the steps by computer, and thus prove identity (†). In particular, Dixon's identity in the generalization of Fjelsted:

$$\sum_k (-1)^k \binom{n+b}{n+k}\binom{b+c}{b+k}\binom{c+n}{c+k} = \frac{(n+b+c)!}{n!\,b!\,c!}$$

is proved firstly by taking

$$R(n,k) = \frac{(c+1-k)(b+1-k)}{2(n+k)(n+b+c+1)}$$

thus $G(n,k) = R(n,k)F(n,k-1)$, and secondly by verifying equations (5) and (6) — for which laborious exercise it would be advisable to avail oneself of Macsyma say.

In general there are few known identities involving sums of products of several binomial coefficients. A spectacular generalization of Dixon's beautiful identity is given by equation 5.31 on p.171 of [5] which must surely be the *non plus ultra* of the species.

References

[1] A. C. Dixon, *Summation of a certain series*, Proc. London Math. Soc. **35** (1903), 284–289.

[2] J. E. Fjelsted, *A generalization of Dixon's formula*, Math. Scandinavica **2** (1954), 46–48.

[3] I. P. Goulden and D. M. Jackson, Combinatorial enumeration. Wiley, 1983.

[4] R. L. Graham, D. E. Knuth and O. Patashnik, Concrete mathematics. Addison-Wesley, 1989.

[5] E. T. Whittaker, *Alfred Cardew Dixon*, J. London Math. Soc. 12 (1937), 145–154.

[6] H. S. Wilf, Generatingfunctionology. Academic Press, 1990.

James Ward,
University College,
Galway.

SOME GROUPS OF EXPONENT p

J. D. Reid

§1 Introduction.

By the *exponent* of a (finite) group G is meant the least common multiple of the orders of the elements of G. It is a well known elementary exercise that groups of exponent 2 are abelian; and all groups of order p^2, p a prime, are abelian. On the other hand there are examples of non-abelian groups of exponent p ($p > 2$) and order p^3, or p^4, that go back to Burnside, at least (e.g. [1]). Taking a direct product of a non-abelian group of order p^3, for example, with an elementary abelian p-group of order p^n will, of course, give an example of a non-abelian group of exponent p and of arbitrarily large finite cardinality. However as an example of a non-abelian group of exponent p such a group offers little more than its non-abelian direct factor.

Our interest in examples of such groups was stimulated by questions of W. W. Comfort. We present here a simple construction of an infinite class of non-trivial (i.e. non-abelian and indecomposable) groups of exponent p, $p > 2$.

Observe that to say that a group G is abelian is to say that it is equal to its centre, $z(G)$, so that the larger the centre of G the more abelian, in a sense, is G. Similarly G is abelian if and only if its derived group G' is trivial so that the smaller the derived group, the more abelian is G. It may happen that $z(G)$ is contained in G' in which case G has no hope of being abelian: the larger the centre in G the larger the derived group, the smaller the derived group the smaller the centre. Hopes for commutativity are frustrated just in proportion to their strength. For the purposes of this discussion we encapsulate this idea in the

Definition 1.1 A group G is *inherently non-abelian* if its centre is contained in its derived group.

Note that if G is a direct product of its subgroups K and M then G is inherently non-abelian if and only if both K and M are inherently non-abelian, so that the indecomposable ones are the ones of interest. We observe also that the group consisting of the identity element alone is the only abelian inherently non-abelian group.

Our object is to prove the following

Theorem 1.2. *For each odd prime p and every integer $s > 0$ there exists an indecomposable inherently non-abelian group G of exponent p and order $p^{s(p-1)+1}$.*

There are several ways to go about this. We have chosen what seems to us a fairly natural and conceptual one. For another more elementary but perhaps slightly ad hoc approach, see the remarks at the end of the paper.

§2 Finite Fields.

We recall some facts about finite fields. Let L be a field of cardinality p^s and let F be the extension of L of degree p. Then F is a Galois extension of L with cyclic Galois group which we denote by Γ. Let σ be a generator of Γ.

