Contents

1 Introduction

1.1 Definition of a group

We will talk about symmetry and use that to motivate the definition of a group. Here are the symmetries of a triangle.

Figure 1 shows the symmetries of a triangle.

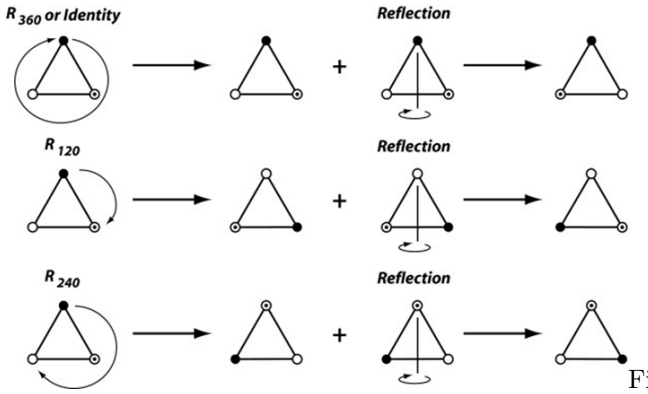

Figure 1

Notice some key properties:

- If I do one symmetry and then another symmetry, I get a symmetry.

- The do nothing symmetry exists, and we call it the identity.

- I can do symmetries in reverse. For example, I can pick up a triangle, move it around and that is a symmetry, and then reversing that movement is also a symmetry, as expected.

This motivates the definition of a group. Infinite groups but we can think of finite groups as a set of symmetries. A group is a set, with a binary operation which I will call *, which satisfies the following properties. Note that a binary operation is an operation that takes 2 things and outputs a third thing. For example, multiplication in the real numbers is a binary operation, because I can do (one number)*(another number)=(a third number).

A group is a set with a binary operation such that:

- For any a, b in the group, $a * b$ is in the group.

- There is a(n) (right) identity element, ie an element e such that $a * e = a$ for any a in the group. We usually write e to mean identity.

- All elements in the group have (right) inverses, ie for any a in the group there is an element b such that $a * b = e$

We can think of * as composing symmetries (doing one after the other). However, there is another rule for a group which is associativity, ie that $(a * b) * c$ always equals $a * (b * c)$. This is obvious in the case of symmetries: If I do symmetry 1 then do symmetry 2 followed by symmetry 3, vs if I do symmetry 1 followed by symmetry 2 then do symmetry 3, I will end up with the same result. This means we can move brackets around when doing algebra with groups, which is nice. Groups can be thought of algebraically or in terms of symmetries, and generally we do it algebraicly for infinite groups and as symmetries for finite groups.

However, groups are NOT commutitive in general. We cannot say that $a * b$ always is equal to $b * a$. For example, one can check that doing one of the reflections followed by a rotation yields a different ending state than doing the rotation first then the reflection in the triangle case. A commutative group is called an abelian group.

1.2 Basic properties

We would like to show that identity elements of groups work both ways, ie that e*a=a for any a, and the same for inverses, ie that if a*b=e then b*a=e as well. We also would like to show that the identity element is unique, so that we can justify saying "**the** identity element", and also that inverses are unique. We have to be very careful, as if we define that the identity is such that e*a=a for any a but the inverse of a is the element such that a*b=e, then this is a left identity and a right inverse, and this allows for some sets that do not fit the standard definition of groups. For example, if we define a group {a,b} with the binary operation defined by a*b=b (ie always pick the element on the right), then this is associative, a is a left identity, a and b have a right inverse in the form of a, but it does not satisfy the standard definition of a group as it is not the case that we have a right identity or a left inverse.

A group can be defined by having a right identity and right inverse (as we did above), or a left identity and a left inverse (just put the elements in reverse order in the proofs we will do that they are both in fact two sided), or can require them in the first place to be two sided.

Also, we often don't explicitly write * down, as it is implied, as we will do now in the proof.

Lemma. If $ab = e$ then $ba = e$

Proof. $b = be$ (by identity) $= bab$ (since we assume $ab = e$). There exists an element c in the group with bc=e. Multiplying c on both sides of $b = bab$ gives $bc = babc$, but $bc = e$ so we have that $e = bae$, but since anything*e=anything, we have that $ba = e$.

□

Lemma. $ea = a$ for any a.

Proof. $ab = e$ for some b in the group, But then $ba = e$ by the previous lemma, so $ab = e = ba$, so $ea = aba = ae = a$, so $ea = a$.

□

Lemma. Inverses are unique, ie if $ab = e = ab'$, then $b = b'$.

Proof. $b = be = bab' = eb'$ (since $ab = e$ so $ba = e$)$= b'$ (by tthe previous lemma).

□

Lemma. Identites are unique, ie if $ae = ae' = a$, then $e = e'$.

Proof. a has an inverse, lets call that b, then $e = ba = b(ae') = (ba)e' = ee' = e'$ because e is an identity, therefore $e = e'$.

□

Going forward, we will take these facts as obvious.

We typically write the inverse of a as a^{-1}, and we write groups as (The set, the operation) or (the set, the operation, the identity). For example, the integers form a group under addition with identity 0, and we can write it as ($\mathbb{Z}$, +) or ($\mathbb{Z}$, +, 0).

[Lecture 1 ends]

The inverse of an inverse is the original element. This is because a is an element such that $a^{-1}a = e$.

We define $a^n = a * a * a \cdots * a$ with n a's, and $a^{-n} = a^{-1} * a^{-1} * a^{-1} * \cdots * a^{-1}$. We can easily show that this satisfies the obvious properties, ie

$a^{n+m} = a * a * a \cdots * a$ with n+m a's $= (a * a * a \cdots * a)\,[n\ a's] * (a * a * a \cdots * a)\,[m\ a's] = a^n a^m$.

If m is negative and n-m is positive, then

$a^{n-m} = a * a * a \cdots * a$ with n-m a's $= (a * a * a \cdots * a)\,[n\ a's] * \left(a^{-1} * a^{-1} * a^{-1} \cdots * a^{-1}\right)[m\ terms] = a^n a^{-m}$, since all the inverse terms cancel with a non-inverse term. If n-m were negative, or we had -n-m, we could just invert everything and be fine.

$a^{nm} = a * a * a \cdots * a[nm\ a's]$ which can be split into n sets of m a's meaning we get that this is equal to $(a^m)^n$. If n or m were negative, then we could just either flip the sign on n and invert both a^{nm} and $(a^m)^n$, or flip the sign on m and invert both a^{nm} and $(a^m)^n$ since inverting each a^m term is the same as inverting the whole thing. If n and m are both negative, we have that $a^{nm} = (a^{-m})^{-n}$ as flipping the sign of n and m on the right hand side is the same as inverting it twice which makes you go back to where you started.

Of course, a^0 is defined to be the identity element, as $a^0 = a^{1-1} = aa^{-1} = e$ so everything can actually work out.

1.3 Examples

The group that is literally just {e} is called the trivial group.

The set {$\mathbb{Z}$, +, 0} is a group as addition is associative, integers are closed under addition, and -x is an inverse for any x. Also {$\mathbb{Q}$, +, 0}, {$\mathbb{R}$, +, 0}, {$\mathbb{C}$, +, 0} are all groups. These are examples of infinite groups.

The set {$\mathbb{N}$, +, 0} is not a group due to the lack of inverses.

{$\mathbb{Z}$, *, 1} is not a group for the same reason. However {$\mathbb{Q}$, *, 1} is almost a group except for the fact that 0 has no inverse. However {$\mathbb{Q}\backslash\{0\}$, *, 1} is a group.

We already encountered the group of symmetries of a triangle. This group is called S_3 or D_6, it will be later that we get more intuition for why.

$C_n = \{z \in \mathbb{C} : z^n = 1, *, 1\}$ is a group under multiplication. It is turns out that it is isomorphic (meaning it's structurally the same, we will see what this precisely means later) to the group {0, 1, 2, 3, ... n-1, +(mod n), 0}, where $e^{\frac{2ik\pi}{n}}$ in the first group corresponds to k in the second group.

Definition. The order of a group G is the number of elements in G. This is denoted o(G) or $|G|$ or #G.

[Lecture 2 ends]

First, we need a definition, which we probably also come across in the numbers and sets course. A bijection is a function such that every output is mapped to exactly once, so essentially a one-to-one correspondence. And a permutation is a bijection from a set to itself, which is essentially just a re-ordering of the elements of the set.

For a set x, Sym(x) is notation for the set of permutations of x. It turns out that under composition, ie doing one permutation after the other, this forms a group. We can prove this by checking each of the axioms. Figure 2 shows some handwritten working of this.

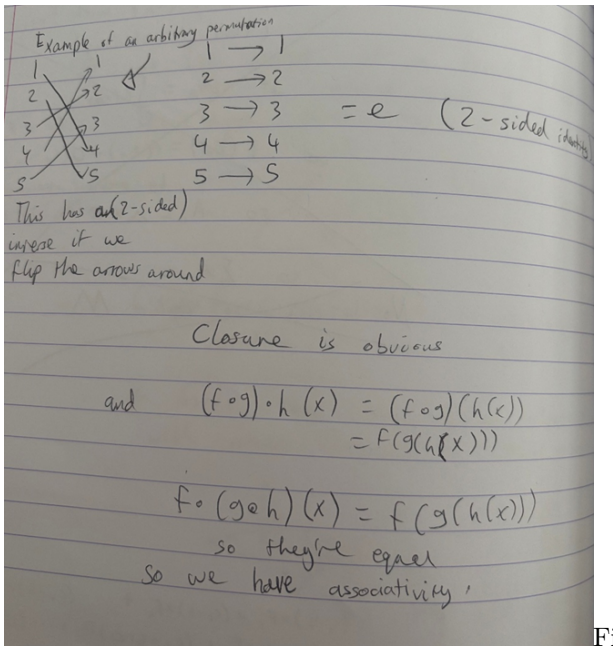

Figure 2

S_n is notation for the group of permutations of any set with n elements, such as {1, 2, 3, ... ,n} under composition. These groups are called **symmetric groups**.

Example. S_3 is the same as the group of symmetries of a triangle as you can think of it as rearranging the vertices, but S_4 is not the same as the group of symmetries of a square because if you swap two adjacent vertices you do not end up with a symmetry of a square that you can get by keeping it rigid and moving it around in space. However, the group of symmetries of a square is a subgroup of S_4, which foreshadows the next definition. S_{52} is the group of shufflings of decks of cards.

It turns out that the order of S_n is n!. To see why, a hint is: Think about how many places there are to map the first element to, then how many places are left to be able to map the second element to, and so on.

Note: From now on we won't always specify the operation of a group when we talk about a group, provided it is implied.

1.4 Subgroups

Definition. A **subgroup** is what you would expect it to be – a subset of a group that is itself a group under the same operation. For example, the group of rotations only of a triangle is a subgroup of the group of symmetries of a triangle,

and the group of symmetries of a square is a subgroup of S_4. To check that a subset is a subgroup, you must check the axioms, ie that

1. The identity is in the subgroup
2. All elements in the subgroup have their inverse in the subgroup
3. For all a, b in the subgroup, a.b is in the subgroup.

Note that associativity is trivially inherited.

Example. The trivial group is a subgroup of every group, and every group is a subgroup of itself. Any other subgroup is called a proper subgroup

Notation: We write H≤G if H and G are groups with H a subgroup of G. We often do use a capital H to refer to subgroups.

Example. Under addition, $\mathbb{Z}\leq\mathbb{Q}\leq\mathbb{R}\leq\mathbb{C}$.

Example. For n a non-negative integer Define n$\mathbb{Z}$ as the set of all multiples of n in $\mathbb{Z}$, for example $3\mathbb{Z}=\{\ldots, -9, -6, -3, 0, 3, 6, 9,\ldots\}$

n$\mathbb{Z}$ is indeed a group under addition because

1. Identity (0)
2. Closure (Any 2 elements in n$\mathbb{Z}$ is of the form an and bn with a, b integers, and an+bn=(a+b)n with a+b an integer, which is in n$\mathbb{Z}$.
3. Inverses (For any x in n$\mathbb{Z}$ -x is in nz. This is because an and (-a)n are both in n$\mathbb{Z}$ for all integers a)
4. Associativity (Addition is associative)

Theorem. All subgroups of $\mathbb{Z}$ are of the form n$\mathbb{Z}$ with n a non-negative integer.

Proof. Let H be a subgroup of $\mathbb{Z}$. The case where H is the trivial group is just H=$\{0\}$ which is $0\mathbb{Z}$. Otherwise, there exists a non-zero element. If it is negative, then its inverse must be positive, meaning there is always a positive element. There is also a least positive element, and the justification for this is that if there were not a least positive element then there would be an infinitely decreasing chain of positive elements, which is not possible since they are integers so the length of such the chain cannot be longer than the first element in the chain. We have learned in numbers and sets that we have to be careful about assuming that something like a "least positive element" exists. However, it does.

