

# Abstract Algebra

Read: Writing Proofs

Review Chapter 1

1.2 Set Theory

1.3 Mappings

1.4  $A(S)$

1.5 The integers

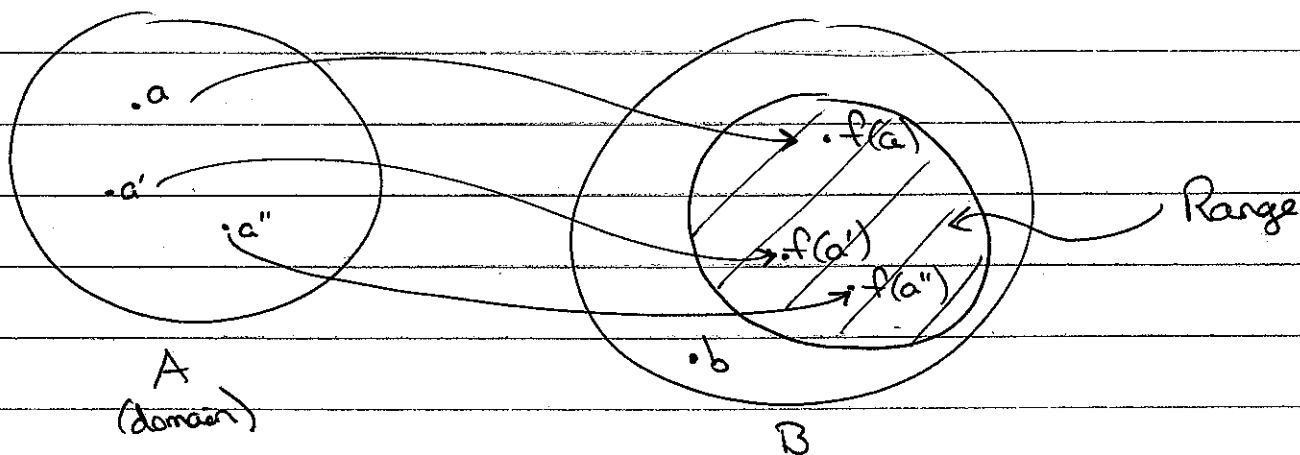
1.6 Induction

1.7 Complex numbers

FUNCTIONS = MAPPINGS

A function  $f$  from a set  $A$  to a set  $B$  is a rule which assigns to each element  $a \in A$  a value  $f(a) \in B$ .

WRITE:  $f: A \rightarrow B$



Each  $a \in A$  is assigned one value.

OK if  $f(a) = f(a')$  for some  $a, a'$ .

The domain of  $f$  is  $A$ .

The range of  $f$  is  $\{f(a) : a \in A\}$ . (everything you end up with)

The image of  $a \in A$  is  $f(a)$ .

More precise

$f$  is  $\{(a, f(a)) : a \in A\}$ .

Note:  $f: A \rightarrow B$  and  $g: A \rightarrow B$  are equal if

$f(a) = g(a)$  for each  $a \in A$ .

Write  $f = g$  in this case.

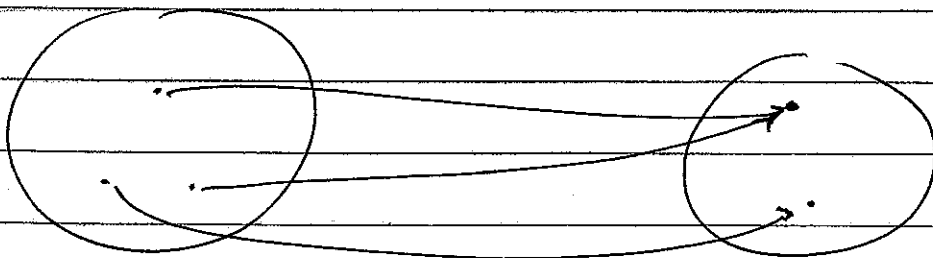
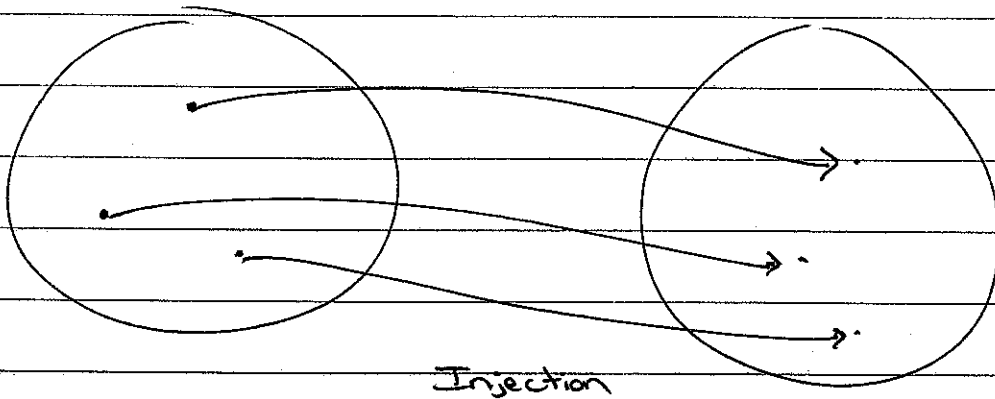
$f$  is injective, or 1-1, if

$$a \neq a' \implies f(a) \neq f(a').$$

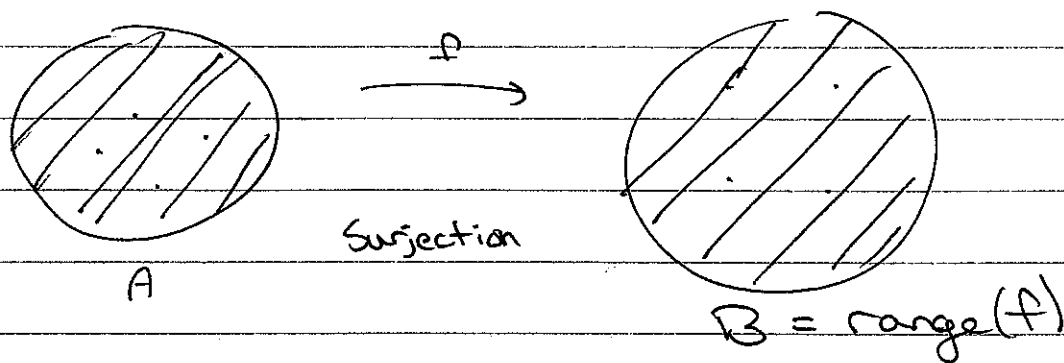
Equivalent (& easier to use:)

