MATH40003 Linear Algebra and Groups
Part II: Groups

David Evans
Department of Mathematics, Imperial College*

February 2, 2021

Contents

1 Groups and Subgroups

Lecture 10

1.1 Binary operations; groups; basic facts

DEFINITION 1.1. Suppose S is a set. A *binary operation* $*$ on S assigns to each ordered pair (a, b) of elements of S an element $a*b$ of S. More formally, $*$ is a function $S \times S \to S$. (Where $S \times S$ is the Cartesian product set $\{(a, b) : a, b \in S\}$.)

This is a very general notion. Here are some examples involving $M_2(\mathbb{R})$: not all of them will lead to groups!

EXAMPLES: Let $S = M_2(\mathbb{R})$. The following are binary operations on S.

(1) $a * b = ab$, the usual matrix multiplication.

(2) $*$ is matrix addition.

(3) $a * b = a$ for all $a, b \in A$ ('projection onto the first coordinate')

(4) $a * b = ab - ba$ (called the Lie product).

(5) Let $S_1 = \{a \in M_2(\mathbb{R}) : a \text{ is invertible}\}$. For $a, b \in S_1$ let $a * b$ be the usual matrix product ab. As the product of two invertible matrices is invertible, this is a binary operation on S_1.

(6) If in (5) we had taken $a * b = a + b$, this would not be a binary operation on S_1 as the sum of two invertible matrices need not be invertible.

You will have seen this before:

DEFINITION 1.2. A binary operation $*$ on a set S is *associative* if

$$\text{for all } a, b, c \in S \text{ we have } a * (b * c) = (a * b) * c.$$

EXERCISE: Which of the binary operations above are associative?

Associativity means that we can unambiguously write an expression such as

$$((a_1 * a_2) * (a_3 * a_4)) * a_5$$

as $a_1 * a_2 * a_3 * a_4 * a_5$. The bracketing is redundant. From now on, we will usually do this when dealing with associative operations.

PUZZLE: How many ways are there of bracketing $a_1 * a_2 * \ldots * a_n$? Try it for $n = 4, 5$. Can you find a general expression?

Now, here is the main definition.

DEFINITION 1.3. A *group* $(G, *)$ consists of a set G with a binary operation $*$ on G satisfying the following:

$\mathcal{G}1$ (Associativity) For all $g, h, k \in G$ we have

$$(g * h) * k = g * (h * k).$$

$\mathcal{G}2$ (Identity axiom) There exists an element $e \in G$ such that for all $g \in G$ we have

$$e * g = g * e = g.$$

We will show that $\mathcal{G}1$ and $\mathcal{G}2$ imply that there is a *unique* such $e \in G$, which we will denote by e or e_G and call it the *identity element* of the group.

$\mathcal{G}3$ (Existence of inverses) With e as in $\mathcal{G}2$, for all $g \in G$ there is an element $h \in G$ such that

$$g * h = h * g = e.$$

We will show that the h here is uniquely determined by g: we call it the *inverse* of g and usually denote it by h^{-1}.

REMARKS: Here, $\mathcal{G}1, \mathcal{G}2, \mathcal{G}3$ are called the *group axioms*. In some books you will see that the following is also included as an axiom:

$\mathcal{G}0$ (Closure) If $g, k \in G$, then $g * k \in G$.

It's not necessary to include this as we are assuming that $*$ is a binary operation on G and so $\mathcal{G}0$ holds anyway.

REMARKS 1.4. Here are some remarks on simplifications to notation and terminology which we shall use throughout.

(1) It is more common to use . instead of $*$ for the group operation: so from now on, you will see $g.h$ rather than $g * h$. In fact, just as in ordinary arithmetic, we often omit the . and just write gh instead of $g.h$. We call the operation the *product* in the group.

(2) A group $(G, *)$ is called *abelian* or *commutative* if for all $g, h \in G$ we have $g * h = h * g$. In such cases, we often write the operation as $+$. When we do this we write the identity element as 0 and the inverse of g as $-g$.

REMARKS 1.5. We now justify the claims made in Definition 1.3. Suppose $(G, .)$ is a group.

(1) We have to show the following, using axioms $\mathcal{G}1$ and $\mathcal{G}2$.

If $e, e' \in G$ and for all $g \in G$

$$e.g = g.e = g \text{ and } e'.g = g.e' = g$$

then $e = e'$.

Proof: Using these equations, we have $e = e.e' = e'$ (exercise: say which of the equations were used here!) $\square$

(2) We have to show the following using the group axioms.

Suppose $g, g', g'' \in G$ and

$$gg' \overset{(1)}{=} e \overset{(2)}{=} g'g \text{ and } gg'' \overset{(3)}{=} e \overset{(4)}{=} g''g.$$

Then $g' = g''$.

Proof: We have

$$(g'g)g'' \overset{(2)}{=} eg'' = g'' \text{ and } g'(gg'') \overset{(3)}{=} g'e = g'.$$

So by Associativity $g' = g''$.

[Exercise: Why is the following not a proof? 'From the equations, we have $g' = g^{-1}$ and $g'' = g^{-1}$, so $g' = g''$.']

We will use the following all the time, usually without mentioning that it's what we are using. It's about manipulating equations in a group.

LEMMA 1.6. *(Equations in groups) Suppose $(G, .)$ is a group and $g, h \in G$.*

(1) For $x \in G$ we have $gx = h \Leftrightarrow x = g^{-1}h$

(2) For $y \in G$ we have $yg = h \Leftrightarrow y = hG^{-1}$.

Proof: (1) $\Rightarrow$: Multiply on the left by g^{-1}:

$$gx = h \Rightarrow g^{-1}(gx) = g^{-1}h \overset{G_1}{\Rightarrow} (g^{-1}g)x = g^{-1}h \Rightarrow ex = g^{-1}h \Rightarrow x = g^{-1}h.$$

$\Leftarrow$: Check that all of the above arrows can be reversed.

(2) Similar, but multiply on the right by g^{-1}. $\square$

The following will look very familiar from matrix multiplication.

LEMMA 1.7. *(Inverse of a product) Suppose $(G, .)$ is a group.*

(1) If $g, h \in G$, then $(gh)^{-1} = h^{-1}g^{-1}$.

(2) If $g_1, \ldots, g_n \in G$, then

$$(g_1 g_2 \ldots g_n)^{-1} = g_n^{-1} \ldots g_2^{-1} g_1^{-1}.$$

Proof: (1) Note that

$$(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1})g)h = h^{-1}eh = h^{-1}h = e.$$

Similarly $gh(h^{-1}g^{-1}) = e$.

(2) Prove this by induction on n. The base case $n = 2$ is (1). $\square$

[Before the next lecture, review the material in the Introductory Module about Bijections (Sections 2.3 and 2.4 there).]

1.2 Examples of groups

Lecture 11

EXAMPLES 1.8. Examples from fields

(1) $\mathbb{R}$ with the operation $+$ is a group. The identity element is 0 and the inverse of $a \in \mathbb{R}$ is $-a$. We refer to this as the additive group of the field $\mathbb{R}$.

(2) $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ with the operation . is a group. The identity element is 1 and the inverse of $a \in \mathbb{R}^\times$ is a^{-1}. We refer to this as the multiplicative group of the field $\mathbb{R}$.

(3) Examples (1), (2) work with any field, not just $\mathbb{R}$.

(4) If F is any field and $n \in \mathbb{N}$, then $(F^n, +)$ is a group.

(5) If V is a vector space (over a field F) then $(V, +)$ is a group.

(6) Let $n \in \mathbb{N}$ and suppose F is a field. The *general linear group* $\mathrm{GL}(n, F)$ (or $\mathrm{GL}_n(F)$) is the set G of $n \times n$ invertible matrices (over F) and operation matrix multiplication. This *is* a group:

- Binary operation: If $A, B \in G$, you can check that $AB \in G$ (because the inverse of AB is $B^{-1}A^{-1}$).
- $\mathcal{G}1$, Associativity: If $A, B, C \in G$, then $A(BC) = (AB)C$: this is a general property of matrix multiplication.
- $\mathcal{G}2$, Existence of identity element: The identity matrix $I_n \in G$ has the required property.
- $\mathcal{G}3$, Existence of inverses: this follows from the definition of G.

Note: $GL(1, F)$ is the multiplicative group $F^\times$.

DEFINITION 1.9. The Symmetric Groups.

Suppose X is any (non-empty) set. (For example, $X = \{1, 2, \ldots, n\}$.) A *permutation of* X is a bijection $\alpha : X \to X$.

For example, if $X = \{1, 2, 3, 4\}$ let α be the map denoted by:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

with $\alpha(1) = 2$, $\alpha(2) = 4$, etc.

More generally we use the following 'two-row' notation for permutations on the set $X = [n] = \{1, 2, \ldots, n\}$. We denote a permutation $\alpha : [n] \to [n]$ by:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix}.$$

Note that the second row here is a 'rearrangement' of $1, 2, 3, \ldots, n$.

Exercise: If $\alpha, \beta : X \to X$ are permutations, then so is the composition $\alpha \circ \beta : X \to X$

$$(\alpha \circ \beta)(x) = \alpha(\beta(x)), \text{ for } x \in X.$$

- See the Introductory Module if you are unsure about this.

Example: If

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

then

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \text{ and } \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}.$$

Let $\mathrm{Sym}(X)$ denote the set of all permutations of X. If $n \in \mathbb{N}$ and $X = [n] = \{1, 2, \ldots, n\}$, we will also denote this by $\mathrm{Sym}(n)$ or S_n.

THEOREM 1.10. *Suppose X is any (non-empty) set. Then* $\mathrm{Sym}(X)$ *with the operation $\circ$ of composition is a group. It is called the symmetric group on X.*

Proof: By the above exercise, we know that $\circ$ is a binary operation on $\mathrm{Sym}(X)$. We proceed to check the group axioms.

