1$ since $d = (n, a)$
thus $b = k$ since $b \mid k$ and $k \mid b$
3) special case recorded for later

Proposition. *(6)*
Let $H = \langle x \rangle$
1) case $|x| = \infty$: $H = \langle x^a \rangle$ iff $a = \pm 1$
2) case $|x| = n < \infty$: $H = \langle x^a \rangle$ iff $(a, n) = 1$
in particular, the number of generators of H is $\phi(n)$ where Euler's ϕ function

Proof.
1) exercise
2) by prop 2, x^a generates a subgroup of H of order $|x^a|$
by prop 5, $|x^a| = |x|$ iff $\frac{n}{(a,n)} = n$ (ie iff $(a, n) = 1$)
$\phi(n)$ is the number of $a \in \{1, 2, ..., n\}$ st $(a, n) = 1$

Example.
- only $\overline{a}$ generates $\mathbb{Z}/n\mathbb{Z}$ iff $(a, n) = 1$
- $\overline{1}, \overline{5}, \overline{7}, \overline{11}$ generate $\mathbb{Z}/12\mathbb{Z}$ and $\phi(12) = 4$

Theorem. *(7)*
Let $H = \langle x \rangle$
1) (every subgroup of H is cyclic) if $K \leq H$, then either $K = \{1\}$ (trivial group) or $K = \langle x^d \rangle$ where d is smallest positive integer st $x^d \in K$
2) case $|H| = \infty$: for any positive integers $a \neq b$, $\langle x^a \rangle \neq \langle x^b \rangle$
3) case $|H| = n < \infty$: for each positive integer a dividing n, $\exists!$ order a subgroup $\langle x^d \rangle$, $d = \frac{n}{a}$. Furthermore, $\forall m \in \mathbb{Z}$, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so subgroups of H correspond bijectively with the positive divisors of n

Proof.
1) let $K \leq H$
case $K = \{1\}$: ok
case $K \neq \{1\}$: let $\mathcal{P} = \{b | b \in \mathbb{Z}^+ \text{ and } x^b \in K\}$
by well ordering principle (§0.2), $\mathcal{P}$ has a minimum element, call it d
will show $\langle x^d \rangle = K$ by showing both containments
($\langle x^d \rangle \leq K$): since K is a subgroup and $x^d \in K$
($K \leq \langle x^d \rangle$): any element of K has form x^a, $a \in \mathbb{Z}$
by division algorithm, $a = qd + r$ for $0 \leq r < d$
so $x^r = x^{a-qd} = x^a (x^d)^{-q} \in K$ since $x^a, x^d \in K$
$r = 0$ since minimality of d
thus $a = qd$ and $x^a = (x^d)^q \in \langle x^d \rangle$
2) exercise, simular to (3) but easier
3) assume $|H| = n < \infty$, $a \mid n$, $d = \frac{n}{a}$
(exists subgroup of order a): prop 5(3) implies $\langle x^d \rangle$ is a subgroup of order a
(unique subgroup of order a): suppose $K \leq H$ and $|K| = a$
part 1 implies $K = \langle x^b \rangle$ where b smallest positive integer st $x^b \in K$
prop 5 implies $\frac{n}{d} = a = |K| = |x^b| = \frac{n}{(n,b)}$
so $d = (n, b)$, in particular, $d \mid b$
so $x^b \in \langle x^d \rangle$
so $K = \langle x^b \rangle \leq \langle x^d \rangle$
so $K = \langle x^d \rangle$ since $|\langle x^d \rangle| = a = |K|$
(final assertion) $\langle x^m \rangle \leq \langle x^{(n,m)} \rangle$ since (check this)
prop 5(2) and prop 2 imply they have same order
thus every subgroup of H arises from a divisor of n

Example. list the subgroups of $\mathbb{Z}/n\mathbb{Z}$ for $n = 12$:
soln: $\mathbb{Z}/12\mathbb{Z} = \langle \overline{1} \rangle = \langle \overline{5} \rangle = \langle \overline{7} \rangle = \langle \overline{11} \rangle$ (order 12)
$\langle \overline{2} \rangle = \langle \overline{10} \rangle$ (order 6)

$\langle\overline{3}\rangle = \langle\overline{9}\rangle$ (order 4)
$\langle\overline{4}\rangle = \langle\overline{8}\rangle$ (order 3)
$\langle\overline{6}\rangle$ (order 2)
$\langle\overline{0}\rangle$ (order 1)
the inclusions between them are given by:
$\langle\overline{a}\rangle \leq \langle\overline{b}\rangle$ iff $(b, 12) \mid (a, 12)$, $1 \leq a,\ b \leq 12$

Claim. (apply to centalizers and normalizers)
Let group G, $x \in G$
- [?] can obtain subgroups of group G by forming $C_G(\langle x\rangle)$ and $N_G(\langle x\rangle)$ for each $x \in G$
- $C_G(\langle x\rangle) = C_G(x)$
  pf: $g \in G$ commutes with x iff commutes with all powers of x
- $\langle x\rangle \leq N_G(\langle x\rangle)$ but equality need not hold
  pf: see section 2 exersice 6

Example. consider $i \in Q_8$
$C_{Q_8}(\langle i\rangle) = \{\pm 1, \pm i\} = \langle i\rangle$
$N_G(\langle i\rangle) = Q_8$

2.4. SUBGROUPS GENERATED BY SUBSETS OF A GROUP.

Remark.
- recall subgroup $\langle x\rangle$ by closing x under group operation (which includes inverse)
- recall $\langle x\rangle$ is the smallest subgroup containing x
  ie if $x \in H$ then $\langle x\rangle \subseteq H$
  ie $\langle x\rangle$ is the unique minimal (ordered by inclusion) element of the set of subgroups containing x
- a motivating question: given object G and subset A, find the smallest "subobject" containing A
  eg G=vector space, $A = \{v_1, v_2, ..., v_n\}$ then the smallest subspace contining A is the span of $\{v_1, v_2, ..., v_n\}$
- this section:
  - will generate subgroup from arbitrary subset A (not just singleton) by closing under group operation (and taking inverses)
  - will show that subgroup generated by A is unique smallest subgroup containing A
- the ideas used in this section will be used later more generally, and maybe without proof

Proposition. *(8)*
let $\mathcal{A}$ nonempty collection of subgroups of G
then intersection is also a subgroup

Proof. (simple application of subgroup criterion; §exercise 10)
let $K = \cap_{H\in\mathcal{A}} H$
$1 \in K$ since identity in each subgroup
$a, b \in K \Leftrightarrow a, b \in$each subgroup
so $ab^{-1} \in K$ since in each subgroup
prop 1 gives $K \leq G$

Definition. the subgroup of G generated by $A \subseteq G$ is $\langle A\rangle = \cap_{A\subseteq H; H\leq G} H$

Claim.
- $\langle A\rangle$ is a group
  pf: $\langle A\rangle$ is nonempty since $G \in \mathcal{A}$
  prop (8) with $\mathcal{A} = \{H \leq G | A \subseteq H\}$
- $\langle A\rangle$ is unique minimal element of $\mathcal{A}$
  pf: $\langle A\rangle \in \mathcal{A}$ since it is a subgroup containing A
  any element of $\mathcal{A}$ contains $\langle A\rangle$ since it is in the intersection

Remark.
- ntn: for finite $A = \{a_1, a_2, ..., a_n\}$, write $\langle a_1, a_2, ..., a_n\rangle$
  ntn: for $\langle A, B\rangle$ instead of $\langle A \cup B\rangle$
- def of $\langle A\rangle$ does not show how to construct elements
  next: characterization which allows generating its elements

Proposition. *(9) (recharacterize $\langle A\rangle$)*
$\langle A\rangle = \overline{A} := \{a_1^{\epsilon_1} a_2^{\epsilon_2} ... a_n^{\epsilon_n} | n \in \mathbb{Z}, n \geq 0, a_i \in A, \epsilon_i = \pm 1\}$
ie the set of all finite products (words) of elements of A and their inverses
also let $\overline{A} = \{1\}$ for $A = \emptyset$
note: a_i's need not be distinct
note: A need not be finite or even ctble

Proof. ($\overline{A}$ is a subgroup):
note: $\overline{A}$ nonempty
if $a, b \in \overline{A}$ where $a = a_1^{\epsilon_1} a_2^{\epsilon_2} ... a_n^{\epsilon_n}$ and $b = b_1^{\delta_1} b_2^{\delta_2} ... b_n^{\delta_n}$
then $ab^{-1} = a_1^{\epsilon_1} a_2^{\epsilon_2} ... a_n^{\epsilon_n} b_n^{-\delta_n} b_{n-1}^{-\delta_{n-1}} ... b_1^{-\delta_1}$
so $ab^{-1} \in \overline{A}$
thus $\overline{A}$ is a subgroup by prop 1
(will show both inclusions of $\overline{A} = \langle A\rangle$)
$\langle A\rangle \leq \overline{A}$ since $A \subseteq \overline{A}$ since each $a \in A$ can be written a
$\overline{A} \leq \langle A\rangle$ since $A \subseteq \langle A\rangle$ and it is closed under products and inverses, so each $a_1^{\epsilon_1} a_2^{\epsilon_2} ... a_n^{\epsilon_n} \in A$

Remark.
- now can rewrite
  $\langle A\rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} ... a_n^{\alpha_n} | a_i \neq a_{i+1} \in A, \alpha_i \in \mathbb{Z}, n \in \mathbb{Z}^+\}$
- if G abelian, can simplify further for $A = \{a_1, ..., a_k\} \subseteq G$:
  $\langle A\rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} ... a_k^{\alpha_k} | \alpha_i \in \mathbb{Z}\}$

Claim.
- if G abelian and each $a_i \in A$ has finite order d_i then $|\langle A\rangle| \leq d_1 d_2 ... d_k$
  (can simplify hypothesis to: each $a_i \in A$ commutes with all others in A)
  pf: there are $d_1 d_2 ... d_k$ distinct products of form $a_1^{\alpha_1} a_2^{\alpha_2} ... a_k^{\alpha_k}$
  and $\leq$ since could have $a^\alpha b^\beta = a^\gamma b^\delta$ even if $a^\alpha \neq a^\gamma$ and $b^\beta \neq b^\delta$
  (see direct products in ch5 for exactly when this happens)
- unlike abelian, if G non-abelian, given orders of a generating set, we cant even bound the order of G
  pf: cant simplify long products *ababab...ab* to form $a^\alpha b^\beta$
  see following examples
  will prove once we develop techniques

