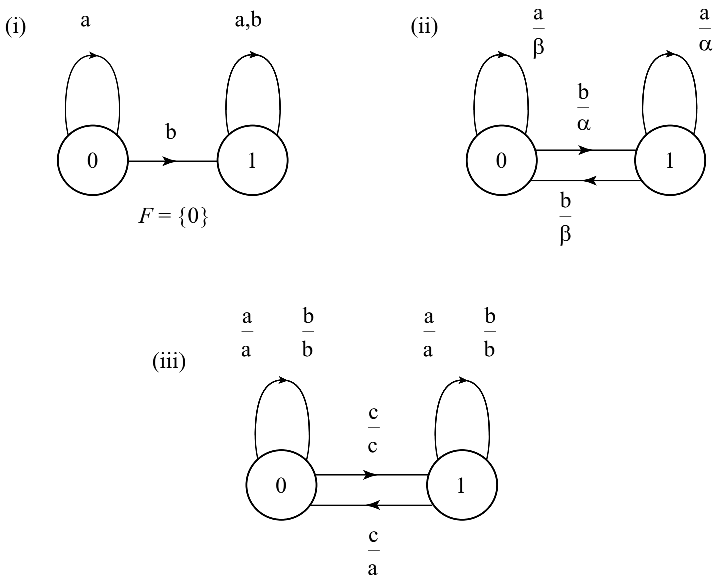

Fig. A8

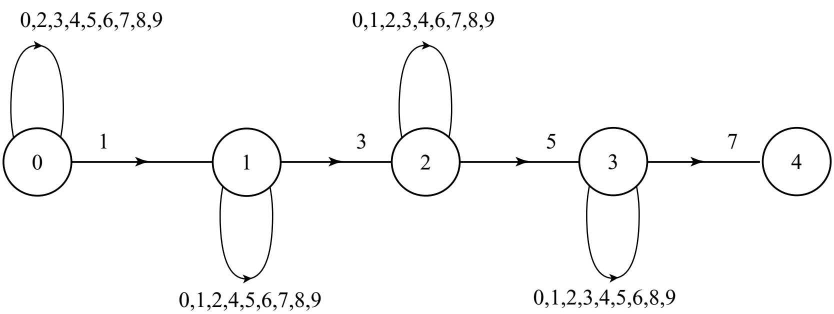

Fig. A9

(iv) If neither X does not love Y nor Y does not love Z then it is raining on Venus. (Equivalently: if X loves Y and Y loves Z then it is raining on Venus.)

2. (i) neither tautology nor contradiction; (ii) neither; (iii) contradiction; (iv) tautology; (v) neither; (vi) tautology.
3. The statement $p \wedge q$ is logically equivalent to $p \wedge (p \to q)$. Also $(p \wedge q) \leftrightarrow p$ is logically equivalent to $p \to q$.

Exercises 3.2

1. (a) (There are other, equivalent, ways of saying these.)
   (i) Everyone who is Scottish likes whisky.
   (ii) Everyone who likes whisky is Scottish.
   (iii) There is someone who is Scottish and does not like whisky.
   (iv) Not everyone who is Scottish likes whisky.
   (v) Not everyone is Scottish and likes whisky.
   (vi) There are at least two people who like whisky.
   (b) (There are other correct solutions.)
   (i) $\exists x\ (\neg S(x) \wedge W(x))$
   (ii) $(\exists x(S(x))) \rightarrow (\exists y(S(y) \wedge W(y)))$
   (iii) $\forall x\ (\neg S(x) \rightarrow \neg W(x))$
   (iv) $\exists x \exists y\ (x \neq y \wedge \neg S(x) \wedge \neg S(y) \wedge W(x) \wedge W(y))$.
2. (i) True, (ii) False, (iii) True, (iv) False.

Exercises 3.3

1. Probably we could construct a proof of this fact using almost any of our methods. Here are just two proofs.
   (i) Proof by induction: when $n = 1$, $n^2 + n + 1$ is 3 which is odd. Now suppose that $n^2 + n + 1$ is odd, then
   $(n + 1)^2 + (n + 1) + 1 = n^2 + 2n + 1 + n + 1 + 1 = (n^2 + n + 1)$
   $+\ 2n + 2$.
   Since $n^2 + n + 1$ is odd and $2n + 2$ is even (being divisible by 2), we see that $(n + 1)^2 + (n + 1) + 1$ is odd as required.
   (ii) Proof by cases: if n is even then n^2 is also even and so $n^2 + n$ is even, so $n^2 + n + 1$ is odd. If n is odd (say $n = 2k + 1$), then n^2 is odd (since it would be $4k^2 + 2k + 1$) so $n^2 + n$ is even and then $n^2 + n + 1$ is odd.
   Thus in either case $n^2 + n + 1$ is odd.
2. Here again methods like argument by cases, contrapositive and contradiction, all lead to fairly easy proofs. Again we give two proofs.
   (i) Proof by cases: if $a + b$ is odd, we consider four cases.
      (a) a, b are both even. In that case $a + b$ is also even, so this case cannot arise.
      (b) If a is even and b is odd, then $a + b$ is odd, so this case can arise.
      (c) If b is even and a is odd, then $a + b$ will be odd and this case can also arise.
      (d) If both a, b are odd then $a + b$ is even so this case does not arise.
      These four cases show that if $a + b$ is odd then precisely one of a, b is odd.

(ii) Proof by contradiction: suppose that $a+b$ is odd but either both or neither of a, b are odd. In either of these cases $a+b$ would be even. (Note that this argument also needs a slight recourse to cases.)

3. Suppose that a, b are integers with $a+b$ even. We want to show that $a-b$ is even. In this case induction does not seem appropriate, but again most other methods could work. We demonstrate two methods.
   (i) Contrapositive: we will show that if $a-b$ is odd then $a+b$ must be odd. If $a-b$ is odd one of a, b must be odd, the other being even (for if both were even (or odd) then $a+b$ would be even). But then $a+b$ is odd.
   (ii) Proof by contradiction: suppose that $a+b$ is even but $a-b$ is odd. Adding these gives

$$(a+b)+(a-b)=2a.$$

However $2a$ is even whereas the sum of an even and an odd integer must be odd, contradiction.

For the last part, to give a counterexample to the claim that if $a+b$ is even then ab is even, take $a=b=1$. Then $a+b=2$ which is even, but $ab=1$ which is odd.

Chapter 4

Exercises 4.1

1. $\pi_1\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 9 & 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$; $\pi_2\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 5 & 4 & 3 & 2 & 1 & 9 & 8 & 7 \end{pmatrix}$;

$\pi_3\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 5 & 4 & 9 & 8 & 7 & 3 & 2 & 1 \end{pmatrix}$; $\pi_3\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 1 & 9 & 8 & 7 & 6 & 5 & 4 \end{pmatrix}$;

$\pi_2\pi_1\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 6 & 1 & 2 & 3 & 7 & 8 & 9 \end{pmatrix}$;

$\pi_2\pi_2\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$;

$\pi_4\pi_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 6 & 1 & 7 & 3 & 5 & 2 & 8 & 4 & 9 & 12 & 11 \end{pmatrix}$;

$\pi_5\pi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 12 & 7 & 2 & 8 & 4 & 6 & 3 & 9 & 11 & 10 & 1 \end{pmatrix}$;

$$\pi_1\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 5 & 4 & 9 & 8 & 7 & 3 & 2 & 1 \end{pmatrix}; \pi_2\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix};$$

$$\pi_2\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 9 & 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}; \pi_3\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 9 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix};$$

$$\pi_2\pi_1\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 1 & 6 & 5 & 4 & 9 & 8 & 7 \end{pmatrix};$$

$$\pi_2\pi_3\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 9 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix};$$

$$\pi_4\pi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 9 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 12 & 10 & 11 \end{pmatrix};$$

$$\pi_5\pi_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 3 & 7 & 9 & 8 & 6 & 2 & 5 & 4 & 12 & 11 & 1 \end{pmatrix}.$$

2. $$\pi_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 1 & 6 & 5 & 4 & 9 & 8 & 7 \end{pmatrix}; \pi_2^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix};$$

$$\pi_3^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 9 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix};$$

$$\pi_4^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 1 & 12 & 10 & 11 \end{pmatrix};$$

$$\pi_5^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 3 & 7 & 5 & 9 & 6 & 2 & 4 & 8 & 12 & 11 & 1 \end{pmatrix}.$$

