GROUPS AND SYMMETRY — ABSTRACT GROUP THEORY

N. P. STRICKLAND

1. The Sylow theorems

Let G be a finite group of order n, say. Lagrange's theorem says that if H is a subgroup of G and $|H| = d$, then d is a divisor of n. It is natural to ask whether the converse is true: given a divisor d of n, can we find a subgroup $H \leq G$ such that $|H| = d$? The answer is no in general; for example one can check that the group A_4 has order 12 but there is no subgroup of order 6. However, if d is a power of a prime number, then the answer turns out to be yes, and in fact we can say a great deal more. This follows from the Sylow theorems, which we will prove in this section.

Fix a finite group G and a prime p. We can write $|G|$ in the form $p^v m$, where p does not divide m. A *Sylow p-subgroup* of G is a subgroup $P \leq G$ such that $|P| = p^v$. We write n_p for the number of Sylow p-subgroups of G (which *a priori* could be zero).

Theorem 1.1. (a) *There is at least one Sylow p-subgroup, so $n_p > 0$.*
(b) *Moreover, n_p divides m and is congruent to 1 mod p.*
(c) *Any two Sylow p-subgroups are conjugate.*
(d) *Any p-subgroup of G is contained in a Sylow p-subgroup.*

Before giving the proof, we outline some applications. These will be discussed in more detail and extended in the next section.

Example 1.2. Let G be a group of order $35 = 5 \times 7$. Then n_5 divides 7 so $n_5 = 1$ or $n_5 = 7$, but also $n_5 = 1 \pmod 5$ so we must have $n_5 = 1$. Thus, there is precisely one subgroup $P \leq G$ with $|P| = 5$. Moreover, we know that n_7 divides 5 and $n_7 = 1 \pmod 7$ so $n_7 = 1$, so there is a unique subgroup $Q \leq G$ of order 7. Using the fact that P is unique we see that it is normal in G; this will be explained in Proposition 1.5 below. Similarly, Q is normal. The order of $P \cap Q$ divides $|P| = 5$ and also divides $|Q| = 7$, so $|P \cap Q| = 1$ so $P \cap Q = \{1\}$. Using this and the fact that P and Q are normal and $|G| = |P||Q|$ one can check that $G \simeq P \times Q \simeq \mathbb{Z}_5 \times \mathbb{Z}_7$. Thus, any group of order 35 is isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_7$.

Example 1.3. Recall that a group G is *simple* if the only normal subgroups of G are $\{1\}$ and G. Let G be a simple group of order 60. We'll outline a proof that G must be isomorphic to A_5. Note that $60 = 2^2 \times 15$ so n_2 divides 15 by part (b) of the Theorem, so $n_2 \in \{1, 3, 5, 15\}$. If $n_2 = 1$ then the unique Sylow 2-subgroup is normal, contradicting the simplicity of G. A slightly more complicated argument shows that n_2 cannot be 3 either. Indeed, G acts by conjugation on the set of Sylow 2-subgroups, giving a homomorphism $\phi\colon G \to S_{n_2}$. This is nontrivial, because all Sylow 2-subgroups are conjugate, by part (c) of the Theorem. This means that $\ker(\phi) \neq G$ and $\ker(\phi)$ is a normal subgroup of G so we must have $\ker(\phi) = \{1\}$. This means that ϕ is injective, so $|G| \leq |S_{n_2}|$, so $n_2! \geq 60$. As $4! = 24$ and $5! = 120$ the equation $n_2! \geq 60$ is equivalent to $n_2 \geq 5$. We already know that $n_2 \in \{1, 3, 5, 15\}$ so $n_2 = 5$ or $n_2 = 15$. In fact the case $n_2 = 15$ cannot occur (although we will not prove this here) so $n_2 = 5$. We thus have an injective homomorphism $\phi\colon G \to S_5$. As ϕ is injective, the image $\phi(G)$ has order 60, and one can check that A_5 is the only subgroup of S_5 of order 60, so ϕ gives an isomorphism $G \simeq A_5$.

