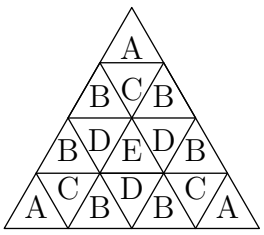
MAS114: Semester 2 Solution Booklet

1 Orbits, Functions and Symmetries

1. (Homework problem)

2. (a) There are 7 triangles made up of 4 small triangles. In the diagram, there are three with bases on the lowest horizontal line, two with bases on the next horizontal line up, and two, one of which points upwards, with bases on the next horizontal line up. There are 3 triangles made up of 9 small triangles, one in each corner.



(b)

j small triangles	no. of orbits	no. of elements in each orbit	total
$j = 1$	5	3,6,3,3,1	16
$j = 4$	3	3,3,1	7
$j = 9$	1	3	3
$j = 16$	1	1	1
total	10	—	27

The five orbits of small triangles are indicated by the letters $A - E$ in the diagram above.

3. (a) $f_{50}f_{100} = f_{150}$; (b) $f_{50}g_{100} = g_{150}$; (c) $g_{50}f_{100} = g_{-50}$; $g_{50}g_{100} = f_{-50}$.

4. (a) $(\mathrm{rot}_\alpha \mathrm{rot}_\beta)\,\mathrm{rot}_\gamma = \mathrm{rot}_{\alpha+\beta}\,\mathrm{rot}_\gamma = \mathrm{rot}_{\alpha+\beta+\gamma}$.

   (b) $(\mathrm{ref}_\alpha \mathrm{ref}_\beta)\,\mathrm{ref}_\gamma = \mathrm{rot}_{\alpha-\beta}\,\mathrm{ref}_\gamma = \mathrm{ref}_{\alpha-\beta+\gamma}$.

   (c) $(\mathrm{ref}_\alpha \mathrm{rot}_\beta)\,\mathrm{ref}_\alpha = \mathrm{ref}_{\alpha-\beta}\,\mathrm{ref}_\alpha = \mathrm{rot}_{-\beta}$.

   (d) $(\mathrm{rot}_\alpha \mathrm{ref}_\beta)\,\mathrm{rot}_\alpha = \mathrm{ref}_{\alpha+\beta}\,\mathrm{rot}_\alpha = \mathrm{ref}_\beta$.

5. (Homework problem)

6.

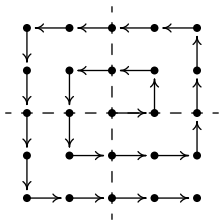
D_3	e	r_1	r_2	s_1	s_2	s_3
e	e	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	e	s_2	s_3	s_1
r_2	r_2	e	r_1	s_3	s_1	s_2
s_1	s_1	s_3	s_2	e	r_2	r_1
s_2	s_2	s_1	s_3	r_1	e	r_2
s_3	s_3	s_2	s_1	r_2	r_1	e

7. Six are surjective. (It is easier to count the non-surjective ones of which there are two, the first and last of those displayed in the problem. A non-surjective function from $\{1,2,3\}$ to $\{1,2\}$ must either send every element of $\{1,2,3\}$ to 1 or send every element of $\{1,2,3\}$ to 2.) None are injective as at least two of $1,2,3$ must be sent to the same element of $\{1,2\}$.

8. There are $3 \times 3 = 9$ functions f from $\{1,2\}$ to $\{1,2,3\}$. There are 3 choices, $1,2$ or 3, for $f(1)$ and, for each of these, there are three choices for $f(2)$. Of these 9 functions, none are surjective, the range $\{f(1), f(2)\}$ has at most two elements so cannot be all of the codomain $\{1,2,3\}$. Six are injective. The three that are not injective are those that send 1 and 2 to the same element of the codomain $\{1,2,3\}$.

9. (Homework problem)

10. (a)



(b) Following the path indicated, we can list the elements of $\mathbb{Z}[i]$ to obtain $\mathbb{Z}[i] = \{0, 1, 1+i, i, -1+i, -1, -1-i, -i, 1-i, 2-i, \ldots\}$. Thus $\mathbb{Z}[i]$ is countable.

11. (Homework problem)

2 Permutations

1. In two-row notation,
$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 1 & 2 & 7 & 8 & 4 & 3 \end{pmatrix}.$$

2. Here, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$ and $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$.

3. To form a k-cycle $(a_1\ a_2\ \ldots a_k)$ in S_6 (where $2 \leq k \leq 6$), there are 6 choices for a_1 and then 5 for a_2 and so on, with $6 - k + 1$ choices for a_k. Hence there are $6 \times 5 \times \ldots \times (6 - k + 1)$ expressions $(a_1\ a_2\ \ldots a_k)$. But each k-cycle occurs in k different ways, depending on the choice of starting number, so we have to divide by k to get the number of *different* k-cycles, namely $\frac{6\times5\times\ldots\times(6-k+1)}{k} = \frac{6!}{k(6-k)!}$. This formula gives 15 transpositions (2-cycles), 40 3-cycles, 90 4-cycles, 144 5-cycles and 120 6-cycles.

