CHAPTER 16
GROUPS, CODING THEORY, AND POLYA'S METHOD OF ENUMERATION

Section 16.1

1. (a) Yes. The identity is 1 and each element is its own inverse.
(b) No. The set is not closed under addition and there is no identity.
(c) No. The set is not closed under addition.
(d) Yes. The identity is 0; the inverse of $10n$ is $10(-n)$ or $-10n$.
(e) Yes. The identity is 1_A and the inverse of $g : A \to A$ is $g^{-1} : A \to A$.
(f) Yes. The identity is 0; the inverse of $a/(2^n)$ is $(-a)/(2^n)$.

2. (c) $ab = ac \Longrightarrow a^{-1}(ab) = a^{-1}(ac) \Longrightarrow (a^{-1}a)b = (a^{-1}a)c \Longrightarrow eb = ec \Longrightarrow b = c$

(d) $ba = ca \Longrightarrow (ba)a^{-1} = (ca)a^{-1} \Longrightarrow b(aa^{-1}) = c(aa^{-1}) \Longrightarrow be = ce \Longrightarrow b = c$

3. Subtraction is not an associative (closed) binary operation – e.g., $(3-2)-4 = -3 \neq 5 = 3-(2-4)$.

4. (i) For all $a, b, c \in G$,
$(a \circ b) \circ c = (a+b+ab) \circ c = a+b+ab+c+(a+b+ab)c = a+b+ab+c+ac+bc+abc$
$a \circ (b \circ c) = a \circ (b+c+bc) = a+b+c+bc+a(b+c+bc) = a+b+c+bc+ab+ac+abc.$
Since $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$ it follows that the (closed) binary operation is associative.
(ii) If $x, y \in G$, then $x \circ y = x+y+xy = y+x+yx = y \circ x$, so the (closed) binary operation is also commutative.
(iii) Can we find $a \in G$ so that $x = x \circ a$ for all $x \in G$?
$x = x \circ a \Longrightarrow x = x+a+xa \Longrightarrow 0 = a(1+x) \Longrightarrow a = 0$, because x is arbitrary, so 0 is the identity for this (closed) binary operation.
(iv) For $x \in G$, can we find $y \in G$ with $x \circ y = 0$? Here $0 = x \circ y = x+y+xy \Longrightarrow -x = y(1+x) \Longrightarrow y = -x(1+x)^{-1}$, so the inverse of x is $-x(1+x)^{-1}$.
It follows from (i) - (iv) that $(G, \circ)$ is an abelian group.

5. Since $x, y \in \mathbf{Z} \Longrightarrow x+y+1 \in \mathbf{Z}$, the operation is a (closed) binary operation (or $\mathbf{Z}$ is closed under $\circ$). For all $w, x, y \in \mathbf{Z}$, $w \circ (x \circ y) = w \circ (x+y+1) = w+(x+y+1)+1 = (w+x+1)+y+1 = (w \circ x) \circ y$, so the (closed) binary operation is associative. Furthermore, $x \circ y = x+y+1 = y+x+1 = y \circ x$, for all $x, y \in \mathbf{Z}$, so $\circ$ is also commutative. If $x \in \mathbf{Z}$ then $x \circ (-1) = x+(-1)+1 = x [= (-1) \circ x]$, so -1 is the identity element for $\circ$. And finally, for

each $x \in \mathbf{Z}$, we have $-x-2 \in \mathbf{Z}$ and $x \circ (-x-2) = x+(-x-2)+1 = -1 [= (-x-2)+x]$, so $-x-2$ is the inverse for x under $\circ$. Consequently, $(\mathbf{Z}, \circ)$ is an abelian group.

6. (i) For all $(a,b),(u,v),(x,y) \in S$ we have
$(a,b) \circ [(u,v) \circ (x,y)] = (a,b) \circ (ux, vx+y) = (aux, bux+vx+y)$
$[(a,b) \circ (u,v)] \circ (x,y) = (au, bu+v) \circ (x,y) = (aux, (bu+v)x+y) = (aux, bux+vx+y)$,
so the given (closed) binary operation is associative.
(ii) To find the identity element we need $(a,b) \in S$ such that $(a,b) \circ (u,v) = (u,v) = (u,v) \circ (a,b)$ for all $(u,v) \in S$.
$(u,v) = (u,v) \circ (a,b) = (ua, va+b) \Longrightarrow u = ua$ and $v = va+b \Longrightarrow a = 1$ and $b = 0$.
In addition, $(1,0) \circ (u,v) = (1 \cdot u, 0 \cdot u + v) = (u,v)$, so $(1,0)$ is the identity for this (closed) binary operation.
(iii) Given $(a,b) \in S$ can we find $(c,d) \in S$ so that $(a,b) \circ (c,d) = (c,d) \circ (a,b) = (1,0)$?
$(1,0) = (a,b) \circ (c,d) = (ac, bc+d) \Longrightarrow 1 = ac$, $0 = bc+d \Longrightarrow c = a^{-1}$, $d = -ba^{-1}$.
Since $(a^{-1}, -ba^{-1}) \circ (a,b) = (a^{-1}a, (-ba^{-1})a + b) = (1,0)$, $(a^{-1}, -ba^{-1})$ is the inverse of (a,b) for this (closed) binary operation.
From (i)-(iii) it follows that $(S, \circ)$ is a group. Since $(1,2),(2,3) \in S$ and $(1,2) \circ (2,3) = (2,7)$, while $(2,3) \circ (1,2) = (2,5)$, this group is nonabelian.

7. $U_{20} = \{1,3,7,9,11,13,17,19\}$

$U_{24} = \{1,5,7,11,13,17,19,23\}$

8. Proof: Suppose that G is abelian and that $a, b \in G$. Then $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2$, by using the associative property for a group and the fact that this group is abelian.
Conversely, suppose that G is a group where $(ab)^2 = a^2b^2$ for all $a, b \in G$. If $x, y \in G$, then $(xy)^2 = x^2y^2 \Rightarrow (xy)(xy) = x^2y^2 \Rightarrow x(yx)y = x(xy^2) \Rightarrow (yx)y = xy^2$ (by Theorem 16.1 (c)) $\Rightarrow (yx)y = (xy)y \Rightarrow yx = xy$ (by Theorem 16.1 (d)). Therefore, the group G is abelian.

9. (a) The result follows from Theorem 16.1(b) since both $(a^{-1})^{-1}$ and a are inverses of a^{-1}.
(b) $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}(e)b = b^{-1}b = e$ and $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(e)a^{-1} = aa^{-1} = e$. So $b^{-1}a^{-1}$ is an inverse of ab, and by Theorem 16.1(b), $(ab)^{-1} = b^{-1}a^{-1}$.

10. G abelian $\Longrightarrow a^{-1}b^{-1} = b^{-1}a^{-1}$. By Exercise 9(b), $b^{-1}a^{-1} = (ab)^{-1}$, so G abelian $\Longrightarrow a^{-1}b^{-1} = (ab)^{-1}$. Conversely, if $a, b \in G$, then $a^{-1}b^{-1} = (ab)^{-1} \Longrightarrow a^{-1}b^{-1} = b^{-1}a^{-1} \Longrightarrow ba^{-1}b^{-1} = a^{-1} \Longrightarrow ba^{-1} = a^{-1}b \Longrightarrow b = a^{-1}ba \Longrightarrow ab = ba \Longrightarrow G$ is abelian.

11. (a) $\{0\}$; $\{0,6\}$; $\{0,4,8\}$; $\{0,3,6,9\}$; $\{0,2,4,6,8,10\}$; $\mathbf{Z}_{12}$.
(b) $\{1\}$; $\{1,10\}$; $\{1,3,4,5,9\}$; $\mathbf{Z}_{11}^*$.
(c) $\{\pi_0\}$; $\{\pi_0, \pi_1, \pi_2\}$; $\{\pi_0, r_1\}$; $\{\pi_0, r_2\}$; $\{\pi_0, r_3\}$; S_3

12. (a) There are eight rigid motions for a square: π_0, π_1, π_2, π_3, where π_i is the

counterclockwise rotation through $i(90°)$, $0 \leq i \leq 3$; r_1 is the reflectin in the vertical; r_2 is the reflection in the horizontal; r_3 the reflection in the diagonal from lower left to upper right; and r_4 the reflection in the diagonal from upper left to lower right.

(b)

o	π_0	π_1	π_2	π_3	r_1	r_2	r_3	r_4
π_0	π_0	π_1	π_2	π_3	r_1	r_2	r_3	r_4
π_1	π_1	π_2	π_3	π_0	r_3	r_4	r_2	r_1
π_2	π_2	π_3	π_0	π_1	r_2	r_1	r_4	r_3
π_3	π_3	π_0	π_1	π_2	r_4	r_3	r_1	r_2
r_1	r_1	r_4	r_2	r_3	π_0	π_2	π_3	π_1
r_2	r_2	r_3	r_1	r_4	π_2	π_0	π_1	π_3
r_3	r_3	r_1	r_4	r_2	π_1	π_3	π_0	π_2
r_4	r_4	r_2	r_3	r_1	π_3	π_1	π_2	π_0

π_0 is the group identity.

The inverse of each reflection is the same reflection. The inverse of the rotation π_1 is the rotation π_3, and conversely. The inverse of the rotation π_2 is itself. Also, the inverse of π_0 is π_0.

13. (a) There are 10: five rotations through $i(72°), 0 \leq i \leq 4$, and five reflections about lines containing a vertex and the midpoint of the opposite side.
(b) For a regular n-gon ($n \geq 3$) there are $2n$ rigid motions. There are the n rotations through $i(360°/n)$, $0 \leq i \leq n-1$. There are n reflections. For n odd each reflection is about a line through a vertex and the midpoint of the opposite side. For n even, there are $n/2$ reflections about lines through opposite vertices and $n/2$ reflections about lines through the midpoints of opposite sides.

