



# A Course in Group Theory

John F. Humphreys

# A Course in Group Theory by John F. Humphreys

## Chapter 7: Normal Subgroups and Quotient Groups: Exercises

**7-3:** Let  $G$  be the group  $Q_8$  discussed during the classification of groups of order eight in *Chapter 5*. Let  $N$  be the subset  $\{1, x^2\}$ . Show that  $N$  is a *subgroup* of  $G$ . By listing cosets, show that  $N$  is a *normal subgroup* of  $G$ , and determine the multiplication table for  $G/N$ .

**Answer:** Recall from *Chapter 5* that  $Q_8$  has presentation  $\langle x, y : y^4 = 1, y^2 = x^2 \text{ and } yx = xy^{-1} \rangle$ ; and that  $Q_8$  consists of the following eight elements:  $1, x, x^2, x^3, y, yx, yx^2$  and  $yx^3$ . To show that  $N$  is a subgroup of  $G$ , we must show that  $N$  satisfies the following three requirements:

- (a) the identity element of  $G$  is in  $H$ ;
- (b) if  $x$  and  $y$  are in  $H$ , then so is  $xy$ ;
- (c) if  $h$  is in  $H$ , then so is  $h^{-1}$ .

We see that (a) holds automatically in this case because  $1 \in N$ . To see that (b) holds, all we must note is that  $(x^2)(x^2) = x^4 = 1 \in N$  (as  $1 = y^4 = (y^2)(y^2) = (x^2)(x^2) = x^4$ ) so that  $N$  is closed under *multiplication*. Finally, because  $1^{-1} = 1$ , and because

$$\begin{aligned} (x^2)^{-1} &= (y^2)^{-1} \text{ (as } y^2 = x^2) \\ &= y^{-2} \\ &= y^2 \text{ (as } y^4 = 1) \\ &= x^2 \text{ (as } y^2 = x^2), \end{aligned}$$

then  $N$  is closed when taking *inverses*, and so  $N$  must be a subgroup.

To show that  $N$  is a normal subgroup, we can list all the **left** and **right** cosets of  $N$  and show that each left coset is *equal* to the corresponding right coset:

### LEFT COSETS

$$\begin{aligned} 1N &= 1\{1, x^2\} = \{1, x^2\} \\ xN &= x\{1, x^2\} = \{x, x^3\} \\ x^2N &= x^2\{1, x^2\} = \{x^2, 1\} \\ x^3N &= x^3\{1, x^2\} = \{x^3, x\} \\ yN &= y\{1, x^2\} = \{y, yx^2\} \\ yxN &= yx\{1, x^2\} = \{yx, yx^3\} \\ yx^2N &= yx^2\{1, x^2\} = \{yx^2, y\} \\ yx^3N &= yx^3\{1, x^2\} = \{yx^3, yx\} \end{aligned}$$

### RIGHT COSETS

$$\begin{aligned} N1 &= \{1, x^2\}1 = \{1, x^2\} \\ Nx &= \{1, x^2\}x = \{x, x^3\} \\ Nx^2 &= \{1, x^2\}x^2 = \{x^2, 1\} \\ Nx^3 &= \{1, x^2\}x^3 = \{x^3, x\} \\ Ny &= \{1, x^2\}y = \{y, x^2y\} = \{y, yx^2\}^{*1} \\ Nyx &= \{1, x^2\}yx = \{yx, x^2yx\} = \{yx, yx^3\}^{*2} \\ Nyx^2 &= \{1, x^2\}yx^2 = \{yx^2, x^2yx^2\} = \{yx^2, y\}^{*3} \\ Nyx^3 &= \{1, x^2\}yx^3 = \{yx^3, x^2yx^3\} = \{yx^3, yx\}^{*4} \end{aligned}$$

\*1:  $x^2y = x(xy^{-1})y^2 = x(yx)y^2 = (xy^{-1})y^2xy^2 = (yx)y^2xy^2 = yxx^2xx^2 = yx^6 = yx^2$ .

\*2:  $x^2yx = (x^2y)x = (by^{*1}) = (yx^2)x = yx^3$ .

\*3:  $x^2yx^2 = (x^2y)x^2 = (by^{*1}) = (yx^2)x^2 = yx^4 = y$ .

\*4:  $x^2yx^3 = (x^2y)x^3 = (by^{*1}) = (yx^2)x^3 = yx^5 = yx$ .

As in each case the left coset is *equal* to the right coset, then we can say that the subgroup  $N$  is a **normal** subgroup. To finish the question, we must calculate the multiplication table for  $G/N$ , i.e. for the cosets. From the calculations on the previous page, we see that there are four cosets, namely

$$E = \{1, x^2\}, A = \{x, x^3\}, B = \{y, yx^2\}, \text{ and } C = \{yx, yx^3\}.$$

We can use the calculations done on the previous page to work out what the table should look like: (to get the product of two cosets, we take a coset representative from the first coset and multiply it with the elements in the second coset to get a third coset, the product coset we are looking for.)

$$1E = E, 1A = A, 1B = B, \text{ and } 1C = C;$$

$$xE = A, xA = E, \quad xB = x\{y, yx^2\} = \{xy, xyx^2\} = \{(xy^{-1})y^2, (xy^{-1})y^2x^2\} = \{xyx^2, yxy^2x^2\} \\ = \{yx^3, yx\} = C, \text{ and } xC = x\{yx, yx^3\} = \{yx^2, y\} = B;$$

$$yE = B, yA = C, yB = E, \text{ and } yC = A;$$

$$yxE = C, yxA = B, yxB = yx\{y, yx^2\} = \{yxy, (yxy)x^2\} = \{x, x^3\} = A, \text{ and } yxC = E.$$

*Conclusion:* The multiplication table is as shown on the right.

	E	A	B	C
E	E	A	B	C
A	A	E	C	B
B	B	C	E	A
C	C	B	A	E

**7-4:** Let  $G$  be the dihedral group  $D(4)$ :

$$G = \langle b, a : b^2 = 1 = a^4 \text{ and } ab = ba^{-1} \rangle,$$

and let  $H$  be the subset  $\{1, b\}$ . Prove that  $H$  is **not** a normal subgroup of  $G$ . Show that multiplication of the left cosets of  $H$  in  $G$  is **not** well-defined: there are elements  $x, y, u$  and  $v$  with  $xH = uH$ ,  $yH = vH$ , but  $xyH \neq uvH$ .

**Answer:** To prove that  $H$  is not a normal subgroup of  $G$ , all we must do is to find an element  $g \in G$  such that  $gH \neq Hg$ . Consider the element  $ba \in G$ . Then

$$baH = ba\{1, b\} = \{ba, bab\} = \{ba, b^2a^{-1}\} = \{ba, a^3\}; \\ \text{and } Hba = \{1, b\}ba = \{ba, b^2a\} = \{ba, a\}.$$

As  $baH \neq Hba$ , we conclude that  $H$  is *not* a normal subgroup of  $G$ .

$$\text{Now consider the coset } aH = a\{1, b\} = \{a, ab\} = \{a, ba^{-1}\} = \{a, ba^3\} = ba^3H.$$

$$\text{We also know that } baH = \{ba, a^3\} = a^2H.$$

Following the notation in the question, we therefore let  $x = ba$ ,  $u = a^2$ ,  $y = a$ , and  $v = ba^3$ .

Knowing that  $xH = uH$ , and knowing that  $yH = vH$ , we must now show that  $xyH \neq uvH$  in order to complete the question.

$$\begin{aligned} \text{LHS} &= xyH = (ba)(a)H = ba^2H = ba^2\{1, b\} = \{ba^2, ba^2b\} = \{ba^2, baab\} = \{ba^2, baba^{-1}\} \\ &= \{ba^2, b^2a^{-2}\} = \{ba^2, a^{-2}\} = \{ba^2, a^2\}; \end{aligned}$$

$$\begin{aligned} \text{RHS} &= uvH = (a^2)(ba^3)H = a^2ba^3H = a^2ba^3\{1, b\} = aabaaa\{1, b\} = aba^{-1}aaa\{1, b\} \\ &= ba^{-1}aa\{1, b\} = ba\{1, b\} = \{ba, bab\} = \{ba, b^2a^{-1}\} = \{ba, a^{-1}\} = \{ba, a^3\}. \end{aligned}$$

As  $\text{LHS} \neq \text{RHS}$ , or  $xyH \neq uvH$ , we have shown that the multiplication of the left cosets of  $H$  in  $G$  is **not** well-defined. QED.

## Chapter 8: The Homomorphism Theorem: Exercises

**8-2:** Let  $G$  be the dihedral group  $D(3)$ . Define a map  $\nu: G \rightarrow \{1, -1\}$  by  $\nu(g) = 1$  if  $g$  is a *rotation*, and  $\nu(g) = -1$  if  $g$  is a *reflection*. Prove that  $\nu$  is a *homomorphism*, and calculate its **kernel** and **image**.

**Answer:** Recall that the dihedral group  $D(3)$  has presentation  $D(3) = \langle a, b: b^2 = 1 = a^3, ab = ba^{-1} \rangle$ , and that it has elements  $1, a, a^2, b, ba$  and  $ba^2$ , where the element ‘ $a$ ’ corresponds to an *anticlockwise rotation through  $120^\circ$* , and the element ‘ $b$ ’ corresponds to a *reflection in the vertical axis*.

Using this information, we see that the elements ‘ $a$ ’ and ‘ $a^2$ ’ are *rotations*, while the elements ‘ $b$ ’, ‘ $ba$ ’ and ‘ $ba^2$ ’ are *reflections*. To prove that  $\nu$  is a homomorphism, we must show that  $\nu(xy) = \nu(x)\nu(y)$  for all possible  $x$  and  $y$  in  $D(3)$ . Note that in the following, we invoke Corollary 8.7 ( $\phi(1_G) = 1_H$ ) to define  $\nu(g)$  for  $g = 1$ : we have  $\nu(1_{D(3)}) = 1_{\{1, -1\}} = 1$ .

$x = 1$ :

$$\begin{aligned} y = 1: & \quad \nu(1 \times 1) = \nu(1) = 1 = 1 \times 1 = \nu(1)\nu(1) \\ y = a: & \quad \nu(1 \times a) = \nu(a) = 1 = 1 \times 1 = \nu(1)\nu(a) \\ y = a^2: & \quad \nu(1 \times a^2) = \nu(a^2) = 1 = 1 \times 1 = \nu(1)\nu(a^2) \\ y = b: & \quad \nu(1 \times b) = \nu(b) = -1 = 1 \times -1 = \nu(1)\nu(b) \\ y = ba: & \quad \nu(1 \times ba) = \nu(ba) = -1 = 1 \times -1 = \nu(1)\nu(ba) \\ y = ba^2: & \quad \nu(1 \times ba^2) = \nu(ba^2) = -1 = 1 \times -1 = \nu(1)\nu(ba^2) \end{aligned}$$

$x = a$ :

$$\begin{aligned} y = 1: & \quad \nu(a \times 1) = \nu(a) = 1 = 1 \times 1 = \nu(a)\nu(1) \\ y = a: & \quad \nu(a \times a) = \nu(a^2) = 1 = 1 \times 1 = \nu(a)\nu(a) \\ y = a^2: & \quad \nu(a \times a^2) = \nu(1) = 1 = 1 \times 1 = \nu(a)\nu(a^2) \\ y = b: & \quad \nu(a \times b) = \nu(ab) = \nu(ba^{-1}) = \nu(ba^2) = -1 = 1 \times -1 = \nu(a)\nu(b) \\ y = ba: & \quad \nu(a \times ba) = \nu(aba) = \nu(ba^{-1}a) = \nu(b) = -1 = 1 \times -1 = \nu(a)\nu(ba) \\ y = ba^2: & \quad \nu(a \times ba^2) = \nu(aba^2) = \nu(ba^{-1}a^2) = \nu(ba) = -1 = 1 \times -1 = \nu(a)\nu(ba^2) \end{aligned}$$

$x = a^2$ :

$$\begin{aligned}y = 1: & \quad \nu(a^2 \times 1) = \nu(a^2) = 1 = 1 \times 1 = \nu(a^2)\nu(1) \\y = a: & \quad \nu(a^2 \times a) = \nu(1) = 1 = 1 \times 1 = \nu(a^2)\nu(a) \\y = a^2: & \quad \nu(a^2 \times a^2) = \nu(a) = 1 = 1 \times 1 = \nu(a^2)\nu(a^2) \\y = b: & \quad \nu(a^2 \times b) = \nu(a^2 b) = \nu(aba^{-1}) = \nu(ba^{-2}) = \nu(ba) = -1 = 1 \times -1 = \nu(a^2)\nu(b) \\y = ba: & \quad \nu(a^2 \times ba) = \nu(a^2 ba) = \nu(ba^{-2}a) = \nu(ba^2) = -1 = 1 \times -1 = \nu(a^2)\nu(ba) \\y = ba^2: & \quad \nu(a^2 \times ba^2) = \nu(a^2 ba^2) = \nu(ba^{-2}a^2) = \nu(b) = -1 = 1 \times -1 = \nu(a^2)\nu(ba^2)\end{aligned}$$

$x = b$ :

$$\begin{aligned}y = 1: & \quad \nu(b \times 1) = \nu(b) = -1 = -1 \times 1 = \nu(b)\nu(1) \\y = a: & \quad \nu(b \times a) = \nu(ba) = -1 = -1 \times 1 = \nu(b)\nu(a) \\y = a^2: & \quad \nu(b \times a^2) = \nu(ba^2) = -1 = -1 \times 1 = \nu(b)\nu(a^2) \\y = b: & \quad \nu(b \times b) = \nu(1) = 1 = -1 \times -1 = \nu(b)\nu(b) \\y = ba: & \quad \nu(b \times ba) = \nu(a) = 1 = -1 \times -1 = \nu(b)\nu(ba) \\y = ba^2: & \quad \nu(b \times ba^2) = \nu(a^2) = 1 = -1 \times -1 = \nu(b)\nu(ba^2)\end{aligned}$$

$x = ba$ :

$$\begin{aligned}y = 1: & \quad \nu(ba \times 1) = \nu(ba) = -1 = -1 \times 1 = \nu(ba)\nu(1) \\y = a: & \quad \nu(ba \times a) = \nu(ba^2) = -1 = -1 \times 1 = \nu(ba)\nu(a) \\y = a^2: & \quad \nu(ba \times a^2) = \nu(b) = -1 = -1 \times 1 = \nu(ba)\nu(a^2) \\y = b: & \quad \nu(ba \times b) = \nu(bab) = \nu(b^2 a^{-1}) = \nu(a^2) = 1 = -1 \times -1 = \nu(ba)\nu(b) \\y = ba: & \quad \nu(ba \times ba) = \nu(baba) = \nu(b^2 a^{-1} a) = \nu(1) = 1 = -1 \times -1 = \nu(ba)\nu(ba) \\y = ba^2: & \quad \nu(ba \times ba^2) = \nu(baba^2) = \nu(b^2 a^{-1} a^2) = \nu(a) = 1 = -1 \times -1 = \nu(ba)\nu(ba^2)\end{aligned}$$

$x = ba^2$ :

$$\begin{aligned}y = 1: & \quad \nu(ba^2 \times 1) = \nu(ba^2) = -1 = -1 \times 1 = \nu(ba^2)\nu(1) \\y = a: & \quad \nu(ba^2 \times a) = \nu(b) = -1 = -1 \times 1 = \nu(ba^2)\nu(a) \\y = a^2: & \quad \nu(ba^2 \times a^2) = \nu(ba) = -1 = -1 \times 1 = \nu(ba^2)\nu(a^2) \\y = b: & \quad \nu(ba^2 \times b) = \nu(ba^2 b) = \nu(baba^{-1}) = \nu(b^2 a^{-2}) = \nu(a) = 1 = -1 \times -1 = \nu(ba^2)\nu(b) \\y = ba: & \quad \nu(ba^2 \times ba) = \nu(ba^2 ba) = \nu(a^2) = 1 = -1 \times -1 = \nu(ba^2)\nu(ba) \\y = ba^2: & \quad \nu(ba^2 \times ba^2) = \nu(ba^2 ba^2) = \nu(1) = 1 = -1 \times -1 = \nu(ba^2)\nu(ba^2)\end{aligned}$$

We have now shown (by exhaustive search!) that  $\nu(xy) = \nu(x)\nu(y)$  is true for all possible combinations of  $x$  and  $y$  in  $D(3)$ , and so  $\nu$  must be a homomorphism. QED. The *kernel* of  $\nu$  consists of the elements of  $D(3)$  that map onto  $1 \in \{1, -1\}$ . By the definition of  $\nu$ , and because  $\nu(1_{D(3)}) = 1_{\{1, -1\}}$ , we see that the kernel of  $\nu$  must be the set  $\{1, a, a^2\}$ .

As the set  $\text{Im } \nu$  is the set of elements of  $\{1, -1\}$  which are images of elements of  $D(3)$  under  $\nu$ , then because (e.g.)  $\nu(a) = 1$ , and because (e.g.)  $\nu(b) = -1$ , then  $\text{Im } \nu = \{1, -1\}$ .

**8-5:** Determine the elements of  $\text{Aut}(G)$  when  $G$  is the cyclic group  $C_3$  consisting of the three complex cube roots of unity, namely  $1, \omega$  and  $\omega^2$ , where  $\omega = e^{2\pi i/3}$ . Write down the multiplication table for  $\text{Aut}(G)$ .

**Answer:** Consider that we are trying to *construct* an automorphism  $\varphi: C_3 \rightarrow C_3$ . Because  $\varphi$  must be a homomorphism, then we must have  $\varphi(1_{C_3}) = 1_{C_3}$ . It follows that because  $\varphi$  must be a *surjective* map, then we cannot have  $\varphi(x) = 1$  for any  $x \in C_3$  other than for  $x = 1$ . This leaves us **two** choices for  $\varphi(\omega)$ :  $\varphi(\omega) = \omega$ , or  $\varphi(\omega) = \omega^2$ . Again because  $\varphi$  must be a *surjective* map, then if  $\varphi(\omega) = \omega$ , then we must have  $\varphi(\omega^2) = \omega^2$ . Similarly, if  $\varphi(\omega) = \omega^2$ , then we must have  $\varphi(\omega^2) = \omega$ .

In summary, we have found **two** possible automorphisms:

$\alpha: C_3 \rightarrow C_3$  defined by  $\alpha(1) = 1, \alpha(\omega) = \omega$  and  $\alpha(\omega^2) = \omega^2$ ;

$\beta: C_3 \rightarrow C_3$  defined by  $\beta(1) = 1, \beta(\omega) = \omega^2$  and  $\beta(\omega^2) = \omega$ .

As we have ensured that  $\alpha$  and  $\beta$  are surjective maps, it remains to check that  $\alpha(xy) = \alpha(x)\alpha(y)$  for all  $x, y \in C_3$ ; and that  $\beta(uv) = \beta(u)\beta(v)$  for all  $u, v \in C_3$ . I will do the calculations for  $\alpha$  — the calculations for  $\beta$  will be *similar*.

$$\begin{aligned} x = 1: \quad & y = 1: \alpha(1 \times 1) = \alpha(1) = 1 = 1 \times 1 = \alpha(1)\alpha(1) \\ & y = \omega: \alpha(1 \times \omega) = \alpha(\omega) = \omega = 1 \times \omega = \alpha(1)\alpha(\omega) \\ & y = \omega^2: \alpha(1 \times \omega^2) = \alpha(\omega^2) = \omega^2 = 1 \times \omega^2 = \alpha(1)\alpha(\omega^2) \end{aligned}$$

$$\begin{aligned} x = \omega: \quad & y = 1: \alpha(\omega \times 1) = \alpha(\omega) = \omega = \omega \times 1 = \alpha(\omega)\alpha(1) \\ & y = \omega: \alpha(\omega \times \omega) = \alpha(\omega^2) = \omega^2 = \omega \times \omega = \alpha(\omega)\alpha(\omega) \\ & y = \omega^2: \alpha(\omega \times \omega^2) = \alpha(1) = 1 = \omega \times \omega^2 = \alpha(\omega)\alpha(\omega^2) \end{aligned}$$

$$\begin{aligned} x = \omega^2: \quad & y = 1: \alpha(\omega^2 \times 1) = \alpha(\omega^2) = \omega^2 = \omega^2 \times 1 = \alpha(\omega^2)\alpha(1) \\ & y = \omega: \alpha(\omega^2 \times \omega) = \alpha(1) = 1 = \omega^2 \times \omega = \alpha(\omega^2)\alpha(\omega) \\ & y = \omega^2: \alpha(\omega^2 \times \omega^2) = \alpha(\omega) = \omega = \omega^2 \times \omega^2 = \alpha(\omega^2)\alpha(\omega^2) \end{aligned}$$

To get the multiplication table for  $\text{Aut}(C_3)$ , we must consider all composition maps involving  $\alpha$  and  $\beta$ :

x	$\alpha\alpha(x)$	$\alpha\beta(x)$	$\beta\alpha(x)$	$\beta\beta(x)$
1	1	1	1	1
$\omega$	$\omega$	$\omega^2$	$\omega^2$	$\omega$
$\omega^2$	$\omega^2$	$\omega$	$\omega$	$\omega^2$

Thus the multiplication table for  $\text{Aut}(C_3)$  is as shown on the right.

	$\alpha$	$\beta$
$\alpha$	$\alpha$	$\beta$
$\beta$	$\beta$	$\alpha$

# Chapter 10: The Orbit-Stabiliser Theorem

## Key Definitions and Results

**Definition 10.1:** A  $G$ -set is a set  $X$  together with a rule assigning to each element  $g$  of  $G$  and each element  $x$  of  $X$ , an element  $g \bullet x$  of  $X$  satisfying (G-set 1) for all  $x$  in  $X$ ,  $1_G \bullet x = x$ ; (G-set 2) for all  $g_1$  and  $g_2$  in  $G$  and all  $x$  in  $X$ ,  $(g_1 g_2) \bullet x = g_1 \bullet (g_2 \bullet x)$ .

**Definition 10.8:** Given a  $G$ -set  $X$ , and an element  $x$  of  $X$ , the *stabiliser*  $G_x$  is the set of group elements which fix  $x$ :  $G_x = \{g \in G: g \bullet x = x\}$ . The stabiliser is a *subgroup* of  $G$ .

A way to *change*  $G$  into a  $G$ -set is to define  $g \bullet x$  to be  $g x g^{-1}$ . In this situation, the stabiliser is more commonly known as the *centraliser*  $C_G(x)$ , so that  $C_G(x) = \{g \in G: g x g^{-1} = x\}$ .

There is a *conjugation* action of  $G$  on the set of all subgroups of  $G$ . In this case,  $x \bullet H$  is defined to be  $x H x^{-1}$ . In this situation, the stabiliser of  $H$  is known as the **normaliser**  $N_G(H)$ , the set  $\{g \in G: g H g^{-1} = H\}$ . Note that  $N_G(H)$  always contains  $H$  and that  $H$  is a *normal subgroup* iff  $N_G(H) = G$ .

**Definition 10.12:** Given a  $G$ -set  $X$ , define an *equivalence relation*  $R$  on  $X$  by  $x R y$  iff there exists an element  $g$  in  $G$  with  $y = g \bullet x$ . The *equivalence class* of  $x \in X$  under  $R$  is known as the *orbit* of  $x$ , and is given by  $\text{orb}(x) = \{g \bullet x: g \in G\}$ .