$$f(a) = f(a') \implies a = a'.$$

Each  $a \in A$  goes to a unique  $f(a)$

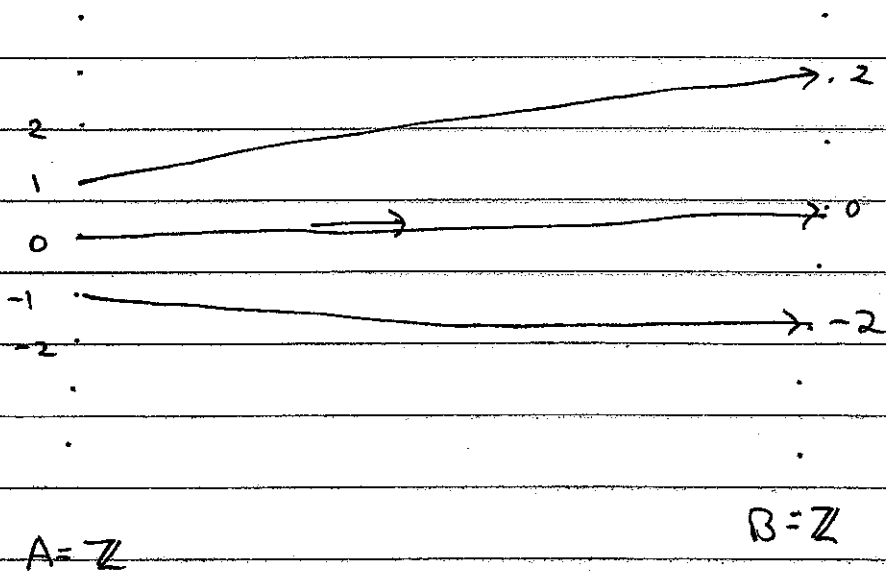


$f$  is surjective, or onto, if its range is all of  $B$ .



$f$  is a bijection if it is both injective & surjective.  
or  $\rightarrow$  Correspondence

Example  $A = \mathbb{Z}$   $B = \mathbb{Z}$   $f: \mathbb{Z} \rightarrow \mathbb{Z}$   
 $f(n) = 2n$



**SURJECTIVE IF  $B = 2\mathbb{Z}$**   
 (not function)

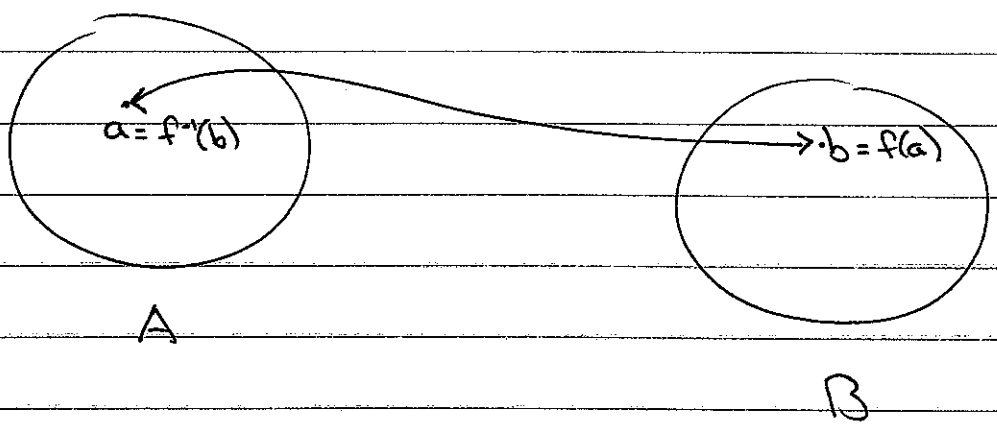
injective but not surjective

$\text{range}(f) = \{2n : n \in \mathbb{Z}\} = 2\mathbb{Z}$  even integers

Definition

If  $f$  is a bijection, then there is an inverse function  $f^{-1}: B \rightarrow A$  defined by:

$$f^{-1}(b) = a \quad \text{if} \quad f(a) = b.$$



Ex:  $A = \mathbb{R}$   $B = \mathbb{R}$   $f(x) = 2x$   $f: \mathbb{R} \rightarrow \mathbb{R}$   
 $f^{-1}(y) = y/2$

Ex: The identity function on a set  $A$  is

$$id_A: A \rightarrow A \quad \text{defined by} \quad id_A(a) = a.$$

This is a bijection, &  $(id_A)^{-1} = id_A$ .

We often want to look at what a function  $f$  does to a whole group of objects.