$\mathcal{G}1$ (Associativity): Composition of functions is associative: if $\alpha, \beta, \gamma \in \mathrm{Sym}(X)$, then $\alpha \circ (\beta \circ \gamma)$ and $(\alpha \circ \beta) \circ \gamma$ are the same function $X \to X$ (for $x \in X$ they both send x to $\alpha(\beta(\gamma(x)))$).

$\mathcal{G}2$ (identity element): The identtity function $\iota : X \to X$, with $\iota(x) = x$ for all $x \in X$, is in $\mathrm{Sym}(X)$ and has the required properties.

$\mathcal{G}3$ (Existence of inverses): If $\alpha \in \mathrm{Sym}(X)$, then it is a bijection and so has an inverse α^{-1} which is also a bijection: $\alpha^{-1}(y) = x \Leftrightarrow \alpha(x) = y$. $\square$

REMARKS: If $\alpha, \beta \in \mathrm{Sym}(X)$ we will often write $\alpha\beta$ instead of $\alpha \circ \beta$. Remember that this is composition of functions and so this means 'apply β first, then α.'
WARNING: Some books or lecture notes will use the notation the other way round.

EXAMPLE/ EXERCISE: Consider the following elements of S_6:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \end{pmatrix}.$$

Compute $\alpha\beta, \beta\alpha, \alpha^{-1}, \beta^{-1}, \alpha\beta\alpha^{-1}$.

Label the vertices of a regular hexagon $1, 2, 3, 4, 5, 6$ (clockwise) and think about how the permutations α, β and these other permutations correspond to symmetries of the regular hexagon.

DEFINITION 1.11. We say that a group $(G, .)$ is a *finite group* if the set G is a finite set. In this case, the *order* of $(G, .)$ is $|G|$, the number of elements in the group.

THEOREM 1.12. *If $n \in \mathbb{N}$, then $|S_n| = n!$*

Proof: We have to count the number of permutations

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

where $a_1, \dots, a_n$ are $1, \dots, n$ in some order.

There are

n choices for a_1;
$n-1$ choices for a_2;
$n-2$ choices for a_3;
...

So there are a total of $n(n-1)(n-2)\dots 2.1 = n!$ possibilities for α. $\square$

1.3 Powers and Subgroups

Lecture 12

DEFINITION 1.13. Suppose $(G, \cdot)$ is a group. For $g \in G$, we let

$$g^0 = e,\ g^1 = g,\ g^2 = g \cdot g,\ g^3 = g \cdot g \cdot g, \dots .$$

More precisely, for $n \in \mathbb{N}$ we define inductively

$$g^0 = e,\ g^1 = g \text{ and } g^{n+1} = g^n \cdot g.$$

We also define $g^{-n} = (g^{-1})^n$.

Using this as our definition, we can then prove the following.

LEMMA 1.14. *With this notation, if $m, n \in \mathbb{Z}$, then*

(o) $g^{m+1} = g^m g$ *and* $g^m g = g g^m$;

(i) $(g^m)^{-1} = g^{-m}$;

(ii) $g^m g^n = g^{m+n} = g^n g^m$;

(iii) $g^{mn} = (g^m)^n$.

EXAMPLE: Let

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4.$$

Then

$$g^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, g^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = g^{-1},\ g^4 = \iota,\ g^5 = g, \dots,\ g^{19} = g^3$$

the last of these because $19 = 4.4 + 3$ and so

$$g^{19} = (g^4)^4 g^3 = \iota^4 g^3 = g^3$$

using the lemma.

Similarly if $n \equiv k \,(\mathrm{mod}\, 4)$, $g^n = g^k$.

Proof of Lemma: It's not trivial to get all of the details correct, though it is quite tedious. The proof should remind you of some things you discussed around Peano's axioms in the Introductory module.

(o) For the first part, if $m \geq 0$, this is by definition. So assume $m = -k$ where $k \in \mathbb{N}$ and prove by induction on k that $g^{-k+1} = g^{-k}g$. The base case is $k = 1$, which follows from $g^0 = e = g^{-1}g$. For the inductive step suppose we know $g^{-k+1} = g^{-k}g$. Then $g^{-(k+1)}g = (g^{-1})^{k+1}g = ((g^{-1})^k g^{-1})g = g^{-k}$, as required (the first two equalities comes from the definitions). The second part is an exercise.

(i) Prove for $m \geq 0$ that $(g^m)(g^{-m}) = e$, by induction on m. Then deduce for $m < 0$.

(ii) We first prove this for $n \geq 0$. We do this by induction on n, regarding m as fixed.

Base case $n = 0$*:* We have $g^{m+0} = g^m$ and $g^m g^0 = g^m e = g^m$, so $g^{m+0} = g^m g^0$.

Inductive step: Suppose we know that $g^{m+n} = g^m g^n$. Then

$$g^{m+(n+1)} = g^{(m+n)+1} \overset{(o)}{=} g^{m+n}g = (g^m g^n)g = g^m(g^n g) = g^m g^{n+1}$$

as required.

Exercise: Complete the proof of (ii) by considering the case $n < 0$.

(iii) Similar, using (ii). □

Remark: on additive notation. If our group is $(G, +)$ and $n \in \mathbb{N}$, we write $g + \ldots + n$ (n times) as ng (not g^n).

Definition 1.15. Suppose $(G, .)$ is a group and $H \subseteq G$. We say that H is a *subgroup* of G (or of $(G, .)$) if H with the binary operation from G is a group, that is:

$$\text{for all } h_1, h_2 \in H \text{ we have } h_1.h_2 \in H$$

and $(H, .)$ satisfies axioms $\mathcal{G}1, \mathcal{G}2, \mathcal{G}3$. We will write $H \leq G$ to indicate that H is a subgroup of G.

Examples: (1) G is a subgroup of G;

(2) $\{e\}$ is a subgroup of G.

In practice, what we use to decide whether a given sub*set* of a group is a subgroup is the direction $\Leftarrow$ of the following.

THEOREM 1.16. *(Test for a subgroup) Suppose $(G,.)$ is a group and $H \subseteq G$. Then H is a subgroup of G if and only if*

(1) $H \neq \emptyset$;

(2) for all $h_1, h_2 \in H$ we have $h_1 h_2 \in H$ (closure under the group operation);

(3) for all $h \in H$ we have $h^{-1} \in H$ (closure under inverses).

EXAMPLE: If $g \in G$, let $H = \{g^m : m \in \mathbb{Z}\}$. This is a subgroup of G, by 1.16 and 1.14.

Proof of 1.16: $\Leftarrow$: Suppose (1), (2), (3) hold for H. By (2), the multiplication . in G gives a binary operation on H. So we need to check that $(H,.)$ satisfies the group axioms.

$\mathcal{G}1$ follows from associativity in G.

For $\mathcal{G}2$, it is enough to show that $e_G \in H$. By (1), there is some $h \in H$. By (3), $h^{-1} \in H$. Then by (2), $hh^{-1} \in H$. So $e_G \in H$.

Then $\mathcal{G}3$ follows from (3).

$\Rightarrow$: If H is a subgroup of G, then (2) holds by definition.

By $\mathcal{G}2$, we know that $H \neq \emptyset$, so (1) holds.

For (3) we first show that $e_G \in H$. Let $h \in H$. As $(H,.)$ is a group, there is some $x \in H$ with $hx = h$. But the only solution to this equation in G is $x = e_G$. So $e_G \in H$. Similarly, the only solution to $hh' = e_G$ in G is $h' = h^{-1}$. As H is a group, there must be a solution in H, so $h^{-1} \in H$, as required for (3). $\square$

REMARK: The direction $\Rightarrow$ shows that if H is a subgroup of G then $e_G \in H$ and inverses are the same in H as they are in G.

Before we give some examples of using the test, we formalise the example given before the above proof by giving some terminology.

DEFINITION 1.17. (1) Suppose $(G,.)$ is a group and $g \in G$. The *cyclic subgroup generated by g* is $\langle g \rangle = \{g^m : m \in \mathbb{Z}\}$.

(2) We say that a group G is *cyclic* if there is $g \in G$ with $\langle g \rangle = G$. In this case, g is called a *generator* of G.

EXAMPLES 1.18. (1) Let $G = \mathrm{GL}(n, \mathbb{R})$ (the group of $n \times n$ invertible matrices over $\mathbb{R}$). We give some subgroups.

(1) Let $H = \{g \in G : \det(g) = 1\}$. We use the subgroup test to check that this is a subgroup of G:

$H \neq \emptyset$ as $I_n \in H$.

H is closed under . as $\det(g_1 g_2) = \det(g_1)\det(g_2)$ so if $g_1, g_2 \in H$, then $g_1 g_2 \in H$.

H is closed under inverses as $\det(g^{-1}) = 1/\det(g)$ for $g \in G$, so if $h \in H$, then $h^{-1} \in H$.

(2) You can use the subgroup test to show that

$$K = \{\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R}\} \leq \mathrm{GL}_2(\mathbb{R}).$$

Note K consists of linear maps $\mathbb{R}^2 \to \mathbb{R}^2$ given by rotations about 0. The subgroup K is abelian, but not cyclic (for example, K is uncountable, whereas any cyclic group is countable).

(3) We have:

$$2\mathbb{Z} \leq \mathbb{Z} \leq \mathbf{Q} \leq \mathbb{R} \leq (\mathbb{C}, +),$$

where $2\mathbb{Z}$ consists of the even integers. Note that $\mathbb{Z} = \langle 1 \rangle$ and $2\mathbb{Z} = \langle 2 \rangle$ are cyclic, but none of the other groups is cyclic.

(4) Consider the unit circle in the complex plane:

$$U = \{e^{i\theta} : \theta \in \mathbb{R}\} = \{z \in \mathbb{C} : |z| = 1\} = \{z \in \mathbb{C} : z\bar{z} = 1\}.$$

This is a subgroup of $(\mathbb{C}^\times, .)$, the multiplicative group of the field of complex numbers. It is abelian, but not cyclic.
[Puzzle: What is the relationship to the group K in (2)?]

(5) Let $n \in \mathbb{N}$ and $\zeta = e^{2\pi i/n} \in \mathbb{C}^\times$. So $\zeta^n = 1$. Then $\langle \zeta \rangle \leq U$ and

$$\langle \zeta \rangle = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$$

is a cyclic group of order n.

