

Introduction

The symmetry group D_3 of the triangle consists of 6 elements: the **identity**, I ; **rotation** through 120° , R ; **rotation** through 240° , R^2 and 3 '**flips**', $S_A (= S)$, S_B , and S_C . It is easy to see that $R^3 = I$. But *what is RS?* We interpret this as "**first do R, then do S**". From the

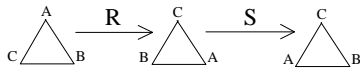
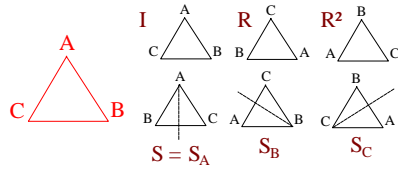
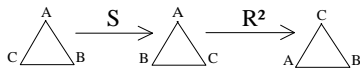


diagram on the left, we see that this produces S_B . But $S_B^2 = I$, so that $(RS)^2 = I$. Can we get S_B other than as RS ?



We could try SR or SR^2 (as shown), or we could *manipulate* $(RS)^2 = I$, $RSRS = I$, \times on **right** by S to give $RSR = S$ (because $S^2 = I$), \times on **right** by $R^{-1} = R^2$ to give $RS = SR^2$. Similarly, $I = R(SR)S$, $SR = R^2S$. So we have $SR = R^2S$ and $SR^2 = RS$. We can get all the elements of D_3 by multiplying S 's and R 's. And, we can work out **products** of such. *Summary:* $D_3 = \{I, R, R^2, S, RS, R^2S\}$. As a "game", try to see what some *other words* in S and R give. Example: $SR^2S^{-1}R^{25}SR^4 = SR^2SRSR = SR^2 = RS$.

30th January 2001

This suggests that *any element of D_3* can be written as a **product** of R 's and S 's in the form R^iS^j , where $0 \leq i \leq 2$, and $0 \leq j \leq 1$. We have a *presentation of this group as follows*: $\langle r, s; r^3=1, s^2=1, (rs)^2=1 \rangle$, where r and s are the **generators** and we have 3 **relations**. **Lemma:** Any word in R 's and S 's can be *reduced* using $R^3 = I$, $S^2 = I$, and $(RS)^2 = I$ into one of the forms R^iS^j for $i = 0, 1, 2$, and $j = 0, 1$.

Proof (fairly *informal*): Suppose that w is a word of R 's, S 's, R^{-1} 's and S^{-1} 's. Call the *number of symbols used the length of w* . If the *length* of w is 0, then $w = I = R^0S^0$. If the *length* of w is 1, then $w = R, S, R^{-1}$ or S^{-1} . If $w = R$, then $i = 1$ and $j = 0$. **OK.** If $w = S$, then $i = 0$ and $j = 1$. **OK.** If $w = R^{-1}$, then $R^3 = I \Rightarrow R^{-1} = R^2$, i.e. $w \rightarrow R^2$, with $i = 2$ and $j = 0$. **OK.** (*Note: read \rightarrow as "reduces to"*). If $w = S^{-1}$, then $S^2 = I \Rightarrow S^{-1} = S$, i.e. $w \rightarrow S$, with $i = 0$ and $j = 1$. **OK.**

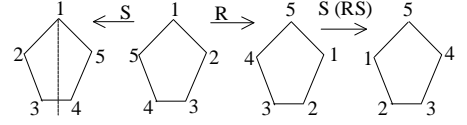
Assume now that we can reduce *any word w of length n* to one of the 6 forms R^iS^j . If w' is of length $n+1$, then $w' = wx$, where w is a word of length n , and $x \in \{R, S, R^{-1}, S^{-1}\}$. But $w \rightarrow R^iS^j$ for some i and j , as shown *above*. So $w' = wx \rightarrow R^iS^jx$. We now have to *effectively check* that any of the 24 words R^iS^jx can be **reduced** to a "*normal*" form.

We can *reduce* further: $S = S^{-1}$, so that if $x = S^{-1}$, and we have **already** done S , then we would be repeating ourselves. Similarly, if R^iS^jR reduces to R^kS^l , then doing it **twice** reduces $R^iS^jR^2$ to *normal* form, i.e. reduces $R^iS^jR^{-1}$ to **normal** form. This leaves R^iS^jR and R^iS^jS to *handle*. If $j = 0$, then we have $R^iS^jR = R^{i+1}$, which is *all right* unless $i = 2$. But $I = R^0S^0$ if $r = 2$. **OR**, we have R^iS — which is already in the *right* form. If $j = 1$, then we have $R^iSS = R^i$. **OK.** **OR**, we have $R^iSR = R^iR^2S = R^{i+2}S \rightarrow$ *normal* form.

Exercises

(1) (a) The symmetry group D_5 of the regular **pentagon** has 10 elements: I , 4 *rotations*, and 5 *flips*. Let R be the rotation clockwise through $2\pi/5$, and let S be the flip about the *vertical* axis of symmetry. Note that $R^5 = I$, $S^2 = I$, and that RS is a “flip” about another axis, so that $(RS)^2 = I$. Show that using the **algebraic** information alone, you can write any word in the R 's and S 's in the form $R^i S^j$, with *suitable ranges for i and j* .

A: We have $I, R, R^2, R^3, R^4, S_1, S_2, S_3, S_4,$ and S_5 ($S = S_1$). As you can *see*, RS produces S_3 . Because $(S_3)^2 = I$, then $(RS)^2 = I$. **I. Presentation:** $D_5 = \langle r, s : r^5 = 1, s^2 = 1, (rs)^2 = 1 \rangle$. The *normal form* in this instance is $R^i S^j$, where $0 \leq i \leq 4$, and $0 \leq j \leq 1$. Now for the proof that *any word* in the R 's and S 's can be written in **normal form**. As before, if the length is *zero* or *one*, we are **OK**.



Assume that we can reduce *any word w of length n* to one of the 10 forms $R^i S^j$. If $w' = wx$ is of length $n+1$, then $w' = R^i S^j x$, where $x \in \{R, S, R^{-1}, S^{-1}\}$. We have to check that the **40 words** $R^i S^j x$ can be reduced to *normal form*. As $S = S^{-1}$, we have only **30 words** to consider. Similarly, $R^{-1} = R^4$, so reducing $R^i S^j R$ to $R^k S^l$ 4 times shows that we can **reduce** $R^i S^j R^{-1}$ to *normal form*. This leaves $R^i S^j R$ and $R^i S^j S$ to **handle** (20 cases). $j = 0$: R^{i+1} (**OK**), **OR** $R^i S$ (**OK**). 10 left to consider. $j = 1$: $(R^i S)S = R^i$ (**OK**), **OR** $R^i SR$. What is SR ? Now $(RS)^2 = I$, so that $RSRS = I$, $SR = R^{-1} S^{-1}$, $SR = R^4 S$. So $R^i SR = R^i R^4 S = R^{i+4} S$, which \rightarrow *normal form*.

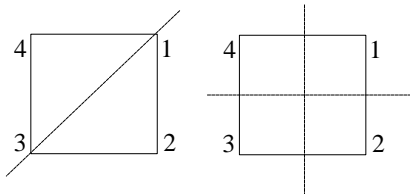
(1) (b) The group D_n is the symmetry group of the **regular n -gon**. How many elements does D_n have? Justify. Noting that a basic *rotation*, R , and a flip, S , will “generate” all the others, write down 3 “independent” relations between them, **generalising** those found for the case $n = 3$, and use them to prove that *any word* in the R 's and S 's can be reduced to $R^i S^j$ for suitable ranges of i and j .

A: D_n will have $n-1$ *rotations*, each of $2\pi/n$. Note that $R^n = I$. We will also have n *flips* for each of the n vertices. Therefore, D_n will have $2n$ **elements**. If a basic rotation, R , and a flip, S , will *generate* all the other elements of D_n , then the $2n$ elements of D_n are as follows: $I, R, R^2, \dots, R^{n-1}; S, RS, R^2S, \dots, R^{n-1}S$. The 3 “independent” relations are $R^n = I, S^2 = I$, and $(RS)^2 = I$.

So $D_n = \langle r, s : r^n = 1, s^2 = 1, (rs)^2 = 1 \rangle$. Now to prove that we can write *any word* in the R 's and S 's in the form $R^i S^j$, where $0 \leq i \leq n-1$, and $0 \leq j \leq 1$. Before we **proceed**, note that $(RS)^2 = I$; $SR = R^{-1} S^{-1}$; $SR = R^{n-1} S$. **Informal Inductive Proof:** Suppose that w is any *valid word*. If the length of w is 0, then $w = I = R^0 S^0$, **OK**. If the *length* is 1, then we have $R^i S^0, R^0 S^1, R^{-1} = R^{n-1}$, or $S^{-1} = S$, all of which are **OK**. Assume now that we can reduce *any word w of length n* to a normal form. If $w' = wx$ is of length $n+1$, where $x \in \{R, S, R^{-1}, S^{-1}\}$, then because we assume that $w \rightarrow R^i S^j$, then $w' = R^i S^j x$. We have $(2n) \times 4$ words *left to check*. But because $S = S^{-1}$, if we consider all words **ending** in S , then we will have considered all words **ending** in S^{-1} as well. Similarly, if $R^i S^j R$ reduces to $R^k S^l$, then doing this $n-1$ times reduces $R^i S^j R^{n-1}$ to *normal form*, i.e. reduces $R^i S^j R^{-1}$ to normal form. This *leaves* the $R^i S^j R$ and the $R^i S^j S$ **cases** to handle.

If $j = 0$, then we have $R^iR = R^{i+1}$, or R^iS , both of which are **OK** (if necessary, we use $R^n = I$ for the **first** expression; the **2nd** is *already* in normal form). If $j = 1$, then we have R^iSR , or R^iSS . Case 1: As $SR = R^{n-1}S$, then $R^iSR = R^iR^{n-1}S = R^{i+n-1}S$, which is **OK** using $R^n = I$ as necessary. Case 2: $R^iSS = R^i$ as $S^2 = I$, so this is **OK**. **End of Proof.**

(T. Porter's Answer): R and S seem to generate *more* elements (visually, the elements R^kS correspond to 'flips' about *other axes of symmetry*). If n is odd, then the axes of symmetry of the regular n -gon pass through a **vertex** and an **opposite edge** so that there are n of them. If n is even, axes come in **two** types: axes through a *pair of opposite vertices*, or through *opposite faces* (as shown: flip $2 \leftrightarrow 4$; and flipping $1 \leftrightarrow 4$ and $2 \leftrightarrow 3$ in diagrams 1 and 2 respectively).



Therefore, there are **n axes of symmetry** in both cases. (Problem for n even: S then is a *vertex axis flip* — will the *face axis flips* be among the RS 's — if so, how *come?*). A good justification should include a **general** case. Do not just look at **low** values of n — beware! To **prove** that there are $2n$ symmetries, you need either to *represent* R by a permutation $(1\ 2\ \dots\ n)$, and then S gets represented by $(2\ n-1)(3\ n-2)\dots$ (handle n odd and n even **separately**), or by a **rotation matrix**, and S by e.g. $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then argue. "Independent Relations": $R^n = I$, $S^2 = I$, and $(RS)^2 = I$.

Proposition: Any word can be reduced. **Proof:** We first note that $RSRS = I$, so that $SR = R^{-1}S^{-1}$. Then $R^n = I$ and $S^2 = 1$ mean that $SR = R^{n-1}S$. If a word w in the R 's and S 's is now given, then $w = R^{\alpha_1}S^{\beta_1}\dots R^{\alpha_m}S^{\beta_m}$. As $R^n = I$, and as $S^2 = I$, we can assume that the word is *rewritten* so that all α_i are in the range $0 \leq \alpha_i < n$, and that $\beta_i = 0$ or 1 . If any $\alpha_i = 0$, or if any $\beta_i = 0$, then we can *reduce further*, e.g. $R^iS^0R^kS = R^{i+k}S$. Assume that this is **done**, so that each α_i is in the range $1 \leq \alpha_i < n$, and that if *any* S occurs, then it has $\beta = 1$. If w is now in the **form** R^iS^j , we are *finished* with the reduction. If not, there is a subword SR somewhere in the **current** form of w . Replace SR by $R^{n-1}S$, and run through the *reduction* once again to get a *shorter* form (proof by induction — omitted). At each stage, m cannot **increase**, and so the process will *terminate* with all R 's to the left of S 's, and all *indices* in the required ranges.

(2) Prove that if the *order* of an element $g \in G$ is n , and if $k > 0$ satisfies $g^k = 1$, then n divides k (hint: use the *division algorithm* for the **natural** numbers). A: By *definition*, if n is the **order** of the element g , then $g^n = 1$. Further, n must be the least positive power of g such that $g^n = 1$. Using the *division algorithm for natural numbers*, we get $k = qn + r$, where $0 \leq r < n$.

So if $g^k = 1$, then $g^{qn+r} = 1$; $(g^{qn})(g^r) = 1$; $(g^n)^q(g^r) = 1$; $(1)^q(g^r) = 1$ — since $g^n = 1$ by *definition*. So $g^r = 1$ (---(1)). Now *because* $0 \leq r < n$, and **because** n is the order of g , so that there is no **positive** integer m less than n such that $g^m = 1$, then to *satisfy equation (1)*, r must be **zero**. Therefore, the remainder is *zero* in $k = qn + r$, so that n divides k exactly. **QED. (T. Porter's Answer):** Recall that the *order* of $g \in G$ is defined to be the least **positive** n such that $g^n = 1$. Suppose that $k > 0$ *satisfies* $g^k = 1$, and that g has *order* n . By *definition*, $k \geq n$, so using the **division** algorithm, there is some $q, r \in \mathbf{N}$, with $0 \leq r < n$, and $k = qn + r$. But *then* $1 = g^k = g^{qn+r} = g^{qn} \cdot g^r = (g^n)^q \cdot g^r = g^r$, *since* $g^n = 1$. As $g^r = 1$, and as $r < n$, then we **must** have $r = 0$, so that n *divides* k .

Review of Group Theory

Group: A set of elements with *multiplication*. An identity 1_G and inverses. Associativity: $(g_1g_2)g_3 = g_1(g_2g_3)$. $1_Gg = g = g1_G$. $g \in G$ gives $g^{-1} \in G$ s.t. $gg^{-1} = 1_G = g^{-1}g$ (inverses). If G is a **finite** group, then $|G|$, the *number of elements in G* , is called the order of G .

Definitions: (a) If G and H are *groups*, a function $\varphi: G \rightarrow H$ is a *group homomorphism* if for all $g_1, g_2 \in G$, $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ (---(i)), and $\varphi(1_G) = 1_H$ (---(ii)). **Note:** this *implies* that $\varphi(g^{-1}) = \varphi(g)^{-1}$. Also note that (i) \Rightarrow (ii), but (ii) is useful to note for its *usefulness*. (i) \Rightarrow (ii): If $g \in G$, then $1_Gg = g$, so that $\varphi(1_G)\varphi(g) = \varphi(1_Gg) = \varphi(g) = 1_H\varphi(g)$, i.e. $\varphi(1_G)\varphi(g) = 1_H\varphi(g)$. So multiply on the *right* by $\varphi(g)^{-1}$ to get (ii).

(b) An *element* $g \in G$ has order n if $g^n = 1$; and if $g^k = 1$ for some $k > 0$, then $k \geq n$. (c) A group G is **Abelian** if for any $g_1, g_2 \in G$, we have $g_1g_2 = g_2g_1$ (pairs of elements *commute*). Note: D_n is not commutative/*abelian* for $n \geq 3$.

Little result: Suppose that $\varphi: G \rightarrow G$ is a *homomorphism*, and that $\varphi(g) = g^2$ for all $g \in G$: then G is *abelian*! (i.e. the **squaring** function is a homomorphism if and only if G is abelian). (d) If $\varphi: G \rightarrow H$ is a *homomorphism*, then $\{g \in G \mid \varphi(g) = 1_H\}$ is a *subgroup* of G called the **kernel** of φ (**subgroup:** if H is a *subset* of a group G with operation \bullet , such that H is a group with the operation \bullet , then H is a **subgroup** of G . **Testing** for a subgroup: H is a *subgroup* of G if, and only if, (a) $xy \in H$ for each $x \in H$ and $y \in H$; (b) $e \in H$; and (c) $x^{-1} \in H$ for *each* $x \in H$).

Proof of the above result: (a) *Suppose* that $x, y \in \ker \varphi$. Then $\varphi(x) = \varphi(y) = 1_H$. It **follows** that $\varphi(xy) = \varphi(x)\varphi(y) = 1_H1_H = 1_H$, showing that $xy \in \ker \varphi$. (b) $\varphi(1_G) = 1_H$, so that $1_G \in \ker \varphi$. (c) $\varphi(x^{-1}) = \varphi(x)^{-1} = 1_H^{-1} = 1_H$, showing that $\varphi(x^{-1}) = 1_H$, and that $x^{-1} \in \ker \varphi$. It follows that $\ker \varphi$ is a *subgroup* of G . In fact, $\ker \varphi$ is a **normal** subgroup (a subgroup H of a group G is a **normal** subgroup if $x^{-1}Hx = H$ for each $x \in G$).

(e) Again, given $\varphi: G \rightarrow H$, the set $\text{Im } \varphi = \{\varphi(g) \mid g \in G\} \leq H$. ($\leq =$ “*is a subgroup of*”). Check that the **image** of φ is a subgroup: in **this** case, (a) suppose that $x, y \in \text{Im } \varphi$. Then $\varphi(a) = x$, and $\varphi(b) = y$, for *some* $a, b \in G$. Is $xy \in \text{Im } \varphi$? If it is, then there is **some** $c \in G$ s.t. $\varphi(c) = xy$. Let $c = ab$. Now $c \in G$ because $a \in G$, $b \in G$, and G is *closed under multiplication* (is a **group**). Then $\varphi(c) = \varphi(ab) = \varphi(a)\varphi(b) = xy$, **OK**. (b) $\varphi(1_G) = 1_H$, so that $1_H \in \text{Im } \varphi$, **OK**. (c) Let $x \in \text{Im } \varphi$, so that there *is an* $\alpha \in G$ s.t. $\varphi(\alpha) = x$. Is $x^{-1} \in \text{Im } \varphi$? Now $\alpha \in G \Rightarrow \alpha^{-1} \in G$. Therefore, $\varphi(\alpha^{-1}) = \varphi(\alpha)^{-1} = x^{-1} \in \text{Im } \varphi$, **OK**.

