Equally Partitioned Groups

David Dynerman
Dept. of Mathematics - University of Wisconsin

Febraury 15^{th}, 2010

1 Introduction

These are notes for a presentation on I. M. Isaacs' classification of finite equally partitioned groups. They closely follow the presentation in [1].

Definition 1. Let G be a group, and let Π be a collection of proper subgroups of G. Π is said to *partition* G if every non-identity element of G is contained in exactly one $H \in \Pi$.

Definition 2. Let G be a finite group. The exponent of G is the least common multiple of the orders of elements of G. In particular, if G has exponent e, then $g^e = 1$ for all g in G.

Example 1. Let G be a p-group of exponent p. We claim that the set of cyclic subgroups of G forms a partition Π of G. First, note that each element of Π is a subgroup of order p, since if G had a cyclic subgroup of order $p^a > p$ then the exponent of G wouldn't be p. It follows that every element H_i of Π is generated by some $g_i \in G$ of order p. Moreover, any two distinct subgroups of Π intersect trivially by Lagrange's theorem.

It remains to see that every element of G lies in precisely one element of Π - but this is easy to see, since if $g \in G$ then $\langle g \rangle \in \Pi$.

Note that each member of the partition Π has the same size. When this condition holds on a partition Π we say that G is equally partitioned by Π. A surprising result proved by I. M. Isaacs is that the the example above is essentially the only example of an equally partitioned finite group.

Theorem 1 (Isaacs)**.** *Let G be an equally partitioned finite group. Then G is a p-group with exponent p.*

As a motivating example, we work out one more group partition. This specific type of partition will be used in our later argument.

Example 2. Suppose that W is a group of order qr for primes q and r, not necessarily distinct. Additionally, assume that each element of W has prime order.

First, if $|W| = q^2$, then W is an elementary abelian q-group, and is partitioned by its $q+1$ cyclic subgroups of order q, and so $|\Pi| = q+1$.

On the other hand, if $|W| = qr$, assume that $r > q$. Then, by index considerations, the number of Sylow r-subgroups of W must be 1 or q. However, since $q < r$ we know that $q \not\equiv 1 \bmod r$ and so $n_r(W) = 1$.

Again by index considerations, the number of Sylow q-subgroups of W is 1 or r. We claim that $n_q(W) = r$, since otherwise, if W had a normal Sylow q-subgroup Q, then W/Q would be cyclic and we'd have $W' \subseteq Q$. However, if R is the Sylow r-subgroup of W then W/R is cyclic and so also $W' \subseteq R$. This implies that $W' \subseteq Q \cap R = 1$. But W can't be abelian, since if W had a commuting element of order q and order r it'd have an element of order qr, which can't happen since by assumption each element of W has prime order.

Thus $n_q(W) = r$. Every non-identity element of W has prime order and so lives in some Sylow subgroup, and since all the Sylow subgroups of W intersect trivially we conclude that W is partitioned by its unique Sylow r-subgroup, together with its r Sylow q-subgroups. In particular, $|\Pi| = r+1$.

2 Partitioning Preliminaries

First we prove a number of useful facts about partitioned groups.

Fact 1. Suppose that a group G is partitioned by Π, and let $H \in \Pi$. Then if $x^m \neq 1 \in H$ for some $x \in G$ we have $x \in H$. This immediately follows from the fact that x lies in some $K \in \Pi$ and so x^m is in K as well, and so $K = H$, since each non-identity element lies in exactly one element of Π.

Lemma 1. *Let G be partitioned by Π and let x and y be non-identity elements that lie in different elements of Π, with $xy = yx$. Then x and y both have order p for some prime.*

Proof. First, suppose that $o(x) < o(y)$ and aim for contradiction. Then we have $(xy)^{o(x)} = x^{o(x)}y^{o(x)} = y^{o(x)} \neq 1$ where $y^{o(x)} \neq 1$ since the order of y is strictly greater than the order of x.

Suppose that y lies in $H \in \Pi$. Then $(xy)^{o(x)} = y^{o(x)} \neq 1$ is also in H and so it follows that $xy \in H$. But then $xyy^{-1} = x \in H$ which contradicts our hypothesis. Thus $o(x) \geq o(y)$. Using the same argument, swapping x and y, we must have $o(y) \geq o(x)$ and so $o(y) = o(x)$.