14.

$$\alpha\beta = \begin{pmatrix}12345\\15234\end{pmatrix}, \qquad \beta\alpha = \begin{pmatrix}12345\\32514\end{pmatrix}, \qquad \alpha^3 = \begin{pmatrix}12345\\12345\end{pmatrix},$$

$$\beta^4 = \begin{pmatrix}12345\\12534\end{pmatrix}, \qquad \alpha^{-1} = \begin{pmatrix}12345\\31245\end{pmatrix}, \qquad \beta^{-1} = \begin{pmatrix}12345\\21453\end{pmatrix},$$

$$(\alpha\beta)^{-1} = \begin{pmatrix}12345\\13452\end{pmatrix}, \qquad (\beta\alpha)^{-1} = \begin{pmatrix}12345\\42153\end{pmatrix}, \qquad \beta^{-1}\alpha^{-1} = \begin{pmatrix}12345\\13452\end{pmatrix}.$$

15. Since $eg = ge$ for all $g \in G$, it follows that $e \in H$ and $H \neq \emptyset$. If $x, y \in H$, then $xg = gx$ and $yg = gy$ for all $g \in G$. Consequently, $(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$ for all $g \in G$, and we have $xy \in H$. Finally, for all $x \in H$ and $g \in G$, $xg^{-1} = g^{-1}x$. So $(xg^{-1})^{-1} = (g^{-1}x)^{-1}$, or $gx^{-1} = x^{-1}g$, and $x^{-1} \in H$. Therefore H is a subgroup of G.

16. (a)

$\omega = (1/\sqrt{2})(1+i)$ $\qquad$ $\omega^2 = i$

$\omega^3 = (1/\sqrt{2})(-1+i)$ $\qquad$ $\omega^4 = -1$

$\omega^5 = (1/\sqrt{2})(-1-i)$ $\qquad$ $\omega^6 = -i$

$\omega^7 = (1/\sqrt{2})(1-i)$ $\qquad$ $\omega^8 = 1$

(b) Let $S = \{\omega^n | 1 \leq n \leq 8\}$. Then for all $1 \leq j, k \leq 8$, $\omega^j \cdot \omega^k = \omega^m$, where $m \equiv j + k \pmod 8$ and $1 \leq m \leq 8$. So S is closed under the binary operation of multiplication, which is commutative and associative for all complex numbers – so, in particular, the complex numbers is S.
The element $\omega^8 = 1$ is the identity element and, for all $1 \leq n \leq 7$, we have $(\omega^n)^{-1} = \omega^{8-n}$, so every element of S has a multiplicative inverse in S.
Consequently, S is an abelian group under multiplication.

17. (a) Let $(g_1, h_1), (g_2, h_2) \in G \times H$. Then $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2)$, where $g_1 \circ g_2 \in G$, $h_1 * h_2 \in H$, since $(G, \circ)$ and $(H, *)$ are closed. Hence $G \times H$ is closed.
For $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$, $[(g_1, h_1) \cdot (g_2, h_2)] \cdot (g_3, h_3) = (g_1 \circ g_2,\ h_1 * h_2) \cdot (g_3, h_3) = ((g_1 \circ g_2) \circ g_3, (h_1 * h_2) * h_3) = (g_1 \circ (g_2 \circ g_3), h_1 * (h_2 * h_3)) = (g_1, h_1) \cdot (g_2 \circ g_3, h_2 * h_3) = (g_1, h_1) \cdot [(g_2, h_2) \cdot (g_3, h_3)]$, since the operations in G and H are associative. Hence, $G \times H$ is associative under $\cdot$.
Let e_G, e_H denote the identities for G, H, respectively. Then (e_G, e_H) is the identity in $G \times H$.
Finally, let $(g, h) \in G \times H$. If g^{-1} is the inverse of g in G and h^{-1} is the inverse of h in H, then (g^{-1}, h^{-1}) is the inverse of (g, h) in $G \times H$.

(b) (i) 216
(ii) $H_1 = \{(x, 0, 0) | x \in \mathbf{Z}_6\}$ is a subgroup of order 6; $H_2 = \{(x, y, 0) | x, y \in \mathbf{Z}_6,\ y = 0, 3\}$ is a subgroup of order 12; $H_3 = \{(x, y, 0) | x, y \in \mathbf{Z}_6\}$ has order 36.
(iii) $-(2, 3, 4) = (4, 3, 2)$; $-(4, 0, 2) = (2, 0, 4)$; $-(5, 1, 2) = (1, 5, 4)$.

18. (a) Since $e \in H$ and $e \in K$, we have $e \in H \cap K$ and $H \cap K \neq \emptyset$. Now let $x, y \in H \cap K$.
$x, y \in H \cap K \Longrightarrow x, y \in H$ and $x, y \in K \Longrightarrow xy \in H$ and $xy \in K$ (since H, K are subgroups) $\Longrightarrow xy \in H \cap K$
$x \in H \cap K \Longrightarrow x \in H$ and $x \in K \Longrightarrow x^{-1} \in H$ and $x^{-1} \in K$ (because H, K are subgroups) $\Longrightarrow x^{-1} \in H \cap K$.
Therefore by Theorem 16.2 we have $H \cap K$ a subgroup of G.
(b) Let G be the group of rigid motions of the equilateral triangle as given in Example 16.7. Let $H = \{\pi_0, \pi_1, \pi_2\}$ and $K = \{\pi_0, r_1\}$. Then H, K are subgroups of G. Here $H \cup K = \{\pi_0, \pi_1, \pi_2, r_1\}$ and, since $r_1 \pi_1 = r_2 \notin H \cup K$, it follows that $H \cup K$ is *not* a subgroup of G.

19. (a) $x = 1, x = 4$ $\qquad$ (b) $x = 1, x = 10$

(c) $x = x^{-1} \Rightarrow x^2 \equiv 1 \pmod p \Rightarrow x^2 - 1 \equiv 0 \pmod p \Rightarrow (x-1)(x+1) \equiv 0 \pmod p \Rightarrow x - 1 \equiv 0 \pmod p$ or $x + 1 \equiv 0 \pmod p \Rightarrow x \equiv 1 \pmod p$ or $x \equiv -1 \equiv p - 1$

(mod p).

(d) The result is true for $p = 2$, since $(2-1)! = 1! \equiv -1 \pmod 2$. For $p \geq 3$, consider the elements $1, 2, \ldots, p-1$ in $(\mathbf{Z}_p^*, \cdot)$, The elements $2, 3, \ldots, p-2$ yield $(p-3)/2$ pairs of the form x, x^{-1}. [For example, when $p = 11$ we find that $2, 3, 4, \ldots, 9$ yield the four pairs 2,6; 3,4; 5,9; 7,8.] Consequently, $(p-1)! \equiv (1)(1)^{(p-3)/2}(p-1) \equiv p-1 \equiv -1 \pmod p$.

20. (a) In $(U_8, \cdot)$ we have $3^2 = 1$, so $3 = 3^{-1}$, and $5^2 = 1$, so $5 = 5^{-1}$.
(b) In $(U_{16}, \cdot)$ we have $7^2 = 1$, so $7 = 7^{-1}$, and $9^2 = 1$, so $9 = 9^{-1}$.
(c) Let $x = (2^{k-1} - 1)$ in $(U_{2^k}, \cdot)$. One finds that $x^2 = (2^{k-1} - 1(2^{k-1} - 1) = 2^{2k-2} - 2 \cdot 2^{k-1} + 1 = (2^k)(2^{k-2}) - 2k + 1 = 0(2^{k-2}) - 0 + 1 = 1$, so $x = x^{-1}$. This is also true for $x = (2^{k-1} + 1)$.

Section 16.2

1. (c) If $n = 0$, the result follows from part (a) of Theorem 16.5. So consider $n \in \mathbf{Z}^+$.

For $n = 1$, $f(a^n) = f(a^1) = f(a) = [f(a)]^1 = [f(a)]^n$, so the result follows for $n = 1$. Now assume the result true for $n = k$ (≥ 1) and consider $n = k+1$. Then $f(a^n) = f(a^{k+1}) = f(a^k \cdot a) = f(a^k) \cdot f(a) = [f(a)]^k \cdot f(a) = [f(a)]^{k+1} = [f(a)]^n$. So by the Principle of Mathematical Induction, the result is true for all $n \geq 1$.

For $n \geq 1$, we have $a^{-n} = (a^{-1})^n$ – as defined in the material following Theorem 16.1. So $f(a^{-n}) = f[(a^{-1})^n] = [f(a^{-1})]^n$ by our previous work. Then $[f(a^{-1})]^n = [(f(a))^{-1}]^n = [f(a)]^{-n}$ – by part (b) of Theorem 16.1. Hence $f(a^{-n}) = [f(a)]^{-n}$.

Consequently, $f(a^n) = [f(a)]^n$, for all $a \in G$ and all $n \in \mathbf{Z}$.

2. (a)
$$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$
(b) For all $1 \leq m, n \leq 4$, $A^m \cdot A^n = A^{m+n} = A^r$, where $1 \leq r \leq 4$ and $m+n \equiv r \pmod 4$. Hence the set $\{A, A^2, A^3, A^4\}$ is closed under the binary operation of matrix multiplication. Matrix multiplication is an associative binary operation for all 2×2 real matrices. Consequently, it is associative when restricted to these four matrices.
The matrix $A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity element, and $A^{-1} = A^3$, $(A^2)^{-1} = A^{-2} = A^2$, $(A^3)^{-1} = A^{-3} = A$, and $(A^4)^{-1} = A^{-4} = A^4 = A^0$, so every element has a multiplicative inverse.
Finally, for all $1 \leq m, n \leq 4$, $A^m \cdot A^n = A^{m+n} = A^{n+m} = A^n \cdot A^m$, so $\{A, A^2, A^3, A^4\}$ is an abelian group under ordinary matrix multiplication.
(c) Define $f : \{A, A^2, A^3, A^4\} \longrightarrow G$ by

$$f: \begin{array}{l} A \longrightarrow i \\ A^2 \longrightarrow -1 = i^2 \\ A^3 \longrightarrow -i = i^3 \\ A^4 \longrightarrow 1 = i^4 \end{array} \qquad \text{or} \qquad f: \begin{array}{l} A \longrightarrow -i \\ A^2 \longrightarrow -1 = (-i)^2 \\ A^3 \longrightarrow i = (-i)^3 \\ A^4 \longrightarrow 1 = (-i)^4 \end{array}$$

In either case f is an isomorphism for the two given cyclic groups of order 4.

3. $f(0) = (0,0) \quad f(1) = (1,1) \quad f(2) = (2,0)$
$f(3) = (0,1) \quad f(4) = (1,0) \quad f(5) = (2,1)$

4. Let $x, y \in H$. Since f is onto, there exist $a, b \in G$ with $f(a) = x$, $f(b) = y$. Then $xy = f(a)f(b) = f(ab) = f(ba)$ (since G is abelian) $= f(b)f(a) = yx$, so H is abelian.

