MA301 Algebra

D.H.Fremlin

This course introduces the theory of finite groups, with applications to geometry and combinatorics.

Semigroups

I begin with a short section on the general theory of semigroups.

Definition A **semigroup** is a set F (allowing $F = \emptyset$) together with a binary operation $(x, y) \mapsto xy : F \times F \to F$ which is **associative**, that is, such that $x(yz) = (xy)z$ for all x, y, $z \in F$.

Examples (a) $(\mathbb{N} \setminus \{0\}, +)$, where $\mathbb{N} = \{0, 1, 2, \dots\}$ is the set of non-negative integers.

(b) $(\mathbb{N}, \times)$.

(c) The set of $n \times n$ real matrices, with matrix multiplication.

(c) Let X be any set. Let F be the set of all functions f such that $\operatorname{dom} f \subseteq X$ and $f(x) \in X$ for every $x \in \operatorname{dom} f$, with composition. Then F is a semigroup. **P** (i) If f, $g \in F$ then

$$\operatorname{dom}(f \circ g) = \{x : x \in \operatorname{dom} g,\ g(x) \in \operatorname{dom} f\} \subseteq \operatorname{dom} g \subseteq X$$

and $(f \circ g)(x) = f(g(x)) \in X$ for every $x \in \operatorname{dom}(f \circ g)$, so $f \circ g \in F$; thus $\circ$ is a binary operation on F. (ii) If f, g, $h \in F$ then

$$\begin{aligned}
\operatorname{dom}(f \circ (g \circ h)) &= \{x : x \in \operatorname{dom}(g \circ h),\ (g \circ h)(x) \in \operatorname{dom} f\} \\
&= \{x : x \in \operatorname{dom} h,\ h(x) \in \operatorname{dom} g,\ g(h(x)) \in \operatorname{dom} f\} \\
&= \{x : x \in \operatorname{dom} h,\ h(x) \in \operatorname{dom}(f \circ g)\} \\
&= \operatorname{dom}((f \circ g) \circ h).
\end{aligned}$$

So $(f \circ g) \circ h$ and $f \circ (g \circ h)$ have the same domain. And if x is any point of this common domain,

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

So $(f \circ g) \circ h$ and $f \circ (g \circ h)$ have the same domain and the same value at every point of that domain, and are the same function. **Q**

(e) If F is any semigroup, then for A, $B \subseteq F$ write AB for the set $\{ab : a \in A,\ b \in B\}$. With this multiplication, $\mathcal{P}F$ is a semigroup, because

$$\begin{aligned}
A(BC) = \{ay : a \in A,\ y \in BC\} &= \{a(bc) : a \in A,\ b \in B,\ c \in C\} \\
&= \{(ab)c : a \in A,\ b \in B,\ c \in C\}
\end{aligned}$$

(because multiplication in F is associative)

$$= \{xc : x \in AB,\ c \in C\} = (AB)C.$$

Multiplying strings If F is a semigroup and a, b, c, d belong to F, then

$$(ab)(cd) = ((ab)c)d = (a(bc))d = a((bc)d) = a(b(cd)) = \dots.$$

These notes are distributed to students on the understanding that they have not been fully checked for errors. They are not intended to provide a substitute for attendance at lectures. If you notice a mistake, please tell the lecturer!

Typeset by $\mathcal{AMS}$-TEX

Generally, given any finite string a_0, $a_1, \ldots, a_n$ of elements of a semigroup, we can safely write $a_0a_1\ldots a_n$ for their product, doing the multiplications in any way we like, so long as we keep the elements in order. (We do *not* expect $abc = a(bc) = (ab)c$ to be the same as cba.)

Commutative semigroups However, it does sometimes happen that we can do our multiplications either way round without changing the answers; a semigroup is called **commutative** or **abelian** if $xy = yx$ for all x, y. Of the examples above, $(\mathbb{N}\setminus\{0\},+)$ and $(\mathbb{N},\times)$ are commutative and the others aren't.) This course is going to concentrate on *non-commutative* operations, and commutativity will be rare (and correspondingly important).

Identities If F is a semigroup, an **identity** in F is an $e \in F$ such that $xe = ex = x$ for every $x \in F$.

Theorem If F is a semigroup, it has at most one identity.

proof If e, e' are identities in F, then

$$\begin{aligned} e &= ee' \text{ because } e' \text{ is an identity,}\\ &= e' \text{ because } e \text{ is an identity.}\end{aligned}$$

Remark We can therefore safely speak of *the* identity in a semigroup with identity.

Inverses If F is a semigroup with identity e, and $x \in F$, then an **inverse** of x in F is a $y \in F$ such that $xy = yx = e$.

Theorem If F is a semigroup with identity, then any element of F has at most one identity.

proof If y and z are both inverses of x, then

$$y = ye = y(xz) = (yx)z = ez = z.$$

Definition A **group** is a semigroup with identity in which every element has an inverse.

Remark Because any element of the group has exactly one inverse, we can safely write x^{-1} for the inverse of x, just as we can safely write e for the unique identity of the group.

Theorem Let F be a semigroup with identity e. Then the set F^* of invertible elements of F, with the multiplication inherited from F, is a group.

proof (a) If a, $b \in F^*$ there are x, $y \in F$ such that $ax = xa = by = yb = e$. In this case

$$(ab)(yx) = a(by)x = aex = ax = e, \quad (yx)(ab) = y(xa)b = yeb = yb = e.$$

So ab has an inverse $yx \in F$, and belongs to F^*. This shows that multiplication provides a binary operation from $F^* \times F^*$ to F^*.

(b) If a, b, $c \in F^*$ then $(ab)c = a(bc)$ because the multiplication of F is associative. So F^* is a semigroup.

(c) $ee = e$ so e is its own inverse in F and $e \in F^*$. Now $ae = ea = a$ for every $a \in F^*$ (because $ae = ea = a$ for every $a \in F$), and e is an identity in F^*. Thus F^* is a semigroup with identity.

(d) If $a \in F^*$, there is an $x \in F$ such that $ax = xa = e$. Because $xa = ax = e$, a is an inverse of x in F, and $x \in F^*$. Now $ax = xa = e$ is the identity in F^*, so x is an inverse of a in F^*. As a is arbitrary, every element of F^* is invertible in F^* and F^* is a group.

Remarks Observe that in the argument for (a) of the proof, I showed that $(ab)^{-1} = b^{-1}a^{-1}$, because $abb^{-1}a^{-1} = b^{-1}a^{-1}ab = e$. Similarly, in (d), I showed that $(a^{-1})^{-1} = a$, because $aa^{-1} = a^{-1}a = e$.

Cancellation laws If G is a group, then

$$\text{whenever } ax = ay \text{ in } G, \text{ then } x = y.$$

P $x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = ey = y$. **Q**
Similarly,

$$\text{whenever } xa = ya \text{ in } G, \text{ then } x = y.$$

P $x = xe = x(aa^{-1}) = (xa)a^{-1} = (ya)a^{-1} = y(aa^{-1}) = ye = y$. **Q**

Subgroups: definition Let G be a group. A **subgroup** of G is a subset H of G such that

$$e \in H,$$

$$ab \in H \text{ for all } a,\, b \in H,$$

$$a^{-1} \in H \text{ for every } a \in H.$$

Notation The formula '$H \le G$' is often used to mean 'H is a subgroup of G'.

Theorem If G is a group and H is a subgroup of G, then H, with the multiplication inherited from that of G, is a group in its own right.

proof If a, $b \in H$ then $ab \in H$ (second clause in the definition of 'subgroup'. So multiplication is a binary operation on H.

If a, b, $c \in H$ then $(ab)c = a(bc)$ because the multiplication on G is associative. So H is a semigroup.

The identity e of G belongs to H (first clause in the definition of 'subgroup'), and $ea = ae = a$ for every $a \in H$, so e is also an identity in H, and H is a semigroup with identity.

If $a \in H$, then a^{-1} (the inverse of a in G) belongs to H (third clause in the definition of 'subgroup'), and $aa^{-1} = a^{-1}a = e$, the identity of H; so a^{-1} is an inverse of a in H. Thus every element of H has an inverse in H and H is a group.

Useful Fact If G is a group and H is a subgroup of G, then $H = HH$. **P** $HH = \{ab : a,\, b \in H\} \subseteq H$ just because $ab \in H$ for every a, $b \in H$. On the other hand, $H = \{ae : a \in H\} \subseteq HH$ because $e \in H$. **Q**

Cosets Let G be a group and B a subset of G. Then a **left coset** of B is a set of the form $aB = \{ab : b \in B\} = \{a\}B$ where $a \in B$. Similarly, a **right coset** of B is a set of the form $Ba = \{ba : b \in B\}$.

Remark It is essential to distinguish between a *coset* of B (which is just a subset of G) and its *name* aB or Ba. The point is that the same coset may be expressible as aB in many different ways, but is still only one set.

Lemma Let G be a group and H a subgroup of G. Then every element of G belongs to exactly one left coset of H.

proof Let x be any point of G. Then $x = xe \in xH$ so x belongs to the left coset xH of H.

Now suppose that A is any left coset of H containing x. Then A is expressible as aH for some $a \in H$. Since $x \in A = aH$,

$$xH \subseteq (aH)H = a(HH) = aH = A.$$

On the other hand, there is an $h \in H$ such that $x = ah$. Now

$$a = ae = a(hh^{-1}) = (ah)h^{-1} = xh^{-1} \in xH,$$

so $A = aH \subseteq xHH = xH$. Thus $A = xH$, and xH is the only left coset of H containing x.

Remark Similarly, for any $x \in G$, Hx is the only right coset of H containing x.

Lemma Let G be a group and H a finite subgroup of G. Then every left coset of H has exactly $\#(H)$ members.

proof Let A be a left coset of H. Then A is expressible as aH where $a \in G$. Consider the function

$$h \mapsto ah : H \to aH.$$

This is surjective by the definition of aH. On the other hand, if $ah = ah'$, then $h = h'$, by the cancellation law. So $h \mapsto ah$ is injective, and is a bijection between H and aH. Accordingly $A = aH$ and H must have the same number of members.

Theorem Let G be a finite group and H any subgroup of G. Then

$$\#(G) = \#(H)\times(\text{number of left cosets of } H).$$

proof The left cosets of H cut G up into disjoint sets which are all of the same size $\#(H)$.

Corollary (Lagrange's Theorem) If G is a finite group and H is a subgroup of G, then $\#(H)$ is a factor of $\#(G)$.

Example Consider the group S_3 of bijections from $\{1,2,3\}$ to itself. This has 6 elements, being

$$e, \quad \rho = (\overleftarrow{123}), \quad \rho^2 = (\overleftarrow{132}),$$

$$\sigma = (\overleftarrow{12}), \quad \rho\sigma = (\overleftarrow{13}), \quad \rho^2\sigma = (\overleftarrow{23});$$

we have $\rho^3 = \sigma^2 = e$ and $\sigma\rho = \rho^2\sigma$, so that $\sigma^{-1} = \sigma$ and $\rho^{-1} = \rho^2$.

The sets $H = \{e, \rho, \rho^2\}$ and $K = \{e, \sigma\}$ are subgroups of S_3. Their cosets are

$$H = eH = \rho H = \rho^2 H = He = H\rho = H\rho^2,$$

$$\begin{aligned}\{\sigma, \rho\sigma, \rho\sigma^2\} &= \sigma H = (\rho\sigma)H = (\rho^2\sigma)H \\ &= H\sigma = H(\rho\sigma) = H(\rho^2\sigma);\end{aligned}$$

$$K = eK = \sigma K, \quad \{\rho, \rho\sigma\} = \rho K = (\rho\sigma)K, \quad \{\rho^2, \rho^2\sigma\} = \rho^2 K = (\rho^2\sigma)K,$$

$$K = Ke = K\sigma, \quad \{\rho, \rho^2\sigma\} = K\rho = K(\rho^2\sigma), \quad \{\rho^2, \rho\sigma\} = K\rho^2 = K(\rho\sigma).$$

Note that all the left cosets of H are right cosets, and vice versa; but that the left and right cosets of K are different, except of course for $eK = Ke = K$.

Normal subgroups: Definition If G is a group, a **normal subgroup** of G is a subgroup H such that $aH = Ha$ for every $a \in G$; in this case we write $H \lhd G$.

Remark If H is a subgroup of G, then it is normal iff $aha^{-1} \in H$ for every $h \in H$, $a \in G$. **P** (i) If $H \lhd G$, $a \in G$ and $h \in H$, then $aha^{-1} \in aHa^{-1} = aa^{-1}H = eH = H$. (ii) If H satisfies the condition and $a \in G$, then

$$aHa^{-1} = \{aha^{-1} : h \in H\} \subseteq H,$$

so $aH = aHe = aHa^{-1}a \subseteq Ha$. Similarly, $a^{-1}H \subseteq Ha^{-1}$ and $Ha = eHa = aa^{-1}Ha \subseteq aHa^{-1}a = aH$. So $aH = Ha$. As a is arbitrary, $H \lhd G$. **Q**

Theorem If G is a group and $H \lhd G$, then the set G/H of cosets of H is a group under multiplication of subsets.

proof (a) (The key) If a, $b \in G$ then

$$(aH)(bH) = a(Hb)H = a(bH)H = (ab)(HH) = abH$$

(remember that $HH = H$ for any subgroup H of G).

(b)(i) If A, $B \in G/H$ we can express them as aH, bH where a, $b \in G$; now $AB = aHbH = abH \in G/H$. Thus multiplication of subsets is a binary operation on G/H.

(ii) Multiplication of subsets is an associative operation on $\mathcal{P}G$, so G/H is a semigroup.

(iii) $H = eH \in G/H$. If $A \in G/H$, we can express it as aH where $a \in G$; now

$$AH = aHeH = aeH = aH = A, \quad HA = eHaH = eaH = aH = A.$$

So H is the identity of G/H.

(iv) If $A \in G/H$, we can express it as aH where $a \in G$; now $B = a^{-1}H \in G/H$, and

$$AB = aHa^{-1}H = aa^{-1}H = eH = H, \quad BA = a^{-1}HaH = a^{-1}aH = eH = H.$$

Thus B is the inverse of A in G/H. As A is arbitrary, every element of G/H has an inverse and G/H is a group.

Homomorphisms: Definition If G and H are groups, a function $\phi : G \to H$ is a **homomorphism** if $\phi(ab) = \phi(a)\phi(b)$ for all a, $b \in G$.

Remark Note that in the formula

$$\phi(ab) = \phi(a)\phi(b)$$

we are using two different multiplications. In the product ab we are using the group operation of G and in the product $\phi(a)\phi(b)$ we are using the group operation of H. A stricter notation would be to say 'if $(G, \cdot)$ and $(H, *)$ are groups, a function $\phi : G \to H$ is a homomorphism if $\phi(a \cdot b) = \phi(a) * \phi(b)$ for all a, $b \in G$'. A typical example would be the function $\exp : \mathbb{R} \to]0, \infty[$. Since $\exp(x + y) = \exp(x) \times \exp(y)$ for all real x and y, this is a homomorphism from the group $(\mathbb{R}, +)$ to the group $(]0, \infty[\,, \times)$.

Theorem Let G, H be groups and $\phi : G \to H$ a homomorphism. Then, writing e_G for the identity of G ad e_H for the identity of H,

$$\phi(e_G) = e_H, \quad \phi(a^{-1}) = \phi(a)^{-1} \text{ for every } a \in G.$$

proof (a)

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

cancelling e_G on the right, $e_H = \phi(e_G)$.

(b)

$$\phi(a)^{-1}\phi(a) = e_H = \phi(e_G) = \phi(a^{-1}a) = \phi(a^{-1})\phi(a);$$

cancelling $\phi(a)$ on the right, $\phi(a)^{-1} = \phi(a)^{-1}$.

Examples (i) If $G = (\mathbb{R}, +)$, $H = (]0, \infty[\,, \times)$ and $\phi = \exp$, then $e_G = 0$ and $e_H = 1 = \exp(0)$; if $x \in G$, its inverse in G is $-x$, and $\exp(-x) = \frac{1}{\exp(x)}$ is the inverse of $\exp(x)$ in H.

(ii) If G is any group and $H \lhd G$, then the map $a \mapsto aH : G \to G/H$ is a homomorphism (because $aHbH = abH$ for all a, $b \in G$); the image of e_G is $e_GH = H$, the identity of G/H; and for any $a \in G$ the image of a^{-1} is $a^{-1}H$, which is the inverse of aH in G/H.

Theorem Let G, H and K be groups, and $\phi : G \to H$, $\psi : H \to K$ homomorphisms. Then $\psi\phi : G \to K$ is a homomorphism.

proof If a, $b \in G$, then

$$(\psi\phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b))$$

(because ϕ is a homomorphism)

$$= \psi(\phi(a))\psi(\phi(b))$$

(because ψ is a homomorphism)

$$= (\psi\phi)(a)(\psi\phi)(b).$$

Remark Note that in the line

$$(\psi\phi)(ab) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b))$$

we are using three different multiplications; a stricter notation would be to say that if $\cdot$, $*$ and $\times$ are the multiplications in G, H and K respectively, then

$$(\psi\phi)(a \cdot b) = \psi(\phi(a) * \phi(b)) = \psi(\phi(a)) \times \psi(\phi(b)).$$

Definition If G and H are groups, an **isomorphism** from G to H is a bijective homomorphism. We say that G and H are **isomorphic**, $G \cong H$, if there is an isomorphism from G to H.

Proposition If $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ is a homomorphism, therefore an isomorphism.

proof Because $\phi : G \to H$ is a bijection, $\phi^{-1} : H \to G$ is defined, and is a bijection. If a, $b \in H$ then

$$\phi(\phi^{-1}(a)\phi^{-1}(b)) = \phi(\phi^{-1}(a)) \cdot \phi(\phi^{-1}(b)) = ab = \phi(\phi^{-1}(ab));$$

because ϕ is injective, $\phi^{-1}(a)\phi^{-1}(b) = \phi^{-1}(ab)$; as a and b are arbitrary, ϕ^{-1} is a homomorphism. Since it is also a bijection, it is an isomorphism.