**Theorem 10.16:** The Orbit-Stabiliser Theorem: Let  $G$  be a group and  $X$  be a  $G$ -set. For each  $x$  in  $X$ ,  $|\text{orb}(x)| = |G : G_x|$ . Note that the Orbit-Stabiliser Theorem gives the number of elements in a conjugacy class, namely  $|G|/|C_G(x)|$ .

- The identity element always forms a conjugacy class by *itself*.
- Conjugate elements have the same *order*.
- Let  $H$  be a subgroup of the group  $G$ . Then, for any  $x$  in  $G$ ,  $C_H(x) = C_G(x) \cap H$ .

For any group  $G$ , the centre of  $G$ ,  $Z(G)$ , is given by  $Z(G) = \{z \in G: z x = x z \text{ for all } x \in G\}$ . **Proposition 10.20:** Let  $p$  be a prime integer and let  $G$  be a finite group with  $p^n$  elements. Then  $Z(G)$  contains **more** than one element. **Proposition 10.21:** Let  $G$  be a group such that  $G/Z(G)$  is cyclic. Then  $G$  is abelian, so that  $G = Z(G)$ .

**Corollary 10.22:** Let  $p$  be a prime integer. Any group with  $p^2$  elements is *abelian*.

**Corollary 10.23:** A group with  $p^2$  elements is either *cyclic* or *isomorphic* to the direct product  $C_p \times C_p$ .

**Definition 10.24:** For any subgroup  $H$  of a group  $G$ , define the *centraliser* of  $H$  in  $G$  by  $C_G(H) = \{g \in G: g h g^{-1} = h \text{ for all } h \text{ in } H\}$ . **Proposition 10.25:** Let  $H$  be a subgroup of a group  $G$ . Then for all elements  $g$  in  $G$ ,  $C_H(x) = C_G(x) \cap H$ . **Proposition 10.26:** Let  $H$  be a subgroup of the group  $G$ . Then  $C_G(H)$  is a normal subgroup of the group  $N_G(H)$  and  $N_G(H)/C_G(H)$  is *isomorphic* to a *subgroup* of  $\text{Aut}(H)$ .

## Exercises

**10-2:** Let  $X$  be a  $G$ -set and let  $x \in X$ . Show that for any  $g \in G$ , the stabiliser of  $g \bullet x$  is the subgroup  $gG_xg^{-1}$ .

**Answer:** By definition 10.8, the *stabiliser* of  $g \bullet x$  is the set of group elements which fix  $g \bullet x$ :

$$\begin{aligned} G_{g \bullet x} &= \{h \in G: h \bullet (g \bullet x) = g \bullet x\} \\ &= \{h \in G: hg \bullet x = g \bullet x\} && \text{(by (G-set 2))} \\ &= \{h \in G: g^{-1}hg \bullet x = 1_G \bullet x\} && \text{(by multiplying on the left by } g^{-1}\text{)} \\ &= \{h \in G: g^{-1}hg \bullet x = x\} && \text{(by (G-set 1))} \\ &= \{h \in G: g^{-1}hg \in G_x\} && \text{(by the definition of } G_x, G_x = \{g \in G: g \bullet x = x\}\text{)} \\ &= \{h \in G: hg \in gG_x\} && \text{(by multiplying on the left by } g\text{)} \\ &= \{h \in G: h \in gG_xg^{-1}\} && \text{(by multiplying on the right by } g^{-1}\text{)} \\ &= gG_xg^{-1}. \quad \mathbf{QED.} \end{aligned}$$

**10-5:** Let  $G$  be a finite group with precisely **two** conjugacy classes. Prove that  $G$  has **two elements**.

**Answer:** Assume that  $|G| = n$ . Knowing that  $G$  has **exactly** two conjugacy classes, this enables us to say that  $n \geq 2$  (each conjugacy class has at least one element). From the first bullet point on the previous page, we know that the *identity element* always forms a conjugacy class by itself. Therefore, in this situation, we know that all the other **non-identity** elements of  $G$  will form the *other* conjugacy class. Note that there are a total of  $(n-1)$  non-identity elements in all.

Now we know that the Orbit-Stabiliser Theorem gives us the *number of elements* in a conjugacy class, namely  $|G|/|C_G(x)|$ . Therefore, we must have  $(n-1) = |G|/|C_G(x)|$  ( $x \notin 1_G$ ). As  $C_G(x)$  is a subgroup of  $G$ , then, by Lagrange's Theorem, its order must **divide** the **order** of the group, so that we have

$$\begin{aligned} (n-1)k &= |G| \text{ for some integer } k > 0; \text{ or} \\ (n-1)k &= n \text{ for some integer } k > 0 \text{ (as we have assumed that } |G| = n\text{);} \\ nk - k &= n; \\ n(k-1) &= k; \\ n &= k/(k-1). \end{aligned}$$

As  $n$  is an **integer**, the only assignment for  $k$  that will make the right hand side of the above equation an **integer** is the assignment  $k = 2$ , so that

$$n = 2/(2-1) = 2/1 = 2.$$

Conclusion:  $G$  has only two elements. **QED.**

# Chapter 11: The Sylow Theorems

## Key Definitions and Results

**Definition 11.1:** Let  $p$  be a *prime number*, let  $n$  be a *positive integer*, and let  $k$  be an integer *not divisible* by  $p$ . Let  $G$  be a finite group with  $p^n k$  elements. A Sylow  $p$ -subgroup is a subgroup of  $G$  with  $p^n$  elements.

**Theorem 11.4** (*The First Sylow Theorem*): Let  $p$  be a prime and let  $G$  be a finite group of order  $kp^n$ , where  $p$  does *not* divide  $k$ . Then  $G$  has **at least one** Sylow  $p$ -subgroup.

**Theorem 11.6** (*The Second Sylow Theorem*): The number of Sylow  $p$ -subgroups in a finite group  $G$  is *congruent* to 1 modulo  $p$  (i.e. the number,  $n_p$ , of these subgroups is of the form  $1+tp$  for some integer  $t$ ).

**Definition 11.8:** Let  $p$  be a prime integer. A  **$p$ -group** is a group in which every element has order a *power* of  $p$ . If  $G$  is a finite  $p$ -group, the First Sylow Theorem shows that the number of elements in  $G$  must be a *power* of  $p$ . Conversely, by Corollary 5.12 in the book, any finite group whose order is a power of  $p$  is a  $p$ -group.

**Proposition 11.9:** Let  $P$  be a Sylow  $p$ -subgroup of a finite group  $G$ . Any  $p$ -subgroup of  $N_G(P)$  is contained in  $P$  and, in particular,  $P$  is the *unique* Sylow  $p$ -subgroup of  $N_G(P)$ .

**Theorem 11.10** (*The Third Sylow Theorem*): If  $P$  is a Sylow  $p$ -subgroup of the finite group  $G$ , and if  $Q$  is any  $p$ -subgroup of  $G$ , then  $Q$  is contained in a *conjugate* of  $P$  (i.e.  $Q \subseteq gPg^{-1}$  for some  $g \in G$ ).

**Corollary 11.11** (*The Fourth Sylow Theorem*): Any Sylow  $p$ -subgroups of a finite group  $G$  are *conjugate*, so that the number of Sylow  $p$ -subgroups divides  $|G|$ .

**Remark:** If  $G$  has precisely **one** Sylow subgroup, then this subgroup is **normal**. Conversely, if a Sylow  $p$ -subgroup is **normal**, then, using Corollary 11.11, we see that there can only be **one** Sylow  $p$ -subgroup.

**Proposition 11.14:** Let  $G$  be a finite group. Let  $P$  be a Sylow  $p$ -subgroup of  $G$  and let  $N$  be a normal subgroup of  $G$ . Then (i)  $P \cap N$  is a Sylow  $p$ -subgroup of  $N$ ; and (ii)  $PN/N$  is a Sylow  $p$ -subgroup of  $G/N$ . Note that in order to show that a subgroup  $H$  of a group  $G$  is a Sylow  $p$ -subgroup of  $G$ , we can check that  $H$  is a  *$p$ -subgroup* and that the *index* of  $H$  in  $G$  is *not* divisible by  $p$ .

## Exercises

**11-1:** What (if anything) do the Sylow Theorems enable one to deduce about the number of Sylow  $p$ -subgroups in the following cases:

- |                        |                        |
|------------------------|------------------------|
| (a) $p = 7;  G  = 28;$ | (d) $p = 2;  G  = 12;$ |
| (b) $p = 2;  G  = 48;$ | (e) $p = 3;  G  = 12.$ |
| (c) $p = 2;  G  = 32;$ |                        |

**Answer:** (a)  $28 = 4 \times 7$ . The **First** Sylow Theorem says that there is at least one Sylow 7-subgroup. The **Second** Sylow Theorem says that the number of Sylow 7-subgroups in  $G$  is *congruent* to 1 modulo 7 (i.e.  $n_7 = 1, 8, 15, 22, 29, \dots$ ). The **Fourth** Sylow Theorem says that  $n_7$  divides 28, i.e.  $n_7 = 1, 4, 7$  or 28. Using the information from the Second and Fourth Sylow Theorems enables us to say that  $n_7 = 1$ .

- (b)  $48 = 2 \times 2 \times 2 \times 2 \times 3 = 2^4 \times 3$ .  
2nd Sylow Theorem  $\Rightarrow n_2 = 1, 3, 5, 7, 9, 11, 13, 15, 17, \dots$   
4th Sylow Theorem  $\Rightarrow n_2 = 1, 2, 3, 4, 6, 8, 12, 24$ .  
Conclusion:  $n_2 = 1$  or 3.
- (c)  $32 = 2 \times 2 \times 2 \times 2 \times 2 = 2^5$ .  
2nd Sylow Theorem  $\Rightarrow n_2 = 1, 3, 5, 7, 9, 11, 13, 15, 17, \dots$   
4th Sylow Theorem  $\Rightarrow n_2 = 1, 2$ .  
Conclusion:  $n_2 = 1$ .  
Note:  $G$  is a 2-group so that Sylow's Theorems tell us nothing new.
- (d)  $12 = 2 \times 2 \times 3 = 2^2 \times 3$ .  
2nd Sylow Theorem  $\Rightarrow n_2 = 1, 3, 5, 7, 9, 11, 13, 15, 17, \dots$   
4th Sylow Theorem  $\Rightarrow n_2 = 1, 2, 3, 4, 6, 12$ .  
Conclusion:  $n_2 = 1$  or 3.
- (e)  $12 = 2 \times 2 \times 3 = 2^2 \times 3$ .  
2nd Sylow Theorem  $\Rightarrow n_3 = 1, 4, 7, 10, 13, \dots$   
4th Sylow Theorem  $\Rightarrow n_3 = 1, 2, 3, 4, 6, 12$ .  
Conclusion:  $n_3 = 1$  or 4.

**11-3:** Give an example of a group  $G$  with a Sylow  $p$ -subgroup  $P$  and a subgroup  $H$  such that  $P \cap H$  is *not* a Sylow  $p$ -subgroup of  $H$ .

**Answer:** Consider the group  $G = D_3 = \langle a, b: b^2 = 1 = a^3, ab = ba^{-1} \rangle$ , with elements  $1, a, a^2, b, ba$  and  $ba^2$ . As  $|G| = 6 = 2 \times 3$ , and letting  $p = 2$ , we know that we can find a Sylow 2-subgroup of  $G$ , namely  $P = \langle b \rangle = \{1, b\}$ . But if we now let  $H = \{1, a, a^2\}$ , which is clearly a subgroup of  $G$ , we find that  $P \cap H = \{1\}$ , which is not a Sylow 2-subgroup of  $H$ . QED.

# Chapter 12: Applications of Sylow Theory

## Key Definitions and Results

**Proposition 12.1:** Let  $p$  and  $q$  be primes with  $p > q$ . A group of order  $pq$  has a *normal Sylow  $p$ -subgroup*.

**Proposition 12.2:** Let  $x, y$  be elements of a group  $G$  such that  $xy = yx$ . Then, for all integers  $k$ ,  $(xy)^k = x^k y^k$ .

**Proposition 12.4:** If  $p$  and  $q$  are distinct primes, then a group of order  $p^2q$  has a *normal Sylow subgroup*.

## Exercises

**12-3:** Show that a group with *56 elements* either has a *unique Sylow 2-subgroup* or has a *unique Sylow 7-subgroup*.

**Answer:** As  $56 = 2 \times 2 \times 2 \times 7 = 2^3 \times 7$ , then a group  $G$  with 56 elements has *at least one* Sylow 2-subgroup and *at least one* Sylow 7-subgroup due to Sylow's First Theorem. Using the techniques of the previous set of exercises, the number of Sylow 2-subgroups *divides 56* (so is one of 1, 2, 4, 7, 8, 14 and 28), and is equal to *1 modulo 2* (so is one of 1, 3, 5, 7, ...), so is either 1 or 7. Similarly, the number of Sylow 7-subgroups *divides 56* (so is one of 1, 2, 4, 7, 8, 14 and 28), and is equal to *1 modulo 7* (so is one of 1, 8, 15, 22, ...), so is either 1 or 8.

If the number of Sylow 7-subgroups is 1, then we *automatically* have a unique Sylow 7-subgroup. It remains to show that if the number of Sylow 7-subgroups is 8, then we have a *unique Sylow 2-subgroup*. Consider that the 8 distinct Sylow 7-subgroups are labelled as  $S_1, S_2, \dots, S_8$ .

If  $i$  is different from  $j$  ( $i, j = 1, \dots, 8$ ), then  $S_i \cap S_j$  will be a subgroup of  $S_i$ , which itself is a subgroup of order 7. By Lagrange's Theorem, the subgroup  $S_i \cap S_j$  will have order dividing the order of  $S_i$ , which is 7, so that the order of  $S_i \cap S_j$  will be *either 1 or 7*. But as the Sylow 7-subgroups are **distinct**, then we cannot have  $S_i \cap S_j = S_i$ , and so we must have  $S_i \cap S_j = \{1\}$ .

It follows that because all the subgroup  $S_i$  share one common element (the identity element), then the eight Sylow 7-subgroups will contain a total of  $8 \times 6 = 48$  distinct non-identity elements. This leaves a total of  $56 - 1 - 48 = 7$  non-identity elements *unaccounted for*.

Now remember that as  $56 = 2^3 \times 7$ , a Sylow 2-subgroup will have 8 elements. We know that there **will** be at least one Sylow 2-subgroup in  $G$  due to Sylow's First Theorem, but what will they consist of? Well, if we take the identity element together with the 7 non-identity elements unaccounted for, these eight elements could form a Sylow 2-subgroup. In fact, this is the **only** possibility for a Sylow 2-subgroup, as all the other elements belong to Sylow 7-subgroups. It follows that there can only be **one** Sylow 2-subgroup. QED.

# Chapter 13: Direct Products

## Key Definitions and Results

Recall that, given a *pair* of groups  $G$  and  $H$ , the *direct product*  $G \times H$  is the set of ordered pairs  $(g, h)$  with  $g \in G$  and  $h \in H$  under the multiplication  $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$ .

**Proposition 13.1:** Let  $G$  and  $H$  be any groups. Then (1)  $G \times H$  is *abelian* if and only if both  $G$  and  $H$  are abelian; (2)  $G \times H$  is *isomorphic* to  $H \times G$ ; and (3) if  $G$  and  $H$  are both *cyclic finite groups* and their *orders* have no common divisor greater than 1, then  $G \times H$  is *cyclic*.

**Corollary 13.2:** Let  $n_1, n_2, \dots, n_s$  be any sequence of integers each of which is *greater* than 1, such that the *greatest common divisor* of any distinct pair  $n_i, n_j$  is 1. Let  $G_i$  be a cyclic group of order  $n_i$  ( $1 \leq i \leq s$ ). Then the group  $G_1 \times G_2 \times \dots \times G_s$  is cyclic of order  $n_1n_2 \dots n_s$ .

**Definition 13.3:** Let  $\{G_i: i = 1, \dots, n\}$  be *subgroups* of  $G$ . Then  $G$  is the *internal direct product* of  $\{G_i: i = 1, \dots, n\}$  if (1) each  $G_i$  is a *normal subgroup* of  $G$ ; and (2) every element of  $G$  can be written *uniquely* in the form  $g = g_1g_2 \dots g_n$ , with  $g_i \in G_i$  ( $1 \leq i \leq n$ ).

**Proposition 13.5:** Let  $G_1, G_2, \dots, G_n$  be normal subgroups of  $G$  such that (a)  $(G_1 \dots G_{i-1}) \cap G_i = \{1\}$  ( $i = 2, \dots, n$ ); and (2)  $G = G_1G_2 \dots G_n$ . Then  $G$  is the *internal direct product* of the groups  $G_1, G_2, \dots, G_n$ .

**Corollary 13.6:** Let  $G$  be an *internal direct product* of  $G_1, G_2, \dots, G_n$ . If  $x$  and  $y$  are elements of  $G_i$  and  $G_j$  respectively, with  $i \neq j$ , then  $xy = yx$ .

**Proposition 13.7:** Suppose that  $G$  is the *external direct product* of groups  $G_1, G_2, \dots, G_n$ . Then there are *normal subgroups*  $N_1, N_2, \dots, N_n$  of  $G$  with  $N_i$  *isomorphic* to  $G_i$  (for  $1 \leq i \leq n$ ) such that  $G$  is the *internal direct product* of  $N_1, N_2, \dots, N_n$ . Conversely, if  $G$  is the *internal direct product* of  $N_1, N_2, \dots, N_n$ , then  $G$  is *isomorphic* to the *external direct product* of groups *isomorphic* to  $N_1, N_2, \dots, N_n$ .

**Definition 13.9:** Let  $G$  and  $H$  be groups with  $Z$  a *subgroup* of the centre of  $G$  and let  $W$  be a *subgroup* of the centre of  $H$ . Suppose that there is an *isomorphism*  $\varphi: Z \rightarrow W$ . Using elementary properties of homomorphisms, it may be seen that the set  $X = \{(x, \varphi(x)^{-1}): x \in Z\}$  is a subgroup of the direct product  $G \times H$ . In fact, since  $Z$  and  $W$  are *central*, it is easily seen that  $X$  is a central subgroup of the direct product  $G \times H$ . The *quotient group*  $(G \times H)/X$ , denoted  $G \times_{\varphi} H$ , is the central product of  $G$  and  $H$  via  $\varphi$ .

**Definition 13.11:** Let  $G$  and  $H$  be groups which have *isomorphic quotient groups*, so that there are normal subgroups  $N$  of  $G$  and  $K$  of  $H$  such that there is an isomorphism  $\varphi: G/N \rightarrow H/K$ . The *pullback*  $G \times^{\varphi} H$  of  $G$  and  $H$  via  $\varphi$  is the subset of  $G \times H$  of elements of the form  $(g, h)$ , where  $\varphi(gN) = hK$ . It is easily checked that the pullback is a *subgroup* of  $G \times H$ .

## Exercises

**13-1:** Show that the dihedral group  $D(4)$  is not an internal direct product of any two of its proper subgroups.

**Answer:** Assume that  $D(4)$  is an internal direct product of any two of its proper subgroups, say  $H$  and  $K$ . Because  $D(4)$  has order 8, then Lagrange's Theorem implies that any proper subgroup of  $D(4)$  must have order 2 or 4. Therefore,  $|H| = 2$  or 4 and also  $|K| = 2$  or 4. If both  $H$  and  $K$  have order 2, then there would only be four different elements of the form  $h_i k_j$ , where  $h_i \in H$ ,  $k_j \in K$ , and  $1 \leq i, j \leq 2$ .

According to Definition 13.3, in order for  $D(4)$  to be the direct product of  $H$  and  $K$ , then both  $H$  and  $K$  must be normal in  $D(4)$ , and any element in  $D(4)$  must be able to be written *uniquely* in the form  $g = h_i k_j$ , with  $h_i \in H$  and  $k_j \in K$ . But if there are only **four** different types of elements of the form  $h_i k_j$ , and **eight** elements in  $D(4)$ , then both  $H$  and  $K$  cannot have order 2 (because part (2) of Definition 13.3 would then surely be violated).

In the case that **both**  $H$  and  $K$  have order four, then we would have *sixteen* elements of the form  $h_i k_j$  (where this time  $i$  and  $j$  go from 1 to 4), and so an element of  $D(4)$  would **not** have a **unique** representation of the type  $h_i k_j$  (remember that as each element  $h_i k_j$  is an element of  $D(4)$ , as there are a total of *sixteen* of these elements, and as there are only *eight* elements in  $D(4)$ , then there is bound to be *more than one* way to write down an element of  $D(4)$  in the form  $h_i k_j$ ).

From the above discussion, we conclude that if  $H$  has order 2, then  $K$  must have order 4, and vice-versa. Assume, without loss of generality, that  $|H| = 2$  and that  $|K| = 4$ .  $H$ , being a normal subgroup, will therefore satisfy the condition  $g^{-1}Hg = H$  for all  $g$  in  $D(4)$  (*see Proposition 7.4 at the start of Chapter 7 in the book*).

But as  $H$  consists of the **identity element** plus a **non-identity element**  $\alpha$ , then as we automatically have  $g^{-1}1_H g = 1_H$  for all  $g$  in  $D(4)$ , then in order to satisfy the stated condition, we must have  $g^{-1}\alpha g = \alpha$  for all  $g$  in  $D(4)$ . But this is entirely consistent with the element  $\alpha$  being in the *centre* of  $D(4)$ ,  $Z(D(4))$  ( $\alpha g = g\alpha$  for all  $g$  in  $D(4)$ ). Looking at the answer to question 5 of Exercises 7 at the back of the book, we see that the centre of  $D(4)$  is given by  $Z(D(4)) = \{1, a^2\}$ , where  $D(4)$  has the presentation  $\langle a, b : a^4 = 1 = b^2, ab = ba^{-1} \rangle$ . As we have found in our calculations a non-identity element  $\alpha$  of  $Z(D(4))$ , then we **must** come to the conclusion that  $\alpha = a^2$ , so that  $H$  is equal to the *centre* of  $D(4)$ , i.e.  $H = Z(D(4)) = \{1, a^2\}$ .

Now that we know what  $H$  is, we go on to analyse what  $K$  could consist of. By *exhaustive search*, I worked out that the only subgroups of  $D(4)$  of order 4 are as follows: either  $\{1, a, a^2, a^3\}$ , or  $\{1, a^2, b, ba^2\}$ , or  $\{1, a^2, ba, ba^3\}$ . Now  $K$  could be any one of these subgroups if they are normal, but there is no need to check for normality — in all cases, we have  $H \cap K = \{1, a^2\}$ . Looking at *Proposition 13.5*, we see that in order for  $H$  and  $K$  to form an internal direct product of  $D(4)$ , then we must have  $H \cap K = \{1\}$ . By the above analysis, this is not possible in this situation, so we conclude that  $D(4)$  **cannot be** an internal direct product of any two of its proper subgroups. QED.

**13-5:** Let  $G$  be a cyclic group of order 6 generated by  $x$ , and let  $H$  be the alternating group  $A(4)$ , with  $N$  equal to  $\langle x^3 \rangle$  and  $K$  equal to the subgroup  $\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ . Define a map  $\phi: G/N \rightarrow H/K$  by  $\phi(N) = K$ ;  $\phi(xN) = (1\ 2\ 3)K$ ; and  $\phi(x^2N) = (1\ 3\ 2)K$ . List the elements in the pullback of  $G$  and  $H$  via  $\phi$ .