Next, fix $n < o(x)$, we claim that $o(x^n) = o(x) = o(y)$. Then, x^n and y are commuting elements that lie in different partitions, and so by the argument above $o(x^n) = o(y) = o(x)$. This implies that x has prime order - for example if the order of x is pq, then x^p has order $q < pq$. □

Fact 2. Suppose g and h are integers such that $1 < h < g$. Then $g/h < (g-1)/(h-1)$.

Proof. Note that $g/h > 1$, so we have the following:

$$\begin{aligned} \frac{g}{h(h-1)} &> \frac{1}{h-1} \\ \frac{gh - g(h-1)}{h(h-1)} &> \frac{1}{h-1} \\ \frac{g}{h-1} - \frac{g}{h} &> \frac{1}{h-1} \end{aligned}$$

□

Lemma 2. *Let G be equally partitioned by Π and let $X \subseteq G$ be a non-trivial subset of G. Then there exists $H \in \Pi$ such that H contains no conjugate of X.*

Proof. Suppose that for each $H \in \Pi$ we have a conjugate X_H of X with $X_H \subseteq H$ and aim for contradiction. Let $N_H = \mathbf{N}_H(X_H)$. If we let H act on X_H via conjugation, then H contains $|H : N_H|$ conjugates of X_H. These are all G-conjugates of X, so we have that H contains at least $|H : N_H|$ G-conjugates of X (there may be more since some G-conjugates of X in H may not be H-conjugates of X_H).

Now let $N = \mathbf{N}_G(X)$. Then the number of G-conjugates of X is given by $|G : N|$. However, the number of G-conjugates of X is the same as the number of G-conjugates of X_H, so $|G : N| = |G : \mathbf{N}_G(X_H)|$. Since $N_H \subseteq \mathbf{N}_G(X_H)$ it follows that $|G : N| = |G : \mathbf{N}_G(X_H)| \leq |G : N_H| = |G : H||H : N_H|$.

Re-arranging, we have

$$\begin{aligned} |G : N| &\leq |G : H||H : N_H| \\ \frac{|G : N|}{|G : H|} &\leq |H : N_H| \\ \frac{|H||G : N|}{|G|} &\leq |H : N_H| \end{aligned}$$

Now, we argued above that each $H \in \Pi$ contains at least $|H : N_H|$ conjugates of X, so $|G : N|$, the number of conjugates of X in G is at least as big as the sum of the $|H : N_H|$ for all H in Π.

$$|G : N| \geq \sum_{H \in \Pi} |H : N_H|$$

Substituting the inequality above, we have

$$|G : N| \geq \sum_{H \in \Pi} \frac{|H||G : N|}{|G|}$$

Since G is equally partitioned, this sum doesn't really depend on H, and so we actually have $|G : N| \geq |\Pi||G : N|\frac{|H|}{|G|}$, and so we have $|G| \geq |\Pi||H|$. But this is a contradiction, since $|\Pi||H|$ over counts the number of elements in the group by $|\Pi| - 1$ extra identity elements.

We conclude that there must be some $H \in \Pi$ such that H contains no conjugate of X. □

Lemma 3. *Let G be equally partitioned. Then every element of G has prime order.*

Proof. Suppose G has partition Π, and choose an element x of G with composite order, aiming for contradiction. If $\mathcal{K}$ is the conjugacy class of x then by (Lemma 2) we can choose $H \in \Pi$ such that $H \cap \mathcal{K} = \emptyset$.

Next, note that no element h of H can centralize any element k of $\mathcal{K}$. If this were the case then k and h would be commuting elements in distinct members of Π, and thus by (Lemma 1) we would have $o(h) = o(k) = o(x)$ is prime.

Now, let H act on $\mathcal{K}$ by conjugation. Since no element of H fixes any element of $\mathcal{K}$ this action is faithful. K is then partitioned by orbits of size $|H|$, and so $|H|$ divides $|\mathcal{K}|$

On the other hand, choose $K \in \Pi$ such that $x \in \Pi$. Consider the action of K by conjugation on $\mathcal{K} - K$. Since each element of $\mathcal{K} - K$ lies in a different partition from K we know that no element of K can centralize any element of $\mathcal{K} - K$, since otherwise (Lemma 1) would force an element of $\mathcal{K} - K$ to have prime order and so x would have prime order.