Example. (subgroups generated by small order elements can be complicated)
- consider $D_8 = \langle r, s\rangle$
  D_8 is also generated by $a = s$ and $b = rs$ since $s = a$ and $r = ba = rss$ both belong to $\langle a, b\rangle$
  note $|a| = 2 = |b|$ and $|D_8| = 8$
  so cant write every element of D_8 in form $a^\alpha b^\beta$, $\alpha, \beta \in \mathbb{Z}$
  eg cant even write *aba* in this form
- note: $S_n = \langle(1\ 2), (1\ 2\ 3 ...\ n)\rangle$
  this generated by elements of order 2 and n, yet $|S_n| = n!$
- consider $GL_2(\mathbb{R})$ and consider subgroups generated by $a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{pmatrix}$
  note $a^2 = 1 = b^2$ so each order is 2
  but $ab = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 2 \end{pmatrix}$ has infinite order
  so $\langle a, b\rangle$ has infinite order

Remark.
- so unlike cyclic groups, generating subgroup of non-abelian group by ≥ 2 elements, can be difficult, even to compute order
- but for well chosen generaters, can be useful
  ie to study a subgroup that contains $\langle x\rangle$ properly
  useful to study $\langle x, y\rangle$ where y commutes with x
  ie $y \in C_G(x)$
  then $\langle x, y\rangle$ abelian so order $\leq |x|\,|y|$
  (or choose $y \in N_G(x)$) then analogous bound and $\langle x, y\rangle$ not too complicated, see next chapter)
- non-abelian groups are especially complicated, but other non-group algebraic systems often have more convenient algebraic structure to avoid these complications

2.5. THE LATTICE OF SUBGROUPS OF A GROUP.

Remark.
- this section: visualize a group with a "lattice" of its subgroups
  wont define what a lattice is, but will mention properties
- will use lattices of subgroups through the end of groups, and in galois thy

Definition. (informally)
- lattice is a graph diagram of relationships between subgroups, connections if $\leq$ and no subgroup between
- sublattice can omit some subgroups

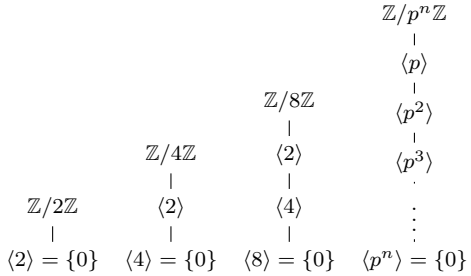
Algorithm.
input: all subgroups of G
output: lattice
position groups of higher order above those of lower order eg trivial 1 at bottom and G at top
draw line A to B if $A \leq B$ and no subgroups properly between A, B

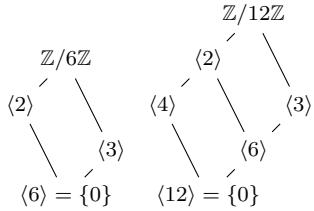
Remark.
- lattices can get complicated, see book Groups of Order 2^n for $n \leq 6$
- sublattices can be drawn for infinite groups

Claim.
- if $A \leq B$, then they will have path(s) passing through any intermediary subgroups
- $\forall H, K \leq G$, their unique smallest supergroup $\langle H, K\rangle$ (called their join) can be found by following paths upward until they meet
  similarly their unique largest subgroup(it is a subgroup by prop 8) (called thier intersection)
- isomorphic graphs $\Rightarrow$ same lattice
  but not converse since examples of size 16

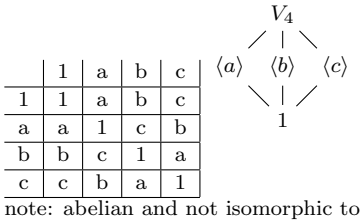
Remark. even though lattices can _not_ distinguish some non-isomorphisms, they are useful to see that two structures have common properties

Example. (proofs in later exercises once we have more thy)
1) $Z_n = \mathbb{Z}/n\mathbb{Z}$
   note: thm7: lattices of subgroups is the lattice of divisors of n (path from a to b if $a \mid b$)
   lattices for $\mathbb{Z}/2\mathbb{Z} = \langle 1\rangle$, $\mathbb{Z}/4\mathbb{Z} = \langle 1\rangle = \langle 3\rangle$, $\mathbb{Z}/8\mathbb{Z} = \langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle$, $\mathbb{Z}/p^n\mathbb{Z}$ for p prime, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$





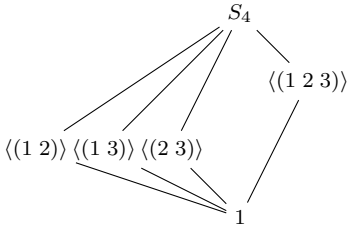
2) The Klein 4-group ("Viergruppe"), V_4, order 4, multiplication table and lattice:



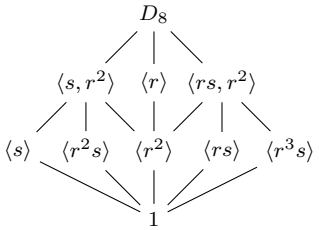
	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

note: abelian and not isomorphic to Z_4
note: to check whether group, check associative law or note that $V_4 \leq D_8$

3) the lattice of S_3 :

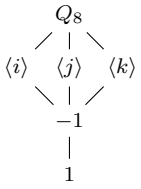


4) lattice of $D_8 = \langle r, s\rangle$

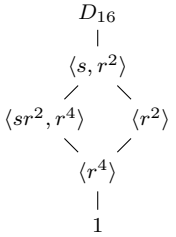


clm: $C_{D_8}(s) = \langle s, r^2\rangle$
pf: $\langle s, r^2\rangle \leq C_{D_8}(s)$ since ($r^2 \in C_{D_8}(s)$ since secion 2) and (an element always belongs in its centralizer)
so either $C_{D_8} = D_8$ or $\langle s, r^2\rangle$
but cant be D_8 since r does not commute with s
ie $r \notin C_{D_8}(s)$

5) lattice of Q_8



6) lattice of D_{16} (big, see book)
sublattice showing relationship between subgroups $\langle sr^2, r^4\rangle$ and $\langle r^2\rangle$



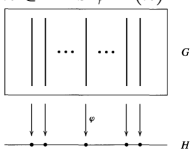
note that their join and intersection are $\langle s, r^2\rangle$ and $\langle r^4\rangle$

Claim. given lattice of subgroups of a group, compute normalizers and centralizers
pf: none, see above eg for D_8

3. QUOTIENT GROUPS AND HOMOMORPHISMS

3.1. DEFINITIONS AND EXAMPLES.

Remark.
- this chapter:
  - "quotient group" of a group G is a "smaller" group which allows studying the structure of G
  - [?] given lattice of subgroups of G, the lattice of subgroups for a quotient is reflected at the top, whereas the lattice for a subgroup is reflected at the bottom
  - using this, will get classification thms
  - will see that quotient groups are essentially equilvalent to the study of homomorphisms
- recall that for any function $\phi : G \to H$, fiber of $h \in H$ is $\phi^{-1}(h) = \{g \in G | \phi(g) = h\}$



Definition. the kernel of homomorphism $\phi : G \to H$ is $\ker\phi = \{g \in G | \phi(g) = 1_H\}$
where $1_H \in H$ identity
ie the fiber of 1_H

Proposition. *(1)*
Let homomorphism $\phi : G \to H$
1) $\phi(1_G) = 1_H$
2) $\phi(g^{-1}) = \phi(g)^{-1}$
3) $\phi(g^n) = \phi(g)^n$
4) $\ker\phi$ is a subgroup of G
5) $\mathrm{Im}\,\phi := \phi(G)$ is a subgroup of H

Proof. long

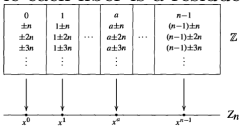
Definition. let $\phi : G \to H$ homomorphism with kernel K
the quotient group ("factor group") G/K ("G modulo K") is the group whose elements are the fibers of ϕ with group operation: (if X_a fiber of $a \in H$ and X_b fiber of $b \in H$ then $X_a X_b$ fiber of $ab \in H$ ie $X_a X_b = X_{ab}$) and identity is K
ntn: G/K since "dividing out" K
intuition: G is partitioned into fibers and the set of fibers is a group with multiplication following from that of H

Claim.
- this is a group
  pf: (associative) since multiplication in H is associative ie $(X_a X_b)X_c = X_{ab}X_c = X_{(ab)c} = X_{a(bc)} = ... = X_a(X_b X_c)$
  (identity) K
  (inverse) inverse of X_a is $X_{a^{-1}}$
- quotient G/K and H are isomorphic

Example. (motivating example)
consider $\phi : \mathbb{Z} \to Z_n$, $\phi(a) = x^a$ from $(\mathbb{Z}, +)$ to $Z_n = \langle x\rangle$ is cyclic group of order n
homomorphism since $\phi(a + b) = x^{a+b} = x^a x^b = \phi(a)\phi(b)$
surjective since $a \mapsto x^a$ so covered by $a = 1, ..., n-1$
the fiber of x^a is

$$\begin{aligned}\phi^{-1}(x^a) &= \{m \in \mathbb{Z} | x^m = x^a\}\\ &= \{m \in \mathbb{Z} | x^{m-a} = 1\}\\ &= \{m \in \mathbb{Z} | n \text{ divides } m - a\} \text{ (prop 2.3)}\\ &= \{m \in \mathbb{Z} | m = a \mod n\}\end{aligned}$$

ie each fiber is a residue class modulo n



the identity is $n\mathbb{Z}$ =all multiples of n, which is a subgroup of $\mathbb{Z}$
the remaining fibers are just translates $a + n\mathbb{Z}$ of this subgroup
the group operation can be performed by multiplying in Z_n then taking the fiber (wrt homomorphism) of the product
but might be easier to multiply representatives of fibers, and mimic multiplication in Z_n

Proposition. *(2) (characterize fibers in terms of kernel)*
Let homomorphism $\phi : G \to H$ with kernel K and denote fiber of $a \in H$ with $X = \phi^{-1}(a)$
a) $\forall u \in X$ $X = \{uk | k \in K\}$ (="uK") (ie $\forall$ representatives $u_1 \in uK$, $u_1 K = uK$)
b) similar but ku and Ku

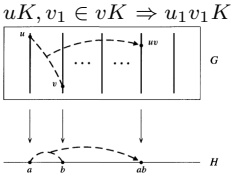
Remark. will see (prop 4) that can replace kernel in prop 2 with any subgroup $N \leq G$ and $u_1 \in uN \Rightarrow u_1 N = uN$ still holds
but first some preliminary stuff...