**Answer:** If  $G$  is a cyclic group of order 6 generated by  $x$ , then  $G = \{1, x, x^2, x^3, x^4, x^5\}$  and  $\langle x^3 \rangle = N = \{1, x^3\}$ . It follows that  $N = 1N = x^3N$ . Similarly, we see that  $K = 1K = (1\ 2)(3\ 4)K = (1\ 3)(2\ 4)K = (1\ 4)(2\ 3)K$ . From this information, and looking at the definition of the isomorphism  $\phi$ , we can find the following elements in the pullback of  $G$  and  $H$  via  $\phi$ :

- |     |                       |  |
|-----|-----------------------|--|
| (1) | $(1, 1)$              | (because $\phi(1N) = \phi(N) = K = 1K$ )               |
| (2) | $(1, (1\ 2)(3\ 4))$   | (because $\phi(1N) = \phi(N) = K = (1\ 2)(3\ 4)K$ )    |
| (3) | $(1, (1\ 3)(2\ 4))$   | (because $\phi(1N) = \phi(N) = K = (1\ 3)(2\ 4)K$ )    |
| (4) | $(1, (1\ 4)(2\ 3))$   | (because $\phi(1N) = \phi(N) = K = (1\ 4)(2\ 3)K$ )    |
| (5) | $(x^3, 1)$            | (because $\phi(x^3N) = \phi(N) = K = 1K$ )             |
| (6) | $(x^3, (1\ 2)(3\ 4))$ | (because $\phi(x^3N) = \phi(N) = K = (1\ 2)(3\ 4)K$ )  |
| (7) | $(x^3, (1\ 3)(2\ 4))$ | (because $\phi(x^3N) = \phi(N) = K = (1\ 3)(2\ 4)K$ )  |
| (8) | $(x^3, (1\ 4)(2\ 3))$ | (because $\phi(x^3N) = \phi(N) = K = (1\ 4)(2\ 3)K$ ). |

Now as  $xN = x\{1, x^3\} = \{x, x^4\}$ , then  $xN = x^4N$ .

Similarly,  $(1\ 2\ 3)K = (1\ 2\ 3)\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$   
 $= \{(1\ 2\ 3), (2\ 4\ 3), (1\ 4\ 2), (1\ 3\ 4)\}$  (composing left to right),

so that  $(1\ 2\ 3)K = (2\ 4\ 3)K = (1\ 4\ 2)K = (1\ 3\ 4)K$ .

We can now find more elements in the pullback of  $G$  and  $H$  via  $\phi$ :

- |      |                    |   |
|------|--------------------|---|
| (9)  | $(x, (1\ 2\ 3))$   | (because $\phi(xN) = (1\ 2\ 3)K$ )                            |
| (10) | $(x, (2\ 4\ 3))$   | (because $\phi(xN) = (1\ 2\ 3)K = (2\ 4\ 3)K$ )               |
| (11) | $(x, (1\ 4\ 2))$   | (because $\phi(xN) = (1\ 2\ 3)K = (1\ 4\ 2)K$ )               |
| (12) | $(x, (1\ 3\ 4))$   | (because $\phi(xN) = (1\ 2\ 3)K = (1\ 3\ 4)K$ )               |
| (13) | $(x^4, (1\ 2\ 3))$ | (because $\phi(x^4N) = \phi(xN) = (1\ 2\ 3)K$ )               |
| (14) | $(x^4, (2\ 4\ 3))$ | (because $\phi(x^4N) = \phi(xN) = (1\ 2\ 3)K = (2\ 4\ 3)K$ )  |
| (15) | $(x^4, (1\ 4\ 2))$ | (because $\phi(x^4N) = \phi(xN) = (1\ 2\ 3)K = (1\ 4\ 2)K$ )  |
| (16) | $(x^4, (1\ 3\ 4))$ | (because $\phi(x^4N) = \phi(xN) = (1\ 2\ 3)K = (1\ 3\ 4)K$ ). |

Finally, as  $x^2N = x^2\{1, x^3\} = \{x^2, x^5\}$ , then  $x^2N = x^5N$ .

Similarly,  $(1\ 3\ 2)K = (1\ 3\ 2)\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$   
 $= \{(1\ 3\ 2), (1\ 4\ 3), (2\ 3\ 4), (1\ 2\ 4)\}$  (composing left to right),

so that  $(1\ 3\ 2)K = (1\ 4\ 3)K = (2\ 3\ 4)K = (1\ 2\ 4)K$ .

We can now find the final batch of elements in the pullback of  $G$  and  $H$  via  $\phi$ :

- |      |                    |   |
|------|--------------------|---|
| (17) | $(x^2, (1\ 3\ 2))$ | (because $\phi(x^2N) = (1\ 3\ 2)K$ )                            |
| (18) | $(x^2, (1\ 4\ 3))$ | (because $\phi(x^2N) = (1\ 3\ 2)K = (1\ 4\ 3)K$ )               |
| (19) | $(x^2, (2\ 3\ 4))$ | (because $\phi(x^2N) = (1\ 3\ 2)K = (2\ 3\ 4)K$ )               |
| (20) | $(x^2, (1\ 2\ 4))$ | (because $\phi(x^2N) = (1\ 3\ 2)K = (1\ 2\ 4)K$ )               |
| (21) | $(x^5, (1\ 3\ 2))$ | (because $\phi(x^5N) = \phi(x^2N) = (1\ 3\ 2)K$ )               |
| (22) | $(x^5, (1\ 4\ 3))$ | (because $\phi(x^5N) = \phi(x^2N) = (1\ 3\ 2)K = (1\ 4\ 3)K$ )  |
| (23) | $(x^5, (2\ 3\ 4))$ | (because $\phi(x^5N) = \phi(x^2N) = (1\ 3\ 2)K = (2\ 3\ 4)K$ )  |
| (24) | $(x^5, (1\ 2\ 4))$ | (because $\phi(x^5N) = \phi(x^2N) = (1\ 3\ 2)K = (1\ 2\ 4)K$ ). |

This concludes our search for elements in the pullback of  $G$  and  $H$  via  $\phi$ .

# Chapter 14: The Classification of Finite Abelian Groups

## Key Definitions and Results

**Proposition 14.2:** Let  $A$  be an *abelian* group, and let  $x$  and  $y$  be elements of  $A$ . Then for any *positive integer*  $k$ ,  $(xy)^k = x^k y^k$ .

**Proposition 14.3:** Let  $G$  be a *finite* group such that, for every prime  $p$  dividing  $|G|$ , the Sylow  $p$ -subgroup of  $G$  is **normal**. Let  $p_1, p_2, \dots, p_r$  be the distinct primes dividing  $|G|$ , and let  $P_i$  be the *Sylow  $p_i$ -subgroup* of  $G$  (for  $1 \leq i \leq r$ ). Then  $G$  is the *internal direct product*  $P_1 \times P_2 \times \dots \times P_r$ . In particular, every *finite abelian group* is the direct product of its *Sylow  $p$ -subgroups*.

**Proposition 14.5:** Let  $G$  be a *finite abelian  $p$ -group* of order  $p^n$ . Then  $G$  is an *internal direct product* of cyclic subgroups of orders  $p^{e_1}, p^{e_2}, \dots, p^{e_r}$ , where  $e_1 \geq e_2 \geq \dots \geq e_r \geq 1$  and  $e_1 + e_2 + \dots + e_r = n$ .

**Corollary 14.7:** A *finite abelian group* of order  $n$  can be written as a **direct product**  $C_{n_1} \times C_{n_2} \times \dots \times C_{n_r}$ , where  $n_i$  is divisible by  $n_j$  for  $j > i$ ,  $n_r \geq 2$ , and  $n_1 n_2 \dots n_r = n$ .

**Definition 14.8:** In order to avoid excessive use of *subscripts* and *superscripts*, we say that a finite abelian  $p$ -group  $G$  is of **type**  $(e_1, e_2, \dots, e_r)$  if  $G \cong C_{p^{e_1}} \times C_{p^{e_2}} \times \dots \times C_{p^{e_r}}$  and  $e_1 \geq e_2 \geq \dots \geq e_r \geq 1$ . The next result introduces two *standard subgroups* of a finite abelian group.

**Proposition 14.9:** Let  $p$  be a prime. For any *finite abelian group*  $G$ , the subset  $G_p$  of  $G$  consisting of elements of order 1 or  $p$  is a *subgroup* of  $G$ . Also, the subset  $G^p$  of  $p$ -th powers of elements of  $G$  is *also* a subgroup of  $G$ . Let  $G$  be an *abelian  $p$ -group* of type  $(e_1, e_2, \dots, e_r)$  with  $t$  the **largest** integer such that  $e_t > 1$ . Then  $G_p$  has order  $p^t$ , and  $G^p$  has type  $(e_1 - 1, e_2 - 1, \dots, e_t - 1)$ .

**Proposition 14.10:** Suppose that  $G$  is an *abelian  $p$ -group*. Then the type of  $G$  is **uniquely** determined. Thus, if  $G$  is of type  $(e_1, e_2, \dots, e_r)$  and *also* of type  $(f_1, f_2, \dots, f_s)$ , then  $r = s$ , and  $e_i = f_i$  for  $1 \leq i \leq r$ .

**Corollary 14.11:** Every *finite abelian group*  $G$  has a **unique** decomposition of the form  $C_{n_1} \times C_{n_2} \times \dots \times C_{n_r}$ , where  $n_i$  is divisible by  $n_j$  for  $j > i$ ,  $n_r \geq 2$ , and  $n_1 n_2 \dots n_r = |G|$ .

**Definition 14.12:** A **field** is a set  $F$  which is an *abelian group* under *addition*. There is also a *multiplication* on  $F$  which is *closed*, *associative* and *commutative*, and there is an *identity* element  $1_F$  which is **not equal** to the zero element. The other axioms are the *distributive laws*,  $x(y+z) = xy+xz$  and  $(x+y)z = xz+yz$ ; and the requirement that every *non-identity element* has a *multiplicative inverse*: if  $x \neq 0$ , then there exists a  $y \in F$  such that  $xy = 1_F$ . Notice that the *non-zero elements* of a field  $F$  form a **group** under multiplication. It is an easy consequence of these axioms that  $0x = 0$  for all elements  $x$  in a field  $F$ .

**Definition 14.13:** A finite abelian  $p$ -group  $G$  is **elementary abelian** if every element of  $G$  has order dividing  $p$ . It follows from the classification theorem that an elementary abelian  $p$ -group is of the form  $C_p \times C_p \times \dots \times C_p$ , so that  $G$  has type  $(1, 1, \dots, 1)$ .

**Proposition 14.14:** Let  $F$  be a finite field. Then there is a prime  $p$  and a positive integer  $n$  such that  $F$  has  $p^n$  elements. The additive group of  $F$  is elementary abelian.

**Proposition 14.15:** The multiplicative group of a finite field is cyclic.

## Exercises

**14-1:** Write down the complete list of abelian groups with 360 elements.

**Answer:** Let  $G$  be a finite abelian group with 360 elements. Corollary 14.11 says that  $G$  has a **unique** decomposition in the form  $C_{n_1} \times C_{n_2} \times \dots \times C_{n_r}$ , where  $n_i$  is divisible by  $n_j$  for  $j > i$ ,  $n_r \geq 2$ , and  $n_1 n_2 \dots n_r = 360$ . We therefore have to find all the possible *valid combinations* of  $n_1 n_2 \dots n_r$ .

Now as  $360 = 2^3 \times 3^2 \times 5$ , then Proposition 14.3 allows us to write  $G$  as the *internal direct product* of its Sylow subgroups, namely  $G \cong C_{2^3} \times C_{3^2} \times C_5$ . We then use Proposition 14.5 to write each Sylow subgroup as a direct product of *cyclic subgroups*. So we can have  $C_{2^3} \cong C_2 \times C_2 \times C_2$ ,  $C_{2^3} \cong C_4 \times C_2$  and  $C_{2^3} \cong C_8$ ;  $C_{3^2} \cong C_3 \times C_3$  and  $C_{3^2} \cong C_9$ ; and  $C_5 \cong C_5$ . This leaves us with the following possible combinations:

$$\begin{array}{ll}
 C_{360} \cong C_8 \times C_9 \times C_5 & \cong C_5 \times C_8 \times C_9 \quad (\text{using Proposition 13.1, part (2)}) \\
 C_{360} \cong C_4 \times C_2 \times C_9 \times C_5 & \cong C_2 \times C_4 \times C_5 \times C_9 \\
 C_{360} \cong C_2 \times C_2 \times C_2 \times C_9 \times C_5 & \cong C_2 \times C_2 \times C_2 \times C_5 \times C_9 \\
 C_{360} \cong C_8 \times C_3 \times C_3 \times C_5 & \cong C_3 \times C_3 \times C_5 \times C_8 \\
 C_{360} \cong C_4 \times C_2 \times C_3 \times C_3 \times C_5 & \cong C_2 \times C_3 \times C_3 \times C_4 \times C_5 \\
 C_{360} \cong C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5 & \cong C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5
 \end{array}$$

We now use Corollary 13.2 *repeatedly* on each above combination so as to obtain a cyclic factor of  $G$ . For example, in the first combination, 5 is coprime so 8 so that  $C_5 \times C_8 \cong C_{40}$ , and then 40 is coprime to 9 so that  $C_{40} \times C_9 \cong C_{360}$ . Thus the above combinations change to the following:

$$\begin{array}{ll}
 C_{360} \cong C_{360} & \\
 C_{360} \cong C_{90} \times C_4 & \text{or} \quad C_{360} \cong C_{180} \times C_2 \\
 C_{360} \cong C_{90} \times C_2 \times C_2 & \\
 C_{360} \cong C_{120} \times C_3 & \\
 C_{360} \cong C_{30} \times C_{12} & \text{or} \quad C_{360} \cong C_{60} \times C_6 \\
 C_{360} \cong C_{30} \times C_6 \times C_2 &
 \end{array}$$

The combinations marked above in **red** are the only ones in which we do not have  $G$  in the form  $C_{n_1} \times C_{n_2} \times \dots \times C_{n_r}$ , where  $n_i$  is divisible by  $n_j$  for  $j > i$ ,  $n_r \geq 2$ , and  $n_1 n_2 \dots n_r = 360$ .

However, by noticing that  $C_4 \cong C_2 \times C_2$  and that  $C_{12} \cong C_6 \times C_2$  (these manipulations are done using the *same methods* as before, where in doing so no **extra** valid combinations are found), then we can change the **red** combinations to *valid* combinations which are *already* in the list, so that we can now write down the **complete** list of abelian groups with 360 elements:

$$\begin{aligned} C_{360} &\cong C_{360} \\ C_{360} &\cong C_{180} \times C_2 \\ C_{360} &\cong C_{120} \times C_3 \\ C_{360} &\cong C_{90} \times C_2 \times C_2 \\ C_{360} &\cong C_{60} \times C_6 \\ C_{360} &\cong C_{30} \times C_6 \times C_2. \end{aligned}$$

**14-2:** Prove that in a *finite abelian p-group* the elements of order dividing  $p^r$  form a **subgroup**. Give an example of a finite p-group in which the elements of order dividing p do **not** form a subgroup.

**Answer:** In order to prove that the elements of order dividing  $p^r$  form a *subgroup* H (say) of a finite abelian p-group G, then we have to show that the *identity element* is in H, that the *product* of any two elements in H is also in H, and that the *inverse* of any element in H is also an element of H. To *begin*, we notice that because the identity element **always** has order 1, and because 1 will **always** divide  $p^r$ , then the identity element will always be an element of H.

*Secondly*, if two elements x and y are in H, then because the orders of x and y divide  $p^r$ , then we must have  $x^{p^r} = y^{p^r} = 1$ . We want to show that the element xy is in H. If it is in H, then its order will divide  $p^r$ , so that we must have  $(xy)^{p^r} = 1$ . But using Proposition 14.2, and knowing that G is an *abelian* group, we notice that  $(xy)^{p^r} = x^{p^r} y^{p^r} = 1 \times 1 = 1$ , so that  $(xy)^{p^r} = 1$  as required.

*Finally*, if an element z is in H, then we must show that  $z^{-1}$  is also in H. By elementary properties of indices,  $(z^{-1})^{p^r} = (z^{p^r})^{-1} = 1^{-1} = 1$ , and so  $z^{-1}$  must be in H. This completes the proof that H is a *subgroup* of G.

Let us now consider the **Dihedral Group D(4)** with presentation  $D(4) = \langle b, a : b^2 = 1 = a^4, ab = ba^{-1} \rangle$  and elements 1, a,  $a^2$ ,  $a^3$ , b, ba,  $ba^2$  and  $ba^3$ . It is clear from the presentation that the element 1 has *order 1*, that the elements a and  $a^3$  have *order 4*, and that the elements  $a^2$  and b have *order 2*. By using the **relations** in the presentation, we can also show that the elements ba,  $ba^2$  and  $ba^3$  also have order 2 (e.g.  $(ba)^2 = baba = b(ab)a = b(ba^{-1})a = b^2 = 1$ ). We have therefore found that D(4) consists of a **single** element of order 1, **five** elements of order 2, and **two** elements of order 4.

Because  $|D(4)| = 8 = 2^3$ , and because the orders of all the elements in D(4) are *powers of 2*, then D(4) is a *finite 2-group*. Further, the elements in D(4) with order dividing 2 are the elements 1,  $a^2$ , b, ba,  $ba^2$  and  $ba^3$ . Because there are exactly **six** elements of this type, then the set  $H = \{1, a^2, b, ba, ba^2, ba^3\}$  cannot possibly form a subgroup of D(4) because Lagrange's Theorem requires that the order of any subgroup **divides** the order of the group, which is not the case in this situation:  $|H| \nmid |D(4)|$ , or  $6 \nmid 8$ .

## Chapter 15: The Jordan-Hölder Theorem

### Key Definitions and Results

**Definition 15.1:** Given a group  $G$ , a *subnormal series* for  $G$  is a **chain**  $G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_r = \{1\}$  of *subgroups* of  $G$ , with  $G_i$  a normal subgroup of  $G_{i-1}$  (for  $i = 1, \dots, r$ ).

**Definition 15.2:** A *normal series* for  $G$  is a **chain**  $G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_r = \{1\}$ , of *normal subgroups* of  $G$ . Note that **every** normal series is subnormal, but that the converse is not true in general.

**Definition 15.5:** Let  $G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_r = \{1\}$  and  $G = H_0 \geq H_1 \geq H_2 \geq \dots \geq H_s = \{1\}$  both be *subnormal series* of  $G$ , denoted as (A) and (B). Then (B) is said to be a **subnormal refinement** of (A) if each group which appears in (A) *also* occurs in (B). Similarly, if (A) and (B) are both *normal series* for  $G$ , then (B) is a **normal refinement** of (A) if each group which appears in (A) *also* occurs in (B).

**Definition 15.6:** The series (A) and (B) are **isomorphic** if there is a *bijection* between the sets  $\{G_0/G_1, G_1/G_2, \dots, G_{r-1}/G_r\}$  and  $\{H_0/H_1, H_1/H_2, \dots, H_{s-1}/H_s\}$  of quotient groups such that groups which correspond under the bijection are *isomorphic*. Thus, in particular,  $r = s$ . Note that this definition applies to the case when (A) and (B) are both *subnormal series* and also to the case when (A) and (B) are both *normal series*.

**Proposition 15.9:** Let  $H, H_1$  and  $K, K_1$  be *subgroups* of a group  $G$  with  $H_1$  a *normal subgroup* of  $H$  and  $K_1$  a *normal subgroup* of  $K$ . Then  $\frac{H_1(H \cap K)}{H_1(H \cap K_1)} \cong \frac{K_1(H \cap K)}{K_1(H_1 \cap K)}$ .

**Theorem 15.10 (Schreier's Refinement Theorem):** Any two *subnormal series* of a group  $G$  have subnormal refinements which are *isomorphic*. Similarly, any two *normal series* of a group  $G$  have *isomorphic* normal refinements. Note that the proof of this theorem uses Proposition 15.9.

**Definition 15.12:** A *composition series* for a group  $G$  is a *subnormal series* without repetitions which can be refined only by **repeating** terms.

**Definition 15.13:** A *chief series* for  $G$  is a *normal series* without repetitions which can be refined (by a normal series) only by **repeating** terms.

**Remark 1:** The infinite cyclic group  $G = \langle x \rangle$  has *neither* a composition series nor a chief series. **Remark 2:** Suppose that we are given a series  $G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_r = \{1\}$  for  $G$  which may be either *normal* or *subnormal*. If we know that for some value of  $i$ , the index of  $G_{i+1}$  in  $G_i$  is a **prime integer**  $p$ , then the series *cannot* be refined between these terms.

**Theorem 15.16 (The Jordan-Hölder Theorem):** If a group has a *composition series* then any two composition series are **isomorphic**. A similar result holds for *chief series*.

## Exercises

**15-1:** Find *composition series* and *chief series* for (a) the **symmetric** group  $S(4)$ ; (b) the **quaternion** group of order 8 with presentation  $\langle a, b: a^4 = 1, a^2 = b^2, ba = ab^{-1} \rangle$ ; and (c) the **dihedral** group  $D(6)$ .

**Answer:** (a)  $S(4)$  is a group with 24 *elements*, thus by Lagrange's Theorem, any subgroups will have order 1, 2, 3, 4, 6, 8, 12 or 24. It is well known that the Alternating Group  $A(4)$  is a subgroup of  $S(4)$ , and because the index of  $A(4)$  in  $S(4)$  is 2 (i.e.  $|S(4):A(4)| = 2$ ), then it follows by Example 7.6 that  $A(4)$  is a **normal** subgroup of  $S(4)$ .

We can now 'borrow' the calculations from Example 15.15, which showed that a composition series for  $A(4)$  is given by  $A(4) \geq V \geq \{1, (1\ 2)(3\ 4)\} \geq \{1\}$ , where  $V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ . Thus a composition series for  $S(4)$  is given by  $S(4) \geq A(4) \geq V \geq \{1, (1\ 2)(3\ 4)\} \geq \{1\}$ . This is supported by the fact that the index of  $A(4)$  in  $S(4)$  is 2; the index of  $V$  in  $A(4)$  is 3, the index of  $\{1, (1\ 2)(3\ 4)\}$  in  $V$  is 2, and the index of  $\{1\}$  in  $\{1, (1\ 2)(3\ 4)\}$  is 2: all of these numbers are **prime** numbers, so that (by Remark 2 on the previous page) the series cannot be refined *without repetitions*, and thus the series must therefore be a composition series.

The above composition series for  $S(4)$  is not a *chief series* for  $S(4)$  because the subgroup  $\{1, (1\ 2)(3\ 4)\}$  is not a normal subgroup of  $S(4)$  (e.g.  $(1\ 2\ 3)\{1, (1\ 2)(3\ 4)\} = \{1, (2\ 4\ 3)\} \neq \{1, (1\ 3\ 4)\} = \{1, (1\ 2)(3\ 4)\}(1\ 2\ 3)$ ). Similarly, none of the other two subgroups of  $V$  (of order 2) are normal in  $S(4)$  either. This eliminates any normal subgroups of *order* 2 from our chief series.