Remark This proposition is not a happy accident. If it hadn't been true we would have changed the definition of 'isomorphism' until it was.

Proposition Isomorphism is an equivalence relation on the class of groups.

proof If G is any group, let $\iota : G \to G$ be the identity map. Then ι is an isomorphism from G to itself so $G \cong G$. Thus $\cong$ is reflexive.

If $G \cong H$, let $\phi : G \to H$ be an isomorphism. Then (by the last proposition) $\phi^{-1} : H \to G$ is an isomorphism, so $H \cong G$. Thus $\cong$ is symmetric.

If $G \cong H$ and $H \cong K$, let $\phi : G \to H$ and $\psi : H \to K$ be isomorphisms. Then $\psi\phi : G \to K$ is a composition of homomorphisms, so is a homomorphism, and is a composition of bijections, so is a bijection. Accordingly $\psi\phi$ is an isomorphism from G to K, and $G \cong K$. Thus $\cong$ is transitive.

Being reflexive, symmetric and transitive, $\cong$ is an equivalence relation.

Definition Let G and H be groups, and $\phi : G \to H$ a homomorphism. The **kernel** of ϕ is $\ker\phi = \{a : a \in G, \phi(a) = e_H\}$; the **image** of ϕ is $\phi[G] = \{\phi(x) : x \in G\}$.

Theorem Let G and H be groups, and $\phi : G \to H$ a homomorphism.
(a) The kernel of ϕ is a normal subgroup of G.
(b) The image of ϕ is a subgroup of H.

proof (a) Write K for the kernel of ϕ. Then $e_G \in K$ because $\phi(e_G) = e_H$. If x, $y \in K$, then

$$\phi(xy) = \phi(x)\phi(y) = e_H e_H = e_H,$$

so $xy \in K$. If $x \in K$, then

$$\phi(x^{-1}) = \phi(x)^{-1} = e_H^{-1} = e_H,$$

so $x^{-1} \in K$. Thus K is a subgroup of G. If $x \in G$ and $k \in K$ then

$$\phi(xkx^{-1}) = \phi(x)\phi(k)\phi(x^{-1}) = \phi(x) \cdot e_H \cdot \phi(x)^{-1} = \phi(x)\phi(x)^{-1} = e_H,$$

so $xkx^{-1} \in K$; as x and k are arbitrary, $K \lhd G$.

(b) $e_H \in \phi[G]$ because $e_H = \phi(e_G)$. If a, $b \in \phi[G]$ there are x, $y \in G$ such that $\phi(x) = a$ and $\phi(y) = b$; now

$$ab = \phi(x)\phi(y) = \phi(xy) \in \phi[G].$$

If $a \in \phi[G]$ there is an $x \in G$ such that $\phi(x) = a$, and now

$$a^{-1} = \phi(x)^{-1} = \phi(x^{-1}) \in \phi[G].$$

Thus $\phi[G]$ is a subgroup of G.

Proposition Let G and H be groups, and $\phi : G \to H$ a homomorphism. Then ϕ is injective iff $\ker\phi = \{e_G\}$.

proof (a) If ϕ is injective, then surely $e_G \in \ker\phi$. But also

$$x \in \ker\phi \Rightarrow \phi(x) = e_H = \phi(e_G) \Rightarrow x = e_G,$$

so $\ker\phi$ contains no other element and is $\{e_G\}$ exactly.

(b) If ϕ is not injective, let x, $y \in G$ be distinct elements such that $\phi(x) = \phi(y)$. Then

$$\phi(x^{-1}y) = \phi(x)^{-1}\phi(y) = \phi(y)^{-1}\phi(y) = e_H,$$

so $x^{-1}y \in \ker\phi$. But $x^{-1}y \neq e_G$ (because $xx^{-1}y = y \neq x = xe_G$, for instance), so $\ker\phi \neq \{e_G\}$.

The First Isomorphism Theorem Let G and H be groups, and $\phi : G \to H$ a homomorphism with kernel K. Then the quotient G/K is isomorphic to the image $\phi[G]$ of ϕ.

proof Note that because $K \lhd G$, we have a group G/K, and because $\phi[G] \leq H$, we can regard $\phi[G]$ as a group in its own right.

(a) (The key.) If x, $y \in G$, then $xK = yK$ iff $\phi(x) = \phi(y)$. **P** (i) If $xK = yK$, then $y = ye \in K$, so there is a $k \in K$ such that $y = xk$; now

$$\phi(y) = \phi(x)\phi(k) = \phi(x)e_H = \phi(x).$$

(ii) If $\phi(x) = \phi(y)$, then

$$\phi(x^{-1}y) = \phi(x)^{-1}\phi(y) = \phi(x)^{-1}\phi(x) = e_H,$$

and $x^{-1}y \in K$; accordingly $y = xx^{-1}y \in xK$ and $yK = xK$. **Q**

(b) We can therefore safely define a function $\psi : G/K \to \phi[G]$ by setting $\psi(xK) = \phi(x)$ for every $x \in G$.

If A, $B \in G/K$, there are x, $y \in G$ such that $A = xK$ and $B = yK$; now $AB = xyK$ so

$$\psi(AB) = \phi(xy) = \phi(x)\phi(y) = \psi(A)\psi(B).$$

Thus ψ is a homomorphism.

If A, $B \in G/K$ and $\psi(A) = \psi(B)$, there are x, $y \in G$ such that $A = xK$ and $B = yK$; now

$$\phi(x) = \psi(A) = \psi(B) = \phi(y)$$

so $A = B$ by (a) above. Thus ψ is injective.

If $a \in \phi[G]$ there is an $x \in G$ such that $a = \phi(x) = \psi(xK)$; thus $\psi : G/K \to H$ is surjective.

Putting these together, $\psi : G/K \to H$ is a bijective homomorphism, that is, an isomorphism.

Cyclic groups Let G be any group and $a \in G$. Define a^n inductively, for $n \in \mathbb{N}$, by setting $a^0 = e$, $a^{n+1} = a^n a$ for every $n \in \mathbb{N}$. (Thus $a^1 = ea = a$, $a^2 = a^1 a = aa$, $a^3 = a^2 a, \dots, a^{71} = a^{70}a, \dots$.) Now for integers $m \leq 0$, set $a^m = (a^{-1})^{-m}$. (Note that if $m = 0$, this definition gives $a^0 = (a^{-1})^0 = e$, as before.)

Proposition If G is a group and $a \in G$, $a^{m+n} = a^m a^n$ for all m, $n \in \mathbb{Z}$.

***proof (a)** $a^{-n+1} = a^{-n}a$ for every integer $n \geq 1$. **P** $-n+1 \leq 0$ and $n-1 \geq 0$ so

$$a^{-n}a = (a^{-1})^n a = (a^{-1})^{n-1}a^{-1}a = (a^{-1})^{n-1} = a^{-n+1}. \textbf{ Q}$$

Consequently $a^{m+1} = a^m a$ for every $m \in \mathbb{Z}$. **P** This is the definition of a^{m+1} if $m \geq 0$, and otherwise is covered by what I have just shown. **Q**

(b) $a^{m+n} = a^m a^n$ for all $m \in \mathbb{Z}$, $n \in \mathbb{N}$. **P** Induce on n. If $n = 0$ we have to show that $a^{m+0} = a^m a^0$, which is true, because $a^0 = e$. For the inductive step to $n+1$, we have

$$a^{m+(n+1)} = a^{(m+n)+1} = a^{m+n}a$$

(by (a))

$$= a^m a^n a$$

(by the inductive hypothesis)

$$= a^m a^{n+1}$$

by the definition of a^{n+1}. Thus the induction proceeds. **Q**

(c) $a^{-m} = (a^{-1})^m$ for every $m \in \mathbb{Z}$. **P** For $m \geq 0$, this is the definition of a^{-m}. For $m < 0$, say $m = -n$ where $n \in \mathbb{N}$, we have

$$(a^{-1})^m = (a^{-1})^{-n} = ((a^{-1})^{-1})^n = a^n. \textbf{ Q}$$

(d) $a^{m+n} = a^m a^n$ for all m, $n \in \mathbb{Z}$. **P** If $n \geq 0$ this is in (b). If $n < 0$, then

$a^m a^n = (a^{-1})^{-m}(a^{-1})^{-n}$

(by (c))

$= (a^{-1})^{-m-n}$

(by (b), because $-n \geq 0$)

$= a^{m+n}$

by (c) again. **Q** So the proof is complete.

Remark What this says is that the map $n \mapsto a^n : \mathbb{Z} \to G$ is a homomorphism between the groups $(\mathbb{Z}, +)$ and $(G, \cdot)$. Its image $\{a^n : n \in \mathbb{Z}\}$ is therefore a subgroup of G (the **cyclic subgroup generated by** a, sometimes written $< a >$), and its kernel $K = \{n : a^n = e\}$ is a (normal) subgroup of $\mathbb{Z}$. (Of course all subgroups of $\mathbb{Z}$ are normal, because $\mathbb{Z}$ is abelian.) Moreover, $< a > \cong \mathbb{Z}/K$, by the First Isomorphism Theorem.

Subgroups of $\mathbb{Z}$: Proposition A subset K of $\mathbb{Z}$ is a subgroup iff it is of the form $n\mathbb{Z} = \{mn : m \in \mathbb{Z}\}$ for some $n \in \mathbb{N}$.

proof (a) For any $n \in \mathbb{Z}$, the map $m \mapsto mn : \mathbb{Z} \to \mathbb{Z}$ is a homomorphism (because $(m + m')n = mn + m'n$ for all m, m'), so its image $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

(b) Suppose that $K \leq \mathbb{Z}$ is a subgroup.

case (i) If $K = \{0\}$ then $K = 0\mathbb{Z}$ is of the required form.

case (ii) Otherwise, there is a non-zero $k_0 \in K$. Now $-k_0$ is the inverse of k_0 in the group $(\mathbb{Z}, +)$, so also belongs to K, and one of k_0, $-k_0$ is greater than 0; so K contains some strictly positive integer. Let n be the *least* member of $K \cap \mathbb{N} \setminus \{0\}$. Then $mn \in K$ for every $m \in \mathbb{N}$ (induce on m). If $k \in K \cap \mathbb{N}$, then k is expressible as $mn + j$ where $m \in \mathbb{N}$ and $0 \leq j < n$; in this case, mn and $-mn$ belong to K, so $j = k + (-mn)$ belongs to K. Since n is the least strictly positive member of K, j must be 0, and $k = mn$. This shows that $K \cap \mathbb{N} = n\mathbb{N}$ is the set of non-negative members of $n\mathbb{Z}$. Of course we now see that, for $k < 0$,

$$k \in K \iff -k \in K \iff -k \in n\mathbb{N} \iff k \in n\mathbb{Z}.$$

So $K = n\mathbb{Z}$ exactly.

The quotients $\mathbb{Z}/n\mathbb{Z}$ If $n = 0$, then the cosets of $n\mathbb{Z} = \{0\}$ are just the singletons $\{m\}$ for $m \in \mathbb{Z}$; the quotient map from $\mathbb{Z}$ onto $\mathbb{Z}/\{0\}$ is bijective, and is an isomorphism between $\mathbb{Z}$ and $\mathbb{Z}/\{0\}$.

If $n \in \mathbb{N}$ is strictly positive, then $K = n\mathbb{Z}$ has exactly n cosets $K, 1 + K, 2 + K, \dots, (n-1) + K$, because every element of $\mathbb{Z}$ is expressible as $mn + j$ for some $j \in \mathbb{Z}_n = \{0, 1, \dots, n-1\}$. The group operation on $\mathbb{Z}/n\mathbb{Z}$ is defined by

$$(i + K) + (j + K) = (i + j) + K \text{ for } i,\ j \in \mathbb{Z}.$$

If i, $j \in \mathbb{Z}_n$, then we might have $i + j \geq n$; but in this case $i + j - n \in \mathbb{Z}_n$ and $(i + j - n) + K = (i + j) + K$. We can therefore identify the group $\mathbb{Z}/n\mathbb{Z}$ with $(\mathbb{Z}_n, +_n)$ where $+_n$ is 'addition modulo n', that is,

$$\begin{aligned} i +_n j &= i + j \text{ if } i + j < n, \\ &= i + j - n \text{ otherwise.} \end{aligned}$$

Returning to the case of a general group G and an element a of G, the cyclic subgroup $< a > = \{a^m : m \in \mathbb{Z}\}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$, and this in turn is either isomorphic to $\mathbb{Z}$ (if the homomorphism $m \mapsto a^m$ is injective) or to $(\mathbb{Z}_n, +_n)$ (if n is the least strictly positive integer belonging to the kernel of the homomorphism, that is, such that $a^m = e$.) Moreover, we can find out which, because if $< a >$ is infinite it must be isomorphic to $\mathbb{Z}$, and if it has n members it must be isomorphic to $\mathbb{Z}_n$. Of course $\mathbb{Z}_1 = \{0\}$ is the trivial group; this is what we get if $a = e$, $< a > = \{e\}$.

Definition If G is a group, the **order** of an element a of G is $\#(< a >)$.

Remarks If the order of a is $n \in \mathbb{N}$, then n is the least integer (greater than 0) such that $a^n = e$, and $< a > \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$; if the order of a is infinite, then $< a > \cong \mathbb{Z}$.

Permutation Groups

Theorem If X is any set, the set of bijections from X to X is a group under composition of functions.

proof It is the group of invertible elements of the semigroup of all functions from X to itself.

Definitions For $n \geq 1$, I will write S_n for the group of all bijections from $\{1, 2, \dots, n\}$ to itself.

For distinct $i_1, \dots, i_k \leq n$, $(\overleftarrow{i_1\, i_2\, \dots\, i_k})$ will be the permutation $\rho \in S_n$ defined by saying that

$\rho(i_1) = i_2,\ \rho(i_2) = i_3, \ldots, \rho(i_{k-1}) = i_k,\ \rho(i_k) = i_1$
and $\rho(j) = j$ for all other $j \leq n$.

We say that two cycles $(\overleftarrow{i_1 \ldots i_k})$ and $(\overleftarrow{j_1 \ldots j_l})$ are **disjoint** if $i_r \neq j_s$ for $r \leq k$, $s \leq l$; that is, if all the numbers moved by one of the cycles is left alone by the other.

Remark Permutations are functions. So when we multiply two cycles together, say $\rho = (\overleftarrow{1234})$ and $\sigma = (\overleftarrow{2345})$, then

$(\overleftarrow{1234})(\overleftarrow{2345})(1) = (\rho\sigma)(1) = \rho(\sigma(1)) = \rho(1) = 2,$
$(\overleftarrow{1234})(\overleftarrow{2345})(2) = (\rho\sigma)(2) = \rho(\sigma(2)) = \rho(3) = 4,$
$(\overleftarrow{1234})(\overleftarrow{2345})(3) = (\rho\sigma)(3) = \rho(\sigma(3)) = \rho(4) = 1,$
$(\overleftarrow{1234})(\overleftarrow{2345})(4) = (\rho\sigma)(4) = \rho(\sigma(4)) = \rho(5) = 5,$
$(\overleftarrow{1234})(\overleftarrow{2345})(5) = (\rho\sigma)(5) = \rho(\sigma(5)) = \rho(2) = 3.$

So

$$(\overleftarrow{1234})(\overleftarrow{2345}) = (\overleftarrow{12453}).$$

Theorem Any permutation in S_n can be expressed as a product of disjoint cycles. The expression is unique except that

(i) you may write the cycles in any order

$[(\overleftarrow{123})(\overleftarrow{45}) = (\overleftarrow{45})(\overleftarrow{123})]$

(ii) you may start a cycle at any point of the cycle

$[(\overleftarrow{1234}) = (\overleftarrow{2341}) = (\overleftarrow{3412})]$

(iii) you may include one-cycles $(\overleftarrow{i})$ or omit them as you like

[$(\overleftarrow{1})$ is the identity permutation.]

The order of a permutation A cycle $\rho = (\overleftarrow{i_1 \ldots i_k})$ moves the numbers $i_1 \ldots i_k$ in a circle; it will take just k moves to get them back to their original positions, so the order of ρ is k.

If we have expressed a permutation ρ as a product $\rho_1\rho_2 \ldots \rho_r$ of disjoint cycles, then each of the ρ_j is acting independently on a set with k_j elements, where k_j is the order of ρ_j. Now a power ρ^n of ρ will get the elements of the jth cycle back into their places iff n is a multiple of k_j. So we shall have everything right iff n is a multiple of every k_j, that is, n is a multiple of the least common multiple of all the k_j; the order of ρ is the l.c.m. of the orders of its disjoint cycles.

Example The order of

$$(\overleftarrow{1\,2})(\overleftarrow{3\,4\,5})(\overleftarrow{6\,7\,8\,9})(\overleftarrow{10\,11\,12\,13\,14\,15})$$

is lcm(2,3,4,6)=12.

Inverses For any cycle we can find its inverse by just writing it backwards: $(\overleftarrow{1234})^{-1} = (\overleftarrow{4321})$. For a product of cycles the same rule applies:

$$((\overleftarrow{123})(\overleftarrow{234})(\overleftarrow{345}))^{-1} = (\overleftarrow{345})^{-1}(\overleftarrow{234})^{-1}(\overleftarrow{123})^{-1} = (\overleftarrow{543})(\overleftarrow{432})(\overleftarrow{321}).$$

(It doesn't matter here whether the cycles are disjoint or not; but if they aren't disjoint then we must make sure to write them in the correct order.)

Definition A **transposition** is a 2-cycle, that is, a permutation of the form $(\overleftarrow{ij})$ exchanging two numbers i and j and leaving everything else unmoved.