CHARACTERIZE QUOTIENT GROUP USING COSETS

Definition. the left coset ("left translate") of $g \in G$ wrt $N \leq G$ is $gN = \{gn | n \in N\}$
right coset ... $Ng = \{ng | n \in N\}$
ntn: for additive, use $g + N$ and $N + g$

Remark.
- (characterize cosets (from §1.7 ex 18)): the right cosets of $N \leq G$ are precisely the "orbits" of N acting on G by left multiplication
- prop 2 restated: fibers of a homomorphism (ie elements of G/K) are left cosets of the kernel (=right cosets of kernel)
- next: multiplication in G/K by multiplying representatives and then taking its coset wrt kernel

Theorem. *(3) (characterize quotient group using cosets of kernel)*
let homomorphism of G to another group, kernel K
group G/K is formed by left cosets of K with operation $uK \circ vK = (uv)K$
(analogously for right cosets)
in particular, this operation is well defined ($u_1 \in uK, v_1 \in vK \Rightarrow u_1 v_1 K = uvK$)



Proof. book

Remark.
ntn: $\overline{u} = uK$, $\overline{G} = G/K$, $\overline{u}\,\overline{v} = \overline{uv}$
ntn: "reducing mod K" is considering the coset containing an element

Example.
1) $\phi : \mathbb{Z} \to Z_n$
   kernel: $n\mathbb{Z}$
   fibers: $a + n\mathbb{Z}$ ie left cosets(=right cosets) of kernel
   quotient group: $\mathbb{Z}/n\mathbb{Z}$ with addition of representatives
   quotient group is isomorphic to images, $Z_n \cong \mathbb{Z}/n\mathbb{Z}$ (see ch 2)
2) let $\phi : G \to H$ isomorphism with kernel $K = 1$
   fibers: singleton subsets of G
   $G/1 \cong G$
3) let trivial homomorphism $\phi : G \to \{1\}$ $\phi(g) = 1$
   $\ker\phi = G$
   $G/G \cong Z_1 = \{1\}$
4) let groups (R^2,vector addition) and $(\mathbb{R}, +)$
   define $\phi : \mathbb{R}^2 \to \mathbb{R}$, $\phi(x, y) = x$ ie projection onto x-axis
   homomorphism since $\phi((x_1, y_1) + (x_2, y_2)) = \phi(x_1 + x_2, y_1 + y_2) = x_1 + x_2 = \phi(x_1 + y_1) + \phi(x_2 + y_2)$
   $\ker\phi = \{(x, y) | x = 0\}$ ie y-axis
   note: $a \in \mathbb{R}$, fiber $\phi^{-1}(a)$ is line $y = a$ ie translate kernel by a
   ie $\overline{(a, 0)} = (a, 0) + y$-axis where representative $(a, 0)$
   note: two ways to describe group operation:
   - in terms of ϕ: sum of lines $x = a$ and $x = b$ is line $x = a + b$

- in terms of representatives of cosets: $\overline{(a,y_1)} + \overline{(b,y_2)} = \overline{(a+b, y_1+y_2)}$

5) (a non-abelian example)
let $\phi : Q_8 \to V_4$, $\phi(\pm 1) = 1$, $\phi(\pm i) = a$, $\phi(\pm j) = b$, $\phi(\pm k) = c$
homomorphism: can show exhaustively, with shortcuts using symmetry
ϕ surjective since obvious
$\ker \phi = \{\pm 1\}$
$Q_8/\{\pm 1\}$ is fibers (=left cosets=right cosets) $\{\pm 1\}$, $\{\pm i\}$, $\{\pm j\}$, $\{\pm k\}$ corresponding to $1, a, b, c$

Remark.
- given subgroup $N \leq G$ which is the kernel of some homomorphism, can proceed without the homomorphism since quotient G/N has multiplication $uNvN = uvN$
- will see (prop 5) that this doesnt work for arbitrary subgroups, since multiplication wont be well-defined
- will see (prop 7) can build group G/N using cosets iff N is the kernel of a homomorphism
- will prove criterion that subgroup N is a kernel, call it "normal" subgroup

Proposition. *(4) (cosets of any subgroup partition the group)*
let $N \leq G$
the set of left cosets of N in G form a partition of G
furthermore, $\forall u, v \in G$, $uN = vN$ iff $v^{-1}u \in N$
in particular, $uN = vN$ iff u, v are in the same coset

Proof. book

Proposition. *(5)*
Let $N \leq G$
1) the operation on the set of left cosets $uN \cdot vN = (uv)N$ is well defined
iff $\forall n \in N$ $\forall g \in G$ $gng^{-1} \in N$
2) if above operation is well defined
then the set of left cosets of N in G form a group G/N with identity $1N$ and inverse of gN is $g^{-1}N$ (ntn $(gN)^{-1}$)

Proof. book

Remark. give a name to subgroups in prop 5...

Definition.
- the conjugate of $n \in N$ by g is gng^{-1}
- the conjugate of N by g is $gNg^{-1} = \{gng^{-1} | n \in N\}$
- g normalizes N means $gNg^{-1} = N$
- normal subgroup $N \leq G$ means every $g \in G$ normalizes N
  ie $\forall g \in G$ $gNg^{-1} = N$
  ie $N_G(N) = G$
  ntn: $N \trianglelefteq G$

Claim. structure of G is reflected in G/N for $N \trianglelefteq G$
eg associative and inverses of G/N induced from G (see section 3 (isomorphism thms) for more relationships between G and its quotient G/N)

Theorem. *(6) (summary)*
Let $N \leq G$. The following are equivalent:
1) $N \trianglelefteq G$
2) $N_G(G) = G$
3) $gN = Ng$ $\forall g \in G$
4) the set of left cosets of N with operation in prop 5 is a group
5) $gNg^{-1} \leq N$ $\forall g \in G$

Proof. see previous results, rest is simple exercises

Remark. methods to compute whether $N \leq G$ is normal
- naively check all conjugates gng^{-1} $\forall n \in N$ $\forall g \in G$
  (but only need $g \in G/N$ since N already normalizes N [?])
- like above but only check conjugate of generators of N lie in N
  (since conjugate of product is product of conjugates and conjugate of inverse is inverse of conjugate, see ex 26)
- if generators of G are known, only check them
- if N finite, suffices to check whether cojugates of generators of N by generators of G are elements of N (ex 29)
- sufficient to prove $N_G(N) = G$

Proposition. *(7)*
$N \leq G$ is normal iff N is kernel of some homomorphism

Proof. book

Remark. name of homomorphism constructed in prop 7..

Definition.
- the natural projection homomorphism is $\pi : G \to \overline{G/N}$, $\pi(g) = gN$
  note: surjection
  ntn: "natural" indicates that the homomorphism is "coordinate-free" ie not described by generators
- the complete preimage of $\overline{H} \leq G/N$ in G is $\pi^{-1}(\overline{H})$

Claim.
- the complete preimage of $\overline{H} \leq G/N$ is a subgroup of G
  this subgroup contains N since $\pi(N) = 1 \in H$
- there is a correspondence between subgroups of G that contain N and subgroups of G/N
  pf: isomorphism thms in section 3

Remark.
- criterion $N_G(N) = G$ allows us to consider normalizer to measure "how close" N is to being a normal subgroup
- being normal is an "embedding" property ie can be normal to some groups and not to others
- recap:
  - kernel of homomorphism is a normal subgroup
  - quotient group G/N (defined with fibers) is naturally isomorphic to $\phi(G)$
  - conversely, if $N \trianglelefteq G$, then can find homomorphism with kernel N
    (namely, natural projection $\pi : G \to G/N$)
  - so can produce normal subgroups and homomorphisms from each other
    so studying one is equivalent to studying the other
- 2 ways to develop the theory of quotient groups are:
  1) through homomorphisms
  2) defining normal subgroups and its associated quotient groups
  we used 1 to emphasize that the elements of the quotient are subsets (=fibers=cosets of kernel)
  our figures display that N and its coset are projected ("collapsed") onto single elements of G/N
  the operation of G/N is performed using representatives of cosets involved