The question now arises as to whether  $V$  is *normal* in  $S(4)$ . It turns out that  $V$  is indeed normal in  $S(4)$  (we could if we really wanted to prove this assertion by showing that  $gV = Vg$  for all  $g \in S(4)$ ). It follows that as  $A(4)$  and  $V$  are normal subgroups of  $S(4)$ , and as there are no normal subgroups of orders 2 or 3, then a chief series for  $S(4)$  is given by  $S(4) \geq A(4) \geq V \geq \{1\}$ .

(b) The quaternion group in question (hereafter referred to as  $Q_8$ ) is a group with 8 *elements*, and thus by Lagrange's Theorem, any subgroups will have order 1, 2, 4 or 8. It is easily shown that  $\langle a \rangle$  is a subgroup of  $A_8$  of order 4, and thus must be a normal subgroup of  $Q_8$  because  $|Q_8:\langle a \rangle| = 2$ .

We now look for a (non-trivial) normal subgroup of  $\langle a \rangle$ . This normal subgroup can only be of order 2, so that the only candidate is  $H = \{1, a^2\}$ . Elements of  $H$  obviously commute with  $a$ , but do they commute with  $b$ ? Well, 1 *always* commutes with anything, so our only problem is in whether we have  $ba^2b^{-1} = a^2$ . Well, as  $a^2 = b^2$ , then  $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ , so we have our answer —  $\{1, a^2\}$  **is** a normal subgroup of  $\langle a \rangle$ . Now note that since  $|Q_8:\langle a \rangle| = 2$ , since  $|\langle a \rangle:\{1, a^2\}| = 2$ , and since  $|\{1, a^2\}:\{1\}| = 2$  — all prime integers — then there are no more refinements, and so the composition group we require is given by  $Q_8 \geq \langle a \rangle \geq \{1, a^2\} \geq \{1\}$ . This is also the *chief group* for  $Q_8$  as  $\{1, a^2\}$  is also a normal subgroup of  $Q_8$  by the same technique used to show that  $\{1, a^2\}$  is a normal subgroup of  $\langle a \rangle$ .

(c) Since  $D(6)$  has 12 elements, then by Lagrange's Theorem, any subgroups will have order 1, 2, 3, 4, 6 or 12. Now if we present  $D(6)$  as  $D(6) = \langle a, b : a^6 = 1 = b^2, bab^{-1} = a^{-1} \rangle$ , then we see that  $\langle a \rangle$  is a subgroup of  $D(6)$  with 6 elements. It therefore follows that  $\langle a \rangle$  is a normal subgroup of  $D(6)$  as  $|D(6) : \langle a \rangle| = 2$ .

Looking for normal subgroups of  $\langle a \rangle$ , we see that the *only* candidates are  $\langle a^2 \rangle$  and  $\langle a^3 \rangle$ . Now as  $\langle a^2 \rangle = \{1, a^2, a^4\}$  is definitely a **subgroup** of  $\langle a \rangle$ , and as  $|\langle a \rangle : \langle a^2 \rangle| = 2$ , then  $\langle a^2 \rangle$  is a **normal subgroup** of  $\langle a \rangle$ . And since  $\langle a^2 \rangle$  has no non-trivial normal subgroups (because of Lagrange's Theorem), then a composition series for  $D(6)$  is given by  $D(6) \geq \langle a \rangle \geq \langle a^2 \rangle \geq \{1\}$ .

To show that  $D(6) \geq \langle a \rangle \geq \langle a^2 \rangle \geq \{1\}$  is a *chief series* for  $D(6)$ , all we need show is that  $\langle a^2 \rangle$  is a **normal subgroup** of  $D(6)$ . Now it is obvious that  $a\langle a^2 \rangle a^{-1} = \langle a^2 \rangle = a^{-1}\langle a^2 \rangle a$ , so we need to look at what  $b\langle a^2 \rangle b^{-1}$  and  $b^{-1}\langle a^2 \rangle b$  are. Now  $b\langle a^2 \rangle b^{-1} = b\{1, a^2, a^4\}b^{-1} = \{1, ba^2b^{-1}, ba^4b^{-1}\} = \{1, (bab^{-1})^2, (bab^{-1})^4\} = \{1, (a^{-1})^2, (a^{-1})^4\} = \{1, a^{-2}, a^{-4}\} = \{1, a^4, a^2\} = \langle a^2 \rangle$ . Similarly,  $b^{-1}\langle a^2 \rangle b = \langle a^2 \rangle$  so that we may apply part (c) of Theorem 7.4 to say that  $\langle a^2 \rangle$  is a normal subgroup of  $D(6)$ \*. Therefore, a chief series for  $D(6)$  is given by  $D(6) \geq \langle a \rangle \geq \langle a^2 \rangle \geq \{1\}$ .

\* We may show that  $g^{-1}\langle a^2 \rangle g = \langle a^2 \rangle = g\langle a^2 \rangle g^{-1}$  for all  $g$  in  $D(6)$  by the fact that as all the elements in  $D(6)$  are words written in the generators  $a$  and  $b$ , then repeated application of  $a^{-1}\langle a^2 \rangle a = \langle a^2 \rangle = a\langle a^2 \rangle a^{-1}$  and  $b^{-1}\langle a^2 \rangle b = \langle a^2 \rangle = b\langle a^2 \rangle b^{-1}$  will allow us to write  $g^{-1}\langle a^2 \rangle g = \langle a^2 \rangle = g\langle a^2 \rangle g^{-1}$  for all  $g$  in  $D(6)$  (*remember that*  $(\alpha_1\alpha_2\dots\alpha_n)^{-1} = (\alpha_n^{-1}\alpha_{n-1}^{-1}\dots\alpha_2^{-1}\alpha_1^{-1})$ ).

**15-3:** Give examples of: (a) a group with a *normal series* with an infinite number of terms; (b) a group with a *composition series* which is not a chief series; and (c) a group with *two different* chief series.

**Answer:** (a) Looking at Remark 1 on page 133 of the book, we see that an example comes from the *infinite cyclic group*  $G = \langle x \rangle$ . Assume that  $G$  has a **finite** normal series of the form  $G = G_0 > G_1 > G_2 > \dots > G_r = \{1\}$ . Since each *subgroup* of a cyclic group is cyclic (Proposition 4.13), so that every **normal subgroup**  $G_i$  is cyclic, then the group  $G_{r-1}$  is cyclic generated by  $x^s$  for some  $s$ . This means that  $G_{r-1}$  is actually an *infinite cyclic group*, so that  $\langle x^{2s} \rangle$  is a proper subgroup of  $G_{r-1}$ . We would then obtain a non-trivial refinement  $G = G_0 > G_1 > G_2 > \dots > G_{r-1} > \langle x^{2s} \rangle > \{1\}$  so that our assumption that  $G$  had a *finite normal series* was false, and so  $G$  must have an **infinite** normal series.

(b) We have *already* encountered such an example in Exercise 15-1, part (a). (c) An example of a group with two different chief series is provided by Examples 15.3, 15.8 and 15.17 in the book. Consider the case of a *cyclic group*  $G = \langle x \rangle$  of order 6. The two series  $G \geq \langle x^2 \rangle \geq \{1\}$  and  $G \geq \langle x^3 \rangle \geq \{1\}$  are two **normal** series for  $G$  since any subgroup of an abelian group is normal. These series are also **chief** series because  $|G : \langle x^2 \rangle| = 2$ ,  $|\langle x^2 \rangle : \{1\}| = 3$ ,  $|G : \langle x^3 \rangle| = 3$ , and  $|\langle x^3 \rangle : \{1\}| = 2$  — all prime numbers, so no more refinements are possible. Finally, notice that because  $G/\langle x^2 \rangle \cong \langle x^3 \rangle$  and  $G/\langle x^3 \rangle \cong \langle x^2 \rangle$ , then these two chief series are *isomorphic* — as required by the Jordan-Hölder Theorem.

# Chapter 16: Composition Factors and Chief Factors

## Key Definitions and Results

**Definition 16.1:** Suppose that  $G = G_0 > G_1 > \dots > G_{r-1} > G_r = \{1\}$  is a *composition series* for the group  $G$ . The *quotient groups*  $G_0/G_1, G_1/G_2, \dots, G_{r-1}/G_r$  are the **composition factors** of  $G$ .

**Definition 16.2:** If  $G = G_0 > G_1 > \dots > G_{r-1} > G_r = \{1\}$  is a *chief series* for the group  $G$ , the *quotient groups*  $G_0/G_1, G_1/G_2, \dots, G_{r-1}/G_r$  are the **chief factors** of  $G$ .

**Remark:** It follows by the Jordan-Hölder Theorem that the set of *composition factors* of a given group  $G$  is *independent* of the *composition series* and this set is therefore an *invariant* of the group  $G$ . A similar remark applies to the *chief factors* of a group.

**Definition 16.3:** A group  $G$  is *simple* if the **only** normal subgroups of  $G$  are  $\{1\}$  and  $G$ .

**Proposition 16.4:** Any *composition factor* of a group is a **simple** group.

**Proposition 16.5:** A *simple abelian group* is cyclic of prime order. In particular, a *composition factor* of a finite abelian group is cyclic of prime order.

**Definition 16.6:** A subgroup  $H$  of a group  $G$  is **characteristic** if for each automorphism  $\varphi$  of  $G$ ,  $\varphi(H) = H$ . **Remark:** Notice that for any *fixed* element  $g \in G$ , the map  $\varphi_g$  defined by  $\varphi_g(x) = gxg^{-1}$  for all  $x \in G$  is an *automorphism* of  $G$ . It follows that any characteristic subgroup is **necessarily** a normal subgroup.

**Proposition 16.8:** Let  $N$  be a *normal* subgroup of a group  $G$  and let  $K$  be a *characteristic* subgroup of  $N$ . Then  $K$  is a *normal* subgroup of  $G$ .

**Definition 16.9:** A group  $G$  is **characteristically simple** if the only characteristic subgroups of  $G$  are  $\{1\}$  and  $G$  itself.

**Proposition 16.10:** Every *chief factor* of a group  $G$  is *characteristically simple*.

**Proposition 16.11:** A *finite characteristically simple group* is a direct product of *isomorphic simple groups*. In particular, a *chief factor* of a finite group is a direct product of isomorphic simple groups.

**Corollary 16.12:** A *finite abelian chief factor* of a group is an *elementary abelian  $p$ -group* for some prime  $p$ .

**Theorem 16.13:** The alternating group  $A(5)$  is a *non-abelian simple group*. **Proposition 16.14:** The alternating group  $A(n)$  is *generated* by its 3-cycles. **Corollary 16.15:** The *only* normal subgroup of  $A(n)$  which contains a 3-cycle is  $A(n)$  itself. **Theorem 16.16:** The group  $A(n)$  is *simple* for  $n \geq 5$ .

## Exercises

**16-1:** Give an example of two *non-isomorphic groups with isomorphic chief series*.

**Answer:** Consider the two groups  $G = D(3)$  and  $H = C(6)$ , both with *six* elements but **not** isomorphic. Since  $D(3)$  has 6 elements, then by Lagrange's Theorem, any subgroups will have order 1, 2, 3 or 6. Now if we present  $D(3)$  as  $D(3) = \langle a, b: a^3 = 1 = b^2, bab^{-1} = a^{-1} \rangle$ , then we see that  $\langle a \rangle$  is a subgroup of  $D(3)$  with 3 elements. It therefore follows that  $\langle a \rangle$  is a **normal** subgroup of  $D(3)$  as  $|D(3):\langle a \rangle| = 2$ .

It follows that  $D(3) \geq \langle a \rangle \geq \{1\}$  is a *chief series* for  $D(3)$  as  $\langle a \rangle$  has no non-trivial normal subgroups. Notice that  $\langle a \rangle$  is isomorphic to  $C(3)$  so that the chief series for  $D(3)$  may be written as  $D(3) \geq C(3) \geq \{1\}$ . Now we saw in Exercise 15-3 that a chief series for  $C(6)$  is given by  $C(6) \geq C(3) \geq \{1\}$ .

To prove that the two series  $D(3) \geq C(3) \geq \{1\}$  and  $C(6) \geq C(3) \geq \{1\}$  are *isomorphic*, we must show that there is a **bijection** between the sets  $\{D(3)/C(3), C(3)/\{1\}\}$  and  $\{C(6)/C(3), C(3)/\{1\}\}$ . But this follows as  $D(3)/C(3)$  and  $C(6)/C(3)$  are both groups of order 2, so must be isomorphic to  $C(2)$ . We therefore conclude that we have found an example of two *non-isomorphic groups* ( $D(3)$  and  $C(6)$ ) with *isomorphic chief series* ( $D(3) \geq C(3) \geq \{1\}$  and  $C(6) \geq C(3) \geq \{1\}$ ).

**16-4:** Let  $H$  be a *characteristic subgroup* of  $G$  and  $K$  be a *characteristic subgroup* of  $H$ . Show that  $K$  is a *characteristic subgroup* of  $G$ .

**Answer:** If  $H$  is a characteristic subgroup of  $G$ , then for each automorphism  $\phi$  of  $G$ , we have  $\phi(H) = H$ . To show that  $K$  is a characteristic subgroup of  $G$ , then we must show that for each automorphism  $\phi$  of  $G$ , we have  $\phi(K) = K$ .

Consider an *arbitrary* automorphism  $\phi$  of  $G$ . We know that  $\phi(H) = H$ , so that for all  $h \in H$ , we have  $\phi(h) \in H$ . Because of this, then we can define an automorphism  $\phi_H$  of  $H$  from the automorphism  $\phi$  of  $G$  by **restricting** the definition of  $\phi$  to involve elements of  $H$  only. This is known as an *induced* automorphism.

Because the subgroup  $K$  is a characteristic subgroup of  $H$ , then we know that  $\phi_H(K) = K$ . But because then it follows that  $K$  is an *invariant* under the **restricted** map  $\phi_H$ , and because  $K$  involves elements of  $H$  only, then  $K$  must also be an invariant under the map  $\phi$  as well, so that  $\phi(K) = K$  as required. QED.

# Chapter 17: Soluble Groups

## Key Definitions and Results

**Definition 17.1:** A group  $G$  is said to be *soluble* if  $G$  has a normal series  $G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_r = \{1\}$  in which the *quotient groups*  $G_0/G_1, G_1/G_2, \dots, G_{r-1}/G_r$  are **abelian** groups.

**Proposition 17.5:** Let  $G$  be a *soluble* group. Then (i) for *any subgroup*  $H$  of  $G$ ,  $H$  is a *soluble* group, and (ii) for *any normal subgroup*  $N$  of  $G$ , the *quotient group*  $G/N$  is soluble.

**Proposition 17.6:** Let  $G$  be a finite *soluble* group. Then (i) if  $G$  is **simple**, then  $G$  is **cyclic** of prime order; (ii) any **composition factor** of  $G$  is *cyclic* of prime order, and (iii) a **chief factor** of  $G$  is an *elementary abelian  $p$ -group* for some prime  $p$ .

**Definition 17.7:** Let  $x$  and  $y$  be *elements* of a group  $G$ . The *commutator*  $[x, y]$  is the element  $xyx^{-1}y^{-1}$ .

**Definition 17.8:** The *commutator subgroup* or *derived group*, denoted by  $[G, G]$  or  $G'$ , is the subgroup generated by *all* commutators:  $[G, G] = G' = \langle [x, y] : x, y \in G \rangle$ .

**Proposition 17.9:** For any group  $G$ , the derived group  $G'$  is a *characteristic subgroup* of  $G$  and is the *smallest* normal subgroup of  $G$  with *abelian quotient group*, in the sense that if  $N$  is a normal subgroup of  $G$  with  $G/N$  abelian, then  $N$  *contains*  $G'$ .

**Remark:** Given a *presentation* for  $G$ , it is quite easy to obtain a presentation for the abelian quotient group  $G/[G, G]$ . This is done by *adding* to the presentation the relations saying that each pair of generators *commute* thereby accounting for the fact that  $G/[G, G]$  is abelian.

**Definition 17.13:** Define the *derived series* of  $G$  iteratively as follows:  $G^{(0)} = G$ ;  $G^{(1)} = G'$ ;  $G^{(2)} = [G', G']$ ; ...;  $G^{(r+1)} = [G^{(r)}, G^{(r)}]$ .

**Proposition 17.14:** Each group  $G^{(n)}$  is a *normal subgroup* of  $G$ .

**Proposition 17.15:** The following *conditions* on a group  $G$  are **equivalent**: (i)  $G$  is *soluble*; (ii)  $G$  has a *subnormal series*  $G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_r = \{1\}$ , with the quotient groups  $G_0/G_1, G_1/G_2, \dots, G_{r-1}/G_r$  *abelian*; (iii) there is an *integer*  $n$  for which  $G^{(n)} = \{1\}$ .

**Proposition 17.16:** Let  $G$  be a group with a **normal subgroup**  $N$  such that  $N$  and  $G/N$  are soluble groups. Then  $G$  is a *soluble* group.

**Remark:** The *analogue* of Proposition 17.16 does not hold for *abelian* groups. The group  $D(3)$  is a *non-abelian* group with an *abelian* normal subgroup  $N$  with  $G/N$  **also** *abelian*.

## Exercises

**17-4:** For any elements  $x, y$  of a group  $G$ , denote by  $x^y$  the *product*  $xyx^{-1}$ . Let  $a, b$  and  $c$  be elements of a group  $G$ . **Prove** that

- (a)  $[ab, c] = [b, c]^a[a, c]$ ; and  
 (b)  $[a, bc] = [a, b][a, c]^b$ .

**Answer:**

$$\begin{aligned}
 \text{(a) LHS} = [ab, c] &= (ab)(c)(ab)^{-1}(c)^{-1} \\
 &= abcb^{-1}a^{-1}c^{-1} \\
 &= abcb^{-1}(c^{-1}a^{-1}ac)a^{-1}c^{-1} \\
 &= abcb^{-1}c^{-1}a^{-1}aca^{-1}c^{-1} \\
 &= a(bcb^{-1}c^{-1})a^{-1}(aca^{-1}c^{-1}) \\
 &= a[b, c]a^{-1}[a, c] \\
 &= [b, c]^a[a, c] = \text{RHS.}
 \end{aligned}$$

$$\begin{aligned}
 \text{(b) LHS} = [a, bc] &= (a)(bc)(a)^{-1}(bc)^{-1} \\
 &= abca^{-1}c^{-1}b^{-1} \\
 &= ab(a^{-1}b^{-1}ba)ca^{-1}c^{-1}b^{-1} \\
 &= aba^{-1}b^{-1}baca^{-1}c^{-1}b^{-1} \\
 &= (aba^{-1}b^{-1})b(aca^{-1}c^{-1})b^{-1} \\
 &= [a, b]b[a, c]b^{-1} \\
 &= [a, b][a, c]^b = \text{RHS.}
 \end{aligned}$$

**17-6:** Let  $G$  be the set of all *real*  $4 \times 4$  matrices of the form

$$\begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Find a formula for the *product* of two elements of  $G$  and find the *inverse* of an element of  $G$ . Deduce that  $G$  is a **group** with respect to matrix multiplication. Let  $A$  be the subset of matrices in  $G$  of the form

$$\begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Show that  $A$  is a *normal abelian subgroup* of  $G$ . Prove that  $G'$  is *contained* in  $A$  and deduce that  $G$  is *soluble*.

**Answer:** Let  $A = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix}$ , and let  $B = \begin{pmatrix} 1 & f & g & h \\ 0 & 1 & 0 & i \\ 0 & 0 & 1 & j \\ 0 & 0 & 0 & 1 \end{pmatrix}$ .

$$AB = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & f & g & h \\ 0 & 1 & 0 & i \\ 0 & 0 & 1 & j \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & f+a & g+b & h+ai+bj+c \\ 0 & 1 & 0 & i+d \\ 0 & 0 & 1 & j+e \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

which is an element of  $G$  — and therefore  $G$  is *closed under matrix multiplication*.

Now to obtain  $A^{-1}$ , we manipulate  $(A | I)$  to get  $(I | A^{-1})$ .

$$\begin{aligned} (A | I) &= \begin{pmatrix} 1 & a & b & c & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & d & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & e & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & a & b & 0 & 1 & 0 & 0 & -c \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & -d \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & -e \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{array}{l} R_1 - cR_4 \\ R_2 - dR_4 \\ R_3 - eR_4 \end{array} \\ &\sim \begin{pmatrix} 1 & a & 0 & 0 & 1 & 0 & -b & -c+be \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & -d \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & -e \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} R_1 - bR_3 \\ &\sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & -a & -b & -c+be+ad \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & -d \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & -e \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} R_1 - aR_2 \\ &= (I | A^{-1}). \end{aligned}$$

$$\text{Therefore, } A^{-1} = \begin{pmatrix} 1 & -a & -b & -c+be+ad \\ 0 & 1 & 0 & -d \\ 0 & 0 & 1 & -e \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

which is an element of  $G$  — and therefore every element of  $G$  has an *inverse*.

As we have shown that  $G$  is **closed** under matrix multiplication and that every element in  $G$  has an **inverse**; plus knowing that matrix multiplication is **associative** and that the  $4 \times 4$  **identity matrix** is an element of  $G$ , we can therefore say that  $G$  forms a *group* under matrix multiplication.

Now to show that A is a *normal subgroup* of G, it is sufficient to show that  $g\alpha g^{-1} = \alpha$  for all  $g \in G$  and all  $\alpha \in A$ . Further, to show that A is an *abelian group*, it is sufficient to show that  $\alpha\beta = \beta\alpha$  for all  $\alpha$  and  $\beta$  in A.

Claim 1:  $g\alpha g^{-1} = \alpha$  for all  $g \in G$  and all  $\alpha \in A$ .

$$\begin{aligned}
 \text{Proof 1: } g\alpha g^{-1} &= \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & a \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & -b & -c+be+ad \\ 0 & 1 & 0 & -d \\ 0 & 0 & 1 & -e \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & a & b & a+c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & -b & -c+be+ad \\ 0 & 1 & 0 & -d \\ 0 & 0 & 1 & -e \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & -a+a & -b+b & (-c+be+ad)-ad-be+a+c \\ 0 & 1 & 0 & -d+d \\ 0 & 0 & 1 & -e+e \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 0 & 0 & a \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \alpha. \text{ QED.}
 \end{aligned}$$

Claim 2:  $\alpha\beta = \beta\alpha$  for all  $\alpha, \beta \in A$ .

$$\begin{aligned}
 \text{Proof 2: } \alpha\beta &= \begin{pmatrix} 1 & 0 & 0 & a \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & \beta \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \beta+a \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 0 & 0 & a+\beta \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \beta \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & a \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \beta\alpha. \text{ QED.}
 \end{aligned}$$

By the above proofs, we deduce that A is a *normal abelian subgroup* of G.

Now in order to show that  $G'$  is contained in  $A$ , it is sufficient to show that any element of  $G'$  is **also** an element of  $A$ . Consider an arbitrary commutator of  $G$ ,  $ghg^{-1}h^{-1}$ , where  $g$  and  $h$  are elements of  $G$ . If we can show that this commutator is also an element of  $A$ , then we have shown that  $G'$  is contained in  $A$ , because (a) all commutators of  $G$  will therefore be elements of  $A$ ; and (b) products of commutators will therefore be elements of  $A$  because  $A$  is a normal abelian subgroup.

