[21] H.E. Rose, *A course in number theory*, Oxford U.P., 1988.

[22] Kenneth H. Rosen, *Elementary Number Theory and its Applications*, Addison-Wesley, 1988.

[23] J. Seberry and J. Pieprzyk, *Cryptography: an introduction to computer security*, Prentice Hall, 1989.

[24] G.J. Simmons, *Cryptology: The Mathematics of secure communications*, Math. Intelligencer **1** (1979), 233-246.

[25] R. Solovay and V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comp. **6** (1977), 84-85.

[26] H.C. Williams, *Factoring on a Computer*, Math. Intelligencer **6** (1984), 29-36.

[27] Dominic Welsh, *Codes and Cryptography*, Oxford U.P., 1988.

Department of Pure Mathematics,
The Queen's University of Belfast.

An Elementary proof that periodicity and generalized-periodicity are equivalent in nilpotent groups

Gary J. Sherman

Let S be a non-empty subset of the group G. An element x of G is said to be S-periodic if there are elements $g_1, \ldots, g_n$ in S for which

$$\prod_{i=1}^{n} g_i^{-1} x g = e.$$

If $S = \{e\}$, then S-periodicity is the usual notion of group periodicity. If $S = G$, then S-periodicity is referred to as generalized-periodicity, a concept which occurs naturally in the theory of partially ordered groups. Indeed, a group admits a partial ordering relation compatible with the group operation if, and only if, the group contains an element which is not generalized-periodic [1]. Another case of special interest is when $S = P(G)$, the set of periodic elements of G. It was shown in [5] that $P(G)$ is a subgroup of G if, and only if, each $P(G)$-periodic element of G is periodic.

If G is abelian, then generalized-periodicity and $P(G)$-periodicity are equivalent to periodicity. Thus, when presented the class of nilpotent groups as a natural generalization of the class of abelian groups one asks: "Is generalized-periodicity equivalent to periodicity in the class of nilpotent groups?" Hollister [3] has shown that the answer to this question is yes. His proof makes use of a deep result from the theory of partially ordered groups and the fact that the periodic elements of a nilpotent group form a subgroup [4]. In this paper we give an elementary proof of Hollister's result and obtain, as a corollary, the fact that $P(G)$ is a subgroup for nilpotent G.

To this end the following two observations are useful. Let x and y be elements of the group G.

Fact 1. If x and y are periodic then xy is generalized-periodic.

Proof. Let x and y be of orders m and n, respectively. Then

$$\prod_{i=0}^{mn-1} x^{-i} xyx^{i} = xy^{mn}x^{mn-1} = e.$$

Notice that if generalized-periodicity is equivalent to periodicity, then $P(G)$ is closed with respect to taking products and inverses; i.e., $P(G)$ is a subgroup.

Fact 2. If a non-trivial power of x commutes with y, then the commutator $[x,y]=x^{-1}y^{-1}xy$ is a generalized-periodic element of the subgroup generated by x and $[x,y]$.

Proof. Let $x^n y = yx^n$ for some positive integer n. Then

$$\begin{aligned}\prod_{i=1}^{n} x^{-n+i}[x,y]x^{n-i} &= x^{-n}(y^{-1}xy)^n \\ &= x^{-n}y^{-1}x^n y \\ &= e.\end{aligned}$$

Notice that $[x,y]$ is conjugated by powers of x.

Theorem. *Generalized-periodicity is equivalent to periodicity in a nilpotent group.*

Proof. Recall that a group, G, is nilpotent of class n if it possesses a series of normal subgroups, $G=G_0\supset G_1\supset\ldots\supset G_n=\{e\}$, in which G_i/G_{i+1} is the center of G/G_{i+1}. Such a series is referred to as the upper central series of G. We proceed by induction on the class of the nilpotent group G.

If G is of class one, then G is abelian and the result is obvious.