Proposition Any permutation in S_n can be expressed as a product of transpositions (counting the identity as a product of no transpositions).

proof Observe that any cycle of length $k \geq 2$ is a product of $k-1$ transpositions; e.g.,

$$(\overleftarrow{123 \ldots k}) = (\overleftarrow{1k})(\overleftarrow{1\ k\text{-}1}) \ldots (\overleftarrow{13})(\overleftarrow{12}).$$

Now any permutation is a product of cycles (counting e as a product of no cycles) and therefore a product of transpositions.

The signature of a permutation Let $n \geq 1$ be an integer, and $\rho \in S_n$ a permutation. Write $c(\rho)$ for the number of cycles in the disjoint-cycle representation of ρ, counting one-cycles.

Thus if $n = 6$ and $\rho = (\overleftarrow{123})(\overleftarrow{45})$, $c(\rho) = 3$, because we must count the one-cycle $(\overleftarrow{6})$ as part of the representation of ρ.
Now we say that ρ is **even**, with **signature** $\epsilon_\rho = (-1)^{n-c(\rho)} = 1$, if $n - c(\rho)$ is even, and otherwise we say that ρ is **odd**, with signature $\epsilon_\rho = (-1)^{n-c(\rho)} = -1$.

Remark Note that if we interpret $(\overleftarrow{12})(\overleftarrow{34})$ as a member of S_4, then its signature is $(-1)^{4-2} = 1$; while if we interpret it as a member of S_5, we have to re-write it as $(\overleftarrow{12})(\overleftarrow{34})(\overleftarrow{5})$, so that its signature is $(-1)^{5-3}$ is still 1. This is an *even* permutation whichever S_n we think of it as belonging to.

Lemma If $\tau \in S_n$ is a transposition, then $\epsilon_{\tau\rho} = -\epsilon_\rho$ for any $\rho \in S_n$.

proof Start by expressing ρ as a product of disjoint cycles, including one-cycles if necessary. Suppose that $\tau = (\overleftarrow{ij})$ where $i, j \leq n$ are distinct.

case 1 Suppose that i and j belong to different cycles of ρ. Since we can write the cycles in any order, we can put the one containing i at the left-hand end of the product, and the one containing j next to it; and since we can start any cycle at any point, we can suppose that these cycles are written $(\overleftarrow{i\ldots})$ and $(\overleftarrow{j\ldots})$, so that

$$\rho = (\overleftarrow{i\ldots})(\overleftarrow{j\ldots})(\overleftarrow{\cdots})\ldots(\overleftarrow{\cdots})$$

(of course one or more of the strings suggested by $\ldots$ might be empty; if $\rho(i) = i$, then the leading cycle is just $(\overleftarrow{i})$). In this case,

$$\begin{aligned}\tau\rho &= (\overleftarrow{ij})(\overleftarrow{i\ldots})(\overleftarrow{j\ldots})(\overleftarrow{\cdots})\ldots(\overleftarrow{\cdots})\\ &= (\overleftarrow{i\ldots j\ldots})(\overleftarrow{j\ldots})(\overleftarrow{\cdots})\ldots(\overleftarrow{\cdots}),\end{aligned}$$

so that $c(\tau\rho) = c(\rho) - 1$ and $\epsilon_{\tau\rho} = -\epsilon_\rho$.

Maybe this step will be more convincing with a couple of examples:

$$(\overleftarrow{12})(\overleftarrow{1345})(\overleftarrow{267})(\overleftarrow{89}) = (\overleftarrow{1345267})(\overleftarrow{89}),$$

$$(\overleftarrow{12})(\overleftarrow{1345})(\overleftarrow{2})(\overleftarrow{789}) = (\overleftarrow{13452})(\overleftarrow{789}).$$

case 2 If i and j belong to the same cycle as ρ, bring it to the left-hand end of the product forming ρ and start it at i, so that

$$\rho = (\overleftarrow{i\ldots j\ldots})(\overleftarrow{\cdots})\ldots(\overleftarrow{\cdots})$$

and

$$\begin{aligned}\tau\rho &= (\overleftarrow{ij})(\overleftarrow{i\ldots j\ldots})(\overleftarrow{\cdots})\ldots(\overleftarrow{\cdots})\\ &= (\overleftarrow{i\ldots})(\overleftarrow{j\ldots})(\overleftarrow{\cdots})\ldots(\overleftarrow{\cdots})\end{aligned}$$

has $c(\tau\rho) = c(\rho) + 1$, so that once again ρ and $\tau\rho$ have opposite parity and $\epsilon_{\tau\rho} = -\epsilon_\rho$.

Examples:

$$(\overleftarrow{12})(\overleftarrow{13425})(\overleftarrow{6789}) = (\overleftarrow{134})(\overleftarrow{25})(\overleftarrow{6789}),$$

$$(\overleftarrow{12})(\overleftarrow{12345}) = (\overleftarrow{1})(\overleftarrow{2345}).$$

Theorem Suppose that $n \geq 1$.
(a) $\rho \in S_n$ is even/odd iff it can be expressed as the product of an even/odd number of transpositions.
(b) $\epsilon_{\rho\sigma} = \epsilon_\rho\epsilon_\sigma$ for all $\rho, \sigma \in S_n$.

proof (a) Note first that $e = (\overleftarrow{1})(\overleftarrow{2})\ldots(\overleftarrow{n})$ has $c(e) = n$ so that $\epsilon_e = (-1)^{n-n} = 1$. Next, any ρ can certainly be expressed as a product $\tau_k\tau_{k-1}\ldots\tau_2\tau_1$ where every τ_j is a transposition, allowing the case $\rho = e$, $k = 0$. In this case,

$\epsilon_e = 1$,
$\epsilon\tau_1 = \epsilon_{\tau_1 e} = -\epsilon_e = -1$,
$\epsilon\tau_2\tau_1 = -\epsilon_{\tau_1} = -(-1) = (-1)^2 = 1$,
$\epsilon\tau_3\tau_2\tau_1 = -\epsilon_{\tau_2\tau_1} = (-1)^3 = -1$,
$\ldots$
$\epsilon\tau_k \ldots \tau_3\tau_2\tau_1 = (-1)^k = 1$ if k is even, -1 if k is odd.

(b) Now if $\rho = \tau_1\tau_2 \ldots \tau_k$ and $\sigma = \tau_1'\tau_2' \ldots \tau_l'$, where all the τ_i, τ_j' are transpositions, $\rho\sigma = \tau_1 \ldots \tau_k\tau_1' \ldots \tau_l'$ is the product of $k + l$ transpositions, so that

$$\epsilon_{\rho\sigma} = (-1)^{k+l} = (-1)^k(-1)^l = \epsilon_\rho\epsilon_\sigma.$$

The group of even permutations The formula '$\epsilon_{\rho\sigma} = \epsilon_\rho\epsilon_\sigma$' can be interpreted as saying: $\epsilon : S_n \to \{-1, 1\}$ is a homomorphism, if $\{-1, 1\}$ is regarded as a group under multiplication (a subgroup of $(\mathbb{R}\setminus\{0\}, \times)$, or the group of invertible elements of the semigroup $(\mathbb{Z}, \times)$). Its kernel is A_n, the group of even permutations, which is therefore a normal subgroup of S_n. Except in the case $n = 1$ (in which case $S_1 = \{e\} = A_1$ has just one element), there is a transposition $\tau = (\overleftarrow{12})$, so that $\epsilon : S_n \to \{-1, 1\}$ is surjective and $S_n/A_n \cong \{-1, 1\}$ (by the First Isomorphism Theorem). In particular, A_n has just two cosets, itself and its complement, and $\#(A_n) = \frac{1}{2}\#(S_n) = \frac{n!}{2}$.

Normal subgroups of A_n and S_n It is a very remarkable fact that A_n and S_n have very few normal subgroups. Actually

the normal subgroups of A_n are exactly $\{e\}$ and A_n itself, except when $n = 4$, in which case $K = \{e, (\overleftarrow{12})(\overleftarrow{34}), (\overleftarrow{13})(\overleftarrow{24}), (\overleftarrow{14})(\overleftarrow{23})\}$ is a normal subgroup of A_4;

the normal subgroups of S_n are $\{e\}$, A_n and S_n itself, except when $n = 4$, in which case $K = \{e, (\overleftarrow{12})(\overleftarrow{34}), (\overleftarrow{13})(\overleftarrow{24}), (\overleftarrow{14})(\overleftarrow{23})\}$ is a normal subgroup of S_4.

The proof of this is long but very instructive. I will break it up into a string of lemmas; most of these have non-trivial ideas in them, but will I hope still be manageable, if you can remember the order they come in.

The first result is actually a bit more than a 'lemma'. Since we are talking about normal subgroups of S_n and A_n, we are repeatedly going to want to look at expressions of the form $\rho\sigma\rho^{-1}$ where ρ, $\sigma \in S_n$. Now when σ is a cycle, this can be calculated particularly easily, as follows.

Proposition If $\sigma = (\overleftarrow{i_1\, i_2 \ldots i_k})$ is a simple cycle in S_n, and $\rho \in S_n$, then $\rho\sigma\rho^{-1}$ is the cycle $(\overleftarrow{\rho(i_1)\, \rho(i_2) \ldots \rho(i_k)})$.

proof Really this is just a direct calculation. If $i \leq n$ is of the form $\rho(i_j)$ where $j \leq k$ then

$$\begin{aligned}\rho\sigma\rho^{-1}(i) = \rho\sigma(i_j) &= \rho(i_{j+1}) \text{ if } j < k,\\ &= \rho(i_1) \text{ if } j = k,\end{aligned}$$

and in either case is equal to $(\overleftarrow{\rho(i_1)\, \rho(i_2) \ldots \rho(i_k)})(i_j)$. While for any other $i \leq n$, $\rho^{-1}(i) \neq i_j$ for every j, so $\sigma\rho^{-1}(i) = \rho^{-1}(i)$ and

$$\rho\sigma\rho^{-1}(i) = \rho\rho^{-1}(i) = i = (\overleftarrow{\rho(i_1)\, \rho(i_2) \ldots \rho(i_k)})(i).$$

Remark It will be particularly important later in the course to know that if σ is a cycle, then $\rho\sigma\rho^{-1}$ is a cycle of the same length.

The formula aba^{-1} is going to be one of the recurrent themes of this course, and it is helpful to have a word for it. If G is any group, then we say that x, $y \in G$ are **conjugate** in G if there is an $a \in G$ such that $axa^{-1} = y$. Later on I will introduce this notion properly. For the moment, note only that if $\sigma \in S_n$ is a cycle, then any conjugate of σ in S_n is a cycle of the same length.

Theorem (part 1) For any $n \geq 1$, $\{e\}$, A_n and S_n are normal subgroups of S_n, and $\{e\}$ and A_n are normal subgroups of A_n. Moreover, K is a normal subgroup of A_4 and K_4.

proof In any group G, $\{e\}$ and G are normal subgroups of G; and $A_n \triangleleft S_n$ because it is the kernel of the homomorphism $\rho \mapsto \epsilon_\rho : S_n \to \{-1, 1\}$.

To see that $K = \{e, (\overleftarrow{12})(\overleftarrow{34}), (\overleftarrow{13})(\overleftarrow{24}), (\overleftarrow{14})(\overleftarrow{23})\}$ is a normal subgroup of S_4, the first step is to check that it is a subgroup. Obviously it contains e, and it is easy to see that every element of K is self-inverse, so K contains the inverses of all its elements. To see that K is closed under multiplication, the most straightforward method is just to calculate all the products, e.g.,

$$(\overleftarrow{12})(\overleftarrow{34})(\overleftarrow{13})(\overleftarrow{24}) = (\overleftarrow{14})(\overleftarrow{23}).$$

The product of any two of the non-identity elements of K is the third.

To see that K is a normal subgroup, let $\sigma \in S_4$, $\rho \in K$ and examine $\sigma\rho\sigma^{-1}$. If $\rho = e$ then of course $\sigma\rho\sigma^{-1} = e \in K$. Otherwise, ρ is of the form $(\overleftarrow{ij})(\overleftarrow{kl})$ where i, j, k, l are all different. So

$$\begin{aligned}\sigma\rho\sigma^{-1} &= \sigma(\overleftarrow{ij})(\overleftarrow{kl})\sigma^{-1}\\ &= \sigma(\overleftarrow{ij})\sigma^{-1}\sigma(\overleftarrow{kl})\sigma^{-1} = (\overleftarrow{\sigma(i)\,\sigma(j)})(\overleftarrow{\sigma(k)\,\sigma(l)})\end{aligned}$$

is another product of disjoint transpositions. But now observe that a product of disjoint transpositions in S_4 is fully determined as soon as we know what 1 is swapped with, so there are only three of them, and all belong to K. So in this case also $\sigma\rho\sigma^{-1} \in K$. As ρ and σ are arbitrary, $K \lhd S_4$.

Since $K \subseteq A_4$, it follows at once that K is also a normal subgroup of A_4.

This is of course the easy part. What we now need to do is to show that there are no other normal subgroups. I begin with an elementary, but not obvious, fact about normal subgroups in general.

Proposition Let G be a group and H a normal subgroup of G. Then $hah^{-1}a^{-1} \in H$ for every $a \in G$, $h \in H$.

proof $h^{-1} \in H$ because H is closed under inversion; $ah^{-1}a^{-1} \in H$ because H is a normal subgroup; and $hah^{-1}a^{-1} \in H$ because H is closed under multiplication.

Remark The expression $hah^{-1}a^{-1} = (ha)(ah)^{-1}$ is called a 'commutator'. If $ah = ha$ then it is equal to the identity; the 'commutators' of a group give us information on 'how non-abelian' it is. We shall not in this course have time to look at them properly, but they are of very great importance in the more advanced theory.

I now give the pair of key facts on which the analysis of normal subgroups of A_4 depends.

Key Lemma Let $n \geq 1$.
(a) Every member of A_n can be expressed as a product of 3-cycles (counting e as a product of no 3-cycles).
(b) If $H \lhd A_n$ and H contains any 3-cycle, then $H = A_n$.

proof (a)(i) The point is that any product $\tau_1\tau_2$ of two transpositions is a product of 3-cycles. **P** We have to look at the possible cases. (i) If $\tau_1 = \tau_2$ then the product is e, which we are counting as a product of 3-cycles. (ii) If τ_1 and τ_2 are disjoint, express them as $(\overleftarrow{ij})$ and $(\overleftarrow{kl})$ where i, j, k, l are all different; then

$$\tau_1\tau_2 = (\overleftarrow{ij})(\overleftarrow{kl}) = (\overleftarrow{kil})(\overleftarrow{ijk})$$

is a product of two 3-cycles. (iii) Otherwise, the cycles of τ_1 and τ_2 must overlap at just one point i say. Putting this at the beginning of both, we have $\tau_1 = (\overleftarrow{ij})$ and $\tau_2 = (\overleftarrow{ik})$ where i, j and k are different. But in this case

$$\tau_1\tau_2 = (\overleftarrow{ij})(\overleftarrow{ik}) = (\overleftarrow{ikj})$$

is a 3-cycle. So we have an appropriate expression in every case. **Q**

(ii) Now any even permutation ρ is either e (which we are counting as a product of 3-cycles) or is of the form $\rho = \tau_1\tau_2\ldots\tau_{2r}$ where $\tau_1, \ldots, \tau_{2r}$ are transpositions. But each of the products $\rho_1 = \tau_1\tau_2$, $\rho_2 = \tau_3\tau_4, \ldots, \rho_r = \tau_{2r-1}, \tau_{2r}$ is a product of 3-cycles, so $\rho = \rho_1\rho_2\ldots\rho_r$ is also a product of 3-cycles.

(b) Note first that if H contains the 3-cycle $(\overleftarrow{ijk}) = (\overleftarrow{kij}) = (\overleftarrow{jki})$ then it contains its inverse $(\overleftarrow{kji}) = (\overleftarrow{jik}) = (\overleftarrow{ikj})$. Next, if H contains the 3-cycle $(\overleftarrow{ijk})$, and $l \leq n$ is distinct from i, j and k, then H contains $(\overleftarrow{ijl})$. **P** We know that $(\overleftarrow{ijl}) \in A_n$, so H contains

$$\begin{aligned}(\overleftarrow{ijk})(\overleftarrow{ijl})(\overleftarrow{ijk})(\overleftarrow{ijl})^{-1} &= (\overleftarrow{ijk})(\overleftarrow{ijl})(\overleftarrow{ijk})(\overleftarrow{lji}) \\ &= (\overleftarrow{ijl}).\ \mathbf{Q}\end{aligned}$$

What this means is that if we have two 3-cycles ρ and ρ', and if they overlap at two points, and H contains one of them, it must contain the other. But now, if ρ and ρ' are 3-cycles overlapping at one point, say $\rho = (\overleftarrow{ijk})$ and $\rho' = (\overleftarrow{ilm})$, and $\rho \in H$, then H contains $(\overleftarrow{ijl})$ and therefore also contains ρ', since $(\overleftarrow{ilm})$ and $(\overleftarrow{ijl})$ overlap in two points. Finally, if ρ and ρ' are disjoint 3-cycles, there is a 3-cycle ρ'' overlapping both, so that if $\rho \in H$ then $\rho'' \in H$ and $\rho' \in H$.

Putting these together, we see that if H contains any 3-cycle it contains every 3-cycle, and therefore every product of 3-cycles. But this means that $H = A_n$, by (a).

We are now ready for the assault on normal subgroups of A_n.

