On Permutation Groups

Alan Turing

1 3

Below is a careful, line-by-line transcription of the visible typed text and the marginal/handwritten edits in the image. Where something is struck out or inserted by hand, bracketed notes indicate it. Likewise, small bits of Turing's algebraic notation are reproduced (with unavoidable uncertainty in places). Ellipses "..." indicate letters or symbols too unclear to recover exactly.

Technique for investigating [handwritten above: "any"] particular upright U.

In order to prove H unexceptional it will suffice to prove that J contains all three-cycles, for if this is so J will be a self conjugate subgroup of S, and since it is not the identity it must be either A or S. It would also be sufficient to prove that J contains all 2-cycles. We shall prove [typed words struck out] [handwritten "Thereom 1" or "Theorem 1"] If J contains a member of form $(\alpha, R^m\alpha)$ or $(\alpha, R^m\alpha)(\beta, \gamma)$ where m is prime to T, then it contains all three-cycles, and in the first case mentioned all two-cycles. [handwritten note near this: "must be greater than 4. $(\alpha, R^m\alpha)(\beta, \gamma)$ must ... comm ..."]

Suppose J contains $(\alpha, R^m\alpha)$. We will write α_k for $R^{mk}(\alpha)$. The symbols $\alpha_0, \alpha_1, \ldots, \alpha_{r-1}$ include all the T symbols. Then J contains [handwritten: "$R^{(\alpha_0,\alpha_1)}$ ..." or similar], i.e. (α_s, α_{s+1}), since this is (α_0, α_2) [...] It therefore contains (α_0, α_2) since this is (α_0, α_2) [handwritten marginal formulas indicating $(\alpha_0, \alpha_2)(\alpha_0, \alpha_1)(\alpha_2, \alpha_1)$, etc.].

(if $T > 2$). It contains (α_0, α_3) which is $(\alpha_0, \alpha_3)(\alpha_0, \alpha_1)(\alpha_2, \alpha_1)(\alpha_2, \alpha_3)$ [...] and repeating the argument it contains (α_0, α_r) if $T > 3$, and repeating the argument it contains (α_0, α_r) for every $\alpha_0 < r$. Finally it contains $(\alpha_{p1}, \alpha_{p2})$ since this is $R^{(m^p)}(\alpha_0, \alpha_2)\, R^{(p^{-1})}$ if $\nu \neq pC(T)$. Thus J contains every two-cycle (and every three-cycle).

Notes:

1. Parenthetical remarks such as “$(\alpha_0, \alpha_2)(\alpha_0, \alpha_1)(\alpha_2, \alpha_1)$” are handwritten corrections or annotations in the margins. 2. Phrases like “must be greater than 4” or “must ... comm ...” are partial handwritten notes near the main text. 3. Where the image is unclear or text is fully struck out, bracketed “[...]” or ellipses indicate uncertain or missing content.

2 5a

Below is a best-effort transcription of the handwritten notes. Because they are somewhat informal, spacing and line breaks are preserved where feasible. Square brackets [. . .] indicate either an illegible segment, an uncertain reading, or clarifying context. Superscripts, subscripts, and negative subscripts appear in math mode (e.g. α_{-1}). Parentheses (. . .) are as in the original notations.

Case 8) $(\alpha_0\ \alpha_1)(\alpha_2\ \alpha_{-2})$

b) $(\alpha_0\ \alpha_1)(\alpha_{-1}\ \alpha_3)$

[There is a sketch of circles labeled α_0, α_1, α_2, α_3, with arrows from $\alpha_0 \to \alpha_1 \to \alpha_3$, and so on.]

Then equivalently

$(\alpha_0\ \alpha_1)(\alpha_2\ \alpha_{-2})$ Then [illegible scribbled text] $(\alpha_3\ \alpha_{-2})(\alpha_{-1}\ \alpha_{-5}?)$ [unclear or partially struck out]

gives $(\alpha_0\ \alpha_1)(\alpha_2\ \alpha_{-3})$ if $T > 7$

ok

[More heavily scribbled writing follows, indecipherable.]