(f) If $x, y \in G$, the commutator, $[x, y]$, is defined to be $xyx^{-1}y^{-1}$. (**Beware:** some textbooks (and GAP) use $x^{-1}y^{-1}xy$). (g) If G is a **group**. and if $H \leq G$, a (*left*) coset gH in G is given by $gH = \{gh \mid h \in H\}$. This gives a *partition* of G into cosets corresponding to an equivalence relation **defined** by $g_1 \sim_H g_2$ if (and *only* if) $g_1g_2^{-1} \in H$. (**Note:** Reflexive: $g_1 \sim_H g_1$ because $g_1g_1^{-1} = 1 \in H$. Symmetric: if $g_1 \sim_H g_2$, then $g_1g_2^{-1} \in H$, so that $g_2g_1^{-1} \in H$, i.e. $g_2 \sim_H g_1$. Transitive: if $g_1 \sim_H g_2$, and if $g_2 \sim_H g_3$, then $g_1g_2^{-1} \in H$, and $g_2g_3^{-1} \in H$. As H is *closed under multiplication*, $g_1g_2^{-1}g_2g_3^{-1} \in H$, i.e. $g_1g_3^{-1} \in H$, $g_1 \sim_H g_3$).

Example: $G = (\mathbf{Z}, +)$, $H = (n\mathbf{Z}, +)$. Here, $x \sim_H y$ if and only if $x \equiv y \pmod n$. There are n cosets, e.g. if $n = 2$, then “ $2\mathbf{Z}$ ” represents the even integers, and “ $1+(2\mathbf{Z})$ ” represents the odd integers. In general, G/H denotes the *set of left cosets of G relative to H* . It normally does not have any **useful** algebraic structure. But let us try to define a *multiplication* on it (because there’s an “obvious” one).

Try $(g_1H).(g_2H) = g_1g_2H$. This may (and usually *does*) depend on the **labels** g_1 and g_2 used. These labels are called “*coset representatives*”. If $g_1 \sim_H g_1'$, then $g_1H = g_1'H$; $g_1g_1'^{-1} \in H$; and $g_1 = hg_1'$ for *some* $h \in H$. Is $g_1g_2H = g_1'g_2H$? Now $g_1g_2 = hg_1'g_2$, so *this is OK!* ($(g_1g_2)(g_1'g_2)^{-1} = g_1g_1'^{-1} \in H$). Now try **changing** the label on the *second* term. If $g_2 \sim_H g_2'$, is $g_1g_2H = g_1g_2'H$? Now $g_2 \sim_H g_2' \Rightarrow g_2g_2'^{-1} = h \in H \Rightarrow g_2 = hg_2' \Rightarrow g_1g_2 = g_1hg_2'$.

So we *don't seem to know* that $g_1g_2 \sim_H g_1g_2'$ (**Note:** $g_1g_2g_2'^{-1}g_1^{-1} = g_1hg_1^{-1}$, and we *do not know* that this is in H — it **won't** be in general). **Example:** $G = D_3$, $H = \{1, S\}$. Here, $RSR^{-1} = RSR^2 = R^2S \notin H$. The construct will **work** if H is normal in G . (H is *normal* in G if given any $g \in G$, we have $gHg^{-1} = H$). If $H \triangleleft G$ ($\triangleleft =$ “normal in”), then the set of cosets G/H has a *natural group structure* called the **quotient** of G by H .

Tutorial

(3) **Commutators.** (a) Suppose that $x = R^iS^j$, and that $y = R^kS^l$ in D_5 . Write $[x,y]$ in the form $R^\alpha S^\beta$, where α and β are *explicitly* given in terms of i, j, k and l . (b) **Repeat** (a) with D_n for an (*arbitrary*) general n . (c) Work out what D_n^{Ab} will be for an *arbitrary* n . (d) If $x_1, x_2, y \in G$, then $[x_1x_2, y] = x_1x_2yx_2^{-1}x_1^{-1}y^{-1} = x_1[x_2, y]x_1^{-1} \cdot [x_1, y]$ by *adding in terms* and their *inverses*. Find a **similar** way to express $[x, y_1y_2]$. (e) Write $[x,y]^{-1}$ as a *commutator*. (f) Find a proof that $G/[G,G]$ is **abelian**.

A: (a) For D_5 , $S^2 = I$, $R^5 = I$, and $SR = R^4S$. **Consider** $[x,y]$. We have 4 cases: $x = R^i$, and $y = R^j$; $x = R^iS$, and $y = R^j$; $x = R^i$, and $y = R^jS$; and $x = R^iS$, and $y = R^jS$. **Recall** that $[x,y] = xyx^{-1}y^{-1}$. **Case 1:** $[x,y] = R^iR^jR^{-i}R^{-j}$. Use $R^{-j} = R^{5-j}$ to get $= R^iR^jR^{5-i}R^{5-j} = R^{i+j+5-i+5-j} = R^{10} = I$. **Case 2:** $[x,y] = R^iSR^jS^{-1}R^{-i}R^{-j}$. **Here**, use $SR^k = R^4SR^{k-1} = R^8SR^{k-2} = \dots = R^{4k}S$. So $[x,y] = R^iR^{4j}SS^{-1}R^{-i}R^{-j} = R^{i+4j-i-j} = R^{3j}$. **Case 3:** $[x,y] = R^iR^jSR^{-i}S^{-1}R^{-j}$. **Here**, use $(R^iS)^{-1} = S^{-1}R^{5-i} = SR^{5-i} = R^{20-4i}S = R^{-4i}S$.

So $[x,y] = R^{i+j}SR^{5-i}S^{-1}R^{-j} = R^{i+j}R^{-4i}SS^{-1}R^{-j} = R^{i+j-4i-j} = R^{-3i}$. Also, **note** in this case a “*sneaky idea*”: $[x,y]^{-1} = [y,x]$. So we **could** have got case 3 *directly* from case 2. **Case 4:** $[x,y] = R^iSR^jSS^{-1}R^{-i}S^{-1}R^{-j} = R^iSR^jR^{-i}S^{-1}R^{-j} = R^iSR^jS^{-1}R^{-i}R^{-j} = R^iR^{4j-4i}SS^{-1}R^{-j} = R^{3j}R^{-3i} = R^{3(j-i)}$.

(b) For D_n , $S^2 = I$, $R^n = I$, and $SR = R^{n-1}S$. **Consider** $[x,y]$. We have the *same 4 cases* as before. **Case 1:** $[x,y] = R^iR^jR^{-i}R^{-j} = I$. **Case 2:** $[x,y] = R^iSR^jS^{-1}R^{-i}R^{-j}$. Use $SR^k = R^{(n-1)k}S$, so that we have $R^iR^{(n-1)j}SS^{-1}R^{-i}S^{-j} = R^{i+(n-1)j-i-j} = R^{(n-2)j}$. **Case 3:** $[x,y] = R^iR^jSR^{-i}S^{-1}R^{-j} = R^{i+j}SR^{-i}S^{-1}R^{-j} = R^{i+j}R^{-(n-1)i}SS^{-1}R^{-j} = R^{i+j-(n-1)i-j} = R^{-(n-2)i}$. **Case 4:** $[x,y] = R^iSR^jSS^{-1}R^{-i}S^{-1}R^{-j} = R^iSR^jS^{-1}R^{-i}R^{-j} = R^iR^{(n-1)(j-i)}SS^{-1}R^{-j} = R^{i+(n-1)(j-i)-j} = R^{(n-2)j+(2-n)i}$.

(c) Using the 12/2/01 lecture, and (b) above, the commutators of D_n are all **rotations**. When n is odd, $[D_n, D_n]$ will contain all *rotations*. Also, all rotations can be realised as a **commutator**. Therefore, $D_n \setminus [D_n, D_n]$ will contain *two cosets*: $\langle R \rangle = \{I, R, \dots, R^{n-1}\}$, and $\langle R \rangle S$. So D_n^{Ab} has *order 2 when n is odd*, and is **isomorphic** to C_2 . When n is even, not all *rotations* can be realised as commutators — we can only obtain **even** powered rotations as commutators. So we will have *4 cosets* in $D_n \setminus [D_n, D_n]$: $\langle R_{1/2} \rangle = \{I, R^2, \dots, R^{n-2}\}$, $R \langle R_{1/2} \rangle$, $\langle R_{1/2} \rangle S$, and $R \langle R_{1/2} \rangle S$. Therefore, D_n^{Ab} has *order 4 when n is even*.

(d) $[x_1 x_2, y] = x_1 x_2 y x_2^{-1} x_1^{-1} y^{-1} = x_1 x_2 y x_2^{-1} y^{-1} y x_1^{-1} y^{-1} = x_1 [x_2, y] y x_1^{-1} y^{-1} = x_1 [x_2, y] x_1^{-1} x_1 y x_1^{-1} y^{-1} = x_1 [x_2, y] x_1^{-1} [x_1, y]$. And $[x, y_1 y_2] = x y_1 y_2 x^{-1} y_2^{-1} y_1^{-1} = x y_1 x^{-1} x y_2 x^{-1} y_2^{-1} y_1^{-1} = x y_1 x^{-1} [x, y_2] y_1^{-1} = x y_1 x^{-1} y_1^{-1} y_1 [x, y_2] y_1^{-1} = [x, y_1] y_1 [x, y_2] y_1^{-1}$. (e) $[x, y]^{-1} = (x y x^{-1} y^{-1})^{-1} = y x y^{-1} x^{-1} = [y, x]$. (f) A group G is **Abelian** if $y \bullet x = x \bullet y \forall x, y \in G$.

The **commutators** $[g_1, g_2]$ in G generate a subgroup $[G, G]$ of G called the *commutator subgroup* of G . This subgroup is **normal** since a **conjugate** of a commutator is again a commutator. We want to *prove that* $g[x, y]g^{-1} = [x', y']$ for some $g \in G$, and $x, x', y, y' \in [G, G]$. Now $g[x, y]g^{-1} = g x y x^{-1} y^{-1} g^{-1}$, and $[g x g^{-1}, g y g^{-1}] = g x g^{-1} g y g^{-1} g x^{-1} g^{-1} g y^{-1} g^{-1} = g x y x^{-1} y^{-1} g^{-1}$, so that $g[x, y]g^{-1} = [g x g^{-1}, g y g^{-1}]$, another *commutator*. Conclusion: $[G, G]$ is a **normal** subgroup.

Now what is an *element* in $G/[G, G]$? It is $g_1[G, G]$ for some $g_1 \in G$. A group is abelian if $x \bullet y = y \bullet x$ for all $x, y \in G$. So if we *have* $g_1[G, G]g_2[G, G] = g_1g_2[G, G]$, and if we have $g_2[G, G]g_1[G, G] = g_2g_1[G, G]$, we need to *prove that* $g_1g_2[G, G] = g_2g_1[G, G]$. But $gK = g'K$ for a **normal** subgroup K happens iff $gg'^{-1} \in K$. In the *above* case, “ gg'^{-1} ” is $g_1g_2(g_2g_1)^{-1} = g_1g_2g_1^{-1}g_2^{-1}$. But this is a *commutator* — so is in $[G, G]$. **Therefore**, $G/[G, G]$ is *Abelian*.

(4) (i) Find the *subgroups* of S_3 . Which are **normal**? (ii) Find the subgroups of D_n for $n = 3$ and 4. Which are **normal**? (iii) Find the *subgroups* of D_n in general. Which are **normal**? (iv) The **dihedral** group D_3 , and S_3 , are isomorphic (so *really the same*). What about D_4 and S_4 ? These have *different orders* (what are they?), so are not isomorphic. Suggest a way of associating a *permutation* of the vertices of a square to a symmetry, and hence find a homomorphism from D_4 to S_4 .

A: The possible permutations in S_3 are given by the **six possible ways** of ordering the numbers a, b and c as 1, 2 and 3 in the second row of $\begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}$. Let $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $r = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $r^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $x = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $y = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, and $z = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. We have *group table* as shown on the right. By **observation**, the subgroups are $\{e\}$, $\{e, r, r^2\}$, $\{e, r, r^2, x, y, z\}$, $\{e, x\}$, $\{e, y\}$, and $\{e, z\}$.

		e	r	r ²	x	y	z
e		e	r	r ²	x	y	z
r		r	r ²	e	z	x	y
r ²		r ²	e	r	y	z	x
x		x	y	z	e	r	r ²
y		y	z	x	r ²	e	r
z		z	x	y	r	r ²	e

Now a subgroup is *normal* if $x^{-1}Hx = H$ for each $x \in G$. We test by this way, or equivalently testing if we have **left** coset = **right** coset. We do this for the *trivial* subgroups (empty and whole), and for $\{e, r, r^2\}$. We need a counter example to prove that the other 3 groups of order 2 are **not** normal, e.g. $y\{e, x\}y^{-1} = y\{e, x\} = \{y, r^2\}y = \{e, z\} \neq \{e, x\}$.

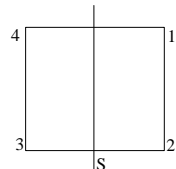
Now as S_3 is *isomorphic* to D_3 , the group table for $D_3 = \{I, R, R^2, S, RS, R^2S\}$ will be the “same” as above, and the *subgroups* will also be the same. For $D_4 = \{I, R, R^2, R^3, S, RS, R^2S, R^3S\}$, with $R^4 = I, S^2 = I, (RS)^2 = I$, and $SR = R^3S$, we have **group** table as shown on the right.

	I	R	R ²	R ³	S	RS	R ² S	R ³ S
I	I	R	R ²	R ³	S	RS	R ² S	R ³ S
R	R	R ²	R ³	I	RS	R ² S	R ³ S	S
R ²	R ²	R ³	I	R	R ² S	R ³ S	S	RS
R ³	R ³	I	R	R ²	R ³ S	S	RS	R ² S
S	S	R ³ S	R ² S	RS	I	R ³	R ²	R
RS	RS	S	R ³ S	R ² S	R	I	R ²	R ³
R ² S	R ² S	RS	S	R ³ S	R ²	R	I	R ³
R ³ S	R ³ S	R ² S	RS	S	R ³	R ²	R	I

Subgroups: $\{I\}, \{I, R^2\}, \{I, S\}, \{I, RS\}, \{I, R^2S\}, \{I, R^3S\}, \{I, R, R^2, R^3\}, \{I, R^2, S, R^2S\}, \{I, R^2, RS, R^3S\}$, and $\{I, R, R^2, R^3, S, RS, R^2S, R^3S\}$. The *trivial* subgroups are normal. This leaves 8 subgroups to check. $\{I, B\}$ is not normal because $R^3\{I, S\}(R^3)^{-1} = R^3\{I, S\}R = \{R^3, R^3S\}R = \{I, R^3SR = R^2S\} = \{I, R^2S\} \neq \{I, S\}$. **Similarly**, $\{I, R^2S\}$ and $\{I, R^3S\}$ are not normal. To check that the rest *are* normal, use *left coset = right coset*, e.g. for $\{I, R, R^2, R^3\}$, the **left** coset of an element, e.g. $RS = \{R^2S, RS, S, R^3S\}$, is equal to the **right** coset for RS .

For D_n , if possible, *draw the table* and observe the subgroups. If this is not possible, we could use **Lagrange’s Theorem**, i.e. the *order* of any subgroup divides the order of the group, $|S| \mid |G|$. This would enable us to specify the **possible** subgroups. For example, for D_{24} , we **could** have subgroups of orders 1, 2, 3, 4, 6, 8, 12 and 24.

(iv) D_4 is the symmetry group of the *square*. R means to rotate 90° clockwise, and S means to flip by the *axis* shown. If we **number** the vertices as shown, we have $I = (1\ 2\ 3\ 4)$, $R = (1\ 2\ 3\ 4)$, and $S = (1\ 4\ 2\ 3)$. We can assign a *permutation* for any element of D_4 . If we define a **function** $f: D_4 \rightarrow S_4$, then $f(I) = (1\ 2\ 3\ 4)$, $f(R) = (1\ 2\ 3\ 4)$, $f(R^2) = (1\ 3\ 2\ 4)$, $f(R^3) = (1\ 2\ 3\ 4)$, $f(S) = (1\ 4\ 2\ 3)$, $f(SR) = (1\ 2\ 4\ 3)$, $f(SR^2) = (1\ 2\ 1\ 3\ 4)$, and $f(SR^3) = (1\ 3\ 2\ 1\ 4)$. The 8 permutations will form a *subgroup* of S_4 , so that D_4 will be **isomorphic** to this *subgroup* of S_4 — therefore D_4 is **homomorphic** to S_4 .



12th February 2001

Example: G group $[G, G] \sim$ subgroup generated by *all commutators* $[x, y]$. **Note:** $[x, y]^{-1} = [y, x]$, but the *product of commutators* need not be a commutator, so take the smallest subgroup of G containing all commutators, or take the set of all **products** of commutators. If $g \in G$, then $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$. So any *conjugate* of a commutator is a commutator. **Since** $gabg^{-1} = gag^{-1}gbg^{-1}$, any *conjugate* of an element in $[G, G]$ is there **already**. **Conclusion:** $[G, G] \triangleleft G$. ($[G, G]$ is the *commutator subgroup* of g).