We will frequently think of elements of Γ as being simply linear transformations in F as vector space over L, so that we may add them together as well as multiply them. For example, in the polynomial ring $L[t]$, t an indeterminate, we have

$$(1-t)(1+t+\cdots+t^{p-1}) = 1-t^p = (1-t)^p = (1-t)(1-t)^{p-1}$$

so that $1+t+\cdots+t^{p-1} = (1-t)^{p-1}$. Hence for the automorphism σ, $1+\sigma+\cdots+\sigma^{p-1} = (1-\sigma)^{p-1}$ and therefore the *trace* map of F over L is given by $(1-\sigma)^{p-1}$. Since the trace map has image L, we have

$$L = (1-\sigma)^{p-1}F.$$

We write H for the set of elements of trace 0. This is an L subspace of F of codimension 1 and is mapped onto itself by

the automorphisms in Γ. Our formula for the trace map shows that $(1-\sigma)F \subseteq H$ since $(1-\sigma)^p = 1-\sigma^p = 0$. On the other hand the trace map itself is not zero so $(1-\sigma)^k$ is non-zero for all k, $0 \le k \le p-1$. It follows that $(1-\sigma)^{k+1}F$ is contained properly in $(1-\sigma)^k F$ for all k, $0 \le k \le p-1$. Since there are p such subspaces of F and F has dimension p over L, it follows that $(1-\sigma)^{k+1}F$ has codimension 1 in $(1-\sigma)^k F$. In particular $(1-\sigma)F$ has codimension 1 in F and the inclusions $(1-\sigma)F \subseteq H \subset F$ yield

$$H = (1-\sigma)F. \tag{1}$$

This is a special case of a general fact about cyclic extensions. See for example [2].

§3 Basic Properties.

We define G to be the semi-direct product of the additive group H and the multiplicative group Γ, noting that elements of Γ induce automorphisms on H. Thus G is the cartesian product of H and Γ with multiplication defined by

$$(x,\rho)(y,\tau) = (x+\rho(y),\rho\tau), x,y \in H; \rho,\tau \in \Gamma.$$

The identity element of G is $(0,1)$ and inverses are given by $(x,\rho)^{-1} = (-\rho^{-1}(x),\rho^{-1})$. We have

$$(x,\rho)(y,\tau)(x,\rho)^{-1} = ((1-\tau)x+\rho(y),\tau) \tag{2}$$

and

$$(x,\rho)(y,\tau)(x,\rho)^{-1}(y,\tau)^{-1} = ((1-\tau)x-(1-\rho)y,1) \tag{3}$$

for $x,y \in H$ and $\rho,\tau \in \Gamma$.

Observe that $\{(x,1) : x \in H\}$ is a normal subgroup of G, that contains G' by (3) above, and is isomorphic to H under the map $x \mapsto (x,1)$. We will frequently identify H and its subgroups with this subgroup of G and its subgroups. For example L will be identified with the subgroup $\{(x,1) : x \in L\}$ of G. Similarly, $\{(0,\rho) : \rho \in \Gamma\}$ is a subgroup of G isomorphic to

Γ and will occasionally be denoted by Γ as well. This should cause no confusion, but can be useful. For example the subgroup $\{(x,\rho) : x \in L, \rho \in \Gamma\}$ of G is isomorphic to the direct product of L and Γ, since Γ acts trivially on L, and by our conventions we would denote it by $L \times \Gamma$, or $L\Gamma$.

A straightforward induction yields a power formula: for $x \in H, \rho \in \Gamma$,

$$(x,\rho)^m = (\sum_{j=0}^{m-1} \rho^j(x), \rho^m).$$

Since Γ has exponent p and H consists of elements of trace 0 this formula shows that $(x,\rho)^p = (0,1)$ if $\rho \neq 1$, while $(x,1)^p = (px,1) = (0,1)$ since we are in characteristic p. Hence

Corollary 3.1. *G has exponent p.*

In the proposition below we use the convention of identifying subgroups of H with certain subgroups of G. Thus by $(1-\sigma)H$ here we mean $\{((1-\sigma)x,1) : x \in H\}$.