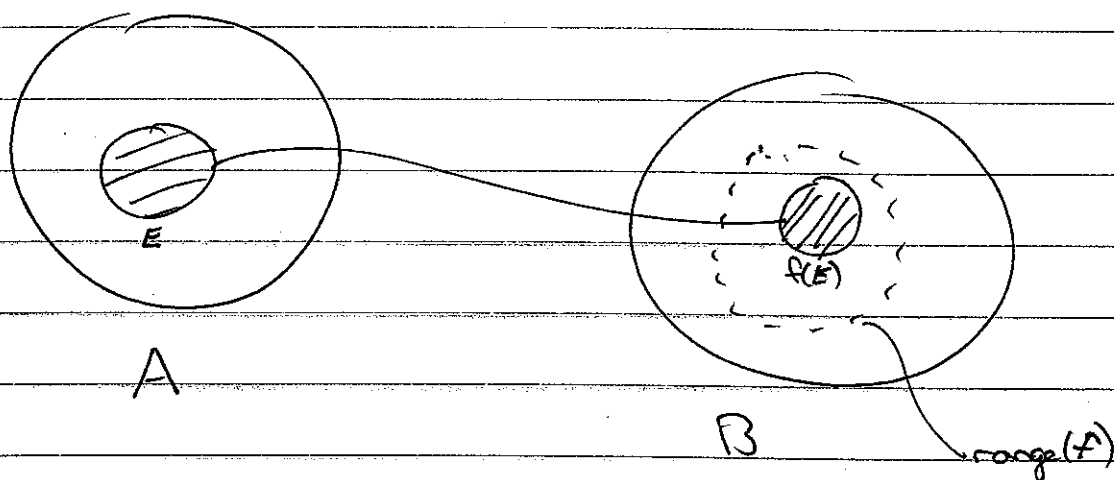
6

### Images

Let  $f: A \rightarrow B$  be a function.

If  $E \subseteq A$ , then the image of  $E$  is

$$f(E) = \{f(a) : a \in E\}$$

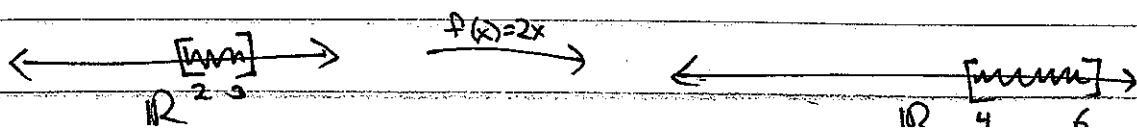


Ex:  $A = \mathbb{R}$   $B = \mathbb{R}$   $f(x) = 2x$   $f: \mathbb{R} \rightarrow \mathbb{R}$

$$E = [2, 3] \quad f(E) = \{f(x) : x \in [2, 3]\}$$

$$= \{2x : 2 \leq x \leq 3\}$$

$$= [4, 6]$$



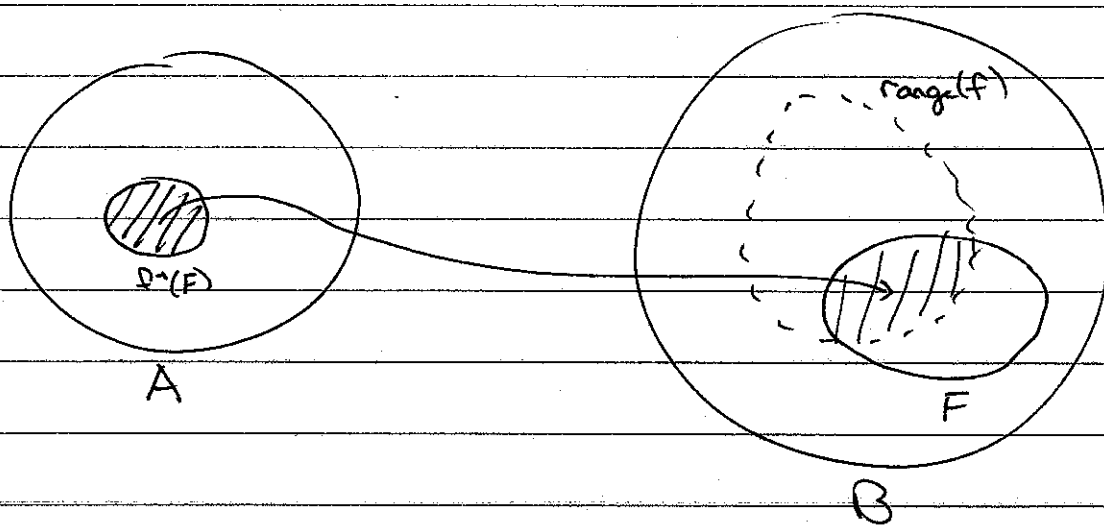
## Preimage

Let  $f: A \rightarrow B$  be a function.

If  $F \subseteq B$ , the preimage of  $F$  is

$$f^{-1}(F) = \{a \in A : f(a) \in F\}$$

NOTE:  $f^{-1}$  here does not stand for inverse function!



Ex:  $A = \mathbb{Z}$   $B = \mathbb{Z}$   $f(n) = 2n$   $f: \mathbb{Z} \rightarrow \mathbb{Z}$

$$F = \{1, 2, \dots, 10\} \quad f^{-1}(F) = \{1, 2, 3, 4, 5\}$$

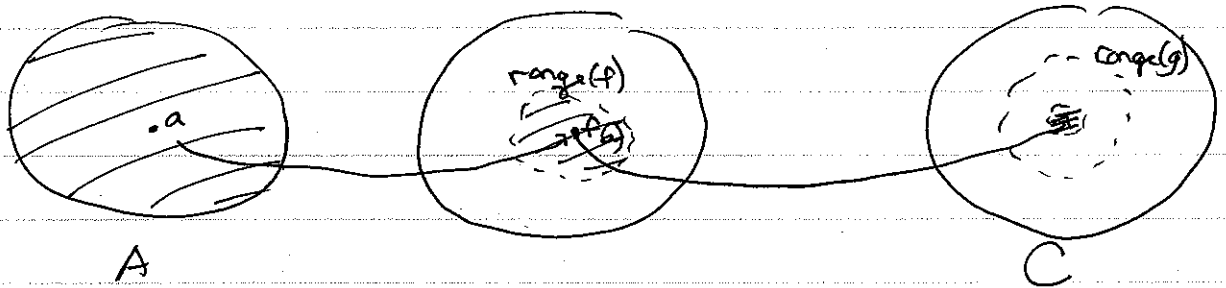
These numbers end up in  $F$   
after applying  $f$