Notes: - The circle-and-arrow diagram appears to show some permutation cycles or orbits labeled “α_0, α_1, α_2, α_3,” along with possibly arrows indicating transitions. - Negative subscripts like “α_{-1}” or “α_{-2}” appear as part of Turing’s notation. - The last lines are almost fully scribbled out, so their precise content cannot be recovered.

3 5

Below is a careful line-by-line rendering of both the typed text and the handwritten/marginal notes visible in your image. Where words or symbols are too faint or otherwise unclear, bracketed ellipses “[...]” or notes indicate this. Strikethrough text is shown with “ ... ,” and handwritten insertions or comments appear in square brackets.

c) $(\alpha_0, \alpha_2)(\alpha_2, \alpha_3)$ belongs to J, where are all different. (handwritten note near “α_2, α_3”: “3 different ??? for x_2, x_3”)

d) $(\alpha_0, \alpha_1)(\beta, \beta')$ belongs to J, where are all different. ([handwritten note: “β different ???”])

e) $(\alpha_0, \alpha_1)(\alpha_{-1}, \alpha_2)$ belongs to J, [handwritten next to it : “(???)$''$]

f) $(\alpha_0, \alpha_1)(\alpha_2, \alpha_3)$ belongs to J, [handwritten next to it : “(???)$''$]

[*P.T.O.* →] [handwritten arrow meaning “please turn over”]

It is easily seen th t cases b) and c) are essentially (by changing th e sigh of m) and that e) and f) are the same. In case a) since $(\alpha, \alpha_2)(\beta', \beta')$ belongs [typed text here partially crossed out or obscured]

[Below that, handwritten permutations:] $\big((\alpha_0, \alpha_1)(\beta)\big)\big((\alpha_0, \alpha_1)(\beta')\big) = (\alpha_0, \alpha_1)(\beta)(\alpha_0, \alpha_1)(\beta')$

[handwritten arrows and notes continuing the algebra, for example] $= (\alpha_0, \alpha_1)(\beta)(\alpha_0, \alpha_2)(\beta') \ldots$ does $(\alpha_0, \alpha_1)(\beta)(\alpha_0, \alpha_2)(\beta') = \ldots$

Notes: - Lines c) and d) ended with “are all different.” in the typescript, struck through. - Marginal notes about “3 different ??? for α_2, α_3” are handwritten, only partially legible. - The final lines (“It is easily seen ...”) are partially crossed out, so text about “and that e) and f) are the same” is partly visible. The subsequent permutations in parentheses are mostly in pen.

4 7

Below is a faithful transcription of the typed text in the image, including spacing and any apparent typos or irregularities (for example, “±t” instead of “It”). Square brackets are used for clarifications where something is ambiguous:

$\pm t$ is very easy to apply theorem II. We my first express U, UR, UR^2 etc., in cycles: this my be done for inst nce by writin g the alph bet out double and also writing out the sequence $UA, UB, \ldots UZ$. By putting the former above the letter in v rious positions we get th e permut tions n UR^s. Among these we may look for permut tions which h ave a three cycle end all other cycles of length pr me to 3. By r ising this to an ppropri te power we obt in e three cycle which my or my not satisfy the conditions in theorem II. If we are not suc cesful we may use other permut tions in HJ. We may also be able in e similer way to generate e permut tion which j a pair of two-cycles.

The following upright wes chosen at rendom :*

ABCDEFGHIJKLMNOPQRSTUVWXYZ
MNYTFBGRSLAKOEWKPCJQZDHVUI

In cycles it is $(AMOWHRCYUZISJLXVDTQPK)(BNEF)(G) = U$. Then $U^{22} := (BE)(NF)$.

The distance BE is 3, which is prime to 26. The dist nce NF is 8. Hence theorem II applies, end J includesthe whole of A, and therefore H includes A.

