Groups 1 - MT342P

Joseph J. Rotman *Advanced Modern Algebra (Part 1)*
David S. Dummit, Richard M. Foote *Abstract Algebra*

1 Homework

1. Recall that a group is a pair $(G, *)$ consisting of a set G and a binary operation on G, i.e. a map $*\colon G \times G \to G$. In the sequel we will also write gh or $g * h$ for $*(g, h)$. This is subject to the following axioms:

   (a) *Associativity:* $\forall x, y, z \in G : (xy)z = x(yz)$.

   (b) *Neutral element:* $\exists n \in G : \forall g \in G : ng = gn = g$. Such an element $n \in G$ is called a **neutral element**. It follows already from this that the neutral element is uniquely determined. We will denote it by n now.

   (c) *Inverse element:* $\forall g \in G \exists h_g \in G : gh_g = h_g g = n$. The element h_g is called the **inverse** of g and denoted by g^{-1}. It follows that the inverse of g is uniquely determined by g.

   In each of the following cases decide whether $(G_i, *_i)$ is a group: If $(G_i, *_i)$ is not a group, show that one of the axioms is violated. If $(G_i, *_i)$ is a group, you do not need to provide a proof. Only identify the neutral element and the inverses.

   (a) $G_a = 2^{\mathbb{N}}$, the **power set** of N, i.e. the set of all subsets of $\mathbb{N}$. For two subsets $A, B \subset \mathbb{N}$ we let

   $$*_a(A, B) = \{m \in \mathbb{N} \mid \text{either } m \in A \text{ or } m \in B\} = (A \setminus B) \cup (B \setminus A)$$

   Solution: This is a group. The neutral element is the empty set and the inverse of a set $A \subset \mathbb{N}$ is A itself.

   (b) $G_b = \mathbb{N}$ the set of natural numbers. $*_b(a, b) = \gcd(a, b)$, the greatest common divisor.
   Solution: This has no neutral element, because if $\gcd(n, b) = b$, then $b|n$, but this is impossible to hold for all $b \in \mathbb{N}$.

   (c) $G_c = \{f\colon \mathbb{R} \to \mathbb{R} \mid \forall w \in \mathbb{R} : f(x + w) = w + f(x)\}$, $*_c(f_1, f_2) = f_1 \circ f_2$, composition.
   Solution: The functions f in this set are determined by their value at 0, we must have $f(x) = x + f(0)$.
   This is a group. The neutral element is the function f with $f(x) = x$. The inverse of the function f is the function g with $g(x) = x - f(0)$.

   (d) $G_d = \mathrm{Hom}(\mathbb{R}^2, \mathbb{R}^2) = M(2 \times 2, \mathbb{R})$ the set of real (2×2)-matrices, $*_d(A, B) = AB - BA$, the commutator of A, B.
   Solution: This is not associative, has no neutral element and has no inverses.

2. A group homomorphism is a map $f\colon G \to Q$, G, Q groups, so that for all $g, g' \in G$ we have

$$f(g'g) = f(g')f(g) \ .$$

A group G is **abelian**, **commutative**, if for all $a, b \in G$ we have $ab = ba$.

On a group G consider the square

$$s\colon G \to G \quad , \quad s(g) = g^2 \ .$$

Prove that the group G is abelian if and only if its squaring map is a group homomorphism.

Solution: If $s\colon G \to G$ is a group homomorphism, then for two elements $a, b \in G$ we must have

$$abab = (ab)^2 = s(ab) = s(a)s(b) = a^2b^2 = aabb \ .$$

Cancelling a and b gives $ba = ab$.

3. A subgroup of a group $(G, *)$ is a subset $H \subset G$ so that $(H, *|_H)$ is a group. Here $*|_H$ denotes the restriction of the binary operation $*\colon G \times G \to G$ to H, i.e. the map

$$*|_H\colon H \times H \to G \quad , \quad (h, h') \mapsto hh' = h * h' \ .$$

This means that H is nonempty and for all $x, y \in H$ we must have $xy^{-1} \in H$.

A group G is **cyclic** if there is an element $g \in G$, called a **generator**, such that every element $h \in G$ is of the form $h = g^n$ for some $n \in \mathbb{Z}$.

Show that a subgroup H of a cyclic group $G =< g >$ is cyclic, i.e. $H =< g^k >$ for some $k \in \mathbb{N}$.

