1/10/10

Groups ①

sets and groups A Green

First Course Abstract Algebra 3 ~~Reading~~ Fraleigh

Groups and Permutations

Defn: We say $(G, *)$ is a group if:
G is a set and $*$ is a binary operation, (such as addition) such that

1. If $a, b \in G$, $a * b \in G$ (condition of closure)
2. If $a, b, c \in G$, $a*(b*c) = (a*b)*c$ (operation is associative)
3. There exists an element $e \in G$ (identity element) such that $a*e = a = e*a$
4. For each $a \in G$ there exists $\bar{a} \in G$ (inverse) such that $a * \bar{a} = e = \bar{a} * a$

E.g. $(\mathbb{Z}, +)$, $e=0$, $\bar{a} = a$ is a group
So is $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$

$(\mathbb{Q} \setminus \{0\}, \times)$ $e = 1$ $\bar{a} = \frac{1}{a}$

Set of rationals with zero removed

Eg. $(\{\pm 1\}, \times)$ $e = 1$ $\bar{a} = a$

Lemma 1.1

Let $(G, *)$ be a group. The identity element e is unique.
i) In fact, if $a*e = a = e'*a$ then $e = e'$
For any $a \in G$, $\bar{a} \in G$ is unique.
ii) In fact, if $b*a = e = a*b'$ then $b = b'$

Abelian $a*b = b*a$ for all $a, b \in G$

Proof of Lemma 1.1

i) $e' = e * e' = e$
ii) Assume ~~a*b~~ $b*a = e = a*b'$
Then $b = b*(a*b') = (b*a)*b' = e*b' = b'$
due to associativity

1. A group may or may not be Abelian or commutative
2. The associative law means we do not need brackets $a*b*c = (a*b)*c = a*(b*c)$

3. Often we drop $*$ and write ab or $a \cdot b$ for $a * b$

Lemma 1.2 i) If $a, b \in G$ $\overline{(ab)} = \bar{b}\bar{a}$
socks and shoes lemma
ii) $\bar{\bar{a}} = a$

Proof $(ab)(\bar{b}\bar{a}) = [(ab)\bar{b}]\bar{a} = [a(b\bar{b})]\bar{a} = (ae)\bar{a}$
$= a\bar{a} = e$

And so $(\bar{b}\bar{a})(ab) = e$,
ii) $\bar{a}\bar{\bar{a}} = e = \bar{\bar{a}}\bar{a}$, also $\bar{a}a = e = a\bar{a}$, so by 1.2, inverse uniqueness, $a =$

Lemma 1.3
(cancellation) If $ax = bx$ then $a = b$
Also $xa = xb \Rightarrow a = b$

Proof $ax = bx$, $a(x\bar{x}) = b(x\bar{x})$, $ae = be$, $a = b$

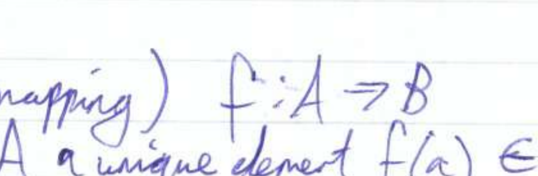
$\boxed{\text{Permutations}}$

If A, B are sets, a function (or a mapping) $f : A \to B$
is a rule which assigns each $a \in A$ a unique element $f(a) \in B$

E.g. $A = \mathbb{R} = B$ $f(x) = x^2$

E.g. A = a deck of cards $= B$, f is a shuffle of A
(set)

Functions are single valued



If $A \to B$ is bijective (one to one correspondance)
If for all $b \in B$ there exists a unique pre image

$f(a) = b$. If $f : A \to B$, A and B are the same size

$f : A \to B$ is Injective if $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$
Surjective if for all $b \in B$ there is an $a \in A$
with $f(a) = b$

Bijective is Both!!
$A = B = X$, $f : X \to X$ is a permutation if bijective

0/10

Groups (1)

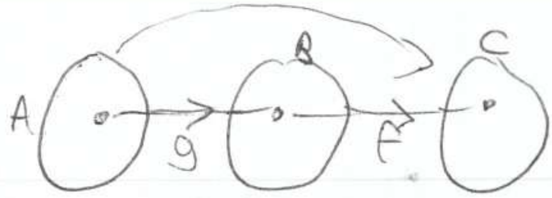
Composite functions

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[rr, bend right, "f \circ g"'] & B \arrow[r, "f"] & C \end{tikzcd}$$

$$f \circ g : A \to C$$
$$a \mapsto f[g(a)]$$

11/10/10

Groups ②



Recap: $(G, *)$ is a group if G is a set
$*$ is a binary operation on G such that
i) G is closed under $*$
ii) associative
iii) identity element
iv) inverse for each element

$g: A \to B$ $\quad f: B \to C \quad f \circ g : A \to C$
$f \circ g(a) = f[g(a)]$

<u>Lemma 1.4</u> $g: A \to B$, $f: B \to C$ are bijective
then $f \circ g : A \to C$ is bijective
In fact if injective or surjective used, lemma still true
$A = B = C = X$
<u>Proof</u>
Let $c \in C$. Let $b \in B$ be a preimage of C in B, so $f(b) = c$. Let $a \in A$ with $g(a) = b$. Then $f \circ g(a) = f(g(a))$
$= f(b) = c$

This a is unique:
if $f \circ g(a_1) = f \circ g(a_2)$ then $f(g(a_1)) = f(g(a_2))$
as f is injective $g(a_1) = g(a_2)$ and as g is also, $a_1 = a_2$ I

$Sym(X)$ = the set of all permutations of a set X.

<u>Theorem 1.5</u> $[Sym(X), \circ]$ is a group, the Symmetry group on X.

<u>Proof</u>
1. If $f, g \in Sym(X)$ then so is $f \circ g$ by <u>1.4</u>

2. $f, g, h \in Sym(X)$. Let $x \in X$
$[(f \circ g) \circ h](x) = (f \circ g)[h(x)] = f\{g[h(x)]\}$

$[f \circ (g \circ h)](x) = f[(g \circ h)(x)] = f\{g[h(x)]\}$
True for all X so $(f \circ g) \circ h = f \circ (g \circ h)$ for ALL functions

3. The identity is $i : X \to X$
$x \mapsto x$

If $f \in Sym(X)$ then $f \circ i = i \circ f$
since if $x \in X$ $f \circ i(x) = f[i(x)] = f(x)$
$i \circ f(x) = i[f(x)] = f(x)$

4. $f \in Sym(X)$. For $y \in X$, take x to be the unique pre image of y under f, define $f^{-1}(y)$ to be this x. Doing it for all $y \in X$, get a function $f^{-1} : X \to X$. Then $f^{-1} \in Sym(X)$ and $f \circ f^{-1} = i = f^{-1} \circ f$
since $f \circ f^{-1}(z) = z$ and $f^{-1} \circ f(z) = z$

Notation: If $|X| = n$ → number of elements, often write $X = [1, n]$
$= \{1, 2, \dots, n\}$

Also write $Sym(X) = S_n$ → symmetric group of degree n
$|X|$ is the degree.

Definition: If G is a group, the order of G is the size $|G|$

$|S_n| = n!$, the order of the symmetric group of degree n

Notation $(G, *)$ is a group, $g \in G$ $\quad g^1 = g$
$n \in \mathbb{Z}$, if $n > 0$, $g^n = \underbrace{g * g * \dots * g}_{n \text{ times}}$ $\quad g^{n+1} = g^n *$

if $n = 0$, $g^0 = e$
if $n < 0$ $\quad g^n = (g^{-1})^{|n|} = (g^{|n|})^{-1}$

Definition Possible that $g^n = e$ for some $n > 0$ the smallest such n is the order of the element g
If no such n exists, g has ∞ order.

Finite element order, finite groups
Likewise with infinite

NOTE
$g^j * g^k = g^{k+j}$

1/10/10

Groups (2)

Lemma 1·6

If G is a finite group, and $g \in G$, then order of g $o(g)$ is finite

(in fact $o(g) \mid |G|$ for any $g \in G$)

Proof, exercise I/4.

Lemma 1·7 If G is a group, $g \in G$ with $o(g) \in \mathbb{N}$ and if $g^m = e$, then $n \mid m$, so $m = qn$ for $q \in \mathbb{Z}$

see N+S

Proof: $m = qn + r$ with $r \in \mathbb{Z}$, $0 \leq r < n$

Then $g^n = e = g^m$, so $g^r = e$ since $g^r = g^{m-qn}$

n is least positive with $g^n = e$ so $r = 0$ $\qquad g^r = g^m \cdot (g^n)$

Example

$S_3 \quad X = \{1, 2, 3\}$ Notation $f \begin{pmatrix} 1, 2, \dots & n \\ f(1), f(2) \dots & n \end{pmatrix}$

$i \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\tau \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma^3 = i$

$\tau^2 = i$

$\sigma\tau$

$\sigma^2\tau$

3/10/10

Groups (3)

~~Degree~~ ~~Order: number of elements~~ For $S_n = Sym(X)$ symetric group

Degree : Number of Points! Order : Number of Elements!

If $|X| = n$, $|S_n| = n!$

$X = \{1, 2, 3\}$ Note, $|X| = 3$, order 3

$S_3 = Sym(X)$ $|S_3| = 3! = 6$, order 6, degree 3

$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ order 1 $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $O(\sigma) = 3$ order of $\sigma = 3$

$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ order 3 $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ order 2

Note! NON ABELIAN

$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ order 2 $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Ex, S_4 has 24 elements.

More transparent notation for permutations; as product of disjoint cycles.

Define: $\sigma \in S_n$ [$= Sym(X)$] is a k cycle written $\sigma = (a_1, a_2 \dots a_k)$

if $\sigma(a_i) = a_{i+1}$

$\sigma(a_k) = a_1$

$\sigma(x) = x$ for all $x \in X$ which are not a_i for any i

Remarks $(a_1, a_2, \dots a_k) = (a_2, a_3, \dots a_k, a_1)$

1. k different ways to write a different cycle.

2. $(a_1\ a_2\ a_3 \dots a_k)^{-1} = (a_1\ a_k\ a_{k-1} \dots a_2)$

3. $\sigma^k = i$, $O(\sigma) = k$

order of sigma is the length of the cycle

Definition: The cycles $\sigma = (a_1\ a_2 \dots a_k)$
and $\tau\ (b_1\ b_2 \dots b_l)$
are disjoint of all a_j, b_i are distinct

Lemma 1.8 Two disjoint cycles commute $(1\ 2) \circ (3\ 4\ 5) = (3\ 4\ 5) \circ (1$

Note: if σ, τ are NOT disjoint, in general they do not commute
$(1\ 2\ 3) \circ (2\ 3) = (2\ 1)(3)$
$(2\ 3) \circ (1\ 2\ 3) = (1\ 3)(2)$

Proof of 1.8 $\sigma = (a_1 \dots a_k)$ $\tau = (b_1 \dots b_l)$ disjoint

$\sigma \circ \tau = \tau \circ \sigma$ because let $x \in X$
if $x = a_i$ then $\sigma\tau(x) = \sigma(\tau(a_i)) = \sigma(a_i)$
$\tau\sigma(x) = \tau(\sigma(a_i)) = \sigma(a_i)$

$x = b_i$ $\sigma\tau(b_i) = \tau(b_i)$
$\tau\sigma(b_i) = \tau(b_i)$
And, if $x \in X$ but not one of a_i, b_i then x is fixed by σ, τ, so $\sigma\tau(x) = x = \tau\sigma(x)$
so $\sigma\tau = \tau\sigma$ $\square$

Disjoint cycle notations for permutations.
Theorem 1.9 Any permutation in S_n can be written as a product of disjoint cycles in an essentially unique way.

$|X| = 8$
$X = \{1, 2 \dots 8\}$ E.g. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 1 & 5 & 8 & 3 & 7 \end{pmatrix} = (1\ 2\ 4)(3\ 6\ 8\ 7)(5)$
$= (6\ 8\ 7\ 3)(2\ 4\ 1)$

Proof: Let $\pi \in S_n$ $X = \{1, \dots, n\}$
Let $a \in X$. Look at $a, \pi(a), \pi^2(a) \dots$
Since X is finite, there is a $k \in \mathbb{N}$ with
$\pi^k(a) \in \{a, \pi(a), \dots \pi^{k-1}(a)\}$. Take smallest k for which this holds.

13/10/10

Groups ③

Claim $\pi^k(a) = a$
if $\pi^k(a) = \pi^j(a)$ with $0 \leq j < k$ $\pi^{k-j}(a) = a$
and $0 < k-j \leq k$ forces $j = 0$

$\pi^k(a) = a$

Put $a_1 = a$, $a_2 = \pi(a)$ ... $a_k = \pi^{k-1}(a)$

If not all points of X have been covered choose b in X different from all previous points. Look at $b, \pi(b), \pi^2(b) \dots$ and let l be the smallest with $\pi^l(b) \in \{b, \pi(b), \dots, \pi^{l-1}(b)\}$

Then put $b_1 = b$ $b_2 = \pi(b)$, ... $b_l = \pi^{l-1}(b)$. Note that b_i are distinct from all previous points since all powers of π are bijective.
After finitely many steps, all points of X will be covered.

Thus $\pi = (a_1 a_2 \dots a_k)(b_1 \dots b_l) \dots$ ← note, finite a product of disjoint cycles

Lemma 1.10 The order of π or $O(\pi)$ is the least common multiple of the length of the cycles in its disjoint cycle notation.

5/10/10

Groups (4)

Lemma 1.10

The order $O(\pi)$ of the permutation π is the Lcm of the lengths of cycles in its disjoint cycle composition.

Proof The disjoint cycles in π commute so $\pi^m = i$ iff $\sigma^m = i$ for each cycle in π.

$[\pi = (\sigma_1 \dots \sigma_L)^m = \sigma_1^m \sigma_L^m]$

Now $\sigma^m = i$ iff length of σ divides m [$o(\sigma) =$ length σ and $\sigma^m = i$ iff order σ / m]

Thus the order of π is the Lcm of cycles in π

Defn A transposition is a 2 cycle.

$\tau = (r\ s)$ swaps two points in X

Lemma 1.11

Any permutation can be written as a product of transpositions.

E.g. $(1\,2\,3\,4\,5) = (1\,2)(2\,3)(3\,4)(4\,5)$

Proof First write π as the product of (disjoint) cycles. Then write

$$(a_1 a_2 \dots a_k) = \underbrace{(a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k)}_{k-1 \text{ transpositions}}$$

Note: $o((1\,2)(2\,3)) = o(1\,2\,3) = 3$

Remark 1.12

A k cycle can be written as the product of $k-1$ transpositions.

Eg. $i = (1\,2)(1\,2)$ → for identity

but in any such product we use an <u>even</u> number of transpositions.

Defn The sign of the permutation π is $(-1)^k$ where k is the number of transpositions in some expression for π as the product of transpositions.