Proof of (a). Let $\mathcal{X}$ be the set of all subsets $X \subseteq G$ such that $|X| = p^v$. In general, any set of order N has $\begin{pmatrix} N \\ M \end{pmatrix}$ subsets of order M, so $|\mathcal{X}| = \begin{pmatrix} p^v m \\ p^v \end{pmatrix}$. We claim that this number is not divisible

Date: December 1, 2003.

by p. To see this, put $q = p^v m - p^v = p^v(m-1)$ and note that $\left(\begin{array}{c} p^v m \\ p^v \end{array} \right) = (p^v m)!/(p^v!\, q!)$. We also have

$$(p^v m)!/q! = (q+1)(q+2)\dots(q+p^v)$$

so

$$\left(\begin{array}{c} p^v m \\ p^v \end{array} \right) = \frac{1}{q+1}\frac{2}{q+2}\cdots\frac{p^v}{q+p^v} = \prod_{j=1}^{p^v}\frac{j}{q+j}.$$

Now let w_j be the largest number such that j is divisible by p^{w_j} (for $j = 1, \dots, p^v$). As $j \leq p^v$ we must have $w_j \leq v$ so the number $q = p^v(m-1)$ is also divisible by p^{w_j}. It follows that $q+j$ is divisible by p^{w_j} as well, so all the p's on the top in our equation for $\left(\begin{array}{c} p^v m \\ p^v \end{array} \right)$ are cancelled out by p's on the bottom. It follows that $|\mathcal{X}| \neq 0 \pmod p$, as claimed.

Now let G act on $\mathcal{X}$ by $gX = \{gx \mid x \in X\}$, and divide $\mathcal{X}$ into orbits under this action, say $\mathcal{X} = \mathcal{X}_1 \cup \dots \cup \mathcal{X}_k$. Orbits are always disjoint so $|\mathcal{X}| = \sum_j |\mathcal{X}_j|$. If each of the numbers $|\mathcal{X}_j|$ were divisible by p, then $|\mathcal{X}|$ would also be divisible by p, contrary to what we just proved. Thus we can choose j such that the number $m' := |\mathcal{X}_j|$ is not divisible by p. Choose an element $X \in \mathcal{X}_j$, so (by the definition of $\mathcal{X}$) X is a subset of G with p^v elements. Put $P = \operatorname{stab}_G(X) = \{g \in G \mid gX = X\}$. The orbit-stabiliser theorem says that $|G| = |\operatorname{stab}_G(X)||\operatorname{orb}_G(X)|$, or in other words $p^v m = |P|m'$. As p^v divides $|P|m'$ and p does not divide m' we see that p^v divides $|P|$. Next, fix an element $x_0 \in X$. For each $g \in P$ we have $gx_0 \in gX = X$ so $Px_0 \subseteq X$, so $p^v = |X| \geq |Px_0| = |P|$. As p^v divides $|P|$ and $|P| \leq p^v$ we must have $|P| = p^v$, so P is a Sylow p-subgroup of G. □

For the remaining parts we need the following lemma. Recall that a *p-group* is a group whose order is a power of the prime p.

Lemma 1.4. *Let P be a finite p-group, and let X be a set with an action of P. Put*

$$\operatorname{Fix}(P) = \operatorname{Fix}(P, X) = \{x \in X \mid gx = x \text{ for all } g \in P\}.$$

Then $|\operatorname{Fix}(P)| = |X| \pmod p$. In particular, if $|X| \neq 0 \pmod p$ then $\operatorname{Fix}(P) \neq \emptyset$.

Proof. The order of P is p^v for some $v \geq 0$. Divide X into orbits and list them in order of size, say $X = X_1 \cup \dots \cup X_k$ with $|X_1| \leq |X_2| \leq \dots \leq |X_k|$. As each set X_j is an orbit, its order divides $|P| = p^v$, so $|X_j| = p^{w_j}$ for some w_j with $0 \leq w_1 \leq w_2 \leq \dots \leq w_k \leq v$. For some r (possibly $r = 0$) we have $w_j = 0$ when $1 \leq j \leq r$ and $w_j > 0$ when $j > r$. We have

$$|X| = \sum_{j=1}^{k} |X_j| = \sum_{j=1}^{r} 1 + \sum_{j=r+1}^{k} p^{w_j} = r + \sum_{j>r} p^{w_j} = r \pmod p.$$

On the other hand, an eement $x \in X$ lies in $\operatorname{Fix}(P)$ if and only if the orbit Px consists of the single element x, so $|\operatorname{Fix}(P)|$ is the number of orbits of size 1, which is r. Thus $|X| = |\operatorname{Fix}(P)| \pmod p$, as claimed.