Let the least positive element of H be n. Then 2n, 3n, 4n, ... are in H by closure, then so are -n, -2n, -3n, ... by inverses, and so is 0 by identity. If this is all of H, then we have n$\mathbb{Z}$ so we are done, but we will prove that in fact, we must have n$\mathbb{Z}$.

Suppose there exists an element x in H with x not a multiple of n. Then by the division algorithm, we can write x=kn+r with k an integer and 0<r<n (strict inequalities since otherwise x would be a multiple of n). But then since x is in H, x-kn is in H by closure, and x-kn=r so r is also in H, but n is the least positive element in H by assumption, but r is positive and less than n, so this is a contradiction. So done.

□

Theorem. (Not mentioned in the lecture but I've seen it mentioned in IA groups notes before and it is very useful) if H is a subset of G and the identity is in H and for all a, b in H, ab^{-1} is in H, then H is a subgroup of G.

Proof. Identity and associativity are immediate. Inverses because if a in H then ea^{-1} is in H since e is in H and with {e, a} our 2 elements we have ea^{-1} in H by the second property. Closure is because if a and b are in H, then we just showed

that so is b^{-1}, therefore so is $a\left(b^{-1}\right)^{-1} = ab$. An analagous result can be proven the same way for the case that $e,\ a^{-1}b$ being in H is the condition.

□

[Lecture 3 ends]

Proposition. If H and K are subgroups of G then so is H∩K

Proof. I will not go through the details, however it is trivial to check the axioms.

□

Notation:

For a set x, <x> means the smallest subgroup containing the set x. Equivalently, it is the intersection of all subgroups of a group which contain the entire set. This is called the group generated by the set x.

Of course, the minimal group generated by a set is the set of products of a bunch of not necessarily distinct elements of the set with their inverses.

1.5 Isometries and dihedral groups

There are many functions from $\mathbb{C}$ to $\mathbb{C}$, however any random such function is not very interesting. However, we care about functions that preserve distance.

Definition. An isometry on $\mathbb{C}$ is a function f from $\mathbb{C}$ to $\mathbb{C}$ such that for any 2 points a and b in $\mathbb{C}$, $|a-b| = |f(a)-f(b)|$. In other words, f preserves distances.

The set of isometries of $\mathbb{C}$ is a group since the identity/do nothing function is an isometry, the inverse of an isometry is isometry, function composition (the implied operation) is associative, and the composition of isometries is an isometry. This is called the isometry group of $\mathbb{C}$.

Lemma. if $|y_1 - x_1| = |y_2 - x_1|$ and $|y_1 - x_2| = |y_2 - x_2|$ then $y_1 - y_2$ is perpendicular to $x_1 - x_2$.

Proof. We will do this visually. Figure 3 shows the kite lemma visually.

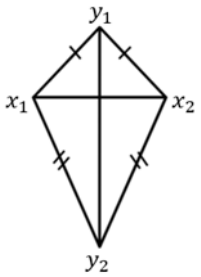

Figure 3

Now we observe that the perpendicular bisector of a line segment is those points that are the same distance away from both ends of the line segment, which explains why the lemma is true.

□

Theorem. If a, b, c are not colinear, and there is an isometry that sends a, b and c to themselves, then this isometry is the identity function.

Theorem. Suppose that the hypotheses above are satisfied but that f is our isometry, then $f(d) = d$.

Suppose that the hypotheses above are satisfied but that f is our isometry and $f(d) \neq d$.

Then, since f is an isometry and sends a b and c to themselves, $|f(d) - f(a)| = |d - a| = |d - f(a)|$

Now let $y_1 := d$ and $y_2 := f(d)$

And in the case where $x_1 := a$ and $x_2 := b$

Then the kite lemma tells us that the line through a and b is perpendicular to the line through d and f(d). But if $x_1 := a$ and $x_2 := c$ then the line through a and c is also perpendicular to the line through d and f(d), contradicting the fact that a, b and c are not colinear.

[Lecture 4 ends]

We will investigate the group D_{2n} which is the group of symmetries of an n-sided polygon.

We can interpret this as the group of isometries of $\mathbb{C}$ that preserves the positions of the vertices but shuffles them around.

The lecturer got stuck on a lot of random details, but essentially this group has size 2n because:

1. There are n choices of where to move the point 1 to in any such isometry
2. There are 2 choices of where to place the adjacent vertices
3. The three point lemma from last lecture fixes the rest

Proposition. Let s be a reflection (ie, each point is sent to its complex conjugate) and r be a rotation (ie, each point is multiplied by $e^{\frac{2i\pi}{n}}$, then $sr^k = r^{-k}s$

Proof. $\overline{e^{\frac{2ik\pi}{n}}z} = \overline{e^{\frac{2ik\pi}{n}}}\overline{z} = e^{\frac{-2ik\pi}{n}}\overline{z}$

□

[Lecture 5 ends]

1.6 Homomorphisms

Definition. Let (G, .) and (H, *) be groups. Then a function φ from G to H is called a homomorphism if for all a and b in G, $\varphi(a.b) = \varphi(a) * \varphi(b)$.

Definition. An **isomorphism** is a homomorphism which is a bijection. Essentially if two groups have an isomorphism between them then they are structurally the same. We say these groups are isomorphic. I will often talk about groups being the same when they are isomorphic.

Example. A function from groups G to H that sends everything in G to the identity of H is a homomorphism, but it is trivial.

Example. It is easy to see that if H is a subgroup of G, then a function H to G that sends all elements to the corresponding element in G is a homomorphism.

Example. The set of square matrices of a certain size with non-zero determinant is a group. The determinant function is a function from these matrices to the non-zero real numbers that is a homomorphism because for matrices A and B, $det(AB) = det(A)det(B)$

Proposition. Let ϕ be a homomorphism G to H. Then $\phi(e_G) = e_H$

Proof. $\phi(e_G)\phi(e_G) = \phi(e_G e_G) = \phi(e_G)$. Therefore $\phi(e_G)$ is the identity, since it can be multiplied by itself and not

change.

□

Proposition. Let ϕ be a homomorphism G to H. Then $\phi\left(g^{-1}\right) = \phi(g)^{-1}$

Proof. $\phi(g)\,\phi\left(g^{-1}\right) = \phi\left(gg^{-1}\right) = \phi(e_G) = e_H$, thus $\phi\left(g^{-1}\right)$ is the inverse of $\phi(g)$.

□

We write A≅B if A is a group isomorphic to B. Isomorphic groups are considered the same group.

Example. The group of positive real numbers under multiplication is isomorphic to the group of all real numbers under addition due to the bijective homomorphism between them defined by the exponential function.

Some obvious statements:

1. If ϕ is an isomorphism so is ϕ^{-1}
2. If ϕ and ψ are isomorphisms so is $\phi \circ \psi$
3. $\cong$ is an equivelence relation as defined in numbers and sets.

Definition. The image of a homomorphism ϕ is the set of stuff ϕ maps to.

Definition. The kernel of a homomorphism ϕ is the set of elements x such that $\phi(x)$ is the identity.

Theorem. Let ϕ be a homomorphism G to G. Then the kernel and image of ϕ are subgroups of G.

Proof. Image:

$e = \phi(e)$ so the identity is in the image

$\phi(g)^{-1} = \phi(g^{-1})$ so inverses of stuff in the image are in the image

$\phi(a)\phi(b) = \phi(ab)$ so products of stuff in the image is in the image.

Kernel:

$\phi(e) = e$ so the identity is in the kernel

If g is in the kernel $\phi(g) = e = e^{-1} = \phi(g)^{-1} = \phi\left(g^{-1}\right)$ so inverses of stuff in the kernel are in the kernel.

If $\phi(a) = \phi(b) = e$ then $\phi(ab) = \phi(a)\,\phi(b) = ee = e$ so we have closure.

□

[Lecture 6 ends]

Proposition.

1. A homomorphism G to H is surjective if and only if its image is H
2. A homomorphism G to H is injective if and only if its kernel is {e}

This result is useful since it allows us to more easily check if a homomorphism is an isomorphism, since an isomorphism is a homomorphism that is injective and surjective.

Proof. 1. This is basically just the definition of surjective.

2. Let ϕ be a homomorphism G to H and suppose it is injective. By the definition of injectivity, only one element can map to the identity of H. Since the identity of G is such an element, it must be the only one, so the kernel of G is {e}. Conversely, suppose that the kernel of G is {e}. Then we want to prove injectivity by supposing $\phi(a) = \phi(b)$ and showing that this implies a=b. So, if $\phi(a) = \phi(b)$ then $\phi\left(ab^{-1}\right) = e$ by homomorphism properties and since the kernel is just e, it means that $ab^{-1} = e$ so $a = b$, completing the proof.

□

1.7 Cyclic and dihedral groups

Definition. A cyclic group is a group generated by a single element. For example, the n'th roots of 1 under multiplication are generated by $e^{\frac{2\pi i}{n}}$. And the integers mod n under addition is generated by 1.

Proposition. In fact, all cyclic groups are isomorphic to either the integers under addition (if they are infinite) or the integers mod n under addition (Which we call C_n if they have size n for finite n).

Proof. Let G be generated by g and S be the set of integers k with $g^k = e$. If some number x is in S, then so is -x since the inverse of the identity is the identity, and 0 is trivially in S, so we can just think about the positive elements of the set.

If S={0} then we never reach the identity – We define a map from $\mathbb{Z}$ to G by sending $k \to g^k$. This is a bijection, since all powers of g are mapped to and the kernel is just 0 since nothing else is in S.

Otherwise let y be the smallest positive element of S, allowed by the well ordering principle. Then the map C_y to G by sending $k \to g^k$ is a homomorphism since $k + j\,(mod\ y) \to g^{k+j} = g^{k+j\ mod\ y}$ since $g^y = e$. Its kernel is $\{0\}$ since if something else z was in the kernel smaller than y then $g^z = 0$ with 0<z<y contradicting the definition of y. Its image is the entire group generated by G has only y distinct elements, since any powers of g can be reduced mod y to something between 0 and y-1, and y different elements get mapped to. So therefore the proof of the proposition is complete.

□

Definition. The order of an element g which we also write as |g| or o(g) is defined as the smallest power of g that equals the identity.

Proposition. Any group of size 2n with elements $r,\ s$ such that $r^n = e = s^2$ and $rs = sr^{-1}$ is isomorphic to D_{2n}.

Proof. We construct here the cayley table and demonstrate that it is unique. This means that the element in the cell of the cayley table is equal to the element in the leftmost column on that row times the element in the topmost row on that column.

The entries highlighted in yellow of the following cayley table (which I claim is unique) are trivially set in stone from the definition above. Note that s is not a power of r otherwise the group would have size n, and thus all elements here are indeed distinct.

Figure 4 shows the cayley table.

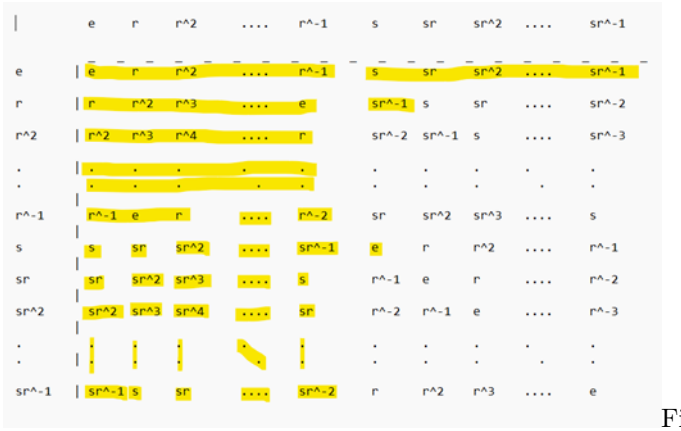

Figure 4

Now we know what multiplying by r on the right will do, so in fact we get some more information for free.

Figure 5 shows the cayley table with more things highlighted as known for sure.

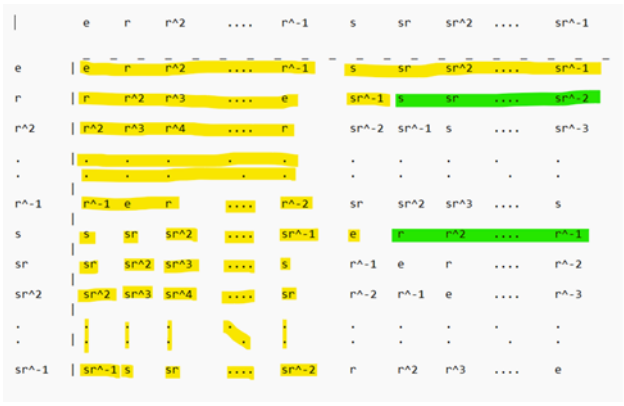

Figure 5

We want to show $r^a s = sr^{-a}$. Note that $rsr = s$ from the table above and therefore $sr^{-a} = (rsr)\, r^{-a} = rsr^{1-a}$. We can apply this repeatedly to get $sr^{-a} = rsr^{1-a} = r^2 sr^{2-a} = \ldots r^a s$. This fills in the blue cells in the image below and thus the purple ones since we can multiply by r on the right.