$\text{Sign}(\pi) = (-1)^k$

E.g In S_3 $i, (1\,2\,3), (1\,3\,2)$ sign $+1$ even

$(1\,2), (1\,3), (2\,3)$ -1 odd

Lemma 1.13

The function, sign: $S_n \to \{\pm 1\}$ is well defined: if $\pi = \tau_1 \dots \tau_k = \tau_1' \dots \tau_l'$ with transpositions then $(-1)^k = (-$

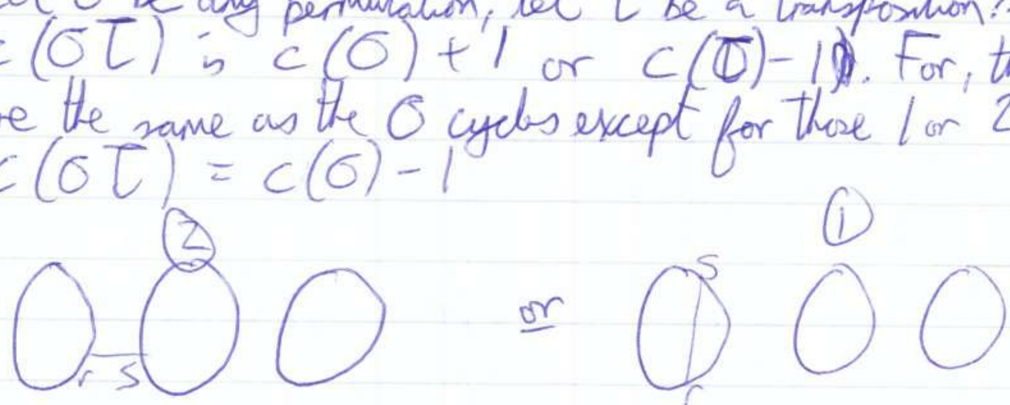
Proof Write $c(\pi)$ for the number of all cycles in the disjoint cycle expression for π including cycles of length 1.

E.g. $c(1) = n$

$c(k \text{ cycle}) = n - k + 1$

Claim Let σ be any permutation, let τ be a transposition say $\tau = (r\ s)$. $c(\sigma\tau)$ is $c(\sigma)+1$ or $c(\sigma)-1$. For, the $\sigma\tau$ cycles are the same as the σ cycles except for those 1 or 2 which contain r, s

$c(\sigma\tau) = c(\sigma) - 1$



In case 1, the cycle containing both r and s becomes the two $\sigma\tau$ cycl

In case 2, the cycles containing r, s become one $\sigma\tau$ cycle.

Case 1. $[(r, r+1 \dots s-1, s, s+1 \dots r-1)](r\ s)$
$= (r\ s+1 \dots r-1)(s\ r+1 \dots s-1)$

Case 2. $\underbrace{[(r\ r+1 \dots r-1)(s\ s+1 \dots s-1)]}_{\sigma}\underbrace{(r\ s)}_{\tau}$
$= (r\ s+1 \dots s-1\ s\ r+1 \dots r-1)$

Claim is proved.

It follows that $(-1)^{c(\sigma\tau)} = -(-1)^{c(\sigma)}$

Consider $\pi = \iota\tau_1\tau_2 \dots \tau_k = \iota\tau_1'\tau_2' \dots \tau_l'$

$$(-1)^{c(\pi)} = (-1)^{c(\iota\tau_1 \dots \tau_k)} = (-1)^{c(\iota)}(-1)^k$$
$$= (-1)^{c(\iota\tau_1 \dots \tau_l)} = (-1)^{c(\iota)}(-1)^l$$

8/10/10

Groups (5)

Recap

Sign of a permutation π is $\pi = (-1)^k$ where k is the number of transpositions with product π.

sign $S_n \to \{\pm\}$ is well defined.

If $\pi = \tau_1 = \tau_2 = \dots \tau_k = \tau_1' = \dots = \tau_l'$
with $\tau_i\ \tau_j$ $\quad (-1)^k = (-1)^l$

Proof write $c(\sigma)$ for the number of cycles in a disjoint cycle expression of σ. If τ is a transposition then $c(\sigma\tau) = c(\sigma) \pm 1$: for, if $\tau = (rs)$ then σ cycles and $\sigma\tau$ cycles are the same, except for those containg r, s.

If r, s are in the same σ cycle, that becomes two $\sigma\tau$ cycles.
If r, s are in two σ cycles this becomes one $\sigma\tau$ cycle.

Hence $(-1)^{c(\pi)} = (-1)^{c(i\tau_1\tau_2 \dots \tau_{k-1}\tau_k)} = (-1)^{c(i\tau_1 \dots \tau_{k-1})}(-1)$
$= (-1)^{c(i)}(-1)^k$

Similarly for $\tau_1'\tau_2' \dots \tau_{l-1}'\tau_l'$ $\quad (-1)^{c(\pi)} = (-1)^{c(i)}(-1)^l$
$(-1)^k = (-1)^l$

$k \equiv l \mod 2$

Remark 1 Perhaps more natural to use index of π
$\mathrm{ind}(\pi) = n - c(\pi) \qquad \pi \in S_n$
e.g. $\mathrm{ind}(1) = 0 \qquad \mathrm{ind}(\tau) = 1$
reflects better the "complexity" of π

$(-1)^{a+b} = (-1)^a(-1)^b$

Mod 2 arithmetic $a \equiv 0$ if a is even, $a \equiv 1$ if a is odd

+mod 2	0	1
0	0	1
1	1	0

Definition If $\pi \in S_n$ say π is an even permutation if $\mathrm{sgn}(\pi) = +1$ otherwise, $\mathrm{sgn}(\pi) = -1$ and π is odd.

Lemma 1.14 $\operatorname{sgn}(\sigma_1 \circ \sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$

Proof If $\sigma_1 = \tau_1 \tau_2 \ldots \tau_k$, $\sigma_2 = \tau_1' \tau_2' \ldots \tau_l$

Then $\sigma_1 \sigma_2 = \tau_1 \ldots \tau_k \tau_1' \ldots \tau_l'$, a product of $k+l$ transpositions

So $\operatorname{sgn}(\sigma_1\sigma_2) = (-1)^{k+l} = (-1)^k(-1)^l = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$

Note Even × Even = Even
Odd × Odd = Even
Even × Odd = Odd

Corollary 1.15 The set of all even permutations of the set X forms a group, $\operatorname{Alt}(X)$, the alternating group on X.
If $|X| = n$, with $A_n = \operatorname{Alt}(X)$, $|A_n| = \frac{n!}{2}$ $n > 1$

Proof $\sigma_1, \sigma_2 \in A_n$ $\sigma_1 \circ \sigma_2 \in A_n$
It is associative, proved in S_n earlier. $i \in A_n$
And, if $\sigma \in A_n$ then the inverse permutation is even.
$\operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(i) = +1$
So $\operatorname{sgn}(\sigma) = +1 \Rightarrow \operatorname{sgn}(\sigma^{-1}) = +1$

Finally, let τ be an odd permutation, fixed, e.g. $\tau = (1\,2)$
Then the mapping

$$\left\{\begin{matrix}\text{all even} \\ \text{permutations of } X\end{matrix}\right\} \Rightarrow \left\{\begin{matrix}\text{all odd permutations} \\ \text{of } X\end{matrix}\right\}$$
$$\sigma \Rightarrow \sigma\tau$$

So half of all permutations of X are even, the other half odd.
So $|A_n| = \frac{1}{2} S_n = \frac{n!}{2}$

Eg. A_4 ; $|A_4| = 12$

$(12)(34)$	(123)	(321)
$(13)(24)$	(124)	(421)
$(14)(23)$	(134)	(431)
	(234)	(432)

Groups (5)

Remark 1·16 Cycles of even length are odd permutations
$\quad\quad\quad\quad\quad\quad\quad\quad$ odd $\quad\quad\quad\quad$ even
(k cycles can be written as products of $k-1$ transpositions)

So a permutation is odd if and only if the number of cycles of even length in its disjoint cycle expression is odd.

An alternative definition of sign:

Definition: Given σ in S_n, let $x_1, \dots x_n$ be n distinct integers.
Define $\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{x_{\sigma(j)} - x_{\sigma(i)}}{x_j - x_i}$ $\quad\quad \frac{x_{\sigma(j)} - x_{\sigma(i)}}{x_j - x_i}$

$n=3$, $\sigma = (123)$, $x_i = i$

$$\varepsilon(\sigma) = \frac{3-2}{2-1} \, \frac{1-2}{3-1} \, \frac{1-3}{3-2} = 1 \times (-1) \times (-1) = +1$$

Lemma 1·17 $\varepsilon(\sigma) = \pm 1$, independent of the x_i used to define it.

In $\varepsilon(\sigma) = (-1)^{N(\sigma)}$ where $N(\sigma) = \# \{ i<j \mid \sigma(i) > \sigma(j)$ (pure)

Proof For each $r < s$, exactly one of $x_r - x_s$ and $x_s - x_r$ appears on top [only $x_s - x_r$ appears in the denominator]

if $\sigma^{-1}(r) < \sigma^{-1}(s)$, it is $x_s - x_r$ that appears
if $\sigma^{-1}(s) < \sigma^{-1}(r)$, it is $x_r - x_s$
Hence the assertion.

Lemma 1·18 For σ, π in S_n, $\varepsilon(\sigma \circ \pi) = \varepsilon(\sigma)\varepsilon(\pi)$

Proof $\varepsilon(\sigma\pi)$

$$= \prod_{i<j} \frac{\sigma\pi(j) - \sigma\pi(i)}{j-i} = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j-i} \prod_{i<j} \frac{\sigma\pi(j) - \sigma\pi(i)}{\sigma(j) - \sigma(i)}$$

$= \varepsilon(\sigma)\varepsilon(\pi)$ since taking $x_i = \sigma(i)$ have
$x_{\pi(i)} = \sigma[\pi(i)]$

10/10

Groups ⑤

If $\tau = (k, l)$ then $N(\tau) = 2(l-k-1)+1$

so $\Sigma(\tau) = -1$

$\# \{ i<j \mid \tau(i) > \tau(j) \}$

The only (i,j) contributing are those with $i = k < j < l$

or $i < k < j = l$

or $i = k, j = l$

<u>Back to general theory</u>

<u>Definition</u> The subset H of G is a <u>subgroup</u> of the group $(G, *)$ (if H is a group with respect to $*$ restricted to H).

i) If $h_1, h_2 \in H$ then $h_1 * h_2 \in H$ — closure

$e \in H$ — identity

if $h \in H$ then its inverse is in H — inverse

associativity is ~~~~ inherited

$H \leq G$

Eg $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$

$(\{\pm 1\}, \times) < (\mathbb{Q} \setminus \{0\}, \times)$

Note: operation must match

Eg. $A_n < S_n$

If $(G, *)$ is a group, $g \in G$

$\langle g \rangle = \{ g^i \mid i \in \mathbb{Z} \}$ is a subgroup of G, the cyclic subgroup generated by g

This is the smallest subgroup of G containing g.

E.g. $\langle (123) \rangle \leq S_3$

$= \{ i, (123), (132) \}$

More generally, if $g_i \in G$ for $i \in I$, some indexing set

$\langle g_i \mid i \in I \rangle \leq G$ is the smallest subgroup of G containing all g_i, $i \in I$

in fact

$$\langle g_i \mid i \in I \rangle = \bigcap_{\substack{H \leq G \\ g_i \in H \ \forall i \in I}} H$$

Defn G is generated by $\{g_i \mid i \in I\}$

if no proper subgroup contains all g_i $H < G$

E.g. $S_n = \langle (i\,j) \mid 1 \leq i < j \leq n \rangle$

Exercise S_n is also generated by 2 elements $= \langle (1\,2), (1\,2 \ldots n) \rangle$

Homomorphisms

A mapping θ from $(G_1, *_1)$ to $(G_2, *_2)$ is a homomorphism if for all $a, b \in G_1$

$$\theta(a * b) = \theta(a) * \theta(b)$$

Eg. $\operatorname{sgn} : S_n \to \{\pm 1\}$
$(S_n, \circ) \quad (\{\pm 1\}, \times)$

is a well defined homomorphism from S_n onto $(\{\pm 1\}, \times)$

e.g. $\operatorname{sgn}(\sigma \tau) = \operatorname{sgn}(\sigma) \operatorname{sgn}(\tau)$

Defn A bijective homomorphism $(G_1, *_1) \to (G_2, *_2)$ is an isomorphism.

E.g $G_1 = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{R} \right\}$ $*_1$ is matrix multiplication

$(G_2, *_2) = (\mathbb{R}, +)$

Then $\theta : G_1 \to G_2$ is an isomorphism. For this a bijection and

$$\theta\left[\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right] = \theta\left[\begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}\right] = a+b$$

$$= \theta\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} + \theta\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

E.g. $G_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a \in \mathbb{R}, a \neq 0 \right\}$ $*$ matrix multiplication

$(G_2, *_2) = \{\mathbb{R} \setminus \{0\}, \times\}$ $\quad \theta : G_1 \to G_2, \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mapsto a$

10/10/10

$\pi^i \pi^j = \pi^{i+j}$

Groups (5)

Consider the cyclic subgroup. $\langle \overbrace{(1 2 \ldots n)}^{\pi} \rangle \leq S_n$
it consists of $i, \pi, \pi^2, \pi^3 \ldots \pi^{n-1}$

Define $C_n = \{0, 1, \ldots, n-1\}$ under $+_n$ addition mod n

$$i + j = \begin{cases} i + j & \text{if in } C_n \\ i + j - kn & \text{otherwise, } k \in \mathbb{N} \end{cases}$$

This is a group, identity 0, inverse i is $n-i$

Then $\langle \pi \rangle \underset{\text{isomorphism}}{\cong} (C_n, +_n)$

$$\theta : \pi^i \mapsto i$$
$$\langle \pi \rangle \to C_n$$

22/10/10 $\theta(a * b) = \theta(a) * \theta(b)$

Groups ⑦

<u>Lemma 1.21</u> i) $i : (G, *) \to (G, *)$ is an isomorphism

ii) If $\theta : (G_1 *_1) \to (G_2 *_2)$ is an isomorphism then $\theta^{-1} : (G_2 *_2) \to (G_1 *_1)$ is an isomorphism

iii) If $\theta : (G_1 *_1) \to (G_2 *_2)$ and $\varphi : (G_2 *_2) \to (G_3 *_3)$ are isomorphisms (or homomorphisms) then $\varphi \circ \theta$ is an isomorphism (or homomorphism)

Thus $G_1 \simeq G_2 \Rightarrow G_2 \simeq G_1$

$G_1 \simeq G_2 \simeq G_3 \Rightarrow G_1 \simeq G_3$

so "Being isomorphic" is an equivalence relation.

<u>Proof</u> i) is clear

ii) Let $c, d \in G_2$

then let $a, b \in G_1$ with $\theta(a) = c$, $\theta(b) = d$

$\theta^{-1}(c *_2 d) = \theta^{-1}[\theta(a) *_2 \theta(b)] = \theta^{-1}\theta(a *_1 b) = a *_1 b$

iii) Let $a, b \in G_1$. Then $\varphi\theta(a *_1 b) = \varphi[\theta(a) *_2 \theta(b)]$
$= \varphi\theta(a) *_3 \varphi\theta(b)$

φ, θ are homomorphisms, so is $\varphi\theta$.