Example. let G group
- 1 and G are normal subgroups of G
  $g/1 \cong G$ and $G/G \cong 1$
- if G is abelian
  - then any $N \leq G$ is normal since $gng^{-1} = gg^{-1}n = n \in N$
  - if also $G = (\mathbb{Z}, +)$, then every subgroup is cyclic $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle$ for some $n \in \mathbb{Z}$
    and quotient groups $\mathbb{Z}/n\mathbb{Z}$ are cyclic with generator $\overline{1} = 1 + n\mathbb{Z}$ where 1 is generator of $(\mathbb{Z}, +)$
  - if $GZ_k = \langle x \rangle$ ie cyclic group of order k
    let $N \leq Z_k$
    prop 2.6 $\Rightarrow$ $N = \langle x^d \rangle$ where d is smallest power of x in N
    quotient $Z_n/N = \{x^\alpha N | \alpha \in \mathbb{Z}\}$ [?]
    $= \langle xN \rangle$ since $x^\alpha N (xN)^\alpha$ since exercise 4
    ie Z_n/N is cyclic with generator xN
    $|xN| = d$ since exercise 5
    prop 2.5 $\Rightarrow d = \frac{|G|}{|N|}$
    summary: quotient groups of cyclic groups are cyclic with generator $\overline{g}$ is the image of generator g of G
    if G also finite, then $|G/N| = \frac{|G|}{|N|}$
- if $N \leq Z(G)$ then $N \trianglelefteq G$ since by def all $gng^{-1} = n \in N$
  note: this generalizes previous example where $Z(G) = G$
  thus $Z(G) \trianglelefteq G$
  - recall $\langle -1 \rangle \leq Q_8$ is normal since homomorphism method
    now we also prove normality since $\langle -1 \rangle = Z(Q_8)$
  - recall $Q_8/\langle -1 \rangle \cong V_4$
    now can prove this using (see method for example with D_8)
  - consider $G = D_8$
    $Z(D_8) = \langle r^2 \rangle = \{1, r^2\}$
    4 cosets: $gZ = \{g, gr^2\}$; $\overline{1} = 1Z$, $\overline{r} = rZ$, $\overline{s} = sZ$, $\overline{rs} = rsZ$
    recall (§2.8 ex10 where we calssified order 4 groups) $D_8/Z(D_8) \cong Z_4$ or V_4
    to diceide which one, observe:
    $(\overline{r})^2 = r^2 Z = 1Z = \overline{1}$
    $(\overline{s})^2 = s^2 Z = 1Z = \overline{1}$
    $(\overline{rs})^2 = (rs)^2 Z = 1Z = \overline{1}$
    so every nonidentity element of D_8/Z has order 2
    so no element of order 4 in the quotient
    so D_8/Z not cyclic
    so $D_8/Z(D_8) \cong V_4$

3.2. MORE ON COSETS AND LAGRANGE'S THM.

Remark. this section:
- Lagrange's thm and easy consequences
- more on cosets of non-normal subgroups

Theorem. *(Lagrange's thm)*
if group G finite and $H \leq G$
then $|H| \mid |G|$ and the number of left cosets of H in G is $\frac{|G|}{|H|}$

Proof. let $|H| = n$ and let the number of left cosets of H in G be k
prop 4 $\Rightarrow$ left cosets of G in G partition G
define map $H \to gH$ (=left coset), $h \mapsto gh$
surjective since def of left coset
injective since $gh_1 = gh_2 \Rightarrow h_1 = h_2$ since left cancellation law
thus $|gH| = |H| = n$
$|G| = kn$ since G is partitioned into k disjoint subsets each with cardinality n

Definition. let G group, possibly finite, and $H \leq G$
the index of H in G, $|H : G|$, is the # of left cosets of H in G

Claim.
- if G finite, $|G : H| = \frac{|G|}{|H|}$
- if G infinite, can have finite or infinite index
  eg $\{0\} \leq \mathbb{Z}$ has infinite index
  eg $\langle n \rangle \leq \mathbb{Z}$ has index n

Remark. now some easy consequences of Lagrange's thm

Corollary. *(9)*
if G finite and $x \in G$
then $|x| \mid absG$
in particular, $x^{|G|} = 1 \ \forall x \in G$

Proof. short

Corollary. *(10)*
if group G has prime order p
then G is cyclic ie $G \cong Z_p$

Proof. short

Example. (more normal subgroups)
1) clm: $\langle (1\ 2\ 3) \rangle \leq S_3$ (ntn $H \leq G$)
then $H \trianglelefteq S_3$
pf: §2.2 $\Rightarrow H \leq N_G(H) \leq G$
Lagrange's thm $\Rightarrow |H| \mid |N_G(H)|$ and $|B_G(H)| \mid |G|$
note: $|G| = 6$ and $|H| = 3$
so either $N_G(H) = H$ or G
note: $(1\ 2)(1\ 2\ 3)(1\ 2)^{-1} = (1\ 3\ 2) = (1\ 2\ 3)^{-1}$
ie $(1\ 2)$ conjugats a generator of H to another generator of H
thus $(1\ \ 2) \in N_G(H)$ since above satisifes §2.4ex24
thus $N_G(H) \neq H$
this $N_G(H) = G$ ie $H \trianglelefteq S_3$
2) (genralization of previous example)
let group G and $H \leq G$ and $|G : H| = 2$
clm: $H \trianglelefteq G$
pf: note: the 2 left cosets must partition G
coset $1H = H$ so other coset must be $gH = G/H$
where $g \in G/H$
similar for right cosets
so $gH = Hg$ and $1H = H1$ ie every left coset=right coset
so $H \trianglelefteq G$ by thm 6
also note $|G/H| = 2$ by def of index
so $G/H \cong Z_2$
note: will generalize this in next chapter
3) $\trianglelefteq$ is not transitive
pf: eg $\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$ since each subgroup fo index 2 in the next
but $\langle s \rangle$ not normal in D_8 since $rsr^{-1} = sr^2 \neq \langle s \rangle$

Remark.
- non-ableian groups can have non-normal subgroups (Q_8 is the only exception)
- there are groups with only the trivial normal subgroups 1 and G
(these are called "simple groups", see ch4)

Example. (non-normal subgroups)
1) consider $H = \langle (1\ 2) \rangle \leq S_3$
clm: $H \not\trianglelefteq S_3$
pf1: $|H : S_3| = 3$
Lagrange's thm $\Rightarrow N_{S_3}(H) = H$ or S_3
$N_{S_3}(H) \neq S_3$ since $(1\ \ 3)(1\ \ 2)(1\ \ 3)^{-1} = (1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin H$
pf2: (using left and right cosets of H)
see book, refers to exercises
pf3: (group operations on left cosets of H in S_3 is not well defined)
eg consider product of $1H$ and $(1\ 3)H$
trying representatives $1, (1\ 2) \in 1H$: $1 \cdot (1\ 3) = (1\ 3)$ and $(1\ 2)(1\ 3) = (1\ 3\ 2)$
but $(1\ 3), (1\ 3\ 2)$ are not in the same left coset
2) (generalize preceding example)
let $G = S_n$ for some $n \in \mathbb{Z}^+$, fix $i \in \{1, 2, ..., n\}$
let $G_i = \{\sigma \in G | \sigma(i) = i\}$ be stabilizer of i
$\tau \in G$ and $\tau(i) = j \Rightarrow \forall \sigma \in G_i$, $\tau\sigma(i) = j$ since def of G_i
furthermore, $\mu \in G$ and $\mu(i) = j \Rightarrow \tau^{-1}\mu(i) = i$
ie $\tau^{-1}\mu \in G_i$
so $\mu \in \tau G_i$
thus $\tau G_i = \{\mu \in G | \mu(i) = j\}$ ie the left coset τG_i is the permutations in S_n which take i to j
note: distinct left cosets have empty intersection
note: there are n distinct left cosets (which equals the number of distinct images of i under action of G)
thus $|G : G_i| = n$
ntn: let $k = \tau^{-1}(i)$ so $\tau(k) = i$
similarly, $G_i\tau = \{\lambda \in G | \lambda(k) = i\}$
let $n > 1$ and $\tau \neq$identity, then $\tau G_i \neq G_i\tau$ since there are permutations st $i \mapsto j$ but $k \not\mapsto i$
thus G_i not a normal subgroup
furthermore, §1ex30 $\Rightarrow N_G(G_i) = G_i$, so G_i is in some sence far from being normal in S_n
3) for D_8, the center $\langle r^2 \rangle$ is the only order 2 normal subgroup

Remark.
- converse of lagrange not true, ie $n \mid |G| \Rightarrow G$ need not have a subgroup of order n
pf: eg A =group of symmetries of regular tetrahedron
$|A| = 12$ (since §1.2ex9)
towards contradiction, suppose $\exists H \leq A$ st $|H| = 6$
then H has index 2 ($= \frac{|A|}{|H|}$
hence $H \trianglelefteq A$ and $A/H \cong Z_2$
$\forall g \in A/H$, $|x|^2 = 1$(=identity) since $|A/H| = 2$
thus $\forall g \in A$, $(gH)^2 = 1H$ ie $\forall g \in A$, $g^2 \in H$
if $g \in A$ and $|g| = 3$, then $g = (g^2)^2 \in H$
thus H must contain all emements of A of order 3
contradiciton since $|H| = 6$ but can exhibit 8 rotations of tetrahedron of order 3
- partial converse to Lagrange's thm:
for finite abelian groups, the full converse of Lagrange is true
ie an abelian group has a subgroup of order of each divisor of G
(see ch6 for weakening abelian assumption)
two other converses follow...

Theorem. *(11) (Cauchy's thn)*
if group G finite and prime $p \mid |G|$
then G has an element of order p

Proof. pf1: next chapter pf2: elegant, outlined in ex 9

Theorem. *(12) (Sylow)*
if group G finite of order $p^\alpha m$, p prime, and $p \nmid m$
then G has subgroup of order p^α

Proof. next chapter

Remark.
- next chapter: derive more info about the # of subgroups of order p^α
- rest of this section: useful results involving cosets

Definition. let H, K finite subgroups
$HK := \{hk | h \in H, k \in K\}$

Proposition. *(13)*
if H, K finite subgroups
then $|HK| = \frac{|H||K|}{|H \cap K|}$

Proof. book

Remark. notice: prop 13 did not assume HK is a subgroup
eg let $G = S_3$, $H = \langle (1\ 2) \rangle$, $K = \langle (2\ 3) \rangle$)
then $|H| = |K| = 2$ and $|H \cap K| = 1$ so $|HK| = 4$
Lagrange's them $\Rightarrow HK$ cannot be a subgroup
thus $S_3 = \langle (1\ 2), (2\ 3) \rangle$

Proposition. *(14)*
let $H, K \leq G$
$HK \leq G$ iff $HK = KH$

Proof. book

Remark. confusing ntn: $HK = KH$ does not imply individual eleements of H, K commute
eg $G = D_{2n}$, $H = \langle r \rangle$, $K = \langle s \rangle$
then $G = HK = KH$ and $rs = sr^{-1}$ ie dont commute
this is an example of the following sufficient condition for HK to be subgroup

Corollary. *(15)*
if $H, K \leq G$ and $H \leq N_G(K)$
then $HK \leq G$
in particular, $K \trianglelefteq G \Rightarrow HK \leq G \ \forall H \leq G$