Under this action, $\mathcal{K} - K$ is partitioned into orbits of size $|K|$, and so we conclude that $|K|$ divides $\mathcal{K} - K$. Above we showed that $|H|$ divides $|\mathcal{K}|$, but since G is equally partitioned we know that $|H| = |K|$ and so $|K|$ divides $|\mathcal{K}|$ and $|\mathcal{K} - K|$. We have $|\mathcal{K} - K| = |\mathcal{K}| - |\mathcal{K} \cap K|$, and so $|K|$ divides $|\mathcal{K} \cap K|$ as well.

Finally, note that $|\mathcal{K} \cap K| < |K|$ since, say, $1 \in K$ but $1 \notin \mathcal{K}$. Thus $0 < |\mathcal{K} \cap K| < |K|$, which contradicts the fact that $|K|$ divides $|\mathcal{K} \cap K|$. We conclude that each element of G has prime order. □

3 General Preliminaries

Here are some standard results, included in [1] for completeness. We deviate a bit from the presentation in [1], based a conversation with I. M. Isaacs.

The following lemma and proof is (Lemma 6.8) in [2], where it's used to prove a nice result about Frobenius actions (Theorem 6.9)

Lemma 4. *Let Π be a partition of a finite group W, and suppose that W acts via conjugation on an abelian group U. If U has an element with order not dividing $|\Pi|-1$, then there exists a member $X \in \Pi$ such that $\mathbf{C}_U(X) > 1$.*

Proof. For any subgroup H of W, and any element u in U, denote the action of $h \in H$ on u by u^h and then define

$$u_H = \prod_{h \in H} u^h$$

This is well-defined since U is abelian, so the order in which we iterate over H doesn't matter. Also, u_H is fixed by any automorphism in $H \subseteq W$ since applying any automorphism in H to u_H simply permutes the elements of the product. Thus, $u_H \subseteq \mathbf{C}_U(H)$.

Now we turn our attention towards the partition, and suppose that $C_U(X) = 1$ for all X, since otherwise there's nothing to show. Then by the above argument $u_X \in \mathbf{C}_U(X)$ and so $u_X = 1$ for all $X \in \Pi$. Then, we have

$$1 = \prod_{X \in \Pi} u_X = u_W u^{|\Pi|-1}$$

To see why the second equality is true, note that as X runs over Π we're adding exactly one factor u^w for each $1 \neq w \in W$ (recall that each non-identity element of W lies in exactly one partition element). Since the identity is in each member of Π, we're also adding $|\Pi|$ factors of u^1 to the product. One of these factors u^1 is accounted for in u_W, and so $\prod u_X = u_W u^{|\Pi|-1}$.

But now, suppose u is an element with order not dividing $|\Pi| - 1$, then $1 = u_W u^{|\Pi|-1}$, but $u^{|\Pi|-1} \neq 1$ and so $u_W \neq 1$. Since $u_W \in \mathbf{C}_U(W) \subseteq \mathbf{C}_U(X)$ for all $X \in \Pi$ we do have $\mathbf{C}_U(X) > 1$ after all. □

Lemma 5. *Suppose G has a nontrivial normal p-subgroup where p is a prime divisor of $|G|$. Assume that every element of G has prime order. Then G cannot have a subgroup W of order qr, where q and r are possibly equal primes different from p.*

Proof. Suppose $1 \neq U \lhd G$ is our given p-subgroup. Note that it's no loss to assume that U is abelian, since if it's not we can replace U with $\mathbf{Z}(U)$ which is non-trivial and normal in G (since it's characteristic in U).

Suppose that W is a subgroup of order qr and aim for contradiction. First note that as discussed in (Example 2) above W has a partition Π of size $q+1$ or $r+1$. Now, since W acts on U by conjugation, we know that every element of U must have order dividing $|\Pi| - 1$, since otherwise (Lemma 4) would imply that some pair of elements from U and W commute. However, this isn't possible since such a pair of elements would imply the existence of an element of order pr or qr contradicting our assumption that all elements of G have prime order.

On the other hand, since $|\Pi| - 1$ is either q or r, we cannot have any element of U with order dividing $|\Pi| - 1$. This contradiction arose from the assumption that G has a subgroup W of order qr. □

For the next lemma, we need a theorem of Burnside's. The proof uses transfer theory, and so we omit it in the interest of keeping the scope of this presentation manageable. Professor Isaacs plans to prove this result in the ongoing Spring 2010 Finite Group Theory course. This appears as (Theorem 5.13) in [2].