<u>Remark 1.22</u> A group $(G *)$ is a cyclic group if $\exists x \in G$ such that all elements in G are powers of x. Any two cyclic groups of the same order are isomorphic.

$G = \langle x^i \mid i \in \mathbb{Z} \rangle$ Note, if $O(x)$ is finite, say $O(x) = n$
$G \simeq C_n \left[\begin{smallmatrix} \{0, 1, \dots, n-1\} \\ * = +_n \end{smallmatrix} \right]$

If $O(x)$ is infinite then $(G, *) \simeq (\mathbb{Z}, +)$ cyclic, generator 1

<u>Justification</u>: Let $\theta : G \to C_n$ [where $n = O(x)$]

$G = \{e, x, x^2, \dots, x^{n-1}\}$

Take $x^j \longmapsto j$

θ is a "well defined" isomorphism.

$j, k \in \{0, 1, \ldots, n-1\}$

If $x^j = x^k$ then $x^{j-k} = e$ $\quad o(x) = n$ so $n \mid j-k$
so $j \equiv k \bmod n$ (same element in C_n).

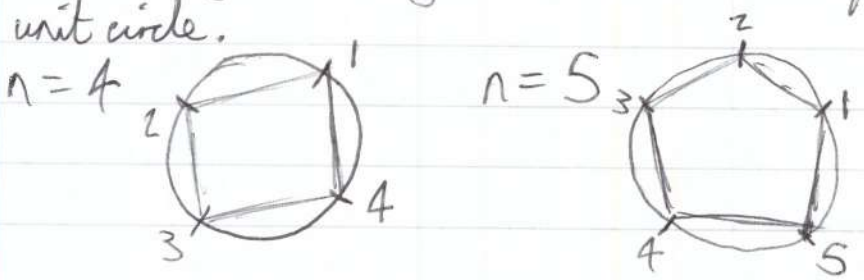
Also θ is bijective, ~~so~~ check.
And θ is a homomorphism, $\theta(x^j \cdot x^k) = \theta(x^{j+k}) = j+k$
$= \theta(x^j) + \theta(x^k)$

However, if $o(x)$ is infinite, let $\theta : G \to \mathbb{Z}$, $x^j \mapsto j$
This is well defined for the same reason: $x^j = x^k$, $x^{j-k} = e$, $j-k = 0$
Bijective and homomorphic.

See Section (4) !

<u>Groups of symmetries of the regular n-gons</u> (dihedral groups D

Take a regular n-gon: n vertices ~~at equal distance~~ regularly distributed on the unit circle.



Symmetries: elements of the symmetry group S_n acting on vertices which do not destroy our n-gon.

E.g. $n = 4$ $\quad$ 4 rotations $i, \underbrace{(1\,2\,3\,4)}_{\sigma}, \sigma^2, \sigma^3$
4 reflections $\underbrace{(1\,2)(3\,4)}_{\tau}, \tau\sigma, \tau\sigma^2, \tau\sigma^3$

8 elements

These form $D_8 < S_4$ $\qquad |D_8| = 8$

(Composition of symmetries is a symmetry, inverse of a symmetry is a symmetry).

22/10/10

Groups ⑦

$n=5 \qquad \sigma = (1\,2\,3\,4\,5)$
$\qquad\qquad \tau = (3\,4)(2\,5)$

General n: $\sigma = (1\,2 \ldots n) \qquad o(\sigma) = n \quad n$ rotations
$\sigma^j \quad j \in \{0,1,\ldots,n-1\}$ forming a cyclic subgroup order

$\tau = (1)(2\ n)(3\ n-1)$ etc

$D_{2n} = \{\sigma^j, \tau\sigma^j \mid j \in \{0,\ldots,n-1\}\}$

<u>Note</u> $\sigma^n = i, \quad \tau^2 = i$
$\sigma\tau = \tau\sigma^{-1}$
$\tau\sigma\tau = \sigma^{-1}$

$\tau = \tau^{-1}$
$\sigma\tau = \sigma\tau^{-1} = (\tau\sigma^{-1})^{-1}$

In general, if a group $(G\ *)$ is generated by two elements s and t, such that $o(s)=n$, $o(t)=2$ and $tst = s^{-1}$

then $|G| = 2n \quad G = \{e, s, \ldots s^{n-1}, t, ts, \ldots ts^{n-1}\}$

For $\langle s,t \rangle = G \qquad s^i t = t s^{-i}$

25/10/10

Groups (8)

Subgroups, cosets, Lagrange's Theorem

~~Lemma~~. If $(G,*)$ is finite, then H is a subgroup then H is a subgroup if $H \neq \emptyset$ and $h_1 * h_2 \in H$.

Lemma 2·1 If $(G *)$ is a group and $H \subseteq G$, then H is a subgroup if $H \neq \emptyset$ and if $a, b \in H$, then $a^{-1} * b \in H$.

Proof Let $a \in H$. Then $e = a^{-1} * a \in H$ $(b=a)$. Also, $a^{-1} = a^{-1} * e \in H$ $(a, b=e)$

Finally, if $a, b \in H$, then $a^{-1} \in H$, so $a * b = (a^{-1})^{-1} * b \in H$

Theorem 2·2 Lagrange If H is a subgroup of the finite group G, then $|H|$ divides $|G|$.

eg. $|G| = 6$. $G = S_3$, Subgroups H order

$H = S_3$ 6

$H = \langle(123)\rangle$ 3

$H = \langle(12)\rangle \langle(13)\rangle \langle(23)\rangle$ 2

$H = i$

Definition: If $H \leq G$, $g \in G$ ~~then let~~ $gH = \{g*h \mid h \in H\}$ the $\boxed{\text{left coset}}$

Lemma 2·3 Let $H \subseteq G$; all left cosets ~~of~~ of H in G have the same size $|H|$.

Proof Define $\theta : H \to gH$, $h \mapsto g*h$. This is a well defined mapping. $g \in G$
It is injective $(gh_1 = gh_2 \Rightarrow h_1 = h_2)$
and surjective. So $|H| = |gH|$ as there is a bijection between them.

Lemma 2·4 Let $H \leq G$. The distinct left cosets of H in G form a partition of G:

(evident) i) any $g \in G$ is in some left coset of H — eg in gH.

ii) if ~~$aH \cap bH$~~ $aH \cap bH \neq \emptyset$ for some $a, b \in G$ then $aH = bH$

Proof of ii) Claim: if $c \in aH$ then $cH = aH$
For, let $c = ah_1$; for any $h \in H$
$ch = ah_1 h \in aH$, so $cH \subseteq aH$
And, $a = ch_1^{-1} \in cH$, so $aH \subseteq cH$ by previous line.

Thus, if $c \in aH \cap bH$, then $aH = cH = bH$ as required.

<u>Proof of 2·2</u> G is partitioned into distinct left cosets of H and all these have the same size $|H| \Rightarrow |H| \mid |G|$

Definition If $H \leq G$, the index $|G:H|$ is the number of distinct left cosets of H in G. $|G:H| = \frac{|G|}{|H|}$.

Remark Converse of Lagrange's Theorem is false.
Eg: A_4 has no subgroup of order 6, A_5 has no subgroup of index 2, 3, 4.

Note (But Sylow's Theorem says that if $|G| = p^a m$ with $p \nmid m$, p a prime then G has subgroups of order p^a.

$\overline{\mathbb{D}}$

25/10/10

Groups (8)

<u>Theorem 2·5</u> If g is an element of the finite group G then $o(g) \mid |G|$
Thus $g^{|G|} = e$.

<u>Proof</u> Let $\langle g \rangle = \{e, g, \ldots, g^{n-1}\}$, where $n = o(g)$
$\subseteq G$
$|\langle g \rangle| = o(g) \mid |G|$ by 2·2.

Thus, if $|G| = q \cdot o(g)$ $q \in \mathbb{Z}$
then $g^{|G|} = (g^{o(g)})^q = e^q = e$.

<u>Corollary 2·6</u> If G is a group of prime order p, then G is cyclic (and hence $G \cong C_p$). In fact G is generated by any of its non identity elements.

<u>Proof</u> Let $g \in G$, $g \neq e$. Then $\langle g \rangle \subseteq G$. Its order divides p, so $o(g)$ must be p. So $|\langle g \rangle| = p$, so $G = \langle g \rangle$.

Returning to the example: $G = S_3$, $|G| = 6$

$H \subseteq G$	
order 6	S_3
order 3	$\langle (123) \rangle$ only one such
order 2	$\langle (12) \rangle, \langle (13) \rangle, \langle (23) \rangle$ 3 such
order 1	i

$gH = \{g * h \mid h \in H\}$

<u>Back to left cosets of H in G</u> $[H \subseteq G]$.
H is one of the left cosets. In fact $gH = H$ if and only if $g \in H$.

Note: $aH = bH$ if and only if $a^{-1}b$ lies in H.
$\Rightarrow$ For, if $b = ah$, then $h = a^{-1}b \in H$.
If $a^{-1}b \in H$, for some h, then $b = ah \in aH$
$\Leftarrow$

Eg $H = \langle (12) \rangle \subseteq G = S_3$

the set of left cosets $\to (G:H)$: $H,\ (123)H,\ (132)H$

$\{i,(12)\}\ \ \{(123),(13)\}\ \ \{(132),(23)\}$

<u>Definition</u> If $H \subseteq G$, $g \in G$ then the <u>right coset</u>
$Hg = \{hg \mid h \in H\}$

<u>Remark 2.2'</u> If G is finite, $H \subseteq G$, then G is partitioned into the distinct right cosets, and they all have the same size as H.

Ex $\#\{\text{left cosets of } H \text{ in } G\} = \#\{\text{right cosets of } H \text{ in } G\}$
Find a natural bijection.

E.g. $H = \langle (12) \rangle < G = S_3$
Then three right cosets are : $H,\ H(123),\ H(132)$.
$\{i,(12)\}\ \ \{(123),(23)\}\ \ \{(132),(13)\}$

Note $aH = bH$ if and only if $a^{-1}b \in H$
$Ha = Hb$ if and only if $ba^{-1} \in H$

27/10/10

Groups (9)

Recall $aH = bH$ iff $a^{-1}b \in H$

Alternatively: Define a relation on G by $a \equiv b$ if $a^{-1}b \in H$.

Claim $\equiv$ is an equivalence relation.

Reflexive	$a^{-1}a \in H$, so $a \equiv a$
Symmetric	$a \equiv b \Leftrightarrow a^{-1}b \in H \Leftrightarrow b^{-1}a \in H \Leftrightarrow b \equiv a$
Transitive	$a \equiv b \equiv c \Rightarrow a \equiv c$
	$a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$

Equivalence classes partition the set G. Here they are the left cosets of H in G.

An application in Number Theory:

Recall $C_n = \{0, 1, \dots, n-1\}$ under $+_n$

Fix $n \in \mathbb{N}$. On $\mathbb{Z}$, define $a \equiv b \mod n$ if $n \mid a-b$

This is an equivalence relation.

The classes are $[0], [1], \dots, [n-1]$

So could take $C_n = \{[0], [1], \dots, [n-1]\}$

with addition $[a] + [b] = [a+b]$

Let $C_n^* = \{ [a] \mid (a,n) = 1 \}$ "units" mod n

$= \{ 1 \leq a \leq n \mid (a,n) = 1 \}$

Define multiplication mod n:

$[a] \times_n [ab]$

This is well defined

$[a], [b] \in C_n^* \Rightarrow (a,n) = 1 = (b,n)$

$\Rightarrow (ab, n) = 1 \Rightarrow [a] \times_n [b] \in C_n^*$

And, if $[a_1] = [a_2]$ and $[b_1] = [b_2]$ then $[a_1 b_1] = [a_2 b_2]$

$a_2 = a_1 + qn$, $b_2 = b_1 + q'n$, then

$a_2 b_2 = (a_1 + qn)(b_1 + q'n) = a_1 b_1 + (qb_1 + q'a_1 + qq')n \in \mathbb{Z}$

Lemma 2.8 $C_n^* = \{[a] \mid (a,n) = 1\}$ is a group under multiplication mod n. $n \in \mathbb{N}$

$[a] \times_n [b] = [ab]$

Proof Well defined, closed. ✓

Associative, as multiplication in $\mathbb{Z}$ is associative. The identity is $[1]$.

Inverses exist: let $[a] \in C_n^*$

since $(a,n) = 1$, $\exists r, s \in \mathbb{Z}$, $ar + ns = 1$

Hence $[a] = [r]^{-1}$ since $ar \equiv 1 \mod 1$

Also, it is abelian.

The order of C_n^*:

Euler Totient Function

$\varphi(n) = \# \{a \in \mathbb{Z} \mid 1 \leq a \leq n, (a,n) = 1\}$

e.g. $n = p$, a prime $\varphi(p) = p - 1$

$n = 4$, $\varphi(4) = 2$

$|C_n^*| = \varphi(n)$

Theorem 2.9 (Fermat Euler) If $n \in \mathbb{N}$, $a \in \mathbb{Z}$ with $(a,n) = 1$ then $a^{\varphi(n)} \equiv 1 \mod n$

Proof Lagrange's Theorem: $[a]^{\varphi(n)} = [1]$ in C_n^*

$a^{\varphi(n)} \equiv 1 \mod n$

27/10/10

Groups (9)

Corollary (Fermat's Little Theorem)
If p is a prime, $a \in \mathbb{Z}$ with $p \nmid a$, the $a^{p-1} \equiv 1 \mod p$

e.g. $p = 101$ $53^{100} \equiv 1 \mod 101$

<u>Small Groups</u> (either small order or elementary structure)
<u>Cyclic groups</u>
Recall: G is cyclic if for some $x \in G$
all elements of G are just powers of X.
Remark: If G is finite, G is cyclic iff there exists $x \in G$ with $o(x) = |G|$

If G is cyclic, generated by x, if $o(x) = n$, then $G \cong (C_n, +_n)$
if $o(x)$ is not finite, $G \cong (\mathbb{Z}, +)$

Lemma 3.1 Any subgroup H of the cyclic group G is cyclic.
If G is generated by x, $H = \langle x^k \rangle$ $H \neq \{e\}$
where k is least positive integer with $x^k \in H$.
<u>Proof</u> Ex 2/6
<u>~~Corollary~~</u> Remark 3.2
Let $a, b \in \mathbb{Z}$, consider the subgroup generated by a and b in $(\mathbb{Z}, +)$
Now an subgroup of $(\mathbb{Z}, +)$ is cyclic so $\langle a, b \rangle = \langle c \rangle$ for some $c \in \mathbb{N}$, Then $c = (a, b)$.
And $c \in \langle a, b \rangle$, so for some $r, s \in \mathbb{Z}$, ~~$c = ab$~~
$c = ra + sb$

3

Direct Product of Groups

Let H, K be groups.