   The total number of permutations in S_6 is $6! = 720$, and we've found that there are 411 cycles (namely all of those listed above plus the 1-cycle, id), so there are more permutations in S_6 that are cycles than aren't.

4. (a) $(1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4)$.

   (b) $(1\ 2\ 3\ 4\ 5)^2 = (1\ 3\ 5\ 2\ 4)$.

   (c) $(1\ 2\ 3\ \ldots 2m-1\ 2m)^2 = (1\ 3\ 5 \ldots 2m-1)(2\ 4\ 6 \ldots 2m)$.

   (d) $(1\ 2\ 3\ \ldots 2m\ 2m+1)^2 = (1\ 3\ 5 \ldots 2m+1\ \ 2\ 4\ 6 \ldots 2m)$.

5. Following the given advice, we find that
$$\alpha = (6\ 7)(5\ 6)(6\ 7)(3\ 4)(4\ 5)(5\ 6)(2\ 3)(3\ 4)(1\ 2)(2\ 3)(3\ 4),$$
   which is an odd permutation, being a product of 11 transpositions.

   (In more detail, we begin by ensuring that the right element, 4, is sent to 1: the three terms on the right hand end send 4 to 1, which never appears again, so $4 \mapsto 1$.

   Next we ensure that the right element, 3, is sent to 2: the three terms on the right hand end send 3 to 4 so the five terms on the right hand end send 3 to 2, which never appears again, so $3 \mapsto 2$.

   The eight terms on the right hand end send 6 to 3, which never appears again, so $6 \mapsto 3$. These terms also send 1 to 4, which never appears again, so $1 \mapsto 4$.

   The ten terms on the right send 7 to 5, which never appears again, so $7 \mapsto 5$. The whole product sends 5 to 6 and 7 to 2.)

6. Applying the given formulas,

$$\begin{aligned}(a_1\ a_2\ a_3\ \ldots\ a_k) &= (a_1\ a_k)(a_1\ a_{k-1})\ldots(a_1\ a_2)\\ &= (1\ a_1)(1\ a_k)(1\ a_1)(1\ a_1)(1\ a_{k-1})(1\ a_1)\ldots(1\ a_1)(1\ a_2)(1\ a_1)\\ &= (1\ a_1)(1\ a_k)(1\ a_{k-1})\ldots(1\ a_2)(1\ a_1)\end{aligned}$$

because $(1\ a_1)^2 = \mathrm{id}$. This then gives $(5\ 6\ 7) = (1\ 5)(1\ 7)(1\ 6)(1\ 5)$.

7. (a) For all $\alpha \in S_n$, $\mathrm{sgn}(\alpha^2) = (\mathrm{sgn}\,\alpha)^2 = (\pm 1)^2 = +1$. The permutation $(1\ 2\ 3\ 4\ 5\ 6)$ is odd, so has sign -1, so α^2 can never equal $(1\ 2\ 3\ 4\ 5\ 6)$.

   (b) $(a_1\ a_2\ a_3\ a_4\ a_5\ a_6)^2 = (a_1\ a_3\ a_5)(a_2\ a_4\ a_6)$ so take $\alpha = (1\ 4\ 2\ 5\ 3\ 6)$. Then $\alpha^2 = (1\ 2\ 3)(4\ 5\ 6)$.

   (c) $(a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7)^2 = (a_1\ a_3\ a_5\ a_7\ a_2\ a_4\ a_6)$ so take $\alpha = (1\ 5\ 2\ 6\ 3\ 7\ 4)$. Then $\alpha^2 = (1\ 2\ 3\ 4\ 5\ 6\ 7)$.

8. (a) (i) $(1\ b\ c) = (1\ c)(1\ b)$.

   (ii) Using Problem 6, $\theta = (1\ 3\ 4)(5\ 6\ 7) = (1\ 4)(1\ 3)(1\ 5)(1\ 7)(1\ 6)(1\ 5)$.

   (b) Pairing off the transpositions on the right hand side of (a)(ii) and applying the formula in (a)(i) to each of the three pairs, $\theta = (1\ 3\ 4)(1\ 7\ 5)(1\ 5\ 6)$. (This method, pairing off the transpositions, could be applied to any even permutation.)

   (c) Cycles of length 3 are even. Therefore any product of cycles of length 3 is even. But α is odd so it cannot be a product of cycles of length 3.

9. (Homework problem)

10. (Homework problem)

3 Groups and subgroups

1. The completed table is

$\times$mod8	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

.

   The table shows that G is closed (as all the entries lie in G) and that $\overline{1}$ is neutral. Each element is its own inverse. This completes three of the group axioms - the fourth is associativity, which does hold in G, so G is a group.

2. In each case we can simply find $x = a^{-1}b$ and $y = ba^{-1}$.

   (a) $x = a^{-1}b = \mathrm{rot}_{\frac{-\pi}{6}} \mathrm{ref}_{\frac{\pi}{2}} = \mathrm{ref}_{\frac{\pi}{3}}$. $y = ba^{-1} = \mathrm{ref}_{\frac{\pi}{2}} \mathrm{rot}_{\frac{-\pi}{6}} = \mathrm{ref}_{\frac{2\pi}{3}}$.