5 11

Below is a faithful transcription of the typed text, preserving spacing and typos:

The detailed search

$T = 1, 2, 3, 4$

$\pm t$ is not difficult to prove that there are no exception l groups when T is 1,2 or 3. The case $T = 4$ needs special investigation as it has been expres ly excluded from theorem $\pm I$. The exceptional uprights in this case are $(1), (13), (24), (13)(24), (12)(34), (32)(14), (1234), (4321)$. The exceptional groups H are the identity, the cyclic groups $((1234)), ((13)(24))$, the four-group, consisting of the identity and all permutations of form $(\alpha\ \beta)(\gamma\ \delta)$, and a group isomorphic with the four group and generated by (13) and (24).

$T = 5$

6 13

Below is a careful transcription of typed text, preserving spacing and typos:

$T = 8$

This needs r-ther more investigation th-n the previous cases, partly because it is the l-rgest numebr yet considered, and partly because it has more factots.

Obviously the permutations which commute with (R) or with a power of R or generate an intransitive group will be exceptional. We will consider that we are looking for other forms of exceptional xxxx upright.

We have various means for dealing with th e permutations.

7 14

This is indicated by the v lue of the commut·tor and ixxx "O.K." Wh en all these fail a query will be shown, end the upright investigated further later.

$t = 1$

We may first go over the main plan, considering seperately what is to be done withthe varòus classes of conjugates in the symmetric group.

666cycles. These are left asi e till the double threes have bèen conidered.

Double threes. Th ese pre arr nged in pairs (as transformed by $(CH)(EF)(DG)^v$) which leaves A,B fixed and xxxxxxxx satisfies $a^vRv^{-1}R'$ and dealt with in detail.

Triple twos. Very few of these n eed to be considered in det il. Those βith the pair (CH) give $(BAC)/(...)$ βith other cycles on a slide, and so are either O.K. under d) or equivalent to a double three. Those with the pair (DH),re reduced to a $t = 4$ case under a), and those with the pair (GG) are paired with ones having (DH).

Four-and-twos need only be considered when their squares are intransitive β or commute with R^4 by theorem II.

Other cases consist of ones wh ree th ree or more letters [...]

8 15a

Below is a best-effort, verbatim transcription of a typed page diagonally crossed out. Spacing, punctuation, and typographical quirks are preserved, with bracketed ellipses for unclear text. Since the entire page is struck through, it was presumably meant to be discarded or revised:

th e analysis rther further. Theorem III effectively enables us to confine our attention to sequences where g is constant throughout each coset of C the commutator group of H. If j represents th e function which is equal to th e reciprocal of th e index of C, for values in C, and is x 0 outside, then Rj operting on any function converts it into one which is constant on the cosets, and has no effect applied to functions already having this property: in fact it averages over cosets. This operator Rj commutes with all Rp. Also if xxx and

then (if g constant in cosets). Thus we can xxxxxx work with f' instead of f and confine ourselves entirely to functions constant in the cosets, i.e. effectively to functions in the factor-group H/C, which is Abelian. We hve thüs reduced the original problem to the c se of en Abelian group.

9 16

Below is a literal transcription, preserving spacing, punctuation, and typos:

The upràght $(CDF)(EGH)$ is exceptionl en d the corresponding group consisgts of the elements withth e invariants

11111111	8	elements	11111111
12214554	64		25527667
13272515	64		13245423
15187216	64		34657564
24636425	64		14737415
33476674	64		12216336
77777777	8		77777777
	336		

Transformation of the group with $(AG)(CH)(EC)$, which commutes with R, gives another group which contins $(CFG)(DEH)$. The invariants of this latter group are given in th e last column. These invariants are useful for verifying that other exceptional uprights belong to these groups.

XXXXXXXXXXX

We have to investig te fiññxx the six-cycles whose squares are exceptional. They are shown below

$(CEDGFH)$ X $(CGDHFE)$ Invariant 15132723 (above) $(CHDETG)$ X $(CDFEGH)$ Invariant 12216336 (above) [$CFFEGD$?] X X [CHE...?] [possibly “Slide (ABDH)(CE) O.K.”?] [$CDEHGF$?] X X [$CFEDGH$?] X

[Handwritten formulas or notes faintly behind text, referencing $(CE)(ABDH)$ etc.]