Hint: Choose a nontrivial element $g^l \in H$ with l minimal.

Solution: Let $l = \min\left\{\lambda \in \mathbb{N} \,\middle|\, 1 \neq g^\lambda \in H\right\}$. If $\mu \in \mathbb{N}$ is so that $g^\mu \in H$, then there are $a, b \in \mathbb{Z}$ so that

$$al + b\mu = \gcd(l, \mu) \ .$$

It follows that

$$g^{\gcd(l,\mu)} = g^{al+b\mu} = (g^l)^a(g^\mu)^b \in H \ .$$

But if $\mu \geq l$ and $l \not| \mu$ then $\gcd(l, \mu) < l$ contradicting the minimality of l. Hence $l|\mu$ and $g^\mu = (g^l)^k$ for some k.

4. Let $H \subset G$ and Q be groups. A group homomorphism $f\colon H \to Q$ **extends** to G if there is a group homomorphism $F\colon G \to Q$ so that $F(h) = f(h)$ for all $h \in H$. Then F is an **extension** of f and f is the **restriction** of F to H.

Does a group homomorphism $f\colon H \to Q$, $H \subset G$ a subgroup, always extend to a group homomorphism $F\colon G \to Q$? Either prove or provide a counterexample.

Solution: Let $G = \mathbb{Z}_4 = \{x^0 = 1, x, x^2, x^3\}$, $x^4 = 1$ and $Q = \mathbb{Z}_2 = \{1 = y^0, y\}$, $y^2 = 1$, be the cyclic groups with 4 respectively 2 elements. Let $H = \{1, x^2\} \subset \mathbb{Z}_4$ be the subgroup generated by the element of order 2. Let $f\colon H \to Q$ be the map with $f(1) = 1$, $f(x^2) = y$. Then f has no extension F because this extension would need to map x to an element $F(x) \in Q$ so that $F(x)^2 = y$. But this is impossible because there is no such element in Q.

5. The order of a group $(G, *)$ is the cardinality of the underlying set i.e. $|G|$.

   The order $|g|$ of an element $g \in G$ is the order of the subgroup generated by g, i.e.

$$\begin{aligned} |g| &= |\{g^n \mid n \in \mathbb{Z}\}| \in \mathbb{N} \cup \{\infty\} \\ &= \min\{n \in \mathbb{N} \mid g^n = 1\} \end{aligned}$$

   By $\mathbb{Z}_d$ we denote the group of remainders modulo $d \in \mathbb{N}$, i.e. $\mathbb{Z}_d = \{[0], [1], \ldots, [d-1]\}$ where $[k] = \{n \in \mathbb{Z} \mid d | n-k\}$, with group operation $[k] + [l] = [k+l]$.

   For each of the groups below, determine the number of its subgroups and their orders.

   (a) $G_a = \mathbb{Z}_9$

   Solution: Besides the trival cases $H = 1$ and $H = G_a$ this group has one subgroup of order 3, the group generated by [3].

   (b) $G_b = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

   Solution: This is a vector space over the field with 3 elements, and subgroups are (linear) subspaces. These can have dimension 0 and 3 in the trivial cases $H = 1$ and $H = G_b$ or dimension 1 or 2.

   Each one dimensional subspace is spanned by exactly two nonzero vectors, and there are $3^3 - 1 = 26$ such vectors. Hence there are 26/2=13 one dimensional subspaces, hence 13 subgroups of order 3.

   A two dimensional subspace is spanned by a pair of linearly independent vectors. There are $(3^3-1)(3^3-3)$ such pairs and $(3^2-1)(3^2-3)$ span the same subspace. Hence there are

$$\frac{(3^3-1)(3^3-3)}{(3^2-1)(3^2-3)} = 13$$

   such vector spaces, i.e. subgroups of order 9.

   (c) $G_c = Q_8$, the quaternion group

$$\begin{aligned} Q_8 &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SU}(2) \,\middle|\, a, b, c, d \in \{0, \pm 1, \pm i\} \right\} \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \right\} \\ &= \{1, -1, i, -i, j, -j, -k = ji, k = ij\} \end{aligned}$$

   Solution: There is only one element of order 2, -1, hence there is also only one order 2 subgroup.

   The elements $\pm i, \pm j, \pm k$ all generate subgroups of order 4. Any two of these generate the whole group and they all contain the element -1 of order two. Thus there are 3 subgroups of order 4.