Proof. short

Definition.
- A <u>normalizes</u> K means $A \subseteq N_G(K)$
- A <u>centralizes</u> K means $A \subseteq C_G(K)$

Remark.
- restate cor 15: HK is a subgroup if H normalizes K
similarly, HK is a subgroup if K normalizes H
- using order formula in prop 13, can sometimes prove that a finite group is a product of two subgroups
eg $G = S_4$, $H = D_8$ (ie permutes vertices of square), $K = \langle (1\ 2\ 3) \rangle$
lagrange's thm $\Rightarrow H \cap K = 1$ (ex8)
prop 13 $\Rightarrow |HK| = 24$
thus $HK = S_4$
$HK = KH$ since HK is a group
exercise: neither H nor K normalizes the other (so cor15 does not give $HK = KH$)

Remark. combinatorial results of this chapter work if used right cosets instead of left
- for normal subgroups, trivial since left cosets = right cosets
- for non-normal subgroups lagrange's thm: # right cosets of $H \leq G$ is $\frac{|G|}{|H|}$
same for infinute groups (ex12)

our use of left cosets will have benefits in next chapter's actions on cosets
ntn: in some books, $G \setminus G$=the set of right cosets
ntn: in some books, if $H \not\trianglelefteq H$, then G/H denotes the "coset space" fo left cosets of H in G

3.3. THE ISOMORPHISM THMS.

Remark. this section
- derive straightforward consequences of the relations between quotient groups and homomorphisms in secion 1
- in particular, the relation between the lattice of subgroups of G/N and that of G

Theorem. *(16) (first isom. thm) (fund. thm of homomorphisms)*
let $\phi : G \to H$ homomorphism of groups

1) ϕ injective iff $\ker \phi = 1$
2) $|G : \ker \phi| = |\phi(G)|$

Proof. exercise

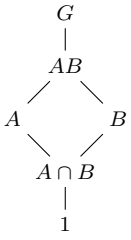
Example. from thy of linear transformations:
$\phi : V \to W$ linear transformation of vector spaces
$\Rightarrow \dim V =$rankϕ+nullityϕ
pf: cor 17(2)

Theorem. *(18) (second or diamond isomorphism thm)*
let $A, B \leq G$ and $A \leq N_G(B)$
then $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$, and $AB/B \cong A \cap B$

Proof. book

Remark.
- this gives new pf to order formula in prop 13 in the special case $A \leq N_G(B)$

- "diamond" since lattice of subgroups:



- quotient AB/A need not be a group (ie A need not be normal in AB)
  however, we still have $|AB : A| = |B : A \cap B|$

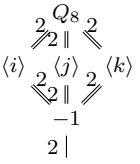
Theorem. *(19) (third isomorphism thm) (quotient groups of quotient groups)*
let $H, K \trianglelefteq G$
then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong G/K$
ntn: bar means quotient by H, so $\overline{G}?\overline{K} = G/K$

Remark.
- "invert and cancel" similar to fractions
- gain no new structural info by taking quotient of quotient groups

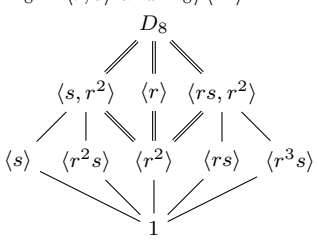
Theorem. *(20) (fourth or lattice isomorphism thm) (relation between lattices of quotient group and group)*
let $N \trianglelefteq G$
then $\exists$ bijection from subgroups $A \leq G$ containing N
to the set of subgroups $\overline{A} = A/N$ of G/N
in particular, every subgroup of G has form A/N (namely its preimage in G under the natural projection homomorphism from G to G/N)
this bijection has the following properties:
1) $A \leq B$ iff $\overline{A} \leq \overline{B}$
2) $A \leq B \Rightarrow |B : A| = |\overline{B} : \overline{A}|$
3) $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$
4) $\overline{A \cap B} = \overline{A} \cap \overline{B}$
5) $A \trianglelefteq G$ iff $\overline{A} \trianglelefteq \overline{G}$

Proof. §1ex1 $\Rightarrow$ the complete preimage of a subgroup in G/B is a subgroup of G
res is straightforward and in exercises

Example.
1) $Q_8/\langle -1\rangle$ (note $\langle -1\rangle \trianglelefteq Q_8$) has lattice which is isomorphic to the lattice of Q_8 above $\langle -1\rangle$
   ntn: double lines indigate which qhotients are isomorphisms [?]
   index $|A : B|$ along path



   note: $Q_8/\langle -1\rangle \cong V_4$
2) $D_8 = \langle r, s\rangle$ and $D_8/\langle r^2\rangle$



   note: should have "2" along each edge, but too crowded

Claim.
- isomorphism types of G/N and N do not determine the isomorphism type of G
  pf: eg above are two lattices of order 8 groups
  $Q_8/\langle -1\rangle \cong D_8/\langle r^2\rangle$ and $\langle -1\rangle \cong \langle r^2\rangle$
  yet $Q_8 \ncong D_8$
  see next section for more
- subgroups of G which do not contain normal subgroup N do not directly correspond to subgroups of G/N
  since N projects to a point in G/N so several subgroups of G can project to same subgroup in the quotient
  natural projection $\pi : G \to G/N$ takes $H \leq G$ and $HN \leq G$ to same image and $N \subseteq HN$ conversely, the preimage of $\overline{H} \leq G/N$ is the unique subgroup of G containing N whose image in G/N is $\overline{H}$
  so the subgroup fo G containing N appears explicitly in the lattice for G/N
- order of any subgroup is product of integers $|A : B|$ along path from identity to that subgroups
  thm 20(2) $\Rightarrow$ these indices remain unchanged in quotients by normal subgroups

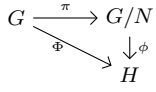
INDUCED HOMOMORPHISM ϕ on G/N

Remark.
- now, definintion of homomorphisms on quotient group
- in this section's proofs, we defined homomorphism ϕ on G/N by defining $\phi(gN)$ (ie on coset gN) in terms of representative g
  and then proved ϕ well defined
- this actualy defines homomorphism Φ on G itself

Claim. (criterion for defining homomorphism on quotients)
ϕ is well defined
$\Leftrightarrow N \leq \ker \Phi$ ie Φ trivial on N

Definition. in this case Φ factors through N
and ϕ is the induced homomorphism on G/N

Remark.
- intuitively, commutative diagram shows $\Phi = \phi \circ \pi$



- now can read §6.3

3.4. COMPOSITION SERIES AND THE HOLDER PROGRAM.

Remark.
- above results (quotient group has lattice of group above normal subgroup) gives a powerful technique in finite (and some branches of infinite) group thy: induction on order of group to use info about G/N and $N \trianglelefteq G$ to prove things about G
- next pf illustrates this induction

Proposition. *(21) (special case of Cauchy's thm, will use in ch 4)*
Let G finite abelian group and prime p divides $|G|$
$\Rightarrow$ G contains an element of order p

Proof. (induction on $|G|$)
assume prop holds for all groups $< |G|$ ie complete induction
$\exists x \in G$ since $|G| > 1$
case $|G| = p$: lagrange's thm $\Rightarrow |x| = p$ so done
so assume $|G| > p$
case $p \mid |x|$: $|x| = pn$ so $x^n = p$ so done
so assume $p \nmid |x|$
let $N = \langle x\rangle$
$N \trianglelefteq G$ since G abelian
Lagrange's thm $\Rightarrow |G/N| = \frac{|G|}{|N|}$
$|G/N| < |G|$ since $N \neq 1$
$p \mid |G/N|$ since $p \nmid |N|$
by induction hypothesis, $\exists \overline{y} = yN \in G/N$ of order p
notes: $y \notin N$ (ie $\overline{y} \neq \overline{1}$) and $y^p \in N$ (ie $y^p = \overline{1}$)
thus $\langle y^p\rangle \neq \langle y\rangle$ ie $|y^p| < |y|$
prop 2.5(2) $\Rightarrow p \mid |y|$
earlier argument (about $|x^n| = p$) $\Rightarrow y$ has order p

Remark.
- recall that the full isomorphism type of G cannot be determined from isomorphism types of N and G/N alone
  so need more data
- prop used abelian group, but in general finding nontrivial ($\neq 1$) and proper ($N < G$) normal subgroup makes this method of proof difficult, which leads to def...

Definition. a (finite or infinite) simple group G means $|G| > 1$ and the only normal subgroups are 1 and G

Claim.
- if $|G|$ prime
  then its only subgroups (let alone nomral ones) are 1 and G
  pf: Lagrange's thm
- every abelian simple group is isomorphic to Z_p for some prime p
  pf ex1
- there are non-abelian simple groups
  pf: smallest one has order 60, see next section, it is a member of an infinite family of simple groups

Remark.
- simple groups, by def, can't be "factored" into pieces like N and G/N so they are analogous to primes in arithmetic of $\mathbb{Z}$
- this analogy is supported by a "unique factorization thm"...

Definition. a composition series is a sequence of groups
$1 = N_0 \leq N_1 \leq N_2 \leq ... \leq N_{k-1} \leq N_k = G$
st composition factors $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is simple

Example. (motivating example)
two composition series for D_8:
$1 \leq \langle s\rangle \leq \langle s, r^2\rangle D_8$
$1 \leq \langle r^2\rangle \leq \langle r\rangle \leq D_8$
each composition factor is isomorphic to simple group Z_2

Theorem. *(22) (Jordan-Holder)*
if $G \neq 1$ finite group, then
1) G has a composition series and
2) its composition factors are unique
namely, let 2 composition series:
$N_0 \leq N_1 \leq ... \leq N_r$ and $M_0 \leq ... \leq M_s$
then $r = s$ and $\exists$ permutation π of $\{1, 2, ..., r\}$ st $M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1}$ for $1 \leq i \leq r$

Proof. straighformward, leave to exercises since will not use this thm to prove others

Remark. (summary)

- each finite group has a "factorization" into composition series
- composition series need not be unique, but the number of composition factors and their isomorphism type are unique
- nonisomorphic groups may have the same (up to isomorphism) list of composition factors
  pf: ex2
- this motivates a 2 part program for classifying all finite groups up to isomorphism...