Now suppose that $|X| \neq 0 \pmod p$. Then $|\operatorname{Fix}(P)| \neq 0 \pmod p$, so $|\operatorname{Fix}(P)| \neq 0$, so $\operatorname{Fix}(X) \neq \emptyset$. □

Proof of (c) and (d). Let P be a Sylow p-subgroup of G, and let Q be any p-subgroup of G. Note that $|P| = p^v$ and $|Q| = p^w$ for some $w \leq v$. As usual we write G/P for the set of right cosets of P, so a typical element of G/P has the form xP for some $x \in G$. Note that $|G/P| = |G|/|P| = m$, which is not divisible by p. We let Q act on G/P by $g * (xP) = gxP$ for $g \in Q$. Note that $|G/P| = m \neq 0 \pmod p$ and Q is a p-group so by Lemma 1.4 there is a fixed point, in other words a coset xP such that $gxP = xP$ for all $g \in Q$. This means that $x^{-1}gxP = P$, so $x^{-1}gx \in P$, so $g = x(x^{-1}gx)x^{-1} \in xPx^{-1}$. This proves that $Q \subseteq xPx^{-1}$. Now xPx^{-1} is conjugate to P so it is a subgroup of G with the same order as P, in other words it is another Sylow p-subgroup. This shows that Q is contained in a Sylow p-subgroup, as claimed in (d).

Now suppose that Q itself is a Sylow p-subgroup. Then $Q \leq xPx^{-1}$ but $|Q| = |xPx^{-1}| = p^v$ so $Q = xPx^{-1}$. Thus Q is conjugate to P, as claimed in (c). □

Proof of (b). Let $\mathcal{P}$ be the set of all Sylow p-subgroups of G, so $n_p = |\mathcal{P}|$. Let G act on $\mathcal{P}$ by conjugation, so $g * P = gPg^{-1}$. Choose a Sylow p-subgroup $P \in \mathcal{P}$, and put

$$N = \mathrm{stab}_G(P) = \{g \in G \mid gPg^{-1} = P\}.$$

It is clear that $P \leq N \leq G$ so p^v divides $|N|$ and $|N|$ divides $p^v m$, so $|N| = p^v k$ for some k dividing m.

As all Sylow p-subgroups are conjugate to P, we have $\mathcal{P} = \mathrm{orb}_G(P)$ and so $|G| = |N||\mathcal{P}|$, so $p^v m = p^v k n_p$, so $m = k n_p$. Thus n_p divides m.

Note also that P can be thought of as a Sylow p-subgroup of N. Part (c) of the Theorem works for any finite group, in particular it works for the group N, so any other Sylow p-subgroup Q of N is conjugate *in* N to P. This means that $Q = gPg^{-1}$ for some $g \in N$. By the definition of N, this means that $Q = P$. Thus, P is the *unique* Sylow p-subgroup of N.

Before we considered the action of all of G on $\mathcal{P}$; now we restrict attention to the action of the subgroup P. Lemma 1.4 tells us that $|\mathrm{Fix}(P, \mathcal{P})| = |\mathcal{P}| = n_p \pmod p$. We want to prove that $n_p = 1 \pmod p$, so it will be enough to show that $\mathrm{Fix}(P, \mathcal{P}) = \{P\}$. Clearly if $g \in P$ then $gPg^{-1} = P$, which shows that $P \in \mathrm{Fix}(P, \mathcal{P})$. Conversely, suppose that $Q \in \mathrm{Fix}(P, \mathcal{P})$, so Q is a Sylow p-subgroup and $gPg^{-1} = P$ for all $g \in Q$. This means that Q is a Sylow p-subgroup of N, which means that $Q = P$ by the previous paragraph. Thus $\mathrm{Fix}(P, \mathcal{P}) = \{P\}$ and $|\mathrm{Fix}(P, \mathcal{P})| = 1$ as required. □

Proposition 1.5. *If $n_p = 1$ then the Sylow p-subgroup of G is a normal subgroup. If $n_p > 1$ then none of the Sylow p-subgroups is normal.*

Proof. Suppose that $n_p = 1$, so there is a unique Sylow p-subgroup, which we call P. If $g \in G$ then gPg^{-1} is a Sylow p-subgroup so it must be equal to P; this says that P is normal.

Now suppose that $n_p > 1$. If P is any Sylow p-subgroup, we can choose a different Sylow p-subgroup, say Q. As all such subgroups are conjugate, there is some $g \in G$ such that $gPg^{-1} = Q \neq P$. This means that P is not normal. □

2. Groups of small order

We now try to classify groups of various small orders, using the Sylow theorems as one of our main tools.

Many of our results involve the cyclic groups:

$$C_n = \{1, R, \dots, R^{n-1}\}$$

with $R^n = 1$. We start with two general facts about these groups.