Let $H \times K$ be $\{(h, k) \mid h \in H, k \in K\}$

This is a group with respect to $(h_1, k_1)(h_2, k_2) = (\underset{\text{in } H}{h_1 h_2}, \underset{\text{in } K}{k_1 k_2})$

This is a group, the new product is well defined, associative,

identity $e_{H \times K} = (e_H, e_K)$

inverse $(h, k)^{-1} = (h^{-1}, k^{-1})$

E.g. $\mathbb{R} \times \mathbb{R} \times \dots \times \mathbb{R} = \mathbb{R}^n$ group (abelian under componentwise addit

$(C_2, +_2), (C_3, +_3)$

$C_2 \times C_3 \simeq C_6$ e.g. generated by $(1, 1)$

29/10/10

Groups (10)

<u>Remark 3·4</u> i) $H \times K$ is abelian iff both H and K are

ii) $|H \times K| = |H|\,|K|$

iii) $H \times K$ contains a subgroup $\{(h, e_K) \mid h \in H\} \simeq H$ and $\{(e_H, k) \mid k \in K\} \simeq K$

The two subgroups intersect in $\{e\}$

Also $(h, e_K)(e_H, k) = (h, k) = (e_H, k)(h, e_K)$.

<u>Lemma 3·5</u> Let G be a group with subgroups H and K such that

1. Each element $g \in G$ can be written as $g = hk$ for some $h \in H$, $k \in K$
2. $H \cap K = \{e\}$
3. $hk = kh$ for all $h \in H$, $k \in K$

Then $G \simeq H \times K$

<u>Proof</u> If $h_1 k_1 = h_2 k_2$ then $h_1 = h_2$, $k_1 = k_2$

$h_2^{-1} h_1 = k_2 k^{-1} \in H \cap K = \{e\}$

So $h_1 = h_2$, $k_1 = k_2$

Define $\theta : G \to H \times K$ $\quad hk \mapsto (h, k)$

This is well defined, by above, bijection.

It is a homomorphism: $\theta(h_1 k_1 ; h_2 k_2) = \theta(h_1 h_2 k_1 k_2)$

$(h_1 h_2, k_1 k_2) = (h_1 k_1)(h_2 k_2) = \theta(h_1 k_1)\theta(h_2 k_2)$

<u>Dihedral Groups</u>

Abstractly, we can define D_{2n} as a group generated by two elements s, t subject to the imposed relations. $s^n = e$, $t^2 = e$, $tst = s^{-1}$

Any such group has $2n$ elements:

$\{e, s, s^2, \ldots, s^{n-1}, t, ts, \ldots, ts^{n-1}\}$ $\quad$ shows st is listed as ~~ts~~ the term

and is isomorphic to the group of symmetries of a regular n-gon.

$\theta : t^i s^j \mapsto \tau^i \sigma^j$ is visibly an isomorphism

Similarly, we can define C_n to be the group generated by an element x with $x^n = e$.

Notation: $C_n = \langle x \mid x^n = e \rangle$

$$D_{2n} = \langle s, t \mid s^n = e, t^2 = e, tsts = e \rangle$$

Groups of order ≤ 8

Order	# groups up to isomorphism	Groups
1	1	$\{e\}$
2	1	C_2
3	1	C_3
4	2	$C_4, C_2 \times C_2$
5	1	C_5
6	2	C_6, D_6
7	1	C_7
8	— — — — — —	— — —

Proof Any group of prime order p is cyclic (corollary of Lagrange's Theorem)

$|G| = 4$ If G contains an element of order 4, then $G \simeq C_4$
Assume $G \not\simeq C_4$, so all non identity elements have order 2.
Let $a \neq b \in G \setminus \{e\}$
Then $G = \{e, a, b, ab\}$ and $ba = ab$
$G \simeq \langle a \rangle \times \langle b \rangle \simeq C_2 \times C_2$

$|G| = 6$ Assume G is not cyclic. Now G contains an element a of order 3 and an element a of order 2.
If all elements have order 2, take $b \neq c$, non identity. Then $\overset{bc}{\overset{\shortparallel}{(bc)^{-1}}} = c^{-1}b^{-1} = cb$ and $\{e, b, c, bc\} \subset G$ Contradiction to Lagrange.

(Exercise: If all elements $G \setminus \{e\}$ have order 2, G is abelian.)
If all elements of $G \setminus \{e\}$ have order 3:

29/10/10

Groups (10)

Take a, c, $\langle a\rangle \neq \langle c\rangle$ Then $\langle a\rangle \cap \langle c\rangle = e$
Then G contains $e, a, a^{-1}, c, c^{-1}, ac, (ac)^{-1}$ all distinct, not so.

(Exercise, if G is a group of even order, it contains an element of order 2)

Then $G = \{e, a, a^2, b, ba, ba^2\}$
Now ab is not a^i, not b. So ab is ba or ba^{-1}. In the former case, G is abelian, in fact C_6 (since $o(ab)=6$) - assumed not.

In the other case, $G = \langle a, b \mid a^3 = i = b^2, bab = a^{-1}\rangle \simeq D_6$

$|G| = 8$. Assume G is not C_8. If all non identity elements have order 2, then G is abelian.
So taking $a \in G\setminus\{e\}$, $b \in G \setminus \langle a\rangle$, $c \in G \setminus \langle a, b\rangle$
we see that

$$\langle a, b\rangle \simeq \langle a\rangle \times \langle b\rangle \simeq C_2 \times C_2$$

and $G \simeq \langle a, b\rangle \times \langle c\rangle \simeq (C_2 \times C_2) \times C_2 \simeq C_2 \times C_2 \times C_2$

Now let $a \in G$ of order 4, $b \in G \setminus \langle a\rangle$.

$ab = ba$
or
$ab = ba^{-1}$

$b^2 = e$
or
$b^2 = a^2$

?/11/10

Groups (11)

|G| order 8

G contains an element of order 8 $\quad C_8$

If all non-id elements have order 2 $\quad C_2 \times C_2 \times C_2$

Assume neither.

Let $a \in G$ order 4, $b \in G \setminus \langle a \rangle$

$$G = \{\underbrace{e, a, a^2, a^3}_{H = \langle a \rangle}, \underbrace{b, ba, ba^2, ba^3}_{bH}\}$$

Contrive to get bab^{-1} is a or a^{-1}.
b^2 is 1 or a^2.

$bab^{-1} = e,\ b^2 = 1 \Rightarrow C_4 \times C_2$
$b^2 = a^2 \not\Rightarrow$
$bab^{-1} = a^{-1}\ b^2 = 1 \Rightarrow D_8$
$bab^{-1} = a^{-1}\ b^2 = a^2 \not\Rightarrow$

|G| = 6

G contains an element of order 3, and one of order 2.

$$G = \{e, a, a^2, b, ba, ba^2\}$$
$ab = ba \rightarrow C_3 \times C_2 \simeq C_6$
$o(ab) = 6$
$ab = ba^{-1} \quad D_6$

Now $b^2 \in \langle a \rangle$ since $bH \neq b^2H$ so $b^2H = H$
If $b^2 = a$, $o(b) = 8$ not so.
$b^2 = e$ or a^2. ab is ba or ba^{-1}
otherwise $a = ba^2b^{-1}$ so $a^2 = (ba^2b^{-1})(ba^2b^{-1}) = e$ not so.

So four cases remain

i) $ab = ba$, $b^2 = 1 \Rightarrow G \cong \langle a \rangle \times \langle b \rangle \cong C_4 \times C_2$

ii) $ab = ba$, $b^2 = a^2$, then $|a^{-1}b| \neq 2$ so replace b by $a^{-1}b$

iii) $bab^{-1} = a^{-1}$, $b^2 = 1$ $\quad G \cong D_8$

iv) $bab^{-1} = a^{-1}$ $b^2 = a^2$ $\quad G \cong Q_8 \rightarrow$ Quaternion group order 8

all elements of G other than a^2 have order 4, so not D_8.

$$Q_8 = \langle a, b \mid a^4 = e, b^2 = a^2, bab^{-1} = a^{-1} \rangle$$

Usual notation (Hamilton)

$-1 = i^2 = j^2 = k^2 = ijk$

We can also write Q_8 as a group of eight 2×2 complex matrices

$\underline{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\quad \underline{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ $\quad \underline{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ $\quad \underline{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

Remark 3.9 $\mathbb{H} = \{ \alpha \underline{1} + \beta \underline{i} + \mu \underline{j} + \delta \underline{k} \mid \alpha, \beta, \mu, \delta \in \mathbb{R} \}$

a 4 dimensional vector space over $\mathbb{R}$, with multiplication which is associative but not commutative. The quaternion algebra.

Remark 3.10 $|G| = 8$ (general n?). Consider first the abelian groups, these are always direct products of cyclic groups (Groups, Rings and Modules IB). Then consider the non abelian groups - harder but more interesting.

Note G order n is cyclic $\Leftrightarrow$ G contains an element of order n.
G is dihedral of order $2n$ if there is an element a of order n inverted by an element of order 2. $bab^{-1} = a^{-1}$

Groups (II)

4. Actions

We have subgroups of symmetric groups $Sym(X)$.
These are permutation groups on X. Here we start from an abstract group and look to embed it into $Sym(X)$.

<u>Defn</u> Let $(G, *)$ be a group, X a nonempty set. We say G acts on X if there is a mapping $\rho : G \times X \Rightarrow X$
$$(g, x) \mapsto g(x)$$
satisfying:
0) $g(x) \in X$
1) $(g * h)(x) = g(h(x))$
2) $e(x) = x$ for all $x \in X$, $g, h \in G$

<u>Lemma 4.1</u> Fix $g \in G$, where G acts on X. Then $\theta_g : X \Rightarrow X$, $x \mapsto g(x)$ is a permutation.

<u>Proof</u> The inverse of θ_g is $\theta_{g^{-1}}$ because $g^{-1}(g(x)) = (g^{-1}g)(x) = e(x) = x$
Must be a bijection $\Rightarrow$ is a permutation.

<u>Lemma 4.2</u> Let G act on X. The mapping $\theta : G \Rightarrow Sym(X)$, $g \mapsto \theta_g$ is a homomorphism, ~~a permutation repres~~ a permutation representation of G.

<u>Proof</u> If $g \in G$, then $\theta_g \in Sym(X)$. Check θ is a homomorphism.
$\theta(g_1 g_2) = \theta_{g_1 g_2} = \theta_{g_1} \circ \theta_{g_2}$: Let $x \in X$.
$\theta_{g_1 g_2}(x) = (g_1 g_2)(x) = g_1(g_2(x)) = \theta_{g_1} \circ \theta_{g_2}(x)$

E.g. $G = D_8$, $G < Sym(X)$ where X is the set of vertices of a square. Certainly G acts on X. Let Y = set of edges of our square. Then G acts on Y also.

Orbits and Stabilisers

Defn The action G on X is <u>transitive</u> if for any $x_1, x_2 \in X$ there is a $g \in G$ with $g(x_1) = x_2$.

Defn If G acts on X, let $x \in X$. The orbit of G on X containing x is $G(x) = \{g(x) \mid g \in G\}$

Note: G is transitive on the set $X \Leftrightarrow \cancel{X} = G(x)$ for $x \in X$

23/11/10

Groups (12)

Homomorphism $\Theta : G \to Sym(X)$

$g \mapsto \Theta_g = g^x$

$(G, *)$ acts on X if there is a mapping

$G \times X \to X$

$(g, x) \to g(x)$

such that 0) $g(x) \in X$

1) $(g_1 * g_2)(x) = g_1(g_2(x))$

2) $e(x) = x$

Then $x \in X$, $g, g_1, g_2 \in G$

Action is transitive if for $x_1, x_2 \in X$, there exists $g \in G$ with $g(x_1) = x_2$

orbit of $x \in X$ is $G(x) = \{ g(x) \mid g \in G \}$

G transitive iff $G(x) = X$ for $x \in X$.

Lemma 4.3 Let G act on X. Each G orbit $G(x)$ is G-invariant:

$g(G(x)) = G(x)$ for $g \in G$

and G is transitive on $G(x)$. The distinct G orbits form a partition of X.

Proof $G(x)$ is G-invariant.

if $g, g' \in G$ then $g'(g(x)) = (g'g)(x) = G(x)$

So G acts on $G(x)$; it is transitive.

If $x_1, x_2 \in G(x)$, let $g_1(x) = x_1$, $g_2(x) = x_2$ $(g_i \in G)$

Then $g_2 g_1^{-1}(x_1) = x_2$ so G is transitive on $G(x)$. To see the final claim, define relation $\sim$ on X by $x_1 \sim x_2$ if $x_2 = g(x_1)$ for some $g \in G$. This is an equivalence relation, the $\sim$ classes form the ~~orbits~~ G orbits and form a partition of X.

Define If G acts on X, the stabiliser of the point x in G is G_x

$G_x = \{ g \in G \mid g(x) = x \}$

1

E.g. $G = D_8$, $X = \{\text{vertices of square}\}$ ↗ or regular n-gon

Let $x = 1$.

Then $G_x = \langle \tau \rangle$ $\qquad \tau = (1)(2\,n)(3\;n-1)\ldots$

Lemma 4.4 If G acts on X, and $x \in X$, the stabiliser G_x is a subgroup of G $\quad G_x \leq G$

Proof First, $e \in G_x$. If $g_1, g_2 \in G_x$, so does $g_1^{-1} g_2$

$g_1(x) = x = g_2(x)$

$(g_1^{-1} g_2)(x) = g_1^{-1}(g_2(x)) = x \qquad g_1^{-1} g_2 \in G_x$

$G(x) = \{ g(x) \mid g \in G \}$

$G_x \leq G$

$\;\;\| \; \{ g \mid g(x) = x \}$

Theorem 4.5 Orbit - Stabiliser Theorem.

Let G act on X, $x \in X$. Then

$$|G| = |G(x)|\,|G_x|$$

In particular, if G is transitive on X then $|G| = |X|\,|G_x|$

E.g. D_{2n} of symmetries on a regular n-gon has order $2n$. It is transitive on the set X of vertices, $|X| = n$ and

$G_1 = \langle (1)(2\;n)(3\;n-1)\ldots \rangle$ order 2.

Proof $G_x \leq G$. Consider the set $(G : G_x)$ of left cosets of G_x in G.

Now $\varphi : (G : G_x) \to G(x) \quad \subseteq X$

$\qquad g G_x \longmapsto g(x)$

φ is a well defined bijection:

If $g G_x = g' G_x$ then $g^{-1} g' \in G_x$, so $(g^{-1} g')(x) = x$

Hence $g'(x) = g(x)$. So φ is well defined.