Figure 6 is also of the Cayley table with stuff highlighted, now taking into account the above fact.

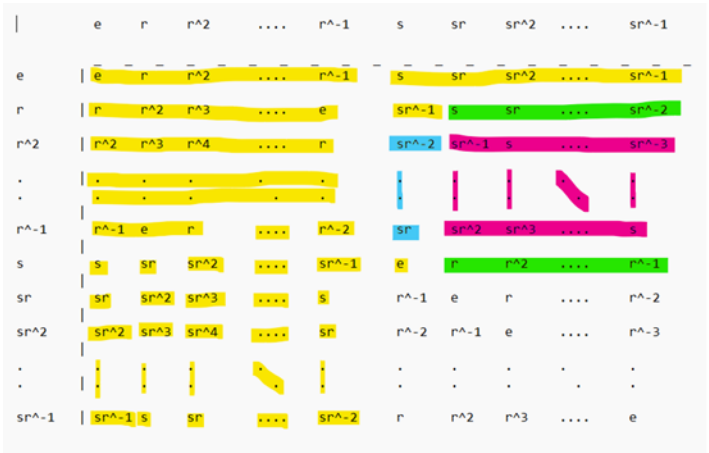

Figure 6

Now it remains to prove that $sr^a s = r^{-a}$ to get the rest of the column with the blue stuff since multiplying by r on the right will give us the rest of the table. To show this is easy: Just multiply s on the left on both sides of the equation $r^a s = sr^{-a}$. So done.

□

[Lecture 7 ends]

2 Cosets and Lagrange's theorem

Theorem. (Lagrange's theorem) If H is a subgroup of G and G is finite then $|H|$ divides $|G|$.

The idea of the proof is pretty simple and obvious once you get it.

Definition. Let H be a subgroup of G and g be an element of G, then the corresponding left coset is the set of elements gh with h in H. The right coset would be defined similarly as the set of elements hg with h in H and the proofs we will do this lecture would be the same.

$G \setminus H$ is defined to be the set of left cosets with respect to H.

Lemma.

1. The union of cosets in a group with respect to any subgroup equals the entire group

2. Cosets are either equal or have empty intersection

Proof. If you have been paying attention this will have reminded you of Equivelence relations from Numbers and Sets. Essentially we will show that the relation a∼b if $a^{-1}b \in H$ is an equivelence relation and that a∼b is equivalent to a and b being in the same coset so that the cosets are actually the equivelence classes. The lemma will follow from basic properties of equivelence relations, ie that they partition sets.

First, we will show that if a∼b then b is in a's coset. We know that $a^{-1}b \in H$ since a∼b by assumption and therefore $a(a^{-1}b) = b$ is in a's left coset with respect to H. But then b's left coset with respect to h contains $b = be$ since the identity is in H since H is a subgroup of G. Conversely, if b is in a's coset then $b = ax$ with x in H, but then since $x = a^{-1}b$ by simple group algebra we have that $a^{-1}b \in H$. Now it remains to show that this is an equivelence relation so it can follow that the cosets are indeed equivelence classes.

Reflexive: a∼a since $e = a^{-1}a \in H$.

Symmetric: If a∼b then $a^{-1}b \in H$ so by inverses, $(a^{-1}b)^{-1} = b^{-1}a \in H$ so b∼a.

Transitive: if a∼b and b∼c then $a^{-1}b, \quad b^{-1}c \in H$ so by closure $a^{-1}c \in H$ so a∼c.

□

Lemma. Fix g in G and a subgroup H of G. Then the map $H \to gH$ (meaning you multiply everything in H by g on the left to get the output) is a bijection.

Proof. Immediate from the fact that a bijection is exactly a map which has a left and right inverse from Numbers and Sets, and such an inverse is given by $K \to g^{-1}K$ so the original map must be a bijection.

□

Definition. The index of a subgroup, denoted $|G : H|$ is the number of cosets in G with respect to H.

However, now we know from the previous lemmas that all cosets with respect to H are the same size and they neatly partition G, and thus $|H||G : H| = |G|$, so |H| divides |G|.

Geometric example of a coset: The set of symmetries of a shape that move a specific vertex to a specific location. also in D_{2n} the set of rotations and the set of elements involving a reflection are cosets as well.

Lets see some examples of why this is useful:

Corollary. The order of an element divides the order of a finite group, because the order of the subgroup generated by that element equals the order of that element which divides the order of the group by Lagrange's theorem.

Corollary. $g^{|G|} = g^{|G:<g>||<g>|} = \left(g^{|<g>|}\right)^{|G:<g>|} = e^{|G:<g>|} = e$.

Corollary. Groups of prime order must be cyclic and generated by all non-identity elements.

[Lecture 8 ends]

Let $\phi(n)$ be the number of integers from 1 to n-1 inclusive that do not have any common factors with n. For some n, let G be the set of such integers with multiplication mod n. If y is in g, there exists integers x and m (this is proven in numbers and sets) such that $xy + mn = 1$, so$xy = 1 \bmod n$, so x is an inverse to y. 1 is an identity and multiplication is associative. Now we just need to check closure: Suppose $ab = c$ and c and n share a common factor: $cb^{-1} = a$ and a is a multiple of c so it also must share the same common factor which is a contradiction, so c is indeed in the set so it is a group.

Now we know that for all g in a group, $g^{|G|} = e$, so in our case this means that if a is coprime to n (meaning a and n share no common factors), then $a^{\phi(n)} = 1 \bmod n$. This is the Fermat-Euler theorem which is proven in numbers and sets, but this proof is here to demonstrate that group theory is actually useful. $a^{p-1} = 1 \bmod p$ which is Fermat's little theorem for prime p is immediate from this.

3 Group actions

3.1 Basic properties

Now we will talk more about the symmetry side of things by talking about group actions.

Definition. An action of a group G on a set X is a map from G*X to X. We write $(g,\ x) \to gx$, you can think of it as what g does to x. It's like each element of g corresponds to a permutation of the elements in x.

Rules for actions:

1. $ex = x$ always
2. $(gh)x = g(hx)$ always

We write $G \curvearrowright X$ to mean G acts on x. If $gx = x$ always this is the trivial action.

Example. S_n acts on the set {1, 2, 3, ... , n} such that if f is a permutation in S_n then $fx = f(x)$.

Example. A subgroup acts on the same set as its parent group.

Example. The group of isometries of $\mathbb{C}$ acts on $\mathbb{C}$.

Example. D_{2n} acts on the vertices of a polygon.

Example. All groups act on themselves such that for elements g and x in g, $gx = gx$, where one side means the action notation and the other side means g and x are being multiplied within the group. This is called the left regular action.

Proposition. An action of a group G on a set X is a homomorphism $\phi : G \to Sym(x)$.

Proof. Suppose$G \curvearrowright X$. Let t_g be the map from X to X that sends x to gx.

This is a bijection because its inverse is the map that sends x to $g^{-1}x$.

This is indeed an inverse because $g^{-1}\left(g\left(x\right)\right) = g\left(g^{-1}\left(x\right)\right) = ex = x$ since we have defined actions to work this way.

However, t_g is now an element of Sym(x) since it is a permutation on x. So define the map $\phi : g \to t_g$. This is a homomorphism because $\phi\left(gh\right) = \left(t_{gh}\right) = t_g \circ t_h$, since $t_{gh}\left(x\right) = \left(gh\right)x = g\left(hx\right) = t_g \circ t_h(x)$.

□

Conversely, given a homomorphism $\phi : G \to Sym(x)$ we can define an action $G \curvearrowright X$ with $gx = \phi(g)\, x$. This is indeed an action since $(gh)\, x = \phi(g)\, \phi(h)\, x = g(hx)$ and $ex = \phi(e)\, x = x$.

Theorem. (Cayley's theorem) Every group is isomorphic to a subgroup of a symmetric group. Furthermore, if G is finite, then G is a subgroup of Sym(x) for some finite x.

Proof. Since $G \curvearrowright G$ by the left regular action, then this is equivalent to a homorphism $\phi : G \to Sym(G)$ by the previous proposition. Let H be the image of ϕ, then since homomorphisms inherit associativity, send products to products, inverses to inverses and identities to identities so H is a subgroup of Sym(G). We need to prove that ϕ is an isomorphism: It is surjective since we defined H to be the image, so we just need to prove that $ker(\phi) = e$. If g Is in$ker(\phi)$ then $\phi(g) = e$, and since this is the identity in $Sym(g)$, this means that $gx = x$ for all x in g, thus $g = e$

□

The intuitive idea for why the theorem above is true is that each element in G corresponds to a permutation in G – Multiplying each element in G on the left by that element permutes the elements.

Definition. Suppose $G \curvearrowright X$ and x∈X. Then the **orbit** of x is the set of all gx with g in G. Example: The orbit of a vertex in the context of D_{2n} is the set of places that the vertex can go to under the symmetries, which in that case is all of them. This is often written as Gx. An action is **transitive** if any x can be taken to any other, such as in the case of D_{2n}.

If we have the same setup as above, then the **stabilizer** of x is the elements g in G such that x=gx. This is often written as G_x or $Stab_G(x)$. An action is **faithful** if the every element in g except the identity does not do nothing to the set it is acting on.

[Lecture 9 ends]

Remark. An action G on X is faithful if and only if the associated homomorphism G to Sym(X) is injective.

Proposition.

1. Suppose G acts on X. Then for any x in X, the stabilizer of x is a subgroup of G.

2. Every element of X is in exactly one orbit, ie the orbits form a partition of X.

Remark. Part 2 will imply that transitivity is equivalent to the statement "there is only one orbit".

Proof (1)

To check if a set is a subgroup, we need to check if e is in the subgroup and if ab^{-1} is in the subgroup for all a and b. I don't know why the lecturer is checking the axioms individually and never proved this criterion to save time. Clearly, the identity is in the stabilizer of x since it does nothing to x. Also, if a and b are in the stabilizer, they do nothing to x, so ab^{-1} also does nothing to x. So done.

Proof (2)

Lets check that being in the same orbit is an equivelence relation. This turns out to be really nice as the three conditions for an equivelence relation correspond to three of the group axioms:

1. Reflexive – x is in its own orbit because of the identity, so this corresponds to existence of an identity element.

2. Symmetric – If x is in y's orbit then y is in x's orbit by the inverse of the element that sends y to x, so this corresponds to existence of inverses.

3. Transitive – If x is in y's orbit and y is in z's orbit, then x is in z's orbit by taking the product of the element sending z to y with the element sending y to x, so this corresponds to closure.

3.2 The orbit stabiblizer theorem

Example. In D_{2n} the stabilizer of a vertex of the n sided polygon it is acting on are exactly the elements which fix it. This always contains the identity and the element that reflects everything about the line through that vertex and the center of the polygon. Notice that the size of the orbit times the size of the stabilizer equals the size of the group: This is an important general theorem which we will prove shortly, but the idea is that the vertex has n places it can go to and exactly 2 ways to go to each vertex so there are 2n total combinations.

Theorem. (Orbit stabilizer theorem) For any group G acting on X, for an element in x, $|Orbit(x)||Stab(x)| = |G|$. Equivalently, the orbit is in bijection with the cosets of the stabilizer since this by Lagrange's theorem would imply $|Orbit(x)||Stab(x)| = |G|$.

Proof. Lets write S to mean Stab(x). Lets define $\Phi : gS \to gx$. Our goal is to show that this is well defined and that it is a bijection from the cosets of S to the orbit of x.

To check that this is well defined, we need to show that if $g_1S = g_2S$ then $g_1x = g_2x$. $g_1S = g_2S$ means that there is an s in S such that $g_1 = g_2s$. But $g_1x = (g_2s)\,x = g_2\,(sx) = g_2x$ by the definition of S, so that proves Φ is well defined.

Proof Φ is surjective: For any gx in the orbit of x, we just need to take the coset constaining g.

Proof Φ is injective: Suppose $\Phi\,(\mathrm{g}_1S) = \Phi(\mathrm{g}_2S)$. Let $s = g_2^{-1}g_1$, then $sx = g_2^{-1}g_1x$. But $\Phi\,(\mathrm{g}_1S) = \Phi(\mathrm{g}_2S)$ so $g_1x = g_2x$. Therefore $sx = g_2^{-1}g_2x = x$, so by definition of S, s is in S. This means that $\mathrm{g}_1S = \mathrm{g}_2S$ as in they are the same coset. So this proves injectivity.