6. By the **isomorphism theorem**, for a **surjective** group homomorphism $f \colon G \to Q$ we have an isomorphism

$$\overline{f} \colon G/\ker(f) \xrightarrow{g\ker(f) \mapsto f(g)} Q \ .$$

   Let G be a finite group and $K \lhd G$ so that $\gcd(|K|, |G/K|) = 1$. Show that $H = K$ if $H < G$ and $|H| = |K|$.

   Solution: Let $q \colon G \to G/K$ be the quotient homomoprhism. Then $q(H) < G/K$, hence

$$|q(H)| \,\Big|\, |G/K|$$

By the isomorphism theorem,

$$q(H) \cong H/(\ker(q)\,|_H)$$

hence

$$|q(H)| \,\Big|\, |H| = |K| \ .$$

It follows that $q(H) = 1_{G/K} = K$, hence $H = K$.

7. Recall that a subgroup $H < G$ of a group G is **normal** if $gHg^{-1} = \{ghg^{-1} \,|\, h \in H\} = H$ (equivalently $gH = Hg$) for all $g \in G$. We then write $H \lhd G$.

   Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in \mathbb{Z}_5^\times, b \in \mathbb{Z}_5 \right\} \subset \mathrm{GL}\left(\mathbb{Z}_5^2\right) \ .$$

   (a) Show that G is a subgroup.

   Hint: For a ring R we denote by $R^\times$ the set of elements with a multiplicative inverse. In particular, for a field k, $\mathbf{k}^\times = \mathbf{k} \setminus \{0\}$

   Solution: We compute

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x^{-1} & -x^{-1}y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ax^{-1} & -ax^{-1}y + b \\ 0 & 1 \end{pmatrix} \ .$$

   (b) Find $A, B \in G$ so that

$$G = \left\{ A^i B^j \,\middle|\, i, j \in \mathbb{Z} \right\} \ .$$

   Hint: First find $x \in \mathbb{Z}_5^\times$ so that $\mathbb{Z}_5^\times = \{1, x, x^2, x^3\}$.

   Solution: We can take $x = 2$. Let

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

   Then the powers of A are

$$A^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad A^1 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad A^2 = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad A^3 = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$$

   and

$$A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = A^0 \ .$$

   Also

$$B^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \ .$$

   Now given $a \in \mathbb{Z}_5^\times$, $b \in \mathbb{Z}_5$, we can solve

$$A^i B^j = \begin{pmatrix} 2^j & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2^j & 2^j k \\ 0 & 1 \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

   for i, j. If $a = 1 = 2^0, 2 = 2^1, 3 = 2^3, 4 = 2^2$ then $i = 0, 1, 3, 2$ respectively, and $k = b/2^i$. Note that these calculations are all in $\mathbb{Z}_5$.

(c) Find a non-trivial normal subgroup $N \lhd G$.

Hint: Determinant.

Solution: The determinant is a group homomorphism $\mathrm{GL}(\mathbb{Z}_5^2) \to \mathbb{Z}_5^\times$, hence so is its restriction to the subgruop $G < \mathrm{GL}(\mathbb{Z}_5^2)$. The kernel is

$$\ker\left(\det\colon G \to \mathbb{Z}_5^\times\right) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{Z}_5^\times, b \in \mathbb{Z}_5, a = 1 \right\} = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbb{Z}_5 \right\} \cong \mathbb{Z}_5 \ .$$

8. Show that a group G of order 10 must contain elements a, u of order 5 and 2 respectively, so that

$$G = \left\{ u^i a^j \;\middle|\; i = 0, 1 \ , \ j = 0, 1, 2, 3, 4 \right\}$$

and $au = ua^k$ for some $k = 1, 2, 3, 4$.

If $k = 1$, then the group is abelian. Show that k can not be 2 nor 3.

Hint: If $au = ua^k$ and $u^2 = 1$, compute $auu = ((au)u) = ua^?$. $k = -1 = 4$ is possible, but you need not show this here.