Theorem If $n \geq 1$ and $H \lhd A_n$, then either $H = \{e\}$ or $H = A_n$ or $n = 4$ and $H = K$.

proof The idea is to work systematically through the possible cases. Each individually is not particularly difficult if we keep hold of a couple of tricks and get them in the right order.

case 1 If H contains a 3-cycle, then $H = A_n$. **P** This is just (b) of the Key Lemma. **Q**

case 2 If H contains a permutation ρ for which the disjoint-cycle representation has a cycle of length 4 or more, then $H = A_n$. **P** Suppose that one of the cycles of ρ is $(\overleftarrow{i_1\,i_2\,i_3 \dots i_k})$ where $k \geq 4$. Then $\sigma = (\overleftarrow{i_1\,i_2\,i_3}) \in A_n$, so H contains

$$\begin{aligned}\rho\sigma\rho^{-1}\sigma^{-1} &= (\overleftarrow{\rho(i_1)\,\rho(i_2)\,\rho(i_3)})(\overleftarrow{i_3\,i_2\,i_1}) \\ &= (\overleftarrow{i_2\,i_3\,i_4})(\overleftarrow{i_3\,i_2\,i_1}) = (\overleftarrow{i_1\,i_4\,i_2}).\end{aligned}$$

But now we have a 3-cycle in H, so $H = A_n$, by case 1. **Q**

case 3 If H contains a permutation ρ which is not a simple 3-cycle, but has a cycle of length 3 in its disjoint-cycle representation, then $H = A_n$. **P** Suppose that $(\overleftarrow{i_1\,i_2\,i_3})$ and $(\overleftarrow{i_4 \dots i_k})$ are two of the cycles in the disjoint-cycle representation of ρ, where $k \geq 5$. Then $\sigma = (\overleftarrow{i_1\,i_2\,i_4}) \in A_n$, so H contains

$$\begin{aligned}\rho\sigma\rho^{-1}\sigma^{-1} &= (\overleftarrow{\rho(i_1)\,\rho(i_2)\,\rho(i_4)})(\overleftarrow{i_4\,i_2\,i_1}) \\ &= (\overleftarrow{i_2\,i_3\,i_5})(\overleftarrow{i_4\,i_2\,i_1}) \\ &= (\overleftarrow{i_1\,i_4\,i_3\,i_5\,i_2}).\end{aligned}$$

Thus H contains a 5-cycle and must be equal to A_n, by case 2. **Q**

case 4 Suppose that H contains a permutation ρ which has three or more transpositions in its disjoint-cycle representation. Then $H = A_n$. **P** Suppose that the disjoint-cycle representation of ρ has the cycles $(\overleftarrow{i_1\,i_2})$, $(\overleftarrow{i_3\,i_4})$ and $(\overleftarrow{i_5\,i_6})$. Then $\sigma = (\overleftarrow{i_1\,i_3\,i_6}) \in A_n$ so H contains

$$\begin{aligned}\rho\sigma\rho^{-1}\sigma^{-1} &= (\overleftarrow{\rho(i_1)\,\rho(i_3)\,\rho(i_5)})(\overleftarrow{i_5\,i_3\,i_1}) \\ &= (\overleftarrow{i_2\,i_4\,i_6})(\overleftarrow{i_5\,i_3\,i_1})\end{aligned}$$

which is a product of disjoint 3-cycles; by case 3, $H = A_n$. **Q**

case 5 Suppose that $n \neq 4$ and that H contains a permutation ρ of the form $(\overleftarrow{i_1\,i_2})(\overleftarrow{i_3\,i_4})$ where $i_1, \dots, i_4$ are all different. Then $H = A_n$. **P** Since $i_1, \dots, i_4$ are different, n must be at least 4 and is actually greater than 4. So there is a $j \leq n$ which is different from any of $i_1, \dots, i_4$, and $\sigma = (\overleftarrow{i_1\,i_3\,j}) \in A_n$. Accordingly H contains

$$\begin{aligned}\rho\sigma\rho^{-1}\sigma^{-1} &= (\overleftarrow{\rho(i_1)\,\rho(i_3)\,\rho(j)})(\overleftarrow{j\,i_3\,i_1}) \\ &= (\overleftarrow{i_2\,i_4\,j})(\overleftarrow{j\,i_3\,i_1}) = (\overleftarrow{i_1\,i_2\,i_4\,j\,i_3})\end{aligned}$$

and $H = A_n$ by case 2.

The case $n \neq 4$ If $n \neq 4$ and $H \neq \{e\}$, then H must contain some $\rho \neq e$, and because ρ cannot be a transposition we are in one of the cases 1-5, so that $H = A_n$. Thus if $n \neq 4$ the only normal subgroups of A_n are $\{e\}$ and A_n.

For $n = 4$ there is a final case to consider.

case 6 Suppose that $n = 4$ and that H is neither $\{e\}$ nor A_4. Then $H = K$. **P** By case 1, H cannot contain any 3-cycle; since the only elements of A_4 are 3-cycles and double transpositions and the identity, $H \subseteq K$ and H is a subgroup of K. Since $H \neq \{e\}$, it does contain a double transposition $\rho = (\overleftarrow{ij})(\overleftarrow{kl})$ say. Now $\sigma = (\overleftarrow{ijk}) \in A_n$, so H contains

$$\begin{aligned}\rho\sigma\rho^{-1}\sigma^{-1} &= (\overleftarrow{\rho(i)\,\rho(j)\,\rho(k)})(\overleftarrow{kji}) \\ &= (\overleftarrow{jil})(\overleftarrow{kji}) = (\overleftarrow{ik})(\overleftarrow{jl}).\end{aligned}$$

Now this means that H is a subgroup of K with at least members. By Lagrange's theorem, H must be the whole of K. **Q**

So the only normal subgroups of A_4 are $\{e\}$, K and A_4. This completes the proof.

Remark A group G for which the only normal subgroups are $\{e\}$ and G is called **simple**. (This is typical mathspeak. Actually, 'simple' groups are particularly complex for their size, unless they happen to be abelian.) Thus A_n is simple for every $n \neq 4$. A_1 and A_2 are trivial (being the identity alone) and $A_3 = \{e, (\overleftarrow{123}), (\overleftarrow{132})\} \cong \mathbb{Z}_3$ really is simple in every sense. But A_5 is very interesting indeed; I will return to it in the next chapter.

It is an astonishing fact that we have a complete list of finite simple groups (I mean, we have a list of simple groups such that every finite simple group is isomorphic to just one group on the list). The construction of the list was one of the great triumphs of the period 1960-1985. Even odder, the list is made up of five(?) infinite series (two of which are the A_n, for $n \geq 5$, and the $\mathbb{Z}_n$, for n prime; the latter are the only abelian simple groups, apart from $\{e\}$) and twenty-two(?) 'sporadic' groups, of which the largest has (?) members.

Now let us look for the normal subgroups of S_n. Another simple general fact will be useful.

Proposition Let G be a group and H, A two subgroups of G.
(a) $H \cap A$ is a subgroup of G and of A.
(b) If $H \lhd G$ then $H \cap A \lhd A$.

proof (a) $e \in H$ and $e \in A$ so $e \in H \cap A$.

If $x, y \in H \cap A$, then $xy \in H$ and $xy \in A$ so $xy \in H \cap A$.

If $x \in H \cap A$ then $x^{-1} \in H$ and $x^{-1} \in A$ so $x^{-1} \in H \cap A$.

This shows that $H \cap A$ is a subgroup of G. If we think of A as a group in its own right, the same argument shows that $H \cap A$ is a subgroup of A.

(b) If $H \lhd G$, then for any $x \in H \cap A$, $a \in A$ we have

$$axa^{-1} \in H \text{ because } a \in G,\ x \in H \text{ and } H \lhd G,$$

$$axa^{-1} \in A \text{ because } a,\ x \in A \text{ and } A \leq G.$$

So $axa^{-1} \in H \cap A$; as a and x are arbitrary, $H \cap A \lhd A$.

Theorem If $H \lhd S_n$ then H must be either $\{e\}$ or A_n or S_n or (if $n = 4$) K.

proof As in the corresponding theorem for A_n, the main part of the work will involve looking at the structure of possible elements of $H \setminus \{e\}$. But it will be helpful to begin by noting that $H \cap A_n$ is a normal subgroup of A_n (by the Proposition just above) so is either $\{e\}$ of A_n or (if $n = 4$) K. Next, if $H \cap A_n = A_n$, then H must be equal to either A_n or S_n. **P** We have $A_n \subseteq H \subseteq S_n$ so

$$\tfrac{n!}{2} = \#(A_n) \leq \#(H) \leq \#(S_n) = n!.$$

But Lagrange's theorem tells us that $\#(H)$ is a factor of $\#(S_n)$, so it must be equal to either $\#(S_n)$ or to $\frac{1}{2}\#(S_n)$; that is, H must be either S_n or A_n. **Q**

Now we can start looking at possible cases.

case 1 If H contains a permutation ρ for which the disjoint-cycle representation has a cycle of length 3 or more, then $H = A_n$ or $H = S_n$. **P** Suppose that one of the cycles of ρ is $(\overleftarrow{i_1\, i_2 \ldots i_k})$ where $k \geq 3$. Then $\sigma = (\overleftarrow{i_1\, i_2}) \in S_n$, so H contains

$$\begin{aligned}\rho\sigma\rho^{-1}\sigma^{-1} &= (\overleftarrow{\rho(i_1)\, \rho(i_2)})(\overleftarrow{i_2\, i_1}) \\ &= (\overleftarrow{i_2\, i_3})(\overleftarrow{i_2\, i_1}) = (\overleftarrow{i_1\, i_3\, i_2}).\end{aligned}$$

But now we have a 3-cycle in $H \cap A_n$, so $H \cap A_n = A_n$, by the Key Lemma, and H is either A_n or S_n. **Q**

case 2 Suppose that H contains a permutation ρ which has three or more transpositions in its disjoint-cycle representation. Then $H = A_n$ or $H = S_n$. **P** Suppose that the disjoint-cycle representation of ρ has the cycles $(\overleftarrow{i_1\, i_2})$, $(\overleftarrow{i_3\, i_4})$ and $(\overleftarrow{i_5\, i_6})$. Then $\sigma = (\overleftarrow{i_1\, i_3\, i_6}) \in S_n$ so H contains

$$\begin{aligned}\rho\sigma\rho^{-1}\sigma^{-1} &= (\overleftarrow{\rho(i_1)\, \rho(i_3)\, \rho(i_5)})(\overleftarrow{i_5\, i_3\, i_1}) \\ &= (\overleftarrow{i_2\, i_4\, i_6})(\overleftarrow{i_5\, i_3\, i_1})\end{aligned}$$

which is a product of disjoint 3-cycles and belongs to $H \cap A_n$. Thus $H \cap A_n$ cannot be $\{e\}$ or K and must be A_n, and H is either A_n or S_n. **Q**

case 3 Suppose that $n \neq 4$ and that H contains a permutation ρ of the form $(\overleftarrow{i_1\, i_2})(\overleftarrow{i_3\, i_4})$ where $i_1, \ldots, i_4$ are all different. Then $H = A_n$ or $H = S_n$. **P** Since $H \cap A_n \neq \{e\}$ and $n \neq 4$, $H \cap A_n = A_n$ and H is either A_n or S_n. **Q**

case 4 Suppose that H contains a transposition $\rho = (\overleftarrow{ij})$. Then $H = S_n$. **P** For any transposition $(\overleftarrow{kl}) \in S_n$, there is a $\sigma \in S_n$ such that $\sigma(i) = k$ and $\sigma(j) = l$; but now H contains

$$\sigma\rho\sigma^{-1} = (\overleftarrow{\sigma(i)\, \sigma(j)}) = (\overleftarrow{kl}).$$

Thus H contains every transposition and every product of transpositions. Since every permutation is a product of transpositions, $H = S_n$. **Q**

case 5 Suppose none of the above occur. Then H can contain only $\{e\}$ and double-transpositions, so $H \subseteq A_n$. But in this case $H = H \cap A_n \lhd A_n$, so either $H = \{e\}$ or $H = A_n$ or $n = 4$ and $H = K$. This completes the proof.

Isometry Groups

Suppose that X is any subset of $\mathbb{R}^m$, where $m \geq 1$. Then we have a distance $d : X \times X \to [0, \infty[$ defined by setting $d(\mathbf{x}, \mathbf{y}) = \sqrt{\sum_{i=1}^{m} |x_i - y_i|^2}$ if $\mathbf{x} = (x_1, \ldots, x_m)$, $\mathbf{y} = (y_1, \ldots, y_m) \in X$. An **isometry** of X is a function $f : X \to X$ such that $d(f(\mathbf{x}), f(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})$ for all $\mathbf{x}$, $\mathbf{y} \in X$. It is not hard to see that the set of bijective isometries from X to itself is a subgroup of the group of all bijections from X to itself.

Dihedral groups Now suppose that P_n is a regular polygon with $n \geq 3$ vertices. Then the isometries of P_n have to carry vertices to vertices, so we can identify every isometry of P_n with a permutation of the vertices, and if we label the vertices $1, 2, \ldots, n$ anticlockwise in order around the polygon we can think of isometries of P_n as members of S_n. Two of these we can identify easily:

$\rho = (\overleftarrow{12 \ldots n})$ corresponds to an anticlockwise rotation through an angle of $2\pi/n$

$\sigma = (\overleftarrow{1n})(\overleftarrow{2\ n-1})(\overleftarrow{3\ n-2})\ldots$ corresponds to a reflection about an axis through the centre of P_n and the midpoint of the edge between the vertices 1 and n.

(The specification of σ just above tails off a little vaguely. If n is *even*, then σ has got just $\frac{n}{2}$ transpositions, ending with $(\overleftarrow{\frac{n}{2}\ \frac{n}{2}+1})$, since the axis of reflection passes through the edge between the vertices $\frac{n}{2}$ and $\frac{n}{2}+1$.

If n is *odd*, then the axis of rotation passes through the vertex $\frac{n+1}{2}$, which is therefore unmoved, and the last transposition in σ is $(\overleftarrow{\tfrac{n-1}{2}\ \tfrac{n+3}{2}})$, exchanging the two neighbours of $\frac{n+1}{2}$.)

If we look at these, we see that $\rho^n = e$, and also that $e = \rho^0$, ρ, $\rho^2, \ldots, \rho^{n-1}$ are all different; next, that $\sigma^2 = e$; and also that $\sigma \neq \rho^i$ for any i. This means that

$$e, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}$$

are all different. (If $\sigma\rho^i = \sigma\rho^j$, where $i, j < n$, then $\rho^i = \rho^j$ so $i = j$; thus all the permutations in the second half of the list are different. If $i, j < n$, then $\sigma \neq \rho^{i-j}$ so $\rho^i \neq \sigma\rho^j$; thus the two halves of the list don't overlap.)

On the other hand, P_n has just $2n$ isometries, because we can put vertex 1 into any of two places, we shall then have 2 possible neighbouring places for vertex 2, and after this we have to put the rest of the vertices into order, clockwise or anticlockwise. So our list

$$\{e, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}\}$$

covers all the permutations corresponding to isometries of P_n, and forms a subgroup of S_n; it is called D_n, the **dihedral group** of order $2n$.

To understand the structure of the group D_n, having listed its members as $\{\sigma^i\rho^j : 0 \leq i < 2,\ 0 \leq j < n\}$, we have to be able to form its multiplication table. The key calculation is that of $\rho\sigma$. Now we know that $\sigma = \sigma^{-1}$, so

$$\begin{aligned}\rho\sigma = \sigma\sigma\rho\sigma^{-1} &= \sigma(\overleftarrow{\sigma(1)\,\sigma(2)\ldots\sigma(n)})\\ &= \sigma(\overleftarrow{n\ n-1\ n-2\ldots 3\,2\,1}) = \sigma\rho^{-1}.\end{aligned}$$

This enables us to do all the multiplications:

$$\rho^i \cdot \rho^j = \rho^{i +_n j}$$

(where $+_n$ is addition mod n)

$$\begin{aligned}\sigma\rho^i \cdot \rho^j &= \sigma\rho^{i+_n j},\\ \rho^i \cdot \sigma\rho^j &= \sigma(\sigma\rho^i\sigma^{-1})\rho^j = \sigma(\sigma\rho\sigma^{-1})^i\rho^j\end{aligned}$$

(because when we multiply $\sigma\rho\sigma^{-1}$ by itself i times, all the intermediate $\sigma^{-1}\sigma$s cancel)

$$= (\rho^{-1})^i\rho^j = \sigma\rho^{j-i} = \sigma\rho^{j-_n i}$$

(where $-_n$ is subtraction mod n)

$$\sigma\rho^i \cdot \sigma\rho^j = \sigma\sigma\rho^{j-_n i} = \rho^{j-_n i}.$$

We should be able to do these whenever we want to, so as long as we keep a firm hold of the formula $\sigma\rho\sigma^{-1} = \rho^{-1}$ we shouldn't need to remember the rest. There is another reason for hanging onto this. Consider any of the permutations in the second half of the list of elements of D_n. For any $i < n$ we have

$$(\sigma\rho^i)^2 = \sigma\rho^i\sigma^{-1}\rho^i = \rho^{-i}\rho^i = e,$$

$$(\sigma\rho^i)\rho(\sigma\rho^i)^{-1} = \sigma\rho^i\rho\rho^{-i}\sigma^{-1} = \sigma\rho\sigma^{-1} = \rho^{-1}.$$

So our key formulae

$$\rho^n = \sigma^2 = e, \quad \sigma\rho\sigma^{-1} = \rho^{-1}$$

are valid not only for the given σ, but for *any* of the reflections $\sigma\rho^i$.

Note that if n is *odd*, then all the reflections $\sigma\rho^i$ are reflections about an axis through a vertex and the midpoint of the opposite edge. On the other hand, if n is *even*, half of the axes are through midpoints of opposite sides, and half are through opposite pairs of vertices.