Facts: (i) If G is abelian, then $[G, G] = \{1\}$. (ii) It can *happen* that $[G, G] = G$. (iii) The quotient group $G^{Ab} = G/[G, G]$ is *always* abelian — it is the “**abelianisation**” of G . **Application:** If G is suspected of being infinite, see if G^{Ab} is infinite (very *easy* to do). If Yes, G is infinite; but No: “test fails”. **Example:** $D_3^{Ab} = ?$ What are the *commutators*: they are $[R^iS^j, R^kS^l] = R^iS^jR^kS^lS^{-j}R^{-i}S^{-l}R^{-k}$. If $j = l = 0$, then $[R^i, R^k] = 1$. If $j = l = 1$, then $[R^iS, R^kS] = R^{i+k}$. If $j = 0$, and if $l = 1$, then $[R^i, R^kS] = R^{-i}$. And if $j = 1$, and if $l = 0$, then $[R^iS, R^k] = R^k$.

Each commutator is a *rotation*, and any rotation can be *realised* as a commutator. So $[D_3, D_3] = \langle R \rangle = \{I, R, R^2\}$ (**Note:** “ $\langle \rangle$ ” represents “subgroup **generated** by”). The two *cosets* are $\langle R \rangle = \{I, R, R^2\}$ and $S\langle R \rangle = \{S, RS, R^2S\}$. So D_3^{Ab} has **order** 2, or $[D_3, D_3]$ has **index** 2 in D_3 . Further, $D_3^{Ab} \cong C_2$ ($\cong =$ “*isomorphic* to”). **Note:** $S\langle R \rangle S\langle R \rangle = S^2\langle R \rangle = \langle R \rangle$.

Theorem (1st Isomorphism Theorem): If $\phi: G \rightarrow H$ is a homomorphism, then ϕ induces between $G/\text{Ker } \phi$ and $\text{Im } \phi$. **Proof:** The elements of $G/\text{Ker } \phi$ are cosets $g \text{Ker } \phi$, and if $gk \in g\text{Ker } \phi$, then $\phi(gk) = \phi(g)\phi(k) = \phi(g)$, since $\phi(k) = 1$. All the elements of a coset get mapped by ϕ to the same element, the image of the “label” used. This suggests defining $\phi_*: G/\text{Ker } \phi \rightarrow \text{Im } \phi$ by $\phi_*(g \text{Ker } \phi) = \phi(g)$ (we have already checked ϕ_* is “well defined”).

It is ϕ_* that we will show is an isomorphism, by (i) showing that ϕ_* makes sense (i.e. is independent of the choices); (ii) showing that ϕ_* is a homomorphism; (iii) showing that ϕ_* is onto (i.e. is an epimorphism); and (iv) showing that ϕ_* is 1-1 (i.e. is a monomorphism). Write $K = \text{Ker } \phi$. (i) If $gK = g'K$, then $g' = gk$ for some $k \in K$, and we know that $\phi(g) = \phi(g')$, i.e. $\phi_*(gK)$ is independent of the choice of g . (ii) Note that $g_1K.g_2K = g_1g_2K$; $\phi_*(g_1g_2K) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \phi_*(g_1K)\phi_*(g_2K)$. So ϕ_* is a homomorphism.

13th February 2001

(iii) If we have some $h \in \text{Im } \phi$, it is there because it is the image of something, g , say, i.e. $h = \phi(g) = \phi_*(gK)$, so that h is the image of gK under ϕ_* . (iv) A group homomorphism θ is 1-1 if and only if $\text{Ker } \theta = \{1\}$, because $\theta(g_1) = \theta(g_2)$ implies $\theta(g_1g_2^{-1}) = 1$, i.e. $g_1g_2^{-1} \in \text{Ker } \theta$. If $\text{Ker } \theta = \{1\}$, then $g_1g_2^{-1} \in \text{Ker } \theta$. If $\text{Ker } \theta = \{1\}$, then $g_1g_2^{-1} = 1$, i.e. $g_1 = g_2$, and if θ is 1-1, the only thing in $\text{Ker } \theta$ will be 1. So we need only check $\text{Ker } \phi_*$. Suppose that $gK \in \text{Ker } \phi_*$, then $\phi_*(gK) = 1_H$. LHS = $\phi(g)$, i.e. $g \in \text{Ker } \phi$; and $gK = K$, i.e. $\text{Ker } \phi_* = \{1\}$, so that ϕ_* is 1-1. All together, ϕ_* is an isomorphism.

Corollary (2nd Isomorphism Theorem): Suppose that $K \triangleleft H \triangleleft G$ (with $K \triangleleft G$), then $H/K \triangleleft G/K$, and $G/H \cong (G/K)/(H/K)$. **Proof:** Define $\phi: G/K \rightarrow G/H$ so that $\phi(gK) = gH$ (check that if $g_1K = g_2K$, then $g_1H = g_2H$). Method: $g_1K = g_2K \Rightarrow g_1g_2^{-1} \in K \subset H \Rightarrow g_1H = g_2H$. So ϕ is well-defined. ϕ is obviously a homomorphism, since $g_1Kg_2K = g_1g_2K$. And ϕ is onto, so that $\text{Im } \phi = G/H$. By the 1st Isomorphism Theorem, $(G/K)/\text{Ker } \phi \cong G/H$. But $gK \in \text{Ker } \phi$ if and only if $\phi(gK) = 1_H$, i.e. $gH = 1_H$, i.e. $g \in H$. So $gK \in \text{Ker } \phi \Leftrightarrow g \in H$, so that $gK \in H/K$. Thus $\text{Ker } \phi = H/K$. Therefore, $(G/K)/(H/K) \cong G/H$ as required.

Lagrange's Theorem

Suppose that G is a group, and that $H \leq G$ is a subgroup. If g_1H and g_2H are two left cosets, then $g_1h \rightarrow g_2h$; $g_1H \rightarrow g_2H$ is a bijection. **Proof:** This mapping is given by multiplying by $g_2g_1^{-1}$ on the left. The inverse mapping is multiplication by $g_1g_2^{-1}$. **End of Proof** (so that all cosets gH have the “same size” — and the same size as H).

Suppose that G is finite, then the cosets of H partition G into a collection of subsets of equal size, $|H|$. The number of cosets in $[G:H]$ is called the index of H , and we have $[G:H]$ cosets, each of size $|H|$, which together exhaust G , i.e. $|G| = [G:H]|H|$. **Theorem** (Lagrange): If G is finite, then the order of any subgroup divides the order of G .

Example: Any group of order 13 has only two subgroups: 1, and the whole group. It is therefore cyclic, since if g is any element ($\neq 1$), then $\langle g \rangle$ is the subgroup generated by g (and must be the whole of the group). All groups of order 13 are isomorphic to C_{13} . The same argument works for any group of order p , where p is a prime.

Corollary: If G has order n , then any *element* $g \in G$ has order *dividing* n . **Proof:** $H = \langle g \rangle$ has order the *order* of g , but $|H|$ divides n . (**Note:** g has order m if $g^m = 1$; and if $g^k = 1$, for $k > 0$, then $m \leq k$).

Exercises

Symmetric Groups. Example: S_3 , the symmetric group on three symbols, $\{1,2,3\}$. This is made up of all the **permutations** of $\{1,2,3\}$. One notation for the permutations is “*function notation*”: for instance, $\sigma = ({}^1_1 \ {}^2_3 \ {}^3_2)$ is the permutation that **interchanges** 2 and 3, but leaves 1 unchanged. The more *economical* notation is “*cycle notation*”. Here, this permutation would be represented as $(2\ 3)$. In **cycle** notation, $S_3 = \{(), (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.

To *compose permutations*, we will read from left to right, so for instance $(1\ 2)(1\ 2\ 3)(1\ 3) = ()$, the *identity* element, since 1 goes to 2 (in the first bracket), then to 3, and then back to 1. Similarly for 2 and 3. Now the **elements** $(1\ 2)$, $(2\ 3)$ and $(1\ 3)$ are *2-cycles (or transpositions)* and have order 2. The elements $(1\ 2\ 3)$ and $(1\ 3\ 2)$ are *3-cycles* — *and have order 3*. For inverses, $(1\ 2\ 3)^{-1} = (1\ 3\ 2)$, as you can easily *check*.

In general, we have the **symmetric** group S_n of permutations of $\{1,2,\dots,n\}$. We can use *function notation* such as $\sigma = ({}^1_5 \ {}^2_1 \ {}^3_4 \ {}^4_2 \ {}^5_3)$. The corresponding *cycle notation* would be $(1\ 5\ 3\ 4\ 2)$, a 5-cycle. Not **all** permutations give cycles: $\sigma = ({}^1_5 \ {}^2_1 \ {}^3_4 \ {}^4_3 \ {}^5_2)$ corresponds to $(1\ 5\ 2)(3\ 4)$, a **product** of cycles. Any permutation can be written as a *product of disjoint cycles*.

Exercises. (1) (i) Write the *permutation* $\sigma = ({}^1_6 \ {}^2_4 \ {}^3_7 \ {}^4_2 \ {}^5_5 \ {}^6_1 \ {}^7_8 \ {}^8_9 \ {}^9_3)$ as a product of **disjoint** cycles. (ii) Let $\sigma = (i_1, i_2, \dots, i_r)$ be a cycle in S_n . Show that it can be written as a *product of disjoint cycles*. (Hint: σ will split $\{1,2,\dots,n\}$ into a *collection* of “orbits”). A: (i) $(16)(24)(3789)$ by *writing* it out.

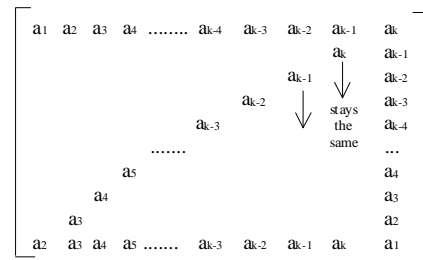
(ii) Given a $\sigma = (i_1, i_2, \dots, i_r)$, write it out in *function notation* to begin with, so that $\sigma = ({}^1_a \ {}^2_b \ {}^3_c \ \dots \ {}^r_n)$. Then, follow the **first** cycle, starting at 1 until it *closes*, then choose the next unused number and follow its cycle, etc., until **all** numbers have been covered. Then write out the (*disjoint*) cycles next to one another.

(2) (i) Find the **inverse** of $(1\ 3\ 2\ 4)$ working in S_4 (or for that matter, S_n , for any $n \geq 4$). (ii) Let $\sigma = (i_1, i_2, \dots, i_r)$ be a cycle in S_n : what is σ^{-1} ? Give a **proof**. A: $(1324)^{-1} = ({}^1_{31} \ {}^2_{42} \ {}^3_{23} \ {}^4_{14})$. Therefore, $(1324)^{-1} = (1423)$. Check by **computing** $(1324)(1423)$. If $\sigma = (i_1, i_2, \dots, i_r)$, then $\sigma^{-1} = (i_r, \dots, i_2, i_1)$. **Proof:** In σ , i_1 goes to i_2 so that in σ^{-1} , i_2 must go to i_1 , which it *does*. Similarly for all other *consecutive entries* in σ .

(3) Find two *two-cycles* whose product is a 3-cycle. If we call these α and β , is $\alpha\beta = \beta\alpha$? Conjecture when do two cycles *commute*? Try out some examples: why do your examples behave as they do? (i.e. hopefully **some** commute, while **others** don't). A: (13) and (34) produce (134) . Let $\alpha\beta = (13)(34) = ({}^1_{13} \ {}^2_{22} \ {}^3_{44} \ {}^4_{31})$. But $(34)(13) = ({}^1_{34} \ {}^2_{22} \ {}^3_{11} \ {}^4_{43}) \neq \alpha\beta$. **Proposition:** two 2-cycles commute if they are *disjoint*, i.e. they do not share any common entries.

(4) It is known that every **permutation** is a product of transpositions. Find transpositions that when multiplied in a *suitable order*, give you the 5-cycle (1 2 3 4 5)? Repeat with (1 2 3 4 5 6). What about (1 2 4 5 3 6)? **Prove** the result we started with. (In fact, this proves that the transpositions *generate* the group S_n , but what are the **relations**? Think about this for $n = 4$).

A: $(12345) = (12)(23)(34)(45)$. Test by **writing** it out. Similarly, $(123456) = (12)(23)(34)(45)(56)$, and $(124536) = (12)(24)(45)(53)(36)$. **Proof:** We want to prove that $(a_1 a_2 a_3 \dots a_k) = (a_1 a_2)(a_2 a_3)\dots(a_{k-1} a_k)$. We look at the *situation* shown on the right. Note that we write the **top** line specially, and only write in what changes. What is happening is that for every *transposition*, we are changing an entry on the diagonal, and **cycling** the last entry to the first entry *slowly*. This is, if we have k elements in the permutation, there are $k-1$ transpositions, so that we can cycle *successfully*. Note that a more formal proof can be done by **induction** (look in a book).



(5) The groups D_3 and S_3 are *isomorphic* (how could you prove this?), but D_n is only isomorphic to a **proper** subgroup of S_n if $n \geq 4$. Find a *suitable set of permutations* on 1, 2, 3 and 4, corresponding to D_4 (the symmetry group of the **square**). Generalise ... eventually to a **general n**.

A: For the proof of *isomorphism*, define a function f between the 2 groups, and show that it is **well defined, injective and surjective**. Remember that in the previous exercises, we constructed a *subgroup* of S_4 from D_4 by letting $I = (1\ 2\ 3\ 4)$, $S = (1\ 4\ 2\ 3\ 2\ 4\ 1)$, and $R = (1\ 4\ 2\ 1\ 3\ 2\ 4\ 3)$. In general, $D_n = \{I, R, \dots, R^{n-1}, S, SR, SR^{n-1}\}$.

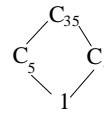
We can provide a set of *generating permutations* in S_n which generate a **subgroup** of S_n according to D_n : $I = (1\ 2\ 3\ \dots\ n)$, $R = (1\ n\ 2\ 1\ 3\ 2\ 4\ 3\ 5\ 4\ 6\ 5\ \dots\ n\ n-1)$, and $S = (1\ 1\ 2\ n\ 3\ n-1\ 4\ n-2\ \dots\ n-3\ n-2\ n-1\ 3\ n_2)$ for n odd, and $S = (1\ n\ 2\ n-1\ 3\ n-2\ \dots\ n-2\ 3\ n-1\ 2\ n_1)$ for n even. To see this, picture a *triangle, square, pentagon*, etc., and note that S goes **through** a vertex when n is odd (and therefore vertex “1” remains unchanged), and for n even, **all** the vertices are “swapped”.

Standard Examples

Cyclic Groups: All elements are *powers of a single element*, $C_n = \{1, x, \dots, x^{n-1}\} = \langle x \mid x^n = 1 \rangle$. Also, $C_\infty = \{1, x, x^2, \dots, x^{-1}, x^{-2}, \dots\}$. A cyclic group is *necessarily* abelian. **Example:** $C_6 = \{1, a, a^2, a^3, a^4, a^5\}$ (orders 1, 6, 3, 2, 3 and 6). If we **write** $\langle x \rangle$ for the subgroup generated by $x \in G$, in C_6 , $\langle a^2 \rangle \cong C_3$, and $\langle a^3 \rangle \cong C_2$. In C_n , $\langle x \mid x^n = 1 \rangle$. **Claim:** x^r has order $n/\gcd(r, n)$.

Proof of claim: We know that $\gcd(r, n) = \alpha n + \beta r$. Now $(x^r)^{n/\gcd(r, n)} = (x^n)^{r/\gcd(r, n)} = 1^{r/\gcd(r, n)} = 1$. Therefore, the order of x^r *divides* $n/\gcd(r, n)$. Try this with $\gcd(r, n) = 1$. Here, $1 = \alpha n + \beta r$. We know that $(x^r)^n = 1$, since all elements have *order dividing* n . Now $x = x^{\alpha n + \beta r} = x^{\beta r}$. If order $x^r = s < n$, then $(x^{\beta r})^s = 1$, since $(x^r)^s = 1$, i.e. $x^s = 1$, with $s < n$ — *OOPS* — so we **cannot** have $s < n$, and we must therefore have $s = n$. Back to the **general** case. Now order $(x^r) = s = (\text{want}) = n/\gcd(r, n)$. **Assume** that $s < n/\gcd(r, n)$. Therefore, $sgcd < n$. But $\gcd = \alpha n + \beta r$; $sgcd = \alpha sn + \beta sr$. It follows that $x^{sgcd} = x^{\alpha sn + \beta sr} = x^{\alpha sn} x^{\beta sr}$. But $x^{\alpha sn} = 1$ (because $x^n = 1$), and $x^{\beta sr} = ((x^r)^s)^\beta = 1^\beta = 1$. Therefore, $x^{s \cdot gcd} = 1$ — *OOPS* — since $sgcd < n$, and x has *order* n .

Facts. If $\gcd(r,n) = 1$, then $\langle x^r \rangle = C_n$. **Example:** in C_{35} , there is *one element of order one*, 4 elements of **order 5** ($x^7, x^{14}, x^{21}, x^{28}$), 6 elements of order 7 ($x^5, x^{10}, x^{15}, x^{20}, x^{25}, x^{30}$), and all other elements are of *order 35*. (Here we use $\text{order}(x^r) = n/\gcd(r,n) = 35/\gcd(r,35)$). We have a **Hasse** diagram as shown. 5 and 7 are coprime: $3 \times 7 - 4 \times 5 = 1$. So $x = (x^7)^3(x^5)^{-4} = (x^7)^3(x^5)^3$. Therefore, any *element* in C_{35} can be written as a **product** of an element of *order 5* and an element of *order 7* (possibly with one or another trivial). More *exactly*, for any $c \in C_{35}$, we have $c = ab$, where $a \in C_5$, and $b \in C_7$.