[Note that if you draw the elements of $\langle \zeta \rangle$ on an Argand diagram, they form the vertices of a regular n-gon on the unit circle.]

(6) Suppose F is any field and $n \in \mathbb{N}$. Consider the group $(F^n, +)$. Any subspace of F^n is a subgroup of this, but the converse is not necessarily true. For example $\mathbf{Q}^2$ is a subgroup of $\mathbb{R}^2$, but it is not a subspace.

(7) Let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \in S_4.$$

Then $V = \{\iota, \alpha, \beta, \gamma\} \leq S_4$ is a subgroup of S_4, called the Klein four-group. We have $g^2 = \iota$ for all $g \in V$. So V is abelian but not cyclic.

[Remark: it would be good to revise thing in the Introductory module around the Division - Remainder Theorem, gcd's and the Euclidean algorithm.]

1.4 Orders of elements

Lecture 13

From now on we will usually write 'G is a group' instead of $(G, .)$ is a group.'

DEFINITION 1.19. Suppose G is a group and $g \in G$. We say that g has *finite order* if there is $n \in \mathbb{N}$ (with $n \geq 1$) such that $g^n = e$. In this case, the least such n with $g^n = e$ is called the *order* of g, denoted by $\mathrm{ord}(g)$. If there is no such $n \in \mathbb{N}$, we say that g has *infinite order*.

EXAMPLES: (1) For any group G, the identity element e has order 1.

(2) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$ has order 3; $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ has order 2.

(3) $2 \in \mathbb{R}^\times$ has infinite order; $-1 \in \mathbb{R}^\times$ has order 2.

(4) For $n \in \mathbb{N}$, $\zeta = e^{2\pi i/n} \in \mathbb{C}^\times$ has order n.

(5) The matrix $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{R})$ has order 3.

(6) (Ex.) Think about orders of rotations in $\mathrm{GL}_2(\mathbb{R})$.

THEOREM 1.20. *Suppose G is a group and $g \in G$ has finite order n. Then:*

(1) For $m, l \in \mathbb{Z}$ we have

$$g^l = g^m \Leftrightarrow n \mid (l - m) \Leftrightarrow l \equiv m \,(\mathrm{mod}\, n).$$

(2) In particular, $g^m = e \Leftrightarrow n \mid m$.

(3) We have $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ and $|\langle g \rangle| = n$.

So $\mathrm{ord}(g) = |\langle g \rangle|$.

Proof: (1) $\Leftarrow$: Let $s = l - m$ and suppose $n \mid s$. So there is $t \in \mathbb{Z}$ with $s = nt$. Then

$$g^s = g^{nt} = (g^n)^t = e^t = e.$$

Thus $e = g^s = g^{l-m} = g^l g^{-m}$. Multiplying by g^m, we obtain $g^m = g^l$, as required.

$\Rightarrow$: Suppose $g^l = g^m$. Then $g^{l-m} = e$. By the Quotient - Remainder Theorem (Introductory Module, 3.2.3) there are $q, r \in \mathbb{Z}$ with

$$l - m = qn + r \text{ and } 0 \leq r < n.$$

Then

$$e = g^{l-m} = g^{qn+r} = g^{qn} g^r = (g^n)^q g^r = e g^r = g^r.$$

By minimality of n and $0 \leq r < n$, we therefore have $r = 0$. Thus $n \mid (l - m)$, as required.

(2) By (1) with $l = 0$.

(3) Every $l \in \mathbb{Z}$ is congruent modulo n exactly one of $0, 1, \ldots, n-1$. So the result we require follows from (1). $\square$

The following is a useful simplification of the test for being a subgroup of a finite group.

THEOREM 1.21. *Suppose G is a finite group.*

(1) Every element of G has finite order.

(2) If $H \subseteq G$ is a non-empty subset of G and for all $h_1, h_2 \in H$ we have $h_1 h_2 \in H$, then H is a subgroup of G.

Proof: (1) Consider $g, g^2, g^3, \ldots \in G$. As $|G|$ is finite, there exist $0 < m < l$ with $g^m = g^l$. Then $g^{l-m} = e$ and $l - m > 0$. So g has finite order.

(2) We have to show that H is closed under inverses. Let $h \in H$. By (1) there is $n \in \mathbb{N}$ with $h^n = e$. We want to show $h^{-1} \in H$. We can assume that $h \neq e$, so $n > 1$. Then $h^{-1} = h^{n-1}$ and $n - 1 \geq 1$. As $h \in H$ and H is closed under multiplication, it follows that $h^{n-1} \in H$. So $h^{-1} \in H$. $\square$

1.5 More on cyclic groups

Lecture 14

The following tells us everything about subgroups of cyclic groups.

THEOREM 1.22. *Suppose $(G, .)$ is a cyclic group and $G = \langle g \rangle$.*

(1) If $H \leq G$, then H is cyclic.

(2) Suppose $|G| = n$ (that is, g has order n), and $m \in \mathbb{Z}$. Let $d = gcd(m, n)$, the greatest common divisor of m and n. Then

$$\langle g^m \rangle = \langle g^d \rangle \text{ and } |\langle g^d \rangle| = n/d.$$

In particular,

$$\langle g^m \rangle = G \Leftrightarrow gcd(m, n) = 1.$$

(3) If $|G| = n$ and $k \leq n$, then G has a subgroup of order k if and only if $k \mid n$. In this case, the subgroup is $g^{n/k}$.

EXAMPLE/ EXERCISE: Let $g = e^{2\pi i/6} \in \mathbb{C}^\times$ and $G = \langle g \rangle$. So G is a cyclic group of order 6. The subgroups of G have orders 1,2,3 and 6. They are:

$\{1\}$;

$\langle g^3 \rangle = \{1, -1\}$;

$\langle g^2 \rangle = \{1, g^2, g^4\}$;

$\langle g \rangle = G$.

There is one element of order 2, two elements of order 3, and two elements of order 6.

Proof of Theorem: (1) We may assume that $H \neq \{e\}$. Let d be the least element of $\{n \in \mathbb{N} : g^n \in H\}$ (noting that this set is non-empty).

Claim: $H = \langle g^d \rangle$.

As $g^d \in H$ and $H \leq G$, we have $\langle g^d \rangle \leq H$. So let $h \in H$. Then $h = g^m$ for some $m \in \mathbb{Z}$. We can write $m = qd + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < d$. So $h = g^{qd+r} = (g^d)^q g^r$. Thus $g^r = h(g^d)^{-q} \in H$, as $h \in H$ and $g^d \in H$. Minimality of d therefore gives $r = 0$. So $h = g^{qd} = (g^d)^q \in \langle g^d \rangle$, as required.

(2) As $d = gcd(m, n)$ there are $k, l \in \mathbb{Z}$ with $d = km + ln$ (the Bézout Identity).

To show that $\langle g^m \rangle = \langle g^d \rangle$ it is enough to prove that $g^m \in \langle g^d \rangle$ and $g^d \in \langle g^m \rangle$. Because $d \mid m$, g^m is a power of g^d, so the first of these is true. For the second, note that

$$g^d = g^{km+ln} = (g^m)^k (g^n)^l = (g^m)^k$$

as $n = \text{ord}(g)$, so $g^n = e$. This $g^d \in \langle g^m \rangle$.

Now consider what is $|\langle g^d \rangle|$. Because $d \mid n$ we can write $n = df$ for some $f \in \mathbb{N}$. Then $\langle g^d \rangle = \{g^0, g^d, \ldots, g^{(f-1)d}\}$ as $g^{fd} = e$. Now, $g^0, g^d, g^{2d}, \ldots, g^{(f-1)d}$ are distinct as $d, \ldots, (f-1)d$ are less than n. It follows that $|\langle g^d \rangle| = f = n/d$.

(3) The first part is by (1) and (2). If $k \mid n$, then by (2), the unique subgroup with k elements is $\langle g^{n/k} \rangle$. $\square$

An application. We will give an application of the previous theorem to prove a result due to Gauss on the *Euler totient function*: an important function in elementary number theorem. You can find an application of Gauss' result on the problem sheet, where it is used to prove the useful fact that every *finite* subgroup of the multiplicative group of a field is cyclic.

Definition: For $n \in \mathbb{N}$, the Euler totient function $\phi(n)$ is

$$|\{k \in \mathbb{N} : 1 \leq k \leq n \text{ and } gcd(k, n) = 1\}|.$$

Thej following Corollary to Theorem 1.22 is due to C. F. Gauss.

Corollary 1.23. *For all $n \in \mathbb{N}$ we have*

$$\sum_{1 \leq d \leq n,\, d \mid n} \phi(d) = n.$$

Example: $n = 6$ has divisors $d = 1, 2, 3, 6$. We compute that $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(6) = 2$. Summing these does indeed give 6.

Proof of Corollary: Let G be a cyclic group of order n. By 1.22(3), if $d \mid n$ then G has a *unique* subgroup G_d of order d. Thus, G_d contains every element of G of order d (because this will generate a subgroup of order d).

We also know, by 1.22(1), that G_d is cyclic, and therefore by 1.22(2), G_d has $\phi(d)$ elements of order d.

Any element of G has order dividing $n = |G|$ (by 1.22(2)). Then counting elements of G according to their possible orders (and therefore which G_d they generate) gives

$$\sum_{1 \le d \le n,\, d \mid n} \phi(d) = n. \; \square$$

1.6 Generating other subgroups

What about subgroups generated by more than one element? In general, this is a much harder question than understanding cyclic groups (or cyclic subgroups). But at least we can make some definitions.

DEFINITION 1.24. Suppose $(G, .)$ is a group and $S \subseteq G$ is non-empty. Let

$$S^{-1} = \{g^{-1} : g \in G\}$$

and

$$\langle S \rangle = \{g_1 g_2 \dots g_k : k \in \mathbb{N} \text{ and } g_1, g_2, \dots, g_k \in S \cup S^{-1}\}.$$

So $\langle S \rangle$ is the set of all products of elements of S and their inverses (allowing repetitions).