The isometry group of the regular tetrahedron Consider a regular tetrahedron with vertices v_1, v_2, v_3, v_4. Then any isometry of the tetrahedron corresponds to a permutation of these vertices, so the isometry group can be identified with a subgroup of S_4. To see which subgroup, observe that there are 24 isometries, 12 of which are rotations. **P** We can move v_1 to any vertex by a rotation, and having done so we can move v_2 to any of the remaining three. With two vertices fixed, we cannot rotate any further; but we can exchange the two remaining vertices by a reflection in the plane through the fixed edge and the midpoint of the opposite edge. So we have $4 \cdot 3 = 12$ rotations and $4 \cdot 3 \cdot 2 = 24$ isometries. **Q**

Since $\#(S_4) = 24$, the subgroup corresponding to the isometry group Isom(tetrahedron) must be the whole of S_4, and Isom(tetrahedron) $\cong S_4$. It follows that Rot(tetrahedron) $\cong A_4$. To see this, the following fact is useful:

> **Proposition** If G is a finite group and H is a subgroup of G such that $\#(H) = \frac{1}{2}\#(G)$, then $H \lhd G$.
>
> **proof** The cosets of H (whether left or right) have the same number of elements as H and are either equal to H or disjoint from H. Now $\#(G \setminus H) = \#(H)$, so any coset of H other than H itself must be $G \setminus H$. This means that if $x \in G$, either $x \in H$ and $xH = H = Hx$, or $x \notin H$ and $xH = G \setminus H = Hx$. So $H \lhd G$.

Now we know that Rot(tetrahedron) has 12 elements, so corresponds to a subgroup of S_4 with 12 elements; this subgroup must be normal; but we know all about the normal subgroups of S_4, and the only one with 12 elements is A_4. So Rot(tetrahedron) must be isomorphic to A_4.

[Alternatively: we have 8 rotations which keep one vertex fixed, and act as a 3-cycle on the other 3; 3 rotations which exchange vertices in two pairs, being 120° rotations about axes through the midpoints of opposite edges; and one identity rotation. Since this makes 12, we have no further rotations. The corresponding elements of S_4 are the 8 3-cycles, 3 double-transpositions and the identity, which make A_4 exactly.]

The 6 transpositions in S_4 correspond to the 6 reflections in planes through edges and midpoints of opposite edges. The 6 4-cycles in S_4 do not correspond to either simple rotations or simple reflections of the cube.

Note that we can distinguish two kinds of rotation of order 3. Each of these keeps one vertex fixed and rotates the face opposite it, and if we look at that face from the outside (so that the fixed vertex is at the back) then the rotation may be either clockwise or anti-clockwise. Imagine that the vertices are labelled $v_1, \ldots, v_4$ in such a way that (v_1, v_2, v_3) appear clockwise around a face and v_4 is behind it. Then the other three faces, taking the vertices in clockwise order viewed from in front of the face, are (v_1, v_4, v_2), (v_1, v_3, v_4) and (v_2, v_4, v_3). So the 'clockwise' rotations correspond to the 3-cycles $(\overleftarrow{123})$, $(\overleftarrow{142})$, $(\overleftarrow{134})$ and $(\overleftarrow{243})$, while their inverses (or squares) $(\overleftarrow{132})$, $(\overleftarrow{124})$, $(\overleftarrow{143})$ and $(\overleftarrow{234})$ correspond to 'anticlockwise' rotations. Now any two 3-cycles are conjugate in S_4, because if we have $(\overleftarrow{i_1\, i_2\, i_3})$ and $(\overleftarrow{j_1\, j_2\, j_3})$ we can find a $\rho \in S_4$ such that $\rho(i_1) = j_1$, $\rho(i_2) = j_2$ and $\rho(i_3) = j_3$, so that $(\overleftarrow{j_1\, j_2\, j_3}) = \rho(\overleftarrow{i_1\, i_2\, i_3})\rho^{-1}$. But it may not be possible to find such a ρ in A_4; for instance, if we want to express $(\overleftarrow{132})$ as $(\overleftarrow{\rho(1)\, \rho(2)\, \rho(3)})$, we shall have to take $\rho = (\overleftarrow{23})$, which is odd. I mention this here because the 'clockwise' cycles $(\overleftarrow{123})$, $(\overleftarrow{142})$, $(\overleftarrow{134})$ and $(\overleftarrow{243})$ are conjugate in A_4 (for instance, $(\overleftarrow{142}) = \rho(\overleftarrow{123})\rho^{-1}$ where $\rho = (\overleftarrow{243}) \in A_4$), the 'anticlockwise' cycles $(\overleftarrow{132})$, $(\overleftarrow{124})$, $(\overleftarrow{143})$ and $(\overleftarrow{234})$ are conjugate in A_4, but no 'clockwise' cycle is conjugate (in A_4) to any 'anticlockwise' cycle.

The subgroup $K = \{e, (\overleftarrow{12})(\overleftarrow{34}), (\overleftarrow{13})(\overleftarrow{24}), (\overleftarrow{14})(\overleftarrow{23})\}$ corresponds to the identity rotation ι and the three 180° rotations about axes through midpoints of opposite edges. It is the case that these axes pass at right angles through the centre of the cube; K corresponds to the rotations which do not exchange any of these axes.

The isometry group of the cube Turning to the cube, we have 24 rotations (8 choices for first vertex, 3 choices for one of its neighbours) and 48 isometries (given a fixed edge, we can reflect in the plane through that edge and the opposite edge). Now the rotation group Rot(cube) is isomorphic to S_4. **P** Consider the 4 long diagonals. The action of Rot(cube) on these corresponds to a homomorphism from the rotation group to S_4. If we look at a 180° rotation about an axis through the midpoints of two opposite edges, this exchanges two of the diagonals and leaves the other two unmoved; so every transposition is in the image H of Rot(cube), and H must be S_4. Since the number of rotations is $6 \cdot 4 = 8 \cdot 3 = 24 = \#(S_4)$, the homomorphism must be injective as well as surjective and is an isomorphism.

[Alternative argument: A 90° rotation about an axis through the midpoints of opposite faces corresponds to a 4-cycle in S_4, and a 120° rotation about a long diagonal corresponds to a 3-cycle. So H has subgroups of orders 3 and 4 and has at least 12 members. But the only subgroup of S_4 with 12 members is A_4, which does not contain any 4-cycle, so H must be the whole of S_4.]**Q**

Since $\mathrm{Rot(cube)} \cong S_4$, we ought to be able to distinguish 'odd' from 'even' rotations. If we look at the 8 vertices, we can label them 'white' and 'black' in such a way that adjacent vertices are always of different colours. Now if we look at those rotations which take vertices to other vertices of the same colour, we find that there are 12 of them (since our first vertex now has only 4 possible places, but its neighbour still has a choice of 3); and since the only subgroup of S_4 with 12 members is A_4, we must have the right subgroup of Rot(cube).

Similarly, we ought to be able to find the rotations corresponding to members of the subgroup $K = \{e, (\overleftarrow{12})(\overleftarrow{34}), (\overleftarrow{13})(\overleftarrow{24}), (\overleftarrow{14})(\overleftarrow{23})\}$. These are the rotations which hold all three principal axes of the cube fixed, where by 'principal axis' I mean an axis through midpoints of opposite faces. The double-transpositions correspond to 180° rotations about a principal axis.

The isometry group of the cube is not (yet) on our list of standard groups. I note here only that since Rot(cube) is just half of Isom(cube), $\mathrm{Rot(cube)} \lhd \mathrm{Isom(cube)}$. There is a particularly important member of $\mathrm{Isom(cube)} \setminus \mathrm{Rot(cube)}$, which I will call t; this is the isometry which takes every point to its balancing point on the other side of the centre of the cube. t exchanges all 4 pairs of opposite vertices. (It cannot be a rotation because it keeps all the diagonals fixed.) We have $t^2 = \iota$, the identity; moreover, $tf = ft$ for every $f \in \mathrm{Isom(cube)}$. **P** If $f \in \mathrm{Isom(cube)}$ and v is any vertex, then $v' = t(v)$ is the opposite vertex. Now the distance from $f(v)$ to $f(v')$ must be the same as the distance from v to v', that is, $\sqrt{3}$ if the cube has sides of length 1, so that $f(v)$ and $f(v')$ are also opposite vertices, that is, $tf(v) = f(v') = ft(v)$. As this is true for every v, $tf = ft$. **Q**

If we set $C = < t > = \{\iota, t\} \cong \mathbb{Z}_2$, then $C\,\mathrm{Rot(cube)} = \mathrm{Isom(cube)}$ and the combination of properties

$$C \cong \mathbb{Z}_2,\ \mathrm{Rot(cube)} \cong S_4,\ C \cap \mathrm{Rot(cube)} = \{\iota\},\ C\,\mathrm{Rot(cube)} = \mathrm{Isom(cube)},$$
$$fg = gf \text{ for every } f \in \mathrm{Rot(cube)} \text{ and every } g \in C$$

is enough to determine Isom(cube) up to isomorphism.

The isometry group of a regular octahedron Every regular octahedron has a cube inside it, with the vertices of the cube at the centres of the faces of the octahedron. Isometries of the octahedron take the cube to itself, and vice versa, so $\mathrm{Isom(octahedron)} \cong \mathrm{Isom(cube)}$ and $\mathrm{Rot(octahedron)} \cong \mathrm{Rot(cube)} \cong S_4$.

The isometry group of a regular dodecahedron A regular dodecahedron has 20 vertices and 30 edges. In its faces we can inscribe 5 cubes; each cube has each of its 12 edges in a different face of the dodecahedron; two cubes meet at each vertex.

The dodecahedron has 60 rotations (you have 12 choices of where to put a face, then 5 choices of which way round to put it; *or* you have 20 choices of where to put a vertex, then 3 places for one of its neighbours; *or* you have 30 choices of where to put an edge, then a choice of which way round its vertices should be). It has 120 isometries (after fixing two neighbouring vertices, you can now reflect in the plane through them and the centre of the dodecahedron).

Any isometry of the dodecahedron acts as a permutation of the five cubes, so we have a homomorphism $\phi : \mathrm{Isom(dodecahedron)} \to S_5$. Set $H = \phi[\mathrm{Rot(dodecahedron)}] \cap A_5$, so that H is a subgroup of S_5 (being the intersection of two subgroups) and therefore a subgroup of A_5. Now $H = A_5$.

P method 1 If we look at a 120° rotation about a long diagonal, this leaves two of the cubes fixed and moves the other three in a cycle, so H contains a 3-cycle and has a subgroup of order 3.

If we look at a 72° rotation about an axis through the midpoints of a pair of opposite faces, this moves all five cubes in a cycle, so H contains a 5-cycle and has a subgroup of order 5.

If we look at a 180° rotation about an axis through the midpoints of a pair of opposite edges, this leaves one cube in place and exchanges the others in pairs, so H contains a double-transposition and has a subgroup of order 2.

By Lagrange's theorem, $\#(H)$ must be a multiple of 3, 5 and 2 and therefore is a multiple of 30. It is also a factor of 60. But A_5 has no normal subgroup of order 30, so can have no subgroup of order 30, and $\#(H) \neq 30$. It follows that $\#(H) = 60$ and $H = A_5$.

method 2 There are $\frac{5\cdot4\cdot3}{3} = 20$ 3-cycles in A_5. Also there are 10 long diagonals of the dodecahedron, and about each of these there are two 120° rotations, one each way, each corresponding to a 3-cycle in A_5.

So every 3-cycle corresponds to a rotation and belongs to H. Since every member of A_5 is a product of 3-cycles, $H = A_5$. **Q**

Thus $\phi[\text{Rot(dodecahedron)}]$ includes A_5. But $\#(\text{Rot(dodecahedron)}) = \#(A_5)$, so $\phi[\text{Rot(dodecahedron)}]$ must be A_5 exactly, and $\phi : \text{Rot(dodecahedron)} \to A_5$ must be a bijection, therefore an isomorphism. So $\text{Rot(dodecahedron)} \cong A_5$.

Now $\#(\text{Isom(dodecahedron)}) = 120 = \#(S_5)$ and both Isom(dodecahedron) and S_5 have subgroups isomorphic to A_5. However, $\text{Isom(dodecahedron)} \not\cong S_5$. **P** Consider the isometry t of the dodecahedron which takes every point to its balancing point on the opposite side of the centre of the dodecahedron. Then $t^2 = \iota$ and $tf = ft$ for every $f \in \text{Isom(dodecahedron)}$ (just as for the cube). So $\{\iota, t\}$ is a normal subgroup of Isom(dodecahedron) with two elements, and we know that S_5 has no such subgroup. **Q**

Now let us try to classify the rotations of the dodecahedron.

(i) We know that there are $\frac{5\cdot4\cdot3\cdot2\cdot1}{5} = 24$ 5-cycles in A_5. If we look at rotations about axes through midpoints of opposite faces, we see that there are 6 such axes, and for each axis there are two 72° rotations (one each way) and two 144° rotations, all of which are of order 5; so between them they give us $6 \cdot 4 = 24$ rotations of order 5, which must correspond to the 24 5-cycles in A_5.

Note that these 5-cycles come in two types: those corresponding to 72° rotations and those corresponding to 144° rotations. What is happening here is that while in S_5 all 5-cycles are conjugate, in A_5 the 5-cycles fall into two conjugacy classes (just as the 3-cycles do in A_4).

(ii) We know that there are $\frac{5\cdot4\cdot3}{3} = 20$ 3-cycles in A_5; as described in 'method 2' above, all of these are got by rotations about long diagonals.

(iii) There are $\frac{5\cdot4\cdot3\cdot2}{2\cdot2\cdot2} = 15$ double-transpositions in A_5. Also there are 15 pairs of opposite edges, so there are fifteen 180° rotations about axes through the midpoints of opposite edges. This means that every double-transposition corresponds to such a rotation.

check: $24 + 20 + 15 = 59$; add one for the identity, we have all the members of A_5 and therefore all the rotations of the dodecahedron.

Group Actions

Definition Let G be a group and X a set. An **action** of G on X is a function $(a, x) \mapsto a\bullet x : G \times X \to X$ such that

$$(ab)\bullet x = a\bullet(b\bullet x), \quad e\bullet x = x$$

whenever $a, b \in G$ and $x \in X$.

Examples (a) If G is any group, the **left action** of G on itself is defined by the formula

$$a\bullet x = ax \text{ for all } a, x \in G.$$

To see that this is an action, we need only check that

$$(ab)\bullet x = (ab)x = a(bx) = a\bullet(b\bullet x),$$

$$e\bullet x = ex = x$$

for all $a, b, x \in G$.

(b) If G is any group, the **right action** of G on itself is defined by the formula

$$a\bullet x = xa^{-1} \text{ for all } a, x \in G.$$

To see that this is an action, we need only check that

$$(ab)\bullet x = x(ab)^{-1} = x(b^{-1}a^{-1}) = (xb^{-1})a^{-1} = a\bullet(xb^{-1}) = a\bullet(b\bullet x),$$

$$e\bullet x = xe^{-1} = x$$

for all $a, b, x \in G$.

(c) If G is any group, the **conjugacy action** of G on itself is defined by the formula

$$a{\bullet}x = axa^{-1} \text{ for all } a,\, x \in G.$$

To see that this is an action, we need only check that

$$(ab){\bullet}x = (ab)x(ab)^{-1} = abxb^{-1}a^{-1} = a(b{\bullet}x)a^{-1} = a{\bullet}(b{\bullet}x),$$

$$e{\bullet}x = exe^{-1} = x$$

for all a, b, $x \in G$.

(d) If $G = \mathrm{Rot(cube)}$ is the rotation group of the cube, and X is the set of principal axes of the cube (i.e., axes through midpoints of opposite faces), then G acts on X, just because any rotation of the cube must move pairs of opposite faces to pairs of opposite faces.

Theorem Let G be a group and X a set. Any action of G on X corresponds to a homomorphism ϕ from G to the group S_X of all bijections from X to itself, defined by the formula

$$\phi(a)(x) = a{\bullet}x \text{ for } a \in G,\, x \in X.$$

Conversely, any homomorphism $\phi : G \to S_X$ corresponds to an action.

proof (a) Given an action $\bullet : G \times X \to X$, then the formula $\phi(a)(x) = a{\bullet}x$ defines a function $\phi(a) : X \to X$ for every $a \in G$, just because $a{\bullet}x \in X$ for every $x \in X$ and $a \in G$.

If $a \in G$, then $\phi(a) : X \to X$ is injective. **P** If x, $y \in X$ and $\phi(a)(x) = \phi(a)(y)$, then

$$\begin{aligned} x &= e{\bullet}x = (a^{-1}a){\bullet}x = a^{-1}{\bullet}(a{\bullet}x) = a^{-1}{\bullet}(\phi(a)(x)) \\ &= a^{-1}{\bullet}(\phi(a)(y)) = a^{-1}{\bullet}(a{\bullet}y) = (a^{-1}{\bullet}a){\bullet}y = e{\bullet}y = y.\mathbf{Q} \end{aligned}$$

If $a \in G$, then $\phi(a) : X \to X$ is surjective. **P** If $y \in X$, then

$$\phi(a)(a^{-1}{\bullet}y) = a{\bullet}(a^{-1}{\bullet}y) = (aa^{-1}){\bullet}y = e{\bullet}y = y. \; \mathbf{Q}$$

Thus $\phi(a) \in S_X$ for every $a \in G$, and ϕ is a function from G to S_X. Now ϕ is a homomorphism. **P** If a, $b \in G$ and $x \in X$,

$$\begin{aligned} \phi(ab)(x) &= (ab){\bullet}x = a{\bullet}(b{\bullet}x) \\ &= \phi(a)\big(\phi(b)(x)\big) = \big(\phi(a) \circ \phi(b)\big)(x). \end{aligned}$$

As x is arbitrary,

$$\phi(ab) = \phi(a) \circ \phi(b).$$

As a and b are arbitrary, $\phi : G \to S_X$ is a homomorphism. **Q**

This shows that, starting from an action $\bullet$ of G on X, the formula $\phi(a)(x) = a{\bullet}x$ defines a homomorphism from G to S_X.