3. $\pi_1\pi_2 = (1\ 7)(2\ 8)(3\ 9)$; $\pi_2\pi_3 = (1\ 6)(2\ 5)(3\ 4)(7\ 9)$;
$\pi_3\pi_1 = (1\ 6\ 7\ 3\ 4\ 9)(2\ 5\ 8)$; $\pi_2\pi_3 = (1\ 3)(4\ 9)(5\ 8)(6\ 7)$;
$\pi_2\pi_1\pi_3 = (1\ 4)(2\ 5)(3\ 6)$; $\pi_2\pi_2\pi_2 = (1\ 9)(2\ 8)(3\ 7)(4\ 6)$;
$\pi_4\pi_5 = (1\ 10\ 9\ 4\ 7\ 2\ 6\ 5\ 3)(11\ 12)$;
$\pi_5\pi_4 = (1\ 5\ 8\ 3\ 7\ 6\ 4\ 2\ 12)(10\ 11)$;
$\pi_1\pi_3 = (1\ 6\ 7\ 3\ 4\ 9)(2\ 5\ 8)$; $\pi_2\pi_2 = \mathrm{id}$;
$\pi_2\pi_1 = (1\ 7)(2\ 8)(3\ 9)$; $\pi_3\pi_3 = (1\ 7\ 4)(2\ 8\ 5)(3\ 9\ 6)$;
$\pi_2\pi_1\pi_2 = (1\ 3)(4\ 6)(7\ 9)$; $\pi_2\pi_3\pi_2 = (1\ 7\ 4)(2\ 8\ 5)(3\ 9\ 6)$;
$\pi_4\pi_4 = (1\ 8\ 6\ 4\ 2\ 9\ 7\ 5\ 3)(10\ 12\ 11)$;
$\pi_5\pi_5 = (1\ 10\ 12)(2\ 3\ 7)(4\ 9)(5\ 8)$;

4. (i) $(1\ 8\ 4\ 6\ 2\ 3)$; (ii) $(1\ 2\ 7\ 5\ 4\ 9\ 3\ 12\ 10)$;
(iii) $(1\ 5\ 9\ 4\ 8\ 3\ 7\ 2\ 6)\,(10\ 11)$.

5. The table is

	id	(1234)	(13)(24)	(1432)	(13)	(24)	(12)(34)	(14)(23)
id	id	(1234)	(13)(24)	(1432)	(13)	(24)	(12)(34)	(14)(23)
(1234)	(1234)	(13)(24)	(1432)	id	(14)(23)	(12)(34)	(13)	(24)
(13)(24)	(13)(24)	(1432)	id	(1234)	(24)	(13)	(14)(23)	(12)(34)
(1432)	(1432)	id	(1234)	(13)(24)	(12)(34)	(14)(23)	(24)	(13)
(13)	(13)	(12)(34)	(24)	(14)(23)	id	(13)(24)	(1234)	(1432)
(24)	(24)	(14)(23)	(13)	(12)(34)	(13)(24)	id	(1432)	(1234)
(12)(34)	(12)(34)	(24)	(14)(23)	(13)	(1432)	(1234)	id	(13)(24)
(14)(23)	(14)(23)	(13)	(12)(34)	(24)	(1234)	(1432)	(13)(24)	id

6. $s = (1\ \ 2\ \ 4\ \ 8\ \ 5\ \ 10\ \ 9\ \ 7\ \ 3\ \ 6)$; $t = (2\ \ 3\ \ 5\ \ 9\ \ 8\ \ 6)(4\ \ 7)$;
$c = (1\ \ 6)(2\ \ 7)(3\ \ 8)(4\ \ 9)(5\ \ 10)$; $cs = (1\ \ 7\ \ 8\ \ 10\ \ 4\ \ 3)(2\ \ 9)$;
$scs = (1\ \ 3\ \ 2\ \ 7\ \ 5\ \ 10\ \ 8\ \ 9\ \ 4\ \ 6)$;
s, 10 times; t, 6 times; cs, 6 times; scs, 10 times.

Exercises 4.2

1. (i) The permutation has order 30 and is odd; (ii) order 30, odd; (iii) order 4, even; (iv) order 1, even.
2. An example is given by the transpositions (1 2) and (2 3).
3. An example is (1 2)(3 4).
5. An example is provided by the transpositions in 2 above.
6. The orders are 5, 6 and 2 respectively.
7. The orders are 2, 3 and 5.
9. The identity element has order 1, the elements (1 2)(3 4), (1 3)(2 4) and (1 4)(2 3) have order 2 and the remaining 8 elements all have order 3: (1 2 3), (1 2 4), (1 3 4), (2 3 4), (1 3 2), (1 4 2), (1 4 3), and (2 4 3).
11. The highest possible order of an element of $S(8)$ is 15, of $S(12)$ is 60 and of $S(15)$ is 105.
12. $o(s) = 10$, $\mathrm{sgn}(s) = -1$, $o(t) = 6$, $\mathrm{sgn}(t) = 1$, $o(c) = 2$, $\mathrm{sgn}(c) = -1$, $o(cs) = 6$, $\mathrm{sgn}(cs) = 1$, $o(scs) = 10$, $\mathrm{sgn}(scs) = -1$.

Exercises 4.3

1. (i) No; 0 has no inverse. (ii) This is a group.
   (iii) No: 2 has no inverse. (iv) This is not a group: not all the functions have inverses.
   (v) This is a group. (vi) This is a group.
   (vii) No: non-associative. (viii) This is a group.
2. Take G to be $S(3)$, a to be (1 2) and b to be (1 3).

5. The required matrix is

$$\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$$

7. The table for $D(4)$ is as shown:

	e	ρ	ρ^2	ρ^3	R	ρR	$\rho^2 R$	$\rho^3 R$
e	e	ρ	ρ^2	ρ^3	R	ρR	$\rho^2 R$	$\rho^3 R$
ρ	ρ	ρ^2	ρ^3	e	ρR	$\rho^2 R$	$\rho^3 R$	R
ρ^2	ρ^2	ρ^3	e	ρ	$\rho^2 R$	$\rho^3 R$	R	ρR
ρ^3	ρ^3	e	ρ	ρ^2	$\rho^3 R$	R	ρR	$\rho^2 R$
R	R	$\rho^3 R$	$\rho^2 R$	ρR	e	ρ^3	ρ^2	ρ
ρR	ρR	R	$\rho^3 R$	$\rho^2 R$	ρ	e	ρ^3	ρ^2
$\rho^2 R$	$\rho^2 R$	ρR	R	$\rho^3 R$	ρ^2	ρ	e	ρ^3
$\rho^3 R$	$\rho^3 R$	$\rho^2 R$	ρR	R	ρ^3	ρ^2	ρ	e

8. The completed table is

	a	b	c	d	f	g
a	c	g	a	f	d	b
b	d	f	b	g	c	a
c	a	b	c	d	f	g
d	b	a	d	c	g	f
f	g	c	f	a	b	d
g	f	d	g	b	a	c

Note that c is the identity element.
Thus $ax = b$ has one solution (g); $xa = b$ also has one (d); $x^2 = c$ has four solutions (c, a, d, and g) and $x^3 = d$ has one solution (d).

Exercises 4.4

1. (i), (ii) and (iii) are semigroups, (iv) and (v) are not.
3. (i) A non-commutative ring with identity and zero-divisors;
   (ii) not a ring (not closed under addition);
   (iii) not a ring (additive inverses missing);
   (iv) commutative ring with identity and zero-divisors;
   (v) commutative ring with no identity and no zero-divisors;
   (vi) commutative ring with no identity but zero-divisors;
   (vii) commutative ring with no identity and no zero-divisors;
   (viii) commutative ring with identity and no zero-divisors.

7. Take, for example, R to be the set of all 2×2 matrices with

$$x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

8. Take, for example, R to be $\mathbb{Z}_2$ and $x = y = [1]_2$.
9. (i) Is a vector space; the other two fail the distributivity axiom: $(\lambda + \mu)A$ is not equal to $\lambda A + \mu A$.