Theorem 2 (Burnside)**.** *Let $P \in \mathrm{Syl}_p(G)$, where G is a finite group, and suppose $P \subseteq \mathbf{Z}(\mathbf{N}_G(P))$. Then G has a normal p-complement.*

Lemma 6. *Suppose that p is the largest prime divisor of $|G|$. Moreover, suppose that every element of G has prime order and that G has a normal p-subgroup. Then G is a p-group or G has a normal Sylow p-subgroup with prime index.*

Proof. Let P be a Sylow p-subgroup of G. There is nothing to prove if $P = G$, so suppose that $P < G$ and let q be the smallest prime divisor of $|G|$. Then, if Q is Sylow q-subgroup of G, we must have $|Q| = q$ since otherwise G would contain a subgroup of order q^2 contradicting (Lemma 5).

Now, let $N = \mathbf{N}_G(Q)$ and $C = \mathbf{C}_G(Q)$. Then we know that $|N : C|$ divides $\phi(q) = q - 1$. But since this index must also divide $|G|$, and q is the smallest prime dividing the order of G, we must have $|N : C| = 1$ and so $N = C$. In this case all of N centralizes Q and so $Q \subseteq \mathbf{Z}(N)$. Applying Burnside's theorem we conclude that G has a normal q-complement M. Additionally, since $|Q| = q$ we know that q is the full q-power dividing G, and so $|G : M| = q$.

Next, note that a Sylow p-subgroup of M is a Sylow p-subgroup of G, and since M is normal it follows that all Sylow p-subgroups of G are contained in M. If $P = M$ then we're done, so assume that $P < M$. This implies that some prime r divides $|M|$, so consider the conjugation action of Q on the set $\mathrm{Syl}_r(M)$.

Fix some $R \in \mathrm{Syl}_r(M)$, and observe that the orbit $\mathcal{O}_R$ has size $|\mathcal{O}_R| = |Q : \mathbf{N}_Q(R)|$. Moreover, since Q has order q it follows that $\mathbf{N}_Q(R)$ is 1 or Q. However, if $\mathbf{N}_Q(R) = 1$ for all Sylow r-subgroups of M then the size of each orbit would be q and so we would have q dividing $|\mathrm{Syl}_r(M)|$. However, this is not possible since $|\mathrm{Syl}_r(M)|$ must divide the order of M and q does not divide the order of M.

From this we conclude that Q normalizes some $R \in \mathrm{Syl}_r(M)$. However, for the same reason that $|Q| = q$ we know that $|R| = r$ and this implies that QR is a subgroup of size qr, contradicting (Lemma 5). We conclude that $P = M$, and so G either is a p-group or has a normal Sylow p-subgroup with prime index. □

Corollary 1. *Assume that every element of G has prime order and that p is the largest prime dividing $|G|$. Then each Sylow p-subgroup of G is a T.I. set. That is, for $P \in \mathrm{Syl}_p(G)$ we have $P \cap P^x = 1$ for all $x \notin \mathbf{N}_G(P)$.*

Proof. Let $P \in \mathrm{Syl}_p(G)$ and choose $D = P \cap P^x$ be chosen such that $|D|$ is as big as possible. Suppose that $1 < D$ and aim for contradiction.

Let $N = \mathbf{N}_G(D)$. We claim that N does not have a unique Sylow p-subgroup. To see why, suppose that $S \subseteq N$ was the only Sylow p-subgroup of N. Then, note that $D < S \cap P$ and $D < S \cap P^x$ since normalizers grow in p-groups.

But now, S is contained in some Sylow p-subgroup T of G. Then we have $D < P \cap T$, and so by the maximality of D we must have $T = P$. But then, since we also have $D < P^x \cap T$ we arrive at the contradiction $D < P^x \cap T = P^x \cap P$.

Thus N must have more than one Sylow p-subgroup. On the other hand, since N satisfies the hypothesis of (Lemma 6) it must have a unique Sylow p-subgroup, and we arrive at a contradiction. We conclude that $D = 1$ and so P is a T.I. set. □

4 Equally Partitioned Groups

With all this built up machinery we can proceed to prove our main result.