10 19a

Below is a best-effort, line-by-line transcription of typed text also crossed out diagonally. Spacing, punctuation, and typographical quirks are preserved. Where characters or words are unclear, bracketed ellipses indicate:

If

$$r = \prod_{i=1}^{N} b_i^{-1} r_i^{s_i} b_i,$$

then

$$\nu\nu(a^{-r}\, a) = \nu\nu\Big(\prod_{i=1}^{N} \big((b_i a)^{-1}\, r_i^{s_i}\, b_i a\big)\Big)$$

i.e. (3,f$_1$) is satisfied. Also

$$\chi_a\Big(a^{-1}\, r_a\, (a\, b)\Big) = \chi_a\Big(\chi_a(\chi_a^{-1} b)\Big)$$

[handwritten marks here]

so that (3,f$_1$, $a^{-1}r_a, b$) is satisfied. But if (3,f$_1$, s_i, r_i, b) are satisfied for all b then (3,f$_1$, r_s, b) is satisfied for all b. Consequently (3,f$_1$) is satisfied and the corollary to theorem 1 applies.

In the cases when the centre of $\mathfrak{M}$ consists either of the identity alone or of the whole group there is always a solution of the equations (6). The expressions on the right h nd sides of these equations always represent centre elements, so that in the case where the centre consists of the identity alone, there is a solution by putting $\zeta_i = 1$ for each i. If $\mathfrak{M}$ is Abelian we [text unclear or incomplete]. For the general case we have to be able to find all the relations (7).

11 20

Below is a literal transcription of typed text, reproduced verbatim:

$t = 2$

We xxxxx find it worth while to apply the principle (ii) bn a rather larger scale. There are four permutations V which leave A and C fixed; xxxxx they are

A B C D E F G H
C B A H G F E D
F A D G B E H
A F C H E B G D

From a single permutation wė thus obtain as many as four xxxx generating isomorphic groups J, e.g. from $(BDEFHG)$

$(BDEFHG)$
$(BHGFDE)$
$(FDBGHE)$
$(FHEBDG)$

These may be trnsformed into eculvlent forms, en d the alphabetically e rliest chosen. We permit taking the reciprocal as a form of transformation. Thus we get $(BDEFHG), (BEDEFGH)$; $(BGDFEH)$? $(BDGTHE)$. By these means we reduce the six-cycles th at need be considered do wn to 18. As before we ectully consider first their squares xxxxxx xxxxxx (double threes) in xx the hope that they will be unexceptionl en d the six cycle need not be specially investigated.

12 21

Below is a verbatim transcription of typed text, preserving spacing and typos. List format with each line starting with a six-cycle in parentheses:

Six cycles and double-threes

$(BDEFHG)$ Slide $(ACG)(BFDHE)$ O.K. indirect
$(BDEFFG)$ SLIDE $(AB)(CEFHD)$ O.K.

$(BDEGFH)$ $(BET)(DGH).\,(CFG)(EHA) = (ATH)(CBEDG)$ O.K.
$(BDGEHF)$ SLIDE $(AD)(FCB)$ O.K.
$(BDBEHG)$ SLIDE $(BAG)(DCEH)$ O.K.
$(BDEHGF)$ Invariant 34657564, giving group K'.
$(BDFEHG)$ SLIDE $(BA)(DCFGH)$ O.K.
$(BDFGHE)$ SLIDE $(BA)(CFD)(HEG)$ O.K.
$(BDFHGE)$ SLIDE $(BAEH)(DCF)$ O.K.
$(BDFHGE)$ SLIDE $(BAEH)(DCF)$ O.K.
$(BDGFEH)$ Invrint 34657564, givin g group K'.
$(BDGHEF)$ SLIDE $(CAE)(FHDGB)$ O.K. indirect.
$(BDGHFE)$ $\{BGF\}(DHE).(CHG)(EAF) = (ABGCE)(DHF)$ O.K. indirect.
$(BDHEFG)$ SLIDE $(BAFG)(DCH)$ O.K.
$(BDHEGF)$ SLIDE $(AH)(BCEDF)$ O.K.
$(BDHFGE)$ SLIDE $(DAEH)(FCG)$ O.K.
$(BDHGFE)$ SLIDE $(AD)(HBFCE)$ O.K.
$(BDHGEF)$ SLIDE $(CAE)(DHBFG)$ O.K. indirect.
$(BEDHGF)$ SLIDE $(AED)(CF)$ O.K.