Chapter 5

Exercises 5.1

2. If $axba^{-1} = b$, multiply on the right first by a then by b^{-1} to obtain $ax = bab^{-1}$. Now multiply by a^{-1} on the left to obtain $x = a^{-1}bab^{-1}$.
3. Let G be the cyclic group with 12 elements and square each of the 12 to get

element	e	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}
square	e	x^2	x^4	x^6	x^8	x^{10}	e	x^2	x^4	x^6	x^8	x^{10}

(remembering that $x^{12} = e$). It is now clear that several elements of G are not squares of other elements, for example, there is no element g with $g^2 = x^3$.
4. (i) A subgroup; (ii) not a subgroup; (iii) not closed; (iv) a subgroup.
5. Take G to be $S(3)$, a to be $(1\ 2)$, b to be $(1\ 3)$ and c to be $(2\ 3)$.
6. Since the number of elements in $\langle x^d \rangle$ is the order of x^d, we first calculate these orders

element	e	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}
order	1	12	6	4	3	12	2	12	3	4	6	12

It is clear that the subgroup generated by x is the whole group G. From the table of orders we also see that G can be generated by x^5, x^7 and x^{11}. Each of these powers (1, 5, 7 or 11), has greatest common divisor 1 with 12, confirming that $\langle x^d \rangle$ has 12 $(= 12/1)$ elements in these cases. Next consider x^2. We see that, since x^2 has order 6, the subgroup has 6 elements in this case. The only other element of order 6 is x^{10}. It is clear that x^2 and x^{10} generate the same subgroup with 6 elements and that 6 is $12/2$ where 2 is the greatest common divisor of 12 with both 2 and with 10. The next element in the list is x^3 which generates a subgroup with 4 elements. The other element of order 4 is x^9. Again these two elements actually generate the same subgroup and $(12, 3) = (12, 9) = 3$ $(= 12/4)$. Next x^4 and x^8

have order 3 and x^8 is the square of x^4, so they generate the same subgroup with 3 elements and $(12, 4) = (12, 8) = 4$ $(= 12/3)$. The only non-identity element we have not discussed is x^6 and this is the unique element of order 2 so the subgroup it generates has 2 $(= 12/6)$ elements.

7. Let m be minimal such that x^m is in H and let x^k be any other element in H (we know that any element of H is a power of x because G is cyclic). Use the division algorithm to write $k = qm + r$ with r less than m. Then x^k is in H (given) and x^{qm} is in H (because x^m is), so since H is a subgroup,

$$x^k(x^{qm})^{-1} = x^{qm+r}x^{-qm} = x^r$$

is an element of H. This contradicts the minimality of m, unless $r = 0$. We have therefore shown that every element of H is a power of x^m and so H is cyclic.

8. We first use induction to show that $(g^{-1}xg)^k = g^{-1}x^k g$. The base case is clear, so suppose that $(g^{-1}xg)^k = g^{-1}x^k g$ for some $k \geq 1$. Then

$$\begin{aligned}(g^{-1}xg)^{k+1} &= (g^{-1}xg)^k(g^{-1}xg) = g^{-1}x^k gg^{-1}xg \\ &= g^{-1}x^k xg = g^{-1}x^{k+1}g\end{aligned}$$

as required. Now suppose that x has order 3. Then $x^3 = e$ and so, for all g in G,

$$(g^{-1}xg)^3 = g^{-1}x^3 g = g^{-1}eg = e$$

so the order of $g^{-1}xg$ divides 3. Since $g^{-1}xg$ does not have order 1 (otherwise x would be e and would not have order 3), we have shown that if x has order 3 then so does $g^{-1}xg$. For the converse, suppose that $g^{-1}xg$ has order 3, then $e = (g^{-1}xg)^3 = g^{-1}x^3 g$ (by the first part). It then follows that $x^3 = e$, so the order of x divides 3. However, x does not have order 1 (otherwise $x = e$ and then $g^{-1}xg = e$ therefore does not have order 3), so g has order 3.

10. One generator for G_{23} is $[5]_{23}$. A generator for G_{26} is $[7]_{26}$. However, G_8 is not cyclic.

Exercises 5.2

1. The left cosets are
$\{[1]_{14}, [13]_{14}\}$, $\{[3]_{14}, [11]_{14}\}$, and $\{[5]_{14}, [9]_{14}\}$.

3. The left cosets are
$\{1, \tau\}$, $\{r, r\tau\}$, $\{r^2, r^2\tau\}$ and $\{r^3, r^3\tau\}$
where r represents rotation through $\pi/4$.

5. Since $\phi(20)$ is 8, the possible orders of elements of G_{20} are 1, 2, 4 or 8. The actual order of $[1]_{20}$ is 1, of $[3]_{20}$ is 4, of $[7]_{20}$ is 4, of $[9]_{20}$ is 2, of $[11]_{20}$ is 2, of $[13]_{20}$ is 4, of $[17]_{20}$ is 4 and of $[19]_{20}$ is 2.

Exercises 5.3

1. (i) $\mathbb{Z}_2 \times \mathbb{Z}_2$; (ii) $\mathbb{Z}_4$; (iii) $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ respectively.
3. Take G to be $S(3)$ and g to be $(1\ 2\ 3)$ to see that f need not be the identity function.
4. The group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.
7. The tables are as shown:

(i)

$\mathbb{Z}_4 \times \mathbb{Z}_2$	(0, 0)	(1, 0)	(2, 0)	(3, 0)	(0, 1)	(1, 1)	(2, 1)	(3, 1)
(0, 0)	(0, 0)	(1, 0)	(2, 0)	(3, 0)	(0, 1)	(1, 1)	(2, 1)	(3, 1)
(1, 0)	(1, 0)	(2, 0)	(3, 0)	(0, 0)	(1, 1)	(2, 1)	(3, 1)	(0, 1)
(2, 0)	(2, 0)	(3, 0)	(0, 0)	(1, 0)	(2, 1)	(3, 1)	(0, 1)	(1, 1)
(3, 0)	(3, 0)	(0, 0)	(1, 0)	(2, 0)	(3, 1)	(0, 1)	(1, 1)	(2, 1)
(0, 1)	(0, 1)	(1, 1)	(2, 1)	(3, 1)	(0, 0)	(1, 0)	(2, 0)	(3, 0)
(1, 1)	(1, 1)	(2, 1)	(3, 1)	(0, 1)	(1, 0)	(2, 0)	(3, 0)	(0, 0)
(2, 1)	(2, 1)	(3, 1)	(0, 1)	(1, 1)	(2, 0)	(3, 0)	(0, 0)	(1, 0)
(3, 1)	(3, 1)	(0, 1)	(1, 1)	(2, 1)	(3, 0)	(0, 0)	(1, 0)	(2, 0)

(ii)

$G_5 \times G_3$	(1, 1)	(2, 1)	(4, 1)	(3, 1)	(1, 2)	(2, 2)	(4, 2)	(3, 2)
(1, 1)	(1, 1)	(2, 1)	(4, 1)	(3, 1)	(1, 2)	(2, 2)	(4, 2)	(3, 2)
(2, 1)	(2, 1)	(4, 1)	(3, 1)	(1, 1)	(2, 2)	(4, 2)	(3, 2)	(1, 2)
(4, 1)	(4, 1)	(3, 1)	(1, 1)	(2, 1)	(4, 2)	(3, 2)	(1, 2)	(2, 2)
(3, 1)	(3, 1)	(1, 1)	(2, 1)	(4, 1)	(3, 2)	(1, 2)	(2, 2)	(4, 2)
(1, 2)	(1, 2)	(2, 2)	(4, 2)	(3, 2)	(1, 1)	(2, 1)	(4, 1)	(3, 1)
(2, 2)	(2, 2)	(4, 2)	(3, 2)	(1, 2)	(2, 1)	(4, 1)	(3, 1)	(1, 1)
(4, 2)	(4, 2)	(3, 2)	(1, 2)	(2, 2)	(4, 1)	(3, 1)	(1, 1)	(2, 1)
(3, 2)	(3, 2)	(1, 2)	(2, 2)	(4, 2)	(3, 1)	(1, 1)	(2, 1)	(4, 1)

(iii)