5. We need to express the element $(4,6)$ of $\mathbf{Z} \times \mathbf{Z}$ in terms of the elements $(1,3)$ and $(3,7)$, so let us write

$$(4,6) = a(1,3) \oplus b(3,7), \quad \text{where } a, b \in \mathbf{Z}.$$

Then $f(4,6) = f(a(1,3) \oplus b(3,7)) = f(a(1,3)) + f(b(3,7)) = af(1,3) + bf(3,7)$.
With $(4,6) = a(1,3) \oplus b(3,7)$ we have $4 = a + 3b$ and $6 = 3a + 7b$, from which it follows that $a = -5$ and $b = 3$.
Consequently, $f(4,6) = -5g_1 + 3g_2$.

6. (a) For each $k \in \mathbf{Z}$, we find that $(k,0) \in \mathbf{Z} \times \mathbf{Z}$ and $f(k,0) = k - 0 = k$, so the function f is onto $\mathbf{Z}$. Furthermore, if (a,b), $(c,d) \in \mathbf{Z} \times \mathbf{Z}$, then $f((a,b) \oplus (c,d)) = f(a+c, b+d) = (a+c) - (b+d) = (a-b) + (c-d) = f(a,b) + f(c,d)$. Consequently, the function f is a homomorphism onto $\mathbf{Z}$.

(b) If $f(a,b) = 0$, then since $f(a,b) = a - b$, it follows that $a = b$. Also, $a = b \Rightarrow a - b = 0 \Rightarrow f(a,b) = 0$. Hence $f(a,b) = 0$ if and only if $a = b$, or $f^{-1}(0) = \{(a,a) | a \in \mathbf{Z}\}$.

(c) Since $f^{-1}(7) = \{(a,b) | f(a,b) = a - b = 7\}$, here we may also write $f^{-1}(7) = \{(b+7, b) | b \in \mathbf{Z}\} = \{(a, a-7) | a \in \mathbf{Z}\}$.

(d) Let $(a,b) \in \mathbf{Z} \times \mathbf{Z}$. We find that $(a,b) \in f^{-1}(E)$ if and only if $f(a,b) = a - b$ is an even integer.
[We may also write $f^{-1}(E) = \{(2m, 2n) | m, n \in \mathbf{Z}\} \cup \{(2m+1, 2n+1) | m, n \in \mathbf{Z}\}$.]

7. (a) $o(\pi_0) = 1$, $o(\pi_1) = o(\pi_2) = 3$, $o(r_1) = o(r_2) = o(r_3) = 2$.

(b) (See Fig. 16.6) $o(\pi_0) = 1$, $o(\pi_1) = o(\pi_3) = 4$, $o(\pi_2) = o(r_1) = o(r_2) = o(r_3) = o(r_4) = 2$.

8. $n = 2: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ has order 2 and generates the cyclic subgroup

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \right\} \quad \text{of} \quad S_5.$$

$n = 3 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$ has order 3 and generates the cyclic subgroup

$$\left\{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}\right\} \quad \text{of} \quad S_5.$$

$n = 4 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$ has order 4 and generates the cyclic subgroup

$$\left\{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}\right\} \quad \text{of} \quad S_5.$$

$n = 5 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ has order 5 and generates the cyclic subgroup

$$\left\{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}\right\} \quad \text{of} \quad S_5.$$

9. (a) The elements of order 10 are 4, 12, 28, and 36.

(b) The elements of order 10 are a^4, a^{12}, a^{28}, and a^{36}.

10. (a) $U_{14} = \{1, 3, 5, 9, 11, 13\} = \{a \in \mathbf{Z}^+ \mid 1 \leq a \leq 13 \text{ and } \gcd(a, 14) = 1\}$.

(b) Since

$3^1 = 3$ $\quad 3^2 = 9$ $\quad 3^3 = 13$

$3^4 = 11$ $\quad 3^5 = 5$ $\quad 3^6 = 1,$

we know that U_{14} is cyclic and $U_{14} = \langle 3 \rangle$.

We also find that

$5^1 = 5$ $\quad 5^2 = 11$ $\quad 5^3 = 13$

$5^4 = 9$ $\quad 5^5 = 3$ $\quad 5^6 = 1,$

so $U_{14} = \langle 5 \rangle$.

There are no other generators for this group.

11. $\mathbf{Z}_5^* = \langle 2 \rangle = \langle 3 \rangle$; $\quad \mathbf{Z}_7^* = \langle 3 \rangle = \langle 5 \rangle$; $\quad \mathbf{Z}_{11}^* = \langle 2 \rangle = \langle 6 \rangle = \langle 7 \rangle = \langle 8 \rangle$.

12. Let $f: G \to G$, defined by $f(a) = a^{-1}$, be an isomorphism. For all $a, b \in G$, $(ab)^{-1} = f(ab) = f(a)f(b) = a^{-1}b^{-1}$. Also $(ab)^{-1} = a^{-1}b^{-1} \Longrightarrow (ab)^{-1} = (ba)^{-1} \Longrightarrow ab = ba$, so G is abelian. Conversely, the function $f : G \to G$ defined by $f(a) = a^{-1}$ is one-to-one and onto for any group G. For G abelian $f(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a)f(b)$, and f is an isomorphism.

13. Let $(G,+)$, $(H,*)$, $(K,\cdot)$ be the given groups. For any $x,y \in G$, $(g \circ f)(x+y) = g(f(x+y)) = g(f(x) * f(y)) = (g(f(x)) \cdot (g(f(y)) = ((g \circ f)(x)) \cdot ((g \circ f)(y))$, since f, g are homomorphisms. Hence, $g \circ f : G \to K$ is a group homomorphism.

14. (a) From Exercise 16 of Section 16.1 we know that $G = \langle \omega \rangle$. It is also true that $G = \langle \omega^3 \rangle = \langle \omega^5 \rangle = \langle \omega^7 \rangle$.

(b) Define $f : G \to \mathbf{Z}_8$ by $f(\omega^n) = [n]$, $1 \leq n \leq 8$. If $1 \leq k, m \leq 8$, then $\omega^k = \omega^m \iff k = m \iff [k] = [m] \iff f(\omega^k) = f(\omega^m)$, so f is a one-to-one function. Since $|G| = |\mathbf{Z}_8|$, it follows from Theorem 5.11 that f is also onto. Finally, for $1 \leq k, m \leq 8$, $f(\omega^k \cdot \omega^m) = f(\omega^{k+m}) = [k+m] = [k] + [m] = f(\omega^k) + f(\omega^m)$, so f is an isomorphism.
Note: Three other isomorphisms are also possible here. They are determined, in each case, by the image of ω. We find these to be:
$f_1 : G \to \mathbf{Z}_8$, where $f_1(\omega) = [3]$;
$f_2 : G \to \mathbf{Z}_8$, where $f_2(\omega) = [5]$; and
$f_3 : G \to \mathbf{Z}_8$, where $f_3(\omega) = [7]$.

15. (a) $(\mathbf{Z}_{12},+) = \langle 1 \rangle = \langle 7 \rangle = \langle 11 \rangle$
$(\mathbf{Z}_{16},+) = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 9 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 15 \rangle$
$(\mathbf{Z}_{24},+) = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle = \langle 19 \rangle = \langle 23 \rangle$

(b) Let $G = \langle a^k \rangle$. Since $G = \langle a \rangle$, $a = (a^k)^s$ for some $s \in \mathbf{Z}$. Then $a^{1-ks} = e$, so $1 - ks = tn$ since $o(a) = n$. $1 - ks = tn \Longrightarrow 1 = ks + tn \Longrightarrow \gcd(k,n) = 1$. Conversely, let $G = \langle a \rangle$ where $a^k \in G$ and $\gcd(k,n) = 1$. Then $\langle a^k \rangle \subseteq G$. $\gcd(k,n) = 1 \Longrightarrow 1 = ks + tn$, for some $s, t \in \mathbf{Z} \Longrightarrow a = a^1 = a^{ks+nt} = (a^k)^s (a^n)^t = (a^k)^s (e)^t = (a^k)^s \in \langle a^k \rangle$. Hence $G \subseteq \langle a^k \rangle$. So $G = \langle a^k \rangle$, or a^k generates G.

(c) $\phi(n)$.

16. If $k \nmid n$, let $n = qk + r$, $0 < r < k$. Then $f(a^n) = f(e_G) = e_H$ and $f(a^n) = (f(a))^n = (f(a))^{qk+r} = (f(a)^k)^q (f(a)^r) = (f(a))^r$. But $(f(a))^r = e_H$ with $0 < r < k$ contradicts $o(f(a)) = k$. Consequently, $k | n$.

Section 16.3

1. (a) $\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \right\}$

(b)

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} H = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} H = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \right\}$$

$$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}H=\left\{\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}H=\left\{\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}H=\left\{\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}H=H$$

2. Let $K=\langle\beta\rangle=\left\{\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\right\}$

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}K=K$$

$$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}\right\}$$

3. 12

4. $H=\langle[3]\rangle=\langle 3\rangle=\{0,3,6,9,12,15,18,21\}$
$1+H=\{1,4,7,10,13,16,19,22\}$
$2+H=\{2,5,8,11,14,17,20,23\}$.

$K = \langle [4] \rangle = \langle 4 \rangle = \{0, 4, 8, 12, 16, 20\}$
$1 + K = \{1, 5, 9, 13, 17, 21\}$
$2 + K = \{2, 6, 10, 14, 18, 22\}$
$3 + K = \{3, 7, 11, 15, 19, 23\}$

5. From Lagrange's Theorem we know that $|K| = 66 (= 2 \cdot 3 \cdot 11)$ divides $|H|$ and that $|H|$ divides $|G| = 660 (= 2^2 \cdot 3 \cdot 5 \cdot 11)$. Consequently, since $K \neq H$ and $H \neq G$, it follows that $|H|$ is $2(2 \cdot 3 \cdot 11) = 132$ or $5(2 \cdot 3 \cdot 11) = 330$.

6. Let G be the set of units in R. $u \in G \Longrightarrow G \neq \emptyset$. Also, the elements of G are associative under multiplication (inherited from the multiplication in R). If $x, y \in G$ then $x^{-1}, y^{-1} \in R$ (and in G), and $(xy)(y^{-1}x^{-1}) = u = (y^{-1}x^{-1})(xy)$, so $xy \in G$. Consequently, G is a multiplicative group.

7. (a)

$\cdot$	(1)(2)(3)(4)	(12)(34)	(13)(24)	(14)(23)
(1)(2)(3)(4)	(1)(2)(3)(4)	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	(1)(2)(3)(4)	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	(1)(2)(3)(4)	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	(1)(2)(3)(4)

It follows from Theorem 16.3 that H is a subgroup of G. And since the entries in the above table are symmetric about the diagonal from the upper left to the lower right, we have H an abelian subgroup of G.