Solution: If all elements of G have order 2, then G is abelian. Since $|G| = 10 > 2$, there would then be two elements $g, h \in G$ of order two generating a subgroup of order 4, isomorphic to $V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$. But 4 does not divide $|G|$, and therefore no such subgroup exists. Thus there are elements of G not of order 2. Let $g \in G$, be such an element $g \neq 1$. Then $|g| = 5$ or 10

If $|g| = 10$, then $G = \langle g \rangle \cong \mathbb{Z}_5$. is cyclic. We can take $a = g^2$, $u = g^5$ and get $au = ua = ua^k$ with $k = 1$.

If $|g| = 5$, then let $v \in G \setminus \langle g \rangle$. By the cancellation rule, the elements

$$1, g, g^2, \ldots, g^4, v, vg, \ldots, vg^4 \tag{1.1}$$

are pairwise different. Since these are $10 = |G|$ in number, the element v^2 must be among them. Again by cancellation, we can not have $v^2 = vg^j$. Thus $v^2 = g^j$ for some $j = 0, 1, 2, 3, 4$. We distinguish two cases:

(a) $\underline{v^2 = g^j,\ j \neq 0}$: Since $\langle g \rangle = \langle g^j \rangle = \langle v^2 \rangle$ for all $j = 1, 2, 3, 4$, we have $G = \langle g, v \rangle = \langle g^j, v \rangle = \langle v \rangle \cong \mathbb{Z}_{10}$. We can take $a = v^2$, $u = v^5$ and get $au = ua = ua^k$ with $k = 1$ as before.

(b) $\underline{v^2 = 1}$: Since all elements of G are listed in (1.1), gv must be one of this list. By cancellation, we cannot have $gv = g^j$ because $v \notin \langle g \rangle$. Therefore we must have

$$gv = vg^k \quad \text{for some} \quad k = 1, 2, 3, 4 \ .$$

We can thus take $u = v$ and $a = g$.

If $gv = vg^k$, then

$$gvv = vg^k v = vvg^{(k^2)}$$

but $vv = 1$, hence

$$g = g^{(k^2)}$$

and $k^2 = 1 \mod 5$. Thus we can only have $k = 1$ or $k = 4 = -1$.

9. The **Heisenberg group** over a field $\mathbf{k}$ (or $\mathbf{k} = \mathbb{Z}$) is

$$H(\mathbf{k}) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbf{k} \right\}$$

(a) Show that $H(\mathbf{k})$ is a subgroup of $\mathrm{GL}(\mathbf{k}^3)$.

(b) Which matrices lie in the center of $H(\mathbf{k})$?

Solution:

$$(a,b,c)(x,y,z) = (a+x, y+az+b, c+z)$$
$$(x,y,z)(a,b,c) = (x+a, b+xc+y, z+c)$$

are equal if and only if

$$az = xc\ .$$

For fixed (a,b,c) this can therefore be so for all (x,y,z) if and only if $a = c = 0$. Thus

$$Z(H(\mathbf{k})) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbf{k} \right\} \cong \mathbf{k}\ .$$

(c) Show that the exponent of $H(\mathbf{k})$ is $p = \operatorname{char}\mathbf{k}$ if this is odd, 4 if this is 2 and ∞ if $\mathbf{k} = \mathbb{Z}$ or $\mathbf{k}$ has characteristic 0.

Hint: The **characteristic** $\operatorname{char}\mathbf{k}$ of a field $\mathbf{k}$ is the order of 1 in the additive group of the field, i.e.

$$\operatorname{char}\mathbf{k} = \min\left\{ n \in \mathbb{N} \;\middle|\; \underbrace{1+1+\cdots+1}_{n \text{ times}} = 0 \right\}$$

or 0 if this set is empty. The charcteristic of a field is always a prime or 0.

The **exponent** of a group is

$$\exp(G) = \min\left\{ n \in \mathbb{N} \;\middle|\; \forall x \in G : x^n = 1 \right\}$$

or ∞ if this set is empty.

Solution:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & nb + \binom{n}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}$$

is never 1 for $n \in \mathbb{N}$, $(a,b,c) \neq 0$,if $\operatorname{char}\mathbf{k} = 0$.

If $\operatorname{char}\mathbf{k} = p \neq 2$, then this vanishes if $p = n$ because then

$$p \Big| n \quad \text{and} \quad p \Big| \binom{n}{2} = \frac{n(n-1)}{2}\ .$$

If $\operatorname{char}\mathbf{k} = 2$ then $\binom{2p}{2} = 6 = 0 \mod 2$, hence the order of every element of $H(\mathbb{Z}_2)$ divides 4. Since

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

there is an element of order 4 in this group, the exponent must therefore be 4.