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	(0, 0, 0)	(1, 0, 0)	(0, 1, 0)	(1, 1, 0)	(0, 0, 1)	(1, 0, 1)	(0, 1, 1)	(1, 1, 1)
(0, 0, 0)	(0, 0, 0)	(1, 0, 0)	(0, 1, 0)	(1, 1, 0)	(0, 0, 1)	(1, 0, 1)	(0, 1, 1)	(1, 1, 1)
(1, 0, 0)	(1, 0, 0)	(0, 0, 0)	(1, 1, 0)	(0, 1, 0)	(1, 0, 1)	(0, 0, 1)	(1, 1, 1)	(0, 1, 1)
(0, 1, 0)	(0, 1, 0)	(1, 1, 0)	(0, 0, 0)	(1, 0, 0)	(0, 1, 1)	(1, 1, 1)	(0, 0, 1)	(1, 0, 1)
(1, 1, 0)	(1, 1, 0)	(0, 1, 0)	(1, 0, 0)	(0, 0, 0)	(1, 1, 1)	(0, 1, 1)	(1, 0, 1)	(0, 0, 1)
(0, 0, 1)	(0, 0, 1)	(1, 0, 1)	(0, 1, 1)	(1, 1, 1)	(0, 0, 0)	(1, 0, 0)	(0, 1, 0)	(1, 1, 0)
(1, 0, 1)	(1, 0, 1)	(0, 0, 1)	(1, 1, 1)	(0, 1, 1)	(1, 0, 0)	(0, 0, 0)	(1, 1, 0)	(0, 1, 0)
(0, 1, 1)	(0, 1, 1)	(1, 1, 1)	(0, 0, 1)	(1, 0, 1)	(0, 1, 0)	(1, 1, 0)	(0, 0, 0)	(1, 0, 0)
(1, 1, 1)	(1, 1, 1)	(0, 1, 1)	(1, 0, 1)	(0, 0, 1)	(1, 1, 0)	(0, 1, 0)	(1, 0, 0)	(0, 0, 0)

(iv)

$G_{12} \times G_4$	(1, 1)	(5, 1)	(7, 1)	(11, 1)	(1, 3)	(5, 3)	(7, 3)	(11, 3)
(1, 1)	(1, 1)	(5, 1)	(7, 1)	(11, 1)	(1, 3)	(5, 3)	(7, 3)	(11, 3)
(5, 1)	(5, 1)	(1, 1)	(11, 1)	(7, 1)	(5, 3)	(1, 3)	(11, 3)	(7, 3)
(7, 1)	(7, 1)	(11, 1)	(1, 1)	(5, 1)	(7, 3)	(11, 3)	(1, 3)	(5, 3)
(11, 1)	(11, 1)	(7, 1)	(5, 1)	(1, 1)	(11, 3)	(7, 3)	(5, 3)	(1, 3)
(1, 3)	(1, 3)	(5, 3)	(7, 3)	(11, 3)	(1, 1)	(5, 1)	(7, 1)	(11, 1)
(5, 3)	(5, 3)	(1, 3)	(11, 3)	(7, 3)	(5, 1)	(1, 1)	(11, 1)	(7, 1)
(7, 3)	(7, 3)	(11, 3)	(1, 3)	(5, 3)	(7, 1)	(11, 1)	(1, 1)	(5, 1)
(11, 3)	(11, 3)	(7, 3)	(5, 3)	(1, 3)	(11, 1)	(7, 1)	(5, 1)	(1, 1)

Of these, the first two are isomorphic to each other and also $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to $G_{12} \times G_4$.

8. The possible orders of the elements in $G \times H$ are the integers of the form $1\text{cm}\{a, b\}$ where a divides 6 and b divides 14. Namely: 1, 2, 3, 6, 7, 14, 21, 42.

Exercises 5.4

2. The first and second detect one error and correct none; the third detects two and corrects one and the fourth detects none and corrects none.
3. The codewords are

000000111	001001110	010010101	011011100
100100011	101101010	110110001	111111000

The code detects two errors and corrects one error.

4. The decoding table is

000000	100110	010101	001011	110011	101101	011110	111000
000001	100111	010100	001010	110010	101100	011111	111001
000010	100100	010111	001001	110001	101111	011100	111010
000100	100010	010001	001111	110111	101001	011010	111100
001000	101110	011101	000011	111011	100101	010110	110000
010000	110110	000101	011011	100011	111101	001110	101000
100000	000110	110101	101011	010011	001101	111110	011000
001100	101010	011001	000111	111111	100001	010010	110100

5. Corrected words are

101110100010	111111111100	000000000000
001000100011	001110101100	

6. The two-column decoding table is

Syndrome	Coset leader
0000	0000000
1101	1000000
1110	0100000
1011	0010000
1000	0001000
0100	0000100
0010	0000010
0001	0000001
0011	0000011
0101	0000101
1001	0001001
0110	0000110
1010	0001010
1100	0001100
1111	1000010
0111	0000111

The syndrome of 1100011 is 0000 so this is a codeword;
the syndrome of 1011000 is 1110 so we correct to 1111000;
the syndrome of 0101110 is 0000 so this is a codeword;
the syndrome of 0110001 is 0100 so corrected word is 0110101;
the syndrome of 1010110 is 0000 so this is a codeword.

7. The two-column decoding table is

Syndrome	Coset leader
000	000000
101	100000
110	010000
011	001000
100	000100
010	000010
001	000001
111	001100

The message is THE END.

Chapter 6

Exercises 6.1

1. (i) $2x^2 + 2x$,
   (ii) $-3x^2 + 2x$,
   (iii) $2x^2 + (7 - 5\mathrm{i})x + (3 - 3\mathrm{i})$,
   (iv) $-3\mathrm{i}x^2 + 2\mathrm{i}x$,
   (v) $2x^2 + x$,
   (vi) $x^2 + 2x$.
2. (i) $x^3 + 8x^2 + 10x + 3$,
   (ii) $x^5 - x^4 - 2x^2 - 1$,
   (iii) $\mathrm{i}x^3 + (3 + 7\mathrm{i})x^2 + (21 + 3\mathrm{i})x + 9$,
   (iv) $-x^5 - (1 + 2\mathrm{i})x^4 + (1 - \mathrm{i})x^3 + (1 + 3\mathrm{i})x^2 + (1 - \mathrm{i})x - 1$,
   (v) $x^4 + x^2 + 1$,
   (vi) $x^5 + x^3 + x^2 + 1$.
3. In the three cases the zeros are: (i) $x = 1, 1 + \mathrm{i}$ or $1 - \mathrm{i}$, (ii) $x = 7\mathrm{i}$ or $-\mathrm{i}$, (iii) $x = [4]_5$ is the only zero.

Exercises 6.2

1. (i) $f(x) = (x^2 + 3x + 6)g(x) + (10x - 5)$,
   (ii) $f(x) = (x + 6)g(x) + (24x - 35)$,
   (iii) $f(x) = (x + 6)g(x) + 3x$.
2. (i) Experiment with small values for x to see that $x = 1$ is a zero. Thus $x - 1$ divides the polynomial, and

$$x^3 - x^2 - 4x + 4 = (x - 1)(x^2 - 4) = (x - 1)(x - 2)(x + 2).$$

   (ii) In this case, we see that $x = 2$ is a zero and

$$x^3 - 3x^2 + 3x - 2 = (x - 2)(x^2 - x + 1).$$

   Using the formula to find the zeros of the quadratic $x^2 - x + 1$, we see at once that this quadratic has no real roots, so we already have a decomposition into irreducible real polynomials.

   (iii) If we continue the factorisation over $\mathbb{C}$, we see that

$$x^3 - 3x^2 + 3x - 2 = (x - 2)(x - w)(x - \overline{w}),$$

   where $w = \frac{1+\mathrm{i}\sqrt{3}}{2}$.

   (iv) Over $\mathbb{Z}_7$, we clearly only need to seek for roots of $g(x) = x^2 - x + 1$ which is done by substituting the seven possible values for x. Then

$g(0) = 1$, $g(1) = 1$, $g(2) = 3$. However $g(3) = 9 - 3 + 1 = 7 = 0$, so 3 is a zero and so $x - 3$ divides $g(x)$. This completes the factorisation as

$$x^3 - 3x^2 + 3x - 2 = (x-2)(x-3)(x-5).$$

(v) It is clear that $x = -1$ is a root of the given polynomial and

$$x^3 + x^2 + x + 1 = (x+1)(x^2+1) = (x+1)(x+1)^2 = (x+1)^3.$$

3. (i) We first see that

$$x^3 + 1 = (x-1)(x^2 + x - 1) + 2x.$$

Then since $x^2 + x - 1 = 2x\left(\frac{1}{2}x + \frac{1}{2}\right) - 1$, a greatest common divisor for the given polynomials is $(-)1$. Then

$$\begin{aligned} -1 &= (x^2 + x - 1) - 2x\left(\tfrac{1}{2}x + \tfrac{1}{2}\right) \\ &= (x^2 + x - 1) - \left((x^3 + 1) - (x-1)(x^2 + x - 1)\right)\left(\tfrac{1}{2}x + \tfrac{1}{2}\right) \\ &= -\tfrac{1}{2}(x+1)(x^3+1) + \tfrac{1}{2}(x^2+1)(x^2+x-1). \end{aligned}$$

(ii) The first step is to note that

$$x^4 + x + 1 = (x)(x^3 + x + 1) + x^2 + 1.$$

Then we find that

$$x^3 + x + 1 = (x)(x^2 + 1) + 1.$$

It follows that 1 is a gcd for the two given polynomials and that

$$\begin{aligned} 1 &= (x^3 + x + 1) - (x)(x^2 + 1) \\ &= (x^3 + x + 1) + (x)\left((x^4 + x + 1) - (x)(x^3 + x + 1)\right) \\ &= (x^3 + x + 1)(x^2 + 1) + x(x^4 + x + 1). \end{aligned}$$

(iii) The first step is to note that

$$x^3 - \mathrm{i}x^2 + 2x - 2\mathrm{i} = (x - \mathrm{i})(x^2 + 1) + x - \mathrm{i}.$$

Then, since $x^2 + 1 = (x + \mathrm{i})(x - \mathrm{i})$, a greatest common divisor is $x - \mathrm{i}$. Also $x - \mathrm{i} = x^3 - \mathrm{i}x^2 + 2x - 2\mathrm{i} - (x - \mathrm{i})(x^2 + 1)$.