(b) Since $|G| = 4! = 24$ and $|H| = 4$, there are $24/4 = 6$ left cosets of H in G.

(c) Consider the function $f : H \to \mathbf{Z}_2 \times \mathbf{Z}_2$ defined by

$f : (1)(2)(3)(4) \to (0, 0)$, $\quad f : (12)(34) \to (1, 0)$,
$f : (13)(24) \to (0, 1)$, $\quad f : (14)(23) \to (1, 1)$.

This function f is one-to-one and onto, and for all $x, y \in H$ we find that

$$f(x \cdot y) = f(x) \oplus f(y).$$

Consequently, f is an isomorphism.
[Note: There are other possible answers that can be given here. In fact, there are six possible isomorphisms that one can define here.]

8. Let $o(a) = k$. Then $|\langle a \rangle| = k$, so by Lagrange's Theorem k divides n. Hence $a^n = a^{km} = (a^k)^m = e^m = e$.

9. (a) If H is a proper subgroup of G, then by Lagrange's Theorem $|H|$ is 2 or p. If $|H| = 2$, then $H = \{e, x\}$ where $x^2 = e$, so $H = \langle x \rangle$. If $|H| = p$, let $y \in H$, where $y \neq e$. Then $o(y) = p$, so $H = \langle y \rangle$.

(b) Let $x \in G$, $x \neq e$. Then $o(x) = p$ or $o(x) = p^2$. If $o(x) = p$, then $|\langle x \rangle| = p$. If $o(x) = p^2$, then $G = \langle x \rangle$ and $\langle x^p \rangle$ is a subgroup of G of order p.

10. Corollary 16.1. $o(a) = |\langle a \rangle|$. By Lagrange's Theorem $|\langle a \rangle|$ divides $|G|$, so $o(a) | |G|$.

Corollary 16.2. Let G be a group with $|G| = p$, a prime. Let $x \in G$, $x \neq e$. By Corollary 16.1, $o(x) = p$, so $G = \langle x \rangle$ and G is cyclic.

11. (a) Let $x \in H \cap K$. $x \in H \Longrightarrow o(x) | 10 \Longrightarrow o(x) = 1, 2, 5,$ or 10. $x \in K \Longrightarrow o(x) | 21 \Longrightarrow o(x) = 1, 3, 7,$ or 21. Hence $o(x) = 1$ and $x = e$.

12. (a) For all $a \in G$, $a^{-1}a = e \in H$, so $a \mathcal{R} a$ and $\mathcal{R}$ is reflexive. If $a, b \in G$ and $a \mathcal{R} b$, then $a \mathcal{R} b \Longrightarrow a^{-1}b \in H \Longrightarrow (a^{-1}b)^{-1} \in H$ (because H is a subgroup) $\Longrightarrow b^{-1}a \in H \Longrightarrow b \mathcal{R} a$, so $\mathcal{R}$ is symmetric. Finally, let a, b, $c \in G$ with $a \mathcal{R} b$ and $b \mathcal{R} c$. Then we have $a^{-1}b, b^{-1}c \in H$ and since H is closed under the group operation, $(a^{-1}b)(b^{-1}c) = a^{-1}(bb^{-1})c = a^{-1}(e)c = a^{-1}c \in H$, so $a \mathcal{R} c$ and $\mathcal{R}$ is transitive. Hence $\mathcal{R}$ is an equivalence relation.

(b) $a \mathcal{R} b \Longrightarrow a^{-1}b \in H \Longrightarrow a^{-1}b = h$, where $h \in H \Longrightarrow bH = (ah)H = a(hH) = aH$. Conversely, $aH = bH \Longrightarrow a \in bH \Longrightarrow a = bh$ for some $h \in H \Longrightarrow h^{-1} = a^{-1}b$, where $h^{-1} \in H \Longrightarrow a^{-1}b \in H$ and $a \mathcal{R} b$.

(c) Let $x \in [a]$. Then $x \mathcal{R} a$ so $x^{-1}a \in H$. Since H is a subgroup, $(x^{-1}a)^{-1} = a^{-1}x \in H$. So $a^{-1}x = h \in H$ and $x = ah \in aH$. Hence $[a] \subseteq aH$. Conversely, if $y \in aH$ then $y = ah_1$, for some $h_1 \in H$. $y = ah_1 \Longrightarrow a^{-1}y = h_1 \in H \Longrightarrow a \mathcal{R} y$. With $\mathcal{R}$ symmetric we also have $y \mathcal{R} a$, and so $y \in [a]$. So here we find $aH \subseteq [a]$. With both inclusions established it now follows that $aH = [a]$.

(d) Define $f : aH \to H$ by $f(ah) = h$, for $h \in H$. $ah_1 = ah_2 \Longleftrightarrow h_1 = h_2 \Longleftrightarrow f(ah_1) = f(ah_2)$, so f is a one-to-one function. Also, for $h \in H$, $f^{-1}(h) \supseteq \{ah\}$, so $f^{-1}(h) \neq \emptyset$, and f is onto. Hence f is bijective and $|aH| = |H|$.

(e) Since $\mathcal{R}$ is an equivalence relation on G, $\mathcal{R}$ induces a partition of G as

$$G = [a_1] \cup [a_2] \cup \ldots \cup [a_t].$$

Hence $[a_i] = a_i H$ for all $1 \leq i \leq t$, and $|a_i H| = |H| = m$ for all $1 \leq i \leq t$. Consequently, $|G| = t|H|$, and $|H|$ divides $|G|$.

13. (a) In $(\mathbf{Z}_p^*, \cdot)$ there are $p - 1$ elements, so by Exercise 8, for each $[x] \in (\mathbf{Z}_p^*, \cdot)$, $[x]^{p-1} = [1]$, or $x^{p-1} \equiv 1 \pmod{p}$, or $x^p \equiv x \pmod{p}$. For all $a \in \mathbf{Z}$, if $p \mid a$ then $a \equiv 0 \pmod{p}$ and $a^p \equiv 0 \equiv a \pmod{p}$. If $p \nmid a$, then $a \equiv b \pmod{p}$, $1 \leq b \leq p-1$ and $a^p \equiv b^p \equiv b \equiv a \pmod{p}$.

(b) In the group G of units of $\mathbf{Z}_n$ there are $\phi(n)$ units. If $a \in \mathbf{Z}$ and $\gcd(a, n) = 1$ then $[a] \in G$ and $[a]^{\phi(n)} = [1]$ or $a^{\phi(n)} \equiv 1 \pmod{n}$

(c) and (d) These results follow from Exercises 6 and 8. They are special cases of Exercise 8.

Section 16.4

1. Here $n = 2573$ and $e = 7$.
The assignment for the given plaintext is:

IN	VE	ST	IN	ST	OC	KS
0813	2104	1819	0813	1819	1402	1018

Since

$(0813)^7 \bmod 2573 = 0462$ $\quad$ $(1819)^7 \bmod 2573 = 1809$
$(2104)^7 \bmod 2573 = 0170$ $\quad$ $(1402)^7 \bmod 2573 = 1981$
$(1819)^7 \bmod 2573 = 1809$ $\quad$ $(1018)^7 \bmod 2573 = 0305,$
$(0813)^7 \bmod 2573 = 0462$

the ciphertext is
0462 0170 1809 0462 1809 1981 0305

2. Here $n = 1459$ and $e = 5$.
The assignment for the given plaintext is:

OR	DE	RA	PI	ZZ	AX
1417	0304	1700	1508	2525	0023

Since

$(1417)^5 \bmod 1459 = 0152$ $\quad$ $(1508)^5 \bmod 1459 = 1177$
$(0304)^5 \bmod 1459 = 0466$ $\quad$ $(2525)^5 \bmod 1459 = 0055$
$(1700)^5 \bmod 1459 = 1318$ $\quad$ $(0023)^5 \bmod 1459 = 0694$

the ciphertext is
0152 0466 1318 1177 0055 0694.

3. Here $n = 2501 = (41)(61)$, so $r = \phi(n) = (40)(60) = 2400$. Further, $e = 11$ is a unit in $\mathbf{Z}_{2400}$ and $d = e^{-1} = 1091$.

Since the encrypted ciphertext is
1418 1436 2370 1102 1805 0250,
we calculate the following:

$(1418)^{1091} \bmod 2501 = 0317$ $\quad$ $(1102)^{1091} \bmod 2501 = 0005$
$(1436)^{1091} \bmod 2501 = 0821$ $\quad$ $(1805)^{1091} \bmod 2501 = 0411$
$(2370)^{1091} \bmod 2501 = 0418$ $\quad$ $(0250)^{1091} \bmod 2501 = 2423$

Consequently, the assignment for the original message is
0317 0821 0418 0005 0411 2423
and this reveals the message as

DRIVE SAFELYX.

4. Here $n = 3053 = (43)(71)$, so $r = \phi(n) = (42)(70) = 2940$. Further, $e = 17$ is a unit in $\mathbf{Z}_{2940}$ and $d = e^{-1} = 173$.

Since the encrypted ciphertext is

0986 3029 1134 1105 1232 2281 2967 0272 1818 2398 1153,
we calculate the following:

$(0986)^{173} \bmod 3053 = 1907$
$(3029)^{173} \bmod 3053 = 0417$
$(1134)^{173} \bmod 3053 = 0408$
$(1105)^{173} \bmod 3053 = 1818$
$(1232)^{173} \bmod 3053 = 0005$
$(2281)^{173} \bmod 3053 = 0419$
$(2967)^{173} \bmod 3053 = 2408$
$(0272)^{173} \bmod 3053 = 1313$
$(1818)^{173} \bmod 3053 = 2012$
$(2398)^{173} \bmod 3053 = 0104$
$(1153)^{173} \bmod 3053 = 1718$

Consequently, the assignment for the original message is
1907 0417 0408 1818 0005 0419 2408 1313 2012 0104 1718
and this reveals the message as

THERE IS SAFETY IN NUMBERS.