□

Example. Consider the group G of symmetries (isometries) of a cube.

Let x be the center of a face. Then there are eight elements in Stab(x): This is because there are eight symmetries of the face so this is exactly D_8.

The orbit of x has size 6 since x can go to any of the 6 faces.

So, by the orbit stabiliser theorem, G has size 48. The intuition is that x can go to any of the 6 faces and then the faces can be rotated 4 times, by thinking like this the orbit stabiliser theorem becomes intuitive. Even though we have not analyzed this group much at all, we can deduce its size.

[Lecture 10 ends]

Theorem (Cauchy's Theorem): If G is a finite group and p is a prime that divides the order of G, then G has an element of order p. This is a tricky proof because we consider some things where it is not obvious why we are considering them.

Proof. Consider the set X of lists of length p of elements in G (p-tuples, not necessarily distinct) $\{g_1, g_2, g_3, \dots g_p\}$ such that the product $g_1g_2 \dots g_p = e$. Define the action of C_p on the tuple such that for t^x in C_p where t generates C_p,and if $x \in X = \{g_1, g_2, \dots g_p\}$, $t^x x = \{g_{x+1}, g_{x+2}, \dots, g_p, g_1, \dots g_x\}$. It is easy to see that this satisfies the definition of an action. Lets check that it is indeed the case that $g_{x+1}g_{x+2} \dots g_pg_1 \dots g_x = e$. Let $a = g_1 \dots g_x,\ b = g_{x+1},\ g_{x+2}, \dots g_p$. Then ab=e implies ba=e since inverses are two sided, so $t^x x$ is in x. Note that if we pick the elements in g in order there are $|G|$ ways to pick the first p-1 elements then the last one is constrained (it must be the inverse of the product of the first p-1 elements of our set) to make the product be the identity, so there are $|G|^{p-1}$ lists in X.

One principle in maths is that counting something in two different ways always gives interesting results. We know that the C_p action partitions x into orbits, suppose there are k. We know by the orbit stabilizer theorem that the size of any orbit has to divide the order of the group which is p, and thus must be either 1 or p. Let l be the number of orbits of size 1. Lets order the x's such that the size of the orbit of some x is 1 exactly when x is in the first l elements of our order.

So, since the orbits partition X, $|X| = l + p(k-l)$, as X is partitioned into l orbits of size 1 and k-l orbits of size p. But $|X| = |G|^{p-1}$, but since p divides $|G|$, p must divide $|X|$ and thus p divides l. If an orbit of a set x is of size 1, that means shifting the elements in x does not change the contents of the set. Essentially we know that all of the elements of x are the same if and only if the size of the orbit of x is 1. In particular, {e, e, e, ... e} is one such list. Therefore l>0, but p divides l so l is not 1 so there is another tuple {g, g, g, ... g}. This implies g has an order which divides p, and thus has order p by definition. So done.

□

Definition. Let G be a group and g,h be elements. The element hgh^{-1} is called the **conjugate** of g by h. Notice that this is similar to diagonalizing matrices. This is essentially saying do h backwards, do g then do h.

Example. If G is an abelian group, then for any g,h in g, $hgh^{-1} = g$ since $hg = gh$. Therefore in an abelian group, the whole conjugate idea is trivial.

Definition. All of the elements conjugate to g by some element is called the **conjugacy class** of g. This is denoted ccl(g).

Note: G acts on itself by conjugation, ie $h(g) = hgh^{-1}$. This is another way a group can act on itself. It is easy to check that this is an action, and the conjugacy classes are exactly the orbits under this action and therefore partition G.

Definition. The **centraliser** of g is the set of h in g such that $\{hgh^{-1} = g\}$. This is the stabilizer of g under the conjugation action. It is exactly the elements of h that commute with g since $hgh^{-1} = g$ if and only if $hg = gh$. It is a subgroup of G since it is a stabilizer of an action.

Definition. The **center** of G, denoted Z(G) is the elements h in G such that hg=gh for all g in G. This is the intersection of all centralisers of the elements of G. Since we know that the intersection of subgroups is a subgroup, the center of G is a subgroup of G.

[Lecture 11 ends]

4 The mobius group

The mobius group is a group of some bijections from $\mathbb{C}$ to $\mathbb{C}$, with the subtle difference that we are working in $\mathbb{C}$ plus an additional point which we call ∞. In this context we will consider dividing by zero to give infinity.

Now lets put the unit sphere into 3D space (x, y, z) with the x-y plane being the complex plane. What you can see is that there is a bijection from points on this sphere to $\{\mathbb{C} \cup \infty\}$, by drawing a straight line from (0, 0, 1) (which we call the north pole) to the point on the sphere and seeing where it hits the complex plane. The point (0, 0, 1) on the sphere is defined to map to the point at infinity, ie the ∞ point. The intuition is that as we get close to the north pole, the corresponding point on the complex plane gets "closer" to infinity, ie larger.

Definition. Let a, b, c, d be complex numbers such that ad-bc is not zero. Then we define a map f from $\mathbb{C} \cup \infty$ to $\mathbb{C} \cup \infty$ by $f(z) = \frac{az+b}{cz+d}$. If $z = -\frac{d}{c}$, we say that f maps to the point at infinity. The point at infinity maps to $\frac{a}{c}$, since as z gets large it is easy to see that $\frac{az+b}{cz+d}$ goes to $\frac{a}{c}$.

If c=0, then ∞ maps to ∞ and everything else maps to $\frac{az+b}{d}$.

The set of such maps under composition is called the mobius group.

We need to check that this is actually a group. Function composition is associative,the identity is the case c=0, d=1, a=1, b=0. By some easy but tedious algebra one can check that the composition of two such functions is another such function. An inverse can be given by $\frac{dz-b}{a-cz}$, and again this is easy but tedious to check, and in checking this we will actually use the fact that ad-bc is not 0.

We see that $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}$, and that $\frac{a_1z+b_1}{c_1z+d_1} \circ \frac{a_2z+b_2}{c_2z+d_2} = \frac{a_1a_2+b_1c_2z+a_1b_2+b_1d_2}{c_1a_2+d_1c_2z+c_1b_2+d_1d_2}$, so composing these maps is like matrix multiplication.

These functions are called mobius transformations and we will investigate their fixed points, ie points such that f(z)=z.

Proposition. If a mobius transformation fixes 3 points, it must be the identity.

Proof. A fixed point satisfies $w = \frac{aw+b}{cw+d}$. If one of the fixed points infinity, then this is only a fixed point if c=0, so the equation becomes dw=aw+b. This means $w = \frac{b}{a-d}$, so there is only 1 (possibly infinite) root unless a=d and b=0 in which case we have the identity. Otherwise, $cw^2 + dw = aw + b$, which only has at most 2 roots unless d=a and c=b=0, in which case we again have the identity map.

□

Note that in fact we always must fix at least one point: In the first case where infinity is fixed this is trivial, and $cw^2 + dw = aw + b$ always has a root unless d=a and c=0, in which case the fact that c=0 means infinity is a fixed point.

For a mobius map μ, we define Fix(μ)={the fixed points of μ}. Example: If μ(z)=2z, then Fix(μ)={0,∞}.

Proposition. (Triple Transitivity) For any triples of distinct points, there exists a unique mobius map that moves them to any other triple of distinct points.

Proof. Lets write down a mobius transformation $a \coloneqq \frac{(z-z_1)(z_2-z_3)}{(z-z_3)(z_2-z_1)}$. One checks that this sends z_1 to 0, z_2 to 1 and z_3 to infinity. If we define $b \coloneqq \frac{(z-w_1)(w_2-w_3)}{(z-w_3)(w_2-w_1)}$, then $b^{-1} \circ a$ sends z_1 to w_1, z_2 to w_2, z_3 to w_3. This is unique as if there was transformations f and g that sent 3 points to the same 3 points, then $f \circ g^{-1}$ fixes those 3 points so it must be the identity by the previous proposition.

□

The mobius group M acting on $\mathbb{C} \cup \infty$ is triply transitive, meaning that it sends any triple of 3 points to any other triple of 3 points. It is sharply triply transitive because this happens in a unique way.

Definition. Let z_1, z_2, z_3, z_4 be in $\mathbb{C} \cup \infty$. There is a unique a in M such that $a(z_1) = 0, a(z_2) = 1, \quad a(z_3) = \infty$. Then we define the cross ratio $[z_1, z_2, z_3, z_4] \coloneqq a(z_4)$. Since $a = \frac{(z-z_1)(z_2-z_3)}{(z-z_3)(z_2-z_1)}$ from earlier, this means that $[z_1, z_2, z_3, z_4] = \frac{(z_4-z_1)(z_2-z_3)}{(z_4-z_3)(z_2-z_1)}$.

[Lecture 12 ends]

Proposition. The mobius transformations$z \to az,\ z \to z + b,\ z \to z^{-1}$ generate the mobius group.

Proof. Let μ be an arbitrary mobius transformation, and let $z_1 = \mu(0),\ z_2 = \mu(1),\ z_3 = \mu(\infty)$. Construct μ_1 such that $\mu_1(z_3) = \infty$. Then either μ_1 is the identity (if $z_3 = \infty$) or $\mu_1 = \frac{c}{z-z_3}$ where $z = z_3$. Let $z_1' = \mu_1(z_1)$ and $z_2' = \mu_2(z_2)$. Let $\mu_2(z) = z - z_1'$. Then note that $\mu_2(\infty) = \infty$ and $\mu_2(z_1') = 0$. Let $z_2'' = \mu_2(\mu_1(z_2))$. Let $a = \frac{1}{z_2''}$ and $\mu_3(z) = az$, then

$$\mu_3 \circ \mu_2 \circ \mu_1(z_1) = 0,\ \mu_3 \circ \mu_2 \circ \mu_1(z_2) = 1,\ \mu_3 \circ \mu_2 \circ \mu_1(z_3) = \infty.$$

Therefore, if we invert $\mu_3 \circ \mu_2 \circ \mu_1$, we get back μ, and it must be exactly μ by the three point lemma from earlier, but we know that each of μ_1, μ_2, μ_3 was a composition of stuff that we claimed was from the generating set, and thus so is μ. So done.

□

Definition. A circle in this context is either a normal circle or a line which includes the point at infinity.

Normal circles are defined by an equation $|z - c| = r$. Lines can be defined by $|z - a| = |z - b|$ as this equation describes the perpendicular bisector of AB.

Theorem. Under mobius transformations, circles get sent to circles. (Or, in the normal sense, lines or circles are sent to either lines or circles).

Proof. Recall that we have the generating set from before. Clearly, under scaling or rotation or shifting, circles are preserved, so we just have to show that the transformation $z \to \frac{1}{z}$ preserves circles.

Lets say we have a circle $|z-c| = r$, then under this transformation, we have $\left|\frac{1}{z} - c\right| = r$. We can use the equation for a circle which we derive in lecture 2 of Vectors and Matrices to get that $\frac{1}{|z|^2} - \frac{c}{\overline{z}} - \frac{\overline{c}}{z} + |c|^2 - r^2 = 0$. Therefore $\left(|c|^2 - r^2\right)|z|^2 - cz - \overline{cz} + 1 = 0$. If $|c| = r$, then this equation is saying $cz + \overline{cz} = 1$. Therefore we have that $|z|^2 = |z|^2 - \frac{\overline{z}}{c} - \frac{z}{\overline{c}} + \frac{1}{|c|^2} = \left|z - \frac{1}{c}\right|^2$. Therefore, we have $|z| = \left|z - \frac{1}{c}\right|$ which is the equation for a line. It makes sense – If you take a circle through the origin and invert it, we stretch it out.

If $|c| \neq r$, then the equation $\left(|c|^2 - r^2\right)|z|^2 - cz - \overline{cz} + 1 = 0$ becomes $|z|^2 - \frac{cz}{\left(|c|^2 - r^2\right)} - \frac{\overline{cz}}{\left(|c|^2 - r^2\right)} + \frac{1}{\left(|c|^2 - r^2\right)} = 0$. The equation $\left|z - \frac{c}{|c|^2 - r^2}\right|^2 = \frac{|c|^2}{\left(|c|^2 - r^2\right)^2} - \frac{1}{|c|^2 - r^2}$is the same as this, by the vectors and matrices formula, and this is the equation for a circle. So done.

□

Corollary. Four points lie on a circle if and only if their cross ratio is either real or it is infinity.