Above analyses are done on the squares of th e six cycles i.e. on the double threes. We must now in ve'tigte the cases of six-cycles where the double threes were exception l

$(BDEHGF)$ SLIDE $(BAG)(FH)(CD)$ O.K.
$(BDGHEF)$ SLIDE $(BAEGH)(CD)$ O.K.

13 22

Below is a line-by-line transcription of the handwritten page titled "Triple Twos," then "Four and twos and fours." Where letters or symbols are partially obscured, bracketed question marks or ellipses appear.

Triple Twos

$(BF)(DA)(GEH)$ X Intransitive Slide $(AF\&D{+}?)(BCF)$ O.K.

$(BF)(DH)(GEA)$ X Intransitive Slide $(AH)(BCG)(Bf)$ O.K.

$(BG)(DA)(EFH)$ X Intransitive $(AH)(BCG)(Bf)$ Slide O.K.

$(BG)(DF)(EAH)$ X Slide $(AH)(BCG)(Bf)$ O.K.

$(BH)(DG)(EAF)$ X Intransitive $(AH)(BCG)(Bf)$ Slide O.K.

$(BH)(DC)(E?F)$ X Slide $(A?H)(BC?)(\ldots?)$ O.K.
(... etc. ...)

Four and twos and fours

We can only need consider those four-and-twos that are intransitive or commute with R^4. Transpositions listed below:

$(EBGD)(F^H)$ (...) $(FBGD)(CE?)$ O.K. $(EBFC)(\ldots?)$ O.K. $((ABFC)(DA))$ O.K. $(EBGA)(H?\ldots)$ O.K. $(EBF\ldots)(CCD)$ O.K. $(ED?GB)(F^H?)$(...)
(... etc. ...)

[One marginal note: "These are none which leave A, C fixed ... except (13)(BH+?), which is Intransitive anyway."]

14 27

Below is a literal transcription of typed text and handwritten edits. No Unicode punctuation; Greek letters and subscripts are rendered in math mode:

Frequency distribution of xxxxxxxxx group elements

We now turn to a rather different topic in connection with the use of identical drums. Even if we know th et all permutations are possible, will they we equally frequent? Fortunately we can answer th is in the affirmative. The problem will be examined under slightly more general conditions. Xxxxxxxxxxxxxxxxxxx No assumptions will be mde about the relationship between th e generetrors $U_1 \ldots M?U_K$, and we will not assume th at the basic group is the symmetric group, but some other group G.

Let us xxxxxxxxxxx suppose th at we feed xxxxxxxxx a certin frequency distribution of g'oup elements into a wheel; how can we c'elulate the frequency distribution of the group elements at th e output of the wheel? Let $g(a)$ be the proportion of the inut elements which re a, and let $F(e)$ be the proportion of group elements effected by the wheel which are e. Then we get output a if the input is b and the wheel effects the group element ab^{-1}. The proportion of such cases is $f(ab^{-1})\,g(b)$, or allowing for the different values of b, a total proportion of $\sum_b f(ab^{-1})\,g(b)$. If then we define the operator R_f by the equation

$$(R_f\,g)(a) \;=\; \sum_b f(ab^{-1})\,g(b),$$

we can say that the frequency distribution for n wheels is given by $R_f^{n-1}\,f$. We wish to determine how this function behaves with increasing n.

15 28

Below is a line-by-line transcription of both typed text and the most legible handwritten annotations:

real

We consider the xxxxxx-valued functions in th e group as forming a xxxxx Euclidean space of h dimensions wh ere h is the order of the g roup H. We may put (g,k) for

$$\frac{1}{h}\sum_a g(a)\,k(a)$$

the scalar product, and $\|g\|$

for the distance from the origin.