   (b) $x = a^{-1}b = (1\ 4\ 2)(1\ 3) = (1\ 3\ 4\ 2)$. $y = ba^{-1} = (1\ 3)(1\ 4\ 2) = (1\ 4\ 2\ 3)$.

   (c) Here the group is Abelian and $x = y = a^{-1}b = \overline{5}\ \overline{4} = \overline{6}$.

3. By multiplying the equation $g^2 = g$ on the left by g^{-1}, we get $g^{-1}gg = g^{-1}g$, so $g = e$.

4. (Homework problem)

5. (Homework problem)

6. $\rho_1\sigma_1 = (1\ 2\ 3)(1\ 2) = (1\ 3) = \sigma_2$, $\sigma_1\rho_1 = (1\ 2)(1\ 2\ 3) = (2\ 3) = \sigma_3$ and $\sigma_1\sigma_2 = (1\ 2)(1\ 3) = (1\ 3\ 2) = \rho_2$. Entering these, the table becomes

S_3	id	ρ_1	ρ_2	σ_1	σ_2	σ_3
id	id	ρ_1	ρ_2	σ_1	σ_2	σ_3
ρ_1	ρ_1		id	σ_2		
ρ_2	ρ_2	id				
σ_1	σ_1	σ_3		id	ρ_2	
σ_2	σ_2				id	
σ_3	σ_3					id

   ρ_1^2 is even, id and ρ_1 already appear in row 2 so $\rho_1^2 = \rho_2$.

   $\rho_1\sigma_3$ is odd, σ_2 already appears in row 2 and σ_3 already appears in column 6, and so $\rho_1\sigma_3 = \sigma_1$.

   $\rho_1\sigma_2$ is odd, σ_2 and σ_1 already appear in row 2, and so $\rho_1\sigma_2 = \sigma_3$.

   Row 3 is now easily completed: ρ_2^2 must be ρ_1 and, as two of the three σ_is already appear in each column, we must have $\rho_2\sigma_1 = \sigma_3, \rho_2\sigma_2 = \sigma_1$ and $\rho_2\sigma_3 = \sigma_2$. The rest of the table is completed in a similar way; for example $\sigma_1\sigma_3$ is even and must be ρ_1 as id and ρ_2 already appear in row 4.

S_3	id	ρ_1	ρ_2	σ_1	σ_2	σ_3
id	id	ρ_1	ρ_2	σ_1	σ_2	σ_3
ρ_1	ρ_1	ρ_2	id	σ_2	σ_3	σ_1
ρ_2	ρ_2	id	ρ_1	σ_3	σ_1	σ_2
σ_1	σ_1	σ_3	σ_2	id	ρ_2	ρ_1
σ_2	σ_2	σ_1	σ_3	ρ_1	id	ρ_2
σ_3	σ_3	σ_2	σ_1	ρ_2	ρ_1	id

7. (Homework problem)

8. (a) F,G,J,P,R

(b) A,B,C,D,E,K,L,M,Q,T,U,V,W

(c) N,S,Z

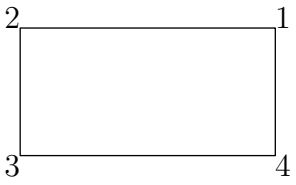
(d) H,I

(e) Y

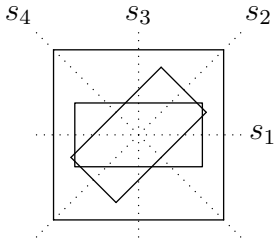
(f) X

(g) O

9. (a) The 4 elements are id, (1 3)(2 4), which is performed by rotation through π, (1 2)(3 4), which is performed by reflection in the y-axis, and (1 4)(2 3), which is performed by reflection in the x-axis.



(b) The rectangle with its longer sides horizontal has group of symmetries $\{e, r_2, s_1, s_3\}$ and the other rectangle has group of symmetries $\{e, r_2, s_2, s_4\}$. Both are subgroups of D_4 isomorphic to Klein's 4-group.



10.

$G \times G$	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,-1)$	$(1,-1)$	$(1,1)$	$(-1,-1)$	$(-1,1)$
$(-1,1)$	$(-1,1)$	$(-1,-1)$	$(1,1)$	$(1,-1)$
$(-1,-1)$	$(-1,-1)$	$(-1,1)$	$(1,-1)$	$(1,1)$

11. Using the formula $|G \times H| = |G||H|$, $|D_4 \times D_6| = 8 \times 12 = 96$, $|S_4 \times K| = 24 \times 4 = 96$ and $|U_3 \times U_{32}| = 3 \times 32 = 96$.

12. The groups concerned are those in Chapter 3, Q1 and Q10. They both have a Cayley table of the form

G	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

.

Each element is its own inverse and the product of any two of a, b, c is the third. In Klein's 4-group in the notes, the Cayley table has the same form with $a = r, b = s, c = t$.