We could also define $\langle \emptyset \rangle = \{e\}$, if we wish.

LEMMA 1.25. *With this notation:*

(1) $\langle S \rangle$ is a subgroup of G.

(2) If $H \le G$ and $S \subseteq H$, then $\langle S \rangle \subseteq H$.

Proof: Exercise: use the test for being a subgroup. $\square$

So $\langle S \rangle$ is the 'smallest' subgroup of G containing S. It is called the subgroup of G *generated by* S.

If $S = \{x_1, \dots, s_r\}$, write $\langle S \rangle$ as $\langle x_1, \dots, s_r \rangle$.

If G is abelian then

$$\langle x_1, \dots, s_r \rangle = x_1^{k_1} x_2^{k_2} \dots x_r^{k_r} : k_1, \dots, k_r \in \mathbb{Z}\}.$$

But in general, deciding what $\langle x_1, \dots, s_r \rangle$ is, even if $r = 2$ is a hard problem.

2 Lagrange's Theorem and Cosets

Lecture 15

In this section we will prove the following and give some applications. The method of proof, involving cosets, is also an important idea which you will see more of in later modules.

THEOREM 2.1. *(Lagrange's Theorem) Suppose $(G,.)$ is a finite group and H is a subgroup of G. Then $|H|$ divides $|G|$.*

So one thing that this tells us is that $G = S_5$, which has order $5! = 120$, cannot have a subgroup of order 50. Here are some more general applications.

THEOREM 2.2. *Suppose G is a finite group of order n. Let $g \in G$. Then:*

(1) The order of g divides n.

(2) $g^n = e$.

Proof: (1) The order of g is $|\langle g\rangle|$ (by 1.20(3)). As $\langle g\rangle$ is a subgroup of G, the result therefore follows from Lagrange's Theorem.

(2) Suppose $\mathrm{ord}(g) = k$. By (1) we have $k \mid n$. Moreover $g^n = (g^k)^{n/k} = e^{n/k} = e$. □

As a special case we have the well-known:

COROLLARY. (Fermat's Little Theorem) Suppose p is any prime. If $x \in \mathbb{Z}$ and $p \not| x$, then $x^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$.

[It follows that for all $k \in \mathbb{Z}$ we have $k^p \equiv k \,(\mathrm{mod}\, p)$.]

Proof: Let $\mathbb{F}_p$ be the field with p elements (that is, $\mathbb{Z}_p$). Consider $(\mathbb{F}_p^\times, .)$, the multiplicative group of the field, consisting of the non-zero elements. Then $|\mathbb{F}_p^\times| = p - 1$.

So for every $g \in \mathbb{F}_p$, we have $g^{p-1} = [1]_p$, the identity element of the field, the residue class of 1, modulo p. If $x \in \mathbb{Z}$ and $p \not| x$, then $[x]_p \neq [0]_p$. So taking $g = [x]_p$ we obtain $[1]_p = [x]_p^{p-1} = [x^{p-1}]_p$. In other words, $x^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$. □

EXAMPLES 2.3. Let $G = S_3$. So $|G| = 6$. Let $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Then $\langle \alpha, \beta\rangle = G$.

Indeed, note that α has order 3 and β has order 2. As $\langle \alpha, \beta\rangle \leq S_3$ has subgroups $\langle \alpha\rangle$ and $\langle \beta\rangle$, it follows from Lagrange's theorem that the order of $\langle \alpha, \beta\rangle$ is divisible by 2 and by 3, and therefore by 6. As S_3 has order 6, it follows that $\langle \alpha, \beta\rangle = S_3$.

THEOREM 2.4. *Suppose p is a prime and G is group of order p. Then G is cyclic. In fact, if $e \neq g \in G$, then $\langle g\rangle = G$.*

Proof: By Lagrange's Theorem $|\langle g\rangle|$ divides p. As $e, g \in \langle g\rangle$ and $e \neq g$ we therefore have $|\langle g\rangle| = p$, because p is a prime. □

We now turn to the proof of Lagrange's Theorem and the key idea of cosets.

DEFINITION 2.5. Suppose $(G, .)$ is a group and $H \leq G$. Let $g \in G$. The subset

$$gH = \{gh : h \in H\} \subseteq G$$

is called a *left coset* of H in G. (Sometimes we will say 'left H-coset.')

So if $H = \{h_1, \ldots, h_r\}$, then $gH = \{gh_1, \ldots, gh_r\}$.

Another way of saying this is that a subset X of G is a left coset of H in G if there exists some $g \in G$ such that $X = gH$. Note that $g \in gH$, so this might give us some clue about which g to take here.

[Remark: Some books, lecture notes and past exam questions will refer to right cosets $Hg = \{hg : h \in H\}$. Essentially everything we do will also work with right cosets in place of left cosets. But we should not mix them.]

In some situations, cosets are actually quite familiar. Here are some examples.

EXAMPLES 2.6. (1) Let $G = (\mathbb{C}^\times, .)$ and $H = \{z \in \mathbb{C}^\times : |z| = 1\}$. So H is a subgroup of G. Let $g = 2 \in \mathbb{C}^\times$. Then the left coset

$$2H = \{2e^{i\theta} : \theta \in \mathbb{R}\} = \{z \in G : |z| = 2\}.$$

Note that this is not a subgroup of G.

More generally, if $w \in \mathbb{C}^\times$, then $wH = \{z \in \mathbb{C}^\times : |z| = |w|\}$.

(2) Let $G = (\mathbb{Z}, +)$ and $H = \{5m : m \in \mathbb{Z}\}$. So H is a subgroup of G. As the group G is written additively, we shall also write H-cosets additively:

$0 + H = H = [0]_5$;

$1 + H = \{1 + 5m : m \in \mathbb{Z}\} = \{k \in \mathbb{Z} : k \equiv 1 \pmod 5\} = [1]_5$;

...

$4 + H = [4]_5$;

...

$6 + H = \{6 + 5m : m \in \mathbb{Z}\} = \{1 + 5m : m \in \mathbb{Z}\} = \{k \in \mathbb{Z} : k \equiv 1 \pmod 5\} = [1]_5$.

So there are 5 left H-cosets

$$0 + H, 1 + H, \ldots, 4 + H$$

and these partition $G = \mathbb{Z}$.

(3) Let A be an $m \times n$ matrix with entries from $\mathbb{R}$. Let $W = \{x \in \mathbb{R}^n : Ax = 0_m\}$, the solution set of the system of homogeneous linear equations with coefficient matrix A. So W is a subspace of $(\mathbb{R}^n, +)$, and therefore a subgroup. Suppose $b \in \mathbb{R}^m$ and there is $c \in \mathbb{R}^n$ with $Ac = b$. Then

$$Ax = b \Leftrightarrow A(x - c) = 0 \Leftrightarrow x - c \in W \Leftrightarrow x \in c + W.$$

So if the the set of solutions to $Ax = b$ is non-empty, then it is a coset of W in $\mathbb{R}^n$.

We saw in these examples that, for a fixed subgroup H, the left H-cosets partition G: every element of G is in exactly one left H-coset. The following lemma supplies the proof of this in general.

LEMMA 2.7. *Suppose $(G, .)$ is a group and $H \leq G$.*

(1) If $g_1, g_2 \in G$ and $g_2 \in g_1H$, then $g_2H = g_1H$.

(2) If $g, k \in G$ and $gH \cap kH \neq \emptyset$, then $gH = kH$.

Proof (1) We first show that if $g_2 \in g_1H$, then $g_2H \subseteq g_1H$.

As $g_2 \in g_1H$ there is $h \in H$ with $g_2 = g_1h$. Any element of g_2H is of the form g_2h' for some $h' \in H$. Then $g_2h' = (g_1h)h' = g_1(hh')$. Because $H \leq G$, we have $hh' \in H$. So $g_2h' \in g_1H$, as required.

Also $g_1 = g_2h^{-1}$ and $h^{-1} \in H$, so $g_1 \in g_2H$. Thus, the same argument gives $g_1H \subseteq g_2H$.

Putting the two parts together gives $g_1H = g_2H$.

(2) Let $x \in gH \cap kH$. By (1), applied twice, we have $gH = xH = kH$. □

LEMMA 2.8. *Suppose $(G, .)$ is a group and $H \leq G$. If $g \in G$, then the map $H \to gH$ given by $h \mapsto gh$ is a bijection. In particular, if H is finite, then $|H| = |gH|$.*

Proof: By definition, the map is surjective. Also, if $gh_1 = gh_2$, then $h_1 = h_2$, so the map is also injective. □

We can now give a proof of Lagrange's Theorem.

Suppose G is a finite group and $H \leq G$.

Consider the left cosets of H in G.

Any one of these has $|H|$ elements (by 2.8).

Any two of them are disjoint (by 2.7).

Moreover, any $g \in G$ lies in some left H-coset, namely gH.

Thus $|G|$ is equal to $|H|$ times the number of distinct left H-cosets.

So $|H|$ divides $|G|$ and $|G|/|H|$ is equal to the number of left H-cosets in G. This concludes the proof of Lagrange's Theorem. □

DEFINITION 2.9. The number of left cosets of H in G is called the *index* of H in G.

REMARKS: If G is finite, this is equal to $|G|/|H|$, by the above. It is also equal to the number of right cosets of H in G, by the same proof. But it is also possible to write down an explicit bijection between the set of left H-cosets and the set of right H-cosets. Can you do this?

We can give a different approach to the proof using equivalence relations, which you encountered in the Introductory Module. But this is really just the same proof!

THEOREM 2.10. *Suppose G is a group and $H \leq G$. Define the relation $\sim$ on G by*

$$g \sim k \Leftrightarrow g^{-1}k \in H.$$

Then

(1) $\sim$ is an equivalence relation on G.

(2) $g \sim k$ iff $gH = kH$.

Proof: (1) is on Question sheet 6.

(2) By 2.7

$$g^{-1}k \in H \Leftrightarrow g^{-1}kH = H \Leftrightarrow kH = gH. \square$$

Note that this tells us that the $\sim$-equivalence classes are the left H-cosets.