5. Here $n = pq = 121,361$ and $r = \phi(n) = 120,432$.

Since $p + q = n - r + 1 = 930$ and $p - q = \sqrt{(n-r+1)^2 - 4n} = \sqrt{864,900 - 485,444} = \sqrt{379,456} = 616$, it follows that

$$p = 157 \text{ and } q = 773.$$

6. Here $n = pq = 5,446,367$ and $r = \phi(n) = 5,441,640$.

Since $p+q = n-r+1 = 4728$ and $p-q = \sqrt{(n-r+1)^2 - 4n} = \sqrt{22,353,984 - 21,785,468} = \sqrt{568516} = 754$, it follows that

$$p = 1987 \text{ and } q = 2741.$$

Section 16.5

1. (a) $e = 0001001$ (b) $r = 1111011$ (c) $c = 0101000$

2. (a) $(0.95)^8(0.05)$ (b) $(0.95)^7(0.05)^2$

(c) $\binom{9}{1}(0.95)^8(0.05)$ (d) $\binom{9}{2}(0.95)^7(0.05)^2$

(e) $\binom{9}{3}(0.95)^6(0.05)^3$ (f) $\binom{7}{3}(0.95)^6(0.05)^3$

3. (a) (i) $D(111101100) = 101$ (ii) $D(000100011) = 000$
(iii) $D(010011111) = 011$

(b) 000000000, 000000001, 100000000

(c) 64

4. (a) $(0.95)^5 + \binom{5}{1}(0.05)(0.95)^4 + \binom{5}{2}(0.05)^2(0.95)^3$

(b) $[(0.95)^5 + \binom{5}{1}(0.05)(0.95)^4 + \binom{5}{2}(0.05)^2(0.95)^3]^3$

(c) $D(r) = 01$ (d) 0000000000, 1000000000, 0000000001

(e) 256

Sections 16.6 and 16.7

1. $S(101010, 1) = \{101010, 001010, 111010, 100010, 101110, 101000, 101011\}$

   $S(111111, 1) = \{111111, 011111, 101111, 110111, 111011, 111101, 111110\}$

2. $S(000000, 1) = \{000000, 100000, 010000, 001000, 000100, 000010, 000001\}$

   $S(010101, 1) = \{010101, 110101, 000101, 011101, 010001, 010111, 010100\}$

   (a) $D(110101) = 01$ (b) $D(101011) = 10$

   (c) $D(001111) = 00$ (d) $D(110000) = 00$

3. (a) $|S(x, 1)| = 11$; $|S(x, 2)| = 56$; $|S(x, 3)| = 176$

   (b) $|S(x, k)| = 1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{k} = \sum_{i=0}^{k} \binom{n}{i}$

4. $k = 8$; $n = 4$

5. (a) The minimum distance between code words is 3. The code can detect all errors of weight ≤ 2 or correct all single errors.
   (b) The minimum distance between code words is 5. The code can detect all errors of weight ≤ 4 or correct all errors of weight ≤ 2.
   (c) The minimum distance between code words is 2. The code detects all single errors but has no correction capability.
   (d) The minimum distance between code words is 3. The code can detect all errors of weight ≤ 2 or correct all single errors.

6. (a) (i) $H \cdot (111101)^{tr} = (101)^{tr}$, so $c = 110101$ and $D(c) = 110$
   (ii) $H \cdot (110101)^{tr} = (000)^{tr}$, so $c = 110101$ and $D(c) = 110$
   (iii) $H \cdot (001111)^{tr} = (010)^{tr}$, so $c = 001101$ and $D(c) = 001$
   (iv) $H \cdot (100100)^{tr} = (010)^{tr}$, so $c = 100110$ and $D(c) = 100$
   (v) $H \cdot (110001)^{tr} = (100)^{tr}$, so $c = 110101$ and $D(c) = 110$
   (vi) $H \cdot (111111)^{tr} = (111)^{tr}$, which doesn't appear among the columns of H.

   Assuming a double error,
   (1) if $111 = 110 + 001$, then $c = 011110$ and $D(c) = 011$;
   (2) if $111 = 011 + 100$, then $c = 101011$ and $D(c) = 101$; and
   (3) if $111 = 101 + 010$, then $c = 110101$ and $D(c) = 110$.

   (vii) $H \cdot (111100)^{tr} = (100)^{tr}$, so $c = 111000$ and $D(c) = 111$
   (viii) $H \cdot (010100)^{tr} = (111)^{tr}$, which doesn't appear among the columns of H.

Assuming a double error,
(1) if $111 = 110 + 001$, then $c = 110101$ and $D(c) = 110$;
(2) if $111 = 011 + 100$, then $c = 000000$ and $D(c) = 000$; and
(3) if $111 = 101 + 010$, then $c = 011110$ and $D(c) = 011$.

(b) No. The results in (vi) and (viii) are not unique.

7. (a) $C = \{00000, 10110, 01011, 11101\}$. The minimum distance between code words is 3, so the code can detect all errors of weight ≤ 2 or correct all single errors.

(b) $$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

(c) (i) 01 (ii) 11 (v) 11 (vi) 10
For (iii) and (iv) the syndrome is $(111)^{tr}$ which is not a column of H. Assuming a double error, if $(111)^{tr} = (110)^{tr} + (001)^{tr}$, then the decoded received word is 01 (for (iii)) and 10 (for (iv)). If $(111)^{tr} = (011)^{tr} + (100)^{tr}$, we get 10 (for (iii)) and 01 (for (iv)).

8. (a) $$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$C = \{000000, 100111, 010010, 001101, 110101, 101010, 011111, 111000\}$
(b) No. The second and fifth columns of H are the same.

9. $G = [I_8|A]$ where I_8 is the 8×8 multiplicative identity matrix and A is a column of eight 1's. $H = [A^{tr}|1] = [11111111|1]$.

10. (a) For each $x \in \{0, 1\}$, $xG = xxxxxxxx$.
(b) $H = [A|I_8]$ where I_8 is the 8×8 multiplicative identity and A is a column of eight 1's.

11. Compare the generator (parity-check) matrix in Exercise 9 with the parity-check (generator) matrix in Exercise 10.

12. Let $c \in \mathbf{Z}_2^n$ be a code word. For all $x \in S(c, k)$ the decoding function of Theorem 16.13 decodes x, and if c_1, c_2 are code words $S(c_1, k) \cap S(c_2, k) = \emptyset$. $x \in S(c, k) \iff d(x, c) \leq k$, so $|S(c, k)| = \sum_{i=0}^{k} \binom{n}{i}$. Consequently, $|M(n, k)|[\sum_{i=0}^{k} \binom{n}{i}]$ accounts for all received words in $\mathbf{Z}_n^2$ that are code words or differ from a code word in k or fewer positions. It follows then that $|M(n, k)|[\sum_{i=0}^{k} \binom{n}{i}] \leq |\mathbf{Z}_2^n| = 2^n$.

For the lower (Gilbert) bound we appeal to error detection. If $r \in \mathbf{Z}_2^n$ and $d(c, r) \leq 2k$, then by Theorem 16.12 we are able to detect r as an incorrect transmission. So for all code words c, $S(c, 2k)$ accounts for the code word c as well as those received words r where $d(c, r) \leq 2k$, but here we may have $S(c_1, 2k) \cap S(c_2, 2k) \neq \emptyset$ for distinct code words

c_1, c_2. If $2^n > |M(n,k)|[\sum_{i=0}^{2k} \binom{n}{i}]$, then there is an element $c^* \in \mathbf{Z}_2^n$ where $d(c^*, c) > 2k$ for all code words c. So we can add c^* to the present set of code words and get a larger code where the minimal distance between code words is still $2k+1$. This, however, contradicts the maximal size $|M(n,k)|$ so $2^n \leq |M(n,k)|[\sum_{i=0}^{2k} \binom{n}{i}]$.

Sections 16.8 and 16.9

1. $\binom{256}{2}$ calculations are needed to find the minimum distance between code words. (A calculation here determines the distance between a pair of code words.) If E is a group homomorphism we need to calculate the weights of the 255 nonzero code words.

2. (a)

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Received word r	$H \cdot r^{tr}$	$c = r + e$	$D(c)$
000011	$(011)^{tr}$	010011	010
100011	$(101)^{tr}$	101011	101
111110	$(110)^{tr}$	011110	011
100001	$(111)^{tr}$	110101	110
001100	$(001)^{tr}$	001101	001
011110	$(000)^{tr}$	011110	011
001111	$(010)^{tr}$	001101	001
111100	$(100)^{tr}$	111000	111

(b) If 100001 is used (in the last row of Table 16.8) as the coset leader instead of 010100, then for $r = 100001$, $H \cdot r^{tr} = (111)^{tr}$. However, if $r = 100001$ and $x = 100001$, then $c = 000000$ (not 110101) and $D(c) = 000$ (not 110).

3. (a)

Syndrome	Coset Leader			
000	00000	10110	01011	11101
110	10000	00110	11011	01101
011	01000	11110	00011	10101
100	00100	10010	01111	11001
010	00010	10100	01001	11111
001	00001	10111	01010	11100
101	11000	01110	10011	00101
111	01100	11010	00111	10001

[The last two rows are not unique.]

(b)

Received Word	Code Word	Decoded Message
11110	10110	10
11101	11101	11
11011	01011	01
10100	10110	10
10011	01011	01
10101	11101	11
11111	11101	11
01100	00000	00

4.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

(a)

$(1000)\,G = 1000110$ $\qquad$ $(1100)\,G = 1100011$

$(1011)\,G = 1011010$ $\qquad$ $(1110)\,G = 1110000$

$(1001)\,G = 1001001$ $\qquad$ $(1111)\,G = 1111111$

(b)

Received word r	$H \cdot r^{tr}$	c	$D(c)$
1100001	$(010)^{tr}$	1100011	1100
1110111	$(111)^{tr}$	1111111	1111
0010001	$(010)^{tr}$	0010011	0010
0011100	$(000)^{tr}$	0011100	0011

(c)

Syndrome	Coset Leader
000	0000000
110	1000000
101	0100000
011	0010000
111	0001000
100	0000100
010	0000010
001	0000001

(d) Same results as in part (b).

5. (a) G is 57×63; H is 6×63
(b) The rate is $57/63$.

6. The rate of the (3,1) triple repetition code is $1/3$. The rate for the Hamming (7,4) code is $4/7$. Since $(4/7) > (1/3)$ the Hamming code is more efficient.