23/11/10

Groups ⑫

Reverse steps (carefully) to show injectivity.
It is surjective because any $y \in Gx$ is $g(x)$ for some g so $gG_x \mapsto y$

E.g. $(G, *)$ any group, $X = G$
The left regular action of G on X
$g^X : x \longmapsto g * x$ for $x \in X = G, g \in G$
This ~~gives~~ action gives a permutation g^X for each $g \in G$.
This gives a homomorphism $\theta : G \to \mathrm{Sym}(G)$

<u>Definition</u> The kernel of the action of G on X is

$\bigcap_{x \in X} G_x$ (the part of the group acting trivially on X).
The action of G on X is faithful if $\bigcap_{x \in X} G_x = \{e\}$

<u>Theorem 4.6</u> (Cayley) Any group G is isomorphic to a subgroup of a symmetry group namely $\mathrm{Sym}(G)$.

<u>Proof</u> The left regular action of G on $X = G$ gives a homomorphism $\theta : G \to \mathrm{Sym}(G)$. This is injective:
if $g^X = e$ then $gx = x$ for all $x \in X$ so $g = e$. Thus $\theta^0 : G \to \theta(G) \leq \mathrm{Sym}(G)$ is an isomorphism onto $\theta(G)$ of $\mathrm{Sym}(G)$

3

E.g. 4.7 The left coset action of G on the set of the left cosets of $H \subseteq G$.

Let $H \subseteq G$, $X = (G : H)$, the set of left cosets of H in G.

For $g \in G$, xH with $x \in G$

$$g : xH \mapsto gxH$$
$$X \to X$$

25/11/10

Groups (13)

E.g. 4.8 $(G, *)$ is a group, $H \leq G$
Let $X = (G:H)$, the set of left cosets of H in G. Then G acts on X via the left coset action.
$G \times X \Rightarrow X$
$(g, xH) \mapsto (g*x)H \quad \in X$

This is well defined
Check: if $x_1 H = x_2 H$ then also $(gx_1)H = (gx_2)H$,
1) For if $x_1^{-1}x_2 \in H$, then $\underbrace{(gx_1)^{-1}(gx_2)}_{=x_1^{-1}x_2} \in H$? well defined
And $(g*x)H \in X$ for $g \in G$, $xH \in X$

2) $(g_1 g_2) xH = ((g_1 g_2)x)H = g_1(g_2(xH))$
3) $e(xH) = xH$ for all xH

The action is transitive: to get from $x_1 H$ to $x_2 H$, let $g = x_2 x_1^{-1}$; then $g(x_1 H) = x_2 H$.
The stabiliser of the "point" $H \in X$ is H.
The stabiliser of the point xH is $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$
$(xhx^{-1})(xH) = xh(x^{-1}xH) = x(hH) = xH$.

Conjugation
Lemma 4.10 Let G be a group, let $X = G$, the set of elements of G.
Define an action: $G \times X \Rightarrow X$, $(g, x) \mapsto g(x) = gxg^{-1}$
This is an action - conjugation action of G.
Proof. Certainly a mapping from $G \times X \Rightarrow X$.
And $(g_1 g_2)(x) = g_1 g_2 x (g_1 g_2)^{-1} = g_1(g_2 x g_2^{-1})g_1^{-1}$
$= g_1(g_2(x))$
and $e(x) = x$ for $x \in X$, so $e: X \Rightarrow X$.

The orbits in the conjugation action are the conjugacy classes.
If $x \in X$, we write $ccl_G(x) = \{gxg^{-1} \mid g \in G\}$
The stabiliser of x is $C_G(x) = \{g \in G,\ gx = xg\}$
all g which commute with given x
centraliser of $x \in G$

<u>Corollary 4.11</u> If G is a finite group, $x \in G$, then $|G| = |ccl_G(x)||C_G(x)|$
<u>Proof</u> Follows from orbit-stabiliser theorem.

The kernel of the conjugation actions of G:

$\bigcap_{x \in G} G_x = \bigcap_{x \in G} C_G(x)$ the centre of G denoted by $Z(G)$
$Z(G) = \{z \in G \mid zx = xz\ \forall x \in G\}$
G is abelian if $Z(G) = G$.

$g \in G$, $g \in Z(G)$ iff $ccl_G(g) = \{g\}$

E.g. $G = D_8$ $|G| = 8$ $G = \langle \sigma, \tau \mid \sigma^4 = i = \tau^2, \tau\sigma\tau^{-1} = \sigma$

$ccl_G(x)$	$\{i\}$	$\{\sigma^2\}$	$\{\sigma, \sigma^{-1}\}$	$\{\tau\sigma, \tau\sigma^{-1}\}$	$\{\tau, \tau\sigma^2\}$
$C_G(x)$	G	G	$\langle \sigma \rangle$	$\langle \tau\sigma, \sigma^2 \rangle$	$\langle \tau, \sigma^2 \rangle$

<u>Remark 4.11</u> Any two conjugate elements of G have the same order:
if $x^n = e$, $(gxg^{-1})^n = gxg^{-1}gxg^{-1} \dots gxg^{-1} = gx^ng^{-1} = gg^{-1}$
And vice versa $(gxg^{-1})^n = e \Rightarrow x^n = e$

~~Conjugac~~

15/11/10

Groups (13)

Conjugacy classes in S_n

If $\pi \in S_n$ is written in disjoint cycle notation (including cycles of length 1) the <u>type</u> of π is defined to be $(n_1\ n_2\ ..\ n_k)$ where π has cycles of length $n_1 \geq n_2 \geq .. \geq n_k > 0$ $\quad n = n_1 + n_2 + \dots + n_k$

E.g. $n=6$ $\quad (123)(46)(5)$ $\quad$ type $(3,2,1)$

$\qquad i$ $\quad$ type $(1,1,1,1,1,1) = (1^6)$

Theorem 4.13

Two permutations of S_n are conjugate in S_n iff they have the same type.

3

28/11/10

Groups (14)

<u>Proof</u> Two permutations in S_n are conjugate if they have the same type.

Let $\sigma = (a_{11} a_{12} \ldots a_{1n_1})(a_{21} a_{22} \ldots a_{2n_2}) \ldots (\ldots a_{kn_k}$
for any $\pi \in S_n$

4.14 $\pi\sigma\pi^{-1} = [\pi(a_{11})\pi(a_{12})\ldots\pi(a_{1n_1})] \ldots [\pi(a_{k1})\ldots\pi(a_{kn_k})]$

for $(\pi\sigma\pi^{-1})\pi(a_{11}) = \pi(a_{12})$
$\pi\sigma\pi^{-1}\ \pi a_{1n_1} = \pi(a_{11})$
So conjugates have the same cycle type.

Conversely, let $\tau = (b_{11}\ b_{12} \ldots b_{1n_1})(b_{21}\ b_{22} \ldots b_{2n_2}) \ldots (b_{k1} \ldots b_{kn_k})$
If $\pi \in S_n$ takes a_{ij} to b_{ij} we see from 4.14 that
$\pi\sigma\pi^{-1} = \tau$ so σ τ are conjugate.

E.g. $(2k)(12)(2k) = (1k)$

<u>Corollary 4.15</u> S_n has $p(n)$ conjugacy classes of elements, where $p(n)$ is the number of partitions $n = n_1 + \ldots + n_k$ with $n_i \in \mathbb{N}$, $n_1 \geq \ldots \geq n_k$, $k \in \mathbb{N}$.

E.g. $n = 4$

Cycle type	x, e.g.	$\lvert ccl_{S_4}(x)\rvert$	$C_{S_4}(x)$	$\lvert C_{S_4}(x)\rvert$	sgn
(1^4)	i	1	S_4	24	+
$(2, 1^2)$	$(1\ 2)$	6	$\langle(12),(34)\rangle$	4	−
$(3, 1)$	(123)	8	$\langle(123)\rangle$	3	+
(2^2)	$(12)(34)$	3	D_8	8	+
(4)	(1234)	6	$\langle(1234)\rangle$	4	−

Conjugacy Classes in A_n

E.g. A_4 has four ccls:

cycle type		$\lvert ccl_{A_4}(x)\rvert$	$C_{A_4}(x)$
1^4		1	A_4
2^2		3	$\langle (12)(34), (13)(24) \rangle$
3	(123)	4	$\langle (123) \rangle$
3	(132)	4	

Let $x \in A_n$. Then $ccl_{A_n}(x) \subseteq ccl_{S_n}(x)$

$$|ccl_{S_n}(x)| = |\underset{\text{index 2}}{S_n} : \underset{\text{index 1 or 2}}{C_{S_n}(x)}|$$

and

$$|ccl_{A_n}(x)| = |A_n : C_{A_n}(x)|$$

(If $C_{S_n}(x)$ contains odd permutation then half are even, half are odd).

Now $A_n < S_n$ index 2.
$C_{A_n}(x) \subseteq C_{S_n}(x)$ index 1 or 2.

Theorem 4.16 Let $x \in A_n$. Then either

$ccl_{A_n}(x) = ccl_{S_n}(x)$ $\quad C_{S_n}(x)$ contains odd permutations.

or $|ccl_{A_n}(x)| = \frac{1}{2}|ccl_{S_n}(x)|$ $\quad C_{S_n}(x) \subseteq A_n$

Theorem 4.17
Let p be a prime. Let G be a finite $p$group so that $|G| = p^a$ for some power a of p. Then $Z(G) = \{z \in G \mid gz = zg, \forall g \in G\}$ is non trivial.

Proof G acts on G by conjugation. We claim that G has at least p conjugacy classes of size 1. By the orbit stabiliser theorem, each conjugacy class in G has size 'some power of p'. Their union is G, size p^a and $\{e\}$ is a ccl of size one. Hence there are at least p ccls of size 1, and the corresponding elements lie in $Z(G)$.

28/10/10

Groups (14)

Theorem 4.18 (Cauchy)
If p is a prime, and G is a group of order divisible by p, then G contains an element of order p.

Proof Let $C_p = \langle x \mid x^p = 1 \rangle$ act on the set X.

$$X = \{(g_1, g_2, \dots g_p) \mid g_i \in G,\ g_1 g_2 g_3 \cdots g_p = e\}$$

by permuting coordinates $x^j : (g_1, \dots, g_p) \longmapsto (g_{1+j}, g_{2+j} \cdots g_{p+j})$
indices modulo p.

Now $|X| = |G|^{p-1}$ so $p \mid |X|$ and X splits into orbits of size 1 or p. Now $\{(e \dots e)\}$ is one orbit of size 1, hence there are others.

$\{(x_1 \dots x_p)\}$ size $1 \Rightarrow x_i = x$ for all i and $x^p = e$.

3

0/11/10

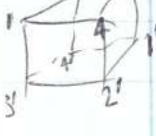
Groups (15)

Groups of symmetries of regular solids

Tetrahedron Let G be the group of all symmetries, G^+ be the group of all rotational symmetries. A Tetrahedron has four vertices; G acts on the set X of vertices, transitively. If v is a vertex in X,
$|G| = 4|G_v| = 4 \cdot 6$ as $|G_v| = 6$
The action is faithful, so we have an injective homomorphism.
$\theta : G \to S_4$ so $\theta(G) = S_4$ as $|G| = |S_4|$
$G \cong S_4$. And $|G^+| = 12$ and $G^+ \cong A_4$.

Cube (or an octahedron)
(Octahedron is dual to a cube: putting vertices in the centres of faces of a cube gives an octahedron, so they have the same groups of symmetries.
Let G be the group of all symmetries,
Let G^+ be the subgroup of rotational symmetries.

Let F be the set of faces of the cube, $|F| = 6$. Now G^+ acts on F, transitively. If $f \in F$ then $|G^+| = 6 \cdot |G^+_f| = 6 \cdot 4 = 24$
Let D be the set of four diagonals of the cube.
Now G, G^+ act transitively on D.



Now G^+ is faithful on D, and the ~~action~~ kernel of the action of G on D is $\langle (11')(22')(33')(44') \rangle$ of order 2.
If G fixes all diagonals, either $i' \mapsto i'$
$g : 1 \mapsto 1 \Rightarrow 1' \mapsto 1'$, $\Rightarrow i \mapsto i$ as $2'$ is further from 1 than 2 et
or
$g : 1 \to 1' \Rightarrow 1' \mapsto 1$ $i \Leftrightarrow i'$ for the same reason
So the kernel of G on D is $\langle (11')(22')(33')(44') \rangle$ and since $K \cap G^+ = \{1\}$, we have that G^+ is faithful. So we get an injective homomorphism $\theta : G^+ \to S_4$ and since $|\theta(G^+)| = 24$
we have $G^+ \cong S_4$

Finally $G \cong G^+ \times \langle g \rangle \cong S_4 \times C_2$ for, G is generated by G^+, $\langle g \rangle$, and g commutes with each element of G and $G^+ \cap \langle g \rangle = \{e\}$

So $G \cong G^+ \times \langle g \rangle$

In fact, writing our cube in $\mathbb{R}^3$, with vertices $(\pm 1, \pm 1, \pm 1)$ then g is obtained from the transformation $-I$.

Dodecahedron (or icosahedron) - a sketch

12 faces, 30 edges, 20 vertices.

$G^+ \subseteq G$ Act on the set F of faces

$|G^+| = 12 |G_F| = 12 \cdot 5 = 60$

Now consider the set C of five cubes embedded: each edge of a cube appears as a diagonal on a face. G acts on C. We can see $6 \cdot 4$ elements of order 5 acting. But A_5 is the subgroup of S_5 generated by these. So $G^+ \cong A_5$

Finally $G \cong A_5 \times C_2$

the kernel of the action of G on C is a subgroup of order 2: placing the dodecahedron in the centre $\underline{O}$, we see the kernel is $\{\pm I\}$

5. Homomorphisms, normal subgroups and quotient groups

Recall $(G, *_G)$, $(H, *_H)$ are groups

$\theta : G \to H$ is a homomorphism if $\theta(g_1 *_G g_2) = \theta(g_1) *_H \theta(g_2)$ for all $g_1, g_2 \in G$

The image of a homomorphism $\theta(G) = \{\theta(g) \mid g \in G\}$

Lemma 5.1 If $\theta : G \to H$ is a homomorphism, then $\theta(G) \leq H$

Proof: $e_H \in \theta(G)$ since $\theta(e_G)\theta(e_G) = \theta(e_G)$

so $e_H = \theta(e_G)$.

Next, if $g \in G$ then $\theta(g^{-1}) = \theta(g)^{-1}$ since $\theta(g)\theta(g^{-1}) = e_H = \theta(g^{-1})\theta(g)$

Finally, take $\theta(g_1)$ $\theta(g_2) \in \theta(G)$.

$\theta(g_1)^{-1} \theta(g_2) = \theta(g_1^{-1} g_2) \in \theta(G)$ so $\theta(G) \leq H$

2/11/10

Groups (16)

Recall G, H, groups. $\Theta : G \to H$ is a homomorphism.
$\Theta(G) \leq H$. kernel:
$\ker\Theta = \{g = G \mid \Theta(g) = e_H\}$

E.g. sgn : $S_n \to \{\pm 1\}$, $\pi \mapsto \mathrm{Sgn}(\pi)$. $\ker \mathrm{sgn} = A_n$

E.g.  $\Theta : \{\mathbb{C}\setminus\{0\}, \times\} \to \{z \in \mathbb{C}^\times \mid |z| = 1\}$

$z \mapsto \frac{z}{|z|}$

A homomorphism onto the unit circle. $\Theta(z_1 z_2) = \frac{z_1 z_2}{|z_1 z_2|} = \Theta(z_1)\Theta(z_2)$
kernel $= \mathbb{R}_{>0}$

<u>Remark 5.2</u> If G is a group acting on the set X, the kernel of the corresponding permutation representation $\Theta : G \to \mathrm{Sym}(X)$, $g \mapsto g^*$ is the kernel of the action.

