General properties of groups and mappings

1 Equivalence Relations as devices for partitioning sets

We often find ourselves examining sets and partitioning them into subsets, ie, breaking them up into disjoint subsets that exhaust the original set

Example: $P = \{$the set of all people in Iceland$\}$

$= \{$male Icelanders$\} \cup \{$female Icelanders$\}$

disjoint — no common elements

assume people only live in one house

Example: $Q = \{$the set of all people living on Iowa Street$\}$

$= \{$those living at 310$\} \cup \{$-- at 312$\} \cup \cdots$

The decomposition into non-overlapping subsets is commonly accomplished by an <u>equivalence relation</u>, ie, a rule that determines whether or not, for any pair of elements of the set, the pair share some specific similarity (eg are both female; live in the same house on Iowa Street).

To be an equivalence relation, and hence to be capable of providing decompositions into disjoint subsets, a rule must obey the following properties

Reflexivity; symmetry; transitivity

1/20

Reflexivity: each element a of the set A must be equivalent to itself; we write $a \sim a$

Symmetry: if $a \in A$ is equivalent to $b \in A$ (ie $a \sim b$) then b is equivalent to a (ie $b \sim a$)

Transitivity: Let a, b, c be elements of A; then if $a \sim b$ and $b \sim c$ we must have $a \sim c$

Example: Assume that all people live in exactly one house. Then "lives in the same house as" is an equivalence relation because

R: people live in the same houses as themselves
S: if I live in the same house as you then you live in the same house as me
T: if Peter lives in the same house as Paul, and Paul lives in the same house as Mary, then Peter lives in the same house as Mary.

Non-example: "is a member of the same militia as" is not an equivalence relation because one can be a member of several Militias

Thus T can fail:

Billy Bob is in the MI militia
Jimmy Ray is in the MI and KY militias
Virgil Joe is in the KY militia

$BB \sim JR$, $JR \sim VJ$ but $BB \not\sim VJ$

2 Conjugacy and Conjugacy classes

- The notion of Conjugacy applies to the elements of a group; it is an equivalence relation that determines whether pairs of elements are "similar" to one another. As such, the set of group elements is decomposed into disjoint (ie non-overlapping) subsets of equivalent elements called Conjugacy classes.

Definition - 2 elements a, b of G are said to be Conjugate to one another if there exists an element g in G such that $a = g b g^{-1}$

g may not be unique; capable g's may depend on the a and b in question; we write $a \sim b$; g is called the conjugating element

- Example: $D_3 = gp\{c, b\}$ $\quad c^3 = b^2 = (bc)^2 = e$

  - c and c^2 are conjugate

    ↗ rotate CCW by $2\pi/3$ ↖ rotate CW by $2\pi/3$

  - What g will do? b or bc or bc^2

    eg $bcb^{-1} = bcb = b(cb) = b(bc^2) = c^2$

• Is Conjugacy an equivalence relation?

R? Is there a g for which $a = gag^{-1}$?
Yes - choose (e.g.) $g = e$.
So we always have $a \sim a$ ✓

S? Does $a \sim b$ imply $b \sim a$?
Suppose $a \sim b$. Then we have a g such that $a = gbg^{-1}$.
Thus we have $b = g^{-1}ag = (g^{-1})\,a(g^{-1})^{-1}$
As $g \in G$ implies $g^{-1} \in G$ we have $b \sim a$ ✓

T? Does $a \sim b$ and $b \sim c$ imply $a \sim c$?
Suppose $a \sim b$ and $b \sim c$.
Then we have $g, h \in G$ such that $a = gbg^{-1}$
$b = hch^{-1}$
So $a = g(hch^{-1})g^{-1} = (gh)c(gh)^{-1}$
As $gh \in G$ we have $a \sim c$ ✓

- Conjugacy classes

Being an equivalence relation, conjugacy provides a decomposition of a group into disjoint subsets of "similar" elements

Called Conjugacy classes

Notation $(a) = \{ b \mid b \sim a \}$

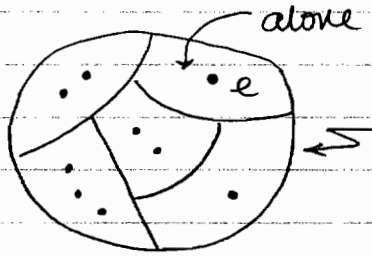
(a): Class of elements Conjugate to a

$\{ b \mid b \sim a \}$: set of elements b such that b is conjugate to a

Strategy for effecting the decomposition (ie partition):