Now  $ghg^{-1}h^{-1}$

$$\begin{aligned}
&= \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & f & g & h \\ 0 & 1 & 0 & i \\ 0 & 0 & 1 & j \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & f & g & h \\ 0 & 1 & 0 & i \\ 0 & 0 & 1 & j \\ 0 & 0 & 0 & 1 \end{pmatrix}^{-1} \\
&= \begin{pmatrix} 1 & f+a & g+b & h+ai+bj+c \\ 0 & 1 & 0 & i+d \\ 0 & 0 & 1 & j+e \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & -b & -c+be+ad \\ 0 & 1 & 0 & -d \\ 0 & 0 & 1 & -e \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -f & -g & -h+gj+fi \\ 0 & 1 & 0 & -i \\ 0 & 0 & 1 & -j \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & -a+f+a & -b+g+b & -c+be+ad-d(f+a)-e(g+h)+h+ai+bj+c \\ 0 & 1 & 0 & -d+i+d \\ 0 & 0 & 1 & -e+j+e \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -f & -g & -h+gj+fi \\ 0 & 1 & 0 & -i \\ 0 & 0 & 1 & -j \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & f & g & be-df-eg-eh+h+ai+bj \\ 0 & 1 & 0 & i \\ 0 & 0 & 1 & j \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -f & -g & -h+gj+fi \\ 0 & 1 & 0 & -i \\ 0 & 0 & 1 & -j \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & -f+f & -g+g & -h+gj+fi-fi-gj+be-df-eg-eh+h+ai+bj \\ 0 & 1 & 0 & -i+i \\ 0 & 0 & 1 & -j+j \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 & be-df-eg-eh+ai+bj \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in A,
\end{aligned}$$

so that  $G'$  is contained in  $A$  ( $G' \leq A$ ) as discussed above.

Now because  $A$  is an *abelian* group, then any **subgroup** of  $A$  will also be an abelian group. It follows that  $G'$  is an abelian group. But if  $G'$  is an abelian group, then by **Example 17.10** in the book (a group  $G$  is abelian if and only if  $G' = \{1\}$ ), we conclude that  $G^{(2)} = \{1\}$ . But if  $G^{(2)} = \{1\}$ , then **Proposition 17.15** (part (iii)) implies that  $G$  is a soluble group, and thus we have reached our required conclusion. QED.

# Chapter 18: Examples of Soluble Groups

## Key Definitions and Results

**Definition 18.1:** For any group  $G$ , let  $Z(G) = Z_1(G)$  denote the *centre* of  $G$ , and let  $Z_0(G)$  denote the subgroup  $\{1\}$ . Let  $Z_2(G)$  be the subgroup of  $G$  defined by  $Z_2(G)/Z(G) = Z(G/Z(G))$ , and in general let  $Z_{i+1}(G)$  be defined by  $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$ . The series  $\{1\} \leq Z(G) \leq Z_2(G) \leq \dots \leq Z_i(G) \leq \dots$  is the *upper central series* for  $G$ .

**Proposition 18.3:** A *finite p-group* is soluble. Every *chief factor* of a finite  $p$ -group is of order  $p$ .

**Definition 18.4:** A group  $G$  is *nilpotent* if the upper central series *terminates* in  $G$ . If the upper central series terminates after  $r$  steps, so that  $Z_r(G) = G$  but  $Z_{r-1}(G) \neq G$ , then we say that  $G$  is *nilpotent of class  $r$* . **Remark:** Proposition 18.3 shows that a *finite p-group* is nilpotent. Since the upper central series is a *normal series*, *any* nilpotent group is *soluble*.

**Proposition 18.5:** Let  $G$  be a nilpotent group and let  $H$  be any subgroup of  $G$  other than  $G$  itself. Then  $H$  is a *proper subgroup* of  $N_G(H)$ .

**Definition 18.6:** A subgroup  $H$  of a group  $G$  is *maximal* if  $H$  is a proper subgroup of  $G$  and no subgroup of  $G$  lies *properly* between  $H$  and  $G$ : if  $K$  is a subgroup of  $G$  with  $H \leq K \leq G$ , then  $K$  is either  $H$  or  $G$ .

**Corollary 18.7:** A *maximal* subgroup of a *nilpotent* group is *normal*.

**Proposition 18.8:** A finite group  $G$  is *nilpotent* if and only if  $G$  is an *internal direct product* of its Sylow subgroups, so that  $G = P_1 \times P_2 \times \dots \times P_r$ , where  $p_1, p_2, \dots, p_r$  are the distinct primes dividing  $|G|$ , and  $P_i$  is the Sylow  $p_i$ -subgroup of  $G$  (for  $1 \leq i \leq r$ ).

**Corollary 18.9:** Every *subgroup* and every *quotient group* of a finite nilpotent group is *nilpotent*. **Remark:** The conclusions of Corollary 18.9 hold for *any* nilpotent group, but a *different* proof is required if the group is *not* finite.

**Proposition 18.10:** Let  $N$  be a *non-trivial normal subgroup* of a finite nilpotent group  $G$ . Then the *intersection*  $N \cap Z(G)$  has order *greater* than 1.

**Proposition 18.11:** Let  $p$  be an *odd* prime. A non-abelian group of order  $p^3$  is *isomorphic* to one of  $\langle x, y: x^p = 1 = y^p, z = [x, y], z^p = 1, zx = xz, zy = yz \rangle$ , or  $\langle x, y: x^{p^2} = 1 = y^p, yxy^{-1} = x^{1+p} \rangle$ .

**Theorem 18.12:** Every group with *less than 60 elements* is soluble.

## Exercises

**18-2:** Let  $G$  be the group of order 27 consisting of the  $3 \times 3$  matrices of the form

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},$$

where  $a$ ,  $b$  and  $c$  are integers *modulo 3*, so that each of  $a$ ,  $b$  and  $c$  may be taken to be one of 0, 1 or 2, with arithmetical operations modulo 3 (so that, for example,  $1+2 = 0$  and  $2 \times 2 = 1$ ). Prove that *every* element of  $G$  has order 3. Find the *centre* of  $G$ . Hence find a *chief series* for  $G$ .

**Answer:** To show that every element of  $G$  has order 3, we show that if  $A$  is an arbitrary element of  $G$ , then  $A^3$  is the  $3 \times 3$  identity matrix.

$$\begin{aligned} \text{Now if } A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \text{ then } A^3 &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 3a & b+2ac+2b+ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Because when working modulo 3 we have  $3x \equiv 0$  for any  $x$ , then we see that  $3a \equiv 0$ , that  $3b+3ac \equiv 0$ , and that  $3c \equiv 0$ , so that  $A^3$  is the  $3 \times 3$  identity matrix *as required*.

Now the *centre* of  $G$  consists of those elements of  $G$  which commute with every element of  $G$ , so that if  $B \in Z(G)$ , then  $BC = CB$  for all  $C \in G$ .

$$\begin{aligned} \text{Now if } B = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}, \text{ and if } C = \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}, \\ \text{then } BC = \begin{pmatrix} 1 & g+d & h+di+e \\ 0 & 1 & i+f \\ 0 & 0 & 1 \end{pmatrix}, \text{ and } CB = \begin{pmatrix} 1 & d+g & e+gf+h \\ 0 & 1 & f+i \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

We see that in order for  $B$  to belong to the *centre* of  $G$ , then we must have  $di = gf$  for all possible  $i$  and  $g$ . But this will only happen if  $d = f = 0$ , leaving us with **three** choices for  $e$  in the matrix  $B$ , and so the three matrices in the centre of  $G$  are as follows:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

At this stage, we have found a *normal series* for  $G$ , namely  $G \geq Z(G) \geq \{1\}$ , by virtue of the fact that  $Z(G)$  is always a normal subgroup of  $G$ . Now the quotient group  $Z(G)\backslash\{1\}$  has **three** elements and so is cyclic of order 3 —and because 3 is a prime number, then by Remark 2 following Definition 15.13 on page 134 in the book, we can say that the normal series cannot be refined between  $Z(G)$  and  $\{1\}$ . However, the series can be refined between  $G$  and  $Z(G)$ :

Consider the subset  $N$  of  $G$  given by setting  $b = 0$  in  $A$ , i.e. the matrices of the form

$$\begin{pmatrix} 1 & a & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

Because there are **three** choices each for  $a$  and  $c$ , then there are **nine** matrices of type  $N$ . To show that the set of matrices given by the set  $N$  is a *subgroup* of  $G$ , all we need do is to show that the product of two elements from  $N$  is an element of  $N$ , and that the inverse of an element from  $N$  is also an element of  $N$ .

$$\text{But since } \begin{pmatrix} 1 & p & 0 \\ 0 & 1 & q \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & r & 0 \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & r+p & 0 \\ 0 & 1 & s+q \\ 0 & 0 & 1 \end{pmatrix} \in N,$$

$$\text{and since } \begin{pmatrix} 1 & t & 0 \\ 0 & 1 & u \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -t & 0 \\ 0 & 1 & -u \\ 0 & 0 & 1 \end{pmatrix} \in N,$$

it follows that  $N$  is a subgroup of  $G$ .

To show that  $N$  is a *normal subgroup* of  $G$ , we recall that all elements of  $G$  have order 3 and so  $G$  is a 3-group (by definition). It therefore follows that  $G$  is *soluble* by Proposition 18.3, and thus  $G$  is *nilpotent* by the Remark following Definition 18.4. Now if  $N$  is a *maximal* subgroup of  $G$ , then it follows that  $N$  is a normal subgroup of  $G$  by Corollary 18.7. But because  $N$  has *order 9* and because  $G$  has *order 27*, then Lagrange's Theorem implies that there are no proper subgroups of  $G$  with order greater than 9 — and so  $N$  must be a *maximal subgroup* of  $G$ , and thus (by the above discussion)  $N$  must be a normal subgroup of  $G$ .

So we have now obtained a refinement of our previous normal series, and the normal series that we are now dealing with is given by  $G \geq N \geq Z(G) \geq \{1\}$ . Now because  $G\backslash N$  is cyclic of order 3, and because  $N\backslash Z(G)$  is also cyclic of order 3, then (as before) there cannot be any refinements of this normal series between  $G$  and  $N$  and between  $N$  and  $Z(G)$ . It therefore follows that the normal series  $G \geq N \geq Z(G) \geq \{1\}$  is a **chief series**.

**18-3:** Let  $P$  be the group  $\langle x, y: x^9 = y^3 = 1, yxy^{-1} = x^4 \rangle$ , so that  $P$  consists of the 27 elements of the form  $x^j y^k$ , with  $j$  being one of  $0, 1, \dots, 8$ , and  $k$  being  $0, 1$  or  $2$ . Show that  $\langle x \rangle$  is a *normal subgroup* of  $P$  and that  $x^3$  is in the *centre* of  $P$ . Find a *chief series* for  $P$ .

**Answer:** To show that  $\langle x \rangle$  is a *normal subgroup* of  $P$ , it is sufficient to show that  $p\langle x \rangle p^{-1} = \langle x \rangle$  for all  $p \in P$ . But because every element of  $P$  can be written in the form  $x^j y^k$  for  $0 \leq j \leq 8$  and  $0 \leq k \leq 2$ , then all we need do in order to show that  $p\langle x \rangle p^{-1} = \langle x \rangle$  for all  $p \in P$  is to show that (a)  $x\langle x \rangle x^{-1} = \langle x \rangle$ , and that (b)  $y\langle x \rangle y^{-1} = \langle x \rangle$ . The result will then follow by *induction*, as  $p\langle x \rangle p^{-1} = x^j y^k \langle x \rangle (x^j y^k)^{-1} = x^j y^k \langle x \rangle y^{-k} x^{-j}$ .

Before starting, note that  $\langle x \rangle$  is the set given by  $\{1, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8\}$  because the *presentation* for  $P$  tells us that  $x^9 = 1$ .

$$\begin{aligned} \text{(a)} \quad & x\langle x \rangle x^{-1} \\ &= x\{1, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8\}x^{-1} \\ &= \{1, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8\} \\ &= \langle x \rangle \text{ as required.} \end{aligned}$$

$$\begin{aligned} \text{(b)} \quad & y\langle x \rangle y^{-1} \\ &= y\{1, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8\}y^{-1} \\ &= \{yy^{-1}, yxy^{-1}, yx^2y^{-1}, yx^3y^{-1}, yx^4y^{-1}, yx^5y^{-1}, yx^6y^{-1}, yx^7y^{-1}, yx^8y^{-1}\} \\ &= \{1, x^4, (x^4)^2, (x^4)^3, (x^4)^4, (x^4)^5, (x^4)^6, (x^4)^7, (x^4)^8\} \\ &\quad (\text{because } y(x^i)y^{-1} = (yxy^{-1})(yxy^{-1})\dots(yxy^{-1}) \text{ (} i \text{ times)} = (x^4)^i) \\ &= \{1, x^4, x^8, x^{12} = x^3, x^{16} = x^7, x^{20} = x^2, x^{24} = x^6, x^{28} = x, x^{32} = x^5\} \\ &= \{1, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8\} \\ &= \langle x \rangle \text{ as required.} \end{aligned}$$

It now follows that  $\langle x \rangle$  is a **normal subgroup** of  $P$ .

To show that  $x^3$  is in the centre of  $P$ , we need to show that  $px^3p^{-1} = x^3$  for all  $p \in P$ . By the same sort of argument as above, this can be achieved by showing that  $x(x^3)x^{-1} = x^3$  and that  $y(x^3)y^{-1} = x^3$ . The first bit follows immediately — and we note from the above calculations that

$$yx^3y^{-1} = (x^4)^3 = x^{12} = x^3 \text{ as required.}$$

It therefore follows that  $x^3$  is an element of  $Z(P)$ . Further, the subgroup generated by  $x^3$ ,  $\langle x^3 \rangle$ , is a *normal* subgroup because (using the same methods as before and using the calculations written down above)  $x\langle x^3 \rangle x^{-1} = \langle x^3 \rangle$  and  $y\langle x^3 \rangle y^{-1} = \langle x^3 \rangle$ , where  $\langle x^3 \rangle = \{1, x^3, x^6\}$ .

It therefore follows that  $P \geq \langle x \rangle \geq \langle x^3 \rangle \geq \{1\}$  is a normal series for  $P$  (as we have shown that  $\langle x \rangle$  and  $\langle x^3 \rangle$  are normal subgroups of  $P$ ). As in Exercise 18-2, because the quotient groups  $P/\langle x \rangle$  and  $\langle x \rangle/\langle x^3 \rangle$  are *cyclic of order 3*, a prime number, then the normal series that we are considering cannot be refined between any of its elements — and thus  $P \geq \langle x \rangle \geq \langle x^3 \rangle \geq \{1\}$  must be a **chief series** for  $P$ . QED.

# Chapter 19: Semidirect Products and Wreath Products

## Key Definitions and Results

**Definition 19.1:** A group  $G$  is a *semidirect product* of a subgroup  $N$  by a subgroup  $H$  if the following conditions are satisfied: (i)  $G = NH$ ; (ii)  $N$  is a *normal* subgroup of  $G$ ; and (iii)  $H \cap N = \{1\}$ .

**Proposition 19.4:** Let  $G$  be a *semidirect product* of  $N$  by  $H$ . For each element  $h$  of  $H$ , the map  $\varphi_h: N \rightarrow N$  defined by  $\varphi_h(n) = hnh^{-1}$  is an *automorphism* of  $N$ . The map  $\varphi: H \rightarrow \text{Aut}(N)$  defined by  $\varphi(h) = \varphi_h$  is a *homomorphism*.

**Proposition 19.5:** Given any groups  $N$  and  $H$ , and a *homomorphism* from  $H$  to  $\text{Aut}(N)$  for which the image of  $h$  is denoted by  $\varphi_h$ , let  $G$  be the set of ordered pairs  $\{(n, h): n \in N, h \in H\}$ . Then  $G$  is a **group** under the multiplication defined by  $(n_1, h_1)(n_2, h_2) = (n_1\varphi_{h_1}(n_2), h_1h_2)$ . The sets  $N_0 = \{(n, 1): n \in N\}$  and  $H_0 = \{(1, h): h \in H\}$  are *subgroups* of  $G$  isomorphic to  $N$  and  $H$ , respectively, and  $G$  is a *semidirect product* of  $N_0$  by  $H_0$ .

**Example 19.6:** One *natural example* of the construction of Proposition 19.5 arises when  $H$  is equal to  $\text{Aut}(N)$  and the map  $\varphi$  is the identity map from  $H (= \text{Aut}(N))$  to  $\text{Aut}(N)$  so that  $\varphi(\phi) = \phi$ . The resulting semidirect product is known as the *holomorph* of  $N$ .

**Remark:** As with internal direct products, it is often convenient to drop the *ordered pair notation*, and write elements of a semidirect product of  $N$  by  $H$  by juxtaposing elements of  $N$  and  $H$ . In this notation, the definition of *multiplication* becomes  $n_1h_1n_2h_2 = n_1\varphi_{h_1}(n_2)h_1h_2$ .

**Definition 19.8:** Let  $G$  and  $H$  be *any two finite groups*. The regular wreath product  $G \text{ rwr } H$  is a semidirect product of the group  $N$  by  $H$ , where  $N$  is  $G^{|H|}$ , the direct product of  $|H|$  copies of  $G$ . Thus, if  $|H| = n$ , then the elements of  $N$  are *n-tuples* of the form  $(g_1, g_2, \dots, g_n)$ , with each  $g_i$  in  $G$ . Now to specify the **extension**, choose some fixed ordering  $h_1, h_2, \dots, h_n$  of the elements of  $H$ . The automorphism  $\varphi_h$  of  $G^n$  associated with an element  $h$  of  $H$  is then *defined by*

$$\varphi_h(g_1, g_2, \dots, g_n) = (g_{\pi(1)}, g_{\pi(2)}, \dots, g_{\pi(n)}),$$

where  $\pi$  is the permutation of  $\{1, \dots, n\}$  defined by  $hh_i = h_{\pi(i)}$ . It may be checked that  $\varphi_h\varphi_k = \varphi_{hk}$ . Thus the map  $H \rightarrow \text{Aut}(G^n)$  determined by  $h \mapsto \varphi_h$  is a *homomorphism*. The semidirect product is therefore *well-defined*. Note that the number of elements in  $G \text{ rwr } H$  is  $n|G|^n$ , where  $n = |H|$ .

**Proposition 19.10:** Let  $p$  be a prime integer, and let  $k$  be *any positive integer*. The Sylow  $p$ -subgroup of the symmetric group  $S(p^k)$  is the **iterated wreath product** (with  $k$  copies of  $C_p$ )

$$(\dots((C_p \text{ rwr } C_p) \text{ rwr } C_p) \dots \text{ rwr } C_p).$$

**Corollary 19.11:** Let  $p$  be a prime and let  $n$  be *any positive integer*. Let

$$n = a_0 + a_1p + a_2p^2 + \dots + a_kp^k \text{ (with } 0 \leq a_i \leq p-1)$$

be the *expansion* of  $n$  to the base  $p$ . Then each Sylow  $p$ -subgroup of the symmetric group  $S(n)$  is a *direct product*  $(S_1)^{a_1} \times (S_2)^{a_2} \times \dots \times (S_k)^{a_k}$ , where  $S_i$  is a *Sylow  $p$ -subgroup* of the symmetric group  $S(p^i)$ , so that  $S_i$  is the *regular wreath product* of  $i$  copies of  $C_p$ .

**Definition 19.12:** Let  $G$  and  $H$  be *finite groups* with  $H$  a subgroup of the symmetric group  $S(n)$ . The *permutation wreath product*,  $G \text{ pwr } H$ , is the semidirect product of a normal subgroup  $N$  by  $H$ , where  $N$  is the direct product of  $n$  copies of  $G$ . Thus, the elements of  $N$  are  $n$ -tuples  $(g_1, g_2, \dots, g_n)$ , with each  $g_i$  in  $G$ . The automorphism  $\phi_h$  of  $G^n$  associated with a permutation  $h$  in  $H$  is then *defined by*  $\phi_h(g_1, g_2, \dots, g_n) = (g_{h(1)}, g_{h(2)}, \dots, g_{h(n)})$ .

**Remark 1:** In the above construction,  $H$  acts by *conjugation* on  $N$ , permuting the  $n$  direct factors. Since the map  $H \rightarrow \text{Aut}(G^n)$  determined by  $h \mapsto \phi_h$  is easily checked to be a *homomorphism*, the semidirect product is *well-defined*. Note that the number of elements in  $G \text{ pwr } H$  is  $|H||G|^n$ .

**Remark 2:** The regular wreath product may be regarded as a *special case* of the permutation wreath product. In this case,  $H$  is regarded in its *regular* permutation representation as a subset of  $S(|H|)$  in which the permutation  $\pi_h$  associated with an element  $h$  of  $H = \{h_1, \dots, h_n\}$  is defined by  $\pi_h(h_i) = hh_i$ . In general, these two constructions have *different orders*. For example, if  $H = S(3)$ , then the group  $G \text{ rwr } H$  would have order  $6|G|^6$ , whereas  $G \text{ pwr } H$  would have order  $6|G|^3$ .

## Exercises

**19-1:** Let each of  $G$ ,  $H$  and  $K$  be *finite non-trivial groups*. Explain why the wreath product  $(G \text{ rwr } (H \text{ rwr } K))$  cannot possibly be *isomorphic* to the wreath product  $((G \text{ rwr } H) \text{ rwr } K)$ .

**Answer:** In Definition 19.8, we found out that the number of elements in  $G \text{ rwr } H$  is given by  $|H||G|^{|H|}$ . It follows that the number of elements in the **first** wreath product,  $(G \text{ rwr } (H \text{ rwr } K))$ , is given by  $(|K||H|^{|K|})|G|^{|K||H|^{|K|}}$ ; and that the number of elements in the **second** wreath product,  $((G \text{ rwr } H) \text{ rwr } K)$ , is given by  $|K|(|H||G|^{|H|})^{|K|}$ . Assuming that the two wreath products are isomorphic, then they must have the same number of elements. It follows that

$$\begin{aligned} (|K||H|^{|K|})|G|^{|K||H|^{|K|}} &= |K|(|H||G|^{|H|})^{|K|}; \\ (|K||H|^{|K|})|G|^{|K||H|^{|K|}} &= |K|(|H|^{|K|}|G|^{|H||K|}); \\ (|K||H|^{|K|})|G|^{|K||H|^{|K|}} &= (|K||H|^{|K|})|G|^{|H||K|}; \\ |G|^{|K||H|^{|K|}} &= |G|^{|H||K|}; \\ |G|^{|H||K|} &= |G|^{|H|}; \end{aligned}$$

As  $G$ ,  $H$  and  $K$  are finite **non-trivial** groups, then it follows that  $|G|^{|H||K|} \neq |G|^{|H|}$ , and therefore the two wreath products  $(G \text{ rwr } (H \text{ rwr } K))$  and  $((G \text{ rwr } H) \text{ rwr } K)$  cannot *possibly* be isomorphic, as they will have different orders. QED.

**19-5:** Construct all *semidirect products* of  $C_3 \times C_3$ .

**Answer:** Consider all possible semidirect products  $G$  of  $N = C_3 = \{1, y, y^2\}$  by  $H = C_3 = \{1, x, x^2\}$ . Looking at Proposition 19.5, we need to associate an automorphism of  $N$  to the elements  $1, x$  and  $x^2$  of  $H$ .