Exercise: write down an equivalence relation on G whose classes are the right H-cosets.

EXAMPLE / EXERCISE: Let $G = S_3$ and $H = \langle \alpha \rangle$ where $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. What are the left H-cosets?

Note that $H = \{\iota, \alpha\}$ so $|H| = 2$ and $|G| = 6$. So there are 3 left H-cosets, one of which is $H = \iota H = \alpha H$. Take $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. As $\beta \notin H$ we have $\beta H \neq H$ and of course $\beta H = \{\beta, \beta\alpha\}$. We compute that $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. So let $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. As $\gamma \notin H \cup \beta H$ the remaining left H-coset is $\gamma H = \{\gamma, \gamma\alpha\}$.

As a further exercise, you could write down the right H-cosets and observe, for example, that $\beta H \neq H\beta$.

Another observation you could make is that:

H consists of the permutations taking $1 \mapsto 1$;

βH consists of the permutations taking $1 \mapsto 2$;

γH consists of the permutations taking $1 \mapsto 3$.

Find an exercise on the problem sheets which relates to this.

3 Homomorphisms

We have spent some time discussing groups. Now we briefly consider the appropriate maps between groups. You should think about how this compares with what happens with vector

spaces where the most important maps between vector spaces are linear maps: the maps which 'respect' the vector space structure.

DEFINITION 3.1. Suppose $(G, .)$ and $(H, .)$ are groups.

(1) A function $\phi : G \to H$ is a *homomorphism* if for all $g_1, g_2 \in G$ we have

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2).$$

[Note that on the left hand side here, the product $g_1 g_2$ uses the group operation in G whereas on the right-hand side, the product $\phi(g_1)\phi(g_2)$ uses the group operation in H.]

(2) If $\phi : G \to H$ is a homomorphism, the *image* of ϕ is

$$\text{im}\phi = \{\phi(g) : g \in G\}.$$

The *kernel* of ϕ is

$$\ker\phi = \{g \in G : \phi(g) = e_H\}.$$

(3) If the homomorphism $\phi : G \to H$ is a bijection, then we say that ϕ is an *isomorphism*. We say that groups G, H are *isomorphic* if there exists an isomorphism $\phi : G \to H$. In this case we write $G \cong H$.

If two groups are isomorphic, then, from the group theoretic viewpoint, they are really 'the same' group with the elements labelled in a different way.

Before we give some examples, we note the following, which should remind you of basic results (and their proofs) about linear maps.

LEMMA 3.2. *Suppose G, H are groups and $\phi : G \to H$ is a homomorphism. Then:*

(i) $\phi(e_G) = e_H$;

(ii) $\phi(g^{-1}) = (\phi(g))^{-1}$, *for all* $g \in G$;

(iii) $\text{im}\phi \leq H$ *and* $\ker\phi \leq G$.

Proof: (i) We have $\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$. In H, the equation $h = hh$ implies $h = e_H$, so we obtain $\phi(e_G) = e_H$.

(ii) We have

$$e_H \overset{(i)}{=} \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$$

and so the result follows.

(iii) Exercise: use 1.16. □

EXAMPLES 3.3. (0) (Trivial examples) Suppose G is any group. The identity map $i : G \to G$ (with $i(g) = g$ for all $g \in G$) is an isomorphism.

If G, H are groups, the map $\psi : G \to H$ with $\psi(g) = e_H$ for all $g \in G$ is a homomorphism.

(1) Suppose F is a field and $G = \mathrm{GL}(n, F)$. The determinant map

$$\det : G \to (F^\times, .)$$

is a homomorphism, by the product formula $\det(g_1 g_2) = \det(g_1)\det(g_2)$.

(2) Suppose $(H, .)$ is any group and $h \in H$. Define $\phi : (\mathbb{Z}, +) \to H$ by $\phi(n) = h^n$, for $n \in \mathbb{Z}$. By the rules for exponents, we know that

$$\phi(m+n) = h^{m+n} = h^m h^n = \phi(m)\phi(n)$$

so ϕ is a homomorphism. The image of ϕ is $\langle h \rangle$. If h has infinite order, then $\ker\phi = \{0\}$. If h has finite order n, then $\ker\phi = n\mathbb{Z}$, by 1.20(2).

(3) The exponential map

$$\exp : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, .)$$

is a homomorphism as $\exp(x+y) = \exp(x)\exp(y)$. As exp here is also a bijection, we have that it is an isomorphism (which may be a bit of a surprise as we would not normally think of the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^{>0}, .)$ as being 'the same group').

(4) The modulus map $|\cdot| : (\mathbb{C}^\times, .) \to (\mathbb{R}^\times, .)$ is a homomorphism with kernel $\{z \in \mathbb{C}^\times : |z| = 1\}$.

Lecture 17

Again, the following lemma corresponds to things you already know about linear maps.

LEMMA 3.4. *Suppose G, H, K are groups.*

(i) A homomorphism $\phi : G \to H$ is injective if and only if $\ker\phi = e_G$.

(ii) If $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms, then the composition $\psi \circ \phi : G \to K$ is a homomorphism.

(iii) If $\phi : G \to H$ is an isomorphism, then the inverse map $\phi^{-1} : H \to G$ is also an isomorphism. (So if $G \cong H$, then $H \cong G$.)

Proof: (i) $\Rightarrow$: We know that $\phi(e_G) = e_H$, so $e_G \in \ker\phi$. Injectivity tells us that $|\ker\phi| \leq 1$. So we must have $\ker\phi = \{e_G\}$.

$\Leftarrow$: Suppose $\ker\phi = \{e_G\}$ and $\phi(g_1) = \phi(g_2)$. Then by 3.2, we have $\phi(g_1 g_2^{-1}) = e_H$, thus $g_1 g_2^{-1} = e_G$. So $g_1 = g_2$.

(ii), (iii): Exercises. □

The first part of the following completes the understanding of cyclic groups. Once you have proved the 1st Isomorphism Theorem in year 2, you will be able to give a more elegant proof using Example 3.3 (2).

THEOREM 3.5. *(1) Suppose G, H are cyclic groups of the same order. Then there is an isomorphism $\alpha : G \to H$.*

(2) If V_1, V_2 are non-cyclic groups of order 4, then $V_1 \cong V_2$.

Proof: (1) Suppose G, H are finite, cyclic of order n with $G = \langle g \rangle$ and $H = \langle h \rangle$. Define $\alpha : G \to H$ by $\alpha(g^k) = h^k$ for $k \in \mathbb{Z}$.

We need to check:

α is well-defined: if $g^k = g^l$, then $h^k = h^l$. To see this, use 1.20 and the fact that g, h both have order n:

$$g^k = g^l \Rightarrow g^{l-k} = e_G \Rightarrow n \mid (l-k) \Rightarrow h^{l-k} = e_H \Rightarrow h^l = h^k.$$

α is injective: All of the above arrows reverse!

α is surjective: By definition.

So α is a bijection and for all $k, l \in \mathbb{Z}$ we have:

$$\alpha(g^k g^l) = \alpha(g^{k+l}) = h^{k+l} = h^k h^l = \alpha(g^k)\alpha(h^k).$$

So α is also a homomorphism.

Now suppose G, H are of infinite order. The only think we need to change in the above proof is when checking α is well-defined and injective. But in this case, if $l \geq k$ we have:

$$g^k = g^l \Rightarrow g^{l-k} = e_G$$

and so $l = k$ as g is of infinite order. The same idea works when reversing the arrows to get injectivity.

(2) So what we want to prove is:

Claim If V_1, V_2 are non-cyclic groups of order 4, then V_1 and V_2 are isomorphic.

Proof: Write the groups mulitplicatively and let $V_1 = \{e, a, b, c\}$. As V_1 is non-cyclic, there is no element of order 4 in V_1. By 2.2, the order of an element divides 4, so each of a, b, c has order 2. Now we show that $ab = c$. The reason is that all of the other possibilities lead to a contradiction:

$ab = a \Rightarrow b = e$;

$ab = b \Rightarrow a = e$;

$ab = e \Rightarrow ab = e = a^2 \Rightarrow b = a$.

Similarly we obtain $bc = a$ and $ca = b$. As V_1 is abelian we therefore have the complete 'multiplication table' of V_1.

But now if we write $V_2 = \{e', a', b', c'\}$ the same reasoning applies: so the nonidentity elements are of order 2 and $a'b' = c'$ etc. It follows that the map

$$e \mapsto e'; a \mapsto a'; b \mapsto b'; c \mapsto c'$$

is an isomorphism from V_1 to V_2. $\square$

4 More on S_n

4.1 Disjoint cycle form

Recall that for $n \in \mathbb{N}$ we denote by S_n the group of all permutations on $[n] = \{1, 2, \ldots, n\}$ (we did not use the notation $[n]$ before, but it's useful). The identity element of S_n is usually denoted by ι, but you can call it e if you prefer.

DEFINITION 4.1. Let $f, g \in S_n$ and $x \in [n]$. We say that f *fixes* x if $f(x) = x$ and f *moves* x if $f(x) \neq x$. The *support* of f is $\{y \in [n] : f(y) \neq y\}$. This is denoted by $\mathrm{supp}(f)$.

We say that f, g have *disjoint supports* (or are *disjoint*) if $\mathrm{supp}(f) \cap supp(g) = \emptyset$.

Note that as f is a bijection, if $f(y) \neq y$ then $f(f(y)) \neq f(y)$: so $f(y) \in \mathrm{supp}(f)$. Also $\mathrm{supp}(f) = \mathrm{supp}(f^{-1})$.

EXAMPLE: (i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{pmatrix}$; then $\mathrm{supp}(f) = \{6, 4, 2\}$.

(ii) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 1 & 6 \end{pmatrix}$; then $\mathrm{supp}(g) = \{1, 3, 5\}$.

So f, g have disjoint supports.

LEMMA 4.2. *If $f, g \in S_n$ have disjoint supports, then:*

(i) $fg = gf$;

(ii) For all $m \in \mathbb{Z}$ we have $(fg)^m = f^m g^m$.