4. We are given that $f(x) = (x - \alpha)g(x) + r(x)$, so substitute $x = \alpha$, to obtain $f(\alpha) = (\alpha - \alpha)g(\alpha) + r(\alpha)$. Since $(\alpha - \alpha)$ is the zero polynomial, and multiplying any polynomial by the zero polynomial gives the zero polynomial, we see that $f(\alpha) = r(\alpha)$, as required.

Exercises 6.3

1. The base case for the induction may be taken for granted (the result is clear when $n = 1$). Now suppose that the result holds when $r = k$ and suppose that f divides the product $f_1(x) \ldots f_{k+1}(x)$. Write $g(x)$ for the product $f_1(x) \ldots f_k(x)$, so we know that f divides $g(x) f_{k+1}(x)$. By the results in this section, we deduce that f divides at least one of $g(x)$ or $f_{k+1}(x)$. Using induction on $g(x)$, we deduce that f divides one of $f_1(x), f_2(x), \ldots, f_{k+1}(x)$.
2. Fermat's Theorem implies that each of the non-zero elements of $\mathbb{Z}_p$ is a zero of the polynomial $x^{p-1} - 1$, and so for each of these $p - 1$ elements i, say, $(x - i)$ divides $x^{p-1} - 1$. Since this polynomial of degree $p - 1$ is divisible by $p - 1$ linear factors, we see that this must be the factorisation of the polynomial.
3. Any quadratic over $\mathbb{Z}_2$ with leading coefficient 1 has to be of the form $x^2 + ax + b$. If $b = 0$, then $x = 0$ would be a root. Therefore we may take our quadratic to be $x^2 + ax + 1$ (since 1 is the only non-zero element in $\mathbb{Z}_2$). Substituting $x = 1$ gives $1 + a + 1$, so if the quadratic is irreducible, this must be non-zero and so the only irreducible quadratic over $\mathbb{Z}_2$ is $x^2 + x + 1$.
   Over $\mathbb{Z}_3$ our irreducible quadratic will have the form $x^2 + ax + b$ where b is 1 or -1. If $b = 1$, the condition that 1 is not a root is that $a - 1$ is non-zero, and the condition that -1 is not a root is that $-a - 1$ is non-zero. The only value of a satisfying both these conditions is $a = 0$. It follows that in this case $x^2 + 1$ is the only irreducible. When $b = -1$, we see that $f(1) = a$ and $f(-1) = -a$, so both $x^2 + x - 1$ and $x^2 - x - 1$ are irreducible. This gives three irreducible quadratics, namely $x^2 + 1$, $x^2 + x - 1$ and $x^2 - x - 1$.
4. If $x^4 + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$, equating coefficients of x^3 (or of x) gives $a + b = 0$ so $a = -b$. Now equate coefficients of x^2 to see that $0 = 2 + ab$, so $ab = -2$ and hence $a^2 = 2$. Thus we may take a to be $\sqrt{2}$ and b to be $-\sqrt{2}$. Then $x^8 - 1 = (x^4 - 1)(x^4 + 1)$. Also $x^4 - 1 = (x^2 + 1)(x^2 - 1)$. Now, $x^2 + 1$ does not factorise over $\mathbb{R}$ whereas $x^2 - 1 = (x + 1)(x - 1)$. Since $x^2 + \sqrt{2}x + 1$ and $x^2 - \sqrt{2}x + 1$ have no real roots, the factorisation of $x^8 - 1$ over $\mathbb{R}$ is

   $$x^8 - 1 = (x - 1)(x + 1)(x^2 + 1)(x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1).$$

   Then, using the quadratic formula, we see that over $\mathbb{C}$ the quadratic $x^2 + \sqrt{2}x + 1$ has zeros $\omega = \frac{-\sqrt{2}+i\sqrt{2}}{2}$ and $\overline{\omega} = \frac{-\sqrt{2}-i\sqrt{2}}{2}$. Similarly, we can find the real and imaginary parts of the zeros of the quadratic

$x^2 - \sqrt{2}x + 1$ (these turn out to be ω^3 and $\overline{\omega^3}$.) The factorisation of $x^8 - 1$ as a product of 8 linear terms is then

$$x^8 - 1 = (x+1)(x-1)(x+\mathrm{i})(x-\mathrm{i})(x-\omega)(x-\overline{\omega})(x-\omega^3)(x-\overline{\omega^3}).$$

When we come to factorise this polynomial over $\mathbb{Z}_3$, we need to find the factorisations of $x^2 + 1$ and $x^4 + 1$. The quadratic is irreducible. The quartic has no linear factors, since neither 1 nor 2 is a root of the polynomial. Since we know (from Exercise 6.3.3) the irreducible quadratics over $\mathbb{Z}_3$, it only remains to see if two of the three can multiply together to give $x^4 + 1$. Since the constant term is 1, the only candidates are $x^2 + x - 1$ and $x^2 - x - 1$. A simple calculation shows that the product of these is indeed $x^4 + 1$, so the complete factorisation of $x^8 - 1$ over $\mathbb{Z}_3$ is

$$x^8 - 1 = (x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1).$$

5. For cubics over $\mathbb{Z}_2$, we again can take the coefficient of x^3 to be 1 and the constant term to be 1, so we consider $f(x) = x^3 + ax^2 + bx + 1$. Putting $x = 1$, we obtain $a + b$, so provided that $a + b$ is non-zero (i.e. a is not equal to b), f will have no linear factor, so will be irreducible. The irreducible cubics are therefore $x^3 + x^2 + 1$ and $x^3 + x + 1$.
6. A general example may be made by taking g and h to be different irreducibles and f to be any scalar multiple of gh, for example, $g(x) = x - 1$, $h(x) = x + 1$ and $f(x) = x^2 - 1$.

Exercises 6.4

1. It follows from our general theory that the polynomial congruence classes are:

$$[0]_f, [1]_f, [2]_f, [x]_f, [1+x]_f, [2+x]_f, [2x]_f, [1+2x]_f, [2+2x]_f.$$

Now using the fact that $f = x^2 + x + 2$, we obtain the following table for the non-zero representatives (we have omitted the brackets and subscripts):

	1	2	x	$1+x$	$2+x$	$2x$	$2x+1$	$2x+2$
1	1	2	x	$1+x$	$2+x$	$2x$	$2x+1$	$2x+2$
2	2	1	$2x$	$2+2x$	$1+2x$	x	$x+2$	$x+1$
x	x	$2x$	$2x+1$	1	$1+x$	$x+2$	$2+2x$	2
$1+x$	$1+x$	$2+2x$	1	$x+2$	$2x$	2	x	$2x+1$
$2+x$	$2+x$	$1+2x$	$1+x$	$2x$	1	$2+2x$	1	$2x$
$2x$	$2x$	x	$x+2$	2	$2+2x$	$1+2x$	$x+1$	1
$1+2x$	$1+2x$	$x+2$	$2x+2$	x	1	$x+1$	2	$2x$
$2+2x$	$2+2x$	$x+1$	2	$1+2x$	$2x$	1	$2x$	$x+2$

Now to find a representative whose powers give all the others, first consider x. Its square is $2x + 1$ whose square is 2 so the eighth power of x is 1. In fact it follows from this that x has eight distinct powers and so these must be all the non-zero polynomial congruence classes.