(d) Show that $H(\mathbf{k})$ is generated by two elements if $\mathbf{k} = \mathbb{Z}$ or $\mathbf{k} = \mathbb{Z}_p$, p a prime.

Solution:

$$\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}^i\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}^j\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}^k\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}^l=\begin{pmatrix}1&i&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&j\\0&0&1\end{pmatrix}\begin{pmatrix}1&k&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&l\\0&0&1\end{pmatrix}$$
$$=\begin{pmatrix}1&i&ij\\0&1&j\\0&0&1\end{pmatrix}\begin{pmatrix}1&k&kl\\0&1&l\\0&0&1\end{pmatrix}$$
$$=\begin{pmatrix}1&i+k&kl+il+ij\\0&1&j+l\\0&0&1\end{pmatrix}$$

Since every element of $H(\mathbf{k})$ can be written in this form, $H(\mathbf{k})$ is generated by

$$a=\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}\quad,\quad b=\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}\ .$$

(e) Find a presentation for $H(\mathbb{Z})$.

Solution: The element $z=\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}$ generates the center of $H(\mathbf{k})$ and

$$z=aba^{-1}b^{-1}=[ab]\ .$$

Then $H(\mathbb{Z})\cong\langle a,b,z\,|\,aba^{-1}b^{-1}=z,az=za,bz=zb\rangle$.

(f) $H(\mathbb{Z}_2)$ has $8=2^3$ elements, and is not abelian. By the classification of small groups, $H(\mathbb{Z}_2)$ must be isomorphic to Q_8 or D_8. Which is it?

Solution:

$$\langle a,b,z\,|\,a^2,b^2,z^2,aba^{-1}b^{-1}=z,az=za,bz=zb\rangle\cong\langle a,b,z\,|\,a^2,b^2,z^2,abab=z,az=za,bz=zb\rangle$$
$$\cong\langle a,b\,|\,a^2,b^2,(ab)^4,aabab=ababa,babab=ababb\rangle$$
$$\underset{ab=i}{\cong}\langle a,i\,|\,a^2,(a^{-1}i)^2,i^4,ai^2=i^2a,a^{-1}i^3=i^2a^{-1}i\rangle$$
$$\cong\langle a,i\,|\,a^2,(a^{-1}i)^2,i^4,ai^2=i^2a\rangle$$
$$\cong\langle a,i\,|\,a^2,ai=i^{-1}a,i^4,ai^2=i^2a\rangle$$
$$\cong\langle a,i\,|\,a^2,ai=i^{-1}a,i^4\rangle\cong D_8$$

10. Recall the **class equation**. If G is a finite group and $C(g)$ denotes the **centraliser** of $g\in G$, i.e.

$$C(g):=\{x\in G\,|\,xgx^{-1}=g\}$$

then there is a bijection

$$G/C(g)\xrightarrow{x\mapsto xgx^{-1}}g^G=\{xgx^{-1}\,|\,x\in G\}\ .$$

The **center** of a group G is

$$Z(G)=\{g\in G\,|\,\forall x\in G:gx=xg\}=\{g\in G\,|\,C(g)=G\}=\{g\in G\,|\,g^G=\{g\}\}$$

i.e. the set of those elements of G with trivial, one-element, singleton, conjugacy class. Let $S \subset G$ be a set containing exactly one element form each non-trival conjugacy class in G. Since G is the union of its conjugacy classes,

$$G = Z(G) \cup \bigcup_{s \in S} s^G \ ,$$

and counting gives the **class equation**

$$|G| = |Z(G)| + \sum_{s \in S} \left|s^G\right| = |Z(G)| + \sum_{s \in S} \frac{|G|}{|C(s)|} \ .$$

Since the center always contains 1, a group with one conjugacy class must be trivial.

If the finite group G has exactly two conjugacy classes, then these must be 1 and $G \setminus 1$. Hence $|G|-1$ divides $|G|$ which is only possible if $|G| = 2$, hence $G \cong \mathbb{Z}_2$.

Find all (isomorphism classes of) groups with exactly three conjugacy classes.