- Pick an element of the group, a
- Scan through all $g \in G$, computing (for each g) gag^{-1} and collecting the results to form: a's conjugacy class
- Repeat for any group element that has not yet been assigned to some conjugacy class
- Stop when all elements have been assigned

Result:



G, decomposed into conjugacy classes (ie subsets of "similar" elements)

Why disjoint? Suppose that b is not in (a) and vice versa. But suppose that c is in (a) and (b). Then $c \sim a$ and $c \sim b$ which, because Conjugacy $\sim$ is an equivalence relation, implies $a \sim b \Rightarrow$ a contradiction.

Example: Any abelian group

Then $gbg^{-1} = bgg^{-1} = b$ for all $b, g \in G$
So elements b are conjugate to themselves and nothing else.

The group decomposes into conjugacy classes each containing exactly one element

Remarks – all elements of an abelian group are "distinct" from one another.

We need some noncommutativity for it to be meaningful to "transform – operate – transform back" and arrive at a different result from merely "operate".

Consider the abelian group C_n. As "flipping" (ie π rotations out of the plane) is not allowed c and c^{n-1} are "different". Compare this with the following nonabelian example

Example: $D_3 = gp\{c, b\}$, $c^3 = b^2 = (bc)^2 = e$

Conjugacy classes: (e) ← always in a class by itself $= \{e\}$

$(c) = \{c, c^2\}$ $\qquad$ $(b) = \{b, bc, bc^2\}$

$bcb^{-1} = bcb = bbc^2 = c^2$ $\qquad$ $cbc^{-1} = cbc^2 = bc$

ie rotatate = flip – rotate' – flip $\qquad$ $c^2bc^{-2} = ccbc = cb = bc^2$

ie single flips about rotated axes

Example : S_n

It can be shown that the conjugacy classes of the permutation group are given by the cycle structure

The possible cycle structures are given by the partitions of n, ie cycles the sum of whose lengths is n

$$l_1 \geq l_2 \geq \cdots \geq l_r$$

For $n=4$ the classes correspond to

$((1234))$	4	cycling 4	# of elements	6
$((123)(4))$	$3 \geq 1$	cycling 3		8
$((12)(34))$	$2 \geq 2$	two nonovertapping pairwise exchanges		3
$((12)(3)(4))$	$2 \geq 1 \geq 1$	one pairwise exchange		6
$((1)(2)(3)(4))$	$1 \geq 1 \geq 1 \geq 1$	Identity permutation		1
				24

↑ cycle notation for an element of S_4 — inside parentheses indicating the corresponding conjugacy class

Subgroups, Cosets and Lagrange's theorem

i) Subgroups – a subgroup H of the group G is a subset of G that itself forms a group under the same composition law as G.

H must be closed under composition (this is in fact sufficient for H to be a group if H is finite)

Associativity, the identity and the existence of inverses are all inherited from G (ie e and h^{-1} are there in G to be used in H)

Note: $\{e\}$ and G are (per our definition) subgroups of G (but they are trivial ones) – any other ones, should they exist, are nontrivial, and are called <u>proper</u> subgroups and denoted $H < G$

Example: D_3 is $gp\{c, b\}$ $\quad c^3 = b^2 = (bc)^2 = e$

$C_2 = \{e, b\}$ and $C_3 = \{e, c, c^2\}$ are examples of proper subgroups

ii. Cosets – another decomposition of a group into disjoint subsets

Pick a group G.
Pick a subgroup of G, called $H = \{h_1, h_2, \ldots, h_r\}$

Form a collection of new sets by left-multiplying the elements of H with each of the elements of g, in turn

$$\begin{aligned} g_1 H &= \{g_1 h_1, g_1 h_2, \ldots, g_1 h_r\} \\ g_2 H &= \{g_2 h_1, g_2 h_2, \ldots, g_2 h_r\} \\ &\vdots \end{aligned}$$

One arrives at a collection of sets, but the collection is an interesting one

- pairs of sets either completely overlap or they have no elements in common
- there are s distinct sets; we call them the <u>left cosets</u>; they all have r elements
- they provide a new partition of G into equivalence classes
- because $e \in H$ and because we scan through all g, all g appear in some coset