HOLDER PROGRAM

Definition. The Holder program is
1) classify all finite simple groups
2) ("extension problem") find all ways to "put together simple groups" to form other groups

Remark.
- these two problems motivated much of the development of group thy
- analogous themes recur throughout math
- the classification of part 1 of Holder program was completed in 1980... thm...

Theorem. *every finite simple group is isomorphic to one of:*
18 (infinite) families of simple groups
and 26 other "sporadic" simple groups

Proof. 5000-1000 pages

Claim. examples of families of finite simple groups
- $\{Z_p | p \text{ prime}\}$
- $\{SL_n(\mathbb{F})/Z(SL_n(\mathbb{F})) | n \in \mathbb{Z}^+, n \geq 2, \mathbb{F} \text{ some fnite field}\}$ are simple except $SL_2(\mathbb{F}_2)$ and $SL_2(\mathbb{F}_3)$ (where $\mathbb{F}_k$ is finite field with k elements)
  note: this family has 2 parameters: n and $\mathbb{F}$
  pf: see book: Finite Group Thy
- Alternating groups
  pf: next section and next chapter

Theorem. *(Fiet-Thompson - a cornerstone of entire classification)*
if G finite simple group of odd order
then $G \cong Z_p$ for some p prime

Proof. 255 pages of hard math

Remark.
- in part 2 of Holder's program, "put 2 groups together" means:
  given groups A, B, describe how to obtain all groups G containing $N \trianglelefteq G$ st $N \cong B$ and $G/N \cong A$
  - eg $A = B = Z_2$
    want to know how to build groups of order 4 from these
    §2.5ex10$\Rightarrow G = Z_4$ or V_4
  - eg all composition factors of G have order 2 $\Leftrightarrow |G| = 2^n$ for some n
    pf: ch6
    note: the # of groups of order 2^n grows (exponentiall in 2^n)
    so can't bound the # of ways to put groups of 2-power order together
- nevertheless, there are powerful techniques to unravel the structure of large classes of groups
- will discuss some ways to build larger groups from smaller ones
  will construct new examples of groups
  will prove som classification thms

SOLVABLE GROUPS

Definition. a solvable group G means $\exists$ chain of subgroups $1 = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_s = G$ st each G_i/G_{i-1} abelian

Remark. this class of groups is useful in the theory of polynomial eqns:
in Galois thy, there is a correspondence between these groups and polynomails solvable by radicals (ie $\exists$ algebraic formula for roots)

Claim.
- finite solvable groups are precisely those groups whose composition factors are all of prime order
  pf ex8
- (generalize Sylow's thm)
  finite group G is solvable
  $\Leftrightarrow \forall$ divisors n of $|G|$ st $(n, \frac{|G|}{n}) = 1$, G has a subgroup of order n
  thm 6.11 and thm 19.8
- N and G/N are solvable
  $\Rightarrow G$ is solvable
  pf: N solvable $\Rightarrow$ chain of subgroups $...N_i...$
  $\overline{G} = G/N$ solvable $\Rightarrow$ chain of subgroups $...\overline{G}_i...$
  lattice isomorphism thm $\Rightarrow \exists G_i \leq G$ st $N \leq G_i$ and $G_i/N = \overline{G}$ and $G_i \trianglelefteq G_{i+1}$ for $0 \leq i < 1$
  3rd ismomorphism thm $\Rightarrow 1 = N_0 \trianglelefteq N_1 \trianglelefteq ... \trianglelefteq N_n = N = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$ is a chain of subgroups of G with successive quoitent groups are abelian

Remark.
- next chapter:
  recall intro to Holder Program (2) with groups A, B combined to build G
  under certain conditions, we are led to the action of A on B
  results about simple and non-simple groups
- next section:
  family of simple groups
  useful later in study of determinants and study of solvability of polynomial eqns

3.5. TRANSPOSITIONS AND THE ALTERNATING GROUP.

Remark.
- recall §1.3: every element of S_n can be written uniquely as product of disjoint cycles
- in contrast, non-disjoint products are not unique
  eg (1 2 3) = (1 3)(1 2) = (1 2)(1 3)(1 2)(1 3) = (1 2)(2 3) = ...

Definition. a transposition is a 2-cycle

Claim. every element of S_n can be written as a product of transpositions
ie $S_n = \langle T \rangle$ where $T = \{(i\ j) | i \leq i < j \leq n\}$
pf: for any m-cycle, $(a_1\ \ a_2 ... a_m) = (ia_1\ a_m)(a_1\ a_{m-1} ... (a_1\ a_2))$
and any permutation in S_n has a cycle decomposition

Example. §1.3 ex about S_{13} rewritten as transpositions

THE ALTERNATING GROUP

Remark.
- recall can write any $\sigma \in S_n$ as product of transpositions
- this can be done in many ways, but always with the same parity (even or odd # of transpositions)

Definition. let polynomail $\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)$
let $\sigma \in S_n$ action on Δ: $\sigma(\Delta) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})$
note: $\sigma(\Delta) = \pm\Delta$ where we collected all negatives from sign changes
the sign of σ is $\epsilon(\sigma) := \begin{cases} +1 & \text{if } \sigma(\Delta) = \Delta \\ -1 & \text{if } \sigma(\Delta) = -\Delta \end{cases}$
σ is even if $\epsilon(\sigma) = 1$, odd of $\epsilon(\sigma) = -1$

Example. see book for example developed during above def

Proposition. *(23)*
the sign $\epsilon : S_n \to \{-1, 1\}$ is a homomorphism where $\{-1, 1\}$ is multiplicative version of Z_2

Proof. book

Example. let $n = 4$, $\sigma = (1\ 2\ 3\ 4)$, and $\tau = (4\ 2\ 3)$ see book

Definition. the alternating group fo degree n, A_n, is the kernel of ϵ, ie the set of even permutations

Claim.
- $|A_n| = \frac{1}{2} |S_n|$
  pf: 1st homomorphism thm $\Rightarrow S_n/A_n \cong \epsilon(S_n) = \{-1, 1\}$
  so $|A_n| = \frac{1}{2} |S_n|$
- note: the non-identity coset, $S_n - A_n$ is the set of all odd permutations
- sign of product of transpositions follow:
  (even)(even)=(odd)(odd)=(even)
  (even)(odd)=(odd)(even)=(odd)
  ie the $\mathbb{Z}/2\mathbb{Z}$ laws
- $\epsilon(\sigma) := \begin{cases} +1 & \text{if } \sigma \text{ is the product of even \# transpo} \\ -1 & \text{if ... odd ...} \end{cases}$
  note: doesnt matter how we write σ as product of transpositions
  pf: $\sigma = \tau_1 \tau_2 ... \tau_k$
  $\epsilon(\sigma) = \epsilon(\tau_1)\epsilon(\tau_2)...\epsilon(\tau_k)$

  $\epsilon(\tau_i) = -1$ for $i = 1, 2, ..., k$
  thus $\epsilon(\sigma) = (-1)^k$
- any m-cycle is odd iff m is even
  pf: m-cycle can be written as $m - 1$ transpositions

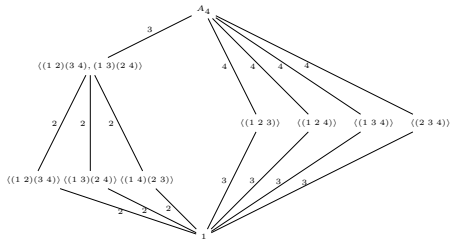
Proposition. *(25)*
$\sigma \in S_n$ is odd
$\Leftrightarrow$ its cycle decomposition has an odd number of cycles of even length

Proof. cycle decomposition $\sigma = \alpha_1 \alpha_2 ... \alpha_n$
$\epsilon(\sigma) = \epsilon(\alpha_1)\epsilon(\alpha_2)...\epsilon(\alpha_n)$
apply recent results

Example.
- $\sigma = (...$see book
  has 3 cycles of even length so $\epsilon(\sigma) = -1$
- $\tau = (...$see book
  has 2 cycles of even length so $\epsilon(\tau) = 1$

Claim.
- parity of order is different from evenness/oddness of permutation:
  - σ odd order $\Rightarrow$ even permutation
    pf: odd order $\Rightarrow$ all cycles in cycle decomposition have odd length $\Rightarrow$ even (in this case 0) number of cycles of even length
  - $|\sigma|$ even $\Rightarrow$ can be either even or odd permutation
    pf: eg (1 2) odd and (1 2)(3 4) is even, and both have order 2
- A_n is a non-abelian simple group $\forall n \geq 5$
  pf: next chapter

Example. A_1 and A_2 are both the trivial group
$|A_3| = 3$ so $A_3 = \langle (1\ 2\ 3) \rangle \cong Z_3$
$|A_4| = 12$ and A_4 is isomorphic to the group of symmetries of a regular tetrahedron (ex7)
lattice of A_4 (note: planar graph):



4. GROUP ACTIONS

Remark. this chapter:
- group G acting on set A
- recurring theme in Math: when one object acts on another, much info can be obtained on both
  this theme will recur in modules, vector spaces, cononical forms of matrices, and Galois thy
- when set A has more structure (eg another group, a vector space), more info on G becomes available
- will prove Sylow's thms and resulting classifications

4.1. GROUP ACTIONS AND PERMUTATION REPRESENTATIONS.

Remark. this section:
- basic thy of group actions
- examples with S_n acting on $\{1, 2, ..., n\}$
- prove that every $\sigma \in S_n$ has unique cycle decomposition

section 2,3: 2 specific groups actions, important results

Remark. recall §1.7,2.2
- $\forall g \in G$, define $\sigma_g : A \to A$, $\sigma_g : a \mapsto g \cdot a$ is a permutation of A
- the permutation representation of a given action is homomorphism $\phi : G \to S_A$, $\phi(g) = \sigma_g$
- the kernel of the action is $\{g \in G | g \cdot a = a \forall a \in A\}$
- the stabilizer of $a \in A$ in G is $G_a = \{g \in G | g \cdot a = a\}$
- a faithful action means its kernel is identity
- the kernel of an action equals the kernel of its permutation representation
- 2 elements of G induce same permutation on A
  $\Leftrightarrow$ they are in the same coset of the kernel
  $\Leftrightarrow$ they are in the same fiber of permutation representation ϕ
  in particular, an action of G on A can be viewed as a faithful action of $G/\ker\phi$ on A
- $G_a \leq G$
  $\ker\phi = \cap_{a \in A} G_a$ ie kernel contained in every stabilizer since kernel stabilizes every point