2. Since 1 is a greatest common divisor for f and t, we know that there exist polynomials u, v such that $1 = uf + vt$. Multiply both sides of this equation by $r - s$ to get $r - s = u(r - s)f + v(r - s)t$. Now suppose that $[rt]_f = [st]_f$, so f divides $rt - st = (r - s)t$. In that case f divides the right-hand side of the above equation, so f divides $r - s$ and $[r]_f = [s]_f$.
3. (i) Since $f(x) = x^2 + x + 1$ is irreducible, our given polynomials, f, g have 1 as a greatest common divisor. Also $x^2 + x + 1 = (x)(x + 1) + 1$ and so $1 = (x^2 + x + 1) - x(x + 1)$. Thus an inverse for $x + 1$ is x.

   (ii) Now consider $x^3 + x^2 + x + 2$ and $x^2 + x$. We have that $x^3 + x^2 + x + 2 = (x)(x^2 + x) + x + 2$, and $x^2 + x = (x + 2)(x + 2) + 2$ (remember $p = 3$!).
   Finally 2 divides $x + 2$, so 2 (or 1) is a greatest common divisor for our given polynomials. This means that

$$\begin{aligned} 1 &= 2(x^2 + x) - 2(x + 2)(x + 2) \\ &= -(x^2 + x) + (x + 2)(x + 2) \\ &= -(x^2 + x) + (x + 2)((x^3 + x^2 + x + 2) - (x)(x^2 + x)). \end{aligned}$$

   After rearranging, this means that an inverse for $x^2 + x$ modulo $x^3 + x^2 + x + 2$ is $2x^2 + x + 2$.

   (iii) Since $x^2 + 1 = (x + 1)(x - 1) + 2$, a greatest common divisor is 2 and $2 = (x^2 + 1) - (x - 1)(x + 1)$, so $1 = (x^2 + 1)/2 - (x - 1)(x + 1)/2$. Thus an inverse for $x + 1$ is $-(x - 1)/2$.

Exercises 6.5

1. Let g be a polynomial over **B**. If g is irreducible, then 1 is not a zero of g so $g(1)$ is equal to 1. However, since every power of 1 is 1 itself, $g(1)$ is simply the sum of the coefficients of g (including the constant term). Since those coefficients which are zero do not contribute to this sum, we deduce that the number of powers of x with non-zero coefficient must be an odd integer.
2. Clearly $x = 1$ is a zero of $x^5 - 1$, and $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$. Now the above quartic has no zeros, so the only possible factorisation would be as a product of irreducible quadratics. However, we

saw in Exercise 6.3.3, that the only irreducible quadratic over **B** is $x^2 + x + 1$. Since the square of $x^2 + x + 1$ is $x^4 + x^2 + 1$, we deduce that $x^4 + x^3 + x^2 + x + 1$ is irreducible. Thus the only possible generator polynomials for cyclic codes are

$$1, \qquad x + 1, \qquad x^4 + x^3 + x^2 + x + 1, \qquad \text{and} \qquad x^5 - 1.$$

The first gives all vectors of length 5 as codewords (and so detects and corrects zero errors), the last has no non-zero codewords. The generator matrices corresponding to $x + 1$ and $x^4 + x^3 + x^2 + x + 1$ are, respectively,

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}; \qquad (1 \quad 1 \quad 1 \quad 1 \quad 1).$$

It is clear that the first of these produces the code consisting of the 16 words of even length in $\mathbf{B}^5$ and so detects an error, but cannot correct any error. The second gives a code with 2 words, and so detects up to 4 errors with 2, or fewer errors, being corrected.

3. The matrix associated with the given code is

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

This code has 16 codewords

0000000	1011000	0101100	1110100
0010110	1001110	0111010	1100010
0011101	1000101	0110001	1101001
0001011	1010011	0100111	1111111

It is clear that the minimum distance between codewords is 3. If, therefore, we add any vector with six zeros and a single 1 to a codeword, we cannot obtain another codeword. It follows that each of the 16 codewords is a distance of 1 away from seven non-codewords, so there are $8 \times 16 = 2^3 \times 2^4 = 2^7$ codewords in these (disjoint, note) 'spheres of radius one' around codewords. As we remarked in the text, this is precisely one of the basic properties of the Hamming code. (In fact looking at the generator matrix for the Hamming code on page 249 in the text, we can see each row is one of the above codewords.)

4. To determine all cyclic codes of length 7, we needed to factorise $x^7 - 1$. Clearly $x - 1$ is a factor. By now the codes associated with 1, $x + 1$ and $x^7 - 1$ are familiar, so we are only left with those polynomials which divide $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. However, we are given one of these in Exercise 6.5.3, so it is only a matter of working out what happens when we divide $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ by $x^3 + x^2 + 1$. The answer turns out to be $g(x) = x^3 + x + 1$ and so we have a complete list of cyclic codes once we know the code associated with $g(x)$. As in Exercise 6.5.3, we can easily write now the generator matrix for this code and hence its codewords. It then turns out that the minimum distance is again 3 and so this code detects up to 2 errors and corrects up to 1 error.
5. Let $p(x)$ be a parity polynomial for a cyclic code of length n and generator polynomial $g(x)$. This means that $p(x)g(x) = x^n - 1 = f(x)$. Thus if g has degree k, then p has degree $n - k$. Now suppose that $c(x)$ is a polynomial with $[c(x)p(x)]_f = [0]_f$, so $f(x)$ divides $c(x)p(x)$. Write $c(x)$ in the form $q(x)g(x) + r(x)$ (with r either zero or of degree less than k) and multiply throughout by $p(x)$ to get $[0]_f = [q(x)p(x)g(x) + r(x)p(x)]_f$. Thus $[0]_f = [r(x)p(x)]_f$ which is impossible unless $r(x)$ is zero, otherwise $r(x)p(x)$ would have degree less than n. We deduce that $r(x)$ is the zero polynomial and so $g(x)$ divides $c(x)$ and, therefore, $c(x)$ is a codeword.

References and further reading

Allenby, R.B.J.T., *Rings, Fields and Groups*, Edward Arnold, London, 1983.
[Further reading in algebra.]

Bell, E.T., *Men of Mathematics*, Simon and Schuster, New York, 1937. Pelican edition (2 vols.), 1953.
[Anecdotal, and not very reliable: but probably the best known biographical/historical work.]

Biggs, N.L., *Discrete Mathematics*, Clarendon Press, Oxford, 1985.
[Comprehensive and readable.]

Boole, G., *An Investigation of the Laws of Thought*, Dover, New York, 1957 (reprint of the 1854 edition).

Boyer, C.B., *A History of Mathematics*, Wiley, New York, 1968.
[From ancient times to the twentieth century; readable and recommended. Contains an extensive annotated bibliography.]

Bühler, W.K., *Gauss*, Springer-Verlag, Berlin, 1981.
[Biography of Gauss.]

Carroll, L., *Symbolic Logic and the Game of Logic*, Dover, New York, 1958 (reprint of the 1896 original).

Dauben, J.W., *Georg Cantor*, Harvard, Cambridge, MA, 1979.
[Engrossing account of a radical shift in mathematics.]

Davenport, H., *The Higher Arithmetic*, 5th edn. Cambridge University Press, Cambridge, 1982.
[Readable account of elementary number theory.]

Diffie, W. and Hellman, M.E., New directions in cryptography, *IEEE Transactions on Information Theory*, **22** (1976), 644–654.

Enderton, H.B., *A Mathematical Introduction to Logic*, 2nd edn., Academic Press, New York, 2001.
[Readable, quite advanced.]

Enderton, H.B., *Elements of Set Theory*, Academic Press, New York, 1977.
[Readable.]

Eves, H., *An Introduction to the History of Mathematics*, 5th edn., Holt, Rinehart and Winston, New York, 1983.
[A popular textbook.]

Fauvel, J. and Gray, J. (eds.), *The History of Mathematics: A Reader*, Macmillan/Open University, London and Milton Keynes, 1988.
[Contains excerpts from original sources.]

Flegg, H.G., *Boolean Algebra*, Macdonald, London, 1971.

Fraenkel, A.A., *Set Theory and Logic*, Addison-Wesley, Reading, MA, 1966.
[Further reading, especially on infinite arithmetic.]

Fraleigh, J.B., *A First Course in Abstract Algebra*, 6th edn., Addison-Wesley, Reading, MA, 1999.
[Further reading in algebra.]

Gauss, C.F., *Disquisitiones Arithmeticae*, translated by A.A. Clarke, Yale University Press, New Haven, CT, 1966, revised by W.C. Waterhouse, Springer-Verlag, New York, 1986.

Grattan-Guinness, I., *The Development of the Foundations of Mathematical Analysis from Euler to Riemann*, MIT Press, Cambridge, MA, 1970.
[Contains much more on the development of the notion of function.]