The Symmetric Group, S_3

S_3 consists of **permutations** of $\{1,2,3\}$. (1 2) means *swap* 1 and 2. $S_3 = \{(1), (1\ 2), (2\ 3), (1\ 3), (1\ 3\ 2), (1\ 2\ 3)\}$. **Note:** (1 2)(2 3) = (1 3 2), and (2 3)(1 2) = (1 2 3). **Note:** in this module, read from *left to right*, although from *right to left* as I did previously is still valid. Just do not mix and match!

20th February 2001

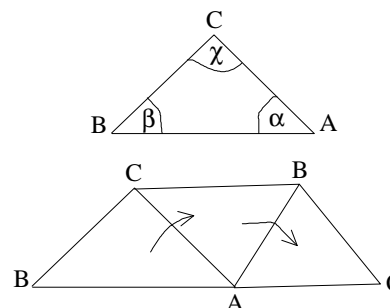
The Symmetric Group on n Symbols, S_n

$|S_n| = n!$, e.g. $|S_6| = 720$. We can give a *schematic* list of elements of S_n : **Identity**, (i j) transpositions ($\binom{n(n-1)}{2}$), (i j k) 3-cycles e.g. (1 3 5). **Note:** (1 3 5) = (3 5 1) = (5 1 3); (i j k)⁻¹ = (i k j). There are k cycles *for each* $k = 2, 3, \dots, n$ (i_1, \dots, i_k). **For** $n \geq 4$, we also get other types of permutations, e.g. (1 2)(3 4), a product of *disjoint cycles*. If the cycles are **not** disjoint, then they interact, e.g. (1 2)(2 3) = (1 3 2), but (2 3)(1 2) = (1 2 3), *non-abelian*.

Disjoint cycles commute: $(i_1 \dots i_k)(j_1 \dots j_l) = (j_1 \dots j_l)(i_1 \dots i_k)$, with $\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_l\} = \emptyset$. Any permutation σ can be **written** as a product of disjoint cycles, e.g. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} = (1\ 3)(2\ 4\ 5)$. Any *permutation* can be written as a product of transpositions, e.g. $\sigma = (1\ 3)(2\ 5)(4\ 5)$. The **sign** of a permutation is the parity (\pm) of the *number of transpositions* involved, e.g. σ is an odd permutation. **Generating sets** for S_n : *all transpositions*; (1 2) plus (1 2 ... n) (or *any transposition* plus *any n-cycle*). **Subgroup** A_n : the group of even permutations.

Triangle Groups and van Dyck Groups

We want to *tessellate (tile)* a space with copies of this triangle. If a, b and c denote **reflections** in BC, CA and AB respectively, then $a^2 = b^2 = c^2 = e$, the identity. The element bc **rotates** the triangle about A through an angle of 2α . To be able to tile, we *need* 2α to divide 2π . Similarly, we need $2\beta/2\pi$ and $2\chi/2\pi$. If it *does tile*, these must be integers $l, m, n \geq 2$ so that $\alpha = \pi/m$, $\beta = \pi/n$, $\chi = \pi/l$, and $(ab)^l = (bc)^m = (ca)^n = e$.

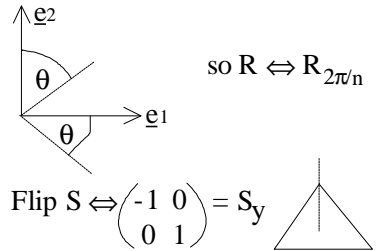


The group *generated* by a, b and c is denoted by $\Delta(l,m,n)$ (**a triangle**, not *delta*). Within this, there is a *subgroup* of index 2 determined by the **rotations**, i.e. generated by ab and bc (ca is there as $ca = (ac)^{-1}$, and $ac = (ab)(bc)$). This *group*, $D(l,m,n)$, the van Dyck group, has **presentation** $D(l,m,n) = \langle x,y \mid x^l = 1, y^m = 1, (xy)^n = 1 \rangle$ ($x = ab, y = bc$).

Matrix Groups

Example: $GL(2, \mathbf{C})$, a group of *invertible (non-singular)* 2×2 matrixes over \mathbf{C} . This has *interesting* subgroups e.g. the **subgroup** Q generated by $\zeta = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ and $\eta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, with $\zeta^4 = 1$, $\eta^2 = \zeta^2$, and $\eta^{-1}\zeta\eta = \zeta^{-1}$. In fact, Q has *order* 8 — but how do you **prove** it? Q has *presentation* $\langle x, y \mid x^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} \rangle$. *Generalisations* of $GL(2, \mathbf{C})$: e.g. $GL(m, \mathbf{C})$, $GL(m, \mathbf{R})$, and $GL(m, \mathbf{Z}_p)$.

D_n is *isomorphic* to a subgroup of $GL(2, \mathbf{R})$ e.g. rotations through $2\pi/n$. A rotation through θ (*clockwise*) is given by $R_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$. The *subgroup* of $GL(2, \mathbf{R})$ generated by $R_{2\pi/n}$ and S_y “looks a lot” like $D_n = \langle r, s \mid r^n = 1, s^2 = 1, (rs)^2 = 1 \rangle$. Now $r \rightarrow R_{2\pi/n}$ and $s \rightarrow S_y$ seems to give a *homomorphism* $D_n \rightarrow GL(2, \mathbf{R})$. It seems to be a *monomorphism*.



Representations of a group. Let G be a group. A *linear representation* of G is a homomorphism $\rho: G \rightarrow GL(m, k)$, where k is a field. It is **faithful** if ρ is a *monomorphism*. **Permutation Representation:** $G \rightarrow S_n$. **Cayley’s Theorem:** If G has *order* n , then it has a *faithful representation*, $\rho: G \rightarrow S_n$. **Proof (Sketch):** Label the elements of G as g_1, \dots, g_n . If $g \in G$, then gg_1 is some “*other*” element of G .

Similarly for g_2 , etc. **Define** $\rho(g) \in S_n$ by $\rho(g)(i)$, where $gg_i = g_{\rho(g)(i)}$. (Or, $gg_i = g_j$ for some j , and *define* $\rho(g)(i) = j$). Now check that ρ is a *homomorphism* and 1-1. **Example:** $G = D_3$. Multiply $\{1, r, r^2, s, rs, r^2s\}$ by r to get $\{r, r^2, 1, rs, r^2s, s\}$, so that $\rho(r) = (1\ 2\ 3)(4\ 5\ 6)$. Multiply by s to get $\{s, r^2s, rs, 1, r^2, r\}$, so that $\rho(s) = (1\ 4)(2\ 6)(3\ 5)$ (*recall* that $sr = r^2s$).

Working with Presentations

Conjugacy. In a group, G , elements x and y in G are said to be *conjugate* if there is some $g \in G$ such that $gxg^{-1} = y$. We also say that y is *obtained by conjugating* x by g . **Lemma:** *Conjugacy* is an equivalence relation. **Proof:** (i) *Reflexive:* x is conjugate to x (use $1, 1x1^{-1} = x$). (ii) *Symmetric:* if $gxg^{-1} = y$, then $(g^{-1})y(g^{-1})^{-1} = x$. (iii) *Transitive:* if $gyg^{-1} = x$, and if $hzh^{-1} = y$, then $(gh)z(gh)^{-1} = x$.

The *equivalence classes* are called **conjugacy** classes. **Example:** $D_5 = \langle r, s \mid r^5 = 1, s^2 = 1, (rs)^2 = 1 \rangle$ (change the *last relation* to $sr = r^4s$). Every element *has the form* $r^i s^j$ for $0 \leq i \leq 4$, and $j = 0, 1$. For the case $j = 0$, it is only conjugate to *itself*. What is **conjugate** to r ? $j = 0$: $r^i r r^{-i} = r$. $j = 1$: $(r^i s)r(s^{-1}r^{-i}) = r^i r^{-1} s^2 r^i = r^{-1}$. So $\{r, r^{-1}\}$ is a *conjugacy class* ($\{r, r^4\}$). Now take r^2 , and *conjugate* with some x : $xr^2x^{-1} = xrx^{-1}xr^{-1} = \{r^2, r^{-2}\} = \{r^2, r^3\}$.

Now *look* at s : $rsr^{-1} = r^2s$; $r^2sr^{-2} = r(rs^{-1})r^{-1} = r(r^2s)r^{-1} = r(r^2)r^{-1}rsr^{-1} = r^2.r^2s = r^4s$. We get $\{s, r^2s, r^4s, rs, r^3s\}$, as *these are the only ones left*. The conjugacy class **structure** is as follows: $\{1\}$, $\{r, r^4\}$, $\{r^2, r^3\}$, and $\{s, r^2s, r^4s, rs, r^3s\}$. Similarly, in D_6 , we get $\{1\}$, $\{r, r^5\}$, $\{r^2, r^4\}$, $\{r^3\}$, $\{s, r^2s, r^4s\}$, and $\{rs, r^3s, r^5s\}$.

Conjugacy

(6) Find all the *conjugacy classes* for a general dihedral group, D_n : (i) for n **even**, and (ii) for n **odd** (the two cases are different, although some of the *working* will be the same). A: $D_n = \langle r, s \mid r^n = 1, s^2 = 1, (rs)^2 = 1 \rangle$. The **last** relation $\Rightarrow rs = s^{-1}r^{-1} = sr^{n-1}$, and $sr = r^{-1}s^{-1} = r^{n-1}s$. We *already know* that **any** element may be written in the form $r^i s^j$ for $0 \leq i \leq n-1$, and $j = 0, 1$.

We **consider conjugating** $r^i s^j$ by r and by s . (**r**) $\underline{j=0}$: $r(r^i)r^{-1} = r^i$. $\underline{j=1}$: $r(r^i s)r^{-1} = r^{i+1}sr^{-1} = r^{i+2}s$ (*reduce* if $i+2 \geq n$). (**s**) $\underline{j=0}$: $s(r^i)s^{-1} = sr^i s = r^{n-i}ss = r^{n-i}$. $\underline{j=1}$: $s(r^i s)s^{-1} = sr^i = r^{n-i}s$. Now if we *try to conjugate* $r^i s^j$ by $r^k s$, we get $(r^k s)(r^i s^j)(s^{-1}r^{-k})$, and so we can *find the conjugacy class* of any element by **repeated application** of conjugation by the r and by the s .

We **start** by considering the conjugacy class containing r . r conjugated by *any power of itself* is just r . r **conjugated** by s is $srs^{-1} = r^{n-1}ss^{-1} = r^{n-1}$. r^{n-1} *conjugated* by any power of r is r^{n-1} . And r^{n-1} *conjugated* by s is $sr^{n-1}s^{-1} = rss^{-1} = r$. Thus the *conjugacy class* is $\{r, r^{n-1}\}$. Now find the conjugacy class *containing* s . s conjugated by s is $sss^{-1} = s$. s *conjugated* by r is $rsr^{-1} = rsr^{n-1} = r^2s$. r^2s *conjugated* by s is $sr^2ss^{-1} = sr^2 = r^{n-1}sr = r^{n-1}(r^{n-1}s) = r^{n-2}s$. r^2s *conjugated* by r is $r^3sr^{-1} = r^4s$. $r^{n-2}s$ *conjugated* by s is $sr^{n-2}ss^{-1} = sr^{n-2} = sr^{n-1}r^{-1} = rsr^{-1} = r^2s$.

$r^{n-2}s$ *conjugated* by r is $r^{n-1}sr^{-1} = r^{n-1}(sr^{n-1}) = r^{n-1}(rs) = r^n = s$. r^4s *conjugated* by s is $sr^4ss^{-1} = sr^4 = r^{n-4}s$. And r^4s *conjugated* by r is $r^5sr^{-1} = r^6s$. So we **have** $\{s, r^2s, r^4s, \dots\} \cup \{r^{n-2}s, r^{n-4}s, \dots\}$. When n is even, e.g. 8, we *have* $\{s, r^2s, r^4s, r^6s\} \cup \{r^6s, r^4s, r^2s, s\} = \{s, r^2s, r^4s, \dots, r^{n-2}s\}$. When n is odd, e.g. 7, we *have* $\{s, r^2s, r^4s, r^6s\} \cup \{r^5s, r^3s, rs\} = \{s, rs, r^2s, r^3s, \dots, r^{n-1}s\}$.

Now find the *conjugacy class containing* r^2 . r^2 conjugated by r is just r^2 . r^2 conjugated by s is $sr^2s^{-1} = r^{n-1}sr s = r^{n-1}r^{n-1}ss = r^{n-2}$. r^{n-2} conjugated by r is just r^{n-2} . And r^{n-2} conjugated by s is $sr^{n-2}s^{-1} = sr^{n-1}r^{-1}s = rsr^{n-1}s = r^2ss = r^2$. Thus the *conjugacy class* is $\{r^2, r^{n-2}\}$. There seems to be a **pattern**, and we would *expect* to get $\{r^3, r^{n-3}\}, \dots$

When n is **odd**, e.g. $n = 5$, we have $\{r, r^4\}, \{r^2, r^3\}, \{r^3, r^2\}, \{r^4, r\}$, i.e. 2 *distinct classes*, or $n-1/2$ *distinct classes*: $\{r, r^{n-1}\}, \{r^2, r^{n-2}\}, \dots, \{r^{(n-1/2)}, r^{n-(n-1/2)}\}$. When n is **even**, e.g. $n = 6$, we have $\{r, r^5\}, \{r^2, r^4\}, \{r^3\}, \{r^4, r^2\}, \{r^5, r\}$, i.e. 3 *distinct classes*, or $n/2$ *distinct classes*: $\{r, r^{n-1}\}, \dots, \{r^{(n/2)-1}, r^{n-((n/2)-1)}\}, \{r^{n/2}\}$. We can now **classify** all the conjugacy classes of D_n for when n is **odd**: we have a total of $n-1/2+2$ *conjugacy classes*, and they are as follows: $\{1\}, \{s, rs, r^2s, \dots, r^{n-1}s\}, \{r, r^{n-1}\}, \{r^2, r^{n-2}\}, \dots, \{r^{n-1/2}, r^{n-(n-1/2)}\}$.

When n is **even**, a *little more work* is required. We have not in this case dealt with the **set** of elements $\{rs, r^3s, \dots, r^{n-1}s\}$. Is *this* a conjugacy class? It turns out that it **is** by analysing the *conjugacy class containing* rs . So we can **list** the $n/2+3$ classes as follows: $\{1\}, \{s, r^2s, r^4s, \dots, r^{n-2}s\}, \{rs, r^3s, r^5s, \dots, r^{n-1}\}, \{r, r^{n-1}\}, \{r^2, r^{n-2}\}, \dots, \{r^{(n/2)-1}, r^{n-((n/2)-1)}\}, \{r^{n/2}\}$. **Note**: Avoid *general examples* as these detract from the general theory.

(7) Find all the *conjugacy classes* of S_4 (think: there are 24 elements — so checking all combinations is not feasible. Try out some **examples**, seeing what conjugation does to 2-cycles, 3-cycles, 4-cycles, and *products of disjoint 2-cycles* in turn). What is **likely** to be the general result on the conjugacy classes in S_n ?

A: $S_4 = \{(1), (12), (13), (14), (23), (24), (34), (123), (132), (143), (124), (134), (142), (12)(34), (23)(14), (24)(13), (234), (243), (1234), (1342), (1243), (1432), (1423), (1324)\}$. Let us try *some simple examples* to start with. 2-cycles: $(13)(\mathbf{12})(31) = (23)$; $(34)(\mathbf{12})(43) = (12)$; $(123)(\mathbf{12})(321) = (13)$; $(13)(24)(\mathbf{12})(13)(24) = (34)$; and $(1423)(\mathbf{12})(3241) = (34)$.

This **suggests** that we will get a conjugacy class of all the 2-cycles, $\{(12), (13), (14), (23), (24), (34)\}$. Similarly, by *testing some 3-cycles, 4-cycles, and disjoint 2-cycles*, we see that the set of those types form **conjugacy classes** by themselves. To “*complete the set*”, note that the **identity** permutation forms a class by itself. Generally, in S_n , we would expect all “types” of permutation to form conjugacy classes, e.g. j -cycles ($2 \leq j \leq n$), disjoint 2-cycles, etc.

(8) Show that x is *central* in G (i.e. $x \in Z(G)$, so that x commutes with **all** the elements of G) if and only if x is in a *conjugacy class* by itself. A: (**if**) Consider that an element $x \in G$ commutes with all the elements $y \in G$, i.e. $xy = yx$. But this *implies* that $xyx^{-1} = x$, therefore x and y are conjugate for all $y \in G$, and therefore x is in a *conjugacy class* by itself. (**only if**) If x is in a conjugacy class by itself, then $xyx^{-1} = x$ for all $y \in g \Rightarrow yx = xy$ for all $y \in G$, and therefore x and y commute. **QED.**

The Quaternion Group and its Relatives

(9) Let $GL(2, \mathbb{C})$ denote the group of all non-singular 2×2 complex matrices. This has a subgroup Q *generated* by the matrices $\xi = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ and $\eta = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, where, *of course*, $i^2 = -1$. Check that $|\langle \xi \rangle| = 4$, and that $\eta \notin \langle \xi \rangle$, so that $|Q| \geq 8$. (*Why?*) Note (and check) that $\eta^2 = \xi^2$, and that $\eta^{-1}\xi\eta = \xi^{-1}$. (Q is called the *quaternion group*).

(ii) Define a **group** G by $\langle x, y \mid x^4 = 1, y^2 = x^2, y^{-1}xy = x^{-1} \rangle$. Prove that *any element* in G can be **rewritten** in the form $x^i y^j$ for some i and j in the ranges $0 \leq i \leq 3$, and $j = 0$ or 1 , so that $|G| \leq 8$. (iii) Prove that $|Q| = 8$.