<u>Definition</u> A subgroup K of G is <u>normal</u> in G if $gK = Kg$ for all $g \in G$
notation $K \trianglelefteq G$
Iff $gKg^{-1} = K$ for all $g \in G$, iff for all $g \in G$, $k \in K$, $gkg^{-1} \in K$

If G is abelian, and $K \leq G$, then $K \trianglelefteq G$.

$G = S_3$ $\quad \langle(123)\rangle \trianglelefteq G$ but $\langle(12)\rangle$ is not normal.

<u>Lemma 5.3</u> If $\Theta : G \to H$ a homomorphism, $\ker\Theta$ is a normal subgroup of G

Proof $K = \ker\Theta$. $K \leq K$: $e_G \in K$ $\quad k_1, k_2 \in K \Rightarrow k_1^{-1}k_2 \in K$
as $\Theta(k_1^{-1}k_2) = \Theta(k_1)^{-1}\Theta(k_2) = e_H$
$K \trianglelefteq G$, $k \in K$, $g \in G \Rightarrow gkg^{-1} \in K$: $\Theta(gkg^{-1}) = \Theta(g)\Theta(k)\Theta(g)^{-1} = e_H$

<u>Lemma 5.4</u> If $\Theta : G \to H$ is a homomorphism, then Θ is injective iff $\ker\Theta = \{e_G\}$

<u>Proof</u> If Θ is injective and $k \in \ker\Theta$ then $\Theta(k) = \Theta(e_G) \Rightarrow k = e_G$
so $\ker\Theta = \{e_G\}$
Conversely, if $\ker\Theta = \{e_G\}$ and $\Theta(g_1) = \Theta(g_2)$ then $\Theta(g_1^{-1}g_2) = e_H$
so $g_1^{-1}g_2 = e_G \Rightarrow g_1 = g_2$

<u>Lemma 5.5</u> If $K < G$ of ~~order~~ index 2 then $K \trianglelefteq G$
<u>Proof</u> Let $g \in G$. If $g \in K$ then $gK = K = Kg$
if $g \in G \setminus K$ then $gK = G \setminus K = Kg$

Lemma 5.6 (= 3.5#) Let G be a group with two normal subgroups. G_1 and G_2 such that $G = \langle G_1, G_2 \rangle$. $G_1 \cap G_2 = \{e\}$
Then $G \cong G_1 \times G_2$.

Proof Let $g_i \in G_i$, then $g_1 g_2 = g_2 g_1$

Commutator of g_1, g_2: $g_1^{-1} g_2^{-1} g_1 g_2 \in G_1 \cap G_2 = \{e\}$ so $g_1 g_2 = g_2 g_1$
as $G_1 \trianglelefteq G$, $G_2 \trianglelefteq G$

Theorem 5.7 Let $K \trianglelefteq G$. Then G/K, the set of right cosets K in G, is a group with respect to the operation $g_1 K * g_2 K = g_1 g_2 K$.

Remark G/K is a quotient group of G, $|G/K| = \frac{|G|}{|K|}$ finite sets

Proof If $g_i K = h_i K$ ~~and~~ then $g_1 g_2 K = h_1 h_2 K$

$h_2^{-1} h_1^{-1} g_1 g_2 = h_2^{-1} k g_2 = k' h_2^{-1} g_2 = k' k_2 \in K$
put $k = h_1^{-1} g_1 \in K$, take $k' \in K$ $h_2^{-1} k = k' h_2^{-1}$
$k_2 \in K$ with $k_2 = h_2^{-1} g_2$
$K \trianglelefteq G$.
So $*$ is well defined, to G/K.
Associative $(g_1 K * g_2 K) * g_3 K = (g_1 g_2 K) * g_3 K = (g_1 g_2) g_3 K$
$= g_1 (g_2 g_3) K = g_1 K * (g_2 g_3 K) = g_1 K * (g_2 K * g_3 K)$.

Identity element is K. Inverse of gK is $g^{-1}K$.

E.g. $G = S_3$, $K = \langle (123) \rangle$ $G/K = \{K, (12)K\} \simeq C_2$

E.g. $D_8 = \langle a, b \mid a^4 = e = b^2, bab^{-1} = a^{-1} \rangle$
$K = \langle a^2 \rangle = Z(D_8) \trianglelefteq D_8$

$D/K = \{K, aK, bK, abK\} \simeq C_2 \times C_2$ Note $Z(G) \trianglelefteq G$

15/11/10

Groups (17)

Theorem 5.8 (Isomorphism theorem)
Let $\theta : G \to H$ be a homomorphism. Then $\theta(G) \leq H$, $\ker\theta \trianglelefteq G$, and $\frac{G}{\ker\theta} \cong \theta(G)$.

We already know $\theta(G) \leq H$, $\ker\theta \trianglelefteq G$. Let

$$\bar\theta : \frac{G}{\ker\theta} \to \theta(G) \leq H$$
$$gk \to \theta(g)$$

$k = \ker\theta$

This is a well defined isomorphism from $\frac{G}{k}$ onto $\theta(G)$.

if $g_1 k = g_2 k$ then $g_1^{-1}g_2 \in k$ so $\theta(g_1^{-1}g_2) = e_H$
$\Rightarrow \theta(g_1) = \theta(g_2)$, $\bar\theta$ is well defined.
as $\bar\theta(g_1 k) = \bar\theta(g_2 k)$

$\bar\theta$ Injective:
Reverse the steps above.

$\bar\theta$ is a homomorphism: $\bar\theta(g_1 k g_2 k) = \theta(g_1 g_2) = \theta(g_1)\theta(g_2) = \bar\theta(g_1 k)\bar\theta(g_2 k)$

$\bar\theta$ is surjective. If $h \in \theta(G)$ then $h = \theta(g)$ $\exists g \in G$, so $h = \bar\theta(gk)$ for this g.

E.g. $\theta : \overset{G}{(\mathbb{R}, +)} \to \overset{H}{\mathbb{C}^*} = (\mathbb{C} \setminus \{0\}, \times)$
$t \to e^{ti}$

This is a homomorphism: $e^{(t_1+t_2)i} = e^{t_1 i} \cdot e^{t_2 i}$
$\theta(G) = S^1$ the unit circle.
$\ker\theta = \langle 2\pi \rangle = \{2\pi n \mid n \in \mathbb{Z}\}$, So $\mathbb{R}/\langle 2\pi\rangle \cong S^1$

E.g. $G = (\mathbb{Z}, +)$ $\theta : G \to H$ for some H, surjective.
(Image of a cyclic group is cyclic, generated by the image of a generator of G
Any subgroup of a cyclic group is cyclic and normal (abelian group).
So $\ker\theta = \langle n \rangle$ $n \in \mathbb{N}_0$ and

$$H \cong \frac{G}{\ker\theta} = \mathbb{Z}/\langle n \rangle \text{ integers mod } n,\ C_n.$$

So the homomorphic images of $(\mathbb{Z}, +)$ are C_n and $(\mathbb{Z}, +)$

Remark 5.9 Any homomorphic image of G is a quotient of G. The converse is also true. Let $k \trianglelefteq G$, form $\bar G = G/k$.

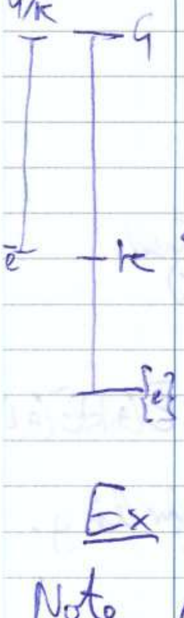
Define $\bar{\ } : G \to G/k = \bar G$ $\quad g \mapsto gk = \bar g$
This is a homomorphism from G onto $\bar G$ with Kernel k.
$\bar{\ }$ is a homomorphism since $\overline{g_1 g_2} = g_1 g_2 k = g_1 k g_2 k = \bar g_1 \bar g_2$
Surjective clearly.
Kernel is k: If $g \in k$ then $\bar g = k$, so $g \in \ker\bar{\ }$
and if $g \in \ker\bar{\ }$, then $gk = k$, so $g \in k$.

A further look at $\theta : G \to \theta(G) \leq H$.

$K = \operatorname{Ker}\theta$

$\bar{G} = \frac{G}{K}$

Remark In GRM IB course next term, will see other Isomorphism theorems e.g. $K \trianglelefteq G$, there is a 1-1 correspondence preserving inclusion between two sets



$$\{\text{all subgroups of } G \text{ containing } K\} \longleftrightarrow \{\text{all subgroups of } \bar{G}\}$$

Note that $\bar{G}$ is smaller than G unless $\{e\}$

Definition A group G is simple of the only normal subgroups are G or $\{e\}$.
Simple goups are the building blocks of all groups.
The abelian simple groups are the cyclic groups of prime order: in an abelian group any subgroup is normal, so a simple group has prime order.

The non-abelian simple groups are more interesting.

Ex A_5 is simple (and indeed, all A_n, $n \geq 5$).

Note A normal subgroup of a group G is a subgroup that is a union of G-ccls.

Now A_5 has ccls of size 1, 12, 12, 15, 20, but the only divisors of 60 we can obtain by joining these are 1 and 60, so A_5 is simple.

17/11/10

Groups (18)

Matrix Groups, I:

General and special linear groups

$S_4 = \{S \mid S$ is a problem$\}$ $|S_4| = 99$, b@*!#@ S_4

Let F be $\mathbb{R}$ or $\mathbb{C}$. (or another field)
Let $M_n(F) = \{$all $n \times n$ matrices with entries in $F\}$
(in particular, $n=2$ or $n=3$)
Recall from Vectors and Matrices: $A, B \in M_n(F)$, $A = (a_{ij})$, $B = (b_{ij})$

$(AB)_{ij} = a_{ik} b_{kj}$. Then $AB \in M_n(F)$. The multiplication is associative:
$(AB)C = A(BC)$

$$((AB)C)_{rs} = (AB)_{rk} C_{ks} = a_{rl} b_{lk} C_{ks} = a_{rl} (BC)_{ls} = (A(BC))$$

Determinants: $A \in M_n(F)$;

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\, a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

E.g. $n=2$, $\det A = a_{11}a_{22} - a_{12}a_{21}$

From Vectors and Matrices, linear algebra. $\det AB = \det A \det B$
$\forall A$ $\det A \neq 0 \iff \exists A^{-1}$ i.e. $\det A \neq 0$ if A is invertible

Lemma 6.1 Let $GL_n(F) = \{A \in M_n(F) \mid A$ is invertible$\}$ ($\det A \neq 0$)
This is a group under matrix multiplication

Proof $G = GL_n(F)$. If $A, B \in G$ then $AB \in G$, for AB is a matrix of the right size and $(AB)^{-1} = B^{-1}A^{-1}$ ($AB\,B^{-1}A^{-1} = I = B^{-1}A^{-1}AB$)
Also $I = I_n$ is the identity. Each element has an inverse and multiplication is associative.
$GL_n(F)$ is the general linear group of $n \times n$ matrices over F.

$SL_n(F)$ is all matrices in F with det 1 i.e. $SL_n(F) = \{A \in GL_n(F) \mid \det A = 1\}$

special linear group

We see $GL_n(F) \to F^\times$ is a homomorphism onto F^*: we have seen $\det AB = \det A \det B$.

Surjective as $\det \begin{pmatrix} \lambda & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix} = \lambda$

$SL_n(F) = \ker \det$ so $\dfrac{GL_n(F)}{SL_n(F)} \cong F^*$ (Isomorphism Theorem)

Remark: Assume normally that $n > 1$, For if $n=1$, $GL_n(F) \cong F^*$, $SL_n(F) = \{1\}$

6·3 The action of $GL_n(F)$ on F^n

F^n = all $n \times 1$ columns $\qquad (A, \underline{v}) \mapsto A\underline{v}$

$A \in GL_n(F)$. $\underline{v} \in F^n$

Ex If, for some $A \in GL_n(F)$, $A\underline{v} = \underline{v}$ $\forall$ $\underline{v} \in F^n \Rightarrow A = I$

So the action of $GL_n(F)$ on F^n is faithful.

Also, the action is transitive on the set $F^n \setminus \{\underline{0}\}$ (and much more, the action is in fact transitive on the set of bases)

6·4 The conjugation action of $GL_n(F)$ on $M_n(F)$:

$(A, X) \in GL_n(F) \times M_n(F)$

$(A, X) \mapsto AXA^{-1}$

This is an extension of the usual conjugation action of $GL_n(F)$ on $GL_n(F)$. Note that if $X \in GL_n(F)$ then $AXA^{-1} \in GL_n(F)$ so the conjugation action has some orbits which are conjugacy classes in $GL_n(F)$ and others consisting of singular matrices in $M_n(F)$.

In any case, the orbits are the <u>similarity</u> classes. $\qquad B = \{e_1, e_2 \ldots e_n\}$

<u>Digession</u> - Preview of V+M IA, Linear Algebra IB

V a vector space of dimension n over the field F.

Let B be a fixed basis of V. Then, we have a bijection (isomorphism)

$V \to F^n$, $\underline{v} \mapsto [\underline{v}]_B$ $\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \vdots \end{pmatrix}$

$\underline{v} = \sum \lambda_i \underline{v}_i$

$\alpha : V \to V$, linear function $[\alpha(\lambda_1\underline{v}_1 + \lambda_2 v_2 \ldots)] = \lambda_1 \alpha(\underline{v}_1) + \ldots$ etc

~~Then α "becomes" the action~~

α has a matrix $[\alpha]_B$, $n \times n$, over F with respect to this Basis so that α "becomes" the transformation described in 6·3, on F^n.

$\underline{v} \in V \longleftrightarrow [\underline{v}]_B \in F_n$

$\alpha : \underline{v} \mapsto \alpha(\underline{v}) \longleftrightarrow [\underline{v}]_B = A[\underline{v}]_B$, $A = [\alpha]_B$

19/11/10

Groups (19)

Taking a different basis B' for V:
$\underline{V} \leftrightarrow [V]_{B'}$ $\quad V \longleftrightarrow F^n$
and $[\alpha]_{B'} = P[\alpha]_B P^{-1}$ for some $P \in GL_n(F)$

P is the change of basis matrix. It becomes important to find "canonical form" of matrices in a given similarity class of $GL_n(F)$ on $M_n(F)$.