The equivalence relation that determines the partition is as follows:

$$a \sim b \quad \text{if} \quad b \in aH .$$

Said another way $a, b \in G$ are said to be equivalent if they differ by an "amount" that can be accommodated by an element of H — we are opting not to resolve differences between elements of G that amount to an element of H

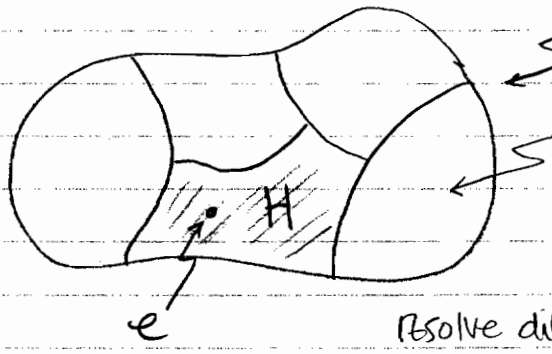
Is this an equivalence relation?

R? Is $a \in aH$?
Yes, because $e \in H$.

S? If $b \in aH$ is $a \in bH$?
Yes, because $b \in aH$ means $b = ah$ for some $h \in H$
So $a = h^{-1}b$ for $h^{-1} \in H$

T? If $b \in aH$ and $c \in bH$ is $a \in cH$?
Yes, because $b \in aH$ means $b = ah_1$ for some $h_1 \in H$
$c \in bH$ -- $c = bh_2$ -- h_2 --
So $a = c\underbrace{h_2^{-1} h_1^{-1}}_{\in H \text{ because } H \text{ is a group}} \in cH$

Being an equivalence relation it does indeed partition G, and does so into sets of "size" r



a coset is a set of $g \in G$ that are similar in the sense that they are identical if we "blur" with H (ie do not resolve differences that are attributable to H)

Pick some choice of g's that between them yield the distinct cosets - call them $\gamma_1, \gamma_2, \ldots \gamma_s$ (not a unique choice)

Then we have a collection of cosets $\{\gamma_1 H, \gamma_2 H, \ldots, \gamma_s H\}$

This set of cosets is denoted G/H

iii. Lagrange's theorem

Now, in a finite group each coset has exactly r elements, r being the order of the subgroup H, which we denote $[h]$.

The cosets partition G into s subsets each containing $[h]$ elements.

So $[g] = s[h]$. (s: size of each coset)

($[g]$: the order of G; s: # of cosets)

Hence we have Lagrange's theorem: The order $[h]$ of any subgroup of G must be a divisor of the order $[g]$ of G

Corollary: Groups of prime order have no proper subgroups

(Example: C_p with p prime)

Example of partitioning by cosets

Take the group $D_3 = gp\{c, b\}$ $\quad c^3 = b^2 = (bc)^2 = e$

It has the proper subgroups

$$\{e, b\},\ \{e, bc\},\ \{e, bc^2\} \quad \text{each} \cong C_2$$

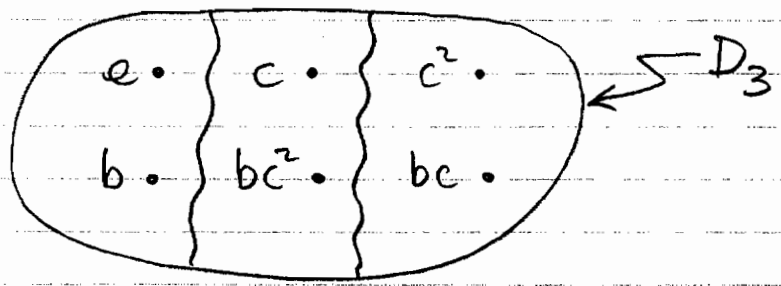
$$\{e, c, c^2\} \quad \cong C_3$$

Select for H the order-2 subgroup $\{e, b\}$

$$eH = \{e, b\}$$
$$cH = \{c, cb\} = \{c, bc^2\}$$
$$c^2H = \{c^2, c^2b\} = \{c^2, bc\}$$
$$bH = \{b, e\} \quad \text{not new}$$
$$bcH = \{bc, bcb\} = \{bc, c^2\} \quad \text{not new}$$
$$bc^2H = \{bc^2, bc^2b\} = \{bc^2, c\} \quad \text{not new}$$