## COMPOSITION

If  $f: A \rightarrow B$  &  $g: B \rightarrow C$  are functions, then their

composition is a function  $g \circ f: A \rightarrow C$  defined by

$$(g \circ f)(a) = g(f(a)) \quad \text{for } a \in A.$$



$$\text{range}(g \circ f) \subseteq \text{range}(g)$$

TheoremComposition of functions is associative:

$$f \circ (g \circ h) = (f \circ g) \circ h$$

$$\begin{cases} f: A \rightarrow B \\ g: B \rightarrow C \\ h: C \rightarrow D \end{cases}$$

Proof: Exercise. ~~show~~ For each  $x \in A$ ,

$$\begin{aligned} (f \circ (g \circ h))(x) &= f((g \circ h)(x)) \\ &= f(g(h(x))) \\ &= (f \circ g)(h(x)) \\ &= ((f \circ g) \circ h)(x). \end{aligned}$$

Hence the functions  $f \circ (g \circ h)$  &  $(f \circ g) \circ h$  are the same function.  $\square$ NOTE IN GENERAL  $f \circ g \neq g \circ f$ !Composition is NOT commutative.  
Order is important.

$$\begin{aligned} \text{Ex } f(x) &= x + 1 & f, g: \mathbb{R} \rightarrow \mathbb{R} \\ g(x) &= x^2 \end{aligned}$$

## Exercises

- a.  $f: A \rightarrow B$  &  $g: B \rightarrow C$  both injective  $\Rightarrow$   $g \circ f$  is injective
- b. " " " " surjective  $\Rightarrow$  " " surjective
- c. " " " " bijective  $\Rightarrow$  " " bijective

## Exercise

Given  $f: A \rightarrow B$  &  $g: B \rightarrow C$ . ~~show~~ Show:

- a.  $g \circ f$  injective  $\Rightarrow$   $f$  injective
- b.  $g \circ f$  surjective  $\Rightarrow$   $g$  surjective.

Give examples of  $f, g$  st.

$g \circ f$  injective but  $g$  is not injective

$g \circ f$  surjective but  $f$  is not surjective.

## Exercise

If  $f: A \rightarrow B$  is a bijection, then

$$f \circ f^{-1} = i_B \text{ (identity on } B) \quad \& \quad f^{-1} \circ f = i_A \text{ (identity on } A).$$

## Exercise

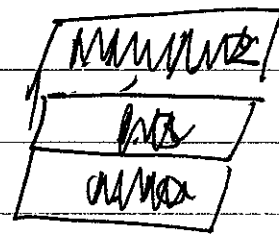
Find examples of functions  $f: A \rightarrow B$  &  $g: B \rightarrow A$  s.t.

$$g \circ f = i_A \text{ but } f \circ g \neq i_B$$

Why does this not contradict the preceding exercise?

Functions usually studied in calculus are  $f: \mathbb{R} \rightarrow \mathbb{R}$ .  
 These are easily visualized via their graphs. More general functions do not have easily visualized graphs.  
 Still, picture  $f$  as taking elements from the domain & giving elements of the range.

## Rigid Motions of the plane & Symmetry

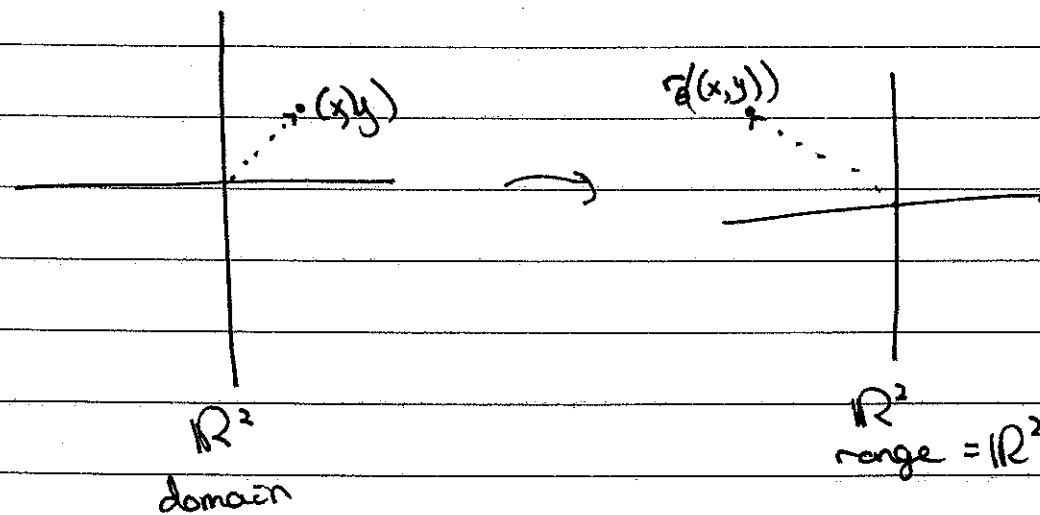


There are many bijections  $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$

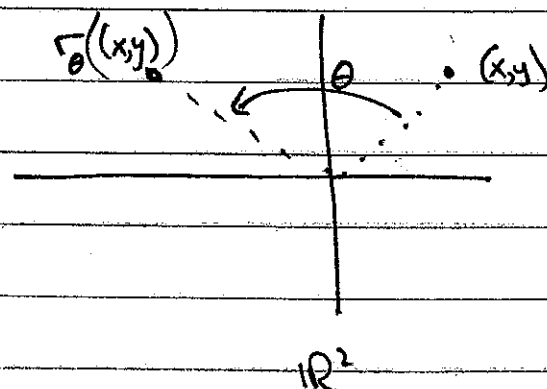
Some of these are rigid motions.

Rotations For each number  $\theta$ , define a function  $r_\theta: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  by

$r_\theta(x, y)$  = the point obtained by rotating  $(x, y)$  by an angle of  $\theta$  around the origin.



