1. GROUPS

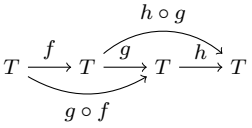
THE DEFINITION OF A GROUP.

Remark. We want to perform operations on sets which are not numbers. If there is symmetry, we might have a group.

Definition. *group, abelian group*

- A *group* is (set G, law of composition written ab $\forall a, b \in G$) s.t.
  (1) closed under the law of composition
  $a, b \in G \Rightarrow ab, ba \in G$
  (2) associative
  $(ab)c = a(bc) = abc$
  (3) identity $e = 1_G \in G$
  $ae = ea = a$
  note: unique since $e = ee' = e'$
  (4) inverses $a^{-1} \in G$
  $a^{-1}a = aa^{-1} = e$
  note: unique since $aa^{-1} = 1 = aa'^{-1}$
  note: opposite order $(ab)^{-1} = b^{-1}a^{-1}$
- An *abelian group* also commutes, $ab = ba$

Example. $\mathrm{Sym}(T)$ *("Symmetries ("permutations") of set T", "Automorphism group")*
$\mathrm{Sym}(T) = (\{\text{all bijections } T \mapsto T\}, \circ)$
$\mathrm{Sym}(T)$ is a group since, for $f, g, h \in \mathrm{Sym}(T)$,
(1) composed bijections is a bijection
$g \circ f(t) = g(f(t)) \in \mathrm{Sym}(T)$
(2) bijections are associative
$(h \circ g) \circ f(t) = h \circ (g \circ f)(t) = h(g(f(t)))$



(3) identity map $e(t) = t$ $\forall t \in T$
$e \circ f(t) = f \circ e(t) = f(t)$
(4) inverse
$f \circ f^{-1}(t) = f^{-1} \circ f(t) = e(t)$

Remark. $\mathrm{Sym}(T)$ is the most general group, all other groups arise by putting extra conditions which preserve structure of the set ie structure preserving bijections

Example.
abelian

- $\mathbb{Z}^+ = (\mathbb{Z}, +)$ with $e = 0$, $a^{-1} = -a$
  note: preserves symmetry of geometric object using shift
  picture: directed graph, each arrow pointing right
- $\mathbb{R}^+ = (\mathbb{R}, +)$ with $e = 0$, $a^{-1} = -a$
- $\mathbb{R}^\times = (\mathbb{R}\backslash\{0\}, \times)$ with $e = 1$, $a^{-1} = \frac{1}{a}$
- $\mathbb{C}^+, \mathbb{C}^\times$ similarly
- (Vector space, elementwise +) with $e = \mathbf{0}$, $\mathbf{a}^{-1} = -\mathbf{a}$
- $M_{n\times n}(\mathbb{R})$ =($\{n \times n$ mxs$\}$, elementwise +) with e =zero mx, $A^{-1} = -A$

non-abelian

- *general linear group of dimension n*
  $\mathrm{GL}_n(\mathbb{R})$ =($\{$all invertable $n \times n$ mxs$\}$, mx multiplication)
  Preserves linearity, $\mathrm{GL}_n(\mathbb{R}) \subset \mathrm{Sym}(\mathbb{R}^n)$
  Group since
  (1) closed under mx multiplication (since $\det(AB) = \det(A)\det(B) \neq 0$)
  (2) mx multiplication is associative
  (3) identity I
  (4) inverse by definition
  Not abelian since mx multiplicaiton not always commutative.
- $\mathrm{GL}_n(\mathbb{C})$, $\mathrm{GL}_n(\mathbb{Q})$ similarly
- (rotations and flips of a square, composition)

Remark. Is there a group of size $n \in \mathbb{N}$?