A: (i) $\xi^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} i^2 & 0 \\ 0 & (-i)^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. $\xi^3 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$. $\xi^4 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} -i^2 & 0 \\ 0 & -i^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$. As $\xi^4 = I$, then the *group generated* by ξ is of **order** 4, i.e. $|\langle \xi \rangle| = 4$ as required. We can *clearly* see that $\eta \notin \langle \xi \rangle$. **Why** is $|Q| \geq 8$? For Q , we have *already found* 4 elements, and, by **multiplying** these on the left by η , we will get *4 other elements*. So, as we have already seen 8 distinct elements, we must have $|Q| \geq 8$. We do the checks by *simple matrix multiplication*, and by noticing that we can **check** $\eta^{-1}\xi\eta = \xi^{-1}$ by *checking* $\xi\eta\xi = \eta$.

(ii) Using the *normal form* defined, we **see** that we can have $1, x, x^2, x^3, y, xy, x^2y$ and x^3y as *valid* elements. Assume that we can reduce *any* word w of length n in the x 's and the y 's to **one** of the 8 forms above. If $w' = wq$ is of *length* $n+1$, then $w' = x^i y^j q$ for $0 \leq i \leq 3$, and $0 \leq j \leq 1$, with $q \in \{x, y, x^{-1}, y^{-1}\}$. We have to *check that the 32 words* can be **reduced** to normal form.

Notice that because $x^3 = x^{-1}$, then if we can *reduce* $x^i y^j x$, then we can **also** reduce $x^i y^j x^{-1}$ — by *reducing* $x^i y^j x^3$ three times using the *previous* method. **Case x.** $x^i y^j x$. If $j = 0$, we have x^{i+1} , which is *OK* as we can *reduce* using $x^4 = 1$ as *necessary*. If $j = 1$, we have $x^i y x$. But $y^{-1} x y = x^{-1}$, so that $y^{-1} x y x = 1$, $y x = x^{-1} y$, so we *have* $x^i x^{-1} y$, which again is *OK* using $x^4 = 1$ as *necessary*.

Case y. $x^i y^j$. If $j = 0$, we have $x^i y$, which is in the normal form. If $j = 1$, then we have $x^i y^2$. But $y^2 = x^2$, so we really have x^{i+2} , which again is OK using $x^4 = 1$ as necessary. Now as $y^2 = x^2 \Rightarrow y^4 = x^4$, if we have handled the case for y , we have handled the case for y^{-1} as well, as to handle y^{-1} , we just handle y^3 3 times. So as **any** word in the x 's and the y 's can be reduced to any of the 8 normal forms, we can say that $|G| \leq 8$.

(T. Porter's Answer): Any element of G can be rewritten in the form $x^i y^j$ for some $0 \leq i \leq 3$, and for some $j = 0, 1$. Suppose that we can reduce any word of length $n-1$ (or less) to one of the **standard** forms. Now assume that $w = w'a$, where w is of length n , so that w' is of length $n-1$, with a being **one** of x, x^{-1}, y or y^{-1} . We can reduce (modulo the relations) w' to $x^i y^j$ for some i and j as before. We now analyse what a does to the **reduced** word.

If $a = y$, and if $j = 0$, then w reduces to $x^i y$. For $a = y^{-1}$ and $j = 0$, w reduces to $x^i y^{-1}$ — but $y^2 = x^2$ and $y^4 = x^4 = 1$, so that $y^{-1} = y^3 = x^2 y$. Therefore, w reduces to $x^{i+2} y$, and possibly further if $i+2 \geq 4$. If $a = y$, and if $j = \pm 1$, then w reduces to $x^i y^2 = x^{i+2}$, or to x^i . If $a = y^{-1}$, and if $j = \pm 1$, then w reduces to $x^i y^{-2} = x^{i-2}$, or to x^i . Both the above could possibly be followed by **further** reductions (mod 4) if $i+2$ or $i-2$ were outside the range $0 \leq i \leq 3$.

If $a = x$, then w reduces to x^{i+1} , or to $x^i y x$. The **first** case is all right as $yx = y^2 y^{-1} x = y^2 x^{-1} y^{-1} = xy^{-1} = xy^3 = x^2 y$, and a further reduction gives us the correct form. Finally, for $a = x^{-1}$, and using $yx^{-1} = xy$, the reduction works as **before**. There are thus at most elements $1, x, x^2, x^3, y, xy, x^2 y, x^3 y$, i.e. $|G| \leq 8$ (but can we be sure that there aren't any duplicates amongst this list?)

(iii) We map $G \rightarrow Q$ by using the two results (i) $|Q| \geq 8$, and (ii) $|G| \leq 8$, to give $|Q| = 8$. We need an isomorphism between the matrices ξ and η , and the generators x and y . We get this by setting $\xi = x$, and setting $\eta = y$. We have **already** shown (in tests) that the relations in (ii) are satisfied by ξ and η in part (i). So $G \cong Q$. **(T. Porter):** The substitution test gives a homomorphism $\varphi: G \rightarrow Q$ given by $\varphi(x) = \xi$, and $\varphi(y) = \eta$. As ξ and η generate Q , this is **onto**; hence $|Q| \leq |G|$, and both *must* be 8.

(10) The generalised quaternion group, Q_{2n} , is defined either as the **subgroup** of $GL(2, \mathbb{C})$ generated by $\xi = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$, and $\eta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, where $\omega = e^{i\pi/n}$; or as being given by the presentation $Q_{2n} = \langle x, y \mid y^2 = x^n, y^{-1} x y = x^{-1} \rangle$. (i) Prove that $x^{2n} = 1$, that $y^4 = 1$, and that any element in Q_{2n} can be written in the form $x^i y^j$, for some i and j in the ranges $0 \leq i \leq 2n-1$, and $j = 0$ or 1 . (ii) Describe all the conjugacy classes of the elements in Q_{2n} . Describe the center of Q_{2n} . Describe the **commutator subgroup** of Q_{2n} . Find the abelianisation of Q_{2n} .

A: Assume that $x = \xi$. Now $\xi^2 = \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega^{-2} \end{pmatrix}$, and $\xi^3 = \begin{pmatrix} \omega^3 & 0 \\ 0 & \omega^{-3} \end{pmatrix}$. Clearly, $\xi^n = \begin{pmatrix} \omega^n & 0 \\ 0 & \omega^{-n} \end{pmatrix}$, depending on if n is odd or even. Thus $\xi^{2n} = \begin{pmatrix} \exp(i\pi) & 0 \\ 0 & \pm \exp(i\pi) \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & \pm(-1) \end{pmatrix}$, and so $\xi^{2n} = \begin{pmatrix} -1 & 0 \\ 0 & \pm(-1) \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & \pm(-1) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$. Therefore, $x^{2n} = 1$. It follows easily that $y^4 = 1$, as $y^2 = x^n \Rightarrow y^4 = x^{2n}$ ($x^{2n} = 1$, so that $y^4 = 1$). Can any element be written in the form $x^i y^j$ for $0 \leq i \leq 2n-1$, and for $0 \leq j \leq 1$?

Assume that we can *reduce* w of length n to normal form. Let $w' = wq$ be of **length** $n+1$, then $w' = x^i y^j q$ for $q \in \{x, y, x^{-1}, y^{-1}\}$. Because $x^{2n} = 1$, then $x^{-1} = x^{2n-1}$, so that if we can handle the case $q = x$, then we can handle the case $q = x^{-1}$ as well. **Similarly**, because $y^4 = 1$, we have $y^3 = y^{-1}$, so if we can *handle* y , we can *handle* y^{-1} as well. **Case x.** $x^i y^j x$. If $j = 0$, we have x^{i+1} , OK, using $x^{2n} = 1$ as *necessary*. If $j = 1$, $x^i y x$. But $y^{-1} x y = x^{-1} \Rightarrow y x = x^{-1} y$, so we *have* $x^i x^{-1} y$, OK. **Case y.** If $j = 0$, we *have* $x^i y$, OK. If $j = 1$, $x^i y^2$. But $y^2 = x^n$, so we *have* x^{i+n} , OK. So **any** word CAN be reduced to *normal* form.

(ii) When we *conjugate* any element $x^i y^j$ by $x^k y^l$, we obtain $x^k y^l x^i y^j y^{-l} x^{-k}$. So we can obtain the *conjugacy class* of any element by **repeated** application of conjugacy by the x and by the y . We start by considering the conjugacy class of x . x conjugated by any power of x is just x . x conjugated by y is $y x y^{-1} = y y^{-1} x^{-1} = x^{-1} = x^{2n-1}$. x^{2n-1} conjugated by any power of x is just x^{2n-1} . x^{2n-1} conjugated by y is $y x^{2n-1} y^{-1} = y x^{-1} y^{-1} = x$. Thus the *conjugacy class* containing x is $\{x, x^{2n-1}\}$.

We now **consider** the conjugacy class containing y . y conjugated by x is $x y x^{-1}$. As $x y = y x^{-1}$, then we *have* $x x y = x^2 y$. y **conjugated** by y is just y . $x^2 y$ conjugated by x is $x^3 y x^{-1} = x^4 y$. $x^2 y$ conjugated by y is $y x^2 y y^{-1} = y x^2 = (x^{-1} y) x = x^{2n-1} y x = x^{2n-1} x^{2n-1} y = x^{2n-2} y$. We will notice a *pattern* developing, and we will expect to get the class $\{y, x^2 y, x^4 y, \dots\} \cup \{x^{2n-2} y, x^{2n-4} y, \dots\}$. This time, it makes **no difference** as to whether n is odd or even, as $2n$ is *always* even. So the conjugacy class **containing** y will always be given by $\{y, x^2 y, x^4 y, \dots, x^{2n-4} y, x^{2n-2} y\}$.

As *before*, we will get conjugacy classes $\{x^2, x^{2n-2}\}, \{x^3, x^{2n-3}\}, \dots$. So, if say $n = 4$, then we get $\{x, x^7\}, \{x^2, x^6\}, \{x^3, x^5\}, \{x^4\}$. If $n = 5$, we will *get* $\{x, x^9\}, \{x^2, x^8\}, \{x^3, x^7\}, \{x^4, x^6\}, \{x^5\}$. We can now *classify* all of the conjugacy classes ($n+3$ of them): $\{y, x^2 y, x^4 y, \dots, x^{2n-4} y, x^{2n-2} y\}, \{x y, x^3 y, \dots, x^{2n-1} y\}, \{x, x^{2n-1}\}, \{x^2, x^{2n-2}\}, \dots, \{x^{n-1}, x^{2n-(n-1)}\}, \{x^n\}$, and $\{1\}$. The **centre** of Q_{2n} is those elements in a *conjugacy class* by themselves. From the list, these are $\{1\}$ and $\{x^n\}$.

Commutators. $[x, y]$. There are 4 cases to consider (as previously). Case 1: $[x, y] = x^i x^j x^{-i} x^{-j} = I$. Case 2: $[x, y] = x^i y x^j y^{-1} x^{-i} x^{-j} = x^i (y x^j) y^{-1} x^{-i-j} = x^i (x^{-j} y) y^{-1} x^{-i-j} = x^{i-j-i-j} = x^{2n-2j}$. Case 3: $[x, y] = x^i x^j y x^{-i} y^{-1} x^{-j} = x^{i+j} x^i y y^{-1} x^{-j} = x^{2i}$. Case 4: $[x, y] = x^i y x^j y y^{-1} x^{-i} y^{-1} x^{-j} = x^i x^{-j} y x^{-i} y^{-1} x^{-j} = x^i x^{-j} x^i y y^{-1} x^{-j} = x^{2i-2j}$. So what are the *commutators* of Q_{2n} ? They are the **even** powers of x , so that $[Q_{2n}, Q_{2n}] = \{1, x^2, x^4, \dots, x^{2n-4}, x^{2n-2}\}$. What is Q_{2n}^{Ab} ? We will have 4 *cosets* in $Q_{2n} \setminus [Q_{2n}, Q_{2n}]$: $\{1, x^2, \dots, x^{2n-2}\} = \langle x_{1/2} \rangle$; $x \langle x_{1/2} \rangle$; $\langle x_{1/2} \rangle y$; and $x \langle x_{1/2} \rangle y$. Therefore, Q_{2n}^{Ab} is of *order* 4 for all n .

(T. Porter's Answer): Recall that as conjugating by ab *corresponds* to first conjugating by b , and **then** by a : $(ab)c(ab)^{-1} = a(bcb^{-1})a^{-1}$; and *conjugating* a **product** $a(xy)a^{-1} = axa^{-1}.aya^{-1}$; it is a *good idea* to work out conjugates of each generator by each (*other*) generator. Now $y x y^{-1} = y^2 (y^{-1} x y) y^{-2} = x^n x^{-1} x^{-n} = x^{-1}$, and $y x^{-1} y^{-1} = (y x y^{-1})^{-1} = x$, so that conjugating x by *itself* gives x back again, so that x is conjugate to **itself** and its **inverse** only: $\{x, x^{-1}\}$, or $\{x, x^{2n-1}\}$ is a *conjugacy class*. Conjugating x^k by some word $a \in Q_{2n}$ gives $a x^k a^{-1} = (a x a^{-1})^k$, so yields *either* x^k , or x^{-k} (since a consists of y 's, y^{-1} 's, x 's and x^{-1} 's only). Hence *each* $\{x^k, x^{2n-k}\}$ is a *conjugacy class*. Note: x^n is in the **centre** of Q_{2n} since $x^n = x^{2n-n}$, so that $\{x^n\}$ is a *conjugacy class*. Turning to the conjugacy class of y , $x y x^{-1} = x^2 y$, since $x y = y x^{-1}$. Now *conjugate* $x^2 y$ by both x and y : $x(x^2 y)x^{-1} = x x^2 x^{-1} . y x y^{-1} = x^4 y$; **and** $y(x^2 y)y^{-1} = y x^2 y^{-1} . y y y^{-1} = x^{2n-2} y$.

Continuing with the *new elements*, we will get all $x^{2k}y$ for $k = 0, \dots, n-1$. This seems to give a *conjugacy class* $\{y, x^2y, \dots, x^{2n-2}y\}$ with n elements. Now *start* with $y^{-1} = y^3 = x^2y$ — but that is *already there!* (Take **care**). What about xy : as $x^{2n} = 1$, this *cannot be written* as $x^{2k}y$, so it isn't there. *Conjugating* xy by y , $y(xy)y^{-1} = yxy^{-1} \cdot y = x^{-1}y$; and by x , $x(xy)x^{-1} = x \cdot xyx^{-1} = x^3y$.

Thus $\{xy, \dots, x^{2k-1}y, \dots, x^{2n-1}y\}$ is a conjugacy class. We *so far have* $\{1\}$, $\{x^n\}$, $\{x^k, x^{2n-k}\}$ for each $k = 1, \dots, n-1$; $\{y, \dots, x^{2n-2}y\}$, and $\{xy, \dots, x^{2n-1}y\}$, so that *counting elements*, we have $1 + 1 + (n-1) \times 2 + n + n = 4n$ elements — **all** elements are accounted for. Any element in $Z(Q_{2n})$ will be in a *singleton conjugacy class*, so that $Z(Q_{2n}) = \{1, x^n\}$.

The *commutator subgroup* of Q_{2n} will be normally generated by $[x, y]$ (since $[y, x] = [x, y]^{-1}$, and we can use *the tutorial questions on page 5* to expand a commutator of a **product** in terms of products of commutators of generators, together with **conjugates** of these commutators). Now $[x, y] = xyx^{-1}y^{-1} = x^2y \cdot y^{-1} = x^2$. The *commutator subgroup* must contain all x^{2k} , where $k \in \{0, 1, \dots, n-1\}$. (Conjugating these yields *elements in the same list* by our **earlier** calculations).

To calculate Q_{2n}^{Ab} , add the commutator $[x, y]$ into the *relations* for Q_{2n} . Informally, one can then **commute** the elements of the relations as they will be *consequences* of the old relations, plus $xy = yx$. So $Q_{2n}^{Ab} = \langle x, y \mid y^2 = x^n, y^{-1}xy = x^{-1}, x^2 = 1 \rangle \cong \langle x, y \mid y^2 = x^n, x^2 = 1, xy = yx \rangle$. If n is *even*, $x^n = 1$, so this **becomes** $\langle x, y \mid y^2 = 1, x^2 = 1, xy = yx \rangle$, which is the *Klein 4 group* $K_4 = C_2 \oplus C_2 = \{1, x, y, xy\}$, with $xy = yx$, $x^2 = 1$, and $y^2 = 1$. If n is **odd**, $y^2 = x^n$ implies that $y^2 = x$, so that $y^4 = 1$ since $x^2 = 1$. This gives C_4 .

5th March 2001

As $N \triangleleft G$ means that $xNx^{-1} = N$ for all $x \in G$, N is **normal** \Leftrightarrow it is a union of *conjugacy classes*. **Example:** List the normal subgroups of D_5 . *Lagrange's Theorem* gives possible orders of subgroups as 1, 2, 5 and 10 (1 = **trivial**; 10 = the **whole** thing). Assume that $H \triangleleft D_5$, and that some element of order 2 is in H . Then $H = D_5$. ($1 \in H$, and some $r^i \in H$ — but then *all of the 5 elements conjugate* to r^i must be **in** H , i.e. $|H| \geq 1+5 = 6$, so that $|H| = 10$).

The *rotation subgroup* $\langle r \rangle = \{1, r, r^2, r^3, r^4\} \triangleleft D_5$. Therefore, $D_5/\langle r \rangle \cong C_2$. **Lemma:** If G is a finite group, and if $H \leq G$, with $[G:H] = 2$, then $H \triangleleft G$. **Proof** (If $x \in G$, xNx^{-1} is a *subgroup* so that $1 \in N$): xN is *either* N or $G \setminus N$ (there are only 2 cosets). Nx is *either* N or $G \setminus N$, **depending** on if $x \in N$, or if $x \in G \setminus N$. In *all* cases, $xN = Nx$, i.e. $xNx^{-1} = N$ as *required*.