Usually picture something like this with domain & range superimposed:



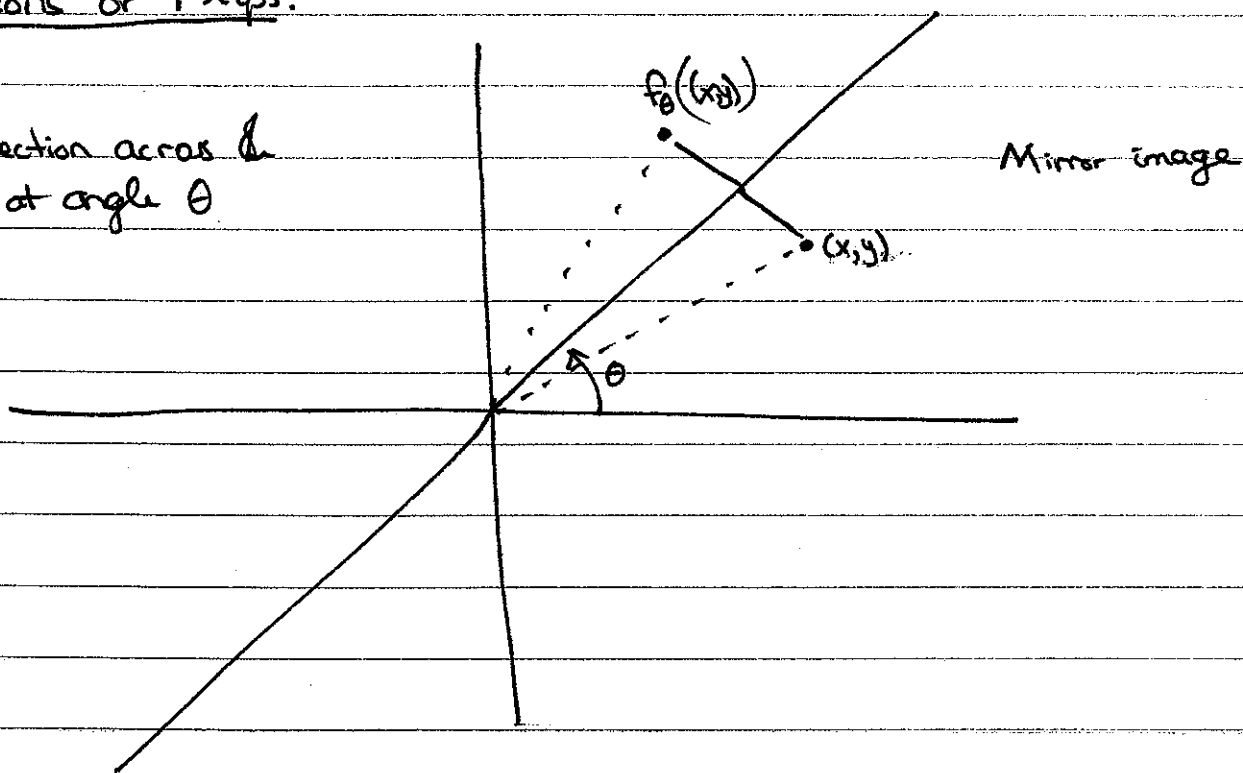
NOTE:  $r_{2\pi} = id_{\mathbb{R}^2} = r_0$

$r_\theta^{-1} = r_{(-\theta)}$

$r_{2\theta} = r_\theta^2 = r_\theta \circ r_\theta$

## Reflections or Flips:

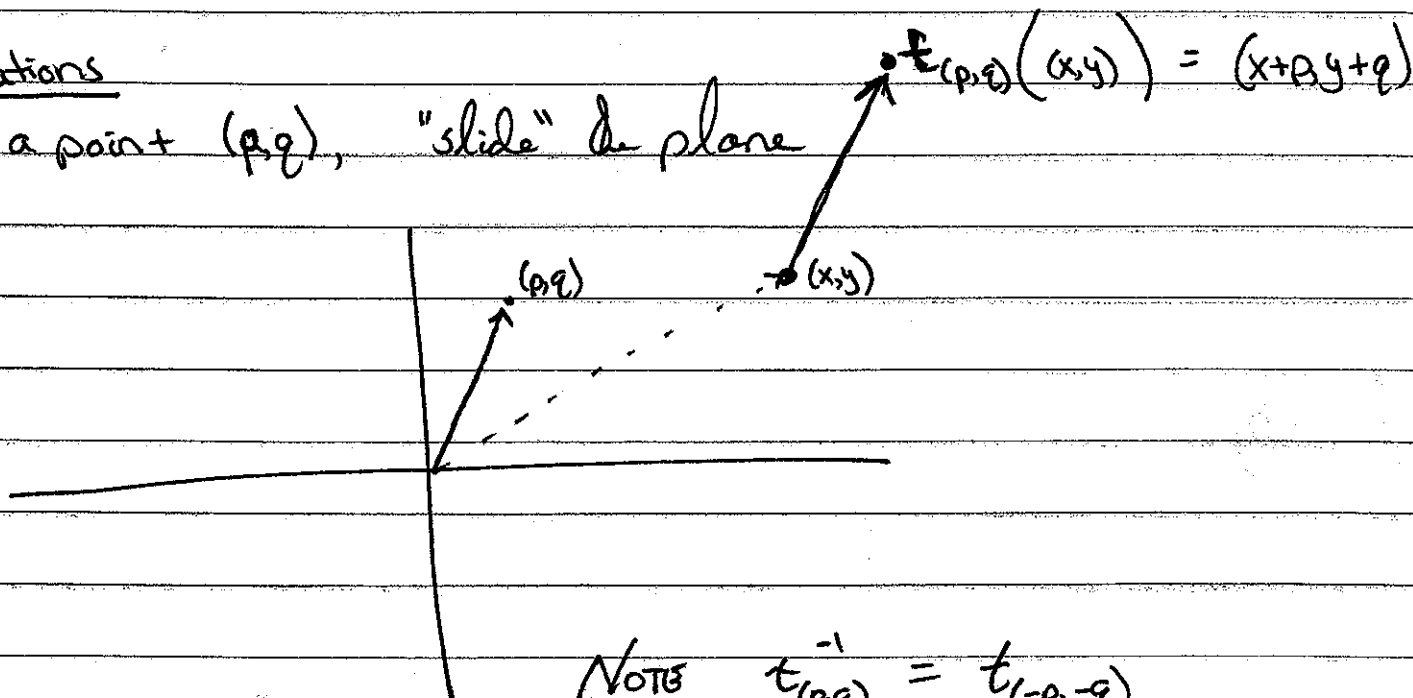
$f_\theta$  = reflection across a line at angle  $\theta$



NOTE:  $f_\theta^2 = f_\theta \circ f_\theta = \text{id}_{\mathbb{R}^2}$  so  $f_\theta = f_\theta^{-1}$ !