4 Cyclic Groups

1. (a) By Fermat's Little Theorem, we know that $\overline{a}^{p-1} = \overline{1}$ in $\mathbb{Z}_p \setminus \{\overline{0}\}$. If n is the order of $\overline{a}$ then, by Theorem 4.11(ii), n must be a factor of $p-1$.

   (b) The following were computed using MAPLE, replacing 43 in the given commands by the appropriate primes.

   Take $p = 11$: modulo 11, the powers of 2 are $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$ so $\overline{2}$ has order $10 = p - 1$.

   Take $p = 13$: modulo 13, the powers of 2 are $2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1$ so $\overline{2}$ has order $12 = p - 1$.

   Take $p = 17$: modulo 17, the powers of 2 are
   $2, 4, 8, 16, 15, 13, 9, 1, 2, 4, 8, 16, 15, 13, 9, 1$ so $\overline{2}$ has order $8 \neq p - 1$.

   Modulo 17, the powers of 3 are
   $3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1$ so $\overline{3}$ has order $16 = p - 1$.

   Take $p = 31$: modulo 31, the powers of 2 are
   $2, 4, 8, 16, 1, 2, 4, 8, 16, 1, 2, 4, 8, 16, 1, 2, 4, 8, 16, 1, 2, 4, 8, 16, 1$
   so $\overline{2}$ has order $5 \neq p - 1$.

   Modulo 31, the powers of 3 are
   $3, 9, 27, 19, 26, 16, 17, 20, 29, 25, 13, 8, 24, 10, 30, 28, 22, 4, 12,$
   $5, 15, 14, 11, 2, 6, 18, 23, 7, 21, 1$
   so $\overline{3}$ has order $30 = p - 1$, and hence $\overline{3}$ generates $\mathbb{Z}_{31} \setminus \{\overline{0}\}$.

   Take $p = 41$: modulo 41, the powers of 2 are
   $2, 4, 8, 16, 32, 23, 5, 10, 20, 40, 39, 37, 33, 25, 9, 18, 36, 31, 21, 1,$
   so $\overline{2}$ has order $20 \neq p - 1$.

   Modulo 41 the powers of 3 are $3, 9, 27, 40, 38, 32, 14, 1$ so $\overline{3}$ has order 8. $\overline{4}$ has order 10 (because $\overline{2}$ has order 20 and $\overline{4} = \overline{2}^2$). Modulo 41 the powers of 5 are
   $5, 25, 2, 10, 9, 4, 20, 18, 8, 40, 36, 16, 39, 31, 32, 37, 21, 23, 33, 1$
   so $\overline{5}$ has order 20. (Alternatively $\overline{5} = \overline{2}^7$ so $\overline{5}$ has order $20 = \dfrac{\text{l.c.m. of } 20, 7}{7}$. See Theorem 4.20.) However modulo 41, the powers of 6 are
   $6, 36, 11, 25, 27, 39, 29, 10, 19, 32, 28, 4, 24, 21, 3, 18, 26, 33, 34, 40,$
   $35, 5, 30, 16, 14, 2, 12, 31, 22, 9, 13, 37, 17, 20, 38, 23, 15, 8, 7, 1$
   so $\overline{6}$ has order $40 = p - 1$, and hence $\overline{6}$ generates $\mathbb{Z}_{41} \setminus \{\overline{0}\}$.

2. (Homework problem)

3. (a) g has order 27, g^9 has order 3 and, by Theorem 4.18, g^{12} has order $9 = \dfrac{108}{12} = \dfrac{\text{l.c.m. of } 12, 27}{12}$.

   (b) The 3 elements of $\langle g^9 \rangle$ are $g^9 (= \text{rot}_{\frac{2\pi}{3}})$, $g^{18} (= \text{rot}_{\frac{4\pi}{3}})$ and $g^{27} = g^0 (= \text{id} = \text{rot}_0)$.

   The 9 elements of $\langle g^{12} \rangle$ are $g^{12} (= \text{rot}_{\frac{8\pi}{9}})$, $g^{24} (= \text{rot}_{\frac{16\pi}{9}})$, $g^{36} = g^9 (= \text{rot}_{\frac{2\pi}{3}})$, $g^{48} = g^{21} (= \text{rot}_{\frac{14\pi}{9}})$, $g^{60} = g^6 (= \text{rot}_{\frac{4\pi}{9}})$, $g^{72} = g^{18} (= \text{rot}_{\frac{4\pi}{3}})$, $g^{84} = g^3 (= \text{rot}_{\frac{2\pi}{9}})$, $g^{96} = g^{15} (= \text{rot}_{\frac{10\pi}{9}})$ and $g^{108} = g^0 (= \text{rot}_0)$.

   (c) $d = 18$, $e = 3$.

4. (a) rot_π.

   (b) (i) Infinitely many (as any reflection has order 2).

   (ii) 5 (all of which are reflections).

   (iii) 7 (one of which is rot_π).