(b) Now suppose that we have a homomorphism $\phi : G \to S_X$ and we define a function $\bullet : G \times X \to X$ by the formula $a{\bullet}x = \phi(a)(x)$. Then, writing $\iota : X \to X$ for the identity function,

$$\begin{aligned} (ab){\bullet}x &= \phi(ab)(x) = \big(\phi(a) \circ \phi(b)\big)(x) \\ &= \phi(a)\big(phi(b)(x)\big) = a{\bullet}(b{\bullet}x), \\ e{\bullet}x &= \phi(e)(x) = \iota(x) = x \end{aligned}$$

for all a, $b \in G$ and $x \in X$, because $\phi(e)$ must be the identity of S_X, which is ι. So $\bullet$ is an action.

Corollary If $\bullet$ is an action of a group G on a set X, then

$$K = \{a : a{\bullet}x = x \text{ for every } x \in X\}$$

is a normal subgroup of G, and G/K is isomorphic to a subgroup of S_X.

proof If $\phi : G \to S_X$ is the homomorphism associated with $\bullet$, then

$$K = \{a : \phi(a)(x) = x \;\forall\; x \in X\} = \{a : \phi(a) = \iota\}$$

is the kernel of ϕ, so is a normal subgroup of G, and $G/K \cong \phi[G] \le S_X$ by the First Isomorphism Theorem.

Remark $\{a : a{\bullet}x = x \text{ for every } x \in X\}$ may be called the **kernel** of the action.

Example When $G = \mathrm{Rot}(\text{cube})$ and X is the set of principal axes of the cube, then K becomes the identity together with the three $180°$ rotations about the principal axes. When we identify G with S_4 in the usual way, K becomes matched with the special normal subgroup of S_4 with 4 elements. When we look at the image of G in $S_X \cong S_3$, we see that a $90°$ rotation about a principal axis give a transposition (of the other two axes), and that all the three transpositions can be got in this way; so the image of G contains every transposition and must be the whole of S_X. What this means is that $G/K \cong S_X$; or, in terms of S_4, $S_4/K \cong S_3$, where in this formula K means the 4-element normal subgroup of S_4.

[As a general rule, whenever you have a normal subgroup you should try to identify the corresponding quotient group.]

Definition Let $\bullet$ be an action of a group G on a set X. For any $x \in X$, the **stabilizer** of x is

$$\mathrm{Stab}(x) = \{a : a \in G,\ a{\bullet}x = x\},$$

and the **orbit** of x is

$$\mathrm{Orb}(x) = \{a{\bullet}x : a \in G\}.$$

Proposition Whenever a group G acts on a set X, the stabilizer of any $x \in X$ is a subgroup of G.

proof $e{\bullet}x = x$ so $e \in \mathrm{Stab}(x)$.

If $a, b \in \mathrm{Stab}(x)$ then

$$(ab){\bullet}x = a{\bullet}(b{\bullet}x) = a{\bullet}x = x,$$

so $ab \in \mathrm{Stab}(x)$.

If $a \in \mathrm{Stab}(x)$ then

$$a^{-1}{\bullet}x = a^{-1}{\bullet}(a{\bullet}x) = (a^{-1}a){\bullet}x = e{\bullet}x = x,$$

so $a^{-1} \in \mathrm{Stab}(x)$.

Proposition Whenever a group G acts on a set X, the orbits in X form a partition of X.

proof (a) For any $x \in X$, $x = e{\bullet}x \in \mathrm{Orb}(x)$, so x belongs to at least one orbit, its own.

(b) If $x, y \in X$ and $\mathrm{Orb}(x) \cap \mathrm{Orb}(y) \neq \emptyset$, then $\mathrm{Orb}(x) = \mathrm{Orb}(y)$. **P** Take $z \in \mathrm{Orb}(x) \cap \mathrm{Orb}(y)$; then there are $a, b \in G$ such that $z = a{\bullet}x = b{\bullet}y$. If $w \in \mathrm{Orb}(x)$, then there is a $c \in G$ such that

$$w = c{\bullet}x = (ca^{-1}a){\bullet}x = (ca^{-1}){\bullet}(a{\bullet}x) = (ca^{-1}){\bullet}(b{\bullet}y) = (ca^{-1}b){\bullet}y \in \mathrm{Orb}(y).$$

As w is arbitrary, $\mathrm{Orb}(x) \subseteq \mathrm{Orb}(y)$. Similarly, $\mathrm{Orb}(y) \subseteq \mathrm{Orb}(x)$, and the two orbits are identical. **Q**

(c) So there can be only one orbit containing any given element of X, and the orbits are a partition of X.

Theorem Let G be a finite group acting on a set X. Then

$$\#(\mathrm{Stab}(x)) \cdot \#(\mathrm{Orb}(x)) = \#(G)$$

for every $x \in G$.

proof Write S for $\mathrm{Stab}(x)$. Now the point is that, for $a, b \in G$, $a{\bullet}x = b{\bullet}x$ iff $aS = bS$. **P** If $a{\bullet}x = b{\bullet}x$, then

$$x = e{\bullet}x = (a^{-1}a){\bullet}x = a^{-1}{\bullet}(a{\bullet}x) = a^{-1}{\bullet}(b{\bullet}x) = (a^{-1}b){\bullet}x,$$

so $a^{-1}b \in S$ and $b = aa^{-1}b \in aS$ and $bS = aS$. On the other hand, if $aS = bS$ then $a = ae \in bS$ so there is a $c \in S$ such that $a = bc$ and

$$a{\bullet}x = (bc){\bullet}x = b{\bullet}(c{\bullet}x) = b{\bullet}x. \quad \mathbf{Q}$$

This means that we have a one-to-one correspondence between members of $\mathrm{Orb}(x)$ and left cosets of S, matching $a{\bullet}x$ with aS. So the number of left cosets of S is exactly $\#(\mathrm{Orb}(x))$. But now Lagrange's theorem tells us that

$$\#(G) = \#(S) \cdot (\text{number of left cosets of } S) = \#(S) \cdot \#(\mathrm{Orb}(x)),$$

as claimed.

Example Once again, let G be the rotation group of the cube and X the set of principal axes. If $x \in X$, then $\mathrm{Orb}(x) = X$, just because we can move any axis to another by a rotation. So $\mathrm{Stab}(x)$ has $\frac{24}{8}$ members.

To see what $\mathrm{Stab}(x)$ looks like, consider the plane through the centre of the cube perpendicular to x. This meets the cube in a square Q say. Any rotation of the cube which returns x to its place must also put Q back where it was, and vice versa. So $\mathrm{Stab}(x)$ corresponds to the rotations and reflections of Q, and is isomorphic to D_4.

(We can also identify $\mathrm{Stab}(x)$ in terms of permutations in S_4. $\mathrm{Stab}(x)$ contains the $90°$ rotation about x, which corresponds to a 4-cycle in S_4. The other members of $\mathrm{Stab}(x)$ are the reflections of Q; two of them are $180°$ rotations about the other two axes, corresponding to double-transpositions in S_4; the other two are $180°$ rotations about the axes which are the diagonals of Q, corresponding to transpositions in S_4. So if H is the subgroup of S_4 corresponding to $\mathrm{Stab}(x) \le \mathrm{Rot(cube)}$, H contains all three double-transpositions and a couple of transpositions. If we label the diagonals in such a way that $(\overleftarrow{12}) \in H$, then H must contain

$$e,\ (\overleftarrow{12})(\overleftarrow{34}),\ (\overleftarrow{13})(\overleftarrow{24}),\ (\overleftarrow{14})(\overleftarrow{23})$$

and also their products with $\sigma = (\overleftarrow{12})$, being

$$(\overleftarrow{12}),\ (\overleftarrow{34}),\ \rho = (\overleftarrow{1423}),\ (\overleftarrow{1324}).$$

Observe that (of course) $\rho^4 = \sigma^2 = e$ and $\sigma\rho\sigma^{-1} = (\overleftarrow{2413}) = \rho^{-1}$.

The conjugacy action Recall that any group G acts on itself through the **conjugacy action** $a{\bullet}x = axa^{-1}$. The stabilizer of $x \in G$ under this action is the **centralizer subgroup** $C_x = \{a : axa^{-1} = x\} = \{a : ax = xa\}$ of elements commuting with x. The orbit of $x \in G$ under the action is the **conjugacy class** $\{axa^{-1} : a \in G\}$ of elements conjugate to x in G. The kernel of the action is the **centre**

$$C = \{a : axa^{-1} = x \text{ for every } x \in G\} = \{a : ax = xa \text{ for every } x \in G\}$$

of G, the set of elements commuting with every element of G.

G is abelian iff $C = G$ iff $C_x = G$ for every $x \in G$ iff every conjugacy class has just one element.

Generally, C consists of those x such that $\{x\}$ is a conjugacy class; $G \setminus C$ is the union of the non-singleton conjugacy classes.

Proposition Let G be a non-abelian group. Then G/C is not cyclic.

proof ? Suppose, if possible, that $G/C = \langle w \rangle = \{w^n : n \in \mathbb{Z}\}$ for some $w \in G/C$. As $G \neq C$, w cannot be the identity of G/C. Express w as bC where $b \in G$. Then $b \notin C$ so there is an $x \in G$ such that $bx \neq xb$.

Consider $v = xC$. We know that $v = w^n$ for some $n \in \mathbb{Z}$. Now $w^n = b^nC$, because the map $y \mapsto yC : G \to G/C$ is a homomorphism. So $xC = b^nC$ and $x \in b^nC$ and $x = b^nc$ for some $c \in C$. Now $bc = cb$, so

$$bx = b(b^nc) = (bb^n)c = b^{n+1}c = (b^nb)c = b^n(bc) = b^n(cb) = (b^nc)b = xb,$$

contrary to the choice of x. **X**

Proposition Suppose that G is a finite group of prime power order, not $\{e\}$. Then the centre of G is not $\{e\}$.

proof Suppose that $\#(G) = p^r$, where p is a prime and $r \ge 1$. G/C is a union of non-trivial conjugacy classes. Now if $x \in G \setminus C$, $\#(C_x) \cdot \#(\text{conjugacy class of } x) = \#(G) = p^r$, so the number of elements of G conjugate to x is a factor of p^r; but it is not 1, because $x \notin C$, so is a multiple of p. Since the non- singleton conjugacy classes of G form a partition of $G \setminus C$, $\#(G \setminus C)$ is a multiple of p and $\#(C) = \#(G) - \#(G \setminus C)$ is a multiple of p. In particular, $C \neq \{e\}$.

Proposition Suppose that G is a group of order p^2, where p is a prime. Then G is abelian.

proof Consider the centre C of G. Then $\#(C)$ is a factor of p^2, by Lagrange's theorem, so is 1 or p or p^2. By the last proposition, it cannot be 1. Also G/C is not cyclic, so $\#(G/C) \neq p$ and $\#(C) \neq p$. We are left with $\#(C) = p^2$, that is, $C = G$, and G is abelian.

Dihedral groups Suppose that $n \ge 3$ and that we take the standard generators ρ, σ of the dihedral group D_n, so that $\rho^n = \sigma^2 = e$ and $\sigma\rho\sigma^{-1} = \rho^{-1}$; in the interpretation of D_n as the isometry group of a regular n-gon, we can take ρ to be the anticlockwise rotation through $(360/n)^\circ$ and σ to be the reflection about an axis through the midpoint of the edge joining the vertices 1 and n and the centre of the polygon.

In this case, the conjugacy class E_ρ of ρ contains (at least) ρ and $\sigma\rho\sigma^{-1} = \rho^{-1}$, and the centralizer C_ρ of ρ contains (at least) the subgroup $<\rho>$ generated by ρ, just because it is a subgroup containing ρ. But as

$$\#(C_\rho)\cdot\#(E_\rho) = \#(D_n) = 2n = 2\#(<\rho>),$$

there is no room for either C_ρ or E_ρ to be larger; so $C_\rho = <\rho>$ and $E_\rho = \{\rho, \rho^{-1}\}$ exactly.

Similarly, for any $i < n$, C_{ρ^i} includes $<\rho>$ and E_{ρ^i} includes $\{\rho^i, \rho^{-i}\}$ (because $\sigma\rho^i\sigma^{-1} = (\sigma\rho\sigma^{-1})^i = \rho^{-i}$); so $C_{\rho^i} = <\rho>$ and $E_{\rho^i} = \{\rho^i, \rho^{-i}\}$ *unless* $\rho^i = \rho^{-i}$, that is, $\rho^{2i} = e$, that is, $i = n/2$. Of course this can happen only when n is even. When n is even, then $\sigma\rho^{n/2}\sigma^{-1} = \rho^{n/2}$, that is, $\sigma\rho^{n/2} = \rho^{n/2}\sigma^{-1}$, and $\sigma \in C_{\rho^{n/2}}$. Since ρ certainly belongs to $C_{\rho^{n/2}}$, $C_{\rho^{n/2}} = D_n$, that is, $\rho^{n/2}$ belongs to the centre C of D_n, and $E_{\rho^{n/2}} = \{\rho^{n/2}\}$.

Geometrically, $\rho^{n/2}$ corresponds to a 180° rotation, which is also the map which takes every vertex to its opposite across the centre of the polygon.

Now consider C_σ. This contains e and σ. If n is odd, it does not contain ρ^i for any i such that $0 < i < n$, so cannot contain $\sigma\rho^i$ for any i such that $0 < i < n$, and $C_\sigma = <\sigma> = \{e, \sigma\}$. In this case, E_σ must have n members and must be the whole of $\{\sigma\rho^i : i \in \mathbb{Z}\} = D_n\setminus <\rho>$.

If n is even, however, $C_\sigma = \{e, \sigma, \rho^{n/2}, \sigma\rho^{n/2}\}$ and E_σ has $n/2$ members. To see what they are, note that $\rho\sigma\rho^{-1} = \sigma\rho^{-2}$ belongs to E_σ; similarly, $\rho^2\sigma\rho^{-2} = \sigma\rho^{-4} \in E_\sigma$, and so on; generally, $\sigma\rho^{-2i} = \sigma\rho^{n-2i} \in E_\sigma$ for every $i \in \mathbb{N}$. Because n is even, this amounts to saying that $\sigma\rho^{2i} \in E_\sigma$ for every $i < \frac{n}{2}$. Since there are $\frac{n}{2}$ such elements, we have found the whole of E_σ.

Geometrically speaking, if n is *odd* then every axis of symmetry of the polygon passes through a vertex and the midpoint of the opposite side, and all the reflections are conjugate. But if n is *even*, then half the axes of symmetry pass through midpoints of opposite sides, and are conjugate to σ as described, and the other half are long diagonals passing through pairs of opposite vertices, and are conjugate to each other but not to σ.

If n is *odd*, then the centre C of D_n is $\{e\}$, and $D_n/C \cong D_n$. If n is *even*, then $C = \{e, \rho^{n/2}\}$. In this case, $\#(D_n/C) = n$. In fact, $D_n/C \cong D_{n/2}$. **P** For $x \in D_n$, write $\bar{x}$ for its image $xC \in D_n/C$; remember that $x \mapsto \bar{x}$ is a homomorphism. So we shall have

$$\bar{\rho}^{n/2} = (\rho^{n/2})^- = \bar{e}, \quad \bar{\sigma}^2 = (\sigma^2)^- = \bar{e},$$

$$\bar{\sigma}\bar{\rho}\bar{\sigma}^{-1} = (\sigma\rho\sigma^{-1})^- = (\rho^{-1})^- = \bar{\rho}^{-1}.$$

Thus $\bar{\rho}$, $\bar{\sigma}$ satisfy the defining relations for $D_{n/2}$ and $D_n/C \cong D_{n/2}$.

Geometrically, for even n, we can think of D_n as acting on the $\frac{n}{2}$ long diagonals of the polygon. The kernel of this action is C and D_n/C is isomorphic to the image of the action. The image $\bar{\rho}$ of ρ acts as an $\frac{n}{2}$-cycle while $\bar{\sigma}$ acts as a reflection.

Automorphism groups If G is a group, an **automorphism** of G is an isomorphism from G to itself. I will write $\operatorname{Aut} G$ for the set of automorphisms of G.

Proposition For any group G, $\operatorname{Aut} G$ is a subgroup of the group S_G of all bijections from G to itself; so $\operatorname{Aut} G$ is a group in its own right.

proof By definition, an isomorphism is a bijection; so $\operatorname{Aut} G \subseteq S_G$. Writing ι for the identity of S_G,

$$\iota(xy) = xy = \iota(x)\iota(y)$$

for all x, $y \in G$, so $\iota : G \to G$ is a homomorphism, therefore an isomorphism, and belongs to $\operatorname{Aut} G$. If ϕ, $\psi \in \operatorname{Aut} G$ then $\phi\circ\psi$ is a homomorphism (because any composition of homomorphisms is a homomorphism), so (being bijective) belongs to $\operatorname{Aut} G$. If $\phi \in \operatorname{Aut} G$, $\phi^{-1} : G \to G$ is an isomorphism (because the inverse of an isomorphism is always an isomorphism), so belongs to $\operatorname{Aut} G$.

Inner automorphisms Again, let G be any group. Then the conjugacy action of G on itself corresponds to a homomorphism from G to S_G; write $\hat{a} \in S_G$ for the bijection corresponding to $a \in G$, so that $\hat{a}(x) = axa^{-1}$ for every $x \in G$. Set $J = \{\hat{a} : a \in G\}$, the image of the homomorphism, and

$$C = \{a : \hat{a} = \iota\} = \{a : axa^{-1} = x \ \forall\, x \in G\} = \{a : ax = xa \ \forall\, x \in G\},$$

so that C is the kernel of the homomorphism and is the centre of G. By the First Isomorphism Theorem, $G/C \cong J$.