## Translations

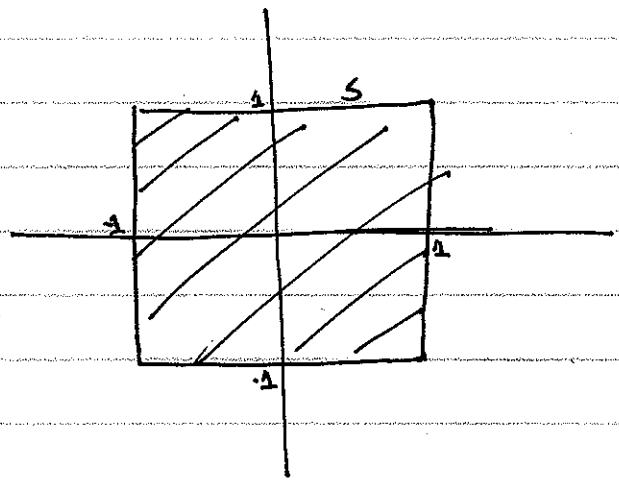
Given a point  $(p, q)$ , "slide" the plane



NOTE  $t_{(p,q)}^{-1} = t_{(-p,-q)}$

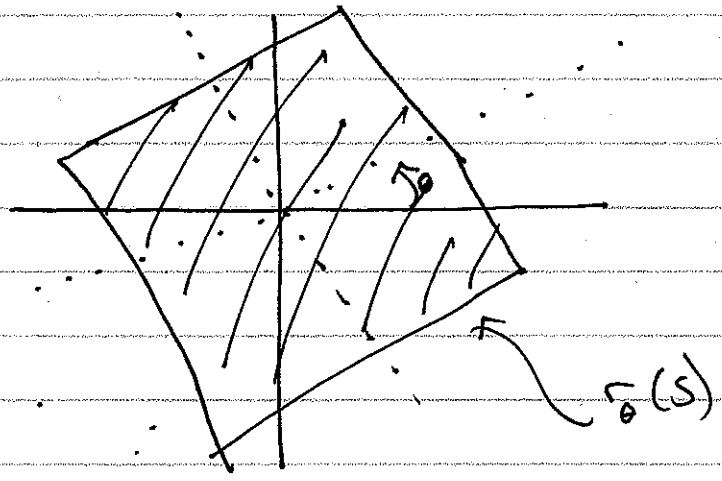
Consider rigid motions & the unit square  $S$

What are the images of  $S$  under rigid motions?



$$S = \{(x, y) : |x| \leq 1 \text{ \& } |y| \leq 1\}$$

Image under rotations:



~~$f_0(S) = S$  for  $\theta = 0, \pi, 2\pi, \dots$~~   
 ~~$\pi/2, \pi, 3\pi/2, 2\pi, \dots$~~   
 ~~$f_0 = f_{2\pi}$  same function~~

There are 4 rotations that "preserve" the square or leave the square "invariant":

$$\Gamma_\theta(S) = S \quad \text{for} \quad \theta = 0, \pi/2, \pi, 3\pi/2$$

Note  $\Gamma_0 = \Gamma_{2\pi} = \Gamma_{4\pi}$  etc are the same function

$$\Gamma_0(x, y) = \Gamma_{2\pi}(x, y) \quad \text{for every } (x, y) \in \mathbb{R}^2.$$

But  $\Gamma_0(x, y) \neq \Gamma_{\pi/2}(x, y)$  for every  $(x, y)$

so these are different functions.

The rotations  $\Gamma_0, \Gamma_{\pi/2}, \Gamma_\pi, \Gamma_{3\pi/2}$

have the property that they leave the square invariant.

This is because the square has symmetries.

Set  $\Gamma = \Gamma_{\pi/2}$ .

Then:

$$\Gamma^0 = \text{id}_{\mathbb{R}^2} = \Gamma_0$$

$\Gamma^0 = r$  to the zeroth power  
 $\Gamma_0 =$  rotation by 0 radians

$$\Gamma^1 = \Gamma = \Gamma_{\pi/2}$$

$$\Gamma^2 = \Gamma_\pi$$

$$\Gamma^3 = \Gamma_{3\pi/2}$$

So the 4 rotations that leave the square invariant are:

$$e = \text{id}_{\mathbb{R}^2}, \quad r, \quad r^2, \quad r^3.$$

Note:  $r^4 = e$        $r^{-1} = r^3$

$$r^5 = r \quad r^{-2} = \del{r^2} r^2$$

$$r^6 = r^2 \quad r^{-3} = r$$

$$\vdots$$

$$\vdots$$

$$r^m \circ r^n = r^{m+n}$$

similar to multiplication rules

So:

$$\{ \dots, r^{-2}, r^{-1}, r^0, r^1, r^2, \dots \} = \{ e, r, r^2, r^3 \}$$

many duplicates

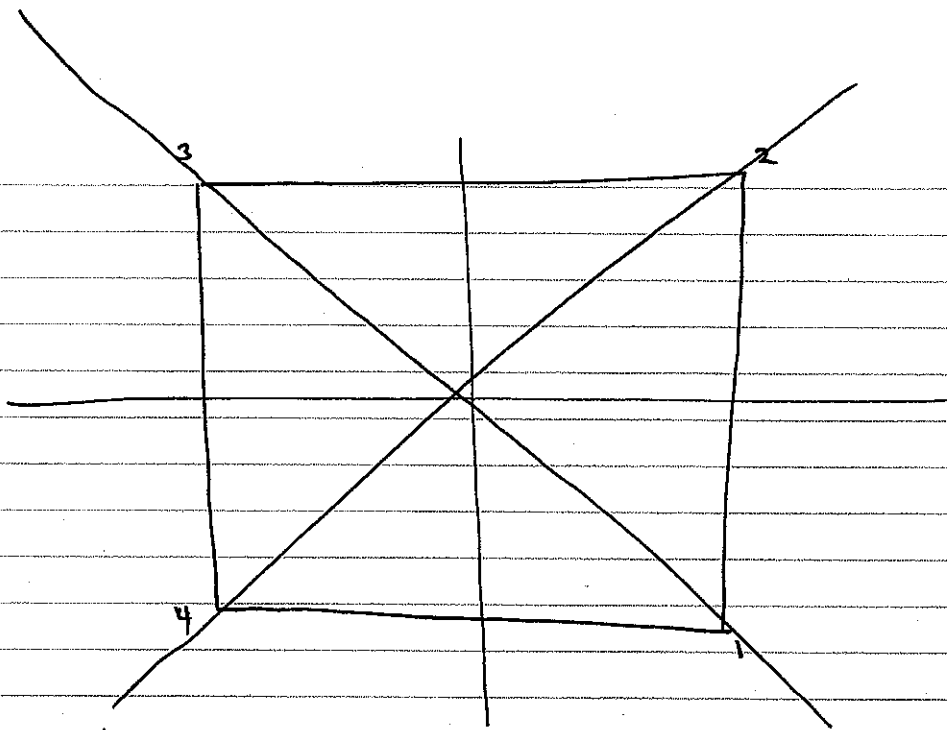
$$\{ r^m : m \in \mathbb{Z} \} = \{ e, r, r^2, r^3 \}.$$

Translations?

No translations preserve  $\square$  square except

$$t_{(0,0)} = \text{id}_{\mathbb{R}^2} = e \quad \text{already got this.}$$

## Flips



label corners to help you see what a flip does.

There are 4 distinct flips that preserve a square:

Call these

$$a = f_0 = \text{flip about } x\text{-axis} = f_\pi$$

$$c = f_{\pi/4} = \text{diagonal} = f_{5\pi/4}$$

$$b = f_{\pi/2} = \text{y-axis} = f_{3\pi/2}$$

$$d = f_{3\pi/4} = \text{other diagonal} = f_{7\pi/4}$$

$a, b, c, d$  are functions, they are the 4 flips that preserve a square.

Note  $a, b, c, d \neq e, r, r^2, r^3$

these are different functions.

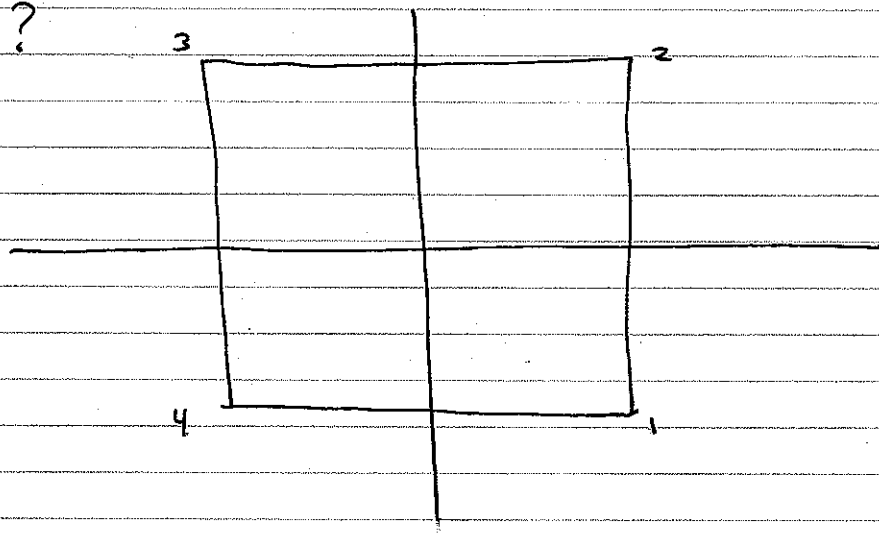
Define

$$G = \{e, r, r^2, r^3, a, b, c, d\}$$

$G$  is a set of 8 functions, each function in  $G$  has the property that it preserves the square.

Any composition of 2 functions from  $G$  would also preserve the square. Let's compute some of these.

$r \circ a = ?$



$r \circ a$  maps:

corner 1	→	corner 3
2	→	2
3	→	1
4	→	4

Same as flip <sup>C</sup>!

In fact:

$$r \circ a = c \text{ meaning } (r \circ a)(x, y) = \begin{matrix} \bullet \\ \bullet \\ \bullet \\ \bullet \end{matrix} (x, y) \quad \forall (x, y)$$

No matter what 2 functions in  $G$  you compose, you get another function in  $G$ .  $G$  is closed under compositions.

$$e \circ r^2 = r^2$$

$$r \circ r^3 = e$$

$$a \circ b = d$$

$$1 \rightarrow 4$$

$$2 \rightarrow 3$$

$$3 \rightarrow 2$$

$$1 \rightarrow 4$$

etc.

~~do not~~

$a \circ r = d$  Note  $r \circ a = c!$  Functions do not commute!

Also  $G$  has an identity element:  
 $e \circ f = f$  &  $f \circ e = f$  for all  $f \in G$ .

Also  $G$  is closed under inverses.

$$a^{-1} = a$$

$$e^{-1} = e$$

$$b^{-1} = b$$

$$r^{-1} = r^3$$

$$c^{-1} = c$$

$$(r^2)^{-1} = r^2$$

$$d^{-1} = d$$

$$(r^3)^{-1} = r$$

AND Composition is associative

$$a \circ (b \circ r) = (a \circ b) \circ r \text{ etc.}$$

(But not commutative!)

$$a \circ r \neq r \circ a$$

$$G = \{e, r, r^2, r^3, a, b, c, d\}$$

Thus  $G$  is a set of 8 elements, together with an "operation" (composition), a way of combining elements together to get other elements, which satisfies

1.  $G$  is closed under composition
2.  $G$  has an identity element
3.  $G$  is closed under inverses
4. The operation (composition) is ~~commutative~~ <sup>associative</sup>

We call  $G$  a group because these properties are satisfied.