5. There are 7, namely $\langle e \rangle = \{e\}$, $\langle r_1 \rangle = \langle r_2 \rangle = \langle r_3 \rangle = \langle r_4 \rangle = \{e, r_1, r_2, r_3, r_4\}$, $\langle s_1 \rangle = \{e, s_1\}$, $\langle s_2 \rangle = \{e, s_2\}$, $\langle s_3 \rangle = \{e, s_3\}$, $\langle s_4 \rangle = \{e, s_4\}$ and $\langle s_5 \rangle = \{e, s_5\}$.

6. There is one subgroup for each of the positive divisors of 8 (see 4.22). The divisors are $1, 2, 4, 8$ and the four subgroups are: $\langle g^1 \rangle = G = \{e, g, g^2, g^3, g^4, g^5, g^6, g^7\}$, $\langle g^2 \rangle = \{e, g^2, g^4, g^6\}$, $\langle g^4 \rangle = \{e, g^4\}$ and $\langle g^8 \rangle = \{e\}$.

   (If you simply apply 4.21, you get that the subgroups are $\langle g^j \rangle$ where $0 \leq j \leq 7$. This gives, apparently, four extra subgroups $\langle g^3 \rangle, \langle g^5 \rangle, \langle g^6 \rangle, \langle g^7 \rangle$. However $\langle g^3 \rangle = \{e, g^3, g^6, g, g^4, g^7, g^2, g^5\} = G$, $\langle g^5 \rangle = \{e, g^5, g^2, g^7, g^4, g, g^6, g^3\} = G$, $\langle g^6 \rangle = \{e, g^6, g^4, g^2\} = \langle g^2 \rangle$, and $\langle g^7 \rangle = \{e, g^7, g^6, g^5, g^4, g^3, g^2, g\} = G$.)

7. As U_{24} is cyclic of order 24, there is one subgroup for each of the positive divisors of 24. (see 4.22). The divisors are $1, 2, 3, 4, 6, 8, 12, 24$ and so there are 8 different subgroups of U_{24}.

5 Group Actions

1. $\text{orb}(1) = \{1, 3, 5\}$, $\text{stab}(1) = \{e, r_3, s_1, s_4\}$.

2. (i) $|\text{orb}(x)| = 2$, $\text{stab}(x) = \{e, r_2, s_1, s_3\}$.

   (ii) $|\text{orb}(x)| = 4$, $\text{stab}(x) = \{e, r_2\}$.

   (iii) $|\text{orb}(x)| = 2$, $\text{stab}(x) = \{e, r_1, r_2, r_3\}$.

3. (Homework problem)

4. (a) The number of essentially different colourings is the number of orbits for the action of the group of rotations of the square, which has four elements, $e = \text{rot}_0, r_1 = \text{rot}_{\frac{\pi}{2}}, r_2 = \text{rot}_\pi$ and $r_3 = \text{rot}_{\frac{3\pi}{2}}$. There are n choices of colour for each of the nine regions so there are n^9 colourings. All are fixed by e so $|\operatorname{fix}(e)| = n^9$.

A	B	A
B	C	B
A	B	A

C	B	A
D	E	D
A	B	C

The colourings fixed by r_1 must have the same colour in each of the regions marked A in the first diagram, a second colour in each B and a third colour for C. Hence $|\operatorname{fix}(r_1)| = n^3$. The colourings fixed by r_3 are the same as those fixed by r_1 so $|\operatorname{fix}(r_3)| = n^3$. The other diagram indicates that $|\operatorname{fix}(r_2)| = n^5$. By the Orbit-Counting Theorem, the total number of essentially different colourings is $\frac{1}{4}(n^9 + n^5 + 2n^3)$.

(b) Here the number of essentially different colourings is the number of orbits for the action of the full group of symmetries of the square. In addition to the rotations in (a), there are four reflections s_1 (in the x-axis), s_2 (in the line $y = x$), s_3 (in the y-axis) and s_4 (in the line $y = -x$). As in (a), $|\operatorname{fix}(e)| = n^9$, $|\operatorname{fix}(r_1)| = n^3$, $|\operatorname{fix}(r_2)| = n^5$ and $|\operatorname{fix}(r_3)| = n^3$.

C	B	A
D	E	F
C	B	A

C	B	A
D	E	B
F	D	C

The lefthand diagram indicates that $|\operatorname{fix}(s_1)| = n^6$ and similarly $|\operatorname{fix}(s_3)| = n^6$. The righthand diagram indicates that $|\operatorname{fix}(s_2)| = n^6$ and similarly $|\operatorname{fix}(s_4)| = n^6$. By the Orbit-Counting Theorem, the total number of essentially different colourings is $\frac{1}{8}(n^9 + 4n^6 + n^5 + 2n^3)$.

(c) The total number of colourings is ${}_9C_3 = 84$ so $|\operatorname{fix}(e)| = 84$.

There are no colourings fixed by r_1 because we cannot have exactly three yellow regions in the first diagram in (a). Thus $|\operatorname{fix}(r_1)| = 0$ and similarly $|\operatorname{fix}(r_3)| = 0$.