Definition. *order ("cardinality"), finite group*

- the *order* $|G|$ of group G is the number of elements
- a *finite group* has finite order

Example. *symmetric ("permutation") group on n letters*

- $S_n = \mathrm{Sym}\{1, 2, \cdots, n\}$ is the set of permutations on $\{1, 2, \cdots, n\}$
  note: order $|S_n| = n!$ (i.e. n ways to choose first element, $n-1$ ways to choose second, etc)
- $S_1 = \{e\}$ is the smallest possible group
- $S_2 = \{e, \tau\}$ where τ is the transposition (exchanges two elements, leaves others alone)
  multiplication table

	e	τ
e	e	τ
τ	τ	e

  abelian since mult table is symmetric about diagonal
- $S_3 = \{e, \tau = (2,1,3), \tau' = (1,3,2), \tau'' = (3,2,1), \sigma = (3,1,2), \sigma' = (2,3,1)\}$
  $= \{e, \tau, \sigma^2\tau, \sigma\tau, \sigma, \sigma^2\}$
  note: smallest non-abelian group

Remark. Will see that finite abelian groups are well understood
preview: every finite abelian group decomposes into pieces that look like $\mathbb{Z}^+$ and quotient $\mathbb{Z}/n\mathbb{Z}$ for some n

SUBGROUPS; CYCLIC SUBGROUPS.

Definition. *subgroups, proper subgroup*

- A *subgroup* $H \subset G$ is a group induced with same law of composition
  i.e. coarse subset which behaves a group
- a *proper subgroup* is a subgroup which is not the trivial $\{e\}$ or G

Example.

- every subgroup of $\mathbb{Z}^+$ is of the form $b\mathbb{Z}$ for some $b \in \mathbb{Z}$
  ie all multiples of b
  preview: quotient of $\mathbb{Z}^+$, $\mathbb{Z}/n\mathbb{Z} \subset \mathbb{Z}$, ie integers modulo n, is _not_ a subgroup of $\mathbb{Z}^+$
- a subgroup of $\mathbb{C}^\times$ is the points on the unit circle in $\mathbb{C}$
- a subgroup of $\mathrm{GL}_2(\mathbb{R})$ is the group of invertable 2×2 upper triangle mxs
- for $k \leq n$, a subgroup of S_n is S_k by fixing $\{k+1, k+2, \cdots, n\}$
  note: $k \geq 3 \Rightarrow$ not abelian
- a subgroup of the symmetries of a regular n-gon is the rotations

Definition. *cyclic subgroup generated by element of group, order of cyclic group, subgroup generated by subset of group*

- the *cyclic subgroup generated by* $x \in G$ is $< x >= \{x^n : n \in \mathbb{Z}\}$ (using multiplicative notation)
  note: $< x >$ is the smallest subgroup which contains x
- the *order of cyclic group* is the smallest $n \in \mathbb{N}$ s.t. $x^n = 1$. Can be infinite order.
- *subgroup generated by* $U \subset G$ is $\{g \in G :$ g = product of elements of U and their inverses$\}$

Example.
cyclic

- $m \subset \mathbb{Z}^+$ generates cyclic subgroup $m\mathbb{Z}$ with infinite order
- $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} \subset \mathrm{GL}_n(\mathbb{R})$ generates a cyclic subgroup of order 6
- $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \subset \mathrm{GL}_n(\mathbb{R})$ generates a cyclic subgroup with infinite order since $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$
- $\mathrm{GL}_n(\mathbb{R})$ is generated by the three types of elementary mxs
- S_3 is generated by $U = \{\tau, \sigma\}$ (see above)

not cyclic

- Klein four group $V = \left\{ \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix} \right\}$
  is generated by any two non-identity elements
  note: its the simplest non-cyclic group
- quaterion group (8 matrices)
  $\left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \right.$
  is generated by $\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

ISOMORPHISM; AUTOMORPHISM; CONJUGATE.

Definition. *isomorphism, isomorphism class, automorphism*

- An *isomorphism* is a bijective map $\phi : G \to G'$ satisfying $\phi(ab) = \phi(a)\phi(b)$ $\forall a, b \in G$
  ie G and G' have same properties, group structure, multiplication table
  note: correspondence with identities ($\phi(1_G) = 1_{G'}$) and inverses ($\phi(a^{-1}) = \phi(a)^{-1}$)
- groups in an *isomorphism class* are *isomorphic* to each other
  notation: $G \approx G'$

Example.