Proof: This was Question 7 on Problem sheet 5. □

DEFINITION 4.3. Let $n \in \mathbb{N}$ and $r \leq n$. Suppose $i_1, \ldots, i_r \in [n]$ are distinct. If $f \in S_n$ fixes the other elements of $[n]$ and

$$f(i_1) = i_2; f(i_2) = i_3; \ldots, f(i_{r-1}) = i_r; f(i_r) = i_1,$$

then f is called an *r-cycle* (or a *cycle of length r*) and we write f as $(i_1, i_2, i_3, \ldots, i_r)$ or (missing out the commas) $(i_1 i_2 i_3 \ldots i_r)$.

EXAMPLES 4.4. (1) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 5 & 2 & 6 \end{pmatrix}$ is a 3-cycle: $f = (2, 4, 5) \in S_6$.

Note that this is the same permutation as $(4, 5, 2) \in S_6$. Note also that it easy to compute directly from the cycle that $f^2 = (254)$ and $f^3 = \iota$ (the identity).

(2) $(1234) \in S_5$ is the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$.

(3) A 1-cycle is the identity permutation!

(4) We multiply cycles as follows: remember they are permutations so they multiply like composition of functions - you start at the right.

If $f = (123) \in S_6$ and $g = (4526) \in S_6$, then

$fg = (126453)$ and $gf = (164523)$ (both in S_6).

Note that we do not always end up with a cycle here:

taking (12) and (13425) in S_6 we have:

$(12)(13425) = (134)(25)(6) = (134)(25)$ as (6) is just the identity. Note that by Lemma 3.2, we have $(134)(25) = (25)(134)$ as the two cycles here have disjoint supports.

Have we simplified (12)(13425) by writing it as (134)(25)? Yes, because in the second of these, the cycles are disjoint, so we can use Lemma 4.2 to compute powers. More on this later.

Lecture 18

(5) Note that when we write, say, $f = (12345) \in S_6$, the cycle goes from left to right, so $f(1) = 2$ etc. Some books might use the same notation to mean $f(2) = 1$.... so be careful.

It is easy to write down the inverse of a cycle: you just write it out the other way. For example if $f = (12345)$ then $f^{-1} = (54321)$. Think about why this is and write down a proof using the definition:

LEMMA 4.5. *If $f = (i_1 i_2 \dots i_r) \in S_n$, then f^{-1} is the r-cycle $g = (i_r i_{r-1} \dots i_2 i_1)$.*

Proof: Check that for all $x \in [n]$ we have $f(g(x)) = x = g(f(x))$. □

The following result is important and generalises what was happening in Example (4) above: writing a permutation as a product of cycles with disjoint supports. The method in the proof is straightforward to apply, but the actual proof is a bit technical so we will leave it until we have done some examples.

THEOREM 4.6. *If $f \in S_n$, then there exist cycles $f_1, f_2, \dots, f_k \in S_n$ with disjoint supports such that $f = f_1 f_2 \dots f_k$.*

REMARKS: The condition on disjoint supports means that if $1 \leq i < j \leq k$ then $\text{supp}(f_i) \cap \text{supp}(f_j) = \emptyset$. If we say that the f_i are not 1-cycles (and assume f is not the identity permutation) and also that $\text{supp}(f_i) \subseteq \text{supp}(f)$, then the representation of f as a product of disjoint cycles is unique, up to rearranging the order of the disjoint cycles in the product. We refer to this as the *disjoint cycle form* of f. A sketch proof of uniqueness is given below.. There are interesting analogies between the result and the Fundamental Theorem of Arithmetic, even though they are very different results.

EXAMPLE: (i) Write

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 5 & 1 & 10 & 9 & 3 & 8 & 7 & 2 & 6 \end{pmatrix}$$

in disjoint cycle form.

Solution: The method is to take an element and keep applying g to see what cycle it produces. If all elements have been used, then we stop; otherwise we take an element not appearing in the cycle and repeat. We keep doing this until there are no more elements left to consider (or if there are only fixed points left to consider, which will only give us 1-cycles and we can ignore these). Doing this we get:

$$g = (1, 4, 10, 6, 3)(2, 5, 9)(7, 8).$$

(I put the commas in because of the 10: (141063) might have been confusing.)

(ii) Compute g^2 and g^{-1}.

Solution: Use 4.2: so writing $g = g_1 g_2 g_3$ in disjoint cycle form we have

$$g^2 = g_1^2 g_2^2 g_3^2 = (1, 10, 3, 4, 6)(2, 9, 5)(7)(8)$$

(and we could miss out $(7)(8)$) and

$$g^{-1} = g_1^{-1} g_2^{-1} g_3^{-1} = (3, 6, 10, 4, 1)(9, 5, 2)(8, 7).$$

(iii) Let $f = (2, 4, 6)(1, 3, 8)(9, 10) \in S_{10}$. Compute fg in disjoint cycle form.

Solution: Apply the method to the product to get: $fg = (1, 6, 8, 7)(2, 5, 10)(3)(4, 9) \in S_{10}$.

Now we can give:

Proof of Theorem 4.6: We prove the result by induction on $m = |\mathrm{supp}(f)|$. If $m = 0$ then $f = \iota = (1)$ and there is nothing to prove.

Assume $m \geq 1$ (and therefore $m \geq 2$ - think about why $m = 1$ cannot happen) and take $i_1 \in \mathrm{supp}(f)$. So $f(i_1) \neq i_1$. Let $f(i_1) = i_2$, $i_3 = f(i_2)$, ... Choose r as small as possible with $f(i_r) \in \{i_1, \ldots, i_{r-1}\}$. Note that there is such an r with $r \leq n$.

Claim: $f(i_r) = i_1$.

Otherwise $f(i_r) = i_j$ for some j with $2 \leq j \leq r - 1$. So $f(i_r) = i_j = f(i_{j-1})$ and therefore (as f is injective) $i_r = i_{j-1}$. But then $f(i_{r-1}) = i_r \in \{i_1, \ldots, i_{r-2}\}$ contradicting minimality of r. $\square_{Claim}$.

It follows that $f = gf_1$ where $f_1 = (i_1, i_2, \ldots, i_r)$ and g has support $\mathrm{supp}(f) \setminus \{i_1, \ldots, i_r\}$. By induction hypothesis we can write $g = f_2 \ldots f_k$ where $f_2, \ldots, f_k$ have disjoint supports. So $f = f_2 \ldots f_k f_1$, a product of cycles with disjoint supports. Note that $f = f_1 f_2 \ldots f_k$, by 4.2. $\square_{4.6}$

Remarks: We can also prove the uniqueness of the expression of a permutation as a product of disjoint cycles by induction on the size of the support:

Use the same notation as in the above proof and suppose we also have $f = h_1 \ldots h_l$ where the h_i are cycles with disjoint supports. We want to prove that $k = l$ and the h_i are a

rearrangement of the f_j. Assume, inductively, this would be true for permutations with smaller support size.

Let $i_1 \in \mathrm{supp}(f)$. By rearranging the cycles if necessary we can assume that i_1 is in the cycles f_k and h_l. As in the above proof, let r be as small as possible with $f^r(i_1) = i_1$. Then by the argument in the proof of the claim in 4.6 we have $f_k = (i_1, f(i_1), f^2(i_1), \ldots, f^{r-1}(i_1)) = h_l$. We can therefore 'cancel' f_k and h_l in the two expressions for f and obtain $f_1 \ldots f_{k-1} = h_1 \ldots h_{l-1}$. The inductive hypothesis then gives that $k-1 = l-1$, so $k = l$, and $f_1, \ldots, f_{k-1}$ is a rearrangement of $h_1, \ldots, h_{l-1}$, as required.

4.2 Applications of disjoint cycle form

REMARKS 4.7. Here's another example of using the method in the proof of 4.6 to write down disjoint cycle form.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 3 & 6 \end{pmatrix} = (12)(345)(6).$$

This expression is unique up to missing out 1-cycles and rearranging the order: we also have $f = (345)(12)$. Note that we can also display the cycles in a number of ways: for example $(345) = (453) = (534)$.

DEFINITION 4.8. The *cycle shape* of a permutation $f \in S_n$ is the sequence of cycle lengths in descending order, including repetitions and fixed points, when it is written in disjoint cycle form.

EXAMPLES: (1) $(12)(345)(6) \in S_6$ has cycle shape $3, 2, 1$.

(2) $(12)(345)(678)(9, 10, 11, 12)(13) \in S_{13}$ has cycle shape 4,3,3,2,1. We also abbreviate this to $(4, 3^2, 2, 1)$ to show that we have two 3-cycles; in this notation, the brackets are optional.

(3) The identity $\iota \in S_9$ has cycle shape 1^9.

EXAMPLES 4.9. What are the possible cycle shapes of elements of S_4? How many permutations are there of each cycle shape?

NOTE: The number of r-cycles on a set of size r is $\frac{1}{r}r!$. This is because we have $r!$ ways of writing the r elements as a sequence $i_1, i_2, \ldots, i_r$ and each r-cycle can be represented in r different ways

$$(i_1, i_2, \ldots, i_r) = (i_2, \ldots, i_r, i_1) = \ldots = (i_r, i_1, i_2, \ldots, i_{r-1}).$$

Thus the number of distinct r-cycles on a set of size $n \geq r$ is

$$\binom{n}{r}\frac{1}{r}r! = \frac{n!}{r(n-r)!}.$$

(It's probably better to understand the reasoning here than memorizing the formula.)

Back to the question:

We see that the possible cycle shapes correspond to the possible partitions of 4: that is, the number of ways of writing 4 as a sum of a sequence of non-zero natural numbers. It's easiest to write these down starting with the biggest number.

The possibilities are:

(i) Cycle shape: 4; Example: (1234); Number of these: $3! = 6$.

(ii) Cycle shape: 3,1; Example: $(123)(4)$; Number of these: $4.2 = 8$.

(iii) Cycle shape: 2,2; Example: $(12)(34)$; Number of these: $\frac{1}{2}\binom{4}{2} = 3$.