Proposition 3.2. *The derived group, G', of G equals $(1-\sigma)H$.*

Proof: For any $\rho, \tau \in \Gamma$ and $x \in H$, we have

$$((1-\tau)x,1) = (x,\rho)(0,\tau)(x,\rho)^{-1}(0,\tau)^{-1} \qquad (4)$$

and by (3)

$$\begin{aligned}(x,\rho)(y,\tau)(x,\rho)^{-1}(y,\tau)^{-1} &= ((1-\tau)x - (1-\rho)y, 1)\\ &= ((1-\tau)x,1)((1-\rho)y,1)^{-1}\end{aligned}$$

so that the elements $((1-\tau)x,1), x \in H, \tau \in \Gamma$, generate G'. Any $\tau \in \Gamma$ has the form σ^k for suitable k, $0 \leq k < p$, so

$$1-\tau = 1-\sigma^k = (1-\sigma)(1+\sigma+\cdots+\sigma^{k-1}).$$

It follows that $((1-\tau)x,1) \in \{((1-\sigma)w,1) : w \in H\} = (1-\sigma)H$ so that $G' \subseteq (1-\sigma)H$.

On the other hand, it is clear from (4) that $(1-\sigma)H \subseteq G'$.

Corollary 3.3. *G' is abelian.*

The following simple fact is obvious but we state it explicitly for emphasis since its corollary lies at the heart of the non-commutativity of G.

Proposition 3.4. *The set H of elements of trace 0 in the extension F of L has cardinality $p^{s(p-1)}$.*

Proof: F has cardinality p^{ps} and the image, L, of the trace map has cardinality p^s. Hence the kernel, H, of the trace map has cardinality $\frac{p^{ps}}{p^s} = p^{s(p-1)}$.

Corollary 3.5. *H and L are equal if and only if $p = 2$.*

§4 Main Results.

We now restrict p to be an odd prime. By the Corollary above, L is then a proper subset of H and since F has degree p over L, we see that H contains a generator of F out of L. As a consequence, the only automorphism of F over L that leaves H elementwise fixed is the identity map. This fact plays a large role in what follows. For example

Proposition 4.1. *The centre, $z(G)$, of G is $\{(x,1) : x \in L\}$.*

Proof: From (2), $(x,\rho) \in z(G)$ if and only if $((1-\tau)x + \rho(y), \tau) = (y,\tau)$ for all $y \in H$, $\tau \in \Gamma$. Taking $\tau = 1$, we obtain $\rho(y) = y$ for all y in H. Hence $\rho = 1$. Now taking $y = 0$ and τ arbitrary in Γ we have $x = \tau(x)$ for all τ so $x \in L$ as required. Conversely it is clear from (2) that $(x,1) \in z(G)$ for all $x \in L$.

Theorem 4.2. *The group G is inherently non-abelian, i.e. $z(G) \subsetneq G'$.*

Proof: We have determined both the centre and the derived group. Each is a subgroup of H, identified with its canonical image in G. We have already observed that $(1-\sigma)^{p-1}F = L$. Hence we have

$$z(G) = L = (1-\sigma)^{p-1}F \subsetneq (1-\sigma)^2 F = (1-\sigma)H = G'$$

by Proposition 4.1, Proposition 3.2 and (1). Note that this inclusion uses again the fact that $p \geq 3$, i.e. $p - 1 \geq 2$.

Another qualitative indication of the lack of commutativity of G is the fact that the centralizer of each element is as small as can be—i.e. elements of G commute only with the obvious, such as their own powers, elements of the centre, etc. It is not hard to identify these centralizers (as we did in our original proof) but we only need the following to complete our discussion. We are indebted to the referee for the elegant treatment of case (iii).

Proposition 4.3. *If $g \notin z(G)$ then the centralizer of g in G is abelian.*

Proof: The non-central elements of G have the form $g = (x, \rho)$, with $x \notin L$ or $\rho \neq 1$. We consider three cases.