Lemma 2.1. *If G is a group and $g \in G$ and $g^n = 1$, then there is a homomorphism $\phi\colon C_n \to G$ with $\phi(R) = g$.*

Proof. As $C_n = \{1 = R^0, R, \dots, R^{n-1}\}$, we can define a function $\phi\colon C_n \to G$ by $\phi(R^i) = g^i$ for $i = 0, \dots, n-1$. To see that this is a homomorphism, consider two elements $R^i, R^j \in C_n$ with $0 \leq i < n$. If $i + j < n$ then

$$\phi(R^i.R^j) = \phi(R^{i+j}) = g^{i+j} = g^i g^j = \phi(R^i)\phi(R^j).$$

Suppose instead that $i + j \geq n$. By assumption we have $0 \leq i, j < n$, so $i + j < 2n$. Thus, if we put $k = i + j - n$ then $0 \leq k < n$, so $\phi(R^k) = g^k$. We also have

$$R^i R^j = R^{i+j} = R^{k-n} = R^k (R^n)^{-1} = R^k$$
$$g^i g^j = g^{i+j} = g^{k-n} = g^k (g^n)^{-1} = g^k$$

so

$$\phi(R^i.R^j) = \phi(R^{i+j}) = \phi(R^k) = g^k = g^i g^j = \phi(R^i)\phi(R^j).$$

We thus have $\phi(R^i.R^j) = \phi(R^i)\phi(R^j)$ in all cases, showing that ϕ is a homomorphism. □

Lemma 2.2. *If n and m are coprime, then $C_{nm} \simeq C_n \times C_m$.*

Proof. We write r_k for the generator of C_k, and define $\phi\colon C_{nm} \to C_n \times C_m$ by $\phi(r_{nm}^i) = (r_n^i, r_m^i)$. It is easy to see that this is a homomorphism. Suppose that r_{nm}^i lies in the kernel of ϕ. This means that $(r_n^i, r_m^i) = (1, 1)$, which means that $r_n^i = 1$ in C_n and $r_m^i = 1$ in C_m. As $r_n^i = 1$ we see that i must be divisible by n, and as $r_m^i = 1$ we see that i must be divisible by m. As n and m are coprime this means that i is divisible by nm, so $r_{nm}^i = 1$. This shows that the kernel of ϕ is the trivial group, so ϕ is injective. This means that $|\phi(C_{nm})| = |C_{nm}| = nm = |C_n \times C_m$, so $\phi(C_{nm})$ must be all of $C_n \times C_m$, so ϕ is surjective as well as injective, so ϕ is an isomorphism. □

We next recall the basic result about groups of prime order.

Proposition 2.3. *If G is a group whose order is a prime number p, then G is isomorphic to C_p.*

Proof. Let g be any element of G other than the identity. Then the order of g is not equal to 1 and it divides p so it must be equal to p. The subgroup generated by g is thus equal to the whole group, and it follows that G is cyclic of order p. More precisely, we can define a homomorphism $\phi\colon C_p \to G$ by $\phi(R^i) = g^i$, and we find that ϕ is an isomorphism. □

We would next like to study groups of order p^2, where p is prime. We will first need a result about general p-groups.

Definition 2.4. The *centre* of a group G is the set $Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$, so an element z lies in the centre if and only if it commutes with all other elements. One checks that $Z(G)$ is a normal subgroup of G and that it is Abelian.

Example 2.5. The centre of the symmetric group S_n is the trivial group (provided that $n > 2$). To see this, suppose that σ lies in the centre. For each i, let ρ_i be the $(n-1)$-cycle formed by the numbers $1, \dots, n$ with i missing, so $\rho_i(i) = i$ and $\rho_i(j) \neq j$ if $j \neq i$. Now $\rho_i\sigma = \sigma\rho_i$ so $\rho_i(\sigma(i)) = \sigma(\rho_i(i)) = \sigma(i)$, so $\sigma(i)$ is fixed by the action of ρ_i. The only fixed point is i, so $\sigma(i) = i$. This holds for all i, so $\sigma = 1$.