We may also put $\overline{g} = \frac{1}{h}\sum_a g(a)$. Schwarz' inequality gives at once $\|g\| \geq \overline{g}$, and if we suppose $g(a) > 0$ on all a, $g(a) > 0$ some a, we shll have $\overline{g} > 0$. We will also suppose $f(a) > 0$ all/b, $f(c) > 0$ some a, $\overline{f} = (?)$. Then we hve

Lemma (a)

If $\overline{f} = 1$ then $\|R_{(g)}f\| \leq \|f\|$, and equality holds only if $g(\ldots)/g(x)$ is independent of x for any g, b for which $f(a) \neq 0$ and $f(b) \neq 0$.

First note th at

$$\left(\frac{1}{h^2}\sum g(x)\,g(c\,x)\right)^2 \leq \ldots$$

[handwritten partial math]

Then

$$\|R_{(g)}f\|^2 = \frac{1}{h^2}\sum_{a,b,x} f(a\,b^{-1})\,g(b)\,f(a\,x^{-1})\,g(x)$$

$$= \frac{1}{h^2} \sum_{c,s,x} f(c)\, f(c\,u)\, g(u\,x)\, g(x) \quad \text{where } u := b\,x^{-1},\ c := a\,b^{-1}$$

$$\leq \sum_{c,s} f(c)\, f(c\,u)\, \|g\|^2$$

$$= [\text{something}]\, \|g\|^2$$

equality holding in the case mentioned. Ths will enable us to …

[Typed lines partially crossed out or faint: "Let us define the 'limiting distribution' f' as the accumulation points of the sequences $g, R_f g, R_f^2 g, f, g, \ldots$"]

Then lemma (a) will enable us to prove …

16 29

Below is a careful transcription of typed text (partly crossed out) and handwritten notes:

Theorem III

The limiting distributions for f are constant throughout the cosets of a certain self-conjugate subgroup H_1 of H. H_1 consists of all expressions xxxxxxxxxxxxxxxxxxxxxxx of the form $U_{m_1}\, U_{m_2}\, \ldots\, U_{m_p}$ where the sum $\sum m_i = 0$. The factor group H/H_1 is cyclic. In the case each [typed text unclear] g is f the limiting distributions have the value θ except in one coset of H_1.

Let k be a limiting distribution. Let it be the limit of the sequence $R_f^r g_s, R_f^r g_j, R_f^r g \ldots$ then [some text about norms] $\|R_f^{n+1} g\| / \|R_f^n g\| > \ldots$ Now $\|R_f^n g\| / \|k\| \to \ldots$ tends to the limit 1 as n tends to infinity, and therefore $\|R_f^{n+1} g\| / \|R_f^n g\|$ tends to 1. But $\|R_f\, u\| / \|u\|$ is a continuous function of u and therefore xxxxxxxxxxxxxxxx limit of the sequence … $\|R_f^k / \|k\| = 1$

Applying lemma (aΦ) to this we see th t there is a function $\phi_\ell(4)$, defined for all expressions of form $a\,b^{-1}$ where $f(a) \neq 0$ $f(b) \neq 0$ such th t $\big(\phi(y\,x) : \phi(y)(k\,x)\big) = \ldots$. By applying the same argument with R_f^n in place of f we find that there is a function $\phi_n(4)$ defined for all expressions of form $a_1\, a_2\, \ldots\, a_k\, b^{-1}\, b_k^{-1} \ldots b_1^{-1}$ where $f(a_1) f(a_2) \ldots f(h_k) \neq 0$, such that $\phi_n(xy) = \phi_n(x)\phi_n(y)$. Whenever $\phi_n(4)$ is defined. The various functions $\phi_n(4)$ must agree wherever their domains overlap, and they may therefore be all represented by one symbol ϕ. In fact we may say that $\phi(x)$ is defined and has the value $\times$ whenever $g(x) := \alpha \ldots$. It now appears that the domain of definition of $\phi(g)$ is a group, for if [handwritten: "$\phi(4, x) = \alpha, \phi(x) = \ldots$" etc.]