Proof. Pick 3 points and let them define a circle and suppose we want to test if a fourth point lies on that circle. Let a be the mobius transformation sending $a(z_1) = 0,\ a(z_2) = 1,\ a(z_3) = \infty$ (By a previous proposition this exists and is unique), then $a(z_4) = [z_1, z_2, z_3, z_4]$ (This is exactly the cross ratio as defined last lecture). But then if z_1, z_2, z_3, z_4 lie on a circle then since circles are preserved, it means that $a(z_4)$ must be real or infinity since $a(z_1), a(z_2), a(z_3)$ lie on the real line with infinity, which we defined to be a circle. Therefore the cross ratio is real or infinity. Conversely, if the cross ratio is real or infinity, then $a^{-1}(0,\ 1,\ \infty, [z_1, z_2, z_3, z_4]) = (z_1, z_2, z_3, z_4)$ and thus since $0,\ 1,\ \infty, [z_1, z_2, z_3, z_4]$ lies on a circle, so does z_1, z_2, z_3, z_4 by preservation of circles.

□

[Lecture 13 ends]

5 Classification of small groups

We will now start trying to find all the groups by order up to isomorphism.

There is only one group of order 1 and that is the trivial group.

Lets try to classify the groups of order 2. But remember all groups of prime order must be cyclic. Therefore this gives that 2, 3, 5, 7, 11, ... has only one group up to isomorphism.

Now lets do order 4. We always have C_4 for the case where every element has order 4. So otherwise, every element has to have order 2. We will do a new definition before we construct this group.

Definition. If G, H are groups, their **direct product** (written GxH) is the group of ordered pairs (g, h) with the operation defined in the obvious way (component-wise), and identity (e, e). We can see that associativity is inherited and that the inverse has the inverses in each coordinate.

The Klein-Four group is defined as $K_4 := C_2 \times C_2$. This is not isomorphic to C_4 since every non-identity element has order 2. Before we prove that these are in fact all the groups of order 4, we will talk more about direct products.

Theorem. (Direct product theorem) If $H_1,\ H_2$ are both subgroups of a group G, and $H_1 \cap H_2 = \{e\}$, and everything in H_1 commutes with everything in H_2 (ie $h_1 h_2 = h_2 h_1$), and the set of elements $H_1 H_2$ is in fact all of G, then G is

isomorphic to $H_1 \times H_2$.

Proof. Notice how we will use all the hypotheses given in the theorem statement – If we don't, then something has either gone wrong, or the hypotheses are redundant. Here we assume h_1, h_2 are in H_1 and H_2 respectively. Lets define a map $\phi : H_1 \times H_2 \to G$ such that $(h_1, h_2) \to h_1 h_2$. This is a homomorphism because for any h_1, h_1', h_2, h_2', $(h_1, h_2)(h_1', h_2') = (h_1 h_1', h_2 h_2') = h_1 h_1' h_2 h_2' = h_1 h_2 h_1' h_2'$ by the hypothesis that these things commute. Therefore we have a homomorphism.

It is surjective by the assumption that the set of elements $H_1 H_2$ is all of G.

It is injective because if $h_1 h_2 = e$, then $h_2 = h_1^{-1}$ which is in H_1 and thus in $H_1 \cap H_2$ so it must be the identity. Thus the kernel is trivial, so injective, so done.

□

Remark. If H_1, H_2 have trivial intersection, then we know that $|H_1|\,|H_2| = |H_1 H_2|$.

Now suppose we have a group of order 4 with every element having order 2.

Proposition. If $|G| = 4$ then G is isomorphic to either C_4 or K_4.

Proof. By Lagrange's theorem, either there is an element of order 4 so we are looking at the cyclic group. If not, every element except for the identity must have order 2. Let a, b be elements in G with order 2. Let H_1 be generated by a and H_2 generated by b. It is immediate from the previous remark that $H_1 H_2$ is in G. But it has order 4 so it must be all of G. We know that if a group has all elements of order 2, all elements commute. You should try to prove this yourself before reading on – it's not very difficult.

The proof is that $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$, since everything is self-inverse. So from the direct product theorem, we have K_4.

□

Another application of DPT is to find when a product of Cyclic groups is Cyclic.

Proposition. If Gcd(m,n)=1, then $C_m \times C_n$ is isomorphism to C_{mn}.

Proof. Let $C_{mn} =< g >$. Let $H_1 =< g^n > \cong C_m$, $H_2 =< g^m > \cong C_n$. g^k is in H_1 if and only if n divides k and g^k is in H_2 if and only if m divides k. Since m and n are coprime, g^k is in $H_1 \cap H_2$ if and only if mn divides k, and thus the intersection is the trivial group. C_{mn} is abelian so that condition is immediate. And we know that $C_m \times C_n$ gives the whole group since it has the right size. So done.

□

Now lets move onto order 6. We claim that C_6, D_6 are the only ones. We note that $D_6 \cong S_3$ since D_6 is all the permutations of the vertices so it is essentially the same thing. By cauchy's theorem, let G have order 6, then there is an element s with order 2 and r with order 3. By Lagrange's theorem, the biggest non-trivial subgroup we can find has order 3. Such a subgroup can be the one generated by r. And then we know that $|G : \langle r \rangle| = 2$ and s is not in <r>. Lets consider the cosets s<r> and <r>s. In both cases, we know that since cosets partition the group and there are 2, they are both the complement of <r>. Therefore, we know that $G = \{e,\ r,\ r^2, s,\ sr,\ r^2\} = \{e,\ r,\ r^2, s,\ rs,\ r^2 s\}$. We know that sr is living in the complement of <r> and thus also in <r>s, so we have 3 cases: Either $sr = s$, $sr = rs$, $sr = r^2 s$. The first one is nonsense since r is not the identity, the second one would mean we have C_6 by the direct product theorem (immediately since s and r commute), and the third one would mean we have D_6. This is the smallest non-abelian group.

[Lecture 14 ends]

Now order 7 is trivial due to being prime again so we will do order 8 now.

We know that $C_2 \times C_2 \times C_2,\ C_4 \times C_2, C_8, D_8$ are distinct groups of order 8. Is this all of them? The answer turns out to be no.

We will now define the quaternion group Q_8. This group consists of the following matrices:

$I_2, -I_2, \begin{pmatrix} \pm i & 0 \\ 0 & \mp i \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \pm i \\ \pm i & 0 \end{pmatrix}$. One can check that this is indeed a group not isomorphic to any of our other order 8 groups, we will come back to this. People usually talk about this group in a different way: We call I=1, -I=-1, $\begin{pmatrix} \pm i & 0 \\ 0 & \mp i \end{pmatrix} = \pm i$, $\begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix} = \pm j$, $\begin{pmatrix} 0 & \pm i \\ \pm i & 0 \end{pmatrix} = \pm k$.

By multiplying out these matrices, we can see that $i^2 = j^2 = k^2 = -1,\ (-1)\, i = -i\ etc,\ ij = k,$

$jk = i,\ ki = j$. Notice the similarity to the cross product on the basis vectors. Also -1 commutes with everything. This is called the Quaternion group. This is not abelian (ij does not equal ji) so if it is on our list the only thing it could be isomorphic to is D_8. But Q_8 has 1 element of order 2 and D_8 has 5, so the quaternion group really is different. We will now prove that we have all the groups of order 8.

By Lagrange, every element has order 1, 2, 4 or 8. If there is an element of order 8 we have C_8 so we're done. There certainly are elements of order 2 by Cauchy's theorem. We may not have an element of order 4 though – It could be the case that every element except the identity has order 2. Such a group must be abelian by a previous proposition, so we can choose elements a, b, c where c is not ab and none are the identity and none are equal to eachother, then consider the subgroups generated by these, and use the direct product theorem twice to get that the group must be isomorphic to $C_2 \times C_2 \times C_2$.

Therefore we may suppose that there is an element of order 4 which we will call a and that there is no element of order 8. Lets consider some b not in <a>. Recall that since $|G : \langle a \rangle = 2$, the left coset that is not <a> is the same as the corresponding right coset, as we did earlier. Ie, b<a>=<a>b. This means that $ba = a^i b$ where i is either 0, 1, 2 or 3. i cannot be 0 since a is not the identity so we really have 3 cases. If i=1, ba=ab so we can easily show that $ba^j = a^j b$ for any j so G is abelian. By the direct product theorem on <b> and <a> we must have $C_4 \times C_2$ if b has order 2. Otherwise, b has order 4. In this case $b^2 = a^2$ since if $b^2 = ba^j$ then $b \in < a >$, and if $b^2 = a^j$ with j not 2 then b has the wrong order. In this case, ab^{-1} is an element of order 2, so by the direct product theorem on $< ab^{-1} >$,

$< a >$, we have $C_4 \times C_2$.

The next case is that $ba = a^2 b$. Rearranging we get $bab^{-1} = a^2$. But this is a problem - a^2 has order 2 but bab^{-1} does not have order 2 since if $ba^2b^{-1} = e$ then $a^2 = beb^{-1} = e$, so we have a contradiction.

In the next case, $ba = a^{-1}b$. If b has order 2, then in fact we must have D_8 by a previous lemma.

Note that if $b^2 = ba^j$ for any j then b would be in the subgroup generated by a. This is not possible, so $b^2 \in < a >$. So we have 2 cases: either $b^2 = e,\ b^2 = a^2$. There are no other cases or else b would have to have order 8. We know we get D_8 if $b^2 = e$, so this leaves the case where $b^2 = a^2$. In this case, o(a)=o(b)=4 and $b^2 = a^2$ and $ba = a^{-1}b$. By setting i=a, j=b and k=ab, and $-1 = a^2 = b^2$, we have the Quaternion group. So we know all the groups of order up to 8. We have

1. 1
2. C_2
3. C_3
4. C_4
5. K_4
6. C_5
7. C_6

8. $D_6 = S_3$
9. C_7
10. C_8
11. $C_4 \times C_2$
12. $C_2 \times C_2 \times C_2$
13. D_8
14. Q_8

6 Normal subgroups and quotients

6.1 Definition and basic properties

Definition. A subgroup H of G is normal if for every $h \in H,\ g \in G,\ ghg^{-1} \in H$. We write $H \lhd G$, or $H \trianglelefteq G$ if we allow for H=G.

Remark

1. $1 \lhd G$ and $G \trianglelefteq G$
2. If G is abelian and H is a subgroup of G then $H \trianglelefteq G$.
3. $< r > \lhd D_{2n}$ because if we conjugate by r, this is trivial, and $(sr^a)\, r^b (sr^a)^{-1} = sr^b s = r^{-b}$
4. $< s >$ is not a normal subgroup of D_{2n} because $rsr^{-1} \neq s$.

Proposition. Let ϕ be a homomorphism. Then if h is in the kernel of ϕ and g is in G, then $\phi\left(ghg^{-1}\right) = \phi(g)\,\phi(h)\,\phi\left(g^{-1}\right) = \phi(g)\,\phi(g)^{-1}$ by definition of the kernel $= e$, so ghg^{-1} is in the kernel. Therefore, kernels are always normal subgroups.

[Lecture 15 ends]

In fact, we can think of a normal subgroup as a subgroup which happens to be a union of conjugacy classes.

Lemma. Normal subgroups are exactly those where the left cosets are the same as the right cosets. \begin{proof} $gH = Hg$ for all $g \Leftrightarrow gHg^{-1} = H$ for all g which is the definition of a normal subgroup. I just multiplied both sides by g^{-1}.

Theorem. If H is a normal subgroup of G then the set of cosets G/H is a group with operation $(g_1 H)\,(g_2 H) = (g_1 g_2)\,H$.

Proof. We need to check that this does not depend on our choice of g_1 and g_2 to make sure our operation is well defined.

□

Suppose $g_1 H = g_1' H$ and $g_2 H = g_2' H$. Then $Hg_2 = Hg_2'$. Then there are h_1, h_2 in H such that $g_1 = g_1' h_1$ and $g_2 = h_2 g_2'$. Therefore $g_1 g_2 = (g_1' h_1)\,(h_2 g_2') = g_1'\,(h_1 h_2)\,g_2' = (g_1')\,(g_2')\,h_3$ for some h_3 in H. So we have the same coset.

Now, associativity is inherited. We have H as the identity coset. And we can check the subgroup criterion: For some $g_1 H,\ g_2 H$, we have that $g_1 g_2^{-1} H$ is in the group.

Definition. The **quotient group** G/H for a normal subgroup H is the group of cosets with respect to H under the operation as defined above.

Example. The trivial group and the whole group are normal subgroups and they are the quotient groups of eachother.

Example. Since $\mathbb{Z}$ under $+$ is abelian, all its subgroups n$\mathbb{Z}$ are normal. So the quotient group $\mathbb{Z}/$n$\mathbb{Z}$ is the set of cosets, which is actually isomorphic to C_n. The coset 1+n$\mathbb{Z}$ generates this.