Proposition 2.6. *If P is a nontrivial p-group then $Z(P) \neq \{1\}$.*

Proof. Let P act on itself by conjugation, so $g * x = gxg^{-1}$. Note that $g * x = x$ if and only if $gx = xg$, or in other words g commutes with x. Thus x is fixed under the action of P iff $g * x = x$ for all g, iff $x \in Z(P)$. Thus Lemma 1.4 tells us that $|Z(P)| = |P| \pmod p$. As P is a nontrivial p-group we have $|P| = p^v$ for some $v > 0$ so $|P| = 0 \pmod p$, so $|Z(P)|$ is divisible by p. Moreover, $1 \in Z(P)$ so $|Z(P)| > 0$. It follows that $|Z(G)| \geq p$, so $Z(G) \neq \{1\}$. □

Lemma 2.7. *Let G be a finite group, and let P and Q be subgroups of G. Define a function $\phi\colon P \times Q \to G$ by $\phi(x, y) = xy$.*

(a) *If every element of P commutes with every element of Q, then ϕ is a homomorphism.*
(b) *If we also have $P \cap Q = \{1\}$, then ϕ is injective.*

Proof. (a) Suppose that every element of P commutes with every element of Q. Consider elements $x_0, x_1 \in P$ and $y_0, y_1 \in Q$, so (x_0, y_0) and (x_1, y_1) are elements of $P \times Q$. We then have

$$\begin{aligned}
\phi((x_0, y_0)(x_1, y_1)) &= \phi((x_0x_1, y_0y_1)) && \text{(definition of } P \times Q) \\
&= x_0x_1y_0y_1 && \text{(definition of } \phi) \\
&= x_0y_0x_1y_1 && \text{(because } x_1 \text{ commutes with } y_0) \\
&= \phi((x_0, y_0))\phi((x_1, y_1)) && \text{(definition of } \phi)
\end{aligned}$$

This shows that ϕ is a homomorphism.

(b) Now suppose as well that $P \cap Q = \{1\}$. Consider an element $(x, y) \in \ker(\phi)$. This means that $(x, y) \in P \times Q$ and and $\phi((x, y)) = 1$, or in other words, $x \in P$ and $y \in Q$ and $xy = 1$. This means that $x = y^{-1}$, and $y \in Q$, so $x \in Q$. We are also given that $x \in P$, so $x \in P \cap Q = \{1\}$, so $x = 1$. This means that $y^{-1} = 1$, so $y = 1$, so $(x, y) = (1, 1)$. This proves that the kernel of ϕ is the trivial group, so ϕ is injective.

□

Proposition 2.8. *Let G be a group of order p^2. Then G is isomorphic either to $C_p \times C_p$ or to C_{p^2} (and so G is always Abelian).*

Proof. If G has an element of order p^2 then it is cyclic and thus isomorphic to C_{p^2}. Suppose instead that all nontrivial elements of G have order p. By Proposition 2.6, we can choose a nontrivial element $z \in Z(G)$. This generates a subgroup $P \leq Z(G) \leq G$ of order p. Let g be any element of G not lying in P, and let Q be the subgroup generated by g, which again has order p. By Lemma 2.7, we can define a homomorphism $\phi\colon P \times Q \to G$ by $\phi(x, y) = xy$. Let H be the image of ϕ, so H is a subgroup of G, so $|H|$ divides $|G| = p^2$, so $|H|$ is 1, p or p^2. It is clear that $P \leq H$ and $g \in H \setminus P$, so $|H| \geq p + 1$, so $|H|$ must be p^2. This means that $H = G$, so ϕ is surjective. As $P \times Q$ and G have the same size, any sutrjective function between them must be bijective, so ϕ is an isomorphism. We also know that P and Q are both isomorphic to C_p, so $G \simeq P \times Q \simeq C_p \times C_p$. □

Proposition 2.9. *Let G be a finite group, and let P and Q be* normal *subgroups of orders p and q. Suppose that p and q are coprime, and that $pq = |G|$. Then $G \simeq P \times Q$.*

Proof. First, put $r = |P \cap Q|$. As $P \cap Q$ is a subgroup of P, we see that r divides p. As $P \cap Q$ is a subgroup of Q, we see that r also divides q. As p and q are coprime, this means that $r = 1$, so $P \cap Q$ is the trivial group.

Now consider elements $x \in P$ and $y \in Q$, and put $z = xyx^{-1}y^{-1}$. We will show that $z \in P \cap Q$, so that $z = 1$. Indeed, we have $y \in Q$ and Q is normal, so $xyx^{-1} \in Q$. As y^{-1} also lies in Q, we deduce that $z = (xyx^{-1})y^{-1} \in Q$. Similarly, we know that $x^{-1} \in P$ and P is normal so $yx^{-1}y^{-1} \in P$. We also know that $x \in P$, so $z = x(yx^{-1}y^{-1}) \in P$. This gives $z \in P \cap Q$, so $z = 1$, or in other words $1 = xyx^{-1}y^{-1}$. If we multiply this on the right by yx, we get $yx = xyx^{-1}y^{-1}yx = xy$, so x commutes with y. Lemma 2.7 now tells us that we can define an injective homomorphism $\phi\colon P \times Q \to G$ by $\phi(x, y) = xy$. As this is injective, we have

$$|\phi(P \times Q)| = |P \times Q| = pq = |G|,$$

so $\phi(P \times Q) = G$, so ϕ is also surjective. This means that ϕ is an isomorphism of groups. □

