On the Proof of a Theorem of Pálfy

Edward Dobson

Department of Mathematics and Statistics
Mississippi State University
PO Drawer MA
Mississippi State, MS 39762 USA

dobson@math.msstate.edu

Submitted: Mar 24, 2006; Accepted: Oct 10, 2006; Published: Oct 19, 2006
Mathematics Subject Classification: 05E99

Abstract

Pálfy proved that a group G is a CI-group if and only if $|G| = n$ where either $\gcd(n, \varphi(n)) = 1$ or $n = 4$, where φ is Euler's phi function. We simplify the proof of "if $\gcd(n, \varphi(n)) = 1$ and G is a group of order n, then G is a CI-group".

In 1987, Pálfy [6] proved perhaps the most well-known result pertaining to the Cayley isomorphism problem. Namely, that a group G of order n is a CI-group if and only if either $\gcd(n, \varphi(n)) = 1$ or $n = 4$, where φ is Euler's phi function. It is worth noting that every group of order n is cyclic if and only if $\gcd(n, \varphi(n)) = 1$. It is the purpose of this note to simplify some parts of Pálfy's original proof.

Definition 1 Let G be a group and define $g_L : G \to G$ by $g_L(x) = gx$. Let $G_L = \{g_L : g \in G\}$. Then G_L is the *left-regular representation of* G. (It is a subgroup of the symmetric group S_G of all permutations on G.) We define a *Cayley object of* G to be a combinatorial object X (e.g. digraph, graph, design, code) such that $G_L \leq \mathrm{Aut}(X)$, where $\mathrm{Aut}(X)$ is the *automorphism group of* X (note that this implies that the vertex set of X is in fact G). To say that G is a *CI-group* means that if X and Y are any Cayley objects of G such that X is isomorphic to Y, then some group automorphism of G is an isomorphism from X to Y.

CI-groups are characterized by the following result due to Babai [1].

Lemma 1 *For a group G, the following are equivalent:*

1. *G is a CI-group,*
2. *for every $\gamma \in S_G$, there exists $\delta \in \langle G_L, \gamma^{-1}G_L\gamma\rangle$ such that $\delta^{-1}\gamma^{-1}G_L\gamma\delta = G_L$.*

We will not simplify all of Pálfy's proof, so it will be worthwhile to discuss exactly which part of his proof we will simplify. First, we will not deal with groups G such that $|G| = 4$ at all. Second, we will only be concerned with showing that if $\gcd(n, \varphi(n)) = 1$, then $\mathbb{Z}_n$ is a CI-group. Third, Pálfy's original proof can be broken into two cases, with the first dealing with the case where $\langle(\mathbb{Z}_n)_L, \gamma^{-1}(\mathbb{Z}_n)_L\gamma\rangle$ is doubly-transitive and the second dealing with the case where $\langle(\mathbb{Z}_n)_L, \gamma^{-1}(\mathbb{Z}_n)_L\gamma\rangle$ is imprimitive (note that as $\mathbb{Z}_n$ is a Burnside group [3, Theorem 3.5A] for n composite, these are the only nontrivial cases). The doubly-transitive case was reduced by Pálfy to the imprimitive case using the fact that all doubly-transitive groups are known [2], which is a consequence of the Classification of the Finite Simple Groups. We shall do the same, using Pálfy's argument. Pálfy handled the imprimitive case by using a sequence of lemmas (Lemmas 1.1-1.4 in [6]) which, while not overly difficult, do involve some tedious calculations and do not seem to make transparent why the condition $\gcd(n, \varphi(n)) = 1$ is crucial. We shall show that Lemma's 1.2-1.4 of [6] can more or less be replaced by an application of Philip Hall's generalization of the Sylow Theorems for solvable groups.

Let π be a set of primes. A π-*group* is a group G such that every prime divisor of $|G|$ is contained in π. A Hall π-subgroup H of G is a subgroup of G such that H is a π-group, and no prime contained in π divides $|G|/|H|$. Hall π-subgroups need not exist, but we remind the reader that Hall's Theorem [4, Theorem 6.4.1] states that they do exist if G is solvable, and in that case any two Hall π-subgroups of G are conjugate in G.

Definition 2 Let G be a transitive permutation group of degree mk that admits a complete block system $\mathcal{B}$ of m blocks of size k. If $g \in G$, then g permutes the m blocks of $\mathcal{B}$ and hence induces a permutation in the symmetric group S_m, which we denote by $g/\mathcal{B}$. We define $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$. Let $\mathrm{fix}_G(\mathcal{B}) = \{g \in G : g(B) = B \text{ for every } B \in \mathcal{B}\}$, and for $B \in \mathcal{B}$, let $\mathrm{Stab}_G(B) = \{g \in G : g(B) = B\}$.