Let us first consider what the elements of the group  $\text{Aut}(N)$  are. Since the automorphism associated to  $1$  must be the identity, we only have two choices to make: to either define  $\varphi(y) = y$  or to define  $\varphi(y) = y^2$ . Therefore, the group  $\text{Aut}(N)$  consists of two elements:

$$\begin{aligned} \alpha: & \quad \alpha(1) = 1, \alpha(y) = y, \alpha(y^2) = y^2; \text{ and} \\ \beta: & \quad \beta(1) = 1, \beta(y) = y^2, \beta(y^2) = y, \end{aligned}$$

with the compositions  $\alpha \circ \alpha = \alpha$ ,  $\alpha \circ \beta = \beta$ ,  $\beta \circ \alpha = \beta$  and  $\beta \circ \beta = \alpha$  ( $\text{Aut}(N)$  is *isomorphic* to  $C_2$ , with  $\beta$  being the ‘generator’ of  $\text{Aut}(N)$ ).

We must now define a homomorphism from  $H$  to  $\text{Aut}(N)$  for which the image of  $h$  in  $H$  is denoted by  $\varphi_h$ . There are eight choices for the homomorphism in all, summarised by the following table:

choice		h ∈ H		
		1	x	x <sup>2</sup>
1	$\varphi_h$	$\alpha$	$\alpha$	$\alpha$
2	$\varphi_h$	$\alpha$	$\alpha$	$\beta$
3	$\varphi_h$	$\alpha$	$\beta$	$\alpha$
4	$\varphi_h$	$\alpha$	$\beta$	$\beta$

choice		h ∈ H		
		1	x	x <sup>2</sup>
5	$\varphi_h$	$\beta$	$\alpha$	$\alpha$
6	$\varphi_h$	$\beta$	$\alpha$	$\beta$
7	$\varphi_h$	$\beta$	$\beta$	$\alpha$
8	$\varphi_h$	$\beta$	$\beta$	$\beta$

But only choice 1 is valid because all the other choices are not *valid homomorphisms*: using the compositions for  $\alpha$  and  $\beta$ , we see that choices 2 and 3 are not valid because  $\varphi_1 = \varphi_{x \times x^2} \neq \varphi_x \varphi_{x^2}$ ; choice 4 is not valid because  $\varphi_{x^2} = \varphi_{x \times x} \neq \varphi_x \varphi_x$ ; and choices 5 to 8 are not valid because  $\varphi_1 = \varphi_{1 \times 1} \neq \varphi_1 \varphi_1$ . This leaves us with only **one** valid homomorphism, choice 1, the identity homomorphism, given by  $\varphi_1 = \alpha$ ,  $\varphi_x = \alpha$ , and  $\varphi_{x^2} = \alpha$ .

It follows that there is only **one** semidirect product of  $C_3 \times C_3$ , and it is given by the group  $G$  consisting of the ordered pairs  $\{(n, h): n \in N, h \in H\}$ , with multiplication defined by

$$\begin{aligned} (n_1, h_1)(n_2, h_2) &= (n_1 \varphi_{h_1}(n_2), h_1 h_2) = (n_1 n_2, h_1 h_2) \\ & \text{(because } \varphi_{h_1} \text{ is the identity homomorphism).} \end{aligned}$$

It now follows that our semidirect product is the internal direct product  $C_3 \times C_3$  (with nine elements).

## Chapter 20: Extensions

### Key Definitions and Results

**Definition 20.1:** A group  $G$  is an *extension* of  $N$  by  $H$  if  $G$  has a *normal subgroup*  $N$  such that the *quotient group*  $G/N$  is *isomorphic* to  $H$ .

**Remark:** Suppose that  $G$  is a *semidirect product* of  $N$  by  $H$ . The First Isomorphism Theorem shows that  $G/N = HN/N \cong H/H \cap N \cong H$ , so that  $G$  is an *extension* of  $N$  by  $H$ .

**Definition 20.4:** Let  $G$  be an extension of  $N$  by  $H$  with  $\phi: H \rightarrow G/N$  an isomorphism. A *section* of  $G$  through  $H$  is any set  $\{s(h): h \in H\}$  of elements of  $G$  such that: (i)  $s(1) = 1$ ; and (ii)  $s(h)$  is a representative for the *right coset*  $\phi(h)$ , so that  $\phi(h) = Ns(h)$ .

**Remark:** If  $G$  is a semidirect product of  $N$  by  $H$ , then the elements of  $H$  are a *section* of  $G$  through  $H$  which is a *subgroup*.

**Remark:** Let  $G$  be an extension of  $N$  by  $H$  with  $\phi: H \rightarrow G/N$  an *isomorphism*. Since  $\phi$  is an isomorphism, for any elements  $h_1$  and  $h_2$  of  $H$ ,  $s(h_1)s(h_2)$  is in the *same* right coset as  $s(h_1h_2)$ , and so there exists an element  $f(h_1, h_2)$  in  $N$  such that  $s(h_1)s(h_2) = f(h_1, h_2)s(h_1h_2)$ .

**Definition 20.6:** Let  $G$  be an extension of  $N$  by  $H$  with  $\{s(h): h \in H\}$  a section of  $G$  through  $H$ . The map  $f: H \times H \rightarrow N$  defined by  $f(h_1, h_2) = s(h_1)s(h_2)(s(h_1h_2))^{-1}$ , for all  $h_1$  and  $h_2$  in  $H$ , is the *sectional factor set* for the extension  $G$ , with section  $\{s(h): h \in H\}$ .

**Remark:** It is clear that in general the sectional factor set depends on the *choice* of section. If  $G$  is a semidirect product of  $N$  by  $H$ , taking the section to be the elements of  $H$ , then there is a sectional factor set such that  $f(h_1, h_2) = 1$  for all  $h_1, h_2 \in H$ .

**Remark:** Recall that sometimes we use *exponential notation* for conjugation, so that  $x^g$  denotes the product  $gxg^{-1}$ .

**Proposition 20.8:** Let  $G$  be an *extension* of  $N$  by  $H$ , and let  $\{s(h)\}$  be a *section* of  $G$  through  $H$ . The *sectional factor set*  $f: H \times H \rightarrow N$  for the extension satisfies the following conditions: (i) for all  $h$  in  $H$ ,  $f(1, h) = 1 = f(h, 1)$ ; and (ii) for all  $h_1, h_2, h_3 \in H$ ,  $f(h_1, h_2)f(h_1h_2, h_3) = f(h_2, h_3)^{s(h_1)}f(h_1, h_2h_3)$ .

**Proposition 20.9:** Let  $G$  be an *extension* of  $N$  by  $H$  with  $\{s(h): h \in H\}$  a *section* of  $G$  through  $H$ , and let  $f$  be the *sectional factor set* of the extension. For each  $h$  in  $H$ , the map  $\phi_h: N \rightarrow N$  defined by  $\phi_h(n) = s(h)n(s(h))^{-1} = n^{s(h)}$  is an *automorphism* of  $N$ . Furthermore, for all  $n$  in  $N$  and for all  $h_1$  and  $h_2$  in  $H$ , we have  $\phi_{h_1}\phi_{h_2}(n) = (\phi_{h_1h_2}(n))^{f(h_1, h_2)}$ .

**Definition 20.10:** Given groups  $N$  and  $H$ , for each  $h$  in  $H$ , let  $\varphi_h$  be an *automorphism* of  $N$  (with  $\varphi_1$  being the *trivial* automorphism). A factor set with respect to the choice  $\{\varphi_h: h \in H\}$  is a map  $f: H \times H \rightarrow N$  such that (i) for all  $h$  in  $H$ ,  $f(1, h) = 1 = f(h, 1)$ ; and (ii) for all  $h_1, h_2$  and  $h_3$  in  $H$ ,  $f(h_1, h_2)f(h_1h_2, h_3) = \varphi_{h_1}(f(h_2, h_3))f(h_1, h_2h_3)$ . We shall say that a factor set  $f$  is *compatible* if also (iii) for all  $n$  in  $N$  and  $h_1, h_2$  in  $H$ ,  $\varphi_{h_1}\varphi_{h_2}(n) = \varphi_{h_1h_2}(n)^{f(h_1, h_2)}$ .

**Remark:** Let  $G$  be an *extension* of  $N$  by  $H$ , and let  $\{s(h): h \in H\}$  be a *section* of  $G$  through  $H$ . By Proposition 20.9, *conjugation* by an element  $s(h)$  of  $G$  is an automorphism  $\varphi_h$  of  $N$  (with conjugation by  $s(1)$  being the *trivial* automorphism). Propositions 20.8 and 20.9 show that the sectional factor set for this extension is then a *compatible factor set* in our newly defined sense.

**Proposition 20.11:** Given groups  $N$  and  $H$ , for each  $h$  in  $H$ , let  $\varphi_h$  be an automorphism of  $N$ , with  $\varphi_1$  being the *identity* map on  $N$ . Suppose that  $f: H \times H \rightarrow N$  is a compatible factor set. Then the set  $G$  of *ordered pairs*  $\{(n, h): n \in N, h \in H\}$  is a group under the multiplication

$$(n_1, h_1)(n_2, h_2) = (n_1\varphi_{h_1}(n_2)f(h_1, h_2), h_1h_2).$$

Furthermore,  $G$  is an extension of a group *isomorphic* to  $N$  by a group *isomorphic* to  $H$ , and  $\{(1, h): h \in H\}$  is a *section* of  $G$  through  $H$ .

**Corollary 20.12:** Let  $G$  be an extension of  $N$  by  $H$ , and let  $\{s(h): h \in H\}$  be a *section* of  $G$  through  $H$ . Let  $f$  be the corresponding *sectional factor set*. Then, if we define  $\varphi_h$  to be conjugation by  $s(h)$ ,  $f$  is a *compatible* factor set. Conversely, given *automorphisms*  $\{\varphi_h: h \in H\}$  of  $N$  and a compatible factor set  $f$ , let  $G$  be the group constructed as in Proposition 20.11. Then  $\{(1, h): h \in H\}$  is a *section* of  $G$  through  $H$ . The map  $N_0 \rightarrow N_0$  defined by  $(h, 1) \mapsto (\varphi_h, 1)$  is conjugation by  $(1, h)$ , and  $f$  is a *sectional factor set*.

**Remark:** It is not in general obvious how to *find* a compatible factor set when  $N$ ,  $H$  and the automorphisms  $\{\varphi_h: h \in H\}$  are given. This is one reason why various *restrictions* are placed on the type of extensions considered. We consider two of these possibilities in the next chapter. If the map  $h \mapsto \varphi_h$  is a homomorphism, then the trivial factor set is *compatible*, and the resulting extension is a *semidirect product*.

## Exercises

**20-1:** When  $G$  is the group  $S(3)$ , regarded as an *extension* of  $A(3)$  by  $C_2$ , determine all the possible *sectional factor sets* of the extension.

**Answer:** Let us first familiarise ourselves with the groups that we are dealing with:

$$S(3) = \{(1), (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\};$$

$$A(3) = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}; \text{ and}$$

$$C_2 = \{1, x\}.$$

As we have assumed that  $S(3)$  is an extension of  $A(3)$  by  $C_2$ , it follows that there is an *isomorphism*  $\phi: C_2 \rightarrow S(3)/A(3)$ . The two elements of the quotient group  $S(3)/A(3)$  are  $A(3)$  itself and  $A(3)g$ , where  $g$  is not an element of  $A(3)$ . Therefore, taking  $g$  to be  $(1\ 2)$  (without loss of generality), we find that the group  $S(3)/A(3)$  can be written as

$$\begin{aligned} S(3)/A(3) &= \{ \{(1), (1\ 2\ 3), (1\ 3\ 2)\}, \{(1), (1\ 2\ 3), (1\ 3\ 2)\}(1\ 2) \} \\ &= \{ \{(1), (1\ 2\ 3), (1\ 3\ 2)\}, \{(1\ 2), (1\ 2\ 3)(1\ 2), (1\ 3\ 2)(1\ 2)\} \} \\ &= \{ \{(1), (1\ 2\ 3), (1\ 3\ 2)\}, \{(1\ 2), (2\ 3), (1\ 3)\} \}. \end{aligned}$$

Now in any isomorphism, the identity element maps onto the identity element, so that we must have  $\phi(1_{C_2}) = 1_{S(3)/A(3)}$ ; or  $\phi(1) = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ . This leaves us no choice but to define  $\phi(x) = \{(1\ 2), (2\ 3), (1\ 3)\}$ .

The next step is to ask ourselves what elements might form part of a section of  $S(3)$  through  $C_2$ . By definition, a section of this type is any set  $\{s(z): z \in C_2\}$  of elements of  $S(3)$  such that (i)  $s(1) = 1$ ; and (ii)  $s(z)$  is a representative for the right coset  $\phi(z)$ , so that  $\phi(z) = Ns(z)$ . From the definition, it follows that in this example such a section will have *two* elements, and it also follows that we will have  $s(1) = 1_{S(3)} = (1)$ .

The only remaining choice is the choice of the right coset representative of  $\phi(x)$  to assign to  $s(x)$ . As  $\phi(x) = \{(1\ 2), (2\ 3), (1\ 3)\}$ , then there are **three** possible right coset representatives, so that there are three possible *sections*:

- (a)  $\{(1), (1\ 2)\}$ ;
- (b)  $\{(1), (2\ 3)\}$ ; and
- (c)  $\{(1), (1\ 3)\}$ .

Let us now go on to find the three sectional factor sets corresponding to the three sections shown above. By Definition 20.6, the map  $f: C_2 \times C_2 \rightarrow A(3)$  defined by  $f(z_1, z_2) = s(z_1)s(z_2)(s(z_1z_2))^{-1}$ , for all  $z_1$  and  $z_2$  in  $C_2$ , is the *sectional factor set* for the extension  $G = S(3)$ , with section given by  $\{s(h): h \in H\}$ . Let us now apply this definition to our three sections to find three sectional factor sets.

Section (a): With  $f(1) = (1)$  and  $f(x) = (1\ 2)$ , we have

$$\begin{aligned} f(1, 1) &= s(1)s(1)(s(1 \times 1))^{-1} = (1)(1)(s(1))^{-1} = (1)(1)((1))^{-1} = (1)(1)(1) = (1); \\ f(1, x) &= s(1)s(x)(s(1 \times x))^{-1} = (1)(1\ 2)(s(x))^{-1} = (1)(1\ 2)((1\ 2))^{-1} = (1)(1\ 2)(2\ 1) = (1); \\ f(x, 1) &= s(x)s(1)(s(x \times 1))^{-1} = (1\ 2)(1)(s(x))^{-1} = (1\ 2)(1)((1\ 2))^{-1} = (1\ 2)(1)(2\ 1) = (1); \text{ and} \\ f(x, x) &= s(x)s(x)(s(x \times x))^{-1} = (1\ 2)(1\ 2)(s(1))^{-1} = (1\ 2)(1\ 2)((1))^{-1} = (1\ 2)(1\ 2)(1) = (1). \end{aligned}$$

Section (b): With  $f(1) = (1)$  and  $f(x) = (2\ 3)$ , we have

$$\begin{aligned} f(1, 1) &= s(1)s(1)(s(1 \times 1))^{-1} = (1)(1)(s(1))^{-1} = (1)(1)((1))^{-1} = (1)(1)(1) = (1); \\ f(1, x) &= s(1)s(x)(s(1 \times x))^{-1} = (1)(2\ 3)(s(x))^{-1} = (1)(2\ 3)((2\ 3))^{-1} = (1)(2\ 3)(3\ 2) = (1); \\ f(x, 1) &= s(x)s(1)(s(x \times 1))^{-1} = (2\ 3)(1)(s(x))^{-1} = (2\ 3)(1)((2\ 3))^{-1} = (2\ 3)(1)(3\ 2) = (1); \text{ and} \\ f(x, x) &= s(x)s(x)(s(x \times x))^{-1} = (2\ 3)(2\ 3)(s(1))^{-1} = (2\ 3)(2\ 3)((1))^{-1} = (2\ 3)(2\ 3)(1) = (1). \end{aligned}$$

Section (c): With  $f(1) = (1)$  and  $f(x) = (1\ 3)$ , we have

$$\begin{aligned} f(1, 1) &= s(1)s(1)(s(1 \times 1))^{-1} = (1)(1)(s(1))^{-1} = (1)(1)((1))^{-1} = (1)(1)(1) = (1); \\ f(1, x) &= s(1)s(x)(s(1 \times x))^{-1} = (1)(1\ 3)(s(x))^{-1} = (1)(1\ 3)((1\ 3))^{-1} = (1)(1\ 3)(3\ 1) = (1); \\ f(x, 1) &= s(x)s(1)(s(x \times 1))^{-1} = (1\ 3)(1)(s(x))^{-1} = (1\ 3)(1)((1\ 3))^{-1} = (1\ 3)(1)(3\ 1) = (1); \text{ and} \\ f(x, x) &= s(x)s(x)(s(x \times x))^{-1} = (1\ 3)(1\ 3)(s(1))^{-1} = (1\ 3)(1\ 3)((1))^{-1} = (1\ 3)(1\ 3)(1) = (1). \end{aligned}$$

As you can see, all the sectional factor sets are trivial, and this is to be expected as the three sets  $\{(1), (1\ 2)\}$ ,  $\{(1), (2\ 3)\}$  and  $\{(1), (1\ 3)\}$  are subgroups of  $S(3)$ .

**20-3:** Find *all extensions* of a cyclic group of order 2 by a cyclic group of order 3.

**Answer:** Let  $N = C_2 = \{1, x\}$ , and let  $H = C_3 = \{1, y, y^2\}$ . According to Proposition 20.11, in order to construct an extension of  $C_2$  by  $C_3$ , we first need to find a compatible factor set  $f: H \times H \rightarrow N$ . In order to do this, we need to choose an automorphism of  $N$  to associate to each element of  $H$ , and then need to define a map  $f: H \times H \rightarrow N$  such that the *three* conditions of Definition 20.10 are satisfied (we need a *compatible* factor set):

- (i) for all  $h$  in  $H$ ,  $f(1, h) = 1 = f(h, 1)$ ;
- (ii) for all  $h_1, h_2$  and  $h_3$  in  $H$ ,  $f(h_1, h_2)f(h_1h_2, h_3) = \varphi_{h_1}(f(h_2, h_3))f(h_1, h_2h_3)$ ; and
- (iii) for all  $n$  in  $N$ , and for all  $h_1, h_2$  in  $H$ ,  $\varphi_{h_1}\varphi_{h_2}(n) = \varphi_{h_1h_2}(n)^{f(h_1, h_2)}$ .

Because  $N = C_2$ , then there is only one element in  $\text{Aut}(N)$ , this element being the identity automorphism,  $\varphi(1) = 1$ , and  $\varphi(x) = x$ . Therefore, each element of  $H$  will be associated to the identity automorphism of  $N$ , so that if we denote the identity automorphism by  $\varphi_1$ , then we have

$$\varphi_1 = \varphi_y = \varphi_{y^2}.$$

We now move on to defining the map  $f: H \times H \rightarrow N$ . To do this, we need to associate an element of  $N = C_2 = \{1, x\}$  to each element of  $H \times H = C_3 \times C_3 = \{(1, 1), (1, y), (1, y^2), (y, 1), (y, y), (y, y^2), (y^2, 1), (y^2, y), (y^2, y^2)\}$ . Now condition (i) of Definition 20.10 forces us to define  $f(1, 1) = f(1, y) = f(1, y^2) = f(y, 1) = f(y^2, 1) = 1$ .

Because we are only dealing with *identity automorphisms*, then condition (ii) of Definition 20.10 simplifies to the following condition:

$$\text{For all } h_1, h_2 \text{ and } h_3 \text{ in } H, \text{ we require that } f(h_1, h_2)f(h_1h_2, h_3) = f(h_2, h_3)f(h_1, h_2h_3).$$

Putting in  $h_1 = h_2 = h_3 = y$ , we see that we need  $f(y, y)f(y^2, y) = f(y, y)f(y, y^2)$ ; or  $f(y^2, y) = f(y, y^2)$ ;

and putting in  $h_1 = h_2 = y, h_3 = y^2$ , we see that we need  $f(y, y)f(y^2, y^2) = f(y, y^2)f(y, 1)$ ; or  $f(y, y)f(y^2, y^2) = f(y, y^2)$  (because  $f(y, 1) = 1$ ).

The above eliminates 12 of the  $2^4 = 16$  possible definitions for  $f$ .

It follows that the remaining possible definitions for  $f$  are as follows:

$k \in H \times H$	$f(k)$			
	Definition A	Definition B	Definition C	Definition D
(1, 1)	1	1	1	1
(1, y)	1	1	1	1
(1, y <sup>2</sup> )	1	1	1	1
(y, 1)	1	1	1	1
(y, y)	1	1	x	x
(y, y <sup>2</sup> )	1	x	1	x
(y <sup>2</sup> , 1)	1	1	1	1
(y <sup>2</sup> , y)	1	x	1	x
(y <sup>2</sup> , y <sup>2</sup> )	1	x	x	1

Condition (iii) of Definition 20.10 does not eliminate any of the above definitions for  $f$  (because  $1^{-1} = 1$ ,  $x^{-1} = x$ , and  $x^2 = 1$  in  $C_2$ ), so we conclude that there are **four** possible compatible factor sets  $f$  for use with Proposition 20.11. So let us now consider the multiplication tables for  $G$  as defined in Proposition 20.11 for the above four factor sets A, B, C and D:

**Definition A**

	(1, 1)	(1, y)	(1, y <sup>2</sup> )	(x, 1)	(x, y)	(x, y <sup>2</sup> )
(1, 1)	(1, 1)	(1, y)	(1, y <sup>2</sup> )	(x, 1)	(x, y)	(x, y <sup>2</sup> )
(1, y)	(1, y)	(1, y <sup>2</sup> )	(1, 1)	(x, y)	(x, y <sup>2</sup> )	(x, 1)
(1, y <sup>2</sup> )	(1, y <sup>2</sup> )	(1, 1)	(1, y)	(x, y <sup>2</sup> )	(x, 1)	(x, y)
(x, 1)	(x, 1)	(x, y)	(x, y <sup>2</sup> )	(1, 1)	(1, y)	(1, y <sup>2</sup> )
(x, y)	(x, y)	(x, y <sup>2</sup> )	(x, 1)	(1, y)	(1, y <sup>2</sup> )	(1, 1)
(x, y <sup>2</sup> )	(x, y <sup>2</sup> )	(x, 1)	(x, y)	(1, y <sup>2</sup> )	(1, 1)	(1, y)

**Definition B**

	(1, 1)	(1, y)	(1, y <sup>2</sup> )	(x, 1)	(x, y)	(x, y <sup>2</sup> )
(1, 1)	(1, 1)	(1, y)	(1, y <sup>2</sup> )	(x, 1)	(x, y)	(x, y <sup>2</sup> )
(1, y)	(1, y)	(1, y <sup>2</sup> )	(x, 1)	(x, y)	(x, y <sup>2</sup> )	(1, 1)
(1, y <sup>2</sup> )	(1, y <sup>2</sup> )	(x, 1)	(x, y)	(x, y <sup>2</sup> )	(1, 1)	(1, y)
(x, 1)	(x, 1)	(x, y)	(x, y <sup>2</sup> )	(1, 1)	(1, y)	(1, y <sup>2</sup> )
(x, y)	(x, y)	(x, y <sup>2</sup> )	(1, 1)	(1, y)	(1, y <sup>2</sup> )	(x, 1)
(x, y <sup>2</sup> )	(x, y <sup>2</sup> )	(1, 1)	(1, y)	(1, y <sup>2</sup> )	(x, 1)	(x, y)

**Definition C**

	(1, 1)	(1, y)	(1, y <sup>2</sup> )	(x, 1)	(x, y)	(x, y <sup>2</sup> )
(1, 1)	(1, 1)	(1, y)	(1, y <sup>2</sup> )	(x, 1)	(x, y)	(x, y <sup>2</sup> )
(1, y)	(1, y)	(x, y <sup>2</sup> )	(1, 1)	(x, y)	(1, y <sup>2</sup> )	(x, 1)
(1, y <sup>2</sup> )	(1, y <sup>2</sup> )	(1, 1)	(x, y)	(x, y <sup>2</sup> )	(x, 1)	(1, y)
(x, 1)	(x, 1)	(x, y)	(x, y <sup>2</sup> )	(1, 1)	(1, y)	(1, y <sup>2</sup> )
(x, y)	(x, y)	(1, y <sup>2</sup> )	(x, 1)	(1, y)	(x, y <sup>2</sup> )	(1, 1)
(x, y <sup>2</sup> )	(x, y <sup>2</sup> )	(x, 1)	(1, y)	(1, y <sup>2</sup> )	(1, 1)	(x, y)

**Definition D**

	(1, 1)	(1, y)	(1, y <sup>2</sup> )	(x, 1)	(x, y)	(x, y <sup>2</sup> )
(1, 1)	(1, 1)	(1, y)	(1, y <sup>2</sup> )	(x, 1)	(x, y)	(x, y <sup>2</sup> )
(1, y)	(1, y)	(x, y <sup>2</sup> )	(x, 1)	(x, y)	(1, y <sup>2</sup> )	(1, 1)
(1, y <sup>2</sup> )	(1, y <sup>2</sup> )	(x, 1)	(1, y)	(x, y <sup>2</sup> )	(1, 1)	(x, y)
(x, 1)	(x, 1)	(x, y)	(x, y <sup>2</sup> )	(1, 1)	(1, y)	(1, y <sup>2</sup> )
(x, y)	(x, y)	(1, y <sup>2</sup> )	(1, 1)	(1, y)	(x, y <sup>2</sup> )	(x, 1)
(x, y <sup>2</sup> )	(x, y <sup>2</sup> )	(1, 1)	(x, y)	(1, y <sup>2</sup> )	(x, 1)	(1, y)

Note that the entries in tables B, C and D which are different from the entries in table A are marked in red.