Proposition 2.10. *Let G be a group of order pq where p and q are primes and $p < q$. Suppose also that $q - 1$ is not divisible by p. Then $G \simeq C_p \times C_q$.*

Proof. We know that n_p divides q and q is prime so $n_p = 1$ or $n_p = q$. However we also know that $n_p = 1 \pmod p$ so p divides $n_p - 1$. We are told that p does not divide $q - 1$, so n_p cannot be equal to q, so $n_p = 1$. It follows that there is a unique Sylow p-subgroup, which we call P. Note that $|P| = p$ and so $P \simeq C_p$, and also that P is normal.

Next, we know that n_q divides p, so $n_q = 1$ or $n_q = p$. We also know that $n_q = 1 \pmod q$, so $n_q - 1$ is divisible by q. Note that $0 < p - 1 < q$, so $p - 1$ cannot be divisible by q, so we must have $n_q = 1$. We therefore have a unique Sylow q-subgroup, which we call Q. We note that $|Q| = q$ and that Q is normal.

It is now clear that the conditions of Proposition 2.9 are satisfied, so $G \simeq P \times Q \simeq C_p \times C_q$. □

Proposition 2.11. *Let p be a prime number with $p > 2$, and let G be a group with $|G| = 2p$. Then either $G \simeq C_p \times C_2 \simeq C_{2p}$ or $G \simeq D_p$.*

Proof. We know that n_p divides 2 and that $n_p - 1$ is divisible by p. It follows that $n_p = 1$, so there is a unique Sylow p-subgroup, which we call P. We choose a nontrivial element $g \in P$, and define an isomorphism $\phi\colon C_p \to P$ by $\phi(R^i) = g^i$.

Next, let Q be a Sylow 2-subgroup, so $|Q| = 2$, so $Q = \{1, h\}$ for some element h with $h^2 = 1$. As P is normal, we know that $hgh^{-1} \in P$, so $hgh^{-1} = g^a$ for some a. It follows that

$$h^2gh^{-2} = hg^ah^{-1} = (hgh^{-1})^a = (g^a)^a = g^{(a^2)}.$$

On the other hand, we have $h^2 = 1$, so $h^{-2} = 1$, so $h^2gh^{-2} = g$. We thus have $g = g^{a^2}$, so $g^{a^2-1} = 1$, so $a^2 - 1$ must be divisible by p. As p is prime and $a^2 - 1 = (a + 1)(a - 1)$, we see that either $a + 1$ or $a - 1$ must be divisible by p.

If $a-1$ is divisible by p then $g^a = g$, so $h^{-1}gh = g$, so g commutes with h. In this case, the conditions of Lemma 2.7 are satisfied and we find that $G \simeq P \times Q \simeq C_p \times C_2 \simeq C_{2p}$.

Suppose instead that $a+1$ is divisible by p. This means that $g^a = g^{-1}$, so $hgh^{-1} = g^{-1}$. We then define a function $\phi\colon D_p \to G$ by $\phi(R^i) = g^i$ and $\phi(R^iS) = g^ih$ for $0 \leq i < p$. It is straightforward to check that this is a homomorphism, the key point being that $SRS^{-1} = R^{-1}$ in D_p, which corresponds to the relation $hgh^{-1} = g^{-1}$ in G. The image of ϕ contains both P and Q, so the order of the image is divisible by p and 2 and thus by $2p$. It follows that ϕ is surjective, but the groups D_p and G have the same order, so ϕ must actually be an isomorphism. □

Remark 2.12. The above proposition can be extended to show that when p and q are distinct primes, any group of order pq is a "semidirect product" of C_p and C_q.

Now consider groups of order at most 40. Using Propositions 2.3, 2.8, 2.10 and 2.11, we can classify all groups of the following orders:

$$1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 15, 17, 19, 22, 23, 25, 26, 29, 31, 33, 35, 37, 38.$$

More work is needed to classify groups of the remaining orders:

$$8, 12, 16, 18, 20, 21, 24, 27, 28, 32, 34, 36, 39.$$