We shall use Pálfy's notation, repeated here for convenience. Let x be the n-cycle $(0\ 1\ \ldots\ n-1)$ (so that $\langle x\rangle = (\mathbb{Z}_n)_L$) and y any conjugate of x in S_n such that $\langle x, y\rangle$ admits a complete block system of m blocks of size k. Let $x^m = z_0 z_1 \cdots z_{m-1}$ where each z_i is a k-cycle that permutes i. Finally, let $P = \langle z_i : i \in \mathbb{Z}_m\rangle$. The following result combines Lemmas 1.2, 1.3, and 1.4 of [6].

Lemma 2 *If $\langle x, y\rangle$ admits a complete block system $\mathcal{B}$ with m blocks of size k such that $y^m \in P$, $\mathbb{Z}_m$ is a CI-group, and* $\gcd(m, k\cdot\varphi(k)) = 1$, *then $\langle y\rangle$ is conjugate to $\langle x\rangle$ in $\langle x, y\rangle$.*

Proof. As $\langle x\rangle$ and $\langle y\rangle$ are abelian, and a transitive abelian subgroup is regular [3, Theorem 4.2A (v)], we have that $\mathrm{fix}_{\langle x\rangle}(\mathcal{B})$ and $\mathrm{fix}_{\langle y\rangle}(\mathcal{B})$ have order k and $\langle x\rangle/\mathcal{B}$, $\langle y\rangle/\mathcal{B}$ are cyclic of order m. As $\mathbb{Z}_m$ is a CI-group, by Lemma 1, there exists $\delta_1 \in \langle x, y\rangle/\mathcal{B}$ such that $\delta_1^{-1}\langle y\rangle\delta_1/\mathcal{B} = \langle x\rangle/\mathcal{B}$. We thus assume without loss of generality that $\langle y\rangle/\mathcal{B} = \langle x\rangle/\mathcal{B}$.

For $i \in \mathbb{Z}_m$, we have that $x^{-1}z_i x = z_{\sigma(i)}$ for some $\sigma \in S_m$ and, as $y^m \in P$ and $\langle y\rangle$ is abelian, we also have that $y^{-1}z_i y = z_{\delta(i)}^{a_i}$ for some $\delta \in S_m$ and $a_i \in \mathbb{Z}_k^*$. We conclude that both x and y normalize P, so that x and y normalize $P' = P \cap \langle x, y\rangle$. Thus $P' \triangleleft \langle x, y\rangle$. Hence $P' \triangleleft \mathrm{Stab}_{\langle x,y\rangle}(B)$, $B \in \mathcal{B}$, so that $\mathrm{Stab}_{\langle x,y\rangle}(\mathcal{B})|_B$ is a transitive group of degree k and contains a normal regular abelian subgroup of degree k. By [3, Corollary 4.2B], we have that $\mathrm{Stab}_{\langle x,y\rangle}(B)|_B$ is isomorphic to the semidirect product $\mathrm{Aut}(\mathbb{Z}_k) \ltimes \mathbb{Z}_k = N(k)$. It is well known that $\mathrm{Aut}(\mathbb{Z}_k)$ is solvable of order $\varphi(k)$, so that $N(k)$ is solvable of order $\varphi(k)\cdot k$. By the Embedding Theorem [5, Theorem 2.6], $\langle x,y\rangle$ is permutation group isomorphic to a subgroup of the wreath product $(\langle x,y\rangle/\mathcal{B}) \wr N(k)$ so that $\langle x,y\rangle$ is permutation group isomorphic to a subgroup of $\mathbb{Z}_m \wr N(k)$. Hence $\langle x,y\rangle$ is solvable. Let π be the set of primes dividing m. As $|\mathbb{Z}_m \wr N(k)| = m\cdot[\varphi(k)\cdot k]^m$ and $\gcd(m,\varphi(k)) = 1$, we have that $\gcd(m,[\varphi(k)\cdot k]^m) = 1$. Thus $\langle x^k\rangle$ and $\langle y^k\rangle$ are Hall π-subgroups of $\langle x,y\rangle$ and by Hall's Theorem are conjugate in $\langle x,y\rangle$. We may thus assume without loss of generality that $\langle x^k\rangle = \langle y^k\rangle$.