In a colouring fixed by r_2 (righthand diagram in (a)), E must be yellow and one of four pairs A,B,C,D is yellow so $|\operatorname{fix}(r_2)| = 4$.

In a colouring fixed by s_1 (lefthand diagram in (b)), either E,D,F are yellow and A,B,C are orange or one of E,D,F and one of A,B,C are

yellow. Hence $|\operatorname{fix}(s_1)| = 1+(3\times 3) = 10$. Similarly $|\operatorname{fix}(s_2)| = |\operatorname{fix}(s_3)| = |\operatorname{fix}(s_4)| = 10$.

By the Orbit-Counting Theorem, the total number of essentially different colourings is $\frac{1}{8}(84 + 4 + 40) = 16$.

5. The number of essentially different colourings is the number of orbits for the action of the group of symmetries $\{e, r, s, t\}$ of the non-square rectangle. There are n choices of colour for each of the four regions so there are n^4 colourings. All are fixed by e so $|\operatorname{fix}(e)| = n^4$.

   The colourings fixed by the rotation r must have the same colour in each pair of opposite corners. Hence $|\operatorname{fix}(r)| = n^2$.

   In a colouring fixed by a reflection, the colour in each region is the same as in its mirror image. There are two pairs of regions and so $|\operatorname{fix}(s)| = n^2 = |\operatorname{fix}(t)|$.

   By the Orbit-Counting Theorem, the total number of essentially different colourings is $\frac{1}{4}(n^4 + 3n^2)$.

6. (i) $\operatorname{stab}(p) = \{\mathrm{id}, (1\ 2)\}$ and $\operatorname{orb}(p) = \{x_1x_2 + x_3^2, x_1x_3 + x_2^2, x_2x_3 + x_1^2\}$.

   (ii) $\operatorname{stab}(p) = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$ and $\operatorname{orb}(p) = \{x_1^2x_2 + x_2^2x_3 + x_3^2x_1, x_1^2x_3 + x_2^2x_1 + x_3^2x_2\}$.

6 Equivalence Relations

1. - Reflexivity: $\frac{1}{2} \not\sim \frac{1}{2}$, because $\frac{1}{2} - 2 \times \frac{1}{2} = -\frac{1}{2} \notin \mathbb{Z}$ so $\sim$ is not reflexive.
   - Symmetry: $0 \sim \frac{1}{2}$, because $0 - 2 \times \frac{1}{2} = -1 \in \mathbb{Z}$, but $\frac{1}{2} \not\sim 0$, because $\frac{1}{2} - 2 \times 0 = \frac{1}{2} \notin \mathbb{Z}$. So $\sim$ is not symmetric.
   - Transitivity: Let $a = 0, b = \frac{1}{2}, c = \frac{1}{4}$. Then $a \sim b$, because $0 - 2 \times \frac{1}{2} = -1 \in \mathbb{Z}$, and $b \sim c$, because $\frac{1}{2} - 2 \times \frac{1}{4} = 0 \in \mathbb{Z}$, but $a \not\sim c$, because $0 - 2 \times \frac{1}{4} = -\frac{1}{2} \notin \mathbb{Z}$. So $\sim$ is not transitive.

2. - Reflexivity: Let $a \in \mathbb{C}$. Then $a - a = 0 \in \mathbb{R}$ so $a \sim a$. Thus $\sim$ is reflexive.
   - Symmetry: Let $a, b \in \mathbb{C}$ be such that $a \sim b$, that is $a - b \in \mathbb{R}$. Then $b - a = -(a - b) \in \mathbb{R}$ so $b \sim a$. Thus $\sim$ is symmetric.
   - Transitivity: Let $a, b, c \in \mathbb{C}$ be such that $a \sim b$ and $b \sim c$, that is $a - b \in \mathbb{R}$ and $b - c \in \mathbb{R}$. Then $a - c = (a - b) + (b - c) \in \mathbb{R}$ so $a \sim c$. Thus $\sim$ is transitive.

   The equivalence class of $11 + 4i$ consists of all complex numbers of the form $a + 4i$, $a \in \mathbb{R}$. So, for example, we can take $4i, 1 + 4i, 2 + 4i$.

7 Cosets and Lagrange's Theorem

1. (a) $eH = H = \{e, s_2\}$. $r_1H = \{r_1e, r_1s_2\} = \{r_1, s_3\}$. $r_2H = \{r_2e, r_2s_2\} = \{r_2, s_1\}$.

   (b) $eH = H = \{e, r_1, r_2\}$. $s_1H = \{s_1e, s_1r_1, s_1r_2\} = \{s_1, s_3, s_2\}$.

   (c) $eH = H = \{e, g^3, g^6, g^9\}$.
   $gH = \{ge, gg^3, gg^6, gg^9\} = \{g, g^4, g^7, g^{10}\}$.
   $g^2H = \{g^2e, g^2g^3, g^2g^6, g^2g^9\} = \{g^2, g^5, g^8, g^{11}\}$.