- Explanation of the counting: there are 4 choices for the first 2-cycle and then the remaining 2 elements form the other 2-cycle. But each permutation with this cycle shape is then chosen twice as $(12)(34) = (34)(12)$, so we divide by 2.

(iv) Cycle shape: 2, 1, 1; Example: $(12)(3)(4)$; Number of these: $\binom{4}{6} = 6$

- note that the double-counting in the previous example does not occur here.

(v) Cycle shape: 1,1,1,1; this is the identity permutation and the number of these is 1.

Note that as a check we add up the possibilities: $6 + 8 + 3 + 6 + 1 = 24 = |S_4|$.

The following allows us to easily compute the order of a permutation from its cycle shape.

THEOREM 4.10. *Suppose $g \in S_n$ is written in disjoint cycle form as $g = g_1 g_2 \dots g_k$ where g_i is an r_i-cycle (for $i = 1, \dots, k$) and $g_1, \dots, g_k$ are disjoint. If $m \in \mathbb{N}$, then:*

(i) $g^m = g_1^m g_2^m \dots g_k^m$;

(ii) $g^m = \iota \Leftrightarrow g_i = \iota$ for all $i = 1, \dots, k$.

(iii) The order of g is the least common multiple $\operatorname{lcm}(r_1, \dots, r_k)$ of the lengths of the disjoint cycles in g.

(iv) $g^{-1} = g_1^{-1} \dots g_k^{-1}$.

Before giving the proof, we do some examples.

EXAMPLES 4.11. **(0)** We can write down the orders of the elements in S_4:

Cycle shape: 4; Example: (1234); order 4.

Cycle shape: 3,1; Example: $(123)(4)$; order 3.

Cycle shape: 2,2; Example: $(12)(34)$; order 2.

Cycle shape: 2, 1, 1; Example: $(12)(3)(4)$; order 2.

Cycle shape: 1,1,1,1; order 1.

(1) $(12)(345)(6789) \in S_9$ has order $\mathrm{lcm}(2,3,4) = 12$.

(2) Find an element of order 15 in S_9: as $15 = \mathrm{lcm}(5,3,1)$ and $9 = 5+3+1$ we can write down $(12345)(678)(9) \in S_9$.

(3) There is no element of order 20 in S_8.

To see this we need to show that there do not exist $r_1, \ldots, r_k \in \mathbb{N}$ such that $\mathrm{lcm}(r_1, \ldots, r_k) = 20$ and $\sum_i r_i = 8$. Suppose there are such r_i. Then one of them would have to be divisible by 5, and therefore be at least 5. One of them would have to be divisible by 4, and therefore be at least 4. So the smallest possibility for having an element of order 20 is 9, not 8.

(Note: $(12345)(6789) \in S_9$ has order 20.)

Proof of Theorem 4.10: (i) is an easy generalisation of Lemma 4.2 (ii).

(ii) $\Rightarrow$ is by (i). For $\Leftarrow$, note that if $g^m = \iota$, then by (i) $g_1^m g_2^m \ldots g_k^m = \iota$. The permutations g_i^m have disjoint supports (although they are not necessarily cycles) as the g_i have disjoint supports. So each g_i^m is the identity.

(iii) By (ii) $g^m = \iota \Leftrightarrow g_i^m = \iota$ for all $i = 1, \ldots, k$. As g_i is an r_i-cycle, its order is r_i. Therefore $g_i^m = \iota \Leftrightarrow r_i | m$. So the smallest $m \in \mathbb{N}$ with $g^m = \iota$ is $\mathrm{lcm}(r_1, \ldots, r_k)$.

(iv) We already know that $g^{-1} = g_k^{-1} \ldots g_1^{-1}$. Note that $\mathrm{supp}(g_i) = \mathrm{supp}(g_i^{-1})$ so $g_1^{-1}, \ldots, g_k^{-1}$ are disjoint and therefore commute. So $g^{-1} = g_1^{-1} \ldots g_k^{-1}$. $\square_{4.10}$

4.3 Dihedral groups

Lecture 19

Suppose $n \in \mathbb{N}$ and $n \geq 3$. Informally, the *dihedral group* D_{2n} is the group of symmetries of a regular n-gon. This is a bit vague, so we shall think of the regular n-gon as centred at $0 \in \mathbb{R}^3$ and having vertices in the xy-plane, labelled $1, 2, \ldots, n$ in a clockwise direction. Every symmetry of the n-gon is determined by its effect on the set of vertices and of course this is a permutation of the vertices. So we may think of the group of symmetries as a subgroup of S_n.

First, we describe the symmetries geometrically:

(a) rotate about the axis (the z-axis) through 0 and perpendicular to the n-gon, through an angle which is a multiple of $2\pi/n$. There are n such rotational symmetries.

(b) (i) Case n odd: Flip (i.e. rotate by π) the n-gon about an axis through 0 and a vertex (we can also view this as a reflection in this axis).

(ii) Case n even: Flip about an axis through two opposite vertices - there are $n/2$ of these; OR flip about an axis through the mid-points of two opposite edges - also $n/2$ of these.

Exercise: Draw some pictures for these in the cases $n = 4$ and $n = 5$.

The composition of two symmetries is another symmetry and each is invertible. Thus we have a group of $2n$ different symmetries of the regular n-gon. As discussed above, we will

think of this as a subgroup of S_n (the group of all permutations of the vertices) and denote it by D_{2n}. It is called the *dihedral group* of order $2n$. (Some books will denote it by D_n.)

We should justify why there are no more that the $2n$ symmetries listed above. It will be enough to show:

THEOREM 4.12. *The group $G \leq S_n$ of permutations induced on the vertices of a regular n-gon by symmetries of the n-gon has size $2n$.*

Proof: Note that as there is a rotation taking any vertex to any other vertex we have $\{g(1) : g \in G\} = [n]$, the set of all vertices. By Question 8 on Sheet 7, we therefore have $|G| = n|H|$ where $H = \{g \in G : g(1) = 1\}$. But the only symmetries fixing the vertex 1 are the identity and the flip about the axis which passes through 0 and 1. So $|H| = 2$ and $|G| = 2n$, as required. □

The lecture could stop here, but maybe you think this is still too informal. In which case we could make things completely precise, but less geometric, in the following way. The idea of course is that a is the flip which fixes 1 and b is the flip which interchanges 1 and n.

DEFINITION 4.13. Let $n \in \mathbb{N}$ with $n \geq 3$. Consider the following elements of S_n in disjoint cycle form:

$$a = (1)(2, n)(3, n-1)\dots$$

and

$$b = (1, n)(2, n-1)\dots.$$

(The precise formulas will depend on whether n is odd or even. If you wish, you can write out the two cases separately, but do the exercise below first.) We define the *dihedral group* D_{2n} to be $D_{2n} = \langle a, b\rangle \leq S_n$.

EXERCISE: Write these out for the cases $n = 4$ and $n = 5$.

If you did the exercise, then you should be able to see that a and b are both permutations of the vertices of the n-gon which are induced by symmetries. So to justify why $\langle a, b\rangle$ contains *all* symmetries, and therefore why the definition is reasonable, we prove:

THEOREM 4.14. *We have $|\langle a, b\rangle| = 2n$.*

Proof: Clearly a, b are of order 2. So by Question 5 of Sheet 8, it will suffice to prove that ab is of order n. But ab is the cycle $(123\dots n)$ (not completely trivial to prove: you would have to check the cases n odd or even separately if you wanted to avoid geometric arguments, but check it for the cases $n = 4, 5$). So we are done. □

4.4 The sign of a permutation; Determinants again

Lecture 20

[On the MathSoc website, you should be able to find Professor Buzzard's M2PM2 (Algebra 2) notes from 2014. He probably also has a webpage with these on. Section 3 of the notes

has material about the sign (or signature) of a permutation; section 7 gives an alternative way of doing determinants using this.]

In Question 3 of Problem Sheet 8, we see that every permutation in S_n can be written as a product of 2-cycles. For example:
$(123) = (12)(23)$
$(1234) = (12)(23)(34)$
$\vdots$
$(1234\ldots r) = (12)(23)\ldots(r-1,r)$.

There is no uniqueness to the factorisation here: the 2-cycles are not assumed to be disjoint. The number of 2-cycles used can vary: for example
$(123) = (13)(32)(13)(32)$.
However, we we see that, for any particular permutation, the number of 2-cycles used is either always odd, or always even.

To prove this, we are going to define a very special homomorphism $\mathrm{sgn} : S_n \to \{1, -1\}$. The group on the right here is considered under multiplication: it is of course a cyclic group of order 2. We might denote it by ± 1 if we get bored with set brackets. The homomorphism will be non-trivial if $n \geq 2$.

Some people call $\mathrm{sgn}(f)$ the *signature* of $f \in S_n$; others call it the *signum* of f. I will call it the *sign* of f. The definition will involve a small detour involving polynomials in several variables.

Let $n \in \mathbb{N}$ with $n \geq 2$. Let $x_1, \ldots, x_n$ be variables. If $P(x_1, \ldots, x_n)$ is any polynomial in variables $x_1, \ldots, x_n$ and $f \in S_n$, then we define $f(P)$ to be the polynomial obtained by permuting the variables using f: so x_i is replaced by $x_{f(i)}$.

Example: Suppose $n = 3$. Consider the permutations $f = (123)$ and $g = (12) \in S_3$. Let $P(x_1, x_2, x_3) = 3x_1^2 - 2x_1x_3$. Then:
fP is the polynomial $3x_2^2 - 2x_2x_1$;
$g(fP)$ is the polynomial $3x_1^2 - 2x_1x_2$.
Notice that $(gf) = (1)(23)$ and so:
$(gf)P$ is the polynomial $3x_1^2 - 2x_1x_2$. Thus $(gf)P = g(fP)$.

More generally we have:

Lemma 4.15. *For all $f, g \in S_n$ and polynomials P in variables $x_1, \ldots, x_n$ we have:*

(i) If $\alpha \in \mathbb{R}$, then: $f(\alpha P) = \alpha f(P)$.