(i) $x \notin L$, $\rho = 1$. Here g is in H which is a commutative maximal subgroup of the non-commutative group G, so $C_G(g) = H$ in this case.

(ii) $x = 0$, $\rho \neq 1$. By (2), $(y, \tau) \in C_G(g)$ if and only if

$$(y, \tau) = (0, \rho)(y, \tau)(0, \rho)^{-1} = (\rho(y), \tau).$$

Thus $C_G(g) = \{(y, \tau) : \rho(y) = y\} = \{(y, \tau) : y \in L\}$ since $\rho \neq 1$ and Γ has ρ as generator. Here then $C_G(g)$ is the direct product of L and Γ.

(iii) It remains to deal with the case $x \neq 0, \rho \neq 1$. The map $\alpha : G \longrightarrow G$ defined by

$$(y, \rho^k)^\alpha = (y + \sum_{j=0}^{k-1} \rho^j(x), \rho^k), (y \in H, k \geq 0)$$

preserves the multiplication in G, hence is an automorphism. Putting $h = (0, \rho)$, we have $C_G(g) = C_G(h^\alpha) = C_G(h)^\alpha$, which is abelian by (ii).

To complete the discussion, we have

Theorem 4.4. *G is indecomposable.*

Proof: Suppose that $G = K \times M$, direct product. Then M is contained in the centralizer of each element of K, and K is contained in the centralizer of each element of M. If K is not contained in $z(G)$, then M is commutative by Proposition 4.3. Similarly for M. Hence we may assume that K, say, is contained in the centre of G.

Now $z(G) = z(K) \times z(M) = K \times z(M)$ since K is commutative. We also have $G' = K' \times M' = M'$ since K is commutative. But this gives $K \subseteq z(G) \subseteq G' = M' \subseteq M$, and since $K \cap M$ is trivial, K is trivial.

Our main result has now been established. The group G is an indecomposable, inherently non-abelian group of exponent p and has order $p^{s(p-1)+1}$.

§5 Remarks. As another approach to this subject one could view a p-dimensional vector space V over the field L of cardinality p^s as an $L[t]$ module via the linear transformation given, in some basis, by the matrix

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 \\ . & . & . & . & \cdots & . \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

Then V would play the role of F in our previous discussion, the kernel of ΣA^j that of H, and in place of σ one would use A.

The groups constructed above have many special properties, perhaps even enough that they admit an easy characterization. We do not pursue that question here though it might be of interest to point out that the subgroup H which plays such a prominent role has a group-theoretic characterization, at least for $p > 3$. For such p, $H = C_G(G')$.

References

[1] W. Burnside, Introduction to Finite Groups (2nd Edition). Dover: New York, 1955.

[2] Nathan Jacobson, Basic Algebra I. Freeman: New York, 1985.

J. D. Reid,
Department of Mathematics,
Wesleyan University,
Middletown,
Connecticut 06459,
USA.

Book Review

Mathematics and its History

(Undergraduate Texts in Mathematics)

J. Stilwell
Springer-Verlag, 1989,
ISBN 3 540 96981 0.

Reviewed by James Ward

John Stilwell, in addition to his original contributions in mathematics, is the translator of Serre's *Trees* (Springer-Verlag), and the author of *Classical Topology and Combinatorial Group Theory*. His experience as a writer on mathematics shows to good advantage in the volume under review.

Proceeding from the observation (probably all too true in many universities) that students are taught Algebra, Calculus, Group Theory, Topology, Measure Theory etc, and are taught little of the connexions between these areas, the author's aim is to combine the ingredients of Mathematics, using History as a leavening agent; the result is very appetizing indeed!

This perspective differs from that of well known books on the subject, such as the works of Boyer and Struik — to name but two — who are more concerned with tracing the evolution of mathematical ideas; also they aspire to produce a complete account of the history of the subject (Struik being telegraphic in style but, given its length, remarkably complete; Boyer is very comprehensive).

In Stilwell's book, the presentation of material in each chapter is followed by a section of Biographical Notes, which in most cases includes illustrations of the mathematicians mentioned in the chapter. This is very useful for a lecturer seeking last-minute