7. (a) The Hamming (7,4) code corrects all single errors in transmission, so the probability of the correct decoding of 1011 is $(0.99)^7 + \binom{7}{1}(0.99)^6(0.01)$

(b) $[(0.99)^7 + \binom{7}{1}(0.99)^6(0.01)]^5$

Section 16.10

1. (a) $\pi_3^* = \begin{pmatrix} C_1C_2C_3C_4C_5C_6C_7C_8C_9C_{10}C_{11}C_{12}C_{13}C_{14}C_{15}C_{16} \\ C_1C_5C_2C_3C_4C_9C_6C_7C_8C_{11}C_{10}C_{15}C_{12}C_{13}C_{14}C_{16} \end{pmatrix}$

$r_2^* = \begin{pmatrix} C_1C_2C_3C_4C_5C_6C_7C_8C_9C_{10}C_{11}C_{12}C_{13}C_{14}C_{15}C_{16} \\ C_1C_5C_4C_3C_2C_6C_9C_8C_7C_{11}C_{10}C_{13}C_{12}C_{15}C_{14}C_{16} \end{pmatrix}$

(b) $r_3^{-1} = r_3$

$r_3^* = (r_3^{-1})^* = \begin{pmatrix} C_1C_2C_3C_4C_5C_6C_7C_8C_9C_{10}C_{11}C_{12}C_{13}C_{14}C_{15}C_{16} \\ C_1C_2C_5C_4C_3C_7C_8C_9C_8C_{10}C_{11}C_{14}C_{13}C_{12}C_{15}C_{16} \end{pmatrix}$

$= (r_3^*)^{-1}$

(c) $\pi_1^* r_1^* = \begin{pmatrix} C_1C_2C_3C_4C_5C_6C_7C_8C_9C_{10}C_{11}C_{12}C_{13}C_{14}C_{15}C_{16} \\ C_1C_2C_5C_4C_3C_7C_8C_2C_8C_{10}C_{11}C_{14}C_{13}C_{12}C_{15}C_{16} \end{pmatrix}$

$= r_3^* = (\pi_1 r_1)^*$.

2. $\alpha = (1247365)$ $\beta = (135)(2674)$
$\gamma = (123)(476)(5)$ $\delta = (14)(2)(375)(6)$

3. (a) $o(\alpha) = 7$; $o(\beta) = 12$; $o(\gamma) = 3$; $o(\delta) = 6$.

(b) Let $\alpha \in S_n$, with $\alpha = c_1c_2 \ldots c_k$, a product of disjoint cycles. Then $o(\alpha)$ is the lcm

of $\ell(c_1), \ell(c_2), \ldots, \ell(c_k)$, where $\ell(c_i) =$ length of c_i, $1 \leq i \leq k$.

4. Here G is the group of Example 16.7.

(a)

$\Psi(\pi_0^*) = 2^3 \quad \Psi(\pi_1^*) = 2 \quad \Psi(\pi_2^*) = 2$
$\Psi(r_1^*) = 2^2 \quad \Psi(r_2^*) = 2^2 \quad \Psi(r_3^*) = 2^2$

The number of distinct colorings is $(1/6)[2^3 + 2 + 2 + 3(2^2)] = 4$.

(b)

$\Psi(\pi_0^*) = 3^3 \quad \Psi(\pi_1^*) = 3 \quad \Psi(\pi_2^*) = 3$
$\Psi(r_1^*) = 3^2 \quad \Psi(r_2^*) = 3^2 \quad \Psi(r_3^*) = 3^2$

The number of distinct colorings is $(1/6)[3^3 + 3 + 3 + 3(3^2)] = 10$.

5. For $0 \leq i \leq 4$, let π_i denote a clockwise rotation through $i(72°)$. Also, there are five reflections r_i, $1 \leq i \leq 5$, each about a line through a vertex and the midpoint of the opposite side. Here $|G| = 10$.

(a) $\Psi(\pi_0^*) = 2^5 \quad \Psi(\pi_i^*) = 2, \quad 2 \leq i \leq 4$
$\Psi(r_i^*) = 2^3, \quad 1 \leq i \leq 5.$

The number of distinct configurations is $(1/10)[2^5 + 4(2) + 5(2^3)] = 8$.

(b) 39

6. (a) (i) Free to move in two dimensions: Here $G = \{\pi_0, \pi_1, \pi_2, \pi_3\}$ where the π_i, $0 \leq i \leq 3$, are as in Example 16.28.
$\Psi(\pi_0^*) = 3^4$, $\Psi(\pi_1^*) = \Psi(\pi_3^*) = 3$, $\Psi(\pi_2^*) = 3^2$.
The number of distinct configurations is $(1/4)[3^4 + 2(3) + 3^2] = 24$.

(ii) Free to move in three dimensions: Here G is the group of Example 16.28.
$\Psi(\pi_0^*) = 3^4$, $\Psi(\pi_1^*) = \Psi(\pi_3^*) = 3$, $\Psi(\pi_2^*) = 3^2$.
$\Psi(r_1^*) = 3^3 = \Psi(r_2^*), \Psi(r_3^*) = 3^2 = \Psi(r_4^*)$.

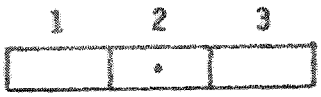
The number of distinct configurations is $(1/8)[3^4 + 2(3) + 3^2 + 2(3^3) + 2(3^2)] = 21$.

(b) (i) Two dimensions: 51 (ii) Three dimensions: 39

7. (a) $G = \{\pi_i | 0 \leq i \leq 3\}$, where π_i is a clockwise rotation through $i \cdot 90°$. The number of distinct bracelets is $(1/4)[4^4 + 4 + 4^2 + 4] = 70$.

(b) $G = \{\pi_i | 0 \leq i \leq 3\} \cup \{r_i | 1 \leq i \leq 4\}$, where each r_i, $1 \leq i \leq 4$, is one of the two reflections about a line through two opposite beads of the midpoints of two opposite lengths of wire. Then the number of distinct bracelets is $(1/8)[4^4+4+4^2+4+4^3+4^3+4^2+4^2] = 55$.

8. (a)



$G = \{\pi_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\}$

$(1/2)[3^3 + 3^2] = 18$; $(1/2)[4^3 + 4^2] = 40$

(b) $G = \{\pi_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\}$

$(1/2)[3^4 + 3^2] = 45$; $(1/2)[4^4 + 4^2] = 136$

(c) n odd: $(1/2)[3^n + 3^{(n+1)/2}]$; $(1/2)[4^n + 4^{(n+1)/2}]$
n even: $(1/2)[3^n + 3^{n/2}]$; $(1/2)[4^n + 4^{n/2}]$

(d) (a) $(1/2)[3 \cdot 2 \cdot 2 + 3 \cdot 2] = 9$; $(1/2)[4 \cdot 3 \cdot 3 + 4 \cdot 3] = 24$
(b) $(1/2)[3 \cdot 2 \cdot 2 \cdot 2 + 0] = 12$; $(1/2)[4 \cdot 3 \cdot 3 \cdot 3 + 0] = 54$.

9. Triangular Figure:
(a) $G = \{\pi_0, \pi_1, \pi_2\}$ $(1/3)[2^4 + 2^2 + 2^2] = 8$
(b) $G = \{\pi_0, \pi_1, \pi_2, r_1, r_2, r_3\}$ $(1/6)[2^4 + 2^2 + 2^2 + 3(2^3)] = 8$

Square Figure:
(a) $G = \{\pi_0, \pi_1, \pi_2\pi_3\}$ $(1/4)[2^5 + 2(2^2) + 2^3] = 12$
(b) $G = \{\pi_0, \pi_1, \pi_2, \pi_3, r_1, r_2, r_3, r_4\}$ $(1/8)[2^5 + 2(2^2) + 2^3 + 2(2^3) + 2(2^4)] = 12$

10. $G = \{\pi_0, \pi_1, \pi_2, \pi_3\}$ $(1/4)[4^5 + 2(4^2) + 4^3] = 280$
$(1/4)[4(3^4) + 2(4)(3) + 4(3^2)] = 96$

11. (a) 140 (b) 102

12. (a) $G = \{\pi_0, \pi_1, \pi_2, \pi_3\}$ $(1/4)[2^{16} + 2(2^4) + 2^8] = 16456$
(b) $G = \{\pi_0, \pi_1, \pi_2, \pi_3, r_1, r_2, r_3, r_4\}$
$(1/8)[2^{16} + 2(2^4) + 2^8 + 2(2^8) + 2(2^{10})] = 8548$

13. $G = \{\pi_i | 0 \le i \le 6\}$, where π_i is the (clockwise) rotation through $i \cdot (360°/7)$.
$(1/7)[3^7 + 6(3)] = 315$

14. (a) If e is the identity of G, then $e^*(x) = x$, so $H = \{\pi \in G | \pi^*(x) = x\} \neq \emptyset$. If $\pi_1, \pi_2 \in G$ and $\pi_1^*(x) = x = \pi_2^*(x)$, then $\pi_1^*\pi_2^*(x) = x = (\pi_1\pi_2)^*(x)$, so $\pi_1\pi_2 \in H$. Also, if $\pi_1^*(x) = x$, then $(\pi_1^*)^{-1}(x) = x = (\pi_1^{-1})^*(x)$, so $\pi_1 \in H \Longrightarrow \pi_1^{-1} \in H$ and, consequently, H is a subgroup of G.

(b) C_1 : The subgroup is $\{\pi_0, r_1\}$
C_{15} : The subgroup is $\{\pi_0, r_3\}$

Section 16.11

1. (a) $(1/4)[5^4 + 5^2 + 2(5)] = 165$
(b) $(1/8)[5^4 + 5^2 + 2(5) + 2(5^2) + 2(5^3)] = 120$

2. (a) $(1/5)[5^5 + 4(5)] = 629$
(b) $(1/10)[5^5 + 4(5) + 5(5^3)] = 377$

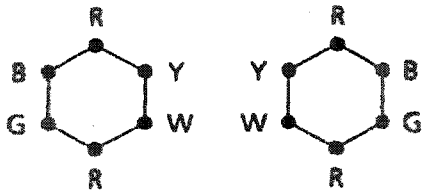
3. (Triangular Figure):
(a) $G = \{\pi_0, \pi_1, \pi_2\}$ $(1/3)[4^4 + 2(4^2)] = 96$
(b) $G = \{\pi_0, \pi_1, \pi_2, r_1, r_2, r_3\}$ $(1/6)[4^4 + 2(4^2) + 3(4^3)] = 80$

(Square Figure):
(a) $G = \{\pi_0, \pi_1, \pi_2, \pi_3\}$, $(1/4)[4^5 + 2(4^2) + 4^3] = 280$
(b) $G = \{\pi_0, \pi_1, \pi_2, \pi_3, r_1, r_2, r_3, r_4\}$ $(1/8)[4^5 + 2(4^2) + 4^3 + 2(4^3) + 2(4^4)] = 220$

(Hexagonal Figure):
(a) $G = \{\pi_0, \pi_1\}$ where π_i is the rotation through $i \cdot 180°$, $i = 0, 1$.
$(1/2)[4^9 + 4^5] = 131,584$
(b) $G = \{\pi_0, \pi_1, r_1, r_2\}$ where $r_1(r_2)$ is the vertical (horizontal) reflection.
$(1/4)[4^9 + 4^5 + 4^5 + 4^7] = 70,144$

4. (a) $(1/12)[3^6 + 2(3) + 2(3^2) + 4(3^3) + 3(3^4)] = 92$
(b) $(1/12)[m^6 + 2m + 2m^2 + 4m^3 + 3m^4]$ is the number of ways to m-color the vertices of a regular hexagon that is free to move in space.