Solution: Let G be such a group. One of the three conjugacy classes must be the trivial group $1 < G$. Let $m \leq n$ be the orders of the other two conjugacy classes. By the class equation, we have that m, n divide $|G|$ and

$$|G| = 1 + m + n \ .$$

In particular, n divides $m + 1$. Since $m \leq n$ there are two cases:

(a) $\underline{n = 1:}$ Then $m = n = 1$ then this leads to $|G| = 3$, $G \cong \mathbb{Z}_3$, which has 3 conjugacy classes.

(b) $\underline{n = m + 1 > 1:}$ Thus m and n are coprime, hence

$$m(m+1) = mn | 1 + m + n = 2(m+1) \quad \Longrightarrow \quad m|2$$

If $m = 1$ then $n = 2$ and $|G| = 4$, hence $G \cong \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$, which are both abelian and have 4 conjugacy classes. If $m = 2$ then $n = 3$ and $|G| = 6$. An abelian group of order 6 has 6 conjugacy classes, so G must be non-abelian. Every non-abelian group of order 6 is isomorphic to S_3, which has 3 conjugacy classes, 1, {3-cycles}, {2-cycles}.

11. An **action** of a group G on a set M is a group homomorphism $\rho : G \to S_M$ from G to the group of permutations of M. We usually suppress ρ in the notation and write $gm := [\rho(g)](m)$. The G-orbit through $m \in M$ is the set $Gm = \{gm \,|\, g \in G\}$. The **isotropy group**, also **stabilizer (group)** of $m \in M$ is the subgroup

$$G_m := \{g \in G \,|\, gm = m\} < G \ .$$

By the **Orbit-Stabiliser Theorem** there are bijections

$$Gm \times G_m \leftrightarrow G \quad \text{and} \quad Gm \leftrightarrow G/G_m \ ,$$

in particular,

$$|G| = |Gm| \times |G_m| \quad , \quad |Gm| = |G/G_m| \ .$$

A **fixed point** of the G-action is a point $m \in M$ so that $gm = m$ for all $g \in G$. Let

$$\mathrm{Fix}_G(M) := \{m \in M \,|\, Gm = m\} \ .$$

Let G be a group of order 121 and M be a set with 130 elements. Show that every action of the group G on M has fixed points. What is the smallest possible number of fixed points?

Solution: By the orbit-stabilizer theorem, the size of each orbit must divide the order of the group. Thus, in this case, orbits can have one, 11, or 121 elements in an orbit. Since 130 is not a sum of multiples of 11 or 121, there must be orbits of lenght 1. There must be at least 9 fixed points.

12. List the center and the conjugacy classes of the nonabelian groups of order ≤ 8.

Solution:

$$\begin{aligned} &S_3 : 1,\ \{(12),(13),(23)\},\ \{(123),(132)\} \quad , \quad Z(S_3) = 1 \\ &D_8 : 1,\ i^2, \{i, i^3\},\ \{c, ci^2\},\ \{ci, ci^3\} \quad , \quad Z(D_8) = \{1, i^2\} \\ &Q_8 : 1,\ \{i^2\},\ \{ij, ji = ij^3\},\ \{i, ij^2\},\ \{j, i^2 j\} \quad , \quad Z(Q_8) = \{1, i^2\} \end{aligned}$$

13. Let M be a set and $G \xrightarrow{\rho} S_M$ be a group homomorphism, an **action of G on M**, or a **G-action on M**. We will write $gm := (\rho(g))(m)$ for $g \in G$, $m \in M$ in the sequel. The **stabilizer group**, or **isotropy group** of $m \in M$ is $G_m = \{g \in G \mid gm = m\}$. This is a subgroup of G, but need not be normal. The **orbit** of $m \in M$ is $Gm = \{gm \mid g \in G\}$. The action is called

(a) *transitive* if $\forall m, n \in M \exists g \in G : gm = n$. This is equivalent to all of M being an orbit of the action.

(b) *faithful* if ρ is injective. This is equivalent to

$$\forall m \in M : gm = g'm \quad \Longrightarrow \quad g = g' \quad (\text{for} \quad g, g' \in G)$$

For $m \in M$, the map $G \xrightarrow{g \mapsto gm} Gm$ is surjective and therefore (by the axiom of choice) it has a right inverse (a "split") $s \colon Gm \to G$, i.e. a map s so that

$$\forall g \in G : (s(gm))m = gm \ .$$

The **orbit stabilizer theorem** says that for every $m \in M$, the map

$$G \xrightarrow{g \mapsto (s(g)^{-1} g, gm)} G_m \times Gm$$

is a bijection. In fact, the inverse of this map is

$$G_m \times Gm \xrightarrow{(h, gm) \mapsto s(gx)h} G \ .$$

An immediate consequence of this is that

$$|G| = |G_m| \times |Gm| \ .$$

Let G act on a set M.