6th March 2001

Centre

If G is a *group*, then the centre of G , $Z(G)$, is given by $\{x \in G \mid \forall g \in G, xg = gx\}$. Now $1 \in Z(G)$; if $x_1, x_2 \in Z(G)$, then $(x_1x_2)g = x_1gx_2 = g(x_1x_2)$; and if $x \in Z(G)$, then $x^{-1} \in Z(G)$. So $Z(G)$ is a *subgroup* of G . **Example:** $D_6 = \langle r, s \mid r^6 = 1, s^2 = 1, (rs)^2 = 1 \rangle$. In *general*, if $x \in Z(G)$, then $gxg^{-1} = x$ for all $g \in G$ (and *conversely*). So $x \in Z(G) \Leftrightarrow x$ is *only conjugate to itself*. In D_6 , the elements in “*singleton*” conjugacy classes are 1 and r^3 , i.e. the **centre** of D_6 is $Z(D_6) = \{1, r^3\}$.

Lemma: If $G = \langle X \mid R \rangle$, then $g \in Z(G)$ if and only if for all $x \in X$, we have $xg = gx$.

Proof: (\Rightarrow) As $X \subset G$, then $xg = gx$ for all $x \in X$ (we knew if “ $\forall g \in G$ ” already). (\Leftarrow) If $y \in G$, then $y = x_1^{\pm 1} \dots x_n^{\pm 1}$, with $x_i \in X$, and assume that for all $x \in X$, we have $xg = gx$. Now look at $yg = x_1^{\pm 1} \dots x_{n-1}^{\pm 1} g x_n^{\pm 1} = \dots = x_1^{\pm 1} g x_2^{\pm 1} \dots x_n^{\pm 1} = g x_1^{\pm 1} \dots x_n^{\pm 1} = gy$.

Proposition: $Z(G) \triangleleft G$. **Proof:** Suppose that if $x \in G$, and if $g \in Z(G)$, then $xgx^{-1} = g \in Z(G)$, so that $xZ(G)x^{-1} = Z(G)$. **Example:** $D_6/Z(D_6)$. $[D_6, Z(D_6)] = 6$. We have two candidates (C_6 and D_3) for the quotient. Which one? Hand Wave! In $D_6/Z(D_6)$, we kill off $Z(D_6)$, so that we kill off r^3 . This suggests that $D_6/Z(D_6)$ should have the presentation $\langle r, s \mid r^6 = 1, s^2 = 1, (rs)^2 = 1, r^3 = 1 \rangle$ ($r^3 = 1$ to “kill off” the centre) $\cong \langle r, s \mid r^3 = 1, s^2 = 1, (rs)^2 = 1 \rangle$ (as $r^6 = 1$ is a consequence of $r^3 = 1$) $\cong D_3$.

Van Dyck's Theorem and the Substitution Test

Formalising “Presentations”: free groups and their quotients. **Free Groups.** The idea is that given a set X , we build a group $F(X)$ from the elements of X (and X^{-1}) with as few constraints as possible. (i) $F(X) = \langle X \mid \rangle$. (ii) If $X = \{a\}$, then $F(X) = \{a^n : n \in \mathbf{Z}\} \cong C_\infty$.

12th March 2001

Example of Construction. Let $X = \{x, y\}$. In $F(X)$, we will need all x^n , where $n \in \mathbf{Z}$, and all y^m , where $m \in \mathbf{Z}$. So we will need all $x^{\alpha_1} y^{\beta_1} x^{\alpha_2} y^{\beta_2} \dots x^{\alpha_r} y^{\beta_r}$, with $\alpha_i, \beta_j \in \mathbf{Z}$. But we can assume that the word is reduced, so that no interior α_i or β_j is zero. **Example:** if $\alpha_2 = 0$, then $x^{\alpha_1} y^{\beta_1} x^0 y^{\beta_2} x^{\alpha_3} \dots = x^{\alpha_1} y^{\beta_1 + \beta_2} x^{\alpha_3}$, i.e. $x^0 = y^0 =$ the identity or empty word.

We can multiply in an obvious way by **concatenation** and **reduction**, e.g. if $w_1 = xyx^2y^{-3}$, and if $w_2 = y^3x^{-1}yx^{-1}$, then $w_1w_2 = (xyx^2y^{-3})(y^3x^{-1}yx^{-1}) = xyx^2y^0x^{-1}yx^{-1}$ (laws of indices) = $xyx^2x^{-1}yx^{-1}$ (reduces to) = $xyxyx^{-1}$ (laws of indices again).

Definition: A group F is free on a subset $X \subseteq F$ if for any group G , and any assignment $\theta: X \rightarrow G$, there is a unique homomorphism $\theta': F \rightarrow G$ restricting to θ , e.g. $X = \{x, y\}$ as before. If G is arbitrary, and if $\theta: X \rightarrow G$ picks out two elements (g_x and g_y), then $\theta'(x^2yx^{-3}y^3x) = g_x^2 g_y g_x^{-3} g_y^3 g_x$. **Example:** $\theta': F(x, y) \rightarrow D_6$ defined by $\theta(x) = r$, and $\theta(y) = s$.

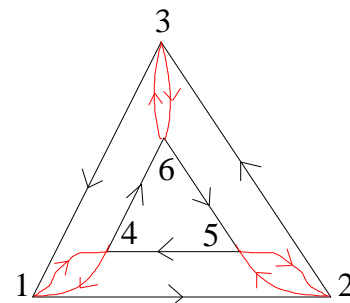
It follows that $\theta'(x^2yx^{-3}y^3x) = r^2sr^{-3}s^3r = r^2sr^3sr = 1$. In fact, θ' is onto (since r and s generate D_6). But another choice of mapping may not yield an epimorphism. Consider $\phi(x) = r^2$, and $\phi(y) = s$. Then $r \notin \text{Im } \phi'$. Note that θ' (from now on, forget the ‘) is an **epimorphism**, since the image of X is a generating set for G in this case. The 1st Isomorphism Theorem says that if $\phi: G \rightarrow H$ is a homomorphism, then $G/\text{Ker } \phi \cong \text{Im } \phi$.

So if ϕ is onto, then all the information on ϕ is **encoded** in its Kernel. In our case, $\theta: F(x, y) \rightarrow D_6$, and its Kernel contains x^6, y^2 and $(xy)^2$. But it also contains x^2yx^2y, yx^6y^{-1} , etc. Ker ϕ is a normal subgroup of $F(x, y)$, so that it is closed under **products, inverses and conjugation**. **CLAIM:** x^2yx^2y is a product of conjugates of $x^6, y^2, xyxy$ and their inverses. Now $xxyxyx = x(xyxy)x^{-1}xy^{-1}xy = x(xyxy)x^{-1} \cdot x(y^2)^{-1}x^{-1}(xyxy)$. **QED.**

The Todd-Coxeter Heuristic

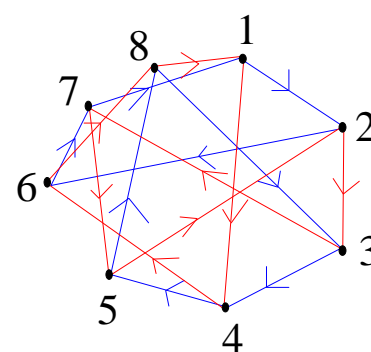
Example: $\langle x, y \mid x^3 = e, y^2 = e, xyxy = e \rangle$. The table *closes up* to give 6 elements, and a permutation representation: $G \rightarrow S_6$, where $x \rightarrow (1\ 2\ 3)(4\ 6\ 5)$, and $y \rightarrow (1\ 4)(2\ 5)(3\ 6)$. We have a *Cayley Colour Graph* as shown.

x				y			x y				x x ⁻¹ y y ⁻¹					
x	x	x		y	y		x	y	x	y	x	x ⁻¹	y	y ⁻¹		
1	2	3	1	1	4	1	1	2	5	4	1	1	2	3	4	4
2	3	1	2	2	5	2	2	3	6	5	2	2	3	1	5	5
3	1	2	3	3	6	3	3	1	4	6	3	3	1	2	6	6
4	6	5	4	4	1	4	4	6	3	1	4	4	6	5	1	1
5	4	6	5	5	2	5	5	4	1	2	5	5	4	6	2	2
6	5	4	6	6	3	6	6	5	2	3	6	6	5	4	3	3



Exercise: Try $\langle a, b \mid baba^{-1} = e, abab^{-1} = e \rangle$, and $\langle x, y \mid x^2y^3, x^3y^4 \rangle$.

a				b			a a ⁻¹ b b ⁻¹							
a	b	a	b ⁻¹	b	a	b	a ⁻¹	a	a ⁻¹	b	b ⁻¹			
1	2	3	4	1	1	4	5	2	1	1	2	7	4	8
2	6	8	3	2	2	3	4	6	2	2	6	1	3	5
3	4	6	7	3	3	7	1	4	3	3	4	8	7	2
4	5	2	6	4	4	6	7	5	4	4	5	3	6	1
5	8	1	2	5	5	2	6	8	5	5	8	4	2	7
6	7	5	8	6	6	8	3	7	6	6	7	2	8	4
7	1	4	5	7	7	5	8	1	7	7	1	6	5	3
8	3	7	1	8	8	1	2	3	8	8	3	5	1	6



For the **second** one, we use the method *described below*, where we have four tables. It turns out that we obtain just *one* element, the *identity* element for the group. Try it out and see — you will get “*deductions*” to place in a table, but at some stage will get e.g. 5 y 5, so in this case, 5 is the **trivial** operation, implying that x is also the **identity** operation, so that we only have 1 element.

Todd-Coxeter Coset Enumeration

Q: Find $|G|$ given $G = \langle g_1, g_2, \dots, g_m \mid r_1, r_2, \dots, r_n \rangle$. **Step 1: Initialise.** Prepare a relations table, ‘REL’, with a column for each relator, and an *unlimited* number of rows. Place a “1” at the beginning and the end of each row. Prepare a *coset-generator table*, ‘CGT’, for storing $\langle \text{coset} \rangle \times \langle \text{generator} \rangle = \langle \text{coset} \rangle$, with one column for **each** of the generators g_i , one column for each g_i^{-1} , and an *unlimited number of rows*. Label the **first** row “1”. (These are the *two tables* shown previously).

Prepare a **deduction** table, ‘DEDN’, with 3 columns; and a **coincidence** table, ‘COIN’, with 2 columns, both having an *unlimited* number of rows. Let \underline{s} denote the number of cosets (elements) defined, and set $\underline{s} = 1$. Now “*add deduction* $x.g_i = y$ ” means to check to see whether $(x g_i y)$, or $(x g_i^{-1} x)$, is already a row in *DEDN*. If not, place $(x g_i y)$ in the 1st available *row* in *DEDN*.

Similarly, “*add coincidence* $u \equiv v$ ” means to **check** to see whether $(u \ v)$ or $(v \ u)$ is a row in COIN. If not, place $(u \ v)$ when $u < v$, or place $(v \ u)$ when $v < u$, in the 1st **available** row in COIN. **Step 2: Make a definition.** If CGT is complete, then **STOP**. Otherwise, *increment* s ($s := s+1$), and define $s = k.g_i^{\pm 1}$ for some $1 \leq k \leq s$, and for some $1 \leq i \leq m$, to *fill in some blank* in CGT. Start a **new** row in REL, and place an “ s ” at the *beginning and end* of each column. Start a new row in CGT, and enter the **new** entries.

Step 3: Fill up the holes. Fill all possible holes in REL using the *entries* in CGT. If a one-hole gap in one of the columns is filled, and we obtain $x \ g_i \ y \ g_i \ z$ (where y is *new*), then either $x.g_i = y$ and $y.g_i = z$ are *already* known; or one of them is known but **another** is a deduction. If there **is** a deduction, *add* this deduction, and *underline* $x \ y$ or $y \ z$ in REL. If DEDN and COIN are **both** empty, go back to step 2, but *otherwise* go on to steps 4 and 5.

Step 4: Process a coincidence. If there is a *non-empty* row in COIN, process this coincidence as follows: if $(x \ y)$, with $x < y$, is a row in COIN, **compare** rows x and y in CGT (and REL) as shown. For each g_i (and *each* g_i^{-1}), if $x.g_i = u$, but $y.g_i$ is blank, do *nothing*; if $y.g_i = v$, but $x.g_i$ is *blank*, add *deduction* $x.g_i = v$; if $x.g_i = u$, and if $y.g_i = u$, do *nothing*; and if $x.g_i = u$, if $y.g_i = v$, and if $u \neq v$, add **coincidence** $u \equiv v$. *Delete* row y in REL and in CGT. **Replace** every y in REL and in GCT by x . **Remove** the row $(x \ y)$ from COIN. Go back to Step 3.

	g_i	g_i^{-1}	g_i	g_i^{-1}
x	7		u	
y		8	v	

Step 5: Process a deduction. If there is a non-empty row in DEDN, *process this deduction* as follows: if $(x \ g_i \ y)$ is a **row** in DEDN, then $x.g_i = y$, and $y.g_i^{-1} = x$. *Check* that $x.g_i$ is *blank* in CGT. If not, and if $x.g_i = z \neq y$ in CGT, then **add** coincidence $z \equiv y$. Usually, $x.g_i$ is *blank*, so put $x.g_i = y$, and put $y.g_i^{-1} = x$ in CGT. *Remove* row $(x \ y)$ from DEDN. Go back to Step 3.

18th March 2001

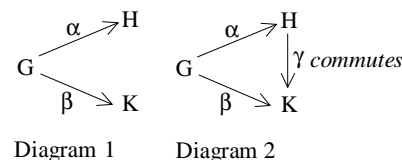
Normal Closure

$(\text{Ker } \phi \rightarrow F(X) \xrightarrow{\phi} G)$. If G is a group, and if $S \subseteq G$, then the **normal closure** of S (in G) is the *smallest* normal subgroup of G containing S . **Lemma:** $\langle\langle S \rangle\rangle = \bigcap \{N \mid N \triangleleft G, S \subseteq N\}$. $\langle\langle S \rangle\rangle$ is also obtainable by forming *all consequences* of S , where a “consequence of S ” is a product of **conjugates** of elements of S .

Generators (more precisely): Suppose that we have $X \subseteq G$, where G is a group, then there is an *inclusion function*, $X \rightarrow G$. This induces a **homomorphism** $\phi: F(X) \rightarrow G$. We say that X is a set of generators for G if ϕ is *onto*. **Proposition:** Every group is a *homomorphic image* of a free group. **Proof:** Take X to be the *underlying* set of G .

Relations (or *relators*): Given a set X of generators (of G), and *thus* $\phi: F(X) \xrightarrow{\text{onto}} G$, a relation is an *element* of $\text{Ker } \phi$, where $\text{Ker } \phi$ is the *relation* subgroup. **Definition:** (a) Given a group G and a set X of *generators*, a subset R of $F(X)$ is called a set of *defining relations* for G if $\langle\langle R \rangle\rangle = \text{Ker } \phi$. (b) A presentation for G is a *pair* $\langle X \mid R \rangle$, where X is a set of **generators**, and R is a set of **defining relations**. G is *finitely generated* if X can be chosen to be finite. G is *finitely presented* if X and R can be chosen to be finite.

Lemma: Let G, H and K be groups, with $\alpha: G \rightarrow H$, and $\beta: G \rightarrow K$, as shown in *diagram 1* — **homomorphisms** with α onto and $\text{Ker } \alpha \subseteq \text{Ker } \beta$. It follows that there is a *homomorphism* $\gamma: H \rightarrow K$, such that $\gamma\alpha = \beta$, i.e. as shown in *diagram 2*. **Sketch Proof** (well definition of γ left as an exercise): The 1st Isomorphism Theorem $\Rightarrow H \cong G/\text{Ker } \alpha$ (α onto). So $\gamma(g \text{ Ker } \alpha) = g\text{Ker}\beta \in \text{Im } \beta \subseteq K$ works. **End of Proof.**



Theorem (van Dyck): If R and S are subsets of $F(X)$, and if $R \subseteq S$, then there is an epimorphism $\langle X|R \rangle \xrightarrow{\theta} \langle X|S \rangle$. The **kernel** of θ is the normal closure of the *image* of $S \setminus R$ as a subset of $\langle X|R \rangle$. **Proof:** Use the lemma for $\langle\langle R \rangle\rangle \subseteq \langle\langle S \rangle\rangle$ ($\text{Ker } \alpha \subseteq \text{Ker } \beta$).

The Substitution Test (Useful)

Suppose that $G := \langle X|R \rangle$, and that H is a **group**. If $\theta: X \rightarrow H$ is a *function*, then θ extends to a homomorphism, $\theta: G \rightarrow H$, if, and only if, for all $x \in X$, and all $r \in R$, the result of *substituting* $\theta(x)$ for x in R yields the **identity** of H . **Example:** $G = D_3$, $X = \{x, y\}$, and $R = \{x^3, y^2, (xy)^2\}$ ($= r_1, r_2, r_3$). Is there a *homomorphism* from D_3 onto $C_3 = \{1, a, a^2\}$? ($= H$).

Try **assigning** elements of C_3 to x and y . (a) Try $\theta(x) = a$, and $\theta(y) = a$. Now $\theta(r_1) = a^3 = 1$ in C_3 , but $\theta(r_2) = a^2 \neq 1$, *no good*. (b) Try $\theta(x) = a$, and $\theta(y) = a^2$ — still *no good*. (c) Try $\theta(x) = a$, and $\theta(y) = 1$. Here, $\theta(r_1) = 1$; $\theta(r_2) = 1^2 = 1$; and $\theta(r_3) = a \cdot 1 \cdot a \cdot 1 = a^2 \neq 1$, *no good*. Proof by **exhaustion** yields that there is no epimorphism from D_3 onto C_3 .