5. (a) $(1/6)[5^6 + 2(5) + 2(5^2) + 5^3] = 2635$
(b) $(1/12)[5^6 + 2(5) + 2(5^2) + 4(5^3) + 3(5^4)] = 1505$
(c)



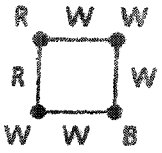
6. (Triangular Figure):
(a) $G = \{\pi_0, \pi_1, \pi_2\}$ $(1/3)[3^6 + 2(3^2)] = 249$
(b) $G = \{\pi_0, \pi_1, \pi_2, r_1, r_2, r_3\}$ $(1/6)[3^6 + 2(4^2) + 3(3^4)] = 165$

(Square Figure):
(a) $G = \{\pi_0, \pi_1, \pi_2, \pi_3\}$ $(1/4)[3^8 + 2(3^2) + 3^4] = 1665$
(b) $G = \{\pi_0, \pi_1, \pi_2, \pi_3, r_1, r_2, r_3, r_4\}$ $(1/8)[3^8 + 2(3^2) + (3^4) + 4(3^5)] = 954$

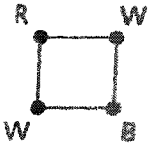
(Hexagonal Figure):
(a) $G = \{\pi_0, \pi_1\}$ $(1/2)[3^{14} + 3^7] = 2,392,578$
(b) $G = \{\pi_0, \pi_1, r_1, r_2\}$ $(1/4)[3^{14} + 3^7 + 3^9 + 3^8] = 1,202,850$

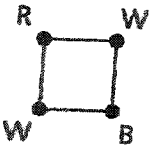
7. (a) $(1/8)[3^4 + 2(3) + 3^2 + 2(3^3) + 2(3^2)] = 21$
(b) $(1/8)[3^8 + 2(3^2) + 3^4 + 2(3^5) + 2(3^5)] = 954$

(c) No, $k = 21$, $m = 21$, so $km = 441 \neq 954 = n$. Here the location of a certain edge must be considered relative to the location of the vertices.

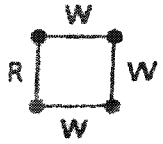
For example, 

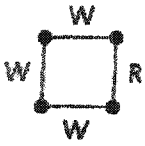
is not equivalent to 

even though 

is equivalent to 

and



is equivalent to 

.

Section 16.12

1. (a) (i) $(1/4)[(r+w)^4 + 2(r^4+w^4) + (r^2+w^2)^2] = r^4 + w^4 + r^3w + 2r^2w^2 + rw^3$
(ii) $(1/8)[(r+w)^4 + 2(r^4+w^4) + 3(r^2+w^2)^2 + 2(r+w)^2(r^2+w^2)] = r^4 + w^4 + r^3w + 2r^2w^2 + rw^3$

(b) (i) $(1/4)[(r+b+w)^4 + 2(r^4+b^4+w^4) + (r^2+b^2+w^2)^2]$
(ii) $(1/8)[(r+b+w)^4 + 2(r^4+b^4+w^4) + 3(r^2+b^2+w^2)^2 + 2(r+b+w)^2(r^2+b^2+w^2)]$

2. The cycle structure representations for the group elements are as follows:
(1) x_1^5 for the identity
(2) x_5 for the four (non-identity) rotations
(3) $x_1x_2^2$ for the five reflections.

The pattern inventory is $(1/10)[(r+b+w)^5 + 4(r^5+b^5+w^5) + 5(r+b+w)(r^2+b^2+w^2)^2]$.
For three red vertices we consider the coefficients of the summands that include r^3:
$(r+b+w)^5$: $\binom{5}{3,1,1} + \binom{5}{3,2,0} + \binom{5}{3,0,2} = 40$
$(r+b+w)(r^2+b^2+w^2)^2$: $\binom{2}{1,1,0} + \binom{2}{1,0,1} = 4$
The answer is $(1/10)[40 + 5(4)] = 6$.

For the two red, one white, and two blue vertices we consider
$(r+b+w)^5$: $\binom{5}{2,1,2} = 30$
$(r+b+w)(r^2+b^2+w^2)^2$: 2

The answer is $(1/10)[30 + 5(2)] = 4$

3. (a) (See Example 16.35)

	Rigid Motion	Cycle Structure Representation
(1)	Identity	x_1^6
(2)	Rotation through 90°	$x_1^2x_4$
	Rotation through 180°	$x_1^2x_2^2$
	Rotation through 270°	$x_1^2x_4$
(3)	Rotations of 180°	x_2^3
(4)	Rotations of 120°	x_3^2

There are then $(1/24)[2^6 + 6(2^3) + 3(2^4) + 6(2^3) + 8(2^2)] = 10$ distinct 2-colorings of the faces of the cube.

(b) $(1/24)[(r+w)^6 + 6(r+w)^2(r^4+w^4) + 3(r+w)^2(r^2+w^2)^2 + 6(r^2+w^2)^3 + 8(r^3+w^3)^2]$

(c) For three red and three white faces we consider the coefficients of the summands that involve r^3w^3 :

$(r+w)^6$:	$\binom{6}{3} = 20$
$3(r+w)^2(r^2+w^2)^2$:	12
$8(r^3+w^3)^2$:	16

The answer is $(1/24)[20 + 12 + 16] = 2$

4. $(36) - (1/12)[3^4 + 8(3^2) + 3(3^2)] = 36 - (1/12)[180] = 21$ compounds have at least one bromine atom.

For the compounds with exactly three hydrogen atoms we need the coefficients of w^3x and w^3y in the pattern inventory.

$(w+x+y+z)^4$: $\binom{4}{3,1,0,0} + \binom{4}{3,0,1,0} = 8$

$8(w+x+y+z)(w^3+x^3+y^3+z^3)$: $8(1+1) = 16$

The answer is $(1/12)[8 + 16] = 2$

5. Let g denote green and y gold.

(Triangular Figure): $(1/6)[(g+y)^4 + 2(g+y)(g^3+y^3) + 3(g+y)^2(g^2+y^2)]$

(Square Figure): $(1/8)[(g+y)^5 + 2(g+y)(g^4+y^4) + (g+y)(g^2+y^2)^2 + 2(g+y)(g^2+y^2)^2 + 2(g+y)^3(g^2+y^2)]$

(Hexagonal Figure): $(1/4)[(g+y)^9 + (g+y)(g^2+y^2)^4 + (g+y)(g^2+y^2)^4 + (g+y)^5(g^2+y^2)^2]$.

6. Here $G = \{\pi_i | 0 \le i \le 6\}$ where π_i is a clockwise rotation through $i \cdot (360°/7)$.
(a) Denote the colors by b: black; r: brown; and w: white.

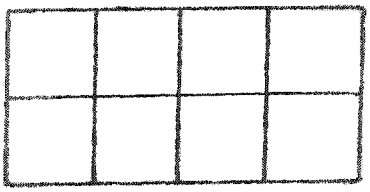
The pattern inventory is $(1/7)[(b+r+w)^7 + 6(b^7+r^7+w^7)]$. In $(b+r+w)^7$ the coefficient

of $b^3r^2w^2$ is $\binom{7}{3,2,2}$, so the answer is $(1/7)\binom{7}{3,2,2} = 30$.

(b) $(1/7)[7$ (for w^7) $+ \binom{7}{5,1,1}$ (for w^5br) $+ \binom{7}{3,2,2}$ (for $w^3b^2r^2$) $+ \binom{7}{1,3,3}$ (for wb^3r^3)$] =$ $(1/7)[7 + 42 + 210 + 140] = 57$

(c) For $n \in \mathbf{Z}^+$, $(1/7)[n^7 + 6n]$ is the number of ways to n-color the seven horses on the carousel. Since this is an integer, 7 divides $(n^7 + 6n)$.

7. (a)



Here $G = \{\pi_0, \pi_1\}$, where π_1 denotes the $180°$ rotation.

$(1/2)[2^8 + 2^4] = 136$ distinct ways to 2-color the squares of the chessboard.

(b) $(1/2)[(r + w)^8 + (r^2 + w^2)^4]$

(c) Four red and four white faces: $(1/2)[\binom{8}{4} + \binom{4}{2}] = 38$
Six red and two white faces: $(1/2)[\binom{8}{6} + \binom{4}{1}] = 16$

8. Here $G = \{\pi_i | 0 \leq i \leq 3\}$ where π_i is a (clockwise) rotation through $i(90°)$.

(a) $(1/4)[2^8 + 2(2^2) + 2^4] = 70$

(b) $(1/4)[3^8 + 2(3^2) + 3^4] = 1665$

(c) For the pattern inventory denote the colors as follows: b: black; g: gold; and u: blue. Then the pattern inventory is given by $(1/4)[(b + g + u)^8 + 2(b^4 + g^4 + u^4)^2 +$ $(b^2 + g^2 + u^2)^4]$.

For four black, two gold, and two blue regions we need the coefficient of $b^4g^2u^2$ in the pattern inventory. This is $(1/4)[\binom{8}{4,2,2} + \binom{4}{2,1,1}] = 108$.

9. Let $c_1, c_2, \ldots, c_m$ denote the m colors. Since the term $(c_1 + c_2 + \ldots + c_m)^n$ is involved in the pattern inventory, there are $\binom{m+n-1}{n}$ distinct summands.

Supplementary Exercises

1. (a) Since $f(e_G) = e_H$, it follows that $e_G \in K$ and $K \neq \emptyset$. If $x, y \in K$, then $f(x) = f(y) = e_H$ and $f(xy) = f(x)f(y) = e_He_H = e_H$, so $xy \in K$. Also, for $x \in K$, $f(x^{-1}) = [f(x)]^{-1} = e_H^{-1} = e_H$, so $x^{-1} \in K$. Hence K is a subgroup of G.