Theorem In the language here, $J \lhd \operatorname{Aut} G$.

proof (a) If $a \in G$, then

$$\hat{a}(xy) = axya^{-1} = axa^{-1}aya^{-1} = \hat{a}(x)\hat{a}(y)$$

for all x, $y \in G$, so that $\hat{a} : G \to G$ is a homomorphism. As we already know that it is a bijection, $\hat{a} \in \operatorname{Aut} G$. This is true for every $a \in G$, so $J \subseteq \operatorname{Aut} G$. Since J is a subgroup of S_G, it is also a subgroup of $\operatorname{Aut} G$.

(b) Now $J \lhd \operatorname{Aut} G$. **P** Suppose that $\phi \in J$ and $\psi \in \operatorname{Aut} G$. Express ϕ as $\hat{a}$, where $a \in G$, and set $b = \psi(a)$. Then, for any $x \in X$,

$$(\psi\phi\psi^{-1})(x) = \psi(\phi(\psi^{-1}(x)))$$

(by the definition of multiplication in S_G)

$$= \psi(a\psi^{-1}(x)a^{-1})$$

(because $\phi = \hat{a}$)

$$= \psi(a)\psi(\psi^{-1}(x))\psi(a^{-1})$$

(because ψ respects multiplication)

$$= \psi(a)x\psi(a)^{-1}$$

(because homomorphisms respect inversion)

$$= bxb^{-1} \qquad = \hat{b}(x).$$

As x is arbitrary, $\psi\phi\psi^{-1} = \hat{b}$ belongs to J; as ψ and ϕ are arbitrary, $J \lhd \operatorname{Aut} G$.

Example: the Klein group K_4 Consider the exceptional normal subgroup $\{e, (\overleftarrow{12})(\overleftarrow{34}), (\overleftarrow{13})(\overleftarrow{24}), (\overleftarrow{14})(\overleftarrow{23})\}$ of A_4 and S_4. This group is abelian, so its centre C is itself, and $J \cong K_4/C$ has just one element.

If we think of K_4 in the abstract, it has elements e, a, b, c with $a^2 = b^2 = c^2 = e$ and $ab = ba = c$, $ac = ca = b$, $bc = cb = a$. This means that any permutation of a, b, c corresponds to an automorphism of K_4, and $\operatorname{Aut} K_4 \cong S_3 \cong D_3$.

Remark Note that if G is any group with four elements, it is isomorphic to either K_4 or $\mathbb{Z}_4$. For if G has an element a of order 4, then $G = < a > \cong \mathbb{Z}_4$. Otherwise, $G \setminus \{e\}$ must have just 3 elements a, b and c. Because the order of any element must divide the order of the group (by Lagrange's theorem), we must have $a^2 = b^2 = c^2 = e$. Now ab cannot be equal to e (because $a \neq b$) nor to a (because $b \neq e$) nor to b (because $a \neq e$). So $ab = c$; and the rest of the multiplication table follows similarly. Thus in this case $G \cong K_4$.

K_4 is sometimes called the **Klein group**.

Example: cyclic groups Suppose that $G = \{e, a, a^2, \ldots, a^{n-1}\}$ where $n \geq 2$. (Of course G is isomorphic to $\mathbb{Z}_n$ but I think it will be less confusing to keep to multiplicative notation.) For $0 \leq i < n$ and $k \in \mathbb{Z}$, set $\phi_k(a^i) = a^{ik}$. Note that $\phi_k(a^j) = a^{jk}$ for any $j \in \mathbb{Z}$. **P** There is some $m \in \mathbb{Z}$ such that $0 \leq j - mn < n$. Since $a^{mn} = (a^n)^m = e$, $a^j = a^{j-mn}$, and

$$\phi_k(a^j) = \phi_k(a^{j-mn}) = a^{(j-mn)k} = a^{jk}a^{-mnk} = a^{jk}. \ \mathbf{Q}$$

It follows that if $0 \leq i, j < n$ then

$$\phi_k(a^i a^j) = \phi_k(a^{i+j}) = a^{(i+j)k} = a^{ik}a^{jk} = \phi_k(a^i)\phi_k(a^j),$$

so that $\phi_k : G \to G$ is a homomorphism.

We also find that $\phi_k\phi_l = \phi_{kl}$ for all k, $l \in \mathbb{Z}$. **P** If $i \in \mathbb{Z}$, then

$$\phi_k(\phi_l(a^i)) = \phi_k(a^{il}) = a^{ikl} = \phi_{kl}(a^i).$$

If $\phi : G \to G$ is any homomorphism, then there is some k such that $0 \le k < n$ and $\phi = \phi_k$. **P** $\phi(a) = a^k$ for some k such that $0 \le k < n$; now $\phi(a^i) = (\phi(a))^i = (a^k)^i = a^{ik}$ for every i, so $\phi = \phi_k$. **Q**

Now $\phi_k \in \operatorname{Aut} G$ iff k and n have no common factor. **P** The kernel of ϕ_k is

$$\{a^i : \phi_k(a^i) = e\} = \{a^i : a^{ik} = e\} = \{a^i : ik \text{ is a multiple of } n\}.$$

Now if k and n have no common factor, ik is a multiple of n iff i is a multiple of n, so $\ker \phi_k = \{e\}$; while conversely, if k and n have a common factor $j > 1$, then $a^i \in H$ where $i = n/j$, so $\ker \phi_k \ne \{e\}$. What this means is that

$$k \text{ and } n \text{ have no common factor} \iff \ker \phi_k = \{e\}$$
$$\iff \phi_k \text{ is injective}$$

(remember that a homomorphism is injective iff its kernel is trivial)

$$\iff \phi_k \text{ is bijective}$$

(because G is finite, so any function from G to itself is bijective iff it is injective)

$$\iff \phi_k \in \operatorname{Aut} G.$$ **Q**

Thus we can identify $\operatorname{Aut} G$ with $\{\phi_k : k \in \mathbb{Z}_n^*\}$, where $\mathbb{Z}_n^* = \{k : 0 \le k < n,\ k \text{ and } n \text{ have no common factor}\}$. To see what the multiplication is, note that if k, $l \in \mathbb{Z}_n^*$ then $\phi_k \phi_l = \phi_{kl}$. Of course kl can be greater than n, but if we look instead at $j = k \times_n l$, where $\times_n$ is multiplication modulo n, there is an $m \in \mathbb{N}$ such that $j = kl - mn$, so that

$$\phi_{kl}(a) = a^{kl} = a^j a^{mn} = a^j$$

and $\phi_{kl} = \phi_j$. Thus the multiplication of $\operatorname{Aut} G$ corresponds to multiplication mod n in $\mathbb{Z}_n^*$.

In particular, $\operatorname{Aut} G$ is abelian.

It is the case that if n is prime then $\mathbb{Z}_n^* = \{1, 2, \dots, n-1\}$ is cyclic; this takes a bit of proving. For an example in which $\mathbb{Z}_n^*$ is not cyclic, try $n = 8$; we have $\mathbb{Z}_8^* \cong K_4$.

Example: D_4 If we take the standard generators ρ, σ of D_4, so that $\rho^4 = \sigma^2 = e$ and $\sigma\rho\sigma^{-1} = \rho^{-1}$, then the centre is $C = \{e, \rho^2\}$, so that $J \cong D_4/C$ has 4 members. To identify the group J, observe that $x^2 \in C$ for every $x \in D_4$ (because $(\sigma\rho^i)^2 = e$ for every i, while $\rho^2 = (\rho^3)^2 = \rho^2$ and $(\rho^2)^2 = e$), so $z^2 = e$ for every $z \in G/C$; this means that $D_4/C \cong K_4$.

Next, $\operatorname{Aut} D_4 \cong D_4$. **P** If $\phi \in \operatorname{Aut} D_4$, then $\phi(e) = e$ and $\phi[C] = C$, so $\phi(\rho^2) = \rho^2$. Let $Q = \{\sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$ be the other four members of D_4 of order 2. Then $\phi(a) \in Q$ for every $a \in Q$. What this means is that $\operatorname{Aut} D_4$ acts on Q. Because every element of D_4 can be expressed as a product of elements of Q, this action is faithful (that is, if ϕ, $\psi \in \operatorname{Aut} G$ and $\phi(a) = \psi(a)$ for every $a \in Q$, then $\phi = \psi$), and $\operatorname{Aut} D_4$ can be identified with a subgroup of the group S_Q of bijections from Q to itself. If we arrange the elements of Q in order around a square, we see that every element of $\operatorname{Aut} D_4$ leaves opposite corners as opposite corners (because it leaves ρ^2 unmoved), so $\operatorname{Aut} D_4$ corresponds to a subgroup of D_4. To see that it corresponds to the whole of D_4, observe that the defining relations remain true of ρ and $\sigma\rho$ (since $(\sigma\rho)^2 = e$ and $(\sigma\rho)\rho(\sigma\rho)^{-1} = \rho^{-1}$), so there is a $\psi_1 \in \operatorname{Aut} G$ with $\psi_1(\rho) = \rho$, $\psi_1(\sigma) = \sigma\rho$, corresponding to a $90°$ rotation of Q; and also that $\hat{\sigma}(\sigma\rho^j) = \sigma\rho^{-j}$, so that $\hat{\sigma}$ corresponds to a reflection in the diagonal $(\sigma, \sigma\rho^2)$. So $\operatorname{Aut} D_4$ corresponds to the whole of D_4. **Q**

Example: $S_3 \cong D_3$ The centre of S_3 is $C = \{e\}$, so $J \cong S_3/C \cong S_3$. In fact $J = \operatorname{Aut} S_3$. **P** Consider the three transpositions in S_3. These are the elements of order 2, so must be permuted by any automorphism of S_3. Also any element of S_3 is a product of transpositions, so an automorphism is determined by its action on the transpositions, and there cannot be more than $3! = 6$ automorphism. As $\#(J) = \#(S_3) = 6$, J must be the whole of $\operatorname{Aut} S_3$.

Theorem Suppose that $n \ge 4$ and $n \ne 6$.

(a) The centre of A_n is $\{e\}$. The automorphism group of A_n is isomorphic to S_n; $J \lhd \operatorname{Aut} A_n$ corresponds to $A_n \lhd S_n$.

(b) The centre of S_n is $\{e\}$. Every automorphism of S_n is an inner automorphism; $\operatorname{Aut} S_n \cong S_n$.

idea of proof (not examinable)

(a) For each $i \le n$, set $H_i = \{\rho : \rho \in A_n,\ \rho(i) = i\}$. Then H_i is a subgroup of A_n (being the stabilizer of i under the natural action of A_n on $\{1, 2, \dots, n\}$. Set $\mathcal{H} = \{H_i : 1 \le i \le n\}$.

key fact For any $\phi \in \operatorname{Aut} A_n$, $\phi[H] \in \mathcal{H}$ for every $H \in \mathcal{H}$.

(This is where we need to know that $n \ne 6$.) Assuming this, the rest is not too hard. We have an action of $\operatorname{Aut} A_n$ on $\{1, \dots, n\}$ defined by setting $\phi \bullet i = j$ if $\phi[H_i] = H_j$. (We have to check is that $(\phi \circ \psi)[H] = \phi[\psi[H]]$ for all ϕ, $\psi \in \operatorname{Aut} A_n$ and every $H \in \mathcal{H}$, but in fact this is true for all functions ϕ, $\psi : A_n \to A_n$ (not just automorphisms) and for all sets $H \subseteq A_n$ (not just these particular subgroups). This action corresponds to a homomorphism $\theta : \operatorname{Aut} A_n \to S_n$, where $\theta(\phi)(i) = j$ if $\phi \bullet i = j$, that is, $\phi[H_i] = H_j$; we need to show that this is bijective.

If $\sigma \in S_n$, there is a corresponding function $\tilde\sigma : A_n \to A_n$ defined by saying that $\tilde\sigma(\rho) = \sigma\rho\sigma^{-1}$ for $\rho \in A_n$ (because $A_n \lhd S_n$). It is easy to check that $\tilde\sigma$ always belongs to $\operatorname{Aut} A_n$ (just as in the proof that inner automorphisms are automorphisms, even though in this case σ need not belong to A_n). Now if $\sigma \in S_n$ and $i \le n$ and $\rho \in A_n$,

$$\begin{aligned} \rho \in H_i &\iff \rho(i) = i \\ &\iff \sigma\rho\sigma^{-1}\sigma(i) = \sigma(i) \iff \sigma\rho\sigma^{-1} \in H_{\sigma(i)}. \end{aligned}$$

So

$$\tilde\sigma[H_i] = \sigma H_i \sigma^{-1} = H_{\sigma(i)},$$

that is, $\theta(\tilde\sigma)(i) = \sigma(i)$. Since this is true for every i, $\theta(\tilde\sigma) = \sigma$. It follows that θ is surjective.

The next fact we need is that if $\phi \in \operatorname{Aut} A_n$ and $\sigma \in A_n$, then $\phi\tilde\sigma\phi^{-1} = \phi(\sigma)^\sim$; this is part of the proof that the inner automorphisms of A_n form a normal subgroup of A_n. From this we can deduce that θ is injective. **P** Suppose that $\phi \in \ker(\theta)$, that is, that $\theta(\phi)$ is the identity of S_n. Then

$$\begin{aligned} \phi(\sigma) &= \theta(\phi(\sigma)^\sim) = \theta(\phi\tilde\sigma\phi^{-1}) \\ &= \theta(\phi)\theta(\tilde\sigma)\theta(\phi)^{-1} = \sigma. \end{aligned}$$

As this is true for every σ, ϕ is the identity ι of $\operatorname{Aut} A_n$. This shows that θ has kernel $\{\iota\}$ and is injective. **Q**

So the homomorphism $\theta : \operatorname{Aut} A_n \to S_n$ is both surjective and injective and is an isomorphism. We see incidentally that this shows that $\operatorname{Aut} A_n = \{\tilde\sigma : \sigma \in S_n\}$; every automorphism of A_n corresponds to the action of a member of S_n, and $\sigma \mapsto \tilde\sigma : S_n \to \operatorname{Aut} A_n$ is an isomorphism. Of course this includes the isomorphism $\sigma \mapsto \tilde\sigma : A_n \to J$ between A_n and the set of inner automorphisms.

(b) To determine the automorphism group of S_n, start by observing that the centre of S_n is $\{e\}$, so that S_n is isomorphic to the group of inner automorphisms of S_n. Next, because A_n is the only subgroup of S_n of order $\frac{n!}{2}$, $\psi[A_n] = A_n$ for every $\psi \in \operatorname{Aut} S_n$, and we have a homomorphism $\chi : \operatorname{Aut} S_n \to \operatorname{Aut} A_n$ defined by saying that $\chi(\psi)$ is the restriction $\phi{\restriction}A_n$ of ψ to A_n for every $\phi \in \operatorname{Aut} S_n$. If $\sigma \in S_n$ and $\hat\sigma$ is the corresponding member of $\operatorname{Aut} S_n$, $\chi(\hat\sigma)$ is just $\tilde\sigma$ as defined in the proof of (a). Since every member of $\operatorname{Aut} A_n$ is of the form $\tilde\sigma$ for some $\sigma \in S_n$, χ is surjective.

χ is injective. **P** Suppose that $\psi \in \operatorname{Aut} S_n$ and $\chi(\psi)$ is the identity of $\operatorname{Aut} A_n$, that is, $\chi(\psi)(\rho) = \rho$ for every $\rho \in A_n$. If $\sigma \in S_n$, then $\psi\hat\sigma\psi^{-1} = \widehat{\psi(\sigma)}$, so

$$\begin{aligned} \psi(\sigma)^\sim &= \chi(\widehat{\psi(\sigma)}) = \chi(\psi)\chi(\hat\sigma)\chi(\psi)^{-1} \\ &= \chi(\hat\sigma) = \tilde\sigma \end{aligned}$$

in $\operatorname{Aut} A_n$. But the map $\sigma \mapsto \tilde\sigma : S_n \to \operatorname{Aut} A_n$ is an isomorphism, and in particular is injective, so we must have $\psi(\sigma) = \sigma$ for every $\sigma \in S_n$, and ψ is the identity of $\operatorname{Aut} S_n$. This shows that the kernel of χ is the trivial subgroup and χ is injective. **Q**

So $\chi : \operatorname{Aut} S_n \to \operatorname{Aut} A_n$ is an isomorphism and every automorphism of S_n is an inner automorphism.

This completes the proof, except for the proof of the 'key fact'.

The case $n = 4$ If $n = 4$, then we can describe the subgroups H_i directly:

$$H_1 = \{e, (\overleftarrow{234}), (\overleftarrow{243})\}, \quad H_2 = \{e, (\overleftarrow{134}), (\overleftarrow{143})\},$$

$$H_3 = \{e, (\overleftarrow{124}), (\overleftarrow{142})\}, \quad H_4 = \{e, (\overleftarrow{123}), (\overleftarrow{132})\}.$$

These use up all the 8 three-cycles in A_4, so they are all four of the subgroups of A_4 of order 3, and must be shuffled by any automorphism of A_4.

The case $n = 5$ If $n = 5$, look at the 3-cycles in A_5. These are the only elements of order 3 in A_5, so any automorphism of A_5 must take 3-cycles to 3-cycles. Next, we can tell whether two 3-cycles belong to a single H_i, because if they don't, then their product is a 5-cycle and has order 5, while if they do, their product is either the identity (order 1) or a 3-cycle (order 3) or a double-transposition (order 2). What this means is that we can group the 30 elements of A_5 with order 3 into 5 collections of 8, each bunch of 8 being characterized by none of their products having order 5; and a subgroup of A_5 belongs to $\mathcal{H}$ iff it is generated by one of these collections. So automorphisms of A_5 shuffle $\mathcal{H}$, and the argument above applies.

Pólya's theorem (non-examinable)

We have a finite set X, a finite set C of 'colours', and a subgroup G of the group S_X of permutations of X. A **colouring** of X is a function $f : X \to C$. For each colouring f, its **weight** is $W(f) = \prod_{x \in X} f(x)$.