Theorem 3. *Let G be equally partitioned with partition Π. Then every $K \in \Pi$ has self-normalizing Sylow p-subgroups, where p is the largest prime divisor of $|G|$.*

Proof. Let p be the largest prime divisor of $|G|$ and let P be a Sylow p-subgroup of G. Consider the group $N = \mathbf{N}_G(P)$. Since G is equally partitioned, by (Lemma 3), every element of G, and thus of N, has prime order. This group has a normal p-subgroup, so applying (Lemma 6) we know that either $P = N$ or $|N : P| = q$ for some prime. This implies that we can write $N = PC$ where C is either trivial or a cyclic group of order q. Also, $P \cap C = 1$, so $|N| = |P||C|$. Additionally, by (Corollary 1) P is a T.I. set.

We'll be computing a few facts about the relevant orders, so to increase readability let $|G| = g$, $|P| = p^a$ and $|C| = c$. Let Π be the given partition and let $|H| = h$ be the size of the partition elements. Finally, let p^b be the p-part of h.

First, observe that since P is a T.I. set we can easily count. Each P contributes $p^a - 1$ distinct elements of order p and G contains $|G : N| = |G : PC| = g/(p^a c)$ different Sylow p-subgroups. It follows that G contains $\frac{g}{p^a c}(p^a - 1)$ elements of order p.

Now, we proved earlier (Lemma 2) that the orbit of any subset under conjugation misses some member of the partition. Thus, choose H in Π such that $H \cap C^g = 1$ for all $g \in G$. Let P_0 be a Sylow p-subgroup of H. We know that P_0 is contained in some Sylow p-subgroup of G, so without loss we can relabel if necessary and assume that $P_0 \subseteq P$.

Since P is a T.I. set, P_0 uniquely determines P. That is, P_0 is contained in precisely one Sylow p-subgroup. Since P_0 canonically determines P, it follows that anything normalizing P_0 must normalize P, and so $\mathbf{N}_H(P_0) \subseteq \mathbf{N}_G(P) = N = PC$. This implies that the order of $\mathbf{N}_H(P_0)$ divides $p^b q$. If C_0 is a Sylow q-subgroup of $\mathbf{N}_H(P_0)$, then $\mathbf{N}_H(P_0) = P_0 C_0$. Moreover, C_0 is contained in some Sylow q-subgroup of N, so $C_0 \subseteq C^g$ for some g. However, we know that $C^g \cap H = 1$ for all g, so $C_0 = 1$ and $P_0 = \mathbf{N}_H(P_0)$. It follows that $|H : P_0| = h/p^b \equiv 1 \bmod p$.

Now, let K be an arbitrary partition member from Π, and let P_1 be a Sylow p-subgroup of K. Following the same reasoning as above, we conclude that $\mathbf{N}_K(P_1) = P_1 C_1$ where C_1 is contained in some conjugate C^x. Since K is arbitrary we no longer assume that $C^x \cap K = 1$. However, $P_1 \cap C_1 = 1$ so we have $|\mathbf{N}_K(P_1)| = |P_1||C_1| = p^b|C_1|$. From this we have $|K : \mathbf{N}_K(P_1)| = h/(p^b|C_1|) \equiv 1 \bmod p$. Since $h/p^b \equiv 1 \bmod p$ it follows that $|C_1| \equiv 1 \bmod p$. On the other hand, we know that $|C_1|$ is either 1 or q where $q < p$. This forces $C_1 = 1$ and so $\mathbf{N}_K(P_1) = P_1$. We've shown that every partition element of Π has self-normalizing Sylow p-subgroups. □

Theorem 4 (Isaacs)**.** *Let G be equally partitioned. Then G is a p-group of exponent p.*

Proof. Let p be the largest prime divisor of $|G|$. Note that by (Lemma 3) we know that each element of G has prime order, so we want to show that $|G|$ is a p-power.

Continuing the notation of the previous proof, let $|G| = g$ and denote the order of each partition member $H \in \Pi$ by h. Let the p-part of g be p^a and the p-part of h be p^b.

Let P be a Sylow p-subgroup of G. We first claim that for any subgroup $U \subseteq G$, if $P \cap U \neq 1$ then $P \cap U$ is a Sylow p-subgroup of U. This follows since P is a T.I. set by

(Corollary 1). If $P \cap U$ wasn't Sylow, then $P \cap U$ would be properly contained in a Sylow p-subgroup S of U, which in turn would be contained in some Sylow p-subgroup T of G. However, then $T \neq P$ since T contains all of S, and this in turn forces $T \cap P \supseteq P \cap U > 1$ contradicting the fact that P is a T.I. set.