Example. Let G be a group and let $|G:H|=2$. Then H is a normal subgroup with the same proof as above when we were classifying groups of order 6, since we have the gH=Hg criterion.

Note: Just because $D_{2n}/C_n \cong C_2$ this does not mean that $C_2 \times C_n \cong D_{2n}$. So these operations are not inverses of eachother.

However, $A \cong B \times C \Rightarrow A/B \cong C$. We will see a proof of this shortly. This is a consequence of the (First) isomorphism theorem. Note (for vectors and matrices purposes) that if

$B \cong (\mathbb{R}^a, +)$, $C \cong \left(\mathbb{R}^b, +\right)$, then $B \times C = \left(\mathbb{R}^{a+b}, +\right)$, and that any a-dimensional plane is isomorphic by rotation to $\mathbb{R}^a$.

6.2 The (first) isomorphism theorem

Theorem. (Isomorphism theorem) If ϕ is a homomorphism then $G/\ker(\phi) \cong \mathrm{Im}(\phi)$.

Proof. Since the kernel is normal, the image is a subgroup. Let $f : G/\ker(\phi) \to \mathrm{Im}(\phi)$ with the rule that we send the coset $gker(\phi) \to \phi(g)$. We need to check that this is well defined, a homomorphism, injective and surjective.

Well defined: Suppose $gker(\phi) = hker(\phi)$. Then $g = hk$ for some k in the kernel of ϕ. $f(gker(\phi)) = \phi(g) = \phi(hk) = \phi(h)\phi(k) = \phi(h)$ since k is in the kernel and ϕ is a homomorphism. But we have to check that f is also a homomorphism. The proof is: $f((g\ker(\phi))(h\ker(\phi))) = f(ghker(\phi)) = \phi(gh) = \phi(g)\phi(h) = f(gker(\phi))f(hker(\phi))$. Proof that f is injective. Let x be in the kernel of f so $f(xker(\phi)) = e$. Then $\phi(x) = e$ by definition of f so x is in the kernel of ϕ. Therefore x is part of the trivial coset, ie the identity coset, ie $xker(\phi) = ker(\phi)$. To prove surjectivity: For a typical element of $Im(\phi)$, $\phi(g) = f(gker(\phi))$, so done.

□

Example. Because $f(x) = e^{\frac{2\pi ix}{n}}$ is a homomorphism from $\mathbb{Z} \to C_n$ with image C_n and kernel $n\mathbb{Z}$, we get $\mathbb{Z}/n\mathbb{Z} \cong C_n$ by the isomorphism theorem.

Similarly, let the complex unit circle be a group U under multiplication. Then the homomorphism from $\mathbb{R} \to U$ by $f(x) = e^{2\pi ix}$ has image U and kernel $\mathbb{Z}$, so $\mathbb{R}/\mathbb{Z} \cong$U.

[Lecture 16 ends]

Definition. A group G is **simple** if the only normal subgroups of G are 1 and itself. An observation is every homomorphism from a simple group is either trivial or injective since the kernel is normal but cnanot be anything other than 1 or G by simplicity.

Definition. A cyclic group of prime order is simple. This is because there cannot be any subgroups other than 1 and itself, so certainly not any normal subgroups.

Recently mathematicians have classified all finite simple groups but it is a massive piece of work that takes tens of thousands of pages that people are still working on writing down properly. We will now study permutations in more detail. Recall that a permutation of a set X is a bijection X to X and Sym(X) is the group of such permutations under composition. Now we're getting into the theory of Rubik's cubes.

7 Permutations

7.1 Basic properties

Definition. Any ordered list of k distinct elements in our set X determines a k-cycle. We just write it as a list like $(a_1 a_2 \dots a_k)$. What this does is takes $a_1 \to a_2, a_2 \to a_3, \dots a_k \to a_1$. We can write a permutation by tracing the cycle of 1 and then tracing the cycle of another element that was not in that cycle until we are done and then expressing the permutation as a product of disjoint cycles. If something is sent to itself, by convention we don't write it.

Example. If 1, 2, 3, 4, 5, 6 is sent to 6, 3, 5, 4, 2, 1 we can write it as (1 6) (2 3 5). We can multiply cycles together and we need to start from the right.

Example. Lets do (1 2)(1 3 2). Multiplying cycles means to compose them. If they are disjoint (ie consisting of different elements) there is not much we can do.

Lets start from the right and trace where 1 goes to. It goes to 3 (second cycle) and then to nothing (first cycle). 3 goes to 2 (second cycle) which goes to 1 (first cycle). So we have a cycle (1 3). 2 should not move because we have a bijection. We can verify this: 2 goes to 1 and back to 2 again. So we have the product (1 2)(1 3 2)=(1 3).

Example. (1 4 3 2)(2 4 3)=(1 4 2 3) which we can check using the same procedure as above.

Remark. The cycle $(a_2 a_3 \dots a_k a_1)$ is trivially equal to $(a_1 a_2 a_3 \dots a_k)$. But it is only in S_3 that every permutation is a cycle. In S_4, we may have something like (1 2)(3 4). These are disjoint because they share no elements. Note that disjoint cycles commute, and this is easy to see: The cycles are doing things to different elements so the order in which we do stuff does not matter since there is no interaction between the sets since they are disjoint. Eg, since (1 2) (3 4) is a product of disjoint cycles it is equal to (3 4) (1 2). The idea is we will write all finite groups as products of disjoint cycles.

Theorem. Every permutation of a finite set is a product of disjoint cycles.

Proof. We can do this constructively as above by picking an element and tracing where it goes and picking an untouched element and tracing that until we are done.

□

Theorem. Every permutation of a finite set is a product of disjoint cycles in a unique way up to reordering the cycles and using $(a_2 a_3 \dots a_k a_1) = (a_1 a_2 a_3 \dots a_k)$, ie starting the cycle somewhere else.

Proof. This result is intuitive but we will prove this formally. Before the proof, we will do an example. Lets try to multiply (1 2)(3 4)(5 6)(1 2 3 4 5 6). 1 goes to itself, 2 goes to 4, 4 goes to 6, 6 goes to 2 and we're back. Now let's try 3, it goes to itself and so does 5. So (1 2)(3 4)(5 6)(1 2 3 4 5 6)=(2 4 6). It is easy to see that we're not gonna have any different product of disjoint cycles since that would imply an element is sent to a different element. Now we will actually prove uniqueness:

Let <f> be the subgroup of permutations in Sym(x) generated by a permutation f. We know from earlier theory that the permutations in <f> acting on X partitions the set X into orbits. The orbit of an element i in x is $i,\ f(i),\ f(f(i)),\ \dots,\ f^{-1}(i)$. So these orbits really do decompose our permutation into disjoint cycles in the way that we want. The only sense in which this was not unique was the choise of orbit representatives (equivalent to shifting elements in a cycle) and the order in which we chose them (equivalent to shifting the order of cycles), so we have uniqueness up to those choices, exactly as required.

□

Definition. The cycle type of a permutation is the unordered list of the size of the disjoint cycles of that permutation. Eg, (1 6)(2 3 5) has cycle type (2,3). But we omit 1's in the cycle types by convention because they're not very interesting.

Remark. The order of a permutation is the lowest common multiple of the numbers in the cycle type.

Definition. A 2-cycle is also called a **transposition**.

Theorem. The set of all transpositions generate the symmetry group on a finite set.

Proof. We can write it as a product of disjoint cycles. But, eg, (1 2 3 4) = (1 2)(2 3)(3 4) and similarly we can decompose any cycle into transpositions.

□

Alternative proof (by induction): It is clearly true for n=2. The only transposition is (2 1) and that generates S_2.

For the inductive step, assume that S_{n-1} is generated by transpositions. Let σ be any element of S_n. If $\sigma(n) = n$, then $\sigma$is in S_{n-1} so it is a product of transpositions. Otherwise, let γ be the transposition $(n\ \sigma(n))$. But $\gamma\sigma(n) = n$so $\gamma\sigma$ is in the natural copy of S_{n-1} sitting in S_n. Therefore, $\gamma\sigma$ is a product of transpositions. But then so is $\gamma\gamma\sigma$ since we just multiplied by a transposition, but $\gamma\gamma = e$ since γ is a transposition, thus we have σ as a product of transpositions. So done.

In fact, the generating set can be made by only swapping neihbouring things. This is called an adjacent transposition. To see why, it is because, eg, (14) = (12)(23)(34)(23)(12).

[Lecture 17 ends]

7.2 The sign of a permutation

We see from the method above that any transposition can be written as not only a product of adjacent transpositions, but an odd number of them.

Theorem. Permutations have a well defined parity – We get there by either and odd or even number of swaps and this cannot change. Equivalently we cannot get from the permutation back to itself in an odd number of swaps.

Proof. There is a proof in my vectors and matrices notes, but we will prove it in a different way shortly.

□

We will show that we need an even number of adjacent transpositions to get to where we started, since after that if we had an odd number of transpositions we could turn it into an odd number of adjacent transpositions.

A pair {i, j} in {1, 2, 3, ... ,n} is an inversion of a permutation if i<j but $\sigma(i) > \sigma(j)$.

Lemma. If $\sigma$is a product of k transpositions, then k is the number of inversions of σ mod 2.

Proof. (Induction on k) If k=1 and we have 1 transpositions we must have 1 inversion, if we have 0 transpositions we have 0 inversions. So we have base cases. Now we need to do the induction step.

Lets call $\sigma = T_1\sigma'$ where T_1 swaps l with l+1 and σ' is a product of k-1 transpositions. We want to show that the number of inversions of σ is one more or one less than the number of inversions of σ'. Anything not involving l or l+1 will not change. Consider the pair i, j such that $\sigma'(i) = l,\ \sigma'(j) = l+1$. Then we have that $\sigma(i) = l+1 > l = \sigma(j)$. Therefore the inversion status of the pair i,j will be reversed. For any other pair, the order will not be affected when we change σ' to σ as we will change between l and l+1 possibly but the other thing we change will stay more or less so we are done with the lemma.

□

Therefore the number of inversions is like a "fingerprint" for how many swaps we have done. So this proves the original statement. In particular, the identity has 0 inversions so we have to have done an even number of transpositions or else we would have an odd number of inversions.

Now we know why if we swap two pieces on a standard rubiks cube we cannot solve it using legal moves because all legal moves can be made from an even number of piece swaps (a rotation is the same as a 4-cycle of corners and 4-cycle of edges).

Theorem. (sign homomorphism) The map $sign: S_n \to C_2$ defined by sending the number of swaps k to $(-1)^k$ is a well defined homomorphism.

Proof. It is well defined by the previous theorem. So we just need to check that it is actually a homomorphism. Note that $\phi(\sigma_1\sigma_2)$ has $k_1 + k_2$ swaps from $\sigma_1,\ \sigma_2$ respectively. Then

$$\phi(\sigma_1)\phi(\sigma_2) = (-1)^{k_1}(-1)^{k_2} = (-1)^{k_1+k_2} = \phi(\sigma_1\sigma_2)$$

□

Now we will define the alternating group as the kernel of this, ie the group of even permutations. We denote A_n for this, and this is a normal subgroup of S_n since it is a kernel and alternatively because it is half the size.

Example. $A_3 = \{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\}$, which is isomorphic to the rotations of a triangle. We get this by considering how we are permuting the vertices, or from the fact that there is only one group of order 3. In fact, $A_3 \cong C_3$.

Remark. The cycle type makes it easy to determine the sign of a permutation as we did with the Rubik's cube example above. A k-cycle $(a_1a_2\dots a_k)$ can be written as $(a_1a_k)(a_1a_{k-1})\dots(a_1a_3)(a_1a_2)$ which has $(k-1)$ transpositions. So it is even if and only if k is odd. Therefore the product of two 4-cycles is the product of two odd things which is even, justifying the example above.

More generally, the cycle type $(k_1, k_2, \dots, k_l)$ is even if and only if the number of even k's (which contribute an odd number of swaps) is even.

Example. (2,2) is an even cycle type, (2,2,2) is an odd cycle type. Adding odd numbers to the cycle type changes nothing and each even number added or remove flips the sign of any permutation of the cycle type.

7.3 Conjugacy classes in permutation groups

Proposition. The conjugacy classes of S_n are exactly the cycle types. Elements are conjugate if and only if their cycle types are the same.

Idea: If we move stuff around, then do some cycles, then move the stuff back, we still did the same cycles to stuff, just moved around.