__Theorem 6.5__ (Jordan-Normal Form for $n=2$)
Given $X \in M_2(\mathbb{C})$, precisely one of:
i) The similarity orbit of X contains $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$, $\lambda \neq \mu \in \mathbb{C}$
ii) The similarity orbit of X contains $\{\lambda I_2\}$
iii) The similarity orbit of X contains a unique matrix $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$

End of Digression

__7. Möbius Transformations__. A Möbius Transformation on $\mathbb{C}$ is a mapping $f(z) = \frac{az+b}{cz+d}$ where $a,b,c,d \in \mathbb{C}$ and $ad-bc \neq 0$

Note that f is injective: $f(z) - f(w) = \frac{(ad-bc)(z-w)}{(cz+d)(cw+d)} \Rightarrow ad-bc \neq 0$

A problem: If $c \neq 0$, $f(-\frac{d}{c})$ is not defined. Introduce a new element, ∞: from $\mathbb{C}_\infty = \mathbb{C} \cup \{\infty\}$
So: Mobius Transformation on $\mathbb{C}_\infty$ is defined by: $f(z) = \frac{az+b}{cz+d}$, $a,b,c,d \in \mathbb{C}$ $ab-bc \neq 0$
and if $c = 0$, $f(\infty) = \infty$, if $c \neq 0$, $f(-\frac{d}{c}) = \infty$, $f(\infty) = \frac{a}{c}$
(note: here $\frac{a}{c}$ had no pre image in $\mathbb{C}$).

This makes f into a permutation on $\mathbb{C}_\infty$.

__Theorem 7.1__ The set of all Mobius Transformations is a group M (a Mobius Group) under composition of functions. $M \leq Sym(\mathbb{C}_\infty)$

__Proof.__ $f(z) = \frac{az+b}{cz+d}$, $a,b,c,d \in \mathbb{C}$, $ab-bc \neq 0$ $\left(\begin{array}{l} c=0, f(\infty)=\infty \\ c \neq 0, f(\infty) = \frac{a}{c}, f(-\frac{d}{c}) = \infty \end{array} \right.$

$$g(z) = \frac{\alpha z + \beta}{\gamma z + \delta}$$

Then $fg \in M$. $fg(z) = \dfrac{a\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) + b}{c\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) + d}$

$$fg(z) = \frac{(a\alpha + b\gamma)z + (a\beta + b\delta)}{(c\alpha + d\gamma)z + (c\beta + d\delta)}$$

$$(a\alpha + b\gamma)(c\beta + d\delta) - (a\beta + b\delta)(c\alpha + d\gamma) = (ad-bc)(\alpha\delta - \beta\gamma) \neq 0$$

$f(z) \leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z \\ 1 \end{pmatrix}$ Need to check finitely many points not yet checked - Lengthy

So M is closed under composition. The composition is associative.
Identity: $i(z) = z$, $\frac{1z+1}{0z+1} \in M$.

<u>Inverses</u> $f(z) = \frac{az+b}{cz+d}$, $ad-bc \neq 0$ etc

$$g(z) = \frac{dz-b}{-cz+a} \quad da-bc\neq 0 \quad : \text{Claim } fg = i = gf$$

If $c=0$, $f(z) = \frac{az+b}{d}$, $g(z) = \frac{dz-b}{a}$ for $z \in \mathbb{C}$

$f(\infty) = \infty = g(\infty)$, so $fg(z) = z = gf(z)$ $\forall z \in \mathbb{C}$

If <u>$c \neq 0$</u> Assume first $z \in \mathbb{C} \setminus \{-\frac{d}{c}\}$. $f: \mathbb{C}\setminus\{-\frac{d}{c}\} \to \mathbb{C}\setminus\{\frac{a}{c}\}$

$fg(z) = z$ ~~$= gf(z)$~~ (when we substitute) for $z \in \mathbb{C}\setminus\{\frac{a}{c}\}$ g doing the opposite
$gf(z) = z$ for $z \in \mathbb{C}\setminus\{-\frac{d}{c}\}$

Finally $gf(-\frac{d}{c}) = g(\infty) = -\frac{d}{c}$; $fg(\frac{a}{c}) = f(\infty) = \frac{a}{c}$
$gf(\infty) = g(\frac{a}{c}) = \infty$, $fg(\infty) = f(-\frac{d}{c}) = \infty$
so $g = f^{-1}$, $g, f \in M$.

<u>Theorem 7.2</u> There is a surjective homomorphism $\theta: GL_2(\mathbb{C}) \to M$ $\quad \mathbb{C}_\infty \to \mathbb{C}_\infty$
surjective with kernel $\{\lambda I_2 \mid \lambda \in \mathbb{C}^\times\}$ $\quad ad-bc\neq 0 \begin{pmatrix} a & b \\ c & d\end{pmatrix} \mapsto \left(f: z \mapsto \frac{az+b}{cz+d}\right)$

Thus $\dfrac{GL_2(\mathbb{C})}{\{\lambda I_2 \mid \lambda \in \mathbb{C}^\times\}} \simeq M$

<u>Proof</u> If $A = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in GL_2(\mathbb{C})$, then $ad-bc\neq 0$, so $\theta(A) \in M$.

θ is a homomorphism: $\theta\left(\begin{pmatrix} a & b \\ c & d\end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta\end{pmatrix}\right) = \theta\begin{pmatrix} a & b \\ c & d\end{pmatrix}\theta\begin{pmatrix} \alpha & \beta \\ \gamma & \delta\end{pmatrix}$

θ is surjective - clear.

Finally the kernel, $\ker\theta = \{\lambda I_2 \mid \lambda \in \mathbb{C}^\times\}$

Any scalar matrix mapped to $i \in M$

Conversely $\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \ker\theta$ then $\frac{az+b}{cz+d} = z$ $\forall z \in \mathbb{C}$
so taking $z = \infty \Rightarrow c = 0$ $\quad z = 1 \Rightarrow a = d$
$z = 0 \Rightarrow b = 0$ $\quad$ scalar. $\begin{pmatrix} a & 0 \\ 0 & a\end{pmatrix}$

21/11/10

Groups (20)

In fact, the restriction θ' of θ to $SL_2(\mathbb{C}) \to M$ is a surjective homomorphism with kernel $\{\pm I\}$ where $\frac{SL_2(\mathbb{C})}{\{\pm I_2\}} \simeq M$

For, if $f(z) = \frac{az+b}{cz+d}$ with $D = ad - bc \neq 0$, then $f(z)$ is the same mapping on $\mathbb{C}_\infty$ as $z \mapsto \frac{D^{-\frac{1}{2}}(az+b)}{D^{-\frac{1}{2}}(cz+d)}$, this has determinant 1. So f is the image of the matrix $D^{-\frac{1}{2}}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

And $\ker\theta \cap SL_2(\mathbb{C}) = \{\pm I_2\}$.

Remark $SL_2(\mathbb{Z}) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ad-bc=1, a,b,c,d \in \mathbb{Z}\right\}$ - modular group
$M(\mathbb{Z}) = \left\{f(z) \mapsto \frac{az+b}{cz+d} \middle| ad-bc=1, a,b,c,d \in \mathbb{Z}\right\}$

$SL_2(\mathbb{Z})/\{\pm I_2\} \simeq M_{\mathbb{Z}}$

Theorem 7.5 The action of M on $\mathbb{C}_\infty$ is sharply tripley transitive.
(tripley) If z_∞, z_0, z_1 are three points in $\mathbb{C}_\infty$ and $w_\infty, w_0, w_1 \in \mathbb{C}_\infty$, there exists an element $f \in M$ with $f: z_\infty \mapsto w_\infty,\ z_0 \mapsto w_0,\ z_1 \mapsto w_1$.
(sharply) This element is unique.
Proof To take z_∞, z_0, z_1 to $\infty, 0, 1$ let $g: z \mapsto \frac{z-z_0}{z-z_\infty}\frac{z_1-z_\infty}{z_1-z_0}$ if $z_\infty, z_0, z_1 \in \mathbb{C}$
and if $z_\infty = \infty$, $z \mapsto \frac{z-z_0}{z_1-z_0}$
$z_1 = \infty$ $z \mapsto \frac{z-z_0}{z-z_\infty}$ $\leftarrow \left(g(\infty) = \frac{a}{c}\right)$ $z_0 = \infty$, $z \mapsto \frac{z_1-z_\infty}{z-z_\infty}$

If now g sends z_∞, z_0, z_1 to $\infty, 0, 1$ and h sends w_∞, w_0, w_1 similarly then $f = h^{-1}g$ is an element sending z_∞, z_0, z_1 to w_∞, w_0, w_1.

(Uniqueness) 7.6 $M_{\infty,0,1} = \{\iota\}$
$M_\infty = \left\{\frac{az+b}{d} \middle| ad \neq 0\right\}$ $[c=0]$

$M_{\infty,0} = \left\{\frac{az}{d} \middle| ad \neq 0\right\}$

In fact, M_{z_∞,z_0,z_1} is also the identity: taking g as before $g^{-1}M_{\infty,0,1}g = M_{z_\infty,z_0,z_1}$, and f above is unique: if f_1 also sends $z_i \mapsto w_i$ for $i = \infty, 0, 1$ then $f_1^{-1}f \in M_{z_\infty,z_0,z_1} = \{\iota\}$ so $f = f_1$.

Conjugacy classes and fixed points of elements in M

Jordan Normal Forms $n=2$
Given $A \in GL_2(\mathbb{C})$ one of:
1) A is conjugate to the diagonal matrix $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$, $\lambda \neq \mu \neq 0$
2) A is λI_2 for some $\lambda \neq 0$
3) A is conjugate to the triangular matrix $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$

Note $PAP^{-1} = B$ then $\theta(P)\theta(A)\theta(P)^{-1} = \theta(B)$
so A, B conjugate in $GL_2(\mathbb{C}) \Rightarrow \theta$ images are conjugate in M.

Deduce ccls in M: $f \in M$

i) f is conjugate to a transformation $z \mapsto \nu z$, $\nu \neq 0, 1$

ii) $f = i$, assumed not so here $(\lambda I_2 \in \ker\theta)$

iii) $h: z \mapsto z + \frac{1}{\lambda}$ can conjugate further to simplify. Take $g(z) = \lambda z$,
ghg^{-1} sends $z \mapsto z + 1$

Theorem 7.7 Any non-identity möbius transformation is conjugate to one of (in M):
i) $z \mapsto az$ $a \in \mathbb{C}$, $a \neq 0, 1$

or iii) $z \mapsto z + 1$

~~Cor~~ Corollary 7.8 Any non-identity Möbius transformation fixes either i) two ~~one~~ points or ii) one ~~two~~ point of $\mathbb{C}_\infty$.

24/11/10

Groups (21)

Alternative Direct Approach (without Jordan Normal Forms)

Let $f(z) = \frac{az+b}{cz+d}$, $ad-bc \neq 0$, $a,b,c,d \in \mathbb{Z}$

Consider fixed points z_i of f in $\mathbb{C}_\infty$.

$az_i + b = (cz_i + d)z_i$ (as $f(z_i) = z_i$)

so z_i are roots of $cz_i^2 + (d-a)z - b = 0$.

If this is non trivial, there are 1 or two roots. If there are two fixed points, z_1, z_2, let $g \in M$, $g(z_1) = 0$, $g(z_2) = \infty$. Then gfg^{-1} fixes $g(z_i)$, so fixes $0, \infty$, so $gfg^{-1}(z) = az$ for some $a \in \mathbb{C}$, $a \neq 0, 1$

If there is only one fixed point in $\mathbb{C}_\infty$, z_1, then let $g(z_1) = \infty$, then gfg^{-1} fixes precisely ∞ and nothing else, in $\mathbb{C}_\infty$. So $gfg^{-1}(z) = \alpha z + \beta$. Now $(\alpha - 1)z + \beta = 0$ has another solution unless $\alpha = 1$, so $gfg^{-1}(z) = z + \beta$. Conjugating a little more, we get f conjugate to $z \mapsto z+1$.

<u>Again</u> (7.8) $f \in M \setminus \{i\}$ fixes a unique point of $\mathbb{C}_\infty$: f conjugate to $z \mapsto z+1$
or f fixes two points of $\mathbb{C}_\infty$: f conjugate to $z \mapsto az$, $a \in \mathbb{C} \setminus \{0,1\}$

<u>E.g 7.9</u> This can be used to work out iterations of Möbius transformations. Suppose $f \in M$, with f fixing precisely one point of $\mathbb{C}_\infty$. What happens to $f^n(z)$ as $n \to \infty$ for any $z \in \mathbb{C}_\infty$?

Answer: $f^n(z) \to z_1$, the fixed point of f, as $n \to \infty$. For some $g \in M$, $gfg^{-1}(z) = h(z) = z+1$ so $gfg^{-1} = h$. Now $h^n : z \mapsto z+$ for any $z \in \mathbb{C}_\infty$ so $h^n(z) \to \infty$ for any $z \in \mathbb{C}_\infty$ as $n \to \infty$

Thus also $h^n(g(z)) \to \infty$, so $f^n(z) = g^{-1}h^n g(z) = z_1$, as required.

<u>Proposition</u> 7.10 Any Möbius transformation $f \in M$ can be written as a product or composition of Möbius transformations $z \mapsto az$, ($a \neq 0$) dilation and rotation and $z \mapsto z+b$, translation, and $z \mapsto \frac{1}{z}$ inversion.

<u>Proof</u> Let $f(z) = \frac{az+b}{cz+d}$, $a,b,c,d \in \mathbb{C}$, $ad-bc \neq 0$.

If $c = 0$, then $f = f_2 f_1$ with $f_1(z) = \frac{a}{d}z$, $f_2(z) = z + \frac{b}{d}$

If $c \neq 0$, $f(z) = \frac{az+b}{cz+d} = \frac{\frac{a}{c}z + \frac{b}{c}}{z + \frac{d}{c}} = A + \frac{B}{z + \frac{d}{c}}$ $\quad A = \frac{a}{c}$, $B = -\frac{ad-bc}{c^2}$

So $f = f_4 f_3 f_2 f_1$, with $f_1(z) = z + \frac{d}{c}$, $f_2(z) = \frac{1}{z}$, $f_3(z) = Bz$, $f_4(z) = z$

Circles and straight lines General equation of a circle or a straight line in $\mathbb{C}$: $Az\bar{z} + B\bar{z} + \bar{B}z + C = 0$ where $A, C \in \mathbb{R}$ $|B|^2 > AC$. $z = x + iy$ $B = b_1 + b_2 i$

$A(x^2+y^2) + 2(b_1 x + b_2 y) + C = 0$, circle or straight line in $\mathbb{C}$

[Straight line $\Leftrightarrow A = 0$; goes through $0 \Leftrightarrow C = 0$]

Theorem 7.12 Möbius transformations take circles/straight lines to circles/straight lines (not respectively).