Hankins, T.L., *Sir William Rowan Hamilton*, Johns Hopkins University Press, Baltimore, MD, 1980.
[Hamilton's life and work.]

Heath, T.L., *The Thirteen Books of Euclid's Elements* (3 vols.), Cambridge University Press, Cambridge, 1908. Reprinted Dover, New York, 1956.

Heath, T.L., *A History of Greek Mathematics*, vol. 1 (from Thales to Euclid), vol. 2 (from Aristarchus to Diophantus), Clarendon Press, Oxford, 1921.
[For many years the standard on Greek Mathematics.]

Heath, T.L., *Diophantus of Alexandria*, 2nd edn., Cambridge University Press, Cambridge, 1910, reprinted by Dover, 1964.

Hill, R., *A First Course in Coding Theory*, Clarendon Press, Oxford, 1986.
[Further reading on (error-correcting) codes.]

Hodges, W., *Logic*, Penguin, Harmondsworth, 1977.

Kalmanson, K., *An Introduction to Discrete Mathematics and its Applications*, Addison-Wesley, Reading, MA, 1986.

Kline, M., *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, New York, 1972.
[Readable and comprehensive: controversial views on the direction of twentieth century mathematics.]

Landau, S., Zero knowledge and the Department of Defense, *Notices Amer. Math. Soc.*, **35** (1988), 5–12.

Ledermann, W., *Introduction to Group Theory*, Oliver and Boyd, Edinburgh, 1973 (reprinted, Longman, 1976).
[Clearly written.]

Li Yan and Du Shiran, *Chinese Mathematics*, translated by Crossley, J.N. and Lun, W.-C., Clarendon Press, Oxford, 1987.
[Up to date and detailed.]

Lyndon, R.C., *Groups and Geometry*, LMS Lecture Note Series vol. 101, Cambridge University Press, Cambridge, 1985.
[Readable.]

MacLane, S. and Birkhoff, G., *Algebra*, Macmillan, New York, 1967.
[A classic text, relatively advanced.]

Manheim, J.H., *The Genesis of Point Set Topology*, Pergamon, Oxford, 1964.
[Especially Chapters I–III for the development of the notion of function.]

Marcus, M., *A Survey of Finite Mathematics*, Houghton Mifflin, Boston, MA, 1969.
[A relatively advanced text on the topic.]

Needham, J., in collaboration with Wang Ling, *Science and Civilisation in China*, vol. 3 (Mathematics and the Sciences of the Heavens and the Earth), Cambridge University Press, Cambridge, 1959.
[The classic text.]

Rabin, M.O., Digitalized signatures and public-key functions as intractable as factorization, Technical Report, MIT/LCS/TR-212, MIT, 1979.

Rivest, R., Shamir, A. and Adleman, L., A method for obtaining digital signatures and public-key cryptosystems, *ACM Communications*, **21** (Feb. 1978), 120–6.

Salomaa, A., *Computation and Automata*, Cambridge University Press, Cambridge, 1985.
[Further reading on finite state machines and related topics. Quite advanced.]

Shamir, A., A polynomial time algorithm for breaking the basic Merkle–Hellman cryptosystem, *IEEE Transactions on Information Theory*, **30** (1984), 699–704.

Shurkin, J., *Engines of the Mind*, W.W. Norton and Co., New York, 1984.
[A lively account of the development of computers.]

van der Waerden, B.L., *A History of Algebra*, Springer-Verlag, Berlin, 1985.
[From the ninth century onwards.]

Venn, J., On the diagrammatic and mechanical representation of propositions and reasonings, *Philos. Mag.*, July 1880.

Weil, A., *Number Theory (An approach through history. From Hammurapi to Legendre)*, Birkhäuser, Boston, MA, 1984.
[Traces the development of number-theoretic concepts.]

Wussing, H., *The Genesis of the Abstract Group Concept*, MIT Press, Cambridge, MA, 1984, translation by A. Shenitzer of *Die Genesis des abstrakten Gruppenbegriffes*, VEB Deutscher Verlag Wiss., Berlin, 1969.

Biography

The following biographical data have been culled mainly from Gillispie, C.C., *et al., Dictionary of Scientific Biography*, Charles Scribner's & Sons, New York, 1970, to which you are referred for (much) more detail. A great deal of information on the history of mathematics, including biographies and contemporary developments, may be found at www-gap.dcs.st-and.ac.uk/history/index.html.

Abel, Niels Henrik: b. Finnöy Island near Stavanger, Norway, 1802; d. Frøland, Norway, 1829. Main work on elliptic integrals and the unsolvability by radicals of the general quintic.

Alembert, Jean le Rond d': b. Paris, France, 1717; d. Paris, France, 1783. Main work in mechanics; an Encyclopédiste.

Argand, Jean Robert: b. Geneva, Switzerland, 1768; d. Paris France, 1822. One of those who found a geometric representation of complex numbers. Also work on the Fundamental Theorem of Algebra.

Babbage, Charles: b. Teignmouth, Devon, England, 1792; d. London, England, 1871. Extremely diverse interests. Designed and partially built mechanical 'computers'.

Bachet de Meziriac, Claude-Gaspar: b. Bourg-en-Bresse, France, 1581; d. Bourg-en-Bresse, France, 1638. Best known for his edition of Diophantus' *Arithmetica* and his book of mathematical recreations and problems, *Problèmes plaisants et délectables qui se font par les nombres*.

Bernoulli, Daniel: b. Groningen, Netherlands, 1700; d. Basel, Switzerland, 1782. Work in mathematics and physics as well as medicine.

Bernoulli, Johann (Jean): b. Basel, Switzerland, 1667; d. Basel, Switzerland, 1748. Work in mathematics, especially the calculus.

Boole, George: b. Lincoln, England, 1815; d. Cork, Ireland, 1864. Worked on logic, probability and differential equations.

Brahmagupta: b. 598; d. after 665. Indian mathematician and astronomer.

Bravais, Auguste: b. Annonay, France, 1811; d. Le Chesnay, France, 1863. Main work on crystallography. Also made contributions in botany, astronomy and surveying.

Cantor, Georg: b. St Petersburg, Russia, 1845; d. Halle, Germany, 1918. His development of set theory and infinite numbers began with work on convergence of trigonometric series.

Cardano, Girolamo: b. Pavia, Italy, 1501; d. Rome, Italy, 1576. Practitioner of medicine. Wrote on many topics including mathematics. Was imprisoned for some months for having cast the horoscope of Christ.

Cauchy, Augustin-Louis: b. Paris, France, 1789; d. Sceaux, near Paris, France, 1857. An oustanding mathematician of the first half of the nineteenth century. Main contributions in analysis.

Cayley, Arthur: b. Richmond, Surrey, England, 1821; d. Cambridge, England, 1895. Practised as a barrister for fourteen years, during which time he wrote about 300 mathematical papers. Main contributions in invariant theory.

De Morgan, Augustus: b. Madura, India, 1806; d. London, England, 1871. Contributions in analysis and logic.

Dedekind, Richard: b. Brunswick, Germany, 1831; d. Brunswick, Germany, 1916. Work in algebra, especially number theory, and analysis.

Descartes, René du Perron: b. La Haye, Touraine, France, 1596; d. Stockholm, Sweden, 1650. Fundamental work in mathematics, physics and especially philosophy.

Diophantus (of Alexandria, Egypt): fl. AD 250. Main work is his *Arithmetica*: a collection of problems representing the high point of Greek work in number theory.

Dirichlet, Gustav Peter Lejeune: b. Düren, Germany, 1805; d. Göttingen, Germany, 1859. Important work in number theory, analysis and mechanics.

Dodgson, Charles Lutwidge: b. Daresbury, Cheshire, England, 1832; d. Guildford, Surrey, England, 1898. Better known as Lewis Carroll, author of the 'Alice' books. Some contributions to mathematics and logic.

Dyck, Walther Franz Anton von: b. Munich, Germany, 1856; d. Munich, Germany, 1934. Noteworthy contributions in various parts of mathematics.

Eratosthenes: b. Cyrene, now in Libya, c. 276 BC; d. Alexandria, Egypt, c. 195 BC. One of the foremost scholars of the time. Best known for his work on geography and mathematics.

Euclid: fl. Alexandria, Egypt (and Athens?), c. 295 BC. Author of the *Elements*, one of the most influential books on Western thought.

Euler, Leonhard: b. Basel, Switzerland, 1707; d. St Petersburg, Russia, 1783. Enormously productive mathematician (wrote and published more than any other mathematician) who also made contributions to mechanics and astronomy.