We see from the above tables that the group  $G$  with factor set A is cyclic of order 6 (*generated* by the element  $(x, y)$ , for instance); that the group  $G$  with factor set B is cyclic of order 6 (*generated* by the element  $(1, y)$ , for instance); that the group  $G$  with factor set C is cyclic of order 6 (*generated* by the element  $(1, y)$ , for instance); and that the group  $G$  with factor set D is also cyclic of order 6 (*generated* by the element  $(1, y^2)$ , for instance). We therefore conclude that *any of the four possible extensions* of a cyclic group of order 2 by a cyclic group of order 3 is a cyclic group of order 6, i.e. we have a direct product  $C_2 \times C_3 \cong C_6$ .

# Chapter 21: Central and Cyclic Extensions

## Key Definitions and Results

**Definition 21.1:** A group  $G$  is a *central extension* of  $N$  by  $H$  if it is an extension of  $N$  by  $H$  and  $N$  is in the *centre* of  $G$ . Suppose that we are given such a central extension  $G$ , with section  $\{s(h)\}$ . Since  $s(h)$  will **commute** with each element of  $N$ , the sectional factor set of the extension satisfies (by Proposition 20.8) the conditions (i) for all  $h$  in  $H$ ,  $f(1, h) = 1 = f(h, 1)$ ; (ii) for all  $h_1, h_2, h_3$  in  $H$ ,  $f(h_1, h_2)f(h_1h_2, h_3) = f(h_2, h_3)f(h_1, h_2h_3)$ . We shall refer to a factor set satisfying these two conditions as a *central factor set*.

Suppose now that we wish to *construct* a central extension of  $N$  by  $H$ . To do this, we choose each automorphism  $\{\phi_h: h \in H\}$  to be the **identity** automorphism of  $N$ . The compatibility condition then holds for *trivial* reasons and the factor set conditions become the requirements that  $f$  be a central factor set: (i) for all  $h$  in  $H$ ,  $f(1, h) = 1 = f(h, 1)$ ; and (ii) for all  $h_1, h_2, h_3$  in  $H$ ,  $f(h_1, h_2)f(h_1h_2, h_3) = f(h_2, h_3)f(h_1, h_2h_3)$ .

**Definition 21.4:** The second special type of extension which we consider is that of a *cyclic extension* of  $N$  by  $H$ . This occurs when  $H$  is a cyclic group. In the case of cyclic extensions, it is possible to give an *explicit* description which enables one to determine the extensions of  $N$  by  $H$ .

**Theorem 21.5:** Let  $G$  be an *extension* of a group  $N$  by a cyclic group  $H = \langle h \rangle$  of order  $r$ . Choose  $s(h)$  to be an element of  $G$  such that  $Ns(h)$  is a *generator* for  $G/N$ , so that  $(s(h))^r = n_0$  for some  $n_0 \in N$ . Then there is an *automorphism*  $\phi$  of  $N$  satisfying the conditions: (a)  $\phi^r$  is *conjugation* by the element  $n_0$  of  $N$ ; and (b)  $\phi$  *fixes*  $n_0$ .

*Conversely*, given an element  $n_0$  of  $N$  and an automorphism  $\phi$  of  $N$  satisfying (a) and (b), then the set of ordered pairs  $(n, h^i)$ , with  $n \in N$  and  $0 \leq i \leq r-1$ , is a *cyclic extension* of  $N$  by  $H$  under the multiplication  $(n_1, h^i)(n_2, h^j) = (n_1(\phi)^i(n_2)f(h^i, h^j), h^{i+j})$ , where  $f(h^u, h^v) = 1$  if  $u+v < r$ , and  $f(h^u, h^v) = n_0$  if  $u+v \geq r$ . It *follows* from this that  $(1, h)^r = (n_0, 1)$ .

**Corollary 21.6:** Let  $G$  be an extension of an abelian group  $N$  by a cyclic group  $H$  of order  $r$ , and let  $Ns(h)$  be a *generator* for  $G/N$ . Then there is an *automorphism*  $\phi$  of  $N$  with  $\phi^r$  the *identity* automorphism, and an element  $n_0$  of  $N$  fixed by  $\phi$  with  $n_0 = (s(h))^r$ . *Conversely*, in order to *construct* a cyclic extension of  $N$  by  $H$ , we need to be given an automorphism  $\phi$  of  $N$  of order  $r$  and an element of  $N$  fixed by  $\phi$ . The group  $G$  then consists of elements  $ns(h^i)$ , where  $s(h)^r$  is the chosen element of  $N$  *fixed* by  $\phi$ .

**Proposition 21.8:** Let  $p$  be an *odd prime* and let  $G$  be a *finite  $p$ -group* which has only **one** subgroup of order  $p$ . Then  $G$  is *cyclic*. **Remark:** It may be shown that a 2-group which only has *one* element of order 2 is either *cyclic* or a *generalised quaternion group*.

**Proposition 21.9:** Let  $p$  and  $q$  be prime integers with  $p > q$ . A group of order  $pq$  has presentation  $\langle x, y: x^p = 1 = y^q, yxy^{-1} = x^k, \text{ with } kq \equiv 1 \pmod{p} \rangle$ . If  $q$  does *not* divide  $p-1$ , then a group of order  $pq$  is *cyclic*.

## Exercises

**21-1:** Let  $N = \langle z \rangle$  be a cyclic group of order 2, and let  $H$  be the non-cyclic group of order 4 with elements  $\{1, a, b, c\}$ . Given that the factor set

f	1	a	b	ab
1	1	1	1	1
a	1	1	z	z
b	1	1	z	z
ab	1	1	1	1

is a *central* factor set, construct the central extension  $G$ . Is  $G$  *isomorphic* to  $D(4)$ ?

**Answer:** As  $N$  is a cyclic group of order 2, it follows that the *only* automorphism of  $N$  is the trivial automorphism  $\varphi_1$  defined by  $\varphi_1(1) = 1$  and  $\varphi_1(z) = z$ . It follows that all the elements of  $H$  are associated to this identity automorphism  $\varphi_1$ , so that  $\varphi_1 = \varphi_a = \varphi_b = \varphi_c$ .

Now because  $H$  is *non-cyclic*, then  $H$  is the Klein 4-group consisting of three non-identity elements of order 2, with multiplication table as shown on the right (see page 27 in the book for the justification of this). As  $c = ab$ , then this accounts for the appearance of the element  $ab$  (and thus the non-appearance of the element  $c$ ) in the central factor set shown above.

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Given the central factor set shown above, Proposition 20.11 implies that the central extension  $G$  is a group consisting of the set of ordered pairs  $\{(n, h) : n \in N, h \in H\}$  under the multiplication

$$(n_1, h_1)(n_2, h_2) = (n_1 n_2 f(h_1, h_2), h_1 h_2).$$

It follows that the *eight* elements of  $G$  are  $(1, 1)$ ,  $(1, a)$ ,  $(1, b)$ ,  $(1, c)$ ,  $(z, 1)$ ,  $(z, a)$ ,  $(z, b)$  and  $(z, c)$ ; and that the multiplication table for  $G$  is as follows:

	(1, 1)	(1, a)	(1, b)	(1, c)	(z, 1)	(z, a)	(z, b)	(z, c)
(1, 1)	(1, 1)	(1, a)	(1, b)	(1, c)	(z, 1)	(z, a)	(z, b)	(z, c)
(1, a)	(1, a)	(1, 1)	(z, c)	(z, b)	(z, a)	(z, 1)	(1, c)	(1, b)
(1, b)	(1, b)	(1, c)	(z, 1)	(z, a)	(z, b)	(z, c)	(1, 1)	(1, a)
(1, c)	(1, c)	(1, b)	(1, a)	(1, 1)	(z, c)	(z, b)	(z, a)	(z, 1)
(z, 1)	(z, 1)	(z, a)	(z, b)	(z, c)	(1, 1)	(1, a)	(1, b)	(1, c)
(z, a)	(z, a)	(z, 1)	(1, c)	(1, b)	(1, a)	(1, 1)	(z, c)	(z, b)
(z, b)	(z, b)	(z, c)	(1, 1)	(1, a)	(1, b)	(1, c)	(z, 1)	(z, a)
(z, c)	(z, c)	(z, b)	(z, a)	(z, 1)	(1, c)	(1, b)	(1, a)	(1, 1)

Now that we have *constructed* the central extension  $G$ , we ask ourselves whether  $G$  is *isomorphic* to  $D(4)$  or not. Recall that  $D(4)$  is the group given by  $D(4) = \langle x, y: x^4 = y^2 = 1, xy = y^{-1}x \rangle$ . It follows that in order to show that  $G$  is isomorphic to  $D(4)$ , we need to find elements in  $G$  that will allow us to present  $G$  as we have just presented  $D(4)$ .

Consider first the orders of the elements of  $G$ . By looking at the table on the previous page, we can work out that the orders of the elements of  $G$  are as follows:

Element	(1, 1)	(1, a)	(1, b)	(1, c)	(z, 1)	(z, a)	(z, b)	(z, c)
Order	1	2	4	2	2	2	4	2

Let  $x = (1, b)$ , and let  $y = (z, 1)$ . From the above table of orders, it follows that we have  $x^4 = 1$  and  $y^2 = 1$ . It only remains to show that  $xy = y^{-1}x$ . Now  $xy = (1, b)(z, 1) = (z, b)$ ; and  $y^{-1}x = yx = (z, 1)(1, b) = (z, b)$ , so that  $xy = y^{-1}x$  as required.

It follows that  $G = \langle x, y: x^4 = y^2 = 1, xy = y^{-1}x \rangle$ , where  $x = (a, b)$  and  $y = (z, 1)$ , so that  $G$  is isomorphic to  $D(4)$ .

## Chapter 22: Groups with at most 31 elements

### Key Definitions and Results

**Definition 22.1:** Let  $p$  be a prime integer. The *automorphism group* of a cyclic group of order  $p$  is cyclic of order  $(p-1)$ .

**Proposition 22.3:** For  $n > 2$ , the automorphism group of a cyclic group  $G$  of order  $2^n$  is a *direct product*  $C_2 \times C_k$ , where  $k = 2^{n-2}$ .

**Proposition 22.4:** Let  $p$  be a *prime*, and let  $G$  be an *elementary abelian  $p$ -group* of order  $p^n$ , so that  $G$  is a *direct product* of  $n$  copies of  $C_p$ . The automorphism group of  $G$  is *isomorphic* to the group  $GL(n, p)$  of invertible  $n \times n$  matrices, with entries in the finite field  $\mathbf{Z}_p$ .

**Proposition 22.6:** The automorphism group of the *dihedral group*  $D(3)$  is isomorphic to  $D(3)$ .

We now start our investigation of groups of given orders by gathering together some of the results from earlier sections. In the following,  $p$  and  $q$  always denote *prime integers*.

(1) A group of order  $p$  is *cyclic* (Proposition 5.19).

(2) A group of order  $p^2$  is *abelian* and is *isomorphic* either to  $C_{p^2}$  or to  $C_p \times C_p$  (Corollaries 10.22 and 10.23).

(3) An abelian group of order  $p^3$  is isomorphic to one of  $C_{p^3}$ ,  $C_{p^2} \times C_p$  or  $C_p \times C_p \times C_p$ . A non-abelian group of order  $p^3$  is isomorphic to the *dihedral* or *quaternion* group when  $p = 2$ , and, for odd  $p$ , the group is *either*  $\langle x, y, z: x^p = y^p = z^p = 1, xz = zx, yz = zy, x^{-1}y^{-1}xy = z \rangle$ , in which every non-identity element has order  $p$ , *or* is  $\langle x, y: x^{p^2} = y^p = 1, y^{-1}xy = x^{1+p} \rangle$ , which has an element of order  $p^2$  (Proposition 18.11).

(4) A group of order  $pq$ , with  $p > q$ , is *cyclic* unless  $q$  divides  $p-1$ , in which case there is also a *non-abelian group*  $pq$  with presentation  $\langle x, y: x^p = 1 = y^q, y^{-1}xy = x^k, \text{ with } k \not\equiv 1 \pmod{p}, \text{ and } k^q \equiv 1 \pmod{p} \rangle$ . (Proposition 21.9).

It is convenient to *recall* some of our standard classes of groups. As well as *cyclic* groups, which exist for every possible order, for every even integer  $2n$ , there is a *dihedral* group  $D(n)$  of order  $2n$  with presentation  $\langle a, b: a^n = 1 = b^2, bab^{-1} = a^{-1} \rangle$ . As we have seen in chapter 17, the commutator quotient group of  $D(n)$  is  $C_2$  if  $n$  is *odd*, and is  $C_2 \times C_2$  if  $n$  is *even*. There is another standard group for integers of the form  $4n$ :

**Proposition 22.7:** For any integer  $n$ , there is a group of order  $4n$  with generators  $a$  and  $b$  satisfying the *relations*  $a^{2n} = 1$ ,  $a^n = b^2$ , and  $bab^{-1} = a^{-1}$ . This is the *generalised quaternion group*  $Q_{4n}$ . Its derived group is generated by  $a^2$ , and its *centre* is generated by  $a^n$ .

**Proposition 22.8:** There are *five* isomorphism classes of groups with 12 elements, namely  $C_{12}$ ,  $C_6 \times C_2$ ,  $D(6)$ , the alternating group  $A(4)$ , and the generalised quaternion group  $Q_{12}$  with presentation  $\langle a, b: a^6 = 1, a^3 = b^2, bab^{-1} = a^{-1} \rangle$ .

The methods that we have outlined have already enabled us to determine the isomorphism classes of groups with *13, 14 or 15 elements*. The next case which requires some discussion is that of groups with 16 elements. Since any 2-group is *nilpotent*, a maximal subgroup of a group of order 16 has 8 elements and is **normal**. We can then use the method of Theorem 21.5 to complete the list of isomorphism types. In the book, these are given in Appendix B, but one of the cases which needs to be considered (the case when there is a *cyclic subgroup with 8 elements*), is easily *generalised* to give the following result.

**Proposition 22.9:** Let  $n$  be an integer greater than 2. Let  $G$  be a group of order  $2^{n+1}$  which has an element of order  $2^n$ . If  $G$  is *abelian*,  $G$  is isomorphic either to a *cyclic group* or to the group  $C_{2^n} \times C_2$ . If  $G$  is *non-abelian*,  $G$  is isomorphic to one of: (a) the *dihedral group*  $D(2^n)$ ; (b) the *generalised quaternion group*,  $Q_{2^{n+1}}$ , with presentation  $\langle a, b: a^{2^n} = 1, b^2 = a^{2^{n-1}}, bab^{-1} = a^{-1} \rangle$ ; (c) the *group* given by  $\langle x, y: x^{2^n} = y^2 = 1, y^{-1}xy = x^{2^{n-1}+1} \rangle$ ; or (d) the *quasi-dihedral group* given by  $\langle x, y: x^{2^n} = y^2 = 1, y^{-1}xy = x^{2^{n-1}-1} \rangle$ .

**Proposition 22.10:** A group with *24 elements* contains a proper normal subgroup of index at most 3.

The above proposition makes it clear how to produce the list of isomorphism classes of groups with *24 elements*. Consider the two possibilities that the group has a normal subgroup of index 3 or one of index 2, and use the methods of extension theory on the list of groups of order 8 and groups of order 12, respectively, to complete the classification. There is considerable effort involved, not least in determining the *isomorphism types* of the constructed groups. The complete list of groups with 24 elements is given in Appendix B in the book.

Similar methods may be used to classify other groups whose orders have a *small* number of prime divisors, but note that these methods have severe limitations. The complete list of isomorphism types of groups of order  $\leq 31$  is presented in Appendix B in the book. The choice of 31 is not arbitrary: there are *51 isomorphism classes* of groups with 32 elements. Even worse, there are *267 isomorphism classes* of groups with 64 elements!

## Exercises

**22-6:** Which of the groups in Proposition 22.8 is isomorphic to  $S(3) \times C_2$ ?

**Answer:** Consider the external direct product  $S(3) \times C_2$ . We know that if two groups are isomorphic, then the two groups must have the same number of elements of a particular order. Therefore, if we can show that a group  $G$  has  $x$  elements of order  $p$ , and that the group  $S(3) \times C_2$  has  $y$  elements of order  $p$ , it follows that if  $x \neq y$ , then  $G$  and  $S(3) \times C_2$  cannot possibly be isomorphic.

So let us first find the multiplication table for  $S(3) \times C_2$  (using the multiplication  $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$ ), and let us then use it to calculate the *order* of each of the 12 elements of  $S(3) \times C_2$ .

	((1), 1)	((12), 1)	((13), 1)	((23), 1)	((123), 1)	((132), 1)	((1), x)	((12), x)	((13), x)	((23), x)	((123), x)	((132), x)
((1), 1)	((1), 1)	((12), 1)	((13), 1)	((23), 1)	((123), 1)	((132), 1)	((1), x)	((12), x)	((13), x)	((23), x)	((123), x)	((132), x)
((12), 1)	((12), 1)	((1), 1)	((123), 1)	((132), 1)	((13), 1)	((23), 1)	((12), x)	((1), x)	((123), x)	((132), x)	((13), x)	((23), x)
((13), 1)	((13), 1)	((132), 1)	((1), 1)	((123), 1)	((23), 1)	((12), 1)	((13), x)	((132), x)	((1), x)	((123), x)	((23), x)	((12), x)
((23), 1)	((23), 1)	((123), 1)	((132), 1)	((1), 1)	((12), 1)	((13), 1)	((23), x)	((123), x)	((132), x)	((1), x)	((12), x)	((13), x)
((123), 1)	((123), 1)	((23), 1)	((12), 1)	((13), 1)	((132), 1)	((1), 1)	((123), x)	((23), x)	((12), x)	((13), x)	((132), x)	((1), x)
((132), 1)	((132), 1)	((13), 1)	((23), 1)	((12), 1)	((1), 1)	((123), 1)	((132), x)	((13), x)	((23), x)	((12), x)	((1), x)	((123), x)
((1), x)	((1), x)	((12), x)	((13), x)	((23), x)	((123), x)	((132), x)	((1), 1)	((12), 1)	((13), 1)	((23), 1)	((123), 1)	((132), 1)
((12), x)	((12), x)	((1), x)	((123), x)	((132), x)	((13), x)	((23), x)	((12), 1)	((1), 1)	((123), 1)	((132), 1)	((13), 1)	((23), 1)
((13), x)	((13), x)	((132), x)	((1), x)	((123), x)	((23), x)	((12), x)	((13), 1)	((132), 1)	((1), 1)	((123), 1)	((23), 1)	((12), 1)
((23), x)	((23), x)	((123), x)	((132), x)	((1), x)	((12), x)	((13), x)	((23), 1)	((123), 1)	((132), 1)	((1), 1)	((12), 1)	((13), 1)
((123), x)	((123), x)	((23), x)	((12), x)	((13), x)	((132), x)	((1), x)	((123), 1)	((23), 1)	((12), 1)	((13), 1)	((132), 1)	((1), 1)
((132), x)	((132), x)	((13), x)	((23), x)	((12), x)	((1), x)	((123), x)	((132), 1)	((13), 1)	((23), 1)	((12), 1)	((1), 1)	((123), 1)

Element	((1), 1)	((12), 1)	((13), 1)	((23), 1)	((123), 1)	((132), 1)	((1), x)	((12), x)	((13), x)	((23), x)	((123), x)	((132), x)
Order	1	2	2	2	3	3	2	2	2	2	6	6

From the above, it follows that  $S(3) \times C_2$  has 1 element of order 1, 7 elements of order 2, 2 elements of order 3, and 2 elements of order 6.

The *five* isomorphism classes of groups with 12 elements in Proposition 22.8 were as follows:  $C_{12}$ ,  $C_6 \times C_2$ ,  $D(6)$ , the alternating group  $A(4)$ , and the generalised quaternion group  $Q_{12}$  with presentation  $\langle a, b: a^6 = 1, a^3 = b^2, bab^{-1} = a^{-1} \rangle$ .

Now as  $C_{12}$  has an element of order 12 (the *generator* of  $C_{12}$ ), and as  $S(3) \times C_2$  has **no** elements of order 12, then it follows that  $C_{12}$  cannot possibly be isomorphic to  $S(3) \times C_2$ . Similarly, as the group  $C_6 \times C_2$  has 6 elements of order 6 (the elements  $(x, 1)$ ,  $(x^5, 1)$ ,  $(x, y)$ ,  $(x^2, y)$ ,  $(x^4, y)$  and  $(x^5, y)$ , if  $C_6 = \{1, x, x^2, x^3, x^4, x^5\}$ , and if  $C_2 = \{1, y\}$ ), and as  $S(3) \times C_2$  has only **two** elements of order 6, then it follows that  $C_6 \times C_2$  cannot possibly be isomorphic to  $S(3) \times C_2$ .

Continuing in the same vein, because  $A(4)$  has *three* elements of order 2 (the elements  $(12)(34)$ ,  $(13)(24)$  and  $(14)(23)$ ), and as  $S(3) \times C_2$  has *seven* elements of order 2, then it follows that  $A(4)$  cannot possibly be isomorphic to  $S(3) \times C_2$ . Finally, because  $Q_{12}$  has at least one element of order 4 (the element  $b$ ), and as  $S(3) \times C_2$  does not have any elements of order 4, then it follows that  $Q_{12}$  cannot possibly be isomorphic to  $S(3) \times C_2$ .