[we used
- $c^2b = ccb = cbc^2 = bc^2c^2 = bc$
- $bcb = bbc^2 = c^2$
- $bc^2b = bccb = bcbc^2 = bbc^2c^2 = c$]

So we have 3 distinct cosets eH, cH, c^2H and they partition the group, as follows



3 Normal (aka invariant or self-conjugate) subgroups

Let H be a subgroup of the group G.
H is said to be a normal subgroup of G if, for all $g \in G$, we have

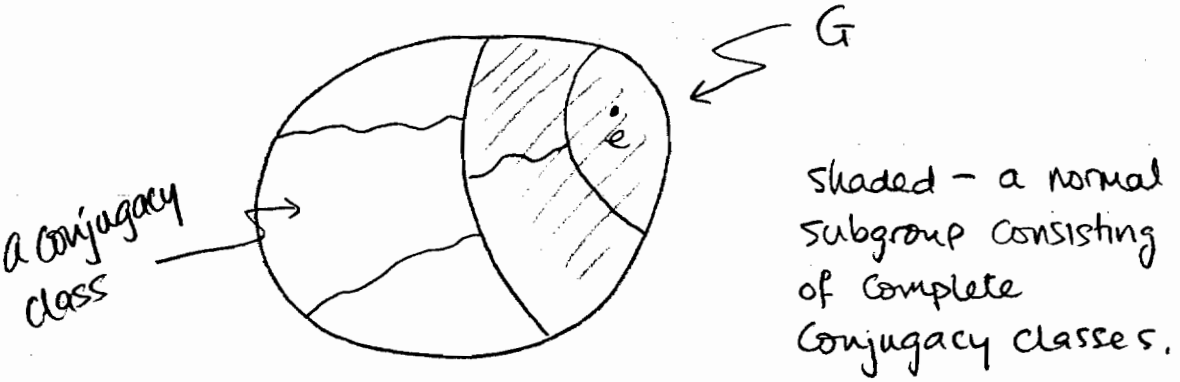
$$gHg^{-1} = H$$

ie the set H is transformed into itself under all possible transformations. (This does not mean that the individual elements $h \in H$ must be transformed into themselves, $ghg^{-1} = h$; the set H may be rearranged but the collection of constituents must reappear somewhere.)

An equivalent definition of a normal subgroup is that its left and right cosets coincide for each fixed value of g:

$$gH = Hg.$$

Note that all the conjugates ghg^{-1} of each element h of H must appear in H for H to be a normal subgroup. This means that H must comprise complete conjugacy classes, not any fragments.



Example: $G = D_3 = gp\{c, b\}$, $c^3 = b^2 = (bc)^2 = e$

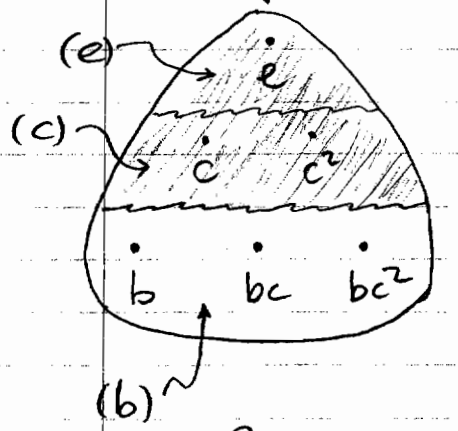
$= \{e, c, c^2, b, bc, bc^2\}$

Conjugacy classes of G: $(e) = \{e\}$ identity

$(c) = \{c, c^2\}$ $2\pi/3$ rotations

$(b) = \{b, bc, bc^2\}$ π rotations

Checking these: $geg^{-1} = e \quad \forall\, g \in G$



$bcb^{-1} = bcb = bbc^2 = c^2$

$bc^2b^{-1} = bccb = bcbc^2 = bbc^2c^2 = c$

$cbc^{-1} = cbc^2 = bc^2c^2 = bc$

$cbcc^{-1} = cb = bc^2$

$cbc^2c = cbc = bc^2c = b$

Proper subgroups of G:

$C_3 = \{e, c, c^2\}$

$C_2 = \{e, b\}, \{e, bc\}, \{e, bc^2\}$

Are any of these <u>normal</u> subgroups?

C_3? Yes; Contains (e), (c)

C_2? NO; Contain (e) but only part of (b)

checking for C_3: $b\{e, c, c^2\}b^{-1} = \{e, bcb, bc^2b\}$

$= \{e, c^2, c\}$, for example

H is rearranged

4 Quotient Groups

Suppose that H is a normal subgroup of G.