We can use a "multiplication table" to show all the possible compositions:

1.4

$e$	$e$	$r$	$r^2$	$r^3$	$a$	$b$	$c$	$d$
$e$	$e$	$r$	$r^2$					
$r$	$r$				$c$			
$r^2$	$r^2$							
$r^3$								
$a$	<del><math>a</math></del>	$d$			$e$			
$b$						$e$		
$c$							$e$	
$d$								$e$

Exercise  
fill in

Often we use multiplicative-like notation

Write just  $ar$  instead of  $a \circ r$

Call  $ar$  the "product" of  $a$  &  $r$  (order important!)

## 1.4 A(S)

### Definition

Let  $S$  be a set. Then

$$A(S) = \{f : f \text{ is a bijection of } S \text{ onto } S\}.$$

### Example

If  $S$  is the unit square, then the rotations & flips we discussed before are some of the bijections of the square onto itself. A bijection doesn't have to be a rigid motion, & it doesn't have to be "continuous".

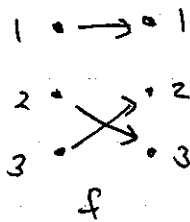
Exercise: Give examples of other bijections of  $S$  onto itself.

### Definition

If  $S = \{1, 2, \dots, n\}$ , then the symmetric group of degree  $n$  is

$$S_n = A(S) = \{f : f \text{ is a bijection of } \{1, 2, \dots, n\} \text{ onto itself}\}.$$

Examples of bijections of  $\{1,2,3\}$  onto itself.



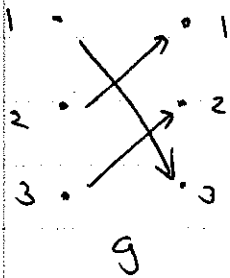
Another notation

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Permutation notation

$$f = (23)$$

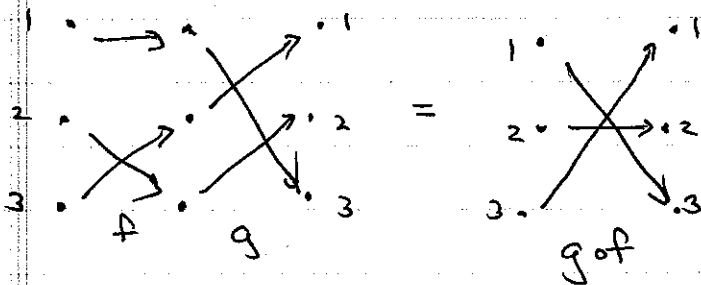
$$\text{or } f = (1)(23)$$



$$g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$g = (132)$$

Composition: Compute  $f \circ g$



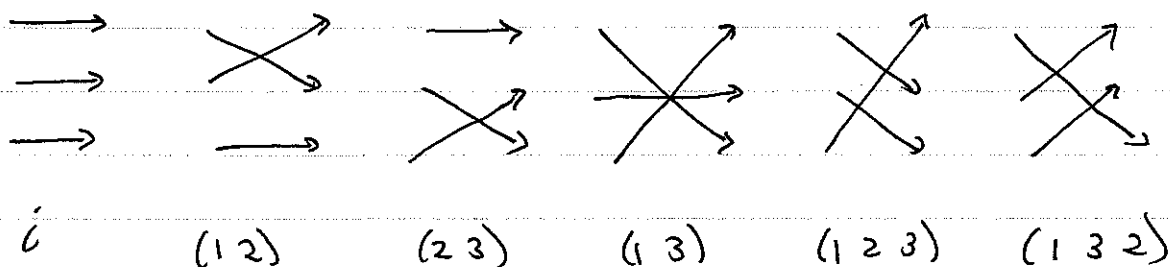
$$f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\text{or } f \circ g = (13) = (13)(2)$$

Exercise:  $f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$$f \circ g = (12) = (12)(3)$$

$S_3$  has 6 elements



Exercise:  $S_n$  has  $n!$  elements.

Properties of  $A(S)$

a.  $A(S)$  is closed under compositions:  $f, g \in A(S) \Rightarrow f \circ g \in A(S)$

b. Composition is associative:  $(f \circ g) \circ h = f \circ (g \circ h) \quad \forall f, g, h \in A(S)$

c.  $\exists$  identity element  $i$  s.t.  $i \circ f = f \circ i \quad \forall f \in A(S)$

d.  $\exists$  inverses:  $f \in A(S) \Rightarrow f^{-1} \in A(S)$  &  
 $f \circ f^{-1} = i = f^{-1} \circ f$

$A(S)$  is an example of a group.

$S_n$  is a finite group.

## Shorthand notation

We often write  $fg$  for  $f \circ g$ , &  $f^2 = f \circ f$ , etc.

### Note

$fg \neq gf$  in general

$(fg)^2 \neq f^2 g^2$  in general.

### Exercise

$$fg = fh \Rightarrow g = h$$

$$fg = hg \Rightarrow f = h$$

Beware:  $fg = gh \not\Rightarrow f = h!$

## 1.5 The Integers

Review the basic properties of

the natural numbers  $\mathbb{N} = \{1, 2, 3, \dots\}$

the integers  $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$

### Well-ordering Principle

Every nonempty set of nonnegative integers has a smallest element.

### Euclidean Algorithm

If  $m, n \in \mathbb{Z}$ ,  $n > 0$ , then  $\exists q, r \in \mathbb{Z}$  with  $0 \leq r < n$  s.t.

$$m = qn + r$$

Fundamental Theorem of Arithmetic

= unique factorization of positive integers as product of primes.

## 1.6 Induction

Review induction.