Example If $X = \{x, y, z, t\}$, $C = \{c, d\}$, $f(x) = f(y) = f(t) = c$ and $f(z) = d$ then $W(f) = c^3 d$.

We count two colourings f and g as 'the same' if there is some $\pi \in G$ such that $g = f\pi$. Now the problem is: for any given weight w, how many 'different' colourings are there with that weight?

Example Suppose we have a cube. How many different ways are there of painting it such that three faces are red, two are blue and one is green, counting two colourings as the same if we can turn one into the other by rotating the cube?

Here $C = \{r, b, g\}$, X is the six-element set of faces of the cube, and G is the 24-element group of rotations of the cube, regarded as permutations of its faces; and we are looking for colourings with weight $r^3 b^2 g$.

Now we need to be a little clearer about this notion of 'the same' and 'different'. The first point to observe is that if F is the set of colourings, that is, the set of all functions from X to C, then we have an action of G on F defined by the formula

$$\pi \bullet f = f\pi^{-1} \text{ for } f \in F, \pi \in G.$$

(Check! (α) If $f : X \to C$ is any function and $\pi : X \to X$ is a permutation, then $\pi^{-1} : X \to X$ and $f\pi^{-1} : X \to C$ are functions, so $\pi \bullet f \in F$ whenever $f \in F$ and $\pi \in G$. (β) If $f \in F$ and π, $\sigma \in G$ then

$$\pi \bullet (\sigma \bullet f) = \pi \bullet (f\sigma^{-1}) = (f\sigma^{-1})\pi^{-1} = f(\sigma^{-1}\pi^{-1}) = f(\pi\sigma)^{-1} = (\pi\sigma) \bullet f.$$

(γ) Writing ι for the identity of G,

$$\iota \bullet f = f\iota^{-1} = f$$

for every $f \in F$.) We therefore have an equivalence relation on X with the orbits of this action as its equivalence classes; two colourings are 'the same' if they belong to the same orbit of the action, and what we are counting is orbits. Next, it is helpful to note straight away that $W(\pi \bullet f) = W(f)$ for every $f \in F$ and $\pi \in G$; this is because

$$W(\pi \bullet f) = W(f\pi^{-1}) = \prod_{x \in X} f(\pi^{-1}(x)) = \prod_{x \in X} f(x) = W(f);$$

the point is that (because π is a bijection) the product $\prod_{x \in X} f(\pi^{-1}(x))$ is just the same as the product $\prod_{x \in X} f(x)$ with the terms in a different order.

All this is really saying is that if your cube has three red faces, two blue faces and one green face, and you rotate it, it still has three red faces, two blue faces and one green face, though you may have found them in a different order.

This means that for any weight w, the set $F_w = \{f : f \in F, W(f) = w\}$ of colourings with that weight is a union of orbits under the action.

The next concept we need is that of 'inventory polynomial'. If $A \subseteq F$ is any set, its **inventory polynomial** is $\sum_{f \in A} W(f)$. Note that this is a kind of homogeneous polynomial of degree $\#(X)$ in the 'variables' c, $d \ldots$ belonging to C.

What we are going to try to do is to calculate the inventory polynomial $I(A)$ of a set $A \subseteq F$ which contains just one member of each orbit. If we can do this, then the number of different colourings with a given weight w will be just $\#(\{f : f \in A, W(f) = w\})$, that is, the coefficient of w in $I(A)$.

The first step is to calculate the inventory polynomial of a particular kind of set. For $\pi \in G$, consider the set $E_\pi = \{f : f \in F, \pi \bullet f = f\}$, the set of colourings fixed under the action of π. Then we find that

$$I(E_\pi) = \prod_{Z \text{ an orbit of } \pi} \sum_{c \in C} c^{\#(Z)}.$$

P (We are coming to the hard bits.) Remember that π is a permutation of the set X. Its orbits therefore are the sets of the form $\{\pi^n(x) : n \in \mathbb{N}\}$ where $x \in X$. If we represent π in cycle notation as

$(\overleftarrow{x_1\,x_2\,\dots\,x_k})(\overleftarrow{x_{k+1}\,\dots\,x_{k+l}})(\overleftarrow{x_{k+l+1}\,\dots})\dots$, remembering to include any one-cycles so that every element of X is listed just once, then the sizes of the orbits will be k, l, $\dots$ and the expression

$$\prod_{Z\text{ an orbit of }\pi}\sum_{c\in C}c^{\#(Z)}$$

will start with the terms $\sum_{c\in C}c^k\cdot\sum_{c\in C}c^l\cdot\dots$. Now, why is this equal to $I(E_\pi)$? Note first that if $f\in F$ then

$$\begin{aligned}
f\in E_\pi &\iff \pi\bullet f=f\\
&\iff f\pi^{-1}=f\\
&\iff f(x)=f(y)\text{ whenever }\pi(x)=y\\
&\iff f\text{ is constant on each orbit of }\pi.
\end{aligned}$$

So, writing $Z_1,\dots,Z_m$ for the orbits of π, $f\in E_\pi$ iff there are $c_1,\dots,c_m\in C$ (not necessarily different) such that $f(x)=c_i$ whenever $x\in Z_i$, for every $i\le m$; and in this case $W(f)=c_1^{\#(Z_1)}c_2^{\#(Z_2)}\dots c_m^{\#(Z_m)}$. Next, for each possible assignment $c_1,\dots,c_m$ of colours, there is just one f such that $f(x)=c_i$ whenever $i\le m$ and $x\in Z_i$. So

$$\begin{aligned}
I(E_\pi)&=\sum_{f\in E_\pi}W(f)\\
&=\sum_{c_1,\dots,c_m\in C}c_1^{\#(Z_1)}\dots c_m^{\#(Z_m)}\\
&=\sum_{c_1\in C}c_1^{\#(Z_1)}\sum_{c_2\in C}c_2^{\#(Z_2)}\dots\sum_{c_m\in C}c_m^{\#(Z_m)}\\
&=\sum_{c\in C}c^{\#(Z_1)}\sum_{c\in C}c^{\#(Z_2)}\dots\sum_{c\in C}c^{\#(Z_m)}\\
&=\prod_{i=1}^{m}\sum_{c\in C}c^{\#(Z_i)}\\
&=\prod_{Z\text{ an orbit of }\pi}\sum_{c\in C}c^{\#(Z)},
\end{aligned}$$

which is what I said. **Q**

We now need to remember the fundamental theorem on orbits and stabilizers for any action. If, for $f\in F$, we write $\mathrm{Orb}(f)=\{\pi\bullet f:\pi\in G\}$ for its orbit and $\mathrm{Stab}(f)=\{\pi:\pi\bullet f=f\}$ for its stabilizer, then $\#(\mathrm{Orb}(f))\cdot\#(\mathrm{Stab}(f))=\#(G)$, that is,

$$\frac{1}{\#(\mathrm{Orb}(f))}=\frac{1}{\#(G)}\cdot\#(\mathrm{Stab}(f))=\frac{1}{\#(G)}\cdot\#(\{\pi:f\in E_\pi\}).$$

Now I put it that way because if we pick a set $A\subseteq F$ containing exactly one point in each orbit under the action of G, then (because the function W is constant on each orbit) then

$$I(A)=\sum_{f\in A}W(f)=\sum_{f\in F}\frac{1}{\#(\mathrm{Orb}(f))}W(f).$$

In this form we are now ready for the assault:

$$
\begin{aligned}
I(A) &= \sum_{f\in F} \frac{1}{\#(\mathrm{Orb}(f))} W(f) \\
&= \sum_{f\in F} \frac{1}{\#(G)} \cdot \#(\{\pi : f \in E_\pi\}) W(f) \\
&= \frac{1}{\#(G)} \sum_{f\in F} \#(\{\pi : f \in E_\pi\}) W(f) \\
&= \frac{1}{\#(G)} \sum_{w\in W} \sum_{f\in F_w} \#(\{\pi : f \in E_\pi\}) w \\
&= \frac{1}{\#(G)} \sum_{w\in W} \#(\{(f,\pi) : f \in F_w \cap E_\pi\}) w \\
&= \frac{1}{\#(G)} \sum_{w\in W} \sum_{\pi\in G} \#(F_w \cap E_\pi) w \\
&= \frac{1}{\#(G)} \sum_{\pi\in G} \sum_{w\in W} \#(F_w \cap E_\pi) w \\
&= \frac{1}{\#(G)} \sum_{\pi\in G} I(E_\pi) \\
&= \frac{1}{\#(G)} \sum_{\pi\in G} \prod_{Z \text{ an orbit of } \pi} \sum_{c\in C} c^{\#(Z)}.
\end{aligned}
$$

And this is Pólya's theorem! Let me gather it up in a proper statement:

Pólya's Theorem Let X be a finite set, G a subgroup of the group of permutations on X, and C a finite set of colours. In the polynomial

$$
\frac{1}{\#(G)} \sum_{\pi\in G} \prod_{Z \text{ an orbit of } \pi} \sum_{c\in C} c^{\#(Z)}
$$

(called the **pattern inventory**), the coefficient of any term $c_1^{k_1} c_2^{k_2} \ldots c_r^{k_r}$ is the number of different ways of colouring k_1 points of X with colour c_1, k_2 points with colour c_2, and so on, counting two colourings as different if one cannot be turned into the other by a permutation in G.

Example To find the number of different colourings of a cube (under rotations) which give it three red faces, two blue faces and one green face:

Here the set X has 6 members, $C = \{r, b, g\}$ and G is the set of rotations of the cube, interpreted as permutations of the set X. For the calculation, we need to classify the members of G, as follows:

one identity element, six orbits of 1 member each; $I(E_\iota) = (r + b + g)^6$;

6 rotations through 90° about a short axis; each has one orbit of 4 members, 2 orbits of 1 member; $I(E_\pi) = (r^4 + b^4 + g^4)(r + b + g)^2$;

3 rotations through 180° about a short axis; each has 2 orbits of 2 members and 2 orbits of 1 member; $I(E_\pi) = (r^2 + b^2 + g^2)^2(r + b + g)^2$;

8 rotations through 120° about a long diagonal; each has 2 orbits of 3 members each; $I(E_\pi) = (r^3 + b^3 + g^3)^2$;

6 rotations through 180° about an axis bisecting two opposite edges; each has 3 orbits of 2 members; $I(E_\pi) = (r^2 + b^2 + g^2)^3$;

(How to be sure we have everything? First check is by the count: $1 + 6 + 3 + 8 + 6 = 24$. You also have to be sure that there is no double counting. The different types have to be really different because they have different cycle structures. Within each type you still need to check that (e.g.) different permutations have different fixed faces.)

Putting these together, we get our formula

$$
\begin{aligned}
I(A) &= \frac{1}{24}\big((r+b+g)^6 + 6(r^4+b^4+g^4)(r+b+g)^2 + 3(r^2+b^2+g^2)^2(r+b+g)^2 \\
&\qquad + 8(r^3+b^3+g^3)^2 + 6(r^2+b^2+g^2)^3\big) \\
&= r^6+b^6+g^6+rb^5+rg^5+r^5b+r^5g+bg^5+b^5g \\
&\quad + 2(r^2b^4+r^2g^4+r^4b^2+r^4g^2+b^2g^4+b^4g^2) \\
&\quad + 2(r^3b^3+r^3g^3+b^3g^3) + 2(rbg^4+r^4bg+rb^4g) + 6r^2b^2g^2 \\
&\quad + 3(r^3b^2g+r^2b^3g+r^3bg^2+r^2bg^3+rb^3g^2+rb^2g^3)
\end{aligned}
$$

(this last step is strictly for `Maple`; but if you did have to do it by hand, there are lots of crosschecks, because you must get whole numbers out after the division by 24, and also the coefficient of r^2bg^3 must be the same as the coefficient of rb^3g^2). So what we find is that (for instance)

there is just one colouring with all faces red;

there are just two colourings with two faces blue and the others green (according to whether the blue faces are together or separate)

there are 3 colourings with three red faces, 2 blue faces and 1 green face (according to whether one of the blue faces is opposite the green face, and if not, according to whether they are opposite each other or adjacent)

there are 6 colourings with two faces of each colour.

Example Let X be the set of vertices of a regular tetrahedron, G the set of rotations of X, and $C = \{r, b, g, y\}$. Then we have the following types of permutation:

one identity permutation; 4 orbits of one element each; $I(E_\iota) = (r+b+g+y)^4$;

8 rotations through 120°; 1 orbit of 3 elements, 1 orbit of one element; $I(E_\pi) = (r^3+b^3+g^3+y^3)(r+b+g+y)$;

3 rotations through 180° about an axis bisecting two opposite edges; 2 orbits of 2 elements each; $I(E_\pi) = (r^2+b^2+g^2+y^2)^2$.

So the pattern inventory is

$$
\begin{aligned}
I(A) &= \frac{1}{12}\big((r+b+g+y)^4 + 8(r^3+b^3+g^3+y^3)(r+b+g+y) \\
&\qquad + 3(r^2+b^2+g^2+y^2)^2\big) \\
&= 2rbgy + r^2gy + r^2by + r^2bg + b^2gy + rb^2g + rb^2y + rbg^2 \\
&\qquad + rby^2 + rg^2y + rgy^2 + bg^2y + bgy^2 \\
&\quad + r^3b + r^3g + r^3y + rb^3 + rg^3 + ry^3 + bg^3 + by^3 + b^3g + b^3y + gy^3 + g^3y \\
&\quad + r^2b^2 + r^2g^2 + r^2y^2 + b^2g^2 + b^2y^2 + g^2y^2 + r^4 + b^4 + g^4 + y^4.
\end{aligned}
$$

What this tells us is that there are *two* ways of colouring the vertices of the tetrahedron with all four colours; but there is only *one* way of colouring them with three colours, once you have decided which colour is repeated.

If you simply want to count all the colourings using these four colours you can put $r = b = g = y$ in the above expression and get

$$\tfrac{1}{12}(4^4 + 8\cdot 4^2 + 3\cdot 4^2) = 36.$$

If you put $y = 0$ in the above expression what you get is

$$
\begin{aligned}
I(A) &= \frac{1}{12}\big((r+b+g)^4 + 8(r^3+b^3+g^3)(r+b+g) + 3(r^2+b^2+g^2)^2 \\
&= r^2bg + rb^2g + rbg^2 + r^3b + r^3g + rb^3 + rg^3 + bg^3 + b^3g \\
&\quad + r^2b^2 + r^2g^2 + b^2g^2 + r^4 + b^4 + g^4,
\end{aligned}
$$

simply missing out all the terms with a y in them; that is, no longer counting any of the colourings which use yellow.

Example Now repeat the above example, allowing reflections as well as rotations. This will add the following permutations to G:

6 transpositions; 1 orbit of 2 members, 2 orbits of 1 member; $I(E_\pi) = (r^2 + b^2 + g^2 + y^2)(r + b + g + y)^2$;

6 four-cycles; 1 orbit of 4 members; $I(E_\pi) = r^4 + b^4 + g^4 + y^4$;

giving a pattern inventory

$$
\begin{aligned}
I(A) = \frac{1}{24}\big(&(r+b+g+y)^4 + 8(r^3+b^3+g^3+y^3)(r+b+g+y)\\
&+ 3(r^2+b^2+g^2+y^2)^2 + 6(r^2+b^2+g^2+y^2)(r+b+g+y)^2\\
&+ 6(r^4+b^4+g^4+y^4)\big)\\
= rbgy &+ r^2gy + r^2by + r^2bg + b^2gy + rb^2g + rb^2y + rbg^2\\
&+ rby^2 + rg^2y + rgy^2 + bg^2y + bgy^2\\
&+ r^3b + r^3g + r^3y + rb^3 + rg^3 + ry^3 + bg^3 + by^3 + b^3g + b^3y + gy^3 + g^3y\\
&+ r^2b^2 + r^2g^2 + r^2y^2 + b^2g^2 + b^2y^2 + g^2y^2 + r^4 + b^4 + g^4 + y^4.
\end{aligned}
$$

(The only difference is that you can no longer tell the four- colourings apart.)

Example Suppose we want to count the different graphs on a set V of four vertices. This corresponds to colouring the set X of six potential edges in two colours y ('yes') and n ('no'). We count two graphs as the same if we can get from one to the other by shuffling vertices. So we are looking at the group S_V of all 24 permutations of V. But for our calculations here, we have to interpret this as a subgroup of S_X when we look at the orbit sizes. So we need an extra column in our list of permutations in G, describing their actions on V as well as their actions on X. The list is

one identity permutation; on X, 6 orbits with one edge in each; $I(E_\iota) = (y+n)^6$;
6 transpositions of vertices; on X, 2 orbits of 2 edges, 2 of 1 edge; $I(E_\pi) = (y^2+n^2)^2(y+n)^2$;
3 double-transpositions of vertices; 2 orbits of 2 edges, 2 of 1 edge; $I(E_\pi) = (y^2+n^2)^2(y+n)^2$;
8 three-cycles of vertices; 2 orbits of 3 edges each; $I(E_\pi) = (y^3+n^3)^2$;
6 four-cycles of vertices; 1 orbit of 4 edges, 1 orbit of 2 edges; $I(E_\pi) = (y^4+n^4)(y^2+n^2)$.

So the pattern inventory is

$$
\begin{aligned}
I(A) &= \tfrac{1}{24}\big((y+n)^6 + 9(y^2+n^2)^2(y+n)^2 + 8(y^3+n^3)^2 + 6(y^4+n^4)(y^2+n^2)\big)\\
&= y^6 + y^5n + 2y^4n^2 + 3y^3n^3 + 2y^2n^4 + yn^5 + n^6,
\end{aligned}
$$

and we have one graph with 6 edges, one with five edges, two with four edges, three with three edges, two with two edges, one with one edge and one with no edges. (Draw them!)