Then the set of cosets G/H has a group structure itself.

(G partitioned – divided up – by H)

Recall that $G/H = \{ \gamma_1 H, \gamma_2 H, \ldots, \gamma_s H \}$, where the γ's are a choice from the g's that get us all the distinct cosets.

We define the product of 2 cosets as follows:

$$(\gamma_i H)(\gamma_j H) = (\gamma_i \gamma_j) H$$

[not necessarily one of the γ's but certainly one of the g's; and the RHS can be got via (exactly) one of the γ's.] (*)

- Closure? Yes – see (*)
- Associativity? $(\gamma_i H)\big((\gamma_j H)(\gamma_k H)\big)$

$$= (\gamma_i H)((\gamma_j \gamma_k) H)$$
$$= (\gamma_i (\gamma_j \gamma_k)) H$$

one of the g's – see (*)

$$((\gamma_i H)(\gamma_j H))(\gamma_k H) = ((\gamma_i \gamma_j) H)(\gamma_k H)$$
$$= ((\gamma_i \gamma_j)\gamma_k) H$$

Yes: same one of the g's

— associativity is inherited from G

- Identity? $(eH)(\gamma H) = (e\gamma)H = \gamma H \Rightarrow$ Yes

↑ Can always take one of the γ's to be e

Inverse of γH? For any γ, the inverse must lie in one of the cosets (the cosets form a partition). Even though γ^{-1} may not appear in the γ's, one of the γ's will produce a coset that is identical to $\gamma^{-1}H$. This coset, then is the inverse of the coset γH.

It appears that we have verified the group structure of G/H but in fact there is one feature left to check: consistency.

We used the γ's to define the cosets but many choices of γ's will accomplish this equally well, eg

$$G/H = \{\gamma_1' H, \ldots, \gamma_s' H\} \leftarrow \text{cosets in same order as before}$$

We need to be sure that we get the same result for multiplication, regardless of the choice of γs

ie $\gamma_1'\gamma_2' H$ must be the same coset as $\gamma_1\gamma_2 H$.

Is this true? Yes, by the following argument:

$\gamma_1' H = \gamma_1 H$, so $\gamma_1' e = \gamma_1 h_1$ for some $h_1 \in H$
$\gamma_2' H = \gamma_2 H$, so $\gamma_2' e = \gamma_2 h_2$ for some $h_2 \in H$

So $\gamma_1'\gamma_2' H = \gamma_1 h_1 \gamma_2 h_2 H = \gamma_1 h_1 \gamma_2 H$
($h_2 H$ rearranges H; $\gamma_2 H = H\gamma_2$; if H is a normal subgroup)
$= \gamma_1 h_1 H \gamma_2 = \gamma_1 H \gamma_2$
($h_1 H$ rearranges H; $H\gamma_2 = \gamma_2 H$)

$= \gamma_1\gamma_2 H$, as required

So indeed, if H is a normal subgroup then the set of cosets G/H has a group structure – it is called a quotient group.

Example : $G = D_3 = gp\{c, b\}$, $c^3 = b^2 = (bc)^2 = e$

$= \{e, c, c^2, b, bc, bc^2\}$

Choose the subgroup $H = \{e, c, c^2\} = \{(e), (c)\}$

Contains complete conjugacy classes, thus H is a normal subgroup

The two left cosets are $eH = e\{e, c, c^2\} = \{e, c, c^2\} \equiv E$

$bH = b\{e, c, c^2\} = \{b, bc, bc^2\} \equiv B$

So we have the set of cosets $G/H = D_3/C_3 = \{E, B\}$

As for the multiplication table, we have

C_2

$EE = (eH)(eH) = (ee)H = eH = E$

$EB = (eH)(bH) = (eb)H = bH = B$

$BE = (bH)(eH) = (be)H = bH = B$

$BB = (bH)(bH) = (bb)H = eH = E$

	E	B
E	E	B
B	B	E

We can also show that $H = \{e, b\}$, whilst certainly a subgroup of D_3, is not a normal subgroup. It does not take together complete conjugacy classes.