Proof. Let $\sigma_1 = \left(a_1^1 \dots a_{l_1}^1\right) \dots \left(a_1^k \dots a_{l_k}^k\right)$ and let σ_2 have the same cycle type, so

$\sigma_2 = \left(b_1^1 \dots b_{l_1}^1\right) \dots \left(b_1^k \dots b_{l_k}^k\right)$ (both allowed as we can write permutations as products of disjoint cycles). If we include 1-cycles, then the things a_i^j are exactly all the elements 1 to n. We can now define a permutation T that sends a_i^j to b_i^j. Now we want to consider $T\sigma_1T^{-1}$: This sends b_i^j to a_i^j then to $a_{i+1 \ mod\ l_i}^j$ then to $b_{i+1 \ mod\ l_i}^j$, so it does the same thing to each element as σ_2, so σ_1 and σ_2 are indeed conjugate, as required, and thus in the same conjugacy class.

We need to show that if we have two conjugate permutations then they have to have the same cycle type.

[Lecture 18 ends]

Finishing the proof that conjugate permutations are exactly those that have the same cycle type: Suppose $\sigma_2 = T\sigma_1T^{-1}$. The above argument shows that if $\sigma_1 = \left(a_1^1 \dots a_{l_1}^1\right) \dots \left(a_1^k \dots a_{l_k}^k\right)$ then we saw that if we write $b_i^j = T(a_i^j)$ then $\sigma_2 = \left(b_1^1 \dots b_{l_1}^1\right) \dots \left(b_1^k \dots b_{l_k}^k\right)$ and thus will have the same cycle type. This works for any T because we can pick any b's depending on where T sends the a's even if T is chosen arbitrarily. This seems abstract but as before there is an intuition for this.

□

We can now count conjugacy classes in S_n and A_n. Lets start with S_3. Its only possible cycle types are (3) which has 2 elements and (2) which has the 3 "reflection" elements and e, since those are the only ways to partition 3 into cycle "classes" up to ordering. Therefore those are the three conjugacy classes.

S_4 has conjugacy classes (4), (3), (2,2), (2), e.

Example. The number of (2,2) cycles in S_4 is 3 because the only possibilities are (1 4)(2 3), (1 3)(2 4) and (1 2)(3 4).

Recall that if a group acts under conjugation, then the orbit stabiliser theorem implies that the size of the centraliser of an element equals the size of the group divided by the size of the orbit which is the size of the conjugacy class.

Therefore, we can find all the centralisers, and we know (in fact we know this for general finite groups) that the size of a conjugacy class divides the order of the group.

Example. The centraliser of (1 2)(3 4) has size 8 because it has to be 24 divided by 3 as 3 is the size of the conjugacy class.

Indeed, if we try to make a list of elements that commute with (1 2)(3 4) we will know we are done when we have 8. We can write down {e, (1 2)(3 4), (1 2), (3 4), (1 3)(2 4), (1 4)(2 3), (1 4 2 3), (1 3 2 4)} which we can verify manually in theory.

We can now make a table:

Cycle type in S_4	Size of conjugacy class	Size of centraliser
e	1	24
(2)	6	4
(3)	8	3
(4)	6	4
(2,2)	3	8

Example. To find how many 3-cycles there are, we see that we can choose any 3 things to be cycled and then have 2 possible orders, so we get $2\begin{pmatrix} 4 \\ 3 \end{pmatrix} = 8$. We can do a similar method for all of them. And we see that the size of the conjugacy classes **add up** to the size of the group which is 24, which suggests we have done this correctly.

Lets now look at alternating groups:

Lemma. Let $\gamma \in A_n$

1. If some odd element of S_n commutes with γ then the conjugacy class in A_n of γ is equal to the conjugacy class in S_n of γ

2. If every element in S_n that commutes with γ is even, then the conjugacy class splits into 2. We will find that $ccl_{S_n}(\gamma) = ccl_{A_n}(\gamma) \cup ccl_{A_n}(t\gamma t^{-1})$ where t is any transposition.

Proof.

$$|S_n| = |ccl_{S_n}(\gamma)|\,|C_{S_n}(\gamma)|$$
$$|A_n| = |ccl_{A_n}(\gamma)|\,|C_{A_n}(\gamma)|$$

By the orbit stabiliser theorem.

We can rearrange (using $|S_n| = 2\,|A_n|$) to get $|ccl_{S_n}(\gamma)| = 2\frac{|C_{A_n}(\gamma)|}{|C_{S_n}(\gamma)|}\,|ccl_{A_n}(\gamma)|$

Now $C_{A_n}(\gamma)$ is exactly the even things that commute with γ. This is equal to the kernel of $C_{S_n}(\gamma)$ under the sign permutation. The image has size 1 or 2, so by the isomorphism theorem the index $|C_{S_n}(\gamma) : C_{A_n}(\gamma)|$ is either 1 or 2.

If there is an odd element of S_n in $C_{S_n}(\gamma)$ then that is exactly saying that $C_{A_n}(\gamma) \neq C_{S_n}(\gamma)$. Therefore this corresponds to the case where the index $|C_{S_n}(\gamma) : C_{A_n}(\gamma)|$ is 2, then $|ccl_{S_n}(\gamma)| = |ccl_{A_n}(\gamma)|$ by the equation we got from orbit-stabiliser, which corresponds to case (i) of the lemma.

Otherwise, the index is 1, which will imply $|C_{S_n}(\gamma)| = |C_{A_n}(\gamma)|$ and $|ccl_{S_n}(\gamma)| = 2\,|ccl_{A_n}(\gamma)|$. Now pick an element σ in $|ccl_{S_n}(\gamma)|$ not in $|ccl_{A_n}(\gamma)|$, then we know that $|ccl_{A_n}(\sigma)| = |ccl_{A_n}(\gamma)|$ is the only possibility so it indeed splits into 2.

Now let t be a transposition, then consider $t\gamma t^{-1}$. If this is in $ccl_{A_n}(\sigma)$, then there is an α in A_n with $\alpha\sigma\alpha^{-1} = t\gamma t^{-1}$, but then the problem is that $t^{-1}\alpha = t\alpha$ (since t is a transposition) commutes with γ and is odd, contradicting the assumption in the lemma.

□

Example. We want to decide if in A_4 the conjugacy classes e, (2,2) and (3) break into 2.

(3) must break into 2 since otherwise the centraliser would have size 1.5. e cannot break into 2 because it has sice 1. There are 3 (2,2) cycles which cannot evenly split into 2. Representatives for the two new conjugacy classes of (3) are (1, 2, 3) and (3, 2, 1).

[Lecture 19 ends]

Lets now look at conjugacy in S_5 and A_5. In S_5 we can count the cycle types, if we do it carefully we see that all of them are:

e, (2), (3), (4), (5), (2,2), (2,3).

Cycle type	Size of ccl	Size of centraliser
e	1	120
2	$\binom{5}{2}$=10	12
3	$2 * \binom{5}{3}$=20	6
4	$6 * \binom{5}{4}$=30	4
5	24	5
2,2	$\frac{1}{2}\binom{5}{2}\binom{3}{2}$=15, half so we don't double count swaps in the other order	8
2,3	20 (same as 3-cycles then forced to swap other 2)	6

As a sanity check we see that the sizes of the conjugacy classes indeed add up to 120.

In A_5, only e, (3), (5), and (2,2) remain, and we need to decide which conjugacy classes split into 2. e and (2,2) do not since they have an odd number of elements, (5) does because its centraliser would have 2.5 elements otherwise. So only (3) needs more careful analysis. Remember that a ccl will split exactly if we can find an odd thing that commutes with it. (4 5) commutes with (1 2 3) so the conjugacy class of (1 2 3) does not split. Now we can make a table of conjugacy classes in A_5.

Cycle type	Size of ccl	Size of centraliser
e	1	60
3	20	3
5	12 (2 conjugacy classes)	5
2,2	15	4

The numbers 1, 20, 12, 12, 15 do add up to 60 which is reassuring.

Theorem. A_5 is simple (it has no non-trivial normal subgroups)

Proof. Suppose N is a normal subgroup of A_5. Then the order of N divides 60. But N has to be a union of conjugacy classes (for n in N, $gng^{-1} \in N$ so ccl(n) is a subset of n). N also contains e. So here are the possible sizes of unions of

conjugacy classes in A_5.

Possibilties:

1. 1+12=13
2. 1+12+15=28
3. 1+12+20=33
4. 1+12+15+20=48
5. 1+12+12=25
6. 1+12+12+15=40
7. 1+12+12+20=45
8. 1+15=16
9. 1+20=21
10. 1+15+20=36

Those are all the possible sizes of non-trivial normal subgroups. None divide 60, so by Lagrange's theorem we are done.

□

8 Matrix groups

Now we will study matrix groups.

$\{M_n(\mathbb{R})\}$ is the set of n*n matrices in the real numbers. This forms a group under addition, and under multiplication it is almost a group if we exclude matrices with determinant 0 to ensure existence of inverses of everything, since associativity is a known property of matrix multiplication. We write $GL_n(\mathbb{R})$ to mean the group of n*n invertible real matrices under multiplication.

Determinant is a homomorphism from this group to the non-zero reals under multiplication as seen as an example when we defined homomorphisms. We can get a kernel of this to make a subgroup: We can write $SL_n(\mathbb{R})$ to mean the group of matrices with determinant 1 and real entries under multiplication. By the isomorphism theorem the quotient of this isomorphic to the non-zero real numbers under multiplication.

Everything here can be done with $\mathbb{R}$ replaced with $\mathbb{C}$.

See vectors and matrices to see what it means for matrices to be similar. But notice that this exactly means that they are conjugate! This conjugation action is basically change of basis.

Proposition. Let V be an n-dimensional real vector space (See vectors and matrices to see what this means) and a be a linear map V to V. If A is an n*n matrix that represents a in some basis, then the orbit of A in $GL_n(\mathbb{R})$ under conjugation, ie the set PAP^{-1} is exactly all the matrices that represent a. This is because the set of invertible matrices P is exactly the set of linearly independent bases we can represent a under, if this makes sense.

Coordinate-independent alternative proof of proposition: A basis defined an isomorphism of n-dimensional vector spaces V from $\mathbb{R}^n$ to V defined in the obvious way (component-wise).

When we say "A represents a", we mean that the isomorphisms in the right arrows are the same in this diagram in figure 7.

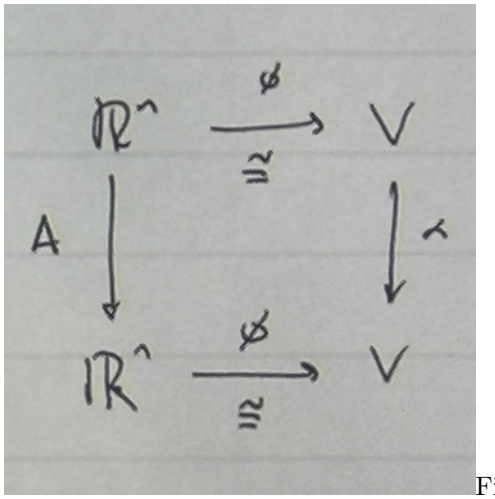

Figure 7

[Lecture 20 ends]

Now we write $a = \phi A \phi^{-1}$. Another basis corresponds to a different isomorphism $\psi : \mathbb{R}^n \to V$, whose basis vectors depends on where $(0, 0, \ldots, 1, \ldots, 0, 0)$.

The transformation $\beta = \psi^{-1} a \psi = \psi^{-1} \phi A \phi^{-1} \psi = PAP^{-1}$ where $P = \psi^{-1}\phi$, where $\psi^{-1}\phi$ is a linear map P to P that is represented by P in the standard basis. Thus the orbit consists exactly of matrices representing a in the different possible bases. P is invertible as it is a bijection V to V, its inverse is $\phi^{-1}\psi$ which we know is also a bijection.

We noticed that multiplication in the mobius group was like 2*2 matrix multiplication. We can now say, precisely, that $GL_2(\mathbb{C})$ is almost isomorphic to the mobius group with the obvious isomorphism.

Proposition. The mobius is the isomorphic to the quotient group $GL_2(\mathbb{C})/\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, and the latter is actually a normal subgroup.

Proof. Lets define a map $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \frac{az+b}{cz+d}$ which is a homomorphism which we showed when we were looking at matrix multiplication. This is surjective and the kernel is when this is the identity, which is exactly when a=d and b=c=0 (as it is exactly when we fix 0, 1 and infinity), so the isomorphism theorem applies and we get the proposition.

□

We define an orthogonal matrices to be matrices that preserve lengths of vectors under linear maps.

Proof this is equivalent to other definitions:

For vectors u,v we nave by simple algebra that $2\,(u.v) = |u|^2 + |v|^2 - |u - v|^2$, so if lengths are preserved then we can substitute u for Au and v for Av into this equation and therefore dot products are preserved as well (RHS (right hand side) will be the same by length preservation so so is LHS). Conversely if we always have that Ax.Ay=x.y, then Ax.Ax=x.x, therefore the length of Ax equals the length of x.