Consider an arbitrary partition member $K \in \Pi$. Then $P \cap K \neq 1$ for some $P \in \mathrm{Syl}_p(G)$, and so we must have $|P \cap K| = p^b$, the full p-part of $|K|$. Now, note that every element of P is in some partition member, so $P = \bigcup_{K \in \Pi}(P \cap K)$. Suppose that P intersects m partition members non-trivially. Since every non-identity element of P is contained in exactly one partition element, we have $|P| - 1 = m(|P \cap K| - 1)$, and so we see that $(p^b - 1)|(p^a - 1)$.

Next, by the Lemma immediately preceding, we know that the Sylow p-subgroups of K are self-normalizing. Since $|K| = h$ and the p-part of $|K|$ is p^b, it follows that the number of Sylow p-subgroups in K is h/p^b. Moreover, by (Corollary 1) each of these Sylow p-subgroups are T.I. sets and so intersect trivially with each other. It follows that K has $(h/p^b)(p^b - 1)$ elements of order p.

Now let's try and count order p elements in all of G. Take N to be the normalizer of a Sylow p-subgroup P of G. Again by (Lemma 6) we can conclude that $N = PC$ where $C = 1$ or C is a q-group for some prime $q \neq p$. Write $|C| = c$, and it follows that the number of Sylow p-subgroups of G is $g/(p^a c)$. Since each Sylow p-subgroup of G is T.I. set, we conclude that G contains $\frac{g}{p^a c}(p^a - 1)$ elements of order p.

On the other hand, since each non-identity element of G lies in exactly one partition member, it follows that $g - 1 = |\Pi|(h - 1)$ and so $|\Pi| = \frac{g-1}{h-1}$. We know that each partition member contains $(h/p^b)(p^b - 1)$ elements of order p, and so it follows that the number of elements in G of order p is given by:

$$\frac{g}{p^a c}(p^a - 1) = \frac{g-1}{h-1}\left(\frac{h}{p^b}(p^b - 1)\right)$$

Re-arranging the above equality, we have

$$\frac{g}{h}\left(\frac{1}{c} \cdot \frac{p^a - 1}{p^a}\right) = \frac{g-1}{h-1}\left(\frac{p^b - 1}{p^b}\right)$$

Since $g/h < (g-1)/(h-1)$ we conclude that $\frac{1}{c}\frac{p^a-1}{p^a}$ is strictly greater than $\frac{p^b-1}{p^b}$. Then we have the following:

$$\frac{1}{c} > \frac{p^a - 1}{p^a} \cdot \frac{1}{c} > \frac{p^b - 1}{p^b} = 1 - \frac{1}{p^b} \geq \frac{1}{2}$$

so we conclude that $c = 1$. Substituting this into the formula counting p-order elements of G we have

$$\begin{aligned} \frac{g}{p^a}(p^a - 1) &= \frac{g-1}{h-1}\left(\frac{h}{p^b}(p^b - 1)\right) \\ (h-1)p^b g(p^a - 1) &= p^a(g-1)h(p^b - 1) \\ gp^b\left((h-1)(p^a - 1)\right) &= hp^a\left((g-1)(p^b - 1)\right) \end{aligned} \tag{1}$$

Since $(p^a - 1)/(p^b - 1)$ is an integer, it follows that $gp^b | hp^a(g-1)$. Next, note that $((g-1), gp^b) = 1$. To see why, note that no prime that divides g can divide $g - 1$, and the primes in gp^b are the same as the primes in g. From this it follows that $gp^b | hp^a$.

The p-parts of gp^b and hp^a are the same, and we know that h divides g and it follows $hp^a|gp^b$ and so $gp^b = hp^a$. Using this we can rewrite (Equation 1)

$$(h-1)(p^a-1) = (g-1)(p^b-1)$$

Multiplying out and subtracting from the equation $hp^a = gp^b$ yields $h + p^a = g + p^b$. But now, since $h < g$ and h divides g it follows that h is at most $g/2$. It follows that

$$\frac{g}{2} \leq g - h = p^a - p^b < p^a$$

It follows that $\frac{g}{p^a} < \frac{1}{2}$. But we also know that p^a divides g, and so $\frac{g}{p^a} = 1$. We've shown that $g = |G| = p^a$ and so G is a p-group of exponent p. □

References

[1] I.M. Isaacs, *Equally partitioned groups*, Pacific J. Math **49** (1973), no. 1, 109–116.

[2] ______, *Finite Group Theory*, Amer Mathematical Society, 2008.