Example.
- S_n acts on $\{1, 2, ..., n\}$ by $\sigma \cdot i = \sigma(i)$ $\forall i \in \{1, 2, ..., n\}$
  permutation representation: $\phi : S_n \to S_n$ identity map
  this action is faithful
  stabilizer G_i (the subgroup of permutations that fix i) is isomorphic to S_{n-1} (§3.2ex15)
- D_8 acts on A =set of four vertices of a square
  ntn: label vertices 1,2,3,4 clockwise (§1.2)
  let r =rotation by $\frac{\pi}{2}$ clockwise
  let s =reflection about line passting through vertices $1, 3$
  ie $\sigma_r = (1\ 2\ 3\ 4)$ and $\sigma_s = (2\ 4)$
  note: permutation repr is homomorphism, so $\sigma_{sr} = \sigma_s\sigma_r = (1\ 4)(2\ 3)$
  action of D_8 on square is faithful since only identity fixes all four vertices
  the stabilizer G_a of vertex a is the subgroup of D_8 of order 2 generated by line of symmetry through a
  eg $G_1 = \langle s \rangle$
- keep labeling of vertices of previous example
  let $A = \{\{1, 3\}, \{2, 4\}\}$
  D_8 acts on A since each symmetry sends a pair of opposite vertices to a pair of opposite vertices
  σ_r interchanges pairs $\{1, 3\}$ $\{2, 4\}$
  σ_s =identity permutation
  this action of D_8 is not faithful: its kernel is $\langle s, r^2 \rangle$
  $\forall a \in A$, G_a =the kernel of the action
- D_8 does not act on $\{\{1, 2\}, \{3, 4\}\}$ since $r \cdot \{1, 2\} = \{2, 3\} \notin A$

Proposition. *(1)*
let group G and nonempty set A
$\exists$ bijection between actions G on A and homomprhisms of G into S_A

Proof. paragraph before prop

Definition. (rephrase permutation representation)

- a permutation representation of group G is any homomorphism of G into S_A for some nonempty A
- an action G on A affords ("indices") the associated permutation representation of G

Remark. intuition for finite:
permutation repr is analogous to the mx repr of a linear transformation
fixing labels on elements of A allows us to consider our permutations as elements of S_n
just like fixing basis allows viewing a linear transformation as a mx

Proposition. *(2)(combinatorial result, will be useful in following sections)*
let group G act on nonempty set A
the relation on A: $a \sim b$ iff $a = g \cdot b$ for some $g \in G$ is an equivalence reln (note: partitions A)
furthermore, $\forall a \in A$, the size of the equiv class containing a is $|G : G_a|$
ie the index of the stabilizer of a

Proof. book

ORBITS

Definition. let group G act on nonempty A

- the orbit of G containing $a \in A$ is the equivalence class $\{g \cdot a | g \in G\}$
  (note: orbits partition A)
- the action is transitive means $\exists!$ orbit ie $\forall a, b \in A$, $\exists g \in G$ st $a = g \cdot b$

Example. Let group G act on set A
- let the action be trivial
  then $G_a = G$ $\forall a \in A$
  orbits are the elements of A
  this action is transitive $\Leftrightarrow |A| = 1$
- S_n acts transitively on $\{1, 2, ..., n\}$ in its usual action of permutations
  G_a has index $n = |A|$ in S_n
- clm: every $H \leq G$ also acts on A
  clm: if G acts transitively on A then $H < G$ need not act transitively
  pf: eg $\langle (1\ 2), (3\ 4) \rangle \leq S_4$ has orbits $\{1, 2\}$ and $\{3, 4\}$ and no element sends 2 to 3
  clm: for any cyclic subgroup $\langle \sigma \rangle \leq S_n$, the orbits of $\langle \sigma \rangle$ are the sets of numbers in individual cycles of the cycle decomposition of $\langle \sigma \rangle$
  eg the orbits of $\langle (1\ 2)(3\ 4\ 5) \rangle$ are $\{1, 2\}$ and $\{3, 4, 5\}$
  pf: discussion below
- D_8 acts transitively on the four vertices of a square
  the stabilizer of any vertex is the subgroup of order 2 (and index 4) generated by the reflection about the line of symmetry passing through that point
- D_8 acts transitively on the set of two pairs of opposite vertices
  the stabilizer of any point is $\langle s, r^2 \rangle$ which is of index 2

CYCLE DECOMPOSIITONS

Claim. every element of S_n has the unique cycle decomposition in §1.3

Definition. a permutation group is a subgroup of a symmetric group

Remark. ntn: for $G \leq S_n$, the orbits on G refer to its orbits on $\{1, 2, ..., n\}$
ntn: the orbits of $\sigma \in S_n$ means the orbits of $\langle \sigma \rangle$ (ie the sets of numbers comprising its cycle decomp)

4.2. GROUPS ACTING ON THEMSELVES BY LEFT MULTIPLICATION - CAYLEY'S THM.

Definition. group G acting on itself by left multiplication means $A = G$ and $g \cdot a = ga$

Remark.
- this satisfies axioms of group action from §1.7
- ntn: additive written $g \cdot a = g + a$ and called "left translation"
- if G finite order n, then label elements of G with integers 1,2,...,n
  this allows describing this action's induced permutation representation wrt permuted labels
  ie $\forall g \in G$, $\sigma_g(i) = j$ iff $gg_i = g_j$
  note: different labelling gives different description of σ_g (see exercises)

Example. consider V_4
label elements $1, a, b, c$ with 1,2,3,4
consider action of left multiplication by group element a:
$a \cdot 1 = a1 = a$ so $\sigma_a(1) = 2$
$a \cdot a = aa = 1$ so $\sigma_a(2) = 1$
$a \cdot b = ab = c$ so $\sigma_a(3) = 3$
$a \cdot c = ac = b$ so $\sigma_a(4) = 4$
so $\sigma_a = (1\ 2)(3\ 4)$
the permutation representation $G \to S_4$ is
$a \mapsto \sigma_a = (1\ 2)(3\ 4)$
$b \mapsto \sigma_b = (1\ 3)(2\ 4)$
$c \mapsto \sigma_c = (1\ 4)(2\ 3)$

Claim.
- action of group on itself by left multiplication is always transitive and faithful
- the stabilizer of any point is identity subgroup

Definition. group G acting on the left cosets of $H \leq G$ by left multiplication:
let $H \leq G$ and A=set of all left cosets of H in G
define action of G on A: $g \cdot aH = gaH$ $\forall g \in G, aH \in H$ where gaH is the left coset with representative ga
note: this satisfies the two axioms of group action

Remark.
- let H=identity subgroup of G
  then $aH = \{a\}$ and this is same as action of G on itself by left multiplication

- to get induced permutation representation:
  label left cosets $a_1H, a_2H, ..., a_mH$
  $\forall g \in G$ define permutation $\sigma_g(i) = j$ iff $ga_iH = a_jH$

Example. consider $H = \langle s \rangle < D_8$
label the left cosets $1H, rH, r^2H, r^3H$ with integers $1, 2, 3, 4$
compute permutation σ_s induced by left multiplication of s on the left coset of H:
$s \cdot 1H = sH = 1H$ so $\sigma_s(1) = 1$
$s \cdot rH = srH = r^3H$ so $\sigma_s(2) = 4$
$s \cdot r^2H = sr^2H = r^2H$ so $\sigma_s(3) = 3$
$s \cdot r^3H = sr^3H = rH$ so $\sigma_s(4) = 2$
thus $\sigma_s = (2\ 4)$
similarly, $\sigma_r = (1\ 2\ 3\ 4)$
note: permutation representation is a homomorphism and cince we know generators r, s, we can compute any compbination eg $\sigma_{sr^2} = \sigma_s\sigma_{r^2}$

Theorem. *(3)*
let $H \leq G$ and A-set of left-cosets of H in G
let π_H be the associated permutation representation
then
1) G acts transitively on A
2) stabilizer G_{1H} is the subgroup H
3) kernel of the action $\ker\pi_H = \cap_{x \in G} xHx^{-1}$ and $\ker\pi_H$ is the largest normal subgroup of G contained in H

Proof. book

Corollary. *(4)(Cayley's thm)*
every group is isomorphic to a subgroup of some symmetric group
ie every group is isomorphic to a permutation group

eg if group G has order n then G is isomorphic to a subgroup of S_n

Example. $V_4 \cong \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle \leq S_4$

Definition. the left regular representation of group is the permutation representation afforded by left multiplication on elements of G (ie on cosets of $H = 1$)

Remark.
- so group thy is just studying subgroups of symmetric groups
  this is how groups were first studied
- but this is not computationally or theoretically practical since S_n is large compared to n
- also the modern approach does not require considering groups as subgroups of some symmetric group
  sour our groups are "coordinate-free"

Corollary. *(5) (generalize result on normality of subgroups of index 2)*
let finite group G of order n
if p is the smallest prime dividing $|G|$
then any subgroup of index p is normal

Proof. book

4.3. GROUPS ACTING ON THEMSELVES BY CONJUGATION – THE CLASS EQUATION.

Definition.
- a group G acting on itself ($A = G$) by conjugation means $g \cdot a = gag^{-1}\ \forall g \in G, a \in G$ where gag^{-1} is operation in G
  note: satisfies 2 axioms of group action since $g_1 \cdot (g_2 \cdot a) = g_1(g_2 a g_2^{-1})g_1^{-1} = (g_1g_2)a(g_1g_2)^{-1} = (g_1g_2)\cdot a$
  and $1 \cdot a = 1a1^{-1} = a$
- conjugate elements $a, b \in G$ means $\exists g \in G$ st $b = gag^{-1}$
  ie a, b are in same orbit of G acting on itself by conjugation
- the conjugacy classes of G are the orbits of G acting on itself by conjugation
  note: they partition G