Application: listing *endomorphisms* and *automorphisms* of groups. **Illustration** of the method: (a) Consider $C_n = \langle x \mid x^n = 1 \rangle$. Define (or try to define) an *endomorphism* $\varphi_r: C_n \rightarrow C_n$, where $\varphi_r(x) = x^r$ ($0 \leq r < n$). This does give an *endomorphism* (by the **substitution** test), where $\varphi_r(x^n) = \varphi_r(x)^n = x^{rn} = (x^n)^r = 1^r = 1$. Which of these are *automorphisms*? **Test for automorphism:** (i) is φ onto?; and (ii) is φ 1-1? ($\varphi: G \rightarrow G$). If G is *finite*, it is enough to check that φ is 1-1, i.e. that $\text{Ker } \varphi$ is *trivial*. **Back** to φ_r . What is $\text{Ker } \varphi_r$? If $1 = \varphi_r(x^s)$, then $x^{sr} = 1$, i.e. $n \mid sr$ (e.g. $\varphi_2: C_6 \rightarrow C_6$, $x^3 \in \text{Ker } \varphi_2$).

20th March 2001

Proposition: φ_r is an *automorphism* if and only if $\text{gcd}(r, n) = 1$. **Proof:** Assume that φ_r is an *automorphism*, then there is some s s.t. $\varphi_r(x^s) = x$ (because φ_r is *onto*), i.e. $x^{rs} = x^1$; $rs \equiv 1 \pmod n$. r has an *inverse* mod n , so that $1 = rs + kn$, and $\text{gcd}(r, n) = 1$. Now **assume** that $\text{gcd}(r, n) = 1$, so $\exists s$ s.t. $rs \equiv 1 \pmod n$. If $x^t \in \text{Ker } \varphi_r$, then $x^{rt} = 1$; $x^t = x^{srt} = 1^s = 1$, i.e. x^t was the *identity*, and the only element in $\text{Ker } \varphi_r$ is the *identity*. Now $\text{Ker } \varphi_r = \{1\}$, so that φ_r is an *automorphism*. **End of Proof.**

Corollary (of the *proof*): If $rs \equiv 1 \pmod n$, then $(\varphi_r)^{-1} = \varphi_s$. The set of *automorphisms* of any group G form a **group**, $\text{Aut}(G)$. Now consider $\alpha: G \xrightarrow{\cong} G$, and $\beta: G \xrightarrow{\cong} G$. The composition is $\beta\alpha: G \rightarrow G$. What is $\text{Aut}(C_n)$? $\text{Aut}(C_n) = \{\varphi_r \mid \text{gcd}(r, n) = 1\}$, and $\varphi_r\varphi_s = \varphi_{rs}$ (reduced mod n if $\geq n$). For *any* n , U_n is the **abelian** group of integers in \mathbf{Z}_n which have *inverses* (under multiplication).

$U_2 = \{1\}$ ($Z_2 = \{0,1\}$). $U_3 = \{1,2\} \cong C_2$ ($Z_3 = \{0,1,2\}$). $U_4 = \{1,3\} \cong C_2$. $U_5 = \{1,2,3,4\} \cong C_4$. $U_6 = \{1,5\} \cong C_2$. $U_7 = \{1,2,3,4,5,6\} \cong C_6$. $U_8 = \{1,3,5,7\} \cong K_4$, the *Klein 4-group* (elements of orders 1 and 2 only). **Corollary:** $\text{Aut}(C_n) \cong U_n$. **Lemma:** If p is *prime*, then $U_p \cong C_{p-1}$ (look up a *proof*). **Proposition:** $\text{Aut}(C_p) \cong C_{p-1}$.

Proposition: If p is *prime*, with $t > 1$, then $\text{Aut}(C_{p^t}) \cong C_{p^{t-1}(p-1)}$. The *orders* are easy to check: Z_{p^t} has p^t *elements*, and p^{t-1} of them have a *factor* in **common** with p^t , thus $|U_{p^t}| = p^t - p^{t-1}$. **Challenges:** (i) Find a *presentation* of $\text{Aut}(C_n)$ if $n = p_1^{t_1} p_2^{t_2}$; (ii) **prove that** $\text{Aut}(C_7) \cong \text{Aut}(C_9)$; that $\text{Aut}(C_{19}) \cong \text{Aut}(C_{27})$; and then *find some more!*

(i) If $n = p_1^{t_1} p_2^{t_2}$, then $\phi(n) = \phi(p_1^{t_1}) \phi(p_2^{t_2}) = [p_1^{t_1-1}(p_1-1)][p_2^{t_2-1}(p_2-1)]$. Therefore, *in this case*, $\text{Aut}(C_n) \cong C_x$, where x is the **red** expression. (ii) $U_7 = \{1,2,3,4,5,6\} \cong C_6$; and $U_9 = \{1,2,4,5,7,8\}$. **Evidence:** (a) we have the same *number of elements* in both groups; (b) we have *matching* element orders: for U_9 , $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64$, OK (as $64 - 9 \times 7 = 1$); $4^3 = 64$; $5^6 = 15625$; $7^3 = 343$; and $8^2 = 64$. For U_7 , $2^3 = 8$; $3^6 = 729$; $4^3 = 64$; $5^6 = 15625$; and $6^2 = 36$.

Note that we have *orders* (2, 3, 3, 6, 6) in each case. Now draw up the **Cayley** table for each group. We want to *swap some rows and columns* in U_9 's table to get the "*same*" table as U_7 . Swaps are influenced by the **matching** orders.

	U_7						U_9								After Swaps on U_9								
Order	U_7	U_9	1	2	3	4	5	6	1	2	4	5	7	8	1	4	2	7	5	8			
2	6	8	1	1	2	3	4	5	6	1	1	2	4	5	7	8	1	1	4	2	7	5	8
3	2,4	4,7	2	2	4	6	1	3	5	2	2	4	8	1	5	7	4	4	7	8	1	2	5
6	3,5	2,5	3	3	6	2	5	1	4	4	4	8	7	2	1	5	2	2	8	4	5	1	7
			4	4	1	5	2	6	3	5	5	1	2	7	8	4	7	7	1	5	4	8	2
			5	5	3	1	6	4	2	7	7	5	1	8	4	2	5	5	2	1	8	7	4
			6	6	5	4	3	2	1	8	8	7	5	4	2	1	8	8	5	7	2	4	1

Experiment, and find that we can *set* ($U_7 = U_9$) $1 = 1$, $2 = 4$, $3 = 2$, $4 = 7$, $5 = 5$, and $6 = 8$ to get the *isomorphism*. **Now** $U_{19} = \{1, 2, \dots, 18\} \cong C_{18}$. And $U_{27} = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$. As before, *find the orders of elements* and match them up; draw **tables**; **swap**; and **find** the isomorphism.

(b) **Dihedral Groups**, $D_n = \langle x, y \mid x^n = y^2 = (xy)^2 = 1 \rangle$. Try to *define* $\phi: D_n \rightarrow D_n$ by $\phi(x) = x^a y^b$, and $\phi(y) = x^c y^d$. **Substitution Test:** if ϕ is to be an *endomorphism*, we need $(x^a y^b)^n = 1$, $(x^c y^d)^2 = 1$, and $(x^a y^b x^c y^d)^2 = 1$. For now, *restrict* to $n = 2m+1$, so that $(x^a y^b)^{2m+1} = 1$. **But** $(x^a y)^{2m+1} = x^a y \neq 1$, so that we *must* have $b = 0$. **Similarly**, $\phi(y^2) = 1$ means that $(x^c y^d)^2 = 1$, and if $d = 0$, this *cannot* happen (n is odd). If $d = 1$, OK. The **only** ϕ 's allowed are as follows: $\phi_{a,c}(x) = x^a$, and $\phi_{a,c}(y) = x^c y$. Proceed as **before** to get *automorphisms*. **n^2+1 endomorphisms:** For *automorphisms*, we need $\text{gcd}(a,n) = 1$, and *any* c will do. Therefore, $|\text{Aut}(D_n)| = n\phi(n)$. (**Notes:** $n = 2m+1$, $\phi =$ Euler's *phi* function, and $\phi(n) = |U_n|$). We have *similar* analysis for when n is even.

Tutorial

H, G, [G:H]. If you know $|H|$ and $[G:H]$, then $|G| = |H|[G:H]$. **Changes** to Todd Coxeter to enumerate *cosets* rather than elements: consider that we have $G = \langle x \mid x^6 \rangle$, and $H = \langle x^3 \rangle$. Add one table for each *given* generator y of H . (The **red** table is the generator of H). From what is *shown*, we deduce that $[G:H] = 3$, and that the **permutation** representation is given by $G \rightarrow S_3$, with $x \rightarrow (1\ 2\ 3)$.

x	x	x	x	x	x
1	2	3	1	2	3
2	3	1	2	3	1
3	1	2	3	1	2

x	x	x
1	2	3

	x	x^{-1}
1	2	3
2	3	1
3	1	2

Let $G = D(3, 3, 2) = \langle x, y \mid x^3, y^3, (xy)^2 \rangle$, and let $H = \langle x \rangle$. From what is shown on the left, we see that $[G:H] = 4$. We know that $|H| \leq 3$, because $x^3 = 1$. Permutation representation: $x \rightarrow (2\ 3\ 4)$, and $y \rightarrow (1\ 2\ 3)$ ($G \xrightarrow{\rho} S_4$). $\rho(x)$ has order 3, so that x has order **divisible** by 3. So

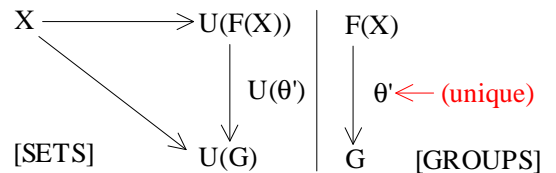
as $x^3 = 1$, we have $O(x) = 3$, i.e. $H = \{1, x, x^2\}$, and $|G| = 12$. **Squeezing** yet further, $(1\ 2\ 3)$ and $(2\ 3\ 4)$ are *even* permutations, and they generate *all even* permutations in S_4 — so they generate A_4 , the *alternating* group (made up of all **even** permutations, where A_4 has order 12). ρ maps *generators to generators* of A_4 , so that $A_4 \cong D(3,3,2)$.

Now consider $D(4, 3, 2) = \langle x, y \mid x^4 = y^3 = (xy)^2 = 1 \rangle$. Take $H = \langle x \rangle$. (**Answer**: $|G| = 24$). Conclusion from the *diagrams*: $[G:H] = 6$. We know that $|H| \leq 4$, because $x^4 = 1$. Permutation representation: $x \rightarrow (2\ 3\ 4\ 5)$, and $y \rightarrow (1\ 2\ 3)(4\ 5\ 6)$. $G \xrightarrow{\rho} S_6$. Now $\rho(x)$ has order 4, so that x has **order** divisible by 4. Therefore, as $x^4 = 1$, $O(x) = 4$, i.e. $H = \{1, x, x^2, x^3\}$, and $|G| = 6 \times 4 = 24$. **QED**.

26th March 2001

Free Groups and Tietze Transformations

Recall that given a set, X , the free group, $F(X)$, on X , is the group which is *freely generated* by the symbols $x \in X$, and x^{-1} for $x \in X$ (so that all words w are made up of x 's and x^{-1} 's, **where** if xx^{-1} or $x^{-1}x$ occurs, it is *cancelled*) Multiplication is by concatenation, followed by (possibly) reduction. Each word can be reduced to a **single** reduced word. Free groups have the *universal* property that $X \xrightarrow{\theta} U(G)$ (where $U(G)$ is the *underlying* set of G) gives the unique extension $F(X) \xrightarrow{\theta'} G$.



Corollary: If we have $f: X_1 \rightarrow X_2$, then f induces a unique $F(f): F(X_1) \rightarrow F(X_2)$. **Proof** (“natural” in the diagram means the natural assignment of the “word” x to the element $x \in X$): This homomorphism, $F(f)$, just **maps** a word in $F(X_1)$ to the **word** in $F(X_2)$ made up from the *images* of the letters.

Example: if $X_1 = \{a, b, c\}$, and if $X_2 = \{x, y\}$, where f is as follows: $f: a \rightarrow x, b \rightarrow x, c \rightarrow y$, then $F(f)(aba^{-1}bc^2) = F(f)(a)F(f)(b)F(f)(a^{-1})... = xxx^{-1}xy^2 = x^2y^2$. **Corollary** (of this): If X_1 and X_2 have the same cardinality, then $F(X_1) \cong F(X_2)$ (pick a *bijection* between X_1 and X_2). The **cardinality** of a base X for $F(X)$ is called the **rank** of $F(X)$.

Tietze Transformations. Consider $S_3 = \langle a, b \mid a^3 = b^2 = (ab)^2 = 1 \rangle$. We also know that S_3 is *generated* by the transpositions (1 2), (1 3), and (2 3), and so has *some presentation of the form* $\langle x, y, z \mid x^2 = 1, y^2 = 1, z^2 = 1, \dots \rangle$. It also has a presentation of the form $\langle a, b, c \mid a^3 = 1, b^2 = 1, c^2 = 1, abc^{-1} = 1 \rangle$. We would *expect* to be able to write x, y and z in terms of a and b (and c) and *vice versa*. The method is (*intuitively*) that of **substitution** and its **inverse**.

Example: In $\langle a, b, c \mid a^2 = b^2 = c = 1 \rangle$, c is *redundant*, and could be omitted to give $\langle a, b \mid a^2 = b^2 = 1 \rangle$. The **aim** is to give some *basic moves on presentations* that leave the group unchanged, and that are “*complete*” in the sense that any **two** presentations of the same group can be *linked* to a series of such moves. In the following, as usual, $G = \langle X \mid R \rangle$.

(**T1**) *Adding a superfluous relation.* $\langle X \mid R \rangle$ becomes $\langle X \mid R' \rangle$, where $R' = R \cup \{r\}$, and $r \in \langle\langle R \rangle\rangle$ is a **consequence** of the given relations. (**T2**) *Removing a superfluous relation.* $\langle X \mid R \rangle$ becomes $\langle X \mid R' \rangle$, where $R' = R \setminus \{r\}$, and $r \in \langle\langle R \rangle\rangle$. (**T3**) *Adding a superfluous generator.* $\langle X \mid R \rangle$ becomes $\langle X' \mid R' \rangle$, where $X' = X \cup \{g\}$, g is a **new symbol not** in X , and $R' = R \cup \{wg^{-1}\}$, where w is a word in the **old** generators. (**T4**) *Removing a superfluous generator* $\langle X \mid R \rangle$ becomes $\langle X' \mid R' \rangle$, where $X' = X \setminus \{g\}$, $R' = R \setminus \{wg^{-1}\}$, and $w \in F(X')$ is a word **not** using g . These form the **Tietze transformations**.

27th March 2001

Example: Consider $D_3 = \langle a, b \mid a^3 = 1, b^2 = 1, (ab)^2 = 1 \rangle$, or $D_3 = \langle a, b, c \mid a^3 = 1, b^2 = 1, c^2 = 1, abc^{-1} = 1 \rangle$. *Intuitively*, we write $c = ab$, and substitute for ab in $(ab)^2 = 1$. *Formally*, $\langle a, b \mid a^3 = 1, b^2 = 1, (ab)^2 = 1 \rangle \xrightarrow{T3} \langle a, b, c \mid a^3 = 1, b^2 = 1, (ab)^2 = 1, abc^{-1} = 1 \rangle \xrightarrow{T1}$, but *need to check* that c^2 is a **consequence** $\longrightarrow \langle a, b, c \mid a^3 = 1, b^2 = 1, (ab)^2 = 1, abc^{-1} = 1, c^2 = 1 \rangle \xrightarrow{T2}$, but *need to check* that $(ab)^2$ is a **consequence** of the others $\longrightarrow \langle a, b, c \mid a^3 = 1, b^2 = 1, c^2 = 1, abc^{-1} = 1 \rangle$.

c^2 needs to be *written* as a product of **conjugates** of $r = a^3$, $s = b^2$, $t = (ab)^2$, $u = abc^{-1}$, and their *inverses*. Now $cb^{-1}a^{-1}abab = cab$. And $c^{-1}(abc^{-1})c = c^{-1}ab$; now *invert*, giving $b^{-1}a^{-1}c$. Therefore, $(cb^{-1}a^{-1})(abab)c^{-1}(cb^{-1}a^{-1})c = u^{-1}.t.c^{-1}(u^{-1})c = c^2$ (so that c^2 *was* a *consequence* of t and u). **Second** check: check that $(ab)^2$ is a *consequence* of r, s, u and $v = c^2$: $uv = abc^{-1}c^2 = abc = c(abc)c^{-1} = cab = cab(abc^{-1}) = cababc^{-1} = c^{-1}(cababc^{-1})c = abab$, **OK**.

Example: Consider $\langle a, b, c, d \mid ab = c, bc = d, cd = a, da = b \rangle = \langle a, b, c, d \mid abc^{-1}, bcd^{-1}, cda^{-1}, dab^{-1} \rangle$. *Informally*, substitute $c = ab$ in the **other** relations, and delete c (T4 *after* using T1 and T2 to **eliminate**), to give $\langle a, b, d \mid bab = d, abd = a, da = b \rangle$. The *2nd relator* gives $bd = 1$, so that $d = b^{-1}$. Substituting b^{-1} for d in the other relations, and **deleting** d , gives $\langle a, b \mid bab = b^{-1}, b^{-1}a = b \rangle$ (T1 and T2 to *process the 2nd relation*; then eliminate d from the *other relations* by using T1 and T2; and **then** use T4). The 2nd relation $\Rightarrow a = b^2$; and *substituting* b^2 for a in the other relations, and then **deleting** a , gives $\langle b \mid bb^2b = b^{-1} \rangle$, or $\langle b \mid b^5 = 1 \rangle \cong C_5$.