- $\phi : \mathbb{Z}^+ \to \{\cdots, a^{-2}, a^{-1}, 1, a, a^2, \ldots\}$, $\phi(n) = a^n$ is isomorphism
  note: additive in domain and multiplicative in range, $\phi(m+n) = a^{m+n} = a^m a^n$
- $\left\{ \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} : x \in \mathbb{R} \right\}$ and $\mathbb{R}^+$ isomorphic since $\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+y \\ & 1 \end{bmatrix}$
- two cyclic subgroups of same order are isomorphic
- S_n and the group of $n \times n$ permutation mxs are isomorphic
- rotations $\{\rho, \rho^2, \rho^3, \rho^4 = e\}$ of square and $\mathbb{Z}/4\mathbb{Z}$ isomorphic using $\phi(\rho^k) = k \mod n$ have isomorphism $\phi(\rho^m\rho^n) = \phi(\rho^{m+n}) = (m+n) \mod 4 = (m \mod 4)(n \mod 4)$

Definition. *automorphism*

- An *automorphism* is an isomorphism from a group to itself

Example.

- the identity map is an automorphism
- a cyclic group of order 3, $\{1, x, x^2\}$, and the transposition which exchanges x and x^2 are automorphic since x^2 also has order 3

Definition. *conjugate, conjugation of group by element*

- the *conjugate* of a by b is bab^{-1}
- $a, a' \in G$ are *conjugate* means $a' = bab^{-1}$ for some $b \in G$
- *conjugation of group G by $b \in G$* is $\phi : G \to G$, $\phi(a) = bab^{-1}$
  note: automorphism since $\phi(xy) = bxyb^{-1} = bxb^{-1}byb^{-1} = \phi(x)\phi(y)$ and inverse is conjugation by b^{-1}.
  note: a and bab^{-1} have same order since automophism

HOMOMORPHISM.

Definition. *homomorphism*
A *homomorphism* is a map $\phi : G \to G'$ satisfying $\phi(ab) = \phi(a)\phi(b)\ \forall a, b \in G$
ie like isomorphism but need not biject
ie preserves group structure at least in some coarse way
note: homomorphism carries identity to identity ($\phi(1_G) = 1_{G'}$) and inverses to inverses ($\phi(a^{-1}) = \phi(a)^{-1}$)

Example.

- $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$
  since $\det(AB) = \det(A)\det(B)$
- sign of a permutation, $\mathrm{sign} : S_n \to \{\pm 1\}$
- $\phi : \mathbb{Z}^+ \to G$, $\phi(n) = a^n$ where $a \in G$
- inclusion map $i : H \to G$, $i(x) = x$ where H is a subgroup of G

Definition. *image of homomorphism, normal subgroup, kernel of homomorphism, center of group*

- the *image* of a homomorphism $\phi : G \to G'$ is $\phi(G) = \{x \in G' : x = \phi(a) \text{ for some } a \in G\}$
  note: $\phi(G) \subseteq G'$ is a subgroup
- N is a *normal subgroup* of G means $\forall a \in N, \forall b \in G$, conjugate $bab^{-1} \in N$
  ie closed under conjugation by all $b \in G$
- the kernel of homomorphism $\phi : G \to G'$ is $\ker\phi = \phi^{-1}(1_{G'}) = \{a \in G : \phi(a) = 1_{G'}\}$
  note: kernel is subgroup of G since $a, b \in \ker\phi \Rightarrow \phi(ab) = \phi(a)\phi(b) = 1$
  note: kernel is normal subgroup since $\phi(bab^{-1}) = \phi(b)1\phi(b)^{-1} = 1$
- the *center* of group G is $Z(G) = \{z \in G : zx = xz\ \forall x \in G\}$
  ie subgroup which comutates with G
  note: center is a normal subgroup since $bab^{-1} = bb^{-1}a = a\ \forall b \in G$

Example.

- Special linear group of dimention n
  $\mathrm{SL}_n(\mathbb{R}) = \{\text{real } n \times n \text{ mxs:} \det A = 1\}$
  is the kernel of the determinant homomorphism $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$
- the *alternating group* $A_n = \{\text{even permutations}\} \subset S_n$
  is the kernel of the sign homomorphism $\mathrm{sign} : S_n \to \{\pm 1\}$
- the kernel of $\phi : \mathbb{Z}^+ \to G$, $\phi(n) = a^n$ where $a \in G$, is $\{n : a^n = 1\} \subset \mathbb{Z}^+$
- any subgroup of an abelian group is normal since $bab^{-1} = a$
- the center of $\mathrm{GL}_n(\mathbb{R})$ is the group of scalar matrices cI

EQUIVALENCE RELATIONS AND PARTITIONS.