2. By Lagrange's Theorem, the order of any subgroup of S_4 must be a factor of 24 (the order of S_4). 5 is not a factor of 24 so S_4 has no subgroup of order 5.

   Let $\theta = (1\ 2\ 3)(4\ 5) \in S_5$. Then θ has order 6, the l.c.m. of 3 and 2, so the cyclic subgroup $\langle\theta\rangle = \{\mathrm{id}, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$ has order 6. An alternative is $H = \{\alpha \in S_5 : \alpha(4) = 4 \text{ and } \alpha(5) = 5\}$, which is a subgroup of S_5 isomorphic to S_3 and has order 6.

3. Note first that S_4 has order $4! = 24$ and that $G = \{e, g, g^2, \ldots, g^{13}\}$, where $g^{14} = e$. Also, Lagrange's theorem states that any subgroup of a group must have an order which divides the order of the group.

   For $d = 2$, we have the subgroup $\{e, g^7\} = \langle g^7\rangle$ of G (this is the only subgroup of G of order 2). We also have subgroups of S_4 of order 2, which are all of the form $\{\mathrm{id}, \tau\}$ where τ is any transposition, e.g. $(1\ 2)$.

   There are no subgroups of G or S_4 of order 5, by Langrange's Theorem.

   For $d = 7$, we have the subgroup $\{e, g^2, g^4, \ldots, g^{12}\} = \langle g^2\rangle$ of G (this is the only subgroup of G of order 7). There is no subgroup of S_4 of order 7 by Lagrange's Theorem.

   There are no subgroups of G or S_4 of order 11, again by Langrange's Theorem.

4. (a) By Lagrange's Theorem, $|H|$ and $|K|$ must each be one of $1, 7, 11, 77$, the factors of $|G|$. As both H and K are nontrivial, neither has order 1. As both H and K are proper, neither has order 77. As $|H| > |K|$ we must have $|H| = 11$ and $|K| = 7$.

   (b) $H \cap K$ is a subgroup of H so, by Lagrange's Theorem, $|H \cap K|$ is a factor of $|H| = 11$. $H \cap K$ is a subgroup of K so, by Lagrange's Theorem, $|H \cap K|$ is a factor of $|K| = 7$. The only (positive) common factor of 7 and 11 is 1 so $H \cap K$ must be $\{e\}$, in other words, the only element of G in both H and K is e.

5. To compute the remainder on dividing 43^{462} by 19, we simplify $\overline{43^{462}}$ in $\mathbb{Z}_{19}$ to $\overline{r}$, where $0 \leq r \leq 18$. Then r is the remainder. As $43 \equiv 5 \bmod 19$, $\overline{43} = \overline{5}$.

So $\overline{43^{462}} = \overline{43}^{462} = \overline{5}^{462}$. By Fermat's Little Theorem, $\overline{5}^{18} = \overline{1}$. Therefore, as 18 divides 450, $\overline{5}^{450} = \overline{1}$ and $\overline{5}^{462} = \overline{5}^{12}$.

Now $\overline{5}^2 = \overline{25} = \overline{6}$ so $\overline{5}^4 = \overline{6}^2 = \overline{36} = \overline{-2}$ (-2 is easier to calculate with than 17). Hence $\overline{5}^{12} = (\overline{5}^4)^3 = (\overline{-2})^3 = \overline{-8} = \overline{11}$. The remainder is 11.

To compute the remainder on dividing 43^{462} by 47, we simplify, $\overline{43^{462}}$ in $\mathbb{Z}_{47}$ to $\overline{r}$, where $0 \leq r \leq 46$. Then r is the remainder. Now $\overline{43^{462}} = \overline{43}^{462}$. By Fermat's Little Theorem, $\overline{43}^{46} = \overline{1}$. Therefore, as 46 divides 460, $\overline{43}^{460} = \overline{1}$ and $\overline{43}^{462} = \overline{43}^2$.

Now $\overline{43}^2 = \overline{-4}^2 = \overline{16}$ so the remainder is 16.

6. Let G be a group of order 6. By Lagrange's Theorem, any proper subgroup of G has order 1,2 or 3. The only subgroup of order 1 is the trivial subgroup $\{e\}$ which is cyclic generated by e. As 2 and 3 are prime, any subgroup of order 2 or 3 must be cyclic by Theorem 7.8(ii).

   S_3 has order 6 so all its proper subgroups are cyclic.

   The cyclic subgroups, and hence all the proper subgroups, of S_3 are

$$\langle \mathrm{id} \rangle = \{\mathrm{id}\}, \quad \langle (1\ 2) \rangle = \{\mathrm{id}, (1\ 2)\},$$

$$\langle (1\ 3) \rangle = \{\mathrm{id}, (1\ 3)\}, \quad \langle (2\ 3) \rangle = \{\mathrm{id}, (2\ 3)\},$$

$$\langle (1\ 2\ 3) \rangle = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\} \text{ and } \langle (1\ 3\ 2) \rangle = \{\mathrm{id}, (1\ 3\ 2), (1\ 2\ 3)\}.$$

   Note that the last two are equal so, including the whole group, there are 6 subgroups, 3 of order 2 and one of each of the orders 1,3,6.