Example.
- clm: if G abelian, then the action of G on itself by conjugation is the trivial action $g \cdot a = a$ and the conjugacy class of each $a \in A$ is $\{a\}$
- clm: if $|G| > 1$, G does not act transitively on itself by conjugation
  pf: $\{1\}$ is always a conjugacy class ie an orbit
  clm: more generally, singleton $\{a\}$ is a conjugacy class
  iff $gag^{-1} = a\ \forall g \in G$
  iff a is in the center of G
- for S_3
  conjugacy classes: $\{1\}$, $\{(1\ 2), (1\ 3)\}, (2\ 3)\}$, $\{(1\ 2\ 3), (1\ 3\ 2)\}$
  this can be computed directly, but some faster techniques for computing conjugacy classes follow, particulary in symmetric groups

Definition.
- (extend above action to be on power set of G, not just singletons)
  group G acts on power set $\mathcal{P}(G)$ with $g \cdot S = gSg^{-1} = \{gsg^{-1} | s \in S\}\ \forall g \in G, S \in \mathcal{P}(G)$
- conjugate subsets $S, T \subseteq G$ means $\exists g \in G$ st $T = gSg^{-1}$
  (iff they are in same orbit of this action)

Proposition. *(6) (computing order of a conjugacy class)*
the number of conjugates of subset S in group G is $|G : N_G(S)|$
ie the index of the normalizer of S
in particular, the number of conjugates of $\{s\}$ is $|G : C_G(s)|$
ie the index of the centralizer of s

Proof. apply prop to G_S which equals $N_G(S)$
second assertion since $N_G(\{s\}) = C_G(s)$

Theorem. *(7) (the class eqn)*
let G finite group
let $g_1, g_2, ..., g_r$ representatives of distinct conjugacy classes not contained in center $Z(G)$
then $|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$

Proof. intuition: conjugacy classes partition G, so add their sizes
see book for full argument

Claim. each summand on rhs divides $|G|$ (since indices of subgroup) so this restricts their possible values
pf: ex6

Example.
- for abelian groups, the class eqn provides no invo since all conjugacy classes have size 1
- when computing conjugacy classes of $\langle g\rangle \leq C_G(s)$
  - eg Q_8
    $\langle i\rangle \leq C_{Q_8}(i) \leq Q_8$
    so $C_{Q_8}(i) = \langle i\rangle$ since $i \notin Z(Q_8)$ and $|Q_8 : \langle i\rangle| = 2$
    thus i has exactly 2 conjugates: i and $-i = kik^{-1}$
    similarly, the other conjugacy classes are $\{1\}$, $\{-1\}$, $\{-i, i\}$, $\{-j, j\}$, $\{-k, k\}$ where the first two form $Z(Q_8)$
    class eqn: $|Q_8| = 2 + 2 + 2 + 2$
- D_8
  note: the three subgroups of index 2 are abelian so $x \notin Z(D_8) \Rightarrow \left|C_{D_8}(x)\right| = 4$
  conjugacy classes of D_8: $\{1\}$, $\{r^2\}$, $\{r, r^3\}$, $\{s, sr^2\}$, $\{sr, sr^3\}$ where the first two form $Z(D_8)$
  class eqn: $|D_8| = 2 + 2 + 2 + 2$

Remark. next: two important consequences of class eqn

Theorem. *(8)*
if p prime and P a group of prime power order (p^α, $\alpha \geq 1$)
then P has nontrivial center ie $Z(P) \neq 1$
note: see ch6 for more groups of prime power order

Proof. book

Corollary. *(9)*
if $|P| = p^2$ for some prime p
then P is abelian
more precicely, P is isomorphic to either Z_{p^2} or $Z_p \times Z_p$

Proof. short

CONJUGACY CLASSES IN S_n

Remark. conjugacy in S_n is analogous to in $GL_n(F)$, change of basis $A \mapsto PAP^{-1}$

Proposition. *(10)*
let $\sigma\tau \in S_n$ st cycle decompositin $\sigma = (a_1\ a_2 ... a_{k_1})(b_1\ b_2 ... b_{k_2})...$
then $\tau\sigma\tau^{-1}$ has cycle decomposition $(\tau(a_1)\ \tau(a_2)...\tau(a_{k_1}))(\tau(b_1)\ \tau(b_2)...\tau(n_{k_2}))...$

Proof. note: $\sigma(i) = j \Rightarrow \tau\sigma\tau^{-1}(\tau(i)) = \tau(j)$

Example. let $\sigma = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9)$, $\tau = (1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$
then $\tau\sigma\tau^{-1} = (3\ 4)(5\ 6\ 7)(8\ 1\ 2\ 9)$

Definition.
- let $\sigma \in S_n$ be disjoint product of cycles of lengths $n_1, n_2, ..., n_r$ with $n_1 \leq n_2 \leq ... \leq n_r$ (including 1-cycles)
  the cycle type of $\sigma \in S_n$ are $n_1, n_2, ..., n_r$
- a partition of $n \in \mathbb{Z}^+$ is any nondecreasing sequence of positive integers whose sum is n

Claim. the cycle type of a permutation is unique
pf: see results from previous section
eg an m-cycle of S_n has cycle type 1,1,...,1,m (with $n - m$ ones)

Proposition. *(11)*
- *two elements of S_n are conjugate in S_n iff they have same cycle type*
- *# of conjugacy classes of S_n = # of partitions of n*

Example.
- let $\sigma_1 = (1)(3\ 5)(8\ 9)(2\ 4\ 7\ 6)$
  let $\sigma_2 = (3)(4\ 7)(8\ 1)(5\ 2\ 6\ 9)$
  let $\tau = (1\ 3\ 4\ 2\ 5\ 7\ 6\ 9)(8)$
  then $\tau\sigma_1\tau^{-1} = \sigma_2$
- let σ_1 above, σ_2 with interchanged (4 7) and (8 1)
  define $\tau = (1\ 3\ 8\ 4\ 2\ 5)(6\ 9\ 7)$
  then $\tau\sigma_1\tau^{-1} = \sigma_2$
  so there are many elments conjugating σ_1 into σ_2
- correspondence between partitions and conjugacy classes:

paritions of $n = 5$	conjugacy class representation (excluding 1-cycles)
1,1,1,1,1	1
1,1,1,2	(1 2)
1,1,3	(1 2 3)
1,4	(1 2 3 4)
5	(1 2 3 4 5)
1,2,2	(1 2)(3 4)
2,3	(1 2)(3 4 5)

Claim.
- if σ is an m-cycle of S_n
  then $C_{S_n}(\sigma) = \{\sigma^i\tau | 0 \leq i \leq m-1,\ \tau \in S_{n-1}\}$
  where S_{n-m} is the subgroup of S_n which fixes all integers appearing in σ, equals identity if $m = n$ or $m = n - 1$
  - pf: prop 6 $\Rightarrow$ # conjugates of m-cycles of σ = index of the centralizer of σ
    ie $\frac{n(n-1)\cdots(n-m+1)}{m} = \frac{S_n}{C_{S_n}(\sigma)}$
    plug $S_n = n!$ to get $|C_{S_n}| = m \cdot (n-m)!$
    σ commutes with any permutation in S_n which fixes integers in σ
    and there are $n - m$ such permutations
    the product of these two accounts for $m \cdot (n - m)!$ elements commuting with σ
    this is the full centralizer of σ in S_n
  - eg the centralizer of $\sigma = (1\ 2\ 5)$ in S_7 is the subgroup $\{(1\ 3\ 5)^i\tau | i = 0, 1, 2,\ \tau$ fixes $1, 3, 5\}$ and where $\tau \in S_A$ where $A = \{2, 4, 6, 7\}$
    so there are 4! choices for τ
    so the centralizer has order $3 \cdot 4! = 72$
- if $H \trianglelefteq G$
  then for every conjugacy class K of G, either $K \subseteq H$ or $K \cap H = \emptyset$
  ie normal subgroup of G is the union of conjugacy classes of G
  pf: $x \in K \cap H \Rightarrow gxg^{-1} \in gHg^{-1}\ \forall g \in G$
  if normal $\Rightarrow gHg^{-1} = H$ so H contains all conjugates of x ie $K \subseteq H$

Theorem. *A_5 is a sunple group*

Proof. long combinatorial argument

RIGHT GROUP ACTIONS

Remark. above group actions are "right group actions"

Definition. a right group action of group G on nonempty set A is map $A \times G \to A$ denoted $a \cdot g$, st
1) $(a \cdot g_1) \cdot g_2 = a \cdot (g_1 g_2)$ $\forall a \in A$, $g_1, g_2 \in G$
2) $a \cdot 1 = a$ $\forall a \in A$

Remark. ntn:

- in a lot of literature, conjugation is written $a^g = g^{-1}ag$ $\forall a, g \in G$
  right group action since $\forall a, g_1, g_2 \in G$
  $(a^{g_1})^{g_2} = g_2^{-1}(g_1^{-1}ag_1)g_2 = (g_1g_2)^{-1}a(g_1g_2) = a^{g_1 g_2}$
  and $a^1 = 1^{-1}a1 = a$
  this looks like "laws of exponentiation" but should not be confused with exponents a^n, $n \in \mathbb{Z}$
- also, $S^g = g^{-1}Sg$

Claim.

- (corresponding group actions)
  given left group action $G \times A \to A$
  then map $A \times G \to A$, $a \cdot g := g^{-1} \cdot a$ is a right group action
  ie g acts on left in same way as g^{-1} acts on right
- the relation conjugacy is same for left and right corresponding actions
  ie 2 elements or subsets of a group are "left conjugate" iff they are "right conjugate"
  pf: the left conjugate of a by g = the right conjugate of a by g^{-1}
- recall left multiplication on the left cosets of a subgroup is a left group action with permutation representation is homomorphism $\phi : G \to S_n$
  similar for right, right, right, and uses postfix ntn for permutations and permutation representation

Remark. should be comfortable with both left and right actions since some actions naturally occur on certain side