Definition. *partition, equivalence relation, equivalence classes, set of equivalence classes*

- a *partition* P of set S is a subdivision of S into nonoverlapping subsets
- an *equivalence relation* $\sim$ on S is a binary relation with properties: reflexive, symmetric, transitive
- *equivalence class* is a subsets of S with equivalent elements, forms a partition on S
- *set of equivalence classes*, $\bar{S}$, is the set whose elements are equivalence classes, each denoted by $\bar{a}$
  notation: $\bar{a} = \bar{b}$ means $a \sim b$
  intuition: $\bar{a}$ is a pile of elements equivalent to $a \in S$

Example.

- partition of $\mathbb{Z}$ with equivalence classes even integers and odd integers, $\bar{\mathbb{Z}} = \{\bar{0}, \bar{1}\}$
- congruence of triangles is an equivalence relation on the set of triangles in the plane

Definition. *equivalence relation determined by a map, fiber*

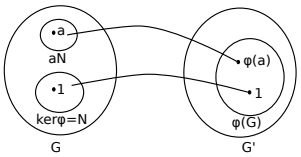
- An *equivalence relation determined by map* $\phi : S \to T$ is $a \sim b \Leftrightarrow \phi(a) = \phi(b)$
- a *fiber* of ϕ is $\phi^{-1}(t) = \{s \in S : \phi(s) = t\}$ for any $t \in \phi(S)$
  note: a fiber is an equivalence class
  note: $\ker\phi$ is the fiber of 1_T

Definition. *congruence relation, congruent, congruence classes*

- a *congruence relation* is the equivalence relation determined by homomorphism $\phi : G \to G'$
  notation: $\equiv$ instead of $\sim$
- a, b *congruent wrt* ϕ means $\phi(a) = \phi(b)$
- *congruence classes*

Definition. *coset*

- Let homomorphism $\phi : G \to G'$.
  The *coset* of $a \in G$ wrt $\ker\phi = N$ is $aN = \{g \in G : g = an \text{ for some } n \in N\}$
  ie the set of all $g \in G$ which are congruent to a
  note: $\phi(aN) = \phi(a)$ since $\phi(an) = \phi(a)$
  note: coset aN is a fiber of ϕ, makes up a congruence class



Example.

- absolute value map $\phi : \mathbb{C}^\times \to \mathbb{R}^\times$, $\phi(a) = |a|$
  equivalence relation $|a| = |b| \Rightarrow a \equiv b$
  fibers, which are also cosets, are concentric circles around 0
- to check whether a homomorphism $\phi : G \to G'$ is an isomorphism, check injection: $\ker\phi = \{1\}$ and surjection: $\phi(G) = G'$

COSETS.

Definition. *left,right coset, cosets are equivalence classes*

- A *left coset* of $a \in G$ wrt subgroup H of G is $aH = \{ah : h \in H\}$
- cosets are equivalence classes for the congruence relation $a \equiv b \Leftrightarrow b = ah$ for some $h \in H$
  ie cosets partition the group
  note: aH is the unique coset containing a
- the *index* of H in G, $[G : H]$, is the number of left cosets of H. Can be infinite
-

Example.

- subgroup H is itself a coset since $1H = H$
- $S_3 = \{1, x, x^2, y, xy, x^2y\}$
  Let $H =< xy >= \{1, xy\}$
  the left cosets of H in G are the three sets (index 3) which partition G
  $\{1, xy\} = H = xyH$, $\{x, x^2y\} = xH = x^2yH$, $\{x^2\} = x^2H = yH$

Example.
$\mathbb{Z}/n\mathbb{Z}$
note: $\mathbb{Z}/4\mathbb{Z}$ isomorphic to square in plane with rotation elements $\{\rho, \rho^2, \rho^3, \rho^4 = e\}$ with $\phi(\rho^k) = k \mod n$ since $\phi(\rho^m\rho^n) = \phi(\rho^{m+n}) = (m+n) \mod 4 = (m \mod 4)(n \mod 4)$