(b) If $x \in K$, then $f(x) = e_H$. For all $g \in G$, $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) =$ $f(g)e_Hf(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$.

Hence, for all $x \in K, g \in G$, we find that $gxg^{-1} \in K$.

2. Let $+$ denote the operation in G, H, and K.

Let $S = \{(h,0) | h \in H\}$. Here 0 is the identity for H (and K) and (0,0) is the identity in G. S is a nonempty subset of G.

The function $f : G \to G$ defined by $f(h,k) = (h,0)$ is a homomorphism with $f(G) = S$, so by part (d) of Theorem 16.5 S is a subgroup of G. The function $g : S \to H$ defined by $g(h,0) = h$ provides an isomorphism between S and H.

In like manner, $\{(0,k) | k \in K\}$ is a subgroup of G that is isomorphic to K.

3. Let $a, b \in G$. Then $a^2b^2 = ee = e = (ab)^2 = abab$. But $a^2b^2 = abab \Longrightarrow aabb = abab \Longrightarrow ab = ba$, so G is abelian.

4. Since G has even order, $G - \{e\}$ is odd. For each $g \in G$, $g \neq e$, if $g \neq g^{-1}$, remove $\{g, g^{-1}\}$ from consideration. As we continue this process we must get to at least one element $a \in G$ where $a = a^{-1}$.

5. Let $G =< g >$ and let $h = f(g)$. If $h_1 \in H$, then $h_1 = f(g^n)$ for some $n \in \mathbf{Z}$, since f is onto. Therefore, $h_1 = f(g^n) = [f(g)]^n = h^n$, and $H = \langle h \rangle$.

6. (a) Since $(1,0) \oplus (0,1) = (1,1)$, it follows that $(1,0) \oplus (0,1) \oplus (1,1) = (1,1) \oplus (1,1) = (0,0)$.

(b) Here we have $((1,0,0) \oplus (0,1,1)) \oplus ((0,1,0) \oplus (1,0,1)) \oplus ((0,0,1) \oplus (1,1,0)) \oplus (1,1,1) = (1,1,1) \oplus (1,1,1) \oplus (1,1,1) \oplus (1,1,1) = (0,0,0)$.

(c) Let $n \in \mathbf{Z}^+, n > 1$. Consider the group $(\mathbf{Z}_2 \times \mathbf{Z}_2 \times \ldots \times \mathbf{Z}_2, \oplus)$, where we have n copies of $\mathbf{Z}_2$, and the group operation $\oplus$ is componentwise addition modulo 2. The sum of all the nonzero (or non-identity) elements in this group is $(0,0,\ldots,0)$, the identity element of the group.
Proof: In this group there are $2^n - 2$ elements where each such element contains at least one 0 and at least one 1. These $2^n - 2$ elements can be considered in $(1/2)(2^n - 2) = 2^{n-1} - 1$ pairs x, y where $x \oplus y = (1,1,\ldots,1)$, the group element where all n components are 1. Therefore the sum of these $2^n - 2$ elements results in $2^{n-1} - 1$ summands of $(1,1,\ldots,1)$, and this *odd* number of summands yields $(1,1,\ldots,1)$. When we add this result to the element $(1,1,\ldots,1)$ we conclude that the sum of all the nonzero elements in this group is the group identity.

7. Proof: For all $a, b \in G$,

$$(a \circ a^{-1}) \circ b^{-1} \circ b = b \circ b^{-1} \circ (a^{-1} \circ a) \Longrightarrow$$
$$a \circ a^{-1} \circ b = b \circ a^{-1} \circ a \Longrightarrow a \circ b = b \circ a,$$

and so it follows that $(G, \circ)$ is an abelian group.

8. For $i = 0$ we find that $n+1$ is in a cycle (of length 1) by itself. Here we have $Q(n,k)$ permutations.

Now let $i = 1$. Here $n+1$ is in a cycle of length 2. The other element can be selected in $n = \binom{n}{1}$ ways, and we have $\binom{n}{1}Q(n-1,k)$ permutations.

When $i = 2$, then $n+1$ is in a cycle of length 3. The other two elements can be selected in $\binom{n}{2}$ ways, and these three elements can be arranged in a cycle of length three in 2! ways. This gives us the $\binom{n}{2}2!Q(n-2,k)$ permutations of $1,2,\ldots,n+1$ represented as a product of disjoint cycles of length at most k, where $n+1$ is in a cycle of length 3.

In general, for $i = t-1$, where $1 \le t \le k$, we find $n+1$ in a cycle of length t. The other $t-1$ elements can be selected in $\binom{n}{t-1}$ ways, and then these t elements can be arranged in a cycle of length t in $(t-1)!$ ways. Then $\binom{n}{t-1}(t-1)!Q(n-(t-1),k)$ counts the permutations of $1,2,3,\ldots,n+1$ represented as a product of disjoint cycles of length at most k, where $n+1$ is in a cycle of length t.

We have counted the same set of permutations in two ways, so it follows that

$$Q(n+1,k) = \sum_{i=0}^{k-1} \binom{n}{i}(i!)Q(n-i,k).$$

9. (a) Consider a permutation σ that is counted in $P(n+1,k)$. If $(n+1)$ is a cycle (of length 1) in σ, then σ (restricted to $\{1,2,\ldots,n\}$) is counted in $P(n,k-1)$. Otherwise, consider any permutation τ that is counted in $P(n,k)$. For each cycle of τ, say $(a_1 a_2 \ldots a_r)$, there are r locations in which to place $n+1$ – (1) Between a_1 and a_2; (2) Between a_2 and a_3; …; $(r-1)$ Between a_{r-1} and a_r; and (r) Between a_r and a_1. Hence there are n locations, in total, to locate $n+1$ in τ. Consequently, $P(n+1,k) = P(n,k-1)+nP(n,k)$.

(b) $\sum_{k=1}^{n} P(n,k)$ counts all of the permutations in S_n, which has $n!$ elements.

10. (a) (i) For all $\sigma,\tau \in S_n$ and $1 \le i \le n$, $|\sigma(i)-\tau(i)| \ge 0$, so $d(\sigma,\tau) \ge 0$.
(ii) $d(\sigma,\tau) = 0 \iff \max|\sigma(i)-\tau(i)| = 0$, $1 \le i \le n \iff |\sigma(i)-\tau(i)| = 0$, $1 \le i \le n \iff \sigma(i) = \tau(i)$, $1 \le i \le n \iff \sigma = \tau$.
(iii) $d(\sigma,\tau) = \max\{|\sigma(i)-\tau(i)||1 \le i \le n\} = \max\{|\tau(i)-\sigma(i)||1 \le i \le n\} = d(\tau,\sigma)$
(iv) Let $d(\rho,\tau) = |\rho(i)-\tau(i)|$ for some $1 \le i \le n$. Then $|\rho(i)-\tau(i)| = |(\rho(i)-\sigma(i))+(\sigma(i)-\tau(i))| \le |\rho(i)-\sigma(i)| + |\sigma(i)-\tau(i)| \le d(\rho,\sigma)+d(\sigma,\tau)$.

(b) Since $d(\pi,\epsilon) = \max\{|\pi(i)-i||1 \le i \le n\}$, it follows that $d(\pi,\epsilon) \le 1 \Longrightarrow \pi(n) = n$ or $\pi(n) = n-1$.

(c) If $\pi(n) = n$ then π restricted to $\{1,2,3,\ldots,n-1\}$ is also a permutation. Hence we may regard π as an element of S_{n-1}, with $d(\pi,\epsilon) \le 1$ (ϵ in S_{n-1}), and there are a_{n-1} such permutations. Should $\pi(n) = n-1$, then we must also have $\pi(n-1) = n$. Then π restricted to $\{1,2,3,\ldots,n-2\}$ is a permutation. Regarding π as an element

of S_{n-2} with $d(\pi,\epsilon) \leq 1$ (ϵ in S_{n-2}), there are a_{n-2} such permutations. Therefore, $a_n = a_{n-1} + a_{n-2}$, $n \geq 2$, $a_1 = 1$, $a_2 = 2$ ($a_0 = 1$), and $a_n = F_{n+1}$, the $(n+1)$st Fibonacci number.

11. (a) Suppose that n is composite. We consider two cases.
(1) $n = m \cdot r$, where $1 < m < r < n$: Here $(n-1)! = 1 \cdot 2 \cdots (m-1) \cdot m \cdot (m+1) \cdots (r-1) \cdot r \cdot (r+1) \cdots (n-1) \equiv 0 \pmod{n}$. Hence $(n-1)! \not\equiv -1 \pmod{n}$.
(2) $n = q^2$, where q is a prime: If $(n-1)! \equiv -1 \pmod{n}$ then $0 \equiv q(n-1)! \equiv q(-1) \equiv n - q \not\equiv 0 \pmod{n}$. So in this case we also have $(n-1)! \not\equiv -1 \pmod{n}$.

(b) From Wilson's Theorem, when p is an odd prime, we find that

$$-1 \equiv (p-1)! \equiv (p-3)!(p-2)(p-1) \equiv (p-3)!(p^2 - 3p + 2) \equiv 2(p-3)! \pmod{p}.$$

12. $G = \{\pi_0, \pi_1, \pi_2, \pi_3\}$

(a) $(1/4)[5^8 + 5^2 + 5^4 + 5^2] = 97,825$

(b) Here four colors are actually used. Nicole can select four colors in $\binom{5}{4} = 5$ ways. For one selection of four colors let $c_i, 1 \leq i \leq 4$, denote that the i-th color is not used. Then using the principle of inclusion and exclusion we have

$N = (1/4)[4^8 + 2(4^2) + 4^4] = 16,456$
$N(c_i) = (1/4)[3^8 + 2(3^2) + 3^4] = 1665,\ 1 \leq i \leq 4$
$N(c_i c_j) = (1/4)[2^8 + 2(2^2) + 2^4] = 70,\ 1 \leq i < j \leq 4$
$N(c_i c_j c_k) = (1/4)[1^8 + 2(1^2) + 1^4] = 1,\ 1 \leq i < j < k \leq 4$
$N(c_1 c_2 c_3 c_4) = 0$
$N(\bar{c}_1 \bar{c}_2 \bar{c}_3 \bar{c}_4) = N - S_1 + S_2 - S_3 + S_4 = 16,456 - \binom{4}{1}(1665) + \binom{4}{2}(70) - \binom{4}{3}(1) + 0 = 10,212.$

The answer then is $(5)(10,212) = 51,060$.