As P' is abelian, y^m commutes with x^m. As $\langle y^k\rangle = \langle x^k\rangle$ and y^m commutes with y^k, we have that y^m also commutes with x^k. As $\langle x^m, x^k\rangle = \langle x\rangle$ is a transitive abelian group, and a transitive abelian group is self-centralizing [3, Theorem 4.2A (v)], we have that $y^m \in \langle x\rangle$. As $\langle y^k\rangle \leq \langle x\rangle$, we have that $\langle y\rangle \leq \langle x\rangle$ so that $\langle y\rangle = \langle x\rangle$. □

For completeness, we include the following proof. Note that it is essentially Pálfy's original proof, with Lemma 2 replacing Lemmas 1.2, 1.3, and 1.4 of [6].

Theorem 3 (Pálfy) *If n is a positive integer and $\gcd(n,\varphi(n)) = 1$, then $\mathbb{Z}_n$ is a CI-group.*

PROOF. Let $n = p_1\cdots p_r$ be the prime factorization of n. (Note that $p_1,\ldots,p_r$ are distinct, because n is relatively prime to $\varphi(n)$.) We proceed by induction on r.

If $r = 1$, then any two regular cyclic subgroups of S_n are Sylow n-subgroups of S_n, and thus are conjugate. The result then follows by Lemma 1.

Assume that the result holds for all n with $\gcd(n,\varphi(n)) = 1$ such that n has $r-1$ distinct prime factors. Let n have $r \geq 2$ distinct prime factors, and x be as above. Let $y \in S_n$ be any n-cycle (so that $\langle y\rangle$ is conjugate to $\langle x\rangle$ in S_n). As $\mathbb{Z}_n$ is a Burnside group, by [3, Theorem 3.5A], we have that $\langle x,y\rangle$ is either doubly-transitive or imprimitive.

If $\langle x,y\rangle$ is imprimitive, admitting a complete block system $\mathcal{B}$ of m blocks of size k, then by [6, Lemma 1.1], there exists $y' \in S_n$ such that y' is conjugate of y in $\langle x,y\rangle$ and $(y')^m \in P$. By Lemma 2, we then have that $\langle y'\rangle$ is conjugate to $\langle x\rangle$ in $\langle x,y'\rangle$, so that $\langle x\rangle$ is conjugate to $\langle y\rangle$ in $\langle x,y\rangle$. By Lemma 1, $\mathbb{Z}_n$ is a CI-group and the result follows by induction.

If $\langle x,y\rangle = S_n$, then clearly $\langle y\rangle$ is conjugate to $\langle x\rangle$ in $\langle x,y\rangle$. If $\langle x,y\rangle = A_n$, then by [6, Lemma 3.1] we have that $\langle y\rangle$ and $\langle x\rangle$ are conjugate in A_n. Thus if $\langle x,y\rangle = A_n$ or S_n, then the result follows by Lemma 1. Otherwise, by [6, Lemma 2.1], there exists a prime divisor p of n such that the Sylow p-subgroups of $\langle x,y\rangle$ have order p. Then $\langle x^{n/p}\rangle$ and $\langle y^{n/p}\rangle$ are Sylow p-subgroups of $\langle x,y\rangle$ and are thus conjugate. Hence there exists $y' \in S_n$ such that $\langle y'\rangle$ is conjugate to $\langle y\rangle$ in $\langle x,y\rangle$ and $(y')^{n/p} = x^{n/p}$. Then $\langle x^{n/p}\rangle \lhd \langle x,y'\rangle$, and so $\langle x,y'\rangle$ admits a complete block system $\mathcal{B}$ consisting of n/p blocks of size p, reducing this case to the imprimitive case above. The result then follows by induction. □

Acknowledgement: The author would like to thank Dave Witte Morris of the University of Lethbridge for several useful discussions concerning this note. The author is also indebted to Dave Witte Morris and Joy Morris for their hospitality at the University of Lethbridge where this work was done.

References

[1] L. Babai, Isomorphism problem for a class of point-symmetric structures, *Acta Math. Sci. Acad. Hung.* **29** (1977), 329-336.

[2] P. J. Cameron, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981) 1–22.

[3] J. D. Dixon, and B. Mortimer, *Permutation Groups*, Springer-Verlag New York, Berlin, Heidelberg, Graduate Texts in Mathematics, **163**, 1996.

[4] D. Gorenstein, *Finite Groups*, Chelsea Publishing Co., New York, 1968.

[5] J. D. P. Meldrum, *Wreath Products of Groups and Semigroups*, Pitman Monographs and Surveys in Pure and Applied Mathematics, **74**, Longman, Harlow, 1995.

[6] P. P. Pálfy, Isomorphism problem for relational structures with a cyclic automorphism, *Europ. J. Comb.* **8** (1987), 35-43.