8 Orbits and Stabilizers

1. (i) $p = x_1x_2x_3 + x_4$: the permutations which send p to itself are those which fix 4 and permute $1, 2$ and 3. There are six ($= 3!$) of these so $|\operatorname{stab}(p)| = 6$. The orbit consists of all polynomials of the form $x_i + x_jx_kx_l$ with i, j, k, l being the distinct numbers from 1 to 4. There are four of these, one for each i. Thus $|\operatorname{orb}(p)| = 4$.

   (ii) $p = x_1x_2 + x_3 + x_4$: the permutations which send p to itself are id, $(1\ 2)$, $(3\ 4)$ and $(1\ 2)(3\ 4)$. Thus $|\operatorname{stab}(p)| = 4$.
   The orbit consists of all polynomials of the form $x_ix_j + x_k + x_l$ with i, j, k, l being the distinct numbers from 1 to 4. There are six of these, namely

$$x_1x_2 + x_3 + x_4, \quad x_1x_3 + x_2 + x_4, \quad x_1x_4 + x_2 + x_3,$$

$$x_2x_3 + x_1 + x_4, \quad x_2x_4 + x_1 + x_3, \quad x_3x_4 + x_1 + x_2.$$

Thus $|\operatorname{orb}(p)| = 6$.

2. $|\operatorname{orb}(1)| = 4$ because $\operatorname{orb}(1) = \{1, 2, 3, 4\}$; for each $i = 1, 2, 3, 4$, there is a permutation which sends 1 to i. As $|\operatorname{orb}(1)||\operatorname{stab}(1)| = |S_4| = 24$, $|\operatorname{stab}(1)| = 6$.

   By 8.3, $\alpha H = \operatorname{send}_1(2)$, the set of permutations which send 1 to 2. There are 6 of these, namely

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

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

3. (i) $|\operatorname{orb}(P)| = 12$, because P can be sent to any of the twelve points $(i, j) \in X$ with $i \neq j$. $|\operatorname{stab}(P)| = 2$, because any permutation which stabilizes P must send 1 to 1 and 2 to 2, and there are 2 such permutations, namely id and (3 4).

   (ii) $|\operatorname{orb}(P)| = 4$, because P can be sent to any of the four points $(i, i) \in X$. $|\operatorname{stab}(P)| = 6$, because the permutations which stabilize P are the six which send 1 to itself.

   (Note that having first found either $|\operatorname{orb}(P)|$ or $|\operatorname{stab}(P)|$, whichever you find easier, you can write down the other from the formula $|\operatorname{orb}(P)||\operatorname{stab}(P)| = 24$.)

4. (a) The stabilizer of the x-axis is $\{\operatorname{rot}_0, \operatorname{rot}_\pi, \operatorname{ref}_0, \operatorname{ref}_\pi\}$, that is, rotations through 0 and π and reflections in the two axes. This is Klein's 4-group.

   (b) By 8.3, the elements which send the x-axis to the y-axis are the elements of the left coset gH where $g = \operatorname{rot}_{\frac{\pi}{2}}$ and $H = \operatorname{stab}(x\text{−axis}) = \{\operatorname{rot}_0, \operatorname{rot}_\pi, \operatorname{ref}_0, \operatorname{ref}_\pi\}$. These are $\operatorname{rot}_{\frac{\pi}{2}} \operatorname{rot}_0 = \operatorname{rot}_{\frac{\pi}{2}}, \operatorname{rot}_{\frac{\pi}{2}} \operatorname{rot}_\pi = \operatorname{rot}_{\frac{3\pi}{2}}, \operatorname{rot}_{\frac{\pi}{2}} \operatorname{ref}_0 = \operatorname{ref}_{\frac{\pi}{2}}$ and $\operatorname{rot}_{\frac{\pi}{2}} \operatorname{ref}_\pi = \operatorname{ref}_{\frac{3\pi}{2}}$. (The 2 reflections are in the lines $y = x$ and $y = -x$.)

5. (a) $\operatorname{stab}(v)$ is the set of all 2×2 real matrices $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ with $\det A \neq 0$ and $A * v = Av = v$. Now

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} a + c \\ b + d \end{pmatrix},$$

and this is equal to $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ if and only if $c = 1 - a$ and $d = 1 - b$. Thus $\mathrm{stab}(v)$ is the set of those 2×2 real matrices A of the form $\begin{pmatrix} a & 1-a \\ b & 1-b \end{pmatrix}$ with $a - b = \det A \neq 0$, that is $\mathrm{stab}(v) = H$. Being a stabilizer, H must be a subgroup of G.

(b) If $w = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ then $\mathrm{stab}(w)$ is the set of all 2×2 real matrices $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ such that $\det A \neq 0$ and $A * w = Aw = w$. Now

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

and this is equal to $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ if and only if $c = 0$ and $d = 1$. Thus $\mathrm{stab}(w)$ is the set of those 2×2 real matrices A of the form $\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix}$ with $a = \det A \neq 0$.