Proof Let $f \in M$. Show f sends circles/straight lines to circles/straight lines.
By 7.10 Enough to check for $f(z) = \frac{1}{z}$ (clear for other transformations).
Now $f(z) = \frac{1}{z}$ ~~preserves~~ gives the equation 7.11 ~~gives~~ the same form.
i.e. $Cz\bar{z} + \bar{B}z + B\bar{z} + A = 0$

Remark Circles in $\mathbb{C}_\infty$: $\{\text{Euclidean circles in } \mathbb{C}\} \cup \{L \cup \{\infty\} \mid L \text{ is a line in } \mathbb{C}\}$

E.g. Find the image of the real axis under $f(z) = \frac{z-i}{z+i}$. It is a "circle" containing $f(\infty), f(0), f(1)$, gives $+1, -1, -i$
$\Rightarrow$ gives unit circle

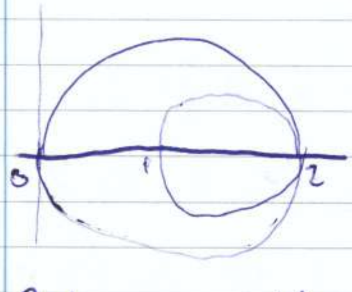
Or f: upper half of complex plane $\longmapsto$ inside the unit circle.

26/11/10

Groups (22)

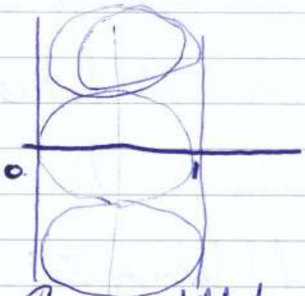
$f \in M \quad f(z) = \frac{az+b}{cz+d},\ a,b,c,d \in \mathbb{C},\ ad-bc \neq 0$

Circles in $\mathbb{C}_\infty$ are preserved by f (e.g. circles and lines in $\mathbb{C}$)



$f(z) = \frac{-z}{z-2}$

$2 \mapsto \infty$
$0 \mapsto 0$
$1 \mapsto 1$



Produce a necklace of touching circles: ↗ then shift back with $f^{-1}(z)$

Cross ratios - Definitions Let $z_i \in \mathbb{C}_\infty$ be distinct, $i = 1,2,3,4$. The cross ratio $[z_1, z_2, z_3, z_4]$ is the elements x of $\mathbb{C}$ such that if $f \in M$

Note conformal mappings preserve angles

taking $f: \begin{array}{ccc|c} z_1 & z_2 & z_3 & z_4 \\ \Downarrow & \Downarrow & \Downarrow & \Downarrow \\ 0 & 1 & \infty & x \end{array}$

that is $[z_1, z_2, z_3, z_4] = f(z_4)$

Thus, if $z_i \neq \infty$ then $[z_1, z_2, z_3, z_4] = \frac{z_4 - z_1}{z_4 - z_3} \cdot \frac{z_2 - z_3}{z_2 - z_1}$

and if some $z_j = \infty$, e.g. $[\infty, z_2, z_3, z_4] = \frac{z_2 - z_3}{z_4 - z_3}$

$[z_1, \infty, z_3, z_4] = \frac{z_4 - z_1}{z_4 - z_3}$

$[z_1, z_2, \infty, z_4] = \frac{z_4 - z_1}{z_2 - z_1} \qquad [z_1, z_2, z_3, \infty] = \frac{z_2 - z_3}{z_2 - z_1}$

Warning !!! Different notations exist so be consistent.

Theorem 7.13 Given $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$, distinct, and w_1, w_2, w_3, w_4 all distinct in $\mathbb{C}_\infty$, there exists $f \in M$ with $f(z_i) = w_i$ for $i = 1, 2, 3, 4$ iff the cross ratios are the same i.e. $[z_1, z_2, z_3, z_4] = [w_1, w_2, w_3, w_4]$

Proof Here we claim (7.14) $f \in M$ preserves cross ratios:

$[z_1, z_2, z_3, z_4] = [f(z_1), f(z_2), f(z_3), f(z_4)]$

Let $g: \Downarrow \begin{array}{cccc} f(z_1) & f(z_2) & f(z_3) & f(z_4) \\ 0 & 1 & \infty & \text{RHS} \end{array}$

Then $g \circ f: \Downarrow \begin{array}{cccc} z_1 & z_2 & z_3 & z_4 \\ 0 & 1 & \infty & \text{RHS} \end{array}$

But $g \circ f(z_4) = \text{LHS}$

So assume the cross ratios are equal, say to x.

Let $h \in M$ take $\downarrow \begin{matrix} z_1 & z_2 & z_3 & z_4 \\ 0 & 1 & \infty & x \end{matrix}$

and $k \in M$ taking $\downarrow \begin{matrix} w_1 & w_2 & w_3 & w_4 \\ 0 & 1 & \infty & x \end{matrix}$

Then $k^{-1}h \in M$ taking $z_i \mapsto w_i$ for $i \in \{1, 2, 3, 4\}$

E.g. z_1, z_2, z_3, z_4 lie on a circle in $\mathbb{C}_\infty$ <u>iff</u> $[z_1, z_2, z_3, z_4] \in \mathbb{R}$

<u>Proof</u> Let $f \in M$ taking z_1, z_2, z_3, z_4 to $0, 1, \infty, x$ $[x$ is $[z_1, z_2, z_3, z$
The "circle" on $0, 1, \infty$ is the real ~~line~~ axis.

<u>Two views of ∞ in $\mathbb{C}_\infty$ - (Beardon) 3.6, 3.8)</u>

1. $F = \mathbb{C}$ $GL_2(\mathbb{C})$ acts on $\mathbb{P}^1(\mathbb{C})$ via $\mathbb{C}^2$.

$A \in GL_2(\mathbb{C})$ $\quad \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{C}^2$ $\quad A : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto A\begin{pmatrix} x \\ y \end{pmatrix}$. A action $\mathbb{C}^2$
and hence A also acts on the set of 1D subspaces.

But $\left\langle \begin{pmatrix} x \\ y \end{pmatrix} \right\rangle \longleftrightarrow \begin{cases} \frac{x}{y} \in \mathbb{C} & \text{if } y \neq 0 \\ \infty & \text{if } y = 0 \end{cases}$

The action of $\frac{GL_2(\mathbb{C})}{\{\text{scalars}\}}$ is right! I.e. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$
If $y = 0$ $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$ $[$so $\infty \mapsto \frac{a}{c}]$

[e.g. $F \in \mathbb{R}$]

2. <u>Riemann Sphere</u>

9/11/10

Groups (23)

unit sphere S in $\mathbb{R}^3$ centre $(0,0,0)$

$N = (0,0,1)$ - north pole

$\varphi : \mathbb{C} \to S \setminus \{N\}$, $z \mapsto z'$

where z' is the unique point not N where the line z to N meets S.
Also $\varphi(\infty) = N$. Can study $\varphi^{-1} f \varphi$ on S

8. Matrix groups: Orthogonal Groups

$F = \mathbb{R}$ $\quad O_n = \{A \in GL_n(\mathbb{R}) \mid AA^T = I\}$ $\quad n \geq 2$ orthogonal group

$SO_n = \{A \in O_n \mid \det A = +1\}$ special orthogonal group

<u>Lemma 8.1</u> $O_n < GL_n(\mathbb{R})$

<u>Proof</u> $A \in O_n \Rightarrow \det A = \pm 1$ as $AA^T = 1$, $(\det A)^2 = 1 \Rightarrow A \in GL_n(\mathbb{R})$

$I_n \in O_n$ as $I_n I_n^T = I_n$

$A, B \in O_n \Rightarrow A^{-1}B \in O_n$: $(A^{-1}B)(A^{-1}B)^T = A^{-1}BB^tA^{-t} = I$

<u>Remark</u> $SO_n < O_n$ of index 2 $\quad \boxed{\text{Note } AA^T = I,\ A^T = A^{-1}}$

For, $\det A = \pm 1$ for any $A \in O_n$

If $A, B \in O_n \setminus SO_n$ then $\det A^{-1}B = 1$ so $A^{-1}B \in SO_n$

And there exists $A \in O_n$ with $\det A = -1$. Note $SO_n \triangleleft O_n$

$O_n / SO_n \cong C_2$

A is orthogonal iff columns of A are orthonormal (iff the rows are orthonormal)

<u>Recall</u> On $\mathbb{R}^n$, we have $\underline{x} \cdot \underline{y} = x_i y_i \in \mathbb{R}$, $|\underline{x}| = (\underline{x} \cdot \underline{x})^{\frac{1}{2}} \geq 0$

<u>Note 8.2</u> Let $A \in GL_n(\mathbb{R})$, let $\underline{x}, \underline{y} \in \mathbb{R}^n$.
Then $A\underline{x} \cdot \underline{y} = \underline{x} \cdot A^T\underline{y}$

For, if $A = (a_{ij})$, $\underline{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ $\quad \underline{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$

$$A\underline{x} \cdot \underline{y} = \sum_i \Big(\sum_j a_{ij} x_j\Big) y_i = \sum_j x_j \Big(\sum_i a_{ij} y_i\Big) = \underline{x} \cdot A^T \underline{y}$$

<u>Lemma 8.3</u> Assume $A \in O_n$, $\underline{x}, \underline{y} \in \mathbb{R}^n$
Then (1) $A\underline{x} \cdot A\underline{y} = \underline{x} \cdot \underline{y}$
(2) $|A\underline{x}| = |\underline{x}|$
(so orthogonal transformations are isometries)

<u>Proof</u> (1) $A\underline{x} \cdot A\underline{y} = \underline{x} \cdot A^TA\underline{y} = \underline{x} \cdot \underline{y}$

(2) $|A\underline{x}|^2 = A\underline{x} \cdot A\underline{x} = |\underline{x}|^2$ so $|A\underline{x}| = \underline{x}$

Partial Converse Any isometry of $\mathbb{R}^n$, fixing $\underline{0}$, is an orthonormal transformation.

8·4 Now, more about $n=2$, $n=3$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $A^T = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, and $AA^T = I = A^TA$

$a^2+b^2 = 1 = c^2+d^2 \quad a^2+c^2 = 1 = b^2+d^2$, $ac - bd = 0 = ab + cd$

So for a unique θ, with $\theta \in [0, 2\pi]$,

$(a, c) = (\cos\theta, \sin\theta) \qquad (b, d) = \pm(-\sin\theta, \cos\theta)$

so A is either $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ $\qquad \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$

$\det A = +1$, $A \in SO_2 \qquad \det A = -1$, $A \in O_2 \setminus SO_2$

The first of these is in SO_2, a ~~reflection~~ rotation by θ, $z \mapsto e^{i\theta} z$

The second is in $O_2 \setminus SO_2$, a reflection in the line $\frac{y}{x} = \frac{\sin\frac{\theta}{2}}{\cos\frac{\theta}{2}}$

$z \mapsto e^{i\theta}\bar{z}$

(To see this checked fixed points: $e^{i\theta}\bar{z} = z \Leftrightarrow e^{i\frac{\theta}{2}}\bar{z} = e^{-\frac{i\theta}{2}} z$

$\Leftrightarrow z e^{-i\frac{\theta}{2}} \in \mathbb{R} \Leftrightarrow z = te^{i\frac{\theta}{2}}$

$\underline{n=3}$ Theorem 8·5 Any matrix A in SO_3 has eigenvalue $+1$. If $\underline{v}$ is a corresponding eigenvector is called an axis of rotation.

Proof The characteristic polynomial is a real cubic, so has a real root λ.
Then $|\lambda| = 1$. If v is a corresponding eigen vector then $|A\underline{v}| = |\lambda \underline{v}| = |\lambda||v| = |$
as A is orthogonal. so $\lambda = \pm 1$.
Either A has 3 real roots all ± 1, product $+1$, so one is $+1$, or the eigenvalues of A are ± 1, α, $\bar{\alpha}$ for some $\alpha \in \mathbb{C} \setminus \mathbb{R}$. Since $\det A = 1$, the first of these is $+1$.

Theorem 8·6 Any matrix in SO_3 is conjugate to $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$ for some $\theta \in [0, 2\pi]$

Theorem 8.6 Any matrix in SO_3 is conjugate to $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$ for some $\theta \in [0, 2\pi$

Proof Let $A \in SO_3$, ~~let~~ choose $\underline{v}$ with $A\underline{v} = \underline{v}$, $|\underline{v}| = 1$.

Let $P \in SO_3$ be a rotation in SO_3 taking $\underline{v}$ to $\underline{e}_1$, where $\underline{e}_1, \underline{e}_2, \underline{e}_3$ is the standard orthonormal basis. So $P\underline{v} = \underline{e}_1$.
Then PAP^{-1} fixes $\underline{e}_1$, hence also $\underline{e}_1^{\perp} = \langle \underline{e}_2, \underline{e}_3 \rangle$ setwise
so acts as $\begin{pmatrix} 1 & & \\ & \cos\theta & -\sin\theta \\ & \sin\theta & \cos\theta \end{pmatrix}$ so the claim follows.

Theorem 8.7 $O_3 \cong SO_3 \times \langle -I_3 \rangle$

Proof $SO_3 \triangleleft O_3$ index 2, $\langle -I_3 \rangle \triangleleft O_3$ order 2.
$\langle -I_3 \rangle \cap SO_3 = \{I_3\}$ so the claim follows from S.S.

More on reflections Some elements in $O_3 \setminus SO_3$ are reflections. Let Π be the plane in $\mathbb{R}^3$ through $\underline{0}$ perpendicular to $\underline{n}$ with $|\underline{n}| = 1$

(8.8) Reflection in plane Π:
$$r_{\underline{n}}(\underline{v}) = \underline{v} - 2(\underline{v} \cdot \underline{n})\underline{n} \qquad \underline{n} \mapsto -\underline{n} \qquad \underline{v} \in \Pi, \underline{v} \mapsto \underline{v}$$

Theorem 8.9 Any orthogonal matrix (ie in O_3) can be written as a product of at most 3 reflections.

Proof Since $O_3 = SO_3 \cup \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} SO_3$, it is enough to show any matrix in SO_3 is a product of at most 2 reflections. Since each element in SO_3 has an axis $\underline{v}$ we can work in $\underline{v}^{\perp}$ and show that any element in SO_2 is the product of at most two reflections

$$\text{But } \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Finite Simple groups $\quad C_p$, p prime $\quad A_n$ for $n \geq 5$

Matrix groups

$F = \mathbb{F}_p$ Galois Field, integers mod p. In fact there is a unique finite field of size p^n for any prime power but no other sizes.

E.g. $GL_n(\mathbb{F}_p) \quad SL_n(\mathbb{F}_p) \quad PSL_n(\mathbb{F}_p) = \dfrac{SL_n(\mathbb{F}_p)}{\{\text{scalar matrices}\}}$ projective special linear group

$PSL_n(\mathbb{F}_q)$ is simple for $n \geq 2$ unless $n = 2$, $q = 2, 3$.

E.g. $n=2$ Finite Möbius group. $F_\infty = \{0, 1, \ldots, p-1, \infty\}$

$|GL_2(\mathbb{F}_p)| = (p^2-1)(p^2-p) \qquad PSL_2(\mathbb{F}_p) = \frac{1}{2}p(p^2-1)$

$|SL_2(\mathbb{F}_p)| = p(p^2-1)$

Ten families of exceptional groups of Lie
26 sporadic simple groups

Mathieu $M_{11} \subset S_{11}$ $\quad |M_{11}| = 7920$

$M \quad |M| \sim 8 \times 10^{53}$