(ii) $g(f(P)) = (gf)(P)$.

Proof: (i) This should be clear.

(ii) To compute $g(f(P))$ we make the successive substitutions

$$x_i \mapsto x_{f(i)} \mapsto x_{g(f(i))},$$

the first gives us $f(P)$ and the second gives $g(f(P))$. But this is also what we would get by making the substitution $x_i \mapsto x_{(gf)(i)}$ and this is $(gf)(P)$. $\square$

Now we focus on the polynomial (over $\mathbb{R}$) $\Delta = \Delta(x_1, \ldots, x_n)$ given by the product of all expressions $(x_i - x_j)$ with $1 \leq i < j \leq n$:

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

You may remember that you have seen this expression before in the Vandermonde determinant.

EXAMPLE: If $n = 3$ and $f = (123)$ then $\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ and $f(\Delta) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = \Delta$ (as there have been two changes of sign here).

If $g = (12) \in S_3$ then $g(\Delta) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -\Delta$ (there is one change of sign).

LEMMA 4.16. *For any $n \geq 2$ and $f \in S_n$, either $f(\Delta) = \Delta$ or $f(\Delta) = -\Delta$.*

Proof: If $k \neq l$ we have a factor $\pm(x_k - x_l)$ appearing exactly once in $f(\Delta)$. It comes from the factor $\pm(x_i - x_j)$ in Δ, where $\{i, j\} = \{f^{-1}(l), f^{-1}(k)\}$. $\square$

DEFINITION 4.17. With this notation, we let $\mathrm{sgn}(f) = 1$ if $f(\Delta) = \Delta$ and $\mathrm{sgn}(f) = -1$ if $f(\Delta) = -\Delta$. Thus $f(\Delta) = \mathrm{sgn}(f)\Delta$.

Now we have the main result:

THEOREM 4.18. *Suppose $n \geq 2$ and $f, g \in S_n$.*

(i) We have $\mathrm{sgn}(fg) = \mathrm{sgn}(f)\mathrm{sgn}(g)$, so $\mathrm{sgn} : S_n \to \pm 1$ is a homomorphism.

(ii) If f is a 2-cycle, then $\mathrm{sgn}(f) = -1$.

(iii) If g is an r-cycle, then $\mathrm{sgn}(g) = (-1)^{r-1}$.

Note that using this it is easy to compute the sign of *any* $h \in S_n$. We write h in disjoint cycle form as $h = h_1 h_2 \ldots h_k$. Using (i), $\mathrm{sgn}(h) = \mathrm{sgn}(h_1)\mathrm{sgn}(h_2)\ldots\mathrm{sgn}(h_k)$, and (iii) tells us how to compute each of the $\mathrm{sgn}(h_i)$.

EXAMPLE: Let $h = (123)(45)(6789) \in S_9$. Then $\mathrm{sgn}(h) = (-1)^2(-1)^1(-1)^3 = 1$.

Proof of 4.18:

(i) We have

$$(gf)(\Delta) \overset{4.15(ii)}{=} g(f(\Delta)) \overset{def}{=} g(\mathrm{sgn}(f)\Delta) \overset{4.15(i)}{=} \mathrm{sgn}(f)g(\Delta) = \mathrm{sgn}(f)\mathrm{sgn}(g)\Delta.$$

But also $(gf)(\Delta) = \mathrm{sgn}(gf)\Delta$. So $\mathrm{sgn}(gf) = \mathrm{sgn}(f)\mathrm{sgn}(g) = \mathrm{sgn}(g)\mathrm{sgn}(f)$.

(ii) First we note that if $f = (12)$, then $f(\Delta) = -1$ as the only factor in Δ which changes sign is $(x_1 - x_2)$.

Now suppose $1 \leq i < j \leq n$ and consider the 2-cycle (ij). There is some $k \in S_n$ with $k(i) = 1$ and $k(j) = 2$. Then one computes that $k^{-1}(12)k = (ij)$ (Exercise!) But then by (i),

$$\mathrm{sgn}((ij)) = \mathrm{sgn}(k^{-1})\mathrm{sgn}((12))\mathrm{sgn}(k) = \mathrm{sgn}((12)) = -1.$$

(Using that ± 1 is an abelian group.)

[There is a different proof of this in Professor Buzzard's notes.]

(iii) An r-cycle g can be written as a product of $r-1$ 2-cycles: see the solution to Question 9(i) on Sheet 8. So by (i) and (ii), $\mathrm{sgn}(g) = (-1)^{r-1}$. $\square$

REMARKS 4.19. (1) A permutation $f \in S_n$ is called *even* if $\mathrm{sgn}(f) = 1$ and *odd* if $\mathrm{sgn}(f) = -1$. This is a bit confusing because a cycle of odd length is an even permutation etc.

The set of even permutations in S_n is a subgroup of S_n (it is the kernel of the homomorphism sgn) called the *alternating group* A_n. If $n \geq 2$, then the index of A_n in S_n is 2: the two cosets are A_n and the set of odd permutations (Ex: prove this!).

(2) By the solution to Question 3(ii) on sheet 8, every permutation $g \in S_n$ can be written as a product of 2-cycles. There is no uniqueness statement here, but because of the sgn function, the parity of the the number of 2-cycles needed cannot be changed for g: we need an even number of 2-cycles if g is an even permutation and an odd number of 2-cycles if g is an odd permutation. This explains the terminology (partly).

Now we can give another expression for the determinant of a matrix $A = (a_{ij}) \in M_n(F)$ (where F is a field).

THEOREM 4.20. *For every matrix $A = (a_{ij}) \in M_n(F)$ we have:*

$$\det(A) = \sum_{f \in S_n} \mathrm{sgn}(f) a_{1f(1)} a_{2f(2)} \dots a_{nf(n)}.$$

So this is a sum of $n!$ terms each one of which is a product of n entries of A where there is exactly one entry from each row and column.

EXERCISE: Write out the above formula in the cases $n = 2$ and $n = 3$ and compare with the usual expressions you know for det in these cases.

Professor Buzzard's notes take this formula as the *definition* of the determinant. He then proves that determinants can be computed by first-row expansion (Proposition 7.5 of his notes). So this gives a proof of the above Theorem. I will sketch a proof of the Theorem which is independent from Professor Buzzard's notes If you want to understand it, it might help to write it out in the case $n = 3$, checking all of the assertions.

Sketch of proof of Theorem:

Before we start, note that the set of even permutation in S_n is the subgroup A_n and if g is any odd permutation, then $gA_n = S_n \setminus A_n = A_n g$ (compare Question 6 on probelm sheet 7, or you can prove this directly). In particular, any odd permutation h can be written in the form $h = fg$ for some unique even permutation $f = hg^{-1}$.

For $A = (a_{ij}) \in M_n(F)$, write

$$\det'(A) = \sum_{f \in S_n} \mathrm{sgn}(f) a_{1f(1)} a_{2f(2)} \dots a_{nf(n)}.$$

We want to show that $\det'(A) = \det(A)$. Recall that det is the unique function $M_n(F) \to F$ satisfying the properties D1, D2, D3, D4 (as in Section 5.1 of Linear Algebra notes; compare with Exercise 1 on Sheet 2). It is not hard to show that $\det'$ satisfies D1, D2, D4, so it is enough to prove that $\det'$ satisfies D3. In other words, we have to show that if A has two consecutive rows equal then $\det'(A) = 0$. To simplify the notation, assume that rows 1 and 2 of A are equal, so $a_{1j} = a_{2j}$ for all $j \leq n$.

Let $g \in S_n$ be the permutation $g = (12)$. This is an odd permutation so $S_n = A_n \cup A_n g$ and thus

$$\det'(A) = \sum_{f \in A_n} \mathrm{sgn}(f) a_{1f(1)} a_{2f(2)} \dots a_{nf(n)} + \sum_{f \in A_n} \mathrm{sgn}(fg) a_{1fg(1)} a_{2fg(2)} \dots a_{nfg(n)}.$$

Now, $\mathrm{sgn}(fg) = -\mathrm{sgn}(f) = -1$ and $g(1) = 2, g(2) = 1, g(3) = 3, \dots, g(n) = n$. So

$$\det'(A) = \sum_{f \in A_n} a_{1f(1)} a_{2f(2)} \dots a_{nf(n)} - \sum_{f \in A_n} a_{1f(2)} a_{2f(1)} a_{3f(3)} \dots a_{nf(n)}.$$

As $a_{1f(2)} = a_{2f(2)}$ and $a_{2f(1)} = a_{1f(1)}$, we obtain $\det'(A) = 0$. □

A different sketch roof: If $f \in S_n$ let M_f be the $n \times n$ matrix with ij entry equal to 1 if $j = f(i)$ and 0 otherwise. Note that another way of thinking of this is that M_f is obtained from the identity matrix I_n by applying the permutation f^{-1} to the rows of I_n: so row i of I_n is row $f^{-1}(i)$ of M_f. (As an exercise, check this with $f = (123) \in S_3$).

Let $A(f)$ be the $n \times n$ matrix with ij entry equal to $a_{if(i)}$ if $j = f(i)$ and 0 otherwise. So $\det(A(f)) = a_{1f(1)} a_{2f(2)} \dots a_{nf(n)} \det(M_f)$.

We can use the linearity property (D2) of determinants (and other properties in 5.1.4 - 5.1.8) to show that

$$\det(A) = \sum_{f \in S_n} \det(A(f)).$$

So it remains to prove that $\det(M_f) = \mathrm{sgn}(f)$. We obtain M_f from I_n by applying the permutation f^{-1} to the rows of I_n. Write f^{-1} as a product of 2-cycles $g_1 \dots g_k$. When we apply this to the rows of I_n we are doing k elementary row operations, each of which interchanges two rows. So $\det(M_f) = (-1)^k \det(I_n) = (-1)^k$. But also $\mathrm{sgn}(f) = \mathrm{sgn}(f^{-1}) = (-1)^k$ as f^{-1} is a product of k 2-cycles. Hence the result. □