Fermat, Pierre de; b. Beaumont-de-Lomagne, France, 1601; d. Castres, France, 1665. Fundamental work in number theory.

Ferrari, Ludovico: b. Bologna, Italy, 1522; d. Bologna, Italy, 1565. Pupil of Cardano; work in algebra.

del Ferro, Scipione: b. Bologna, Italy, 1465; d. Bologna, Italy, 1526. An algebraist, first to find solution of (a particular form of) the cubic equation.

Fibonacci, Leonardo (or Leonardo of Pisa): b. Pisa, Italy, 1170; d. Pisa, Italy after 1240. Author of a number of works on computation, measurement and geometry and number theory.

Fourier, Jean Baptiste Joseph: b. Auxerre, France, 1768; d. Paris, France, 1830. Best known for his work on the diffusion of heat and the mathematics that he introduced to deal with this. Accompanied Napoleon to Egypt, where he held various diplomatic posts.

Frénicle de Bessy, Bernard: b. Paris, France, 1605; d. Paris, France, 1675. Accomplished amateur mathematician. Corresponded with other mathematicians, especially on number theory.

Galois, Evariste: b. Bourg-la-Reine near Paris, France, 1811; d. Paris, France, 1832. Determined conditions for the solvability of equations by radicals; founder of group theory. A fervent republican, he died from a wound received in a possibly contrived duel: his funeral was the occasion of a republican demonstration in Paris.

Gauss, Carl Friedrich: b. Brunswick, Germany, 1777; d. Göttingen, Germany, 1855. One of the greatest mathematicians of all time, he made fundamental contributions to many parts of mathematics and the mathematical sciences.

Gibbs, Josiah Willard: b. New Haven, CT, USA, 1839; d. New Haven, CT, USA, 1903. Important work in thermodynamics and statistical mechanics.

Gödel, Kurt: b. Brünn, now Brno, Czech Republic, 1906; d. Princeton, NJ, USA, 1978. Outstanding mathematical logician of the twentieth century.

Goldbach, Christian: b. Königsberg, Prussia (now Kaliningrad), 1690; d. Moscow, Russia, 1764. Administrator of the Imperial Academy of Sciences in St Petersburg. Corresponded with many scientists and dabbled in mathematics.

Grassmann, Hermann Günther: b. Stettin (now Szczecin, Poland), 1809; d. Stettin, Germany, 1877. Work in geometry and algebra, as well as comparative linguistics and Sanskrit.

Gregory, Duncan Farquharson: b. Edinburgh, Scotland, 1813; d. Edinburgh, Scotland, 1844. Work on laws of algebra.

Hamilton, (Sir) William Rowan: b. Dublin, Ireland, 1805; d. Dunsink Observatory near Dublin, Ireland, 1865. An accomplished linguist by the age of nine, Hamilton made important contributions to mathematics, mechanics and optics.

Hamming, Richard Wesley: b. Chicago, IL, USA, 1915; d. Monterey, CA, USA, 1998. Best known for fundamental work on codes.

Hasse, Helmut: b. Kassel, Germany 1898; d. Ahrensburg, nr. Hamburg, Germany, 1979. Work in number theory.

Hensel, Kurt: b. Königsberg, Germany (now Kaliningrad), 1861; d. Marburg, Germany, 1941. Main work in number theory and related topics.

Hollerith, Herman: b. Buffalo, NY, USA, 1860; d. Washington DC, USA, 1929. His work on the USA census led him to the use of punched card machines for processing data. Founded a company which was later to develop into IBM.

I-Hsing: flourished in China in the early part of the eighth century.

Jordan, Camille: b. Lyons, France, 1838; d. Paris, France 1921. Published in most areas of mathematics: outstanding figure in group theory.

al-Khwarizmi, Abu Ja'far Muhammad ibn Musa: b. before 800; d. after 847. Author of influential treatises on algebra, astronomy and geography.

Klein, Christian Felix: b. Düsseldorf, Germany, 1849; d. Göttingen, Germany, 1925. Contributions in most areas of mathematics, especially geometry and function theory.

Kronecker, Leopold: b. Liegnitz, Germany (now Legnica, Poland), 1823; d. Berlin, Germany, 1891. Work in a number of areas of mathematics, especially elliptic functions.

Lagrange, Joseph Louis: b. Turin, Italy, 1736; d. Paris, France, 1813. Worked in analysis and mechanics as well as algebra.

Leibniz, Gottfried Wilhelm: b. Leipzig, Germany, 1646; d. Hannover, Germany, 1716. One of the inventors of the calculus. Many contributions to mathematics and philosophy.

Liouville, Joseph: b. St-Omer, Pas-de-Calais, France, 1839; d. Paris, France, 1882. Main work in analysis.

Mathieu, Emile Léonard: b. Metz, France, 1835; d. Nancy, France, 1890. Contributions to mathematics and mathematical physics.

Mersenne, Marin: b. Oizé, Maine, France, 1588; d. Paris, France, 1648. Contributions in acoustics and optics and other areas of natural philosophy. Actively aided the development of a European scientific community by his correspondence and drawing many visitors to his convent in Paris.

Newton, Isaac: b. Woolsthorpe, Lincolnshire, England, 1642; d. London, England, 1727. Often classed with Archimedes as the greatest of scientists, his contributions in mathematics were many and he was, with Leibniz, independent co-founder of the calculus.

Pascal, Blaise: b. Clermont-Ferrand, Puy-de-Dôme, France, 1623; d. Paris, France, 1662. Work in mathematics and physics as well as writings in other areas.

Peacock, George: b. Denton, near Darlington, county Durham, England, 1791; d. Ely, England, 1858. Work important in the development of the concept of abstract algebra.

Peirce, Benjamin: b. Salem, MA, USA, 1809; d. Cambridge, MA, USA, 1880. Leading American mathematician of his time.

Peirce, Charles Sanders: b. Cambridge, MA, USA, 1839; d. 1914. Son of Benjamin Peirce, who took great care over his son's mathematical education. His main work was in logic and philosophy.

Philolaus of Crotona (now in Italy): flourished in the second half of the fifth century BC. Proposed a heliocentric astronomical system.

Qín Jiǔsháo: b. Sichuan, China, c.1202; d. Guangdong, China, c.1261. Author of the *Mathematical Treatise in Nine Sections* which includes the 'Chinese Remainder Theorem' and variants of it. A civil servant, accomplished in many areas, notorious for his inclination to poison those he found disagreeable.

Ruffini, Paolo: b. Valentano, Italy, 1765; d. Modena, Italy, 1822. Practised medicine as well as being active in mathematics including work on algebraic equations and probability.

Serret, Joseph Alfred: b. Paris, France, 1819; d. Versailles, France, 1885. Work in various mathematical areas and author of a number of popular textbooks.

Steinitz, Ernst: b. Laurahütte, Silesia, Germany (now Huta Laura, Poland), 1871; d. Kiel, Germany, 1928. Main work on the general algebraic notion of a field.

Sylow, Peter Ludvig Mejdell: b. Christiania (now Oslo), Norway, 1832; d. Christiania, Norway, 1918. Established fundamental results on the structure of finite groups.

Tartaglia (real name Fontana), Niccolò: b. Brescia, Italy, 1499 or 1500; d. Venice, 1557. Contributions to mathematics, mechanics and military science.

Taylor, Brook: b. Edmonton, Middlesex, England 1685; d. London, England 1731. Made contributions to the theory of functions, including infinite series, and physics.

Turing, Alan Mathison: b. London, England, 1912; d. Wilmslow, Cheshire, England, 1954. Known best for 'Turing machines' and his code-breaking work.

Venn, John: b. Hull, Yorkshire, England, 1834; d. Cambridge, England, 1923. Work on probability and logic.

Viète, François: b. Fontenay-le-Comte, Poitou, France, 1540; d. Paris, France, 1603. Work in trigonometry, algebra and geometry. Important innovations in use of symbolism in mathematics.

Wallis, John: b. Ashford, Kent, England, 1616; d. Oxford, England, 1703. Work on algebra and functions.

Weber, Heinrich: b. Heidelberg, Germany, 1842; d. Strasbourg, Germany (now in France), 1913. Work in analysis, mathematical physics and especially algebra.

Zermelo, Ernst Friedrich Ferdinand: b. Berlin, Germany, 1871; d. Freiburg im Breisgau, Germany, 1953. Main work in set theory.

Name index

Subject index

Boldface indicates a page on which a term is defined.