Proposition. This defintion is equivalent to the defintion that the columns form an orthonormal basis. This part will assume knowledge of what δ_{ij} means and what a basis is – see vectors and matrices.

Proof. Consider the standard $\{e_i\}$ basis. Then $\delta_{ij} = e_i.e_j = Ae_i.Ae_j$ so the columns are orthonormal. Because of this, we know that columns orthonormal in A implies $A^T A = I$. But then if we assume this, we easily see that $(Ax.Ay) = x^T A^T Ay = x^T y = x.y$, so dot products are preserved, so this is the converse and we have the equivalence.

□

Now we can see that orthogonal matrices form a group – products and inverses preserve distance and satisfy $A^TA = I$. Their determinant is always 1 or -1 since they are invertible (As $Det(A) = Det\left(A^T\right)$ so $Det(A)^2 = 1$).

[Lecture 21 ends]

The special orthogonal group SO(n) is the group under multiplication of the orthogonal n*n matrices with determinant 1. Since the determinant of an orthogonal matrix is 1 or -1, this is essentially the kernel of the determinant homomorphism as a map from the orthogonal group to the determinant. This is a subgroup of the orthogonal group with index 2 (as there are orthogonal transformations with determinant -1, just take the identity and convert one of the 1's to a -1).

Note that any vector v in $\mathbb{R}^3$ defines a plane perpendicular to it. We can note from Vectors and Matrices when we gave this general formula for reflections about spaces that the matrix reflecting about the normalized vector v (ie rotating 180 degrees around it) is given by $I - 2vv^T$, then we see geometrically that if we take minus this we will end up with a reflection about the plane. Therefore we can write $2vv^T - I$ as a reflection about the plane, provided v is normalized.

As a sanity check lets see algebraically why the reflection about the plane perpendicular to a unit vector v $2vv^T - I$ actually preserves lengths, in order to complement the idea that we know it geometrically.

$\left(2vv^T - I\right)x = 2vv^Tx - Ix = 2v(v.x) - x$. $|2v\,(v.x) - x|^2 = (2v\,(v.x) - x)\,.\,(2v(v.x) - x) = 4v.v(v.x)^2 - 4(v.x)^2 + (x.x) = (x.x) = |x|^2$ because v.v=1, so yes it preserves lengths.

Note that in the basis with v included and everything else perpendicular, our matrix will be represented by a diagonal matrix with 1 in all but 1 entry with -1, so the determinant of any reflection is -1.

Theorem. Every matrix in O(n), ie the group of $n * n$ orthogonal matrices, is a product of at most n reflections.

Proof. Induction on n. This is not hard to see for n=1 where the only orthogonal matrices are (1) and (-1) which are products of 0 and 1 reflections respectively.

Induction step: Fix $A \in O\,(n)$. Consider the standard basis for $\mathbb{R}^n$. Let $v = e_n - Ae_n$. Then a reflection about the plane perpendicular to v will move e_n to Ae_n, as we have defined v to be this way. If we start in the A-transformed world and then apply this, everything else will be perpendicular to e_n since this is all orthogonal transformations. Therefore all the first n-1 transformed basis vectors will be in the natural copy of $\mathbb{R}^{n-1}$, which we can move back to their original positions with n-1 reflections by our induction hypothesis. Therefore we go from the transformed-world to the nothing-world in n reflections which we can just reverse.

□

We can use this theorem when n=2. Since reflections have determinant -1, everything in the special orthogonal group is a product of either 0 or 2 reflections since they have determinant 1.

Lemma. If A is in SO(2) then it is a rotation about the origin. Otherwise it is a reflection

Proof. If it is a product of 0 reflections it is the identity. If it is not in SO(2) then the number of reflections has to be 1 so we do have a reflectoin. If it is a product of 2 reflections we can write $A = S_uS_v$ where S means reflect about this line. $S_uS_vx = x$ means $S_ux = S_vx$ since reflections are self inverse. But v is parallel to $x - S_vx$ and similarly for u, so they are parallel if this happens, which would mean we have the identity. Therefore any non-identity thing in SO(2) is a distance preserving transformation that only fixes the origin. The columns being orthonormal and the determinant being 1 implies the matrix can be written as $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ with $a^2 + b^2 = 1$ so we can write a and b as $\sin(\theta), \cos(\theta)$ for some θ.

□

Lemma. Anything but the identity in SO(3) is a product of 2 reflections and is either the identity or a rotation about a line.

Proof. Anything in SO(3) has to be the product of an even number of reflections, which means if it is not the identity it is a product of 2 reflections. For non parallel u and v the planes perpendicular to u and v through the origin intersect in a line. Therefore this line is fixed by the reflections. By considering what happens to two vectors perpendicular to those lines we see that those must rotate as they stay perpendicular to this line.

□

[Lecture 22 ends]

9 Platonic solids

Now we will talk about platonic solids. While there are infinitely many regular 2 dimensional polygons (triangles, squares, pentagons, hexagons, etc)

Definition. A convex polyhedron $X \in \mathbb{R}^3$ is a platonic solid if every face is a regular polygon of the same type, and the isomstries act transitively on all the faces, and if x is the midpoint of a face then the stabilizer of x under the isometries is isomorphic to the symmetries of the face.

There are five platonic solids: The tetrahedron (4 triagnular faces), the octahedron (8 triangular faces), the icosahedron (20 triangular faces), the cube (6 square faces) and the dodecahedron (12 pentagonal faces). You can prove this by going through the possibilities types of polygons and how many can meet at each vertex.

Figure 8 is an image of the platonic solids.

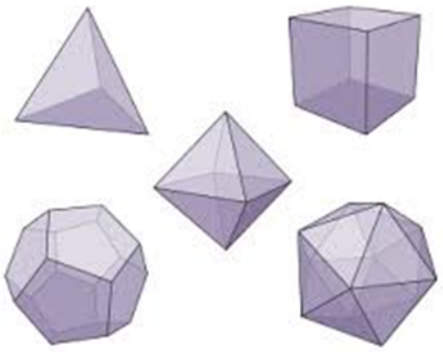

Figure 8

We have five groups to identify for symmetries of these, but it actually turns out that there are only three distinct groups up to isomorphism.

Two solids X and Y are dual if Y can be constructed from X by putting vertices in the center of each face and then joining vertices in adjacent faccts by edges. I'll show what this means using the diagram below that shows that the cube and octahedron are dual. See figure 9.

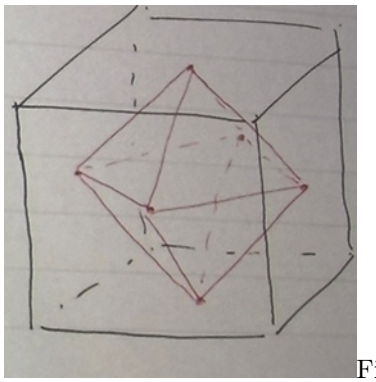

Figure 9

We can see geometrically that if we try to find the dual of the octahedron we will just get a smaller version of the cube. It turns out that the dodecahedron and icosohedron are dual as well, and the dual of a tetrahedron is itself.

Dual things have isomorphic symmetry groups: We can see that any isometry of a cube is an isometry of the octahedron (from the diagram above) and vice versa, and since we have this double inclusion (X contained in Y and Y contained in X) of these finite groups it means they are the same.

Note that the group of isometries of the tetrahedron is isomorphic to S_4 as it is exactly the permutations of the 4 vertices. We can do any swap of 2 vertices by a reflection and thus we generate all of S_4. Formally, there are 4 faces and each one has 6 symmetries so by orbit-stabiliser the size of G is 24. Now let G act on the vertices, then this defines a homomorphsim $G \to S_4$ which is surjective (because we can get any permutation as mentioned above), and injective as the homomorphism only goes to the identity if all 4 vertices are fixed, and this is obviously the identity so the kernel is trivial, so we indeed have a bijection and thus an isomorphism.

We want to identify group of rotational symmetries of the tetrahedron is $G \cap SO(3)$

Lemma. If H is a subgroup of S_n and H has index 2 then $H = A_n$.

Proof. Subgroups of index 2 are always normal. We also have a homomorphism from $S_n \to C_2 = \pm 1$ with kernel H. If this homomorphism sent all transpotisions to 1 then since transpositions generate all of S_n then the kernel would be the whole of S_n. So there is a transposition T that is sent to -1. But then all transpositions are conjugate to this, and thus are sent to -1 as $\phi\left(ABA^{-1}\right) = \phi(B)$ because the range of our homomorphism is an abelian groups so we can expand it using the definition of a homomorphism and cancel the conjugate things. So we are sent to 1 if and only if we have an even number of transpositions. So $H = A_n$.

□

By this lemma, the group of rotations of a tetrahedron is A_4. The rotation group has index 2 because it is the kernel of the determinant homomorphism which has image C_2.

The cube has the same symmetry group G as the octahedron. Now by orbit-stabiliser G has size 48 (in fact we did this example ages ago when we introduced orbit-stabiliser). The group of rotations Htherefore has size 24. G actually acts on the set of the four long diagonals of the cube. We want to show that $\phi : H \to S_4$ is surjective because then it will have to be injective as the sets have the same size. Since transpositions generate we just want to show that each one is in the image of ϕ. Now rotate half a rotation about the axis through an edge and an opposite edge, this transposes two long diagonals. There are six such axes we can rotate about to swap a different set of long diagonals, but there are only six possible swaps of long diagonals so we achieve all six of them. We are missing the symmetry -I, but if we add this in it commutes with everything in S_4, so by the direct product theorem our group is isomorphic to $S_4 \times C_2$.

[Lecture 23 ends]

Now lets identify the symmetry group of the dodecahedron and therefore also the icosahedron.

Let G be the isometry group of a dodecahedron acting on the faces. The orbit has size 12 and the stabiliser is isomorphic to D_{10} so it has size 10 so by orbit stabiliser we are looking at a group of order 120.

Now what we will do is a kind of genius thing. If we draw diagonals on the faces, they inscribe 5 cubes in the dodecahedron. I will just show a picture of this. There are a total of 60 diagonals on the faces and 12 edges per cube so there are 5 cubes total. Figure 10 shows a cube in a dodecahedron to show what I mean.

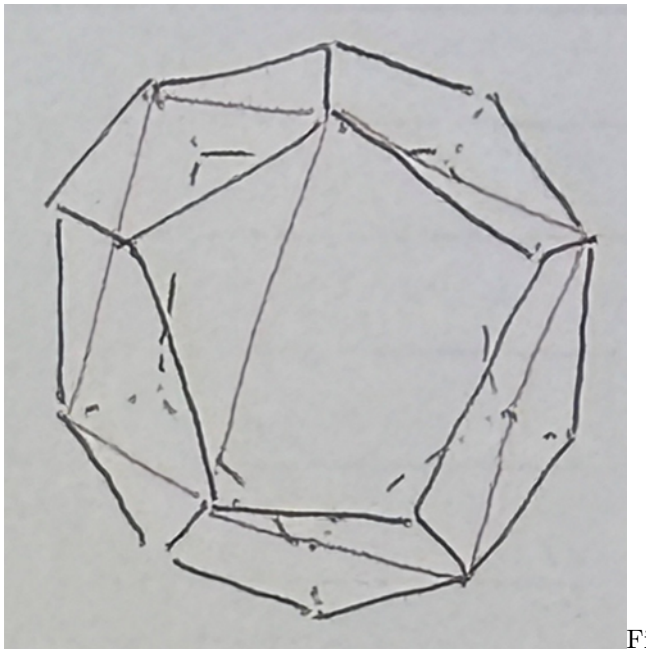
Figure 10

The isometry group of the dodecahedron will act on the set of these cubes. We now have a homomorphism to S_5 and we want to look at what the image is.

Now if we rotate about a long diagonal we get a subgroup of order 3 since we have 3 faces meeting at that vertex. This permutes 3 of the cubes and fixes the 2 through that vertex. Therefore we have all 10 3-cycles in the image by each of the 10 long diagonals, and their inverses, so we have all 20 3-cycles in S_5.

Claim. The set of 3-cycles generate A_5

Proof. We know that the subgroup generated by the 3-cycles is the whole of A_5: eg $(1\ 2\ 3)\,(1\ 3\ 4) = (1\ 4)\,(2\ 3)$, and $(1\ 2\ 3)\,(3\ 4\ 5) = (1\ 2\ 3\ 4\ 5)$, and similarly we can get all 2-2 and 5-cycles. Because of this, we know that the rotation group of the dodecahedron is isomorphic to A_5. But now, by the same reason as the cube, the symmetries of a dodecahedron is isomorphic to the group $A_5 \times C_2$.

□

[Lecture 24 ends]