Direct Product Groups

A group G is said to be the direct product, written $A \times B$, of its two subgroups A and B if

i) $a \in A$ commutes with $b \in B$

ii) every $g \in G$ can be written in a unique way as ab

How does composition work? (compose components separately)

$$g_1 g_2 = (a_1 b_1)(a_2 b_2) = (a_1 a_2)(b_1 b_2)$$

Special case: $e g_2 = e e a_2 b_2 = e a_2 e b_2 = a_2 b_2 = g_2$

Note that both A and B are normal subgroups of G.

E.g. Let $\tilde{a}$ be any element of A, ie $\tilde{a} \in A$.

Then, for all $g \in G$ we have ($\leftarrow$ by (i))

$$g \tilde{a} g^{-1} = (ab) \tilde{a} (ab)^{-1} = ab \tilde{a} b^{-1} a^{-1}$$
$$= a \tilde{a} a^{-1} \in A,$$ as required for a normal subgroup

(and similarly for B)

Hence we have two quotient groups (not just sets): G/A and G/B. These can, respectively, be put in 1:1 correspondence w/ B and A. In other words, the cosets $b_j A$ from which G/A is built are all distinct, so that they can be put in correspondence (1:1) with the elements of B. To see this, first note that G/A consists of the (independent fraction of the) cosets $\{g_1 A, g_2 A, \cdots\}$. Second, note that $g_i A = \underbrace{a_i b_i}_{\text{unique}} A = \underbrace{b_i a_i}_{\text{commute}} A = \underbrace{b_i A}_{\text{rearrangement of } A}$.

Third, all $b_i A$ are independent/distinct because otherwise we would have $b_i a_p = b_j a_q$ for $i \neq j$ and suitable a's which would be a contradiction because the a, b decomposition of each g is supposed to be unique.

So, none of the cosets $b_i A$ overlap and each can be associated with the element b_i of B. (Similarly for G/B.)

Hence we have $G/A \cong B$ and $G/B \cong A$ } and we can "cross-multiply" because we also have $G = A \times B$.

Example: $D_2 = gp\{a,b\}$ with $a^2 = b^2 = (ab)^2 = e$.

D_2 has 2 normal subgroups $A = gp\{a\}$ both isomorphic to C_2
$B = gp\{b\}$

They completely commute: $(ab)^2 = abab = e$
so $aababb = aeb = ab \Rightarrow ba = ab$.

Every element can be written uniquely as $a_i b_j$, as follows:

	a_i	b_j
e	e	e
a	a	e
b	e	b
ab	a	b

And the cosets $b_i A$ are

$e\{e,a\} = \{e,a\}$
$b\{e,a\} = \{b,ab\}$ } distinct

$\Rightarrow$ Can associate with e and b respectively, ie with $B \cong C_2$

$\Rightarrow D_2/C_2 \cong C_2$

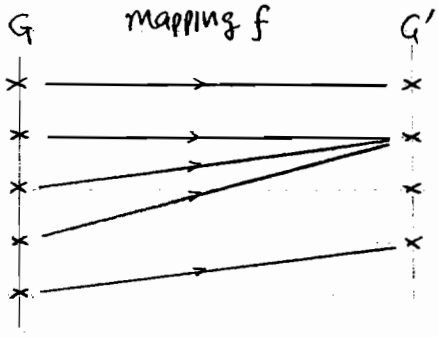
and $D_2 \cong C_2 \times C_2$

Example: Check that $D_3/C_3 = C_2$ but $D_3 \not\cong C_2 \times C_3$

D_3: nonabelian
$C_2 \times C_3$: abelian

Some ideas about Group Homomorphisms

- Let us begin simply with mappings from one group G to another G'



x indicates elements

- Each $g \in G$ goes to a unique image $g' \in G'$
- f can be many-to-one
- Some elements of G' may not be reached
  all reached : onto / surjective
  — not — : into / injective

- image of G : $\mathrm{Im} f$ or $f(G)$; this means
  $\{ g' \in G' \mid g' = f(g) \text{ for some } g \in G \}$

- Example: $f(n) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even} \end{cases}$

$f : \mathbb{Z} \to \mathbb{Z}$ is injective $f : \mathbb{Z} \to \mathbb{Z}_2$ is surjective

- General homomorphism in set theory (special cases of mappings)

  a mapping from one set to another that preserves some structure (details, however, can be blurred to a greater or lesser extent)

- Group homomorphism

  a mapping from one group G to another G', the structure to be preserved being group multiplication

So, the image of the product is the product of the images, ie,

$\forall\, g_1, g_2 \in G$ we have $f(g_1 g_2) = f(g_1)\, f(g_2)$

($g_1 g_2$: multiplication in G; $f(g_1)\, f(g_2)$: in G')

But let us emphasize that although some structure is preserved, some may be lost. (No false information is created.)