This leaves us with the dihedral group  $D(6)$  to consider. To show that  $D(6)$  and  $S(3) \times C_2$  are isomorphic, it is sufficient to show that the multiplication tables for  $D(6)$  and  $S(3) \times C_2$  are the 'same', given an appropriate assignment; and that the two groups have the *same number of elements of any given order*. So let us consider the multiplication table for  $D(6)$ , where  $D(6)$  is presented as follows:  $D(6) = \langle a, b: a^6 = b^2 = 1, ab = ba^{-1} \rangle$ .

$D(6)$  consists of the *twelve* elements  $\{1, a, a^2, a^3, a^4, a^5, b, ba, ba^2, ba^3, ba^4, ba^5\}$ . For the following multiplication table, consider that we *order* the elements of  $D(6)$  in the following way:  $D(6) = \{1, b, ba^2, ba^4, a^2, a^4, a^3, ba^3, ba^5, ba, a^5, a\}$ .

	1	b	ba <sup>2</sup>	ba <sup>4</sup>	a <sup>2</sup>	a <sup>4</sup>	a <sup>3</sup>	ba <sup>3</sup>	ba <sup>5</sup>	ba	a <sup>5</sup>	a
1	1	b	ba <sup>2</sup>	ba <sup>4</sup>	a <sup>2</sup>	a <sup>4</sup>	a <sup>3</sup>	ba <sup>3</sup>	ba <sup>5</sup>	ba	a <sup>5</sup>	a
b	b	1	a <sup>2</sup>	a <sup>4</sup>	ba <sup>2</sup>	ba <sup>4</sup>	ba <sup>3</sup>	a <sup>3</sup>	a <sup>5</sup>	a	ba <sup>5</sup>	ba
ba <sup>2</sup>	ba <sup>2</sup>	a <sup>4</sup>	1	a <sup>2</sup>	ba <sup>4</sup>	b	ba <sup>5</sup>	a	a <sup>3</sup>	a <sup>5</sup>	ba	ba <sup>3</sup>
ba <sup>4</sup>	ba <sup>4</sup>	a <sup>2</sup>	a <sup>4</sup>	1	b	ba <sup>2</sup>	ba	a <sup>5</sup>	a	a <sup>3</sup>	ba <sup>3</sup>	ba <sup>5</sup>
a <sup>2</sup>	a <sup>2</sup>	ba <sup>4</sup>	b	ba <sup>2</sup>	a <sup>4</sup>	1	a <sup>5</sup>	ba	ba <sup>3</sup>	ba <sup>5</sup>	a	a <sup>3</sup>
a <sup>4</sup>	a <sup>4</sup>	ba <sup>2</sup>	ba <sup>4</sup>	b	1	a <sup>2</sup>	a	ba <sup>5</sup>	ba	ba <sup>3</sup>	a <sup>3</sup>	a <sup>5</sup>
a <sup>3</sup>	a <sup>3</sup>	ba <sup>3</sup>	ba <sup>5</sup>	ba	a <sup>5</sup>	a	1	b	ba <sup>2</sup>	ba <sup>4</sup>	a <sup>2</sup>	a <sup>4</sup>
ba <sup>3</sup>	ba <sup>3</sup>	a <sup>3</sup>	a <sup>5</sup>	a	ba <sup>5</sup>	ba	b	1	a <sup>2</sup>	a <sup>4</sup>	ba <sup>2</sup>	ba <sup>4</sup>
ba <sup>5</sup>	ba <sup>5</sup>	a	a <sup>3</sup>	a <sup>5</sup>	ba	ba <sup>3</sup>	ba <sup>2</sup>	a <sup>4</sup>	1	a <sup>2</sup>	ba <sup>4</sup>	b
ba	ba	a <sup>5</sup>	a	a <sup>3</sup>	ba <sup>3</sup>	ba <sup>5</sup>	ba <sup>4</sup>	a <sup>2</sup>	a <sup>4</sup>	1	b	ba <sup>2</sup>
a <sup>5</sup>	a <sup>5</sup>	ba	ba <sup>3</sup>	ba <sup>5</sup>	a	a <sup>3</sup>	a <sup>2</sup>	ba <sup>4</sup>	b	ba <sup>2</sup>	a <sup>4</sup>	1
a	a	ba <sup>5</sup>	ba	ba <sup>3</sup>	a <sup>3</sup>	a <sup>5</sup>	a <sup>4</sup>	ba <sup>2</sup>	ba <sup>4</sup>	b	1	a <sup>2</sup>

Element	1	b	ba <sup>2</sup>	ba <sup>4</sup>	a <sup>2</sup>	a <sup>4</sup>	a <sup>3</sup>	ba <sup>3</sup>	ba <sup>5</sup>	ba	a <sup>5</sup>	a
Order	1	2	2	2	3	3	2	2	2	2	6	6

As you can see, the multiplication tables for  $D(6)$  and  $S(3) \times C_2$  are the *same* (if we set  $((1), 1) = 1$ ,  $((12), 1) = b$ ,  $((13), 1) = ba^2$ ,  $((23), 1) = ba^4$ ,  $((123), 1) = a^2$ ,  $((132), 1) = a^4$ ,  $((1), x) = a^3$ ,  $((12), x) = ba^3$ ,  $((13), x) = ba^5$ ,  $((23), x) = ba$ ,  $((123), x) = a^5$ , and  $((132), x) = a$ ), and the two groups have the *same number of elements of each order* (**one** element of order 1, **seven** elements of order 2, **two** elements of order 3, and **two** elements of order 6). We therefore conclude that the two groups  $D(6)$  and  $S(3) \times C_2$  are *isomorphic*.

# Chapter 23: The Projective Special Linear Groups

## Key Definitions and Results

**Proposition 23.1:** Let  $F$  be a *finite field*. There is a prime integer  $p$ , the *characteristic* of  $F$ , such that  $F$  is an elementary abelian  $p$ -group under addition. It follows that  $F$  has  $q = p^k$  elements for some positive integer  $k$ . The multiplicative group of  $F$  is *cyclic* of order  $q-1$ , and so the multiplicative order of any non-zero element of  $F$  divides  $q-1$ . Conversely, for any divisor  $d$  of  $q-1$ , there is an element in  $F$  of order  $d$ . The number of *solutions* of the equation  $\lambda^n = 1$  in  $F$  is the greatest common divisor of  $n$  and  $q-1$ .

**Definition 23.2:** For any positive integer  $k$  and for any prime integer  $p$ , let  $F$  be a finite field of order  $q = p^k$ . For any positive integer  $n$ , the *general linear group*,  $GL(n, q)$ , is the set of all invertible  $n \times n$  matrices over  $F$  under matrix multiplication.

**Proposition 23.3:** The order of the group  $GL(n, q)$  is  $(q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{n-1})$ .

**Definition 23.5:** The *special linear group*  $SL(n, q)$  is the subgroup of the group  $GL(n, q)$  consisting of those matrices of *determinant* 1.

**Remark:** We saw in Proposition 14.14 that any finite field has order  $q$  for some prime power  $q = p^k$ . In fact, *any two finite fields* with the *same* number of elements are isomorphic. This field is usually denoted by  $GF(q)$  with its multiplicative group of non-zero elements being denoted by  $GF(q)^\times$ . We have also seen that  $SL(n, q)$  is the *kernel* of the homomorphism  $GL(n, q) \rightarrow GF(q)^\times$  defined by  $A \mapsto \det(A)$ . Since there are  $q-1$  possible non-zero determinants, then the Homomorphism Theorem shows that the *index* of  $SL(n, q)$  in  $GL(n, q)$  is  $q-1$ , and that  $SL(n, q)$  is a *normal subgroup*, with the quotient group  $GL(n, q)/SL(n, q)$  isomorphic to the multiplicative group  $GF(q)^\times$ .

**Definition 23.7:** For any positive integer  $n$ , the  $n \times n$  *scalar matrices* over  $GF(q)$  are those matrices in  $SL(n, q)$  which are of the form  $\lambda I_n$  for some  $\lambda \in GF(q)^\times$ .

**Remark:** The scalar matrices *commute* with each matrix, and so any subgroup consisting of scalar matrices is a normal subgroup of any subgroup of  $GL(n, q)$  containing the subgroup.

**Definition 23.8:** The *projective special linear group*  $PSL(n, q)$  is the quotient group  $SL(n, q)/Z$ , where  $Z$  is the *subgroup* of scalar matrices in  $SL(n, q)$ .

**Remark:** If  $\lambda I_n$  has determinant 1, then  $\lambda^n = 1$ , and so the number of elements in  $Z$  is, by Proposition 23.1, the *greatest common divisor*  $d$ , say, of  $n$  and  $q-1$ . Thus  $PSL(n, q)$  has order  $(q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{n-1})/(q-1)d$ . In particular, when  $n = 2$  and when  $p$  is an odd prime, we have  $|PSL(2, q)| = q(q^2-1)2$ .

**Proposition 23.11:** The group  $PSL(2, 5)$  is a *non-abelian simple group*.

**Remark:** It can also be shown that  $\text{PSL}(2, 4)$  is *simple*, although this is easier than in the proof of Proposition 23.11 since  $\text{PSL}(2, 4) = \text{SL}(2, 4)$ .

**Proposition 23.12:** Each of the groups  $\text{PSL}(2, 4)$  and  $\text{PSL}(2, 5)$  is *isomorphic* to the alternating group  $A(5)$ .

**Remark:** The conclusion of Proposition 23.12 holds for any simple group with 60 elements. The method of proof shows that we only need to prove that such a group has 15 *Sylow 2-subgroups*. The main result of this section is the fact that, except when  $q < 4$ , the group  $\text{PSL}(2, q)$  is **simple** for all prime powers  $q = p^k$ . We have seen that the groups  $\text{PSL}(2, 2)$  and  $\text{PSL}(2, 3)$  are genuine exceptions to this result in that both are *soluble* groups, and also that  $\text{PSL}(2, 4)$  and  $\text{PSL}(2, 5)$  are indeed simple. Several preliminaries are needed before we give the main result.

**Definition 23.13:** An element of  $\text{GL}(n, q)$  is a *transvection* if it is of the form  $B_{i,j}(\lambda) = I + E_{i,j}(\lambda)$ , where  $I$  is the identity  $n \times n$  matrix, and  $E_{i,j}(\lambda)$  is an elementary matrix (a matrix with **one** non-zero entry equal to  $\lambda$  in location  $(i, j)$ ). Any transvection has determinant 1, and so (by definition) is in  $\text{SL}(n, q)$ . The importance of these special types of matrices is that, for any matrix  $A$ , the product  $B_{i,j}(\lambda)A$  is the matrix obtained from  $A$  by adding  $\lambda$  times the  $j^{\text{th}}$  row of  $A$  to the  $i^{\text{th}}$  row. Thus, for example,

$$B_{2,3}(2) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 2 & 1 \\ 2 & 1 & 0 \end{pmatrix}.$$

This means that we can duplicate any *row reduction* of any matrix  $A$  by multiplying  $A$  on the left by a sequence of transvections.

**Proposition 23.14:** Every element  $A$  of  $\text{GL}(2, q)$  can be written as a product  $TD$ , where  $T$  is a product of transvections, and  $D$  is the matrix  $\begin{pmatrix} 1 & 0 \\ 0 & \det(A) \end{pmatrix}$ . In particular, each element of  $\text{SL}(2, q)$  is a *product of transvections*.

**Remark:** The next result uses the following elementary fact from the *general theory of vector spaces*: If  $v$  and  $w$  are column vectors of length 2 over  $\text{GF}(q)$ , and neither is a scalar multiple of the other, then the vectors are a *basis* for the vector space of all such column vectors. Thus, any column vector of length 2 over  $\text{GF}(q)$  can be written in the form  $av + bw$  for some  $a, b \in \text{GF}(q)$ .

**Theorem 23.15:** The group  $\text{PSL}(2, q)$  is simple if  $q > 3$ .

**Proposition 23.16:** Let  $q$  be an odd prime power. The matrices  $I$  and  $-I$  are the *only central elements* in  $\text{SL}(2, q)$ .

**Remark:** The results of this chapter can be generalised to matrices of *arbitrary* size. In fact, for any  $n > 2$  and for any prime power  $q$ , the group  $\text{PSL}(n, q) = \text{SL}(n, q)/Z$ , where  $Z$  is the set of scalar matrices of determinant 1, is a *non-abelian* group.

## Chapter 24: The Mathieu Groups

### Key Definitions and Results

In this chapter, we shall construct the *Mathieu group*, and briefly discuss the other Mathieu groups. The group  $M_{11}$  is another example of a finite simple group. However, this group is not one of an infinite family of examples, but is one of the **sporadic** simple groups. The sporadic groups comprise 26 groups which are not members of any of the infinite families of finite simple groups.

We shall define  $M_{11}$  in three steps, the first of these being to define a group  $M_9$  of order 72. The automorphism group of  $N = C_3 \times C_3$  contains the subgroup  $Q$  generated by the following matrices over  $\mathbf{Z}_3$ :

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Since  $A^2 = B^2 = -I$ , and since  $BAB^{-1} = A^{-1}$ , we see that  $Q$  is *isomorphic* to the quaternion group of order 8. We may therefore form the semidirect product of  $N$  by  $Q$ . This subgroup of the holomorph of  $N$  is a group of order 72 which we denote by  $M_9$ . It is also possible to represent the elements of this group as *permutations* in  $S(9)$  as follows: let  $\pi_1$  and  $\pi_2$  be the permutations  $\pi_1 = (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9)$ , and  $\pi_2 = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)$ .

Since  $\pi_1^3 = 1 = \pi_2^3$ , and since  $\pi_1\pi_2 = \pi_2\pi_1$ , the group *generated* by  $\pi_1$  and  $\pi_2$  is isomorphic to  $N$ . Now let  $\rho_1 = (2\ 4\ 3\ 7)(5\ 6\ 9\ 8)$ , and let  $\rho_2 = (2\ 5\ 3\ 9)(4\ 8\ 7\ 6)$ . It may be checked that  $\rho_1^2 = (2\ 3)(4\ 7)(5\ 9)(6\ 8) = \rho_2^2$ , and that  $\rho_2\rho_1\rho_2^{-1} = \rho_1^{-1}$ . Hence  $\langle \rho_1, \rho_2 \rangle$  is isomorphic to the quaternion group of order 8. Then  $\rho_1\pi_1\rho_1^{-1} = \pi_2$ ;  $\rho_1\pi_2\rho_1^{-1} = \pi_1^2$ ;  $\rho_2\pi_1\rho_2^{-1} = \pi_1\pi_2$ ; and  $\rho_2\pi_2\rho_2^{-1} = \pi_1\pi_2^2$ , so that  $\rho_1$  and  $\rho_2$  act on  $\langle \pi_1, \pi_2 \rangle$  in precisely the way in which the matrices  $A$  and  $B$  act on  $C_3 \times C_3$ . This shows that  $\langle \pi_1, \pi_2, \rho_1, \rho_2 \rangle$  is isomorphic to  $NQ$ , as required.

**Definition 24.1:** A subgroup  $G$  of a symmetric group on a set  $X$  is *transitive* if for any element  $x \in X$ , the *orbit* of  $x$  is  $X$ .

**Remark:** Notice that when  $G$  is transitive on  $X$ , the stabiliser  $G_x$  has index  $|X|$  in  $G$ , and that each  $y \in X$  is of the form  $g \cdot x$  for some  $g \in G$ . It follows easily from this that the orbit of any element  $y$  of  $X$  is the *whole* of  $X$ .

**Proposition 24.2:** With the above notation,  $G = \langle \pi_1, \pi_2, \rho_1, \rho_2 \rangle$  is a transitive group of order 72 *isomorphic* to  $M_9$ . The *stabiliser* of 1 is the subgroup  $Q = \langle \rho_1, \rho_2 \rangle$  of order 8. If  $\tau$  is any element of  $G$  **not** in  $Q$ , then  $G = Q \cup Q\tau Q$ , where  $Q\tau Q$  denotes the *double coset*  $\{x\tau y: x, y \in Q\}$ .

The next step is to define the group  $M_{10}$  of *order* 720.

**Proposition 24.3:** Let  $M_{10}$  be the subgroup of  $S(10)$  generated by  $M_9$  together with the permutation  $\sigma = (1\ 10)(4\ 5)(6\ 8)(7\ 9)$ . Then  $M_{10} = M_9 \cup M_9 \sigma M_9$  is a *transitive* group of order 720 in which the *stabiliser* of 10 is the group  $M_9$ .

This argument may be *repeated* to show the following:

**Proposition 24.4:** Let  $M_{11}$  be the subgroup of  $S(11)$  generated by  $M_{10}$  and the permutation  $\nu = (4\ 7)(5\ 8)(6\ 9)(10\ 11)$ . Then  $M_{11} = M_{10} \cup M_{10} \nu M_{10}$  is a *transitive group* of order 7920 in which the *stabiliser* of 11 is the group  $M_{10}$ .

**Remark 1:** The method of proving Proposition 24.4 may be applied once more, by defining the permutation  $\phi = (4\ 9)(5\ 7)(6\ 8)(11\ 12)$ , and setting  $M_{12}$  to be the group generated by  $M_{11}$  and  $\phi$ . Since  $\phi\nu$  is the permutation  $(4\ 9)(5\ 7)(6\ 8)(11\ 12)(4\ 7)(5\ 8)(6\ 9)(10\ 11) = (4\ 5\ 6)(7\ 9\ 8)(10\ 12\ 11)$  of order 3, it can be shown that  $M_{12}$  is the set  $M_{11} \cup M_{11} \phi M_{11}$ , and that  $M_{12}$  is *transitive*, with the stabiliser of 12 being  $M_{11}$ . It follows that  $M_{12}$  is a group with 95,040 elements. This group is also **simple**, but this fact is best proved using *more machinery* from the general theory of permutation groups than we have developed.

**Remark 2:** Similar ideas may be used to construct *another* sequence of Mathieu groups, giving  $M_{20}$ ,  $M_{21}$ ,  $M_{22}$ ,  $M_{23}$  and  $M_{24}$ , with  $|M_{24}| = 24 \times 23 \times 22 \times 21 \times 20 \times 48 = 244,823,040$ . The *basis* for this sequence is the simple group  $M_{21} = \text{PSL}(3, 4)$  of order 20,160. It may be shown that the groups  $M_{22}$ ,  $M_{23}$  and  $M_{24}$  are all *non-abelian simple groups*. These three groups together with  $M_{11}$  and  $M_{12}$  are the **five** sporadic simple Mathieu groups.

**Remark 3:** We constructed  $M_{11}$  via a sequence of *transitive* groups:  $Q$ ,  $M_9$ ,  $M_{10}$  and  $M_{11}$  are transitive on sets with 8, 9, 10 and 11 symbols, respectively. *Furthermore*,  $Q$  is the stabiliser of a point in  $M_9$ , while  $M_9$  is the stabiliser of a point in  $M_{10}$ , and  $M_{10}$  is the stabiliser of a point in  $M_{11}$ . In general, a group  $G$  is 1-transitive if it is *transitive*, and  $G$  is said to be  $k$ -transitive (for  $k \geq 2$ ) if it is transitive and the *stabiliser* of a point is  $(k-1)$ -transitive on the points other than the point being stabilised. In this terminology, the results in Propositions 24.3 and 24.4 can be generalised to give the following theorem:

**Theorem 24.5:** Let  $G$  be a  $k$ -transitive permutation group on a set  $X$ , with  $k \geq 2$ . Let  $X^+$  be obtained from  $X$  by adjoining a point  $*$ . Suppose that there is a permutation  $h$  on  $X^+$ , and an element  $g \in G$  such that  $h$  *interchanges*  $*$  with some  $x$  in  $X$ ;  $h$  fixes an element  $y$  in  $X$ ;  $g$  interchanges  $x$  and  $y$ ;  $(gj)^3$  and  $h^2$  are in  $G$ ; and  $hG_x h = G_x$ . Then the group  $\langle G, h \rangle$  is a  $(k+1)$ -transitive group on  $X^+$  in which the stabiliser of  $*$  is  $G$ .

This theorem was applied in Proposition 24.3 with  $G = M_9$ ,  $X$  being the set  $\{1, 2, \dots, 9\}$ ,  $*$  = 10,  $h = (1\ 10)(4\ 5)(6\ 8)(7\ 9)$ , and  $g$  being the permutation  $(1\ 3)(4\ 9)(5\ 8)(6\ 7)$ ; and again in Proposition 24.4 with  $G$  being  $M_{10}$ ,  $X = \{1, 2, \dots, 10\}$ ,  $*$  = 11,  $h = (4\ 7)(5\ 8)(6\ 9)(10\ 11)$ , and  $g = (1\ 10)(4\ 5)(6\ 8)(7\ 9)$ . However, as we have demonstrated, Theorem 24.5 is *not* essential to a construction of  $M_{11}$ .

We have seen that  $M_{11}$  is an example of a *4-transitive* group. There are other obvious examples of highly transitive groups. The group  $S(n)$  is  $n$ -transitive, and it may be shown that the alternating group  $A(n)$  is  $(n-2)$ -transitive. These facts follow easily from the sequences  $S(1) < S(2) < \dots$ , and  $A(3) < A(4) < \dots$ , the  $k^{\text{th}}$  term in each sequence being *k-transitive*. Apart from these examples, the **only** 4-transitive groups are  $M_{11}$  and  $M_{12}$  (this is actually *5-transitive*),  $M_{23}$  and  $M_{24}$  (this group is *also* 5-transitive).

**Theorem 24.6:** The group  $M_{11}$  is a *finite non-abelian simple group*.

**Remark:** The group  $M_{11}$  is associated with *two* important combinatorial structures, the first of these being a well-known error-correcting code, the ternary Golay code  $G_{11}$ ; and the second of these being the Steiner system, denoted by  $S(r, s, t)$ , which is a collection of  $s$ -element subsets of a set  $S$  containing  $t$  elements, such that any selection of  $r$  elements from  $S$  lies in precisely *one* of the  $s$ -element subsets.

## Chapter 25: The Classification of Finite Simple Groups

### Summary

One of the major intellectual achievements of all time has been the *classification of the finite simple groups*. As we saw in the chapter on the Jordan-Hölder Theorem, these are the ‘*atoms*’ of finite group theory. Chapter 25 presents a survey of the groups occurring in the list of finite simple groups.

An outline of the types of groups which appear in the classification is as follows:

- (1) The abelian simple groups: these are cyclic groups of prime order;
- (2) The alternating groups  $A(n)$  for  $n \geq 5$ ;
- (3) Various families of groups of Lie type. The easiest examples of groups in this class are the groups  $PSL(2, q)$  discussed in Chapter 23;
- (4) The sporadic groups: a set of 26 simple groups which are not accounted for in the previous three categories. The easiest example of a sporadic group is the group  $M_{11}$  discussed in Chapter 24.

Any finite simple group is *isomorphic* to a group in the above list.

Chapter 25 contains an introduction to the groups in the above list, the main discussion being about *classical groups*, which are obtained from groups of matrices over finite fields satisfying certain restrictions. The results on classical groups were unified by Chevalley (1955) and Steinberg (1959), when these groups were seen as groups of Lie type.