Now suppose that G is nilpotent of class n and that generalized-periodicity is equivalent to periodicity in nilpotent groups of class less than n. Let x be a generalized-periodic element of $G-G_{n-1}$ (Each generalized-periodic element of G_{n-1} is periodic since G_{n-1} is the center of G.). For some positive integer k there are $y_1,\ldots,y_k$ in G for which

$$\prod_{i=1}^{k} y_i^{-1}xy_i = e. \tag{i}$$

Applying the identity $y_i^{-1}xy_i = x[x,y_i]$ to (i) we obtain

$$\prod_{i=1}^{k} x[x,y_i] = e. \tag{ii}$$

It also follows from (i) that

$$\prod_{i=1}^{k}(y_i^{-1}G_{n-1})(xG_{n-1})(y_iG_{n-1}) = G_{n-1}$$

in the factor group G/G_{n-1}. Since G/G_{n-1} is a nilpotent group of class less than n the induction hypothesis implies that xG_{n-1} is periodic in G/G_{n-1}. Thus there exists a positive integer m for which $x^m\in G_{n-1}$, the center of G. Fact 2 implies that each of $[x,y_1],\ldots,[x,y_k]$ is generalized-periodic so for $i=1,\ldots,k$ there is a positive integer s_i and there are $z_{i_1},\ldots,z_{i_{s_i}}$ in G such that

$$\prod_{j=1}^{s_i} z_{i_j}[x,y_i]z_{i_j} = e; \tag{iii}$$

$$\text{i.e.,}\quad \prod_{j=1}^{s_i}[x,y_i][[x,y_i],z_{i_j}] = e. \tag{iv}$$

Reasoning with (iii) as with (i), we find $[[x,y_i],z_{i_j}]$ to be generalized-periodic in the subgroup generated by $[x,y_i]$ and $[[x,y_i],z_{i_j}]$. But $[x,y_i]\in G_1$ and $[[x,y_i],z_{i_j}]\in G_2$ so $[[x,y_i],z_{i_j}]$ is generalized-periodic as an element of G_1. By the induction hypothesis and Fact 1, $[[x,y_i],z_{i_j}]\in P(G_2)=P(G)\cap G_2$ which is a normal subgroup of G . From (iv) we have $[x,y_i]^{s_i}P(G_2)=P(G_2)$ in the factor group $G_1/P(G_2)$. Thus, since $[x,y_i]^{s_i}$ is periodic, $[x,y_i]$ must be periodic; i.e., $[x,y_i]\in P(G_1)=P(G)\cap G_1$, which i s a normal subgroup of G. From (ii) it follows that $x^kP(G_1)=P(G_1)$ in the factor group $G/P(G_1)$. We conclude that x is periodic since x^k is periodic.

Corollary. The periodic elements of a nilpotent group form a subgroup.

References

[1] Fuchs, L., *Partially Ordered Algebraic Systems*, Pergamon Press, London, 1963.

[2] Hall, M., *The Theory of Groups*, The Macmillan Company, New York, 1959.

[3] Hollister, H.A., On a condition of Onishi, Proc. Amer. Math. Soc., 19 (1968), 1337-1340.

[4] Kurosh, A.G., *The Theory of Groups*, Second English Edition, Chelsea Publishing Company, New York, 1960.

[5] Sherman G.J., When do the periodic elements of a group form a subgroup?, Math. Mag., 47 (1974), 279-281.

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute
Indiana 47803
USA

Note on the Diophantine Equation

$$x^x y^y = z^z$$

James J. Ward.

In a letter to the Editor of the Irish Times, Dr. Des McHale issued the challenge of finding any solution (x, y, z), with none of x, y, $z = 1$, of the Diophantine equation

$$x^x y^y = z^z.$$

This had appeared as a problem in the first Irish Universities Mathematical Olympiad and apparently none of the contestants found a non–trivial solution. The purpose of this note is to indicate a method for generating solutions to this equation.

Lemma: Suppose X, Y, Z, φ are natural numbers such that

(i) $X + Y - Z = 1$ and

(ii) $\varphi \geq 2$ and

(iii) $\varphi = Z^Z/(X^X Y^Y)$;

then $x = \varphi X, y = \varphi Y, = \varphi Z$ have the property that

$$x^x y^y = z^z.$$

Proof: Consider $x^x y^y$: this equals

$$(\varphi X)^{\varphi X}(\varphi Y)^{\varphi Y} = \varphi^{\varphi(X+Y)}(X^X Y^Y)^{\varphi}.$$

On the other hand z^z equals

$$\varphi^{\varphi Z}(Z^Z)^{\varphi}$$