Details of the 1st to 2nd step: The idea is to *preprocess the presentation* to get rid of c in the other relations. $\langle a, b, c, d \mid abc^{-1}, bcd^{-1}, cda^{-1}, dab^{-1} \rangle = (T1 \text{ twice}) = \langle a, b, c, d \mid abc^{-1}, bcd^{-1}, abd^{-1}b, cda^{-1}, abda^{-1}, dab^{-1} \rangle$. **Check:** $ac^{-1}cd^{-1}b = (abc^{-1})b^{-1}(bcd^{-1})b$ — so it is a *consequence* of the others. Now use T2 twice to give $\langle a, b, c, d \mid abc^{-1}, abd^{-1}b, abda^{-1}, dab^{-1} \rangle = (T4) = \langle a, b, d \mid abd^{-1}b, abda^{-1}, dab^{-1} \rangle$, etc.

Tietze's Theorem (1908): Given two (*finite*) presentations of the same group, one can be obtained from the *other* by a set of **Tietze** transformations. **Proof:** see *Knots and Surfaces*, pages 135 to 138.

Exercises

(1) Calculate *completely* $\text{Aut}(D_3)$ and $\text{Aut}(D_4)$. Note that these have 6 and 8 elements respectively. Try to find **presentations** of the groups. (ii) Applying the **general** method, calculate directly (not using the *formula*) the orders of $\text{Aut}(D_5)$ and $\text{Aut}(D_6)$. (iii) *Longer term and more open ended:* How would the calculation of the **automorphisms** of Q_{2n} differ from that of D_n ?

A: (i) $D_3 = \langle x, y \mid x^3 = y^2 = (xy)^2 = 1 \rangle = \{1, x, x^2, y, xy, x^2y\}$. If $\varphi: D_3 \rightarrow D_3$ is a **homomorphism**, φ is *determined* by the values $\varphi(x)$ and $\varphi(y)$, and we **must** have $(\varphi(x))^3 = 1$, $(\varphi(y))^2 = 1$, and $(\varphi(x)\varphi(y))^2 = 1$. If $(\varphi(x))^3 = 1$, then $\varphi(x) = 1$ or x or x^2 *will do*, but $\varphi(x) = y$ or xy or x^2y will **not** do, as $(x^i y)^3 = x^i y \neq 1$ (for $0 \leq i \leq 2$), as $x^i y$ is of *order* 2. So we have 3 *choices* for $\varphi(x)$. But, we *cannot* choose $\varphi(x) = 1$, as it is not of order 3 — we want an **automorphism**, not an **endomorphism**. So $\varphi(x) = x$ and $\varphi(x) = x^2$ are OK. If $(\varphi(y))^2 = 1$, then $\varphi(y) = x^i$ will *not do*, as $(x^i)^2 = x^{2i} \neq 1$ when we have an *even power* of x ; and $x^3 = 1$ (for the odd case).

Let us check the *other* choices of $\varphi(y)$: **if $\varphi(y) = y$, then $(\varphi(y))^2 = 1$. Similarly for xy and x^2y . $((x^2y)^2 = xxyxxy = xy^{-1}x^{-1}xy^{-1}x^{-1} = 1)$. So we have 3 *choices* for $\varphi(y)$, all of **order** 2, giving the total **possible** number of *combinations* to be $2 \times 3 = 6$. We must now *check that* $(\varphi(x)\varphi(y))^2 = 1$. But all **possible** $\varphi(x)\varphi(y)$ will be in the **red** list above, so it *follows* that $(\varphi(x)\varphi(y))^2 = 1$ in all cases. **Therefore**, $|\text{Aut}(D_3)| = 6$, with $\varphi(x) = x$ or x^2 , and $\varphi(y) = y$ or xy or x^2y .**

Presentation. In the table, we have all the possible *combinations*. Let $e = \varphi_1$, and let $a = \varphi_2$. Now $a^2(x) = \varphi_2(\varphi_2(x)) = \varphi_2(x) = x$, and $a^2(y) = \varphi_2(\varphi_2(y)) = \varphi_2(xy) = \varphi_2(x)\varphi_2(y) = x.y = x^2y$, so that $a^2 = \varphi_3$. Now $a^3(x) = \varphi_2(x) = x$, and $a^3(y) = \varphi_2(x^2y) = x^3y = y$, so that $a^3 = e$, and so a is of *order* 3. Let $b = \varphi_4$. Now $b^2(x) = \varphi_4(x^2) = x$, and $b^2(y) = \varphi_4(y) = y$, so that $b^2 = e$, and so b is of *order* 2. It *looks like* $\text{Aut}(D_3) \cong D_3$. Do a and b *generate* φ_5 and φ_6 ? Now $ab(x) = \varphi_2(\varphi_4(x)) = \varphi_2(x^2) = x^2$, and $ab(y) = \varphi_2(\varphi_4(y)) = \varphi_2(y) = xy$, so that $ab = \varphi_5$. Similarly, $a^2b = \varphi_6$. Finally, is $(ab)^2 = 1$? We *know* that $ab = \varphi_5$, and that $\varphi_5^2 = e$, so that $(ab)^2 = e$. So, *letting* $e = \varphi_1$, $a = \varphi_2$, and $b = \varphi_4$, then $\text{Aut}(D_3) \cong \langle a, b \mid a^3 = e, b^2 = e, (ab)^2 = e \rangle = \{e, a, a^2, b, ab, a^2b\} \cong \{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6\}$.

	$\varphi(x)\varphi(y)$	
φ_1	x	y
φ_2	x	x^2y
φ_3	x	x^2y
φ_4	x^2	y
φ_5	x^2	xy
φ_6	x^2	x^2y

Element | 1 x x^2 x^3 y xy x^2y x^3y Q: Calculate *completely* $\text{Aut}(D_4)$. A: $D_4 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$, with $x^4 = 1$, $y^2 = 1$, and $(xy)^2 = 1$. If $(\varphi(x))^4 = 1$, we need *elements* in D_4 of order 4. From the **table**, we see that the only *options* are $\varphi(x) = x$ or x^3 . If $(\varphi(y))^2 = 1$, we need *elements* in D_4 of order 2. Again, from the table, our **options** are $\varphi(y) = x^2$ or y or xy or x^2y or x^3y . If $(\varphi(x)\varphi(y))^2 = 1$, we need *elements* $\varphi(x)\varphi(y)$ of order 2. There are 10 *possible elements* for $\varphi(x)\varphi(y)$. The ones *where* $\varphi(y) = x^2$ mean that $\varphi(x)\varphi(y) = 1$ — **not** of order 2. So we *conclude* that $|\text{Aut}(D_4)| = 8$, with $\varphi(x) = x$ or x^3 , and $\varphi(y) = y$ or xy or x^2y or x^3y .

Presentation. Let $e = \varphi_1$, and let $a = \varphi_2$ — then $a^2 = \varphi_3$, $a^3 = \varphi_4$, and $a^4 = e$, so that a is of *order* 4. Let $b = \varphi_5$. Now $b^2 = e$, i.e. b is of *order* 2. It **looks** like $\text{Aut}(D_4) \cong D_4$. It is *possible to show* that $ab = \varphi_6$, that $a^2b = \varphi_7$, and that $a^3b = \varphi_8$. Therefore, a and b *generate* all of the φ_i (for $1 \leq i \leq 8$). *Finally*, is $(ab)^2 = e$? We **know** that $ab = \varphi_6$, and that it is *possible to show* that $\varphi_6^2 = e$, so that $(ab)^2 = e$, OK. So *letting* $e = \varphi_1$, $a = \varphi_2$, and $b = \varphi_5$, then $\text{Aut}(D_4) \cong \langle a, b \mid a^4 = e, b^2 = e, (ab)^2 = e \rangle = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\} \cong \{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6, \varphi_7, \varphi_8\}$.

	$\varphi(x)$	$\varphi(y)$
φ_1	x	y
φ_2	x	xy
φ_3	x	x^2y
φ_4	x	x^3y
φ_5	x^3	y
φ_6	x^3	xy
φ_7	x^3	x^2y
φ_8	x^3	x^3y

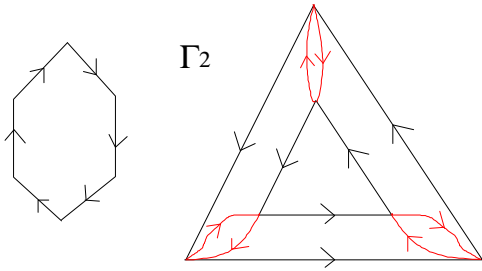
(ii) Calculate $|\text{Aut}(D_5)|$ without using the **formula**. Here, we want $\varphi(x)$ to be an element of *order* 5. In D_5 , the **only** elements of order 5 are x, x^2, x^3 and x^4 . Further, we want $\varphi(y)$ to be an *element* of order 2. Now $(x^a)^2 \neq 1$ for $1 \leq a \leq 4$, as $x^5 = 1$. We *cannot* have $\varphi(y) = 1$ (order 1). So $\varphi(y) = y$ or xy or x^2y or x^3y or x^4y are *all valid* — they have **order** 2. Therefore, we have 4 *choices* for $\varphi(x)$, and 5 choices for $\varphi(y)$, so that we have 20 *combinations* in all. Do all of these have $\varphi(x)\varphi(y)$ of order 2? By *tabulation*, we can answer “**yes**” to this question. Therefore, we conclude that $|\text{Aut}(D_5)| = 20$ (which *agrees* with the formula), with $\varphi(x) = x$ or x^2 or x^3 or x^4 , and $\varphi(y) = y$ or xy or x^2y or x^3y or x^4y .

Q: Calculate $|\text{Aut}(D_6)|$ without using the **formula**. A: By analysing the *orders of elements* in D_6 , $\varphi(x) = x$ or x^5 , as these are the *only* elements of order 5. Further, $\varphi(y) = x^3$ or y or xy or x^2y or ... or x^5y , as these are the *only* elements of order 2. But we **also** need $\varphi(x)\varphi(y)$ to be of order 2. If $\varphi(y) = x^3$, then $\varphi(x)\varphi(y)$ is of *order* 3, *not order* 2 (all **other** $\varphi(y)$ are valid). Therefore, we conclude that $|\text{Aut}(D_6)| = 2 \times 6 = 12$ (which *agrees* with the formula), with $\varphi(x) = x$ or x^5 , and $\varphi(y) = y$ or xy or x^2y or x^3y or x^4y or x^5y .

(iii) Now $Q_{2n} = \{x, y \mid y^2 = x^n, y^{-1}xy = x^{-1}\}$. The calculations would differ in that we would consider *elements* in the set $Q_{2n} = \{x^i y^j \mid 0 \leq i \leq 2n-1, j = 0 \text{ or } 1\}$ as our *transformations*, i.e. $\varphi(x) = x^a y^b$, and $\varphi(y) = x^c y^d$. This time, we *require* $(\varphi(x))^{2n} = 1$, $(\varphi(y))^4 = 1$, and $\varphi(x)\varphi(y)\varphi(x) = \varphi(y)$ for a *valid Automorphism*. We would start by finding all the **orders** of the elements from Q_{2n} , pick *possible* $\varphi(x)$ and $\varphi(y)$ based on the correct **orders**, and then, for each *pair*, we would test to see whether $\varphi(x)\varphi(y)\varphi(x) = \varphi(y)$ was true or not.

The *Todd-Coxeter heuristic* can be adapted to give the number of cosets of a subgroup H in a group G which is presented with *generators* and *relations*. The subgroup H is specified by the generators (which are given as **words** in the generators of G), and the method is essentially the same as for the case $H =$ the identity subgroup handled in the *tutorial*, except that one **more** table is needed for each given generator of G . If you are *given or know* the order of H , then you can **deduce** the order of G if you know the number of *cosets*, which is an output from the heuristic.

(2) Find the **order** of G when $G = \langle a, b \mid a^5 = b^4 = e, b^{-1}ab = a^2 \rangle$, using $H = \langle a \rangle = \langle a \mid a^5 = e \rangle$. Give the *permutation representation* and the *Cayley graph* relative to this **subgroup**. (3) Find the *order* of G when $G = \langle a, b \mid a^4 = e, a^2ba = b^2 \rangle$, using $H = \langle a \rangle = \langle a \mid a^4 = e \rangle$.



Another example: C_6 with $X = \{a\} = \langle a \mid a^6 = 1 \rangle$ will give the **first** graph on the left, while C_6 with $X = \langle a^2, a^3 \rangle$ will give graph Γ_2 on the left. An automorphism of a (*coloured directed*) graph maps **vertices** to **vertices** and **edges** to **edges**, so as to respect **incidence** (i.e. if a goes to $\varphi(a)$, and if b goes to $\varphi(b)$, then an edge *from* a to b corresponds to an edge *from* $\varphi(a)$ to $\varphi(b)$).

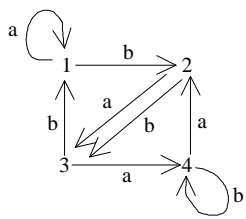
Direction. Colouring/Labelling (if $a \xrightarrow{x} b$ has label x , then **so does** $\varphi(a) \xrightarrow{x} \varphi(b)$).

Theorem (Frucht): Given any (*finite*) group G , there is a labelled directed graph Γ such that $G \cong \text{Aut}(\Gamma)$. **Examples:** $\text{Aut}(\Gamma_1) \cong D_3$, and $\text{Aut}(\Gamma_2) \cong C_6$. You can do this with *any* Cayley Graph.

If you do a **Todd-Coxeter** w.r.t. a subgroup $H (\neq 1)$, the permutation representation gives a Schreier Coset Diagram, e.g. $G = \langle a, b \mid a^3, b^3, (ab)^2 \rangle$, with $H = \langle ab, a^2b^2 \rangle$. We have *tables* (as shown) so that $|G| = 3|H|$. Permutation representation: $G \xrightarrow{\theta} S_3$, with $a \rightarrow (1\ 2\ 3)$, and $b \rightarrow (1\ 3\ 2)$. As $\theta(ab) = 1$, it is unlikely to be a *faithful* representation. It follows that θ is probably **not** an injection. (A T.C

a	a	a	b	b	b	a	b	a	b			
1	2	3	1	1	3	2	1	1	2	1	2	1
2	3	1	2	2	1	3	2	2	3	2	3	2
3	1	2	3	3	2	1	3	3	1	3	1	3

a	b	a	a	b	b	a	b	a ⁻¹ b ⁻¹				
1	2	1	1	2	3	2	1	1	2	3	3	2
H-Table												
								2	3	1	1	3
								3	1	2	2	1



with $k = \langle a \rangle$ gives *another* representation: $a \rightarrow (2\ 3\ 4)$, and $b \rightarrow (1\ 2\ 3)$, with $\theta': G \rightarrow S_4$, and so $G = 4|K|$ (*). Now $\langle (2\ 3\ 4), (1\ 2\ 3) \rangle$ is of *order* 12 (**). Further, $a^3 = 1$, so that $|K| \leq 3$. Now $(*) \Rightarrow |G| \leq 12$, and $(**) \Rightarrow |G| \geq 12$, so that $|G| = 12$. The Schreier Coset Diagram for the *second* representation is as shown on the left.

Exam Paper: May 2001

Answer 3 questions out of 5 (Questions Done: 2, 3, 5)

- (1) Define what it means for a subgroup N of a group G to be normal. **[2 marks]**

A group G is given by the permutation:

$$G := \langle x, y \mid x^6 = e, yxy^{-1} = x^4, y^3 = e \rangle.$$

Prove that:

- (i) Any element of G can be written in at least one way in the form $x^i y^j$ with $0 \leq i \leq 5$ and $0 \leq j \leq 2$. **[8 marks]**
- (ii) The subgroup $N = \langle x \rangle$, generated by the element x , is a *normal* subgroup of G . **[7 marks]**
- (iii) The quotient group G/N is cyclic of order 3. **[3 marks]**
- (2) Define the four Tietze transformations on a group presentation $\langle X \mid R \rangle$, where X is the set of generators and R the set of relators. **[4 marks]**

Show, using Tietze transformations that the group with the presentation:

$$\langle a, b, c \mid a(bc^{-1})b, (cb^{-1})^2a \rangle$$

is cyclic, generated by $x = bc^{-1}$.

[14 marks]

Find the order of x in G .

[2 marks]

- (3) Using the Todd-Coxeter heuristic relative to the subgroup $H = \langle a \rangle$, find the order of the group with presentation:
 $G := \langle a, b \mid a^4 = e, b^3 = e, ab^2a = b \rangle$. **[10 marks]**

Find the order of the subgroup $\langle a^2b \rangle$.

[5 marks]

Show that the subgroup $\langle a^2, aba^{-1} \rangle$ contains the element b and hence show that this subgroup is normal. **[5 marks]**

- (4) (a) Suppose that $\alpha: G \rightarrow G$ is a homomorphism such that for all $g \in G$, $\alpha(g) = g^2$. Prove that G is abelian. **[5 marks]**
- (b) Let x be an element of order n in a group G . Suppose r is a natural number *coprime* to n . Prove that the r^{th} power, x^r , of x also has order n . **[9 marks]**
- (c) Let H be a subgroup of a group G and let $N_G(H) = \{n \in G: n^{-1}Hn = H\}$. Prove that $N_G(H)$ is a subgroup of G and that H is a normal subgroup of $N_G(H)$. **[6 marks]**

- (5) Let G be any group. Define what it means for two elements g and g' of G to be *conjugate*. **[2 marks]**

Prove that *conjugacy* is an equivalence relation. **[7 marks]**

Now consider the dihedral group, D_n , which has presentation:

$$\langle x, y \mid x^n = 1, y^2 = 1, (xy)^2 = 1 \rangle.$$

This has $2n$ elements all of which can be written in the form $x^i y^j$ with $i = 0, 1, \dots, n-1$ and $j = 0, 1$. Find the conjugacy classes of D_n . **[11 marks]**