- Example: $G = \{$ all reals, positive and negative, except 0 $\}$, Composition rule is ordinary multiplication

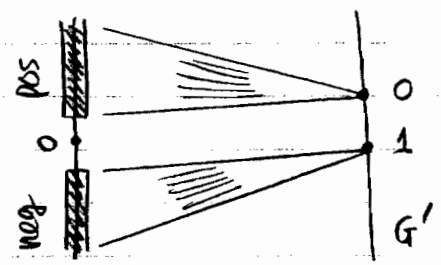
  $G' = \{0, 1\}$, Composition rule is addition mod 2

Let $f(n) = \frac{1}{2}[1 - \mathrm{sgn}(n)] = \begin{cases} 0 & \text{for } n \text{ positive} \\ 1 & \text{for } n \text{ negative} \end{cases}$

The group product rule for G is not violated because

in G			in G'			
pos × pos	=	pos	0 + 0	=	0
pos × neg	=	neg	0 + 1	=	1
neg × pos	=	neg	1 + 0	=	1
neg × neg	=	pos	1 + 1	=	0

But information is certainly lost



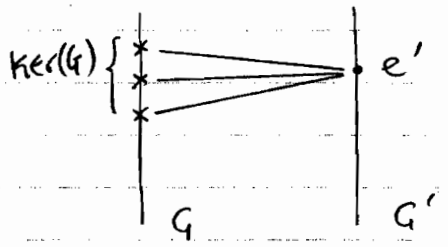
Facts about Group Homomorphisms 1/220

- They are severely restricted, very regular affairs, owing to the demand of not violating any structure (ie information in the group multiplication table)

- The image $f(G)$ is a subgroup of G'.

- The kernel $\ker(G)$ is a normal subgroup of G.

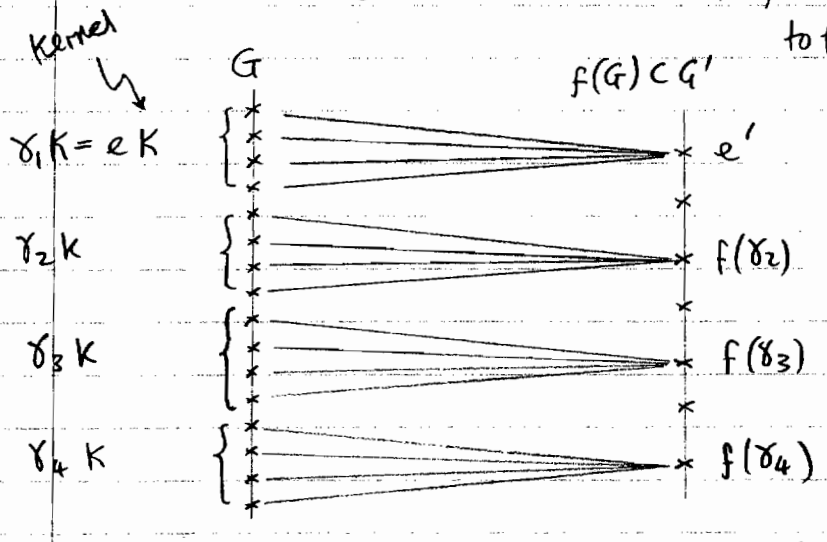
  ↑ that part of G that is mapped into the identity in G'
  $\equiv \{ g \in G \mid f(g) = e' \in G' \}$



- More generally, if $f: G \to G'$ with the kernel K then

  $f(G) \cong G/K$ i.e., the image of G is isomorphic to the quotient group G/K

  (because K is a normal subgroup this set of cosets is a group)



G can be decomposed into cosets $\gamma_i K$ (all have r elements)
f maps all elements of a coset into the same image (which is $f(\gamma_i)$ because $e \in K$); f is an $r:1$ map

Special cases: $K = G \Rightarrow f(g) = e$ (all to the identity)
$K = e \Rightarrow$ f is an isomorphism (aka bijective map); it is 1:1 and preserves group multiplication