17 30

and $k(u_2, x) \geq k(x)$ all x, then $k(u_1, u_2 x?) : \phi(u_1) k(u_2 x?) : \phi(u_1), \phi(u_2), \phi(k(x))$ all x. Thus if y_1 and y_2 belong to the domain of definition of ϕ so does $y_1 y_2$ and $\phi(u_1, y_1, y_2) : \phi(u_1, y_2)(\phi(y_2?))$. It is now immediately seen that the domain of definition is H_1.

The function ϕ is a one dimensional representation of H_1, but it is real and positive and therefore has the value 1 last throughout H_1. This argument may also be expressed without the use of representation theory thus. Since H_1 is finite any element y of it satisfies an equation $y^m = 1$, therefore $((\phi(4))^m \cdot \phi(4^m) = 1$ isn't non sen e non . negativity $\phi(y) > 0$, so $\phi(4) > 1$ But since $g(x)$ is always positive [handwritten: "non-negative"] and so this implies that $g(x)$ is constant throughout each coset of H.

It now only remains to investigate the c$\sim$her$\sim$racter of the group H_1. It is easily seen to be self-invariant or self-conjugate, since if aba^{-1} belongs to H_1, and $b \in H$, the total of exponents of group generators U_r in aba^{-1} must be 0, those in a^{-1} canceling with those in a. Hence aba^{-1} belongs to H_1.

Now let us take a particular generator U_1. Then the cosets $H_1 U_1^m$ exhaust the group H. For if p is an element of H it will be a product of generators; let the total of exponents be m. Then U_1^{-m} has total exponents 0, en d so belongs to H_1. i.e. [a belongs to $H_1 U_1^m$.]

If U_1^s is the lowest power of U_1 which belongs to H_1 then H/H_1 is evidently isomorphic with the cyclic group of order s.

In the c se th t g is f, all the group elements for which $R_f^{(n-1)} xxxxx$ is not zero are products of n generators en d th erefore belong to $H_1 U_1^n$.

18 31

Example

As an example let us consider the quaternion group consisting of $1, i, j, k, i', j', k'$, with the table

	i	j	k	i'	j'	k'	$\ldots$
i'	k'	j'	i	k	j	$\ldots$	
k'	j	i'	$\ldots$				
j'	i	k'	$\ldots$				
$\vdots$							

(and so on, rows/columns for $1, i, j, k, i', j', k'$ ...)

and let U_1 be i and U_2 be j. The various functions $R_f^n f$ are given in the table below

n	i	i'	j	j'	k	k'
1	$\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0
2	0	0	$\frac{1}{4}$	$\frac{1}{2}$	0	$\frac{1}{4}$
3	0	$\frac{1}{4}$	0	$\frac{1}{4}$	0	...
4	...					
5	...					
6	...					

It is seen th t the group H_1 is the group generated by k, it has factor group which is cyclic of order 2.

19 32a

Below is a faithful attempt to capture the clearly legible text. Most typed text from the reverse side is too faint:

[Handwritten in green ink]: On Permutation Groups

[Typed text in background is largely illegible. No further text discernible.]

20 32-Permutation-Groups

Below is a literal transcription of typed text, preserving minor misspellings and strikethroughs:

Case of sym metric and alternating groups

In the case under consider tion at th e beginning of our analy sis, H was unless the upright U was ex ceptl eith er the symmetric or the alternating group. In this case H_1 is xxxxxxx also either the symmetric or th e altern ting group, for it is self conjugate in H. It will b e the xxxxxxx group if the generators are all of th e s me r rity, and the symmetric group otherwise.

We th erefore conclude th t when th e uprigh t is not exception al th e distributions with large numbers of wheels are uniform throughout the alternating group (even perms). If odd permutations are possible with the given upright and number of wheels the distribution is uniform throughout the symmetric group (all perms).