(a) Show that G acts faithfully if $\bigcap_{m \in M} G_m = 1$.

(b) There is an induced action of G on the set of 2-sets in M,

$$\binom{M}{2} = \{\{a, b\} \mid a, b \in M,\ a \neq b\}$$

given by

$$g\{a, b\} := \{ga, gb\} \ .$$

The action of G on M is called **2-transitive** if the induced action on $\binom{M}{2}$ is transitive. Is there any 2-transitive action of the quaternion group Q_8 on a set M with more than 2 elements?

Solution: No. If G acts transitively on $\binom{M}{2}$, then $\left|\binom{M}{2}\right| = \frac{|M|^2 - |M|}{2}$ must divide $|G|$. But $\frac{m^2 - m}{2} \Big| |Q_8| = 8$ only for $m = 2$

(c) Let G be a group of odd order, acting 2-transitively on a set M. Show that for any $a, b \in M$, $a \neq b$, we have

$$|G_a \cap G_b| = \frac{2\,|G|}{|M|^2 - |M|} \ .$$

Solution: Let $a, b \in M$, $a \neq b$. If $g \in G$ is in the stabiliser of the induces action of G on $\binom{M}{2}$ at $\{a, b\}$, then

$$g\,\{a, b\} = \{ga, gb\} = \{a, b\} \ ,$$

which leaves two cases

i. $\underline{ga = a, gb = b:}$ In this case $g \in G_a \cap G_b$

ii. $\underline{ga = b, gb = a:}$ Then $g^k a = b, g^k b = a$ for any odd k. But since $|G|$ is odd we may take $k = |G|$. However, since $g^{|G|} = 1$, a contradiction.

Thus $G_{\{a,b\}} = G_a \cap G_b$. By the orbit stabilizer theorem for the action of G on $\binom{M}{2}$,

$$|G| = \left|\binom{M}{2}\right| \times \left|G_{\{a,b\}}\right| = \frac{|M|^2 - |M|}{2}\,|G_a \cap G_b| \ .$$

14. Every group G acts on itself via **conjugation**. Thus there is a group homomorphism $c\colon G \to \mathrm{Aut}\,(G)$, $c(g)(x) = x^g := gxg^{-1}$. This action need not be faithful, nor transitive but is via automorphisms. This is not to be confused with the left regular representation, which is always transitive, faithful but almost never via automorphisms. The orbits of the conjugation-action are called **conjugacy classes** and the stabiliser groups **centralisers**. Thus the centraliser of $x \in G$ is $C(x) = \{g \in G \,\big|\, gxg^{-1} = x\}$, i.e. the subgroup of G consisting of all elements commuting with x.

(a) Clearly, for every $x \in G$, $\langle x\rangle < C(x)$, because for every $k \in \mathbb{Z}$, x^k commutes with x. Thus $|C(x)| \geq |x|$.
Let G be a finite group with "minimal centralisers", i.e. so that $|C(x)| = |x|$ for all $x \in G \setminus \{1\}$. Show that $|G|$ must be square-free, i.e.

$$|G| = p_1 \cdots p_r$$

with pairwise different primes, $p_1 < p_2 < \cdots < p_r$.
Solution: If the order of $x \in G$, $x \neq 1$ is not prime, then $\langle x\rangle$ contains elements of order smaller than that of x but with the same centraliser. Thus all elements of G must be of prime order. By the assumption the centralisers therefore also are of prime order. Assume now that

$$|G| = p^a m \quad , \quad p \nmid m \quad , \quad a > 1 \ .$$

Since $|C(x)| = |x|$ is prime,

$$p \,\Big|\, \frac{|G|}{|C(x)|} \quad \text{for all} \quad x \in G \setminus \{1\} \ .$$

Let S be a section for the conjugation, i.e. a subset of G containing exactly one element from each conjugacy class except 1. The class equation then gives

$$|G| = 1 + \sum_{x \in S} \frac{|G|}{|C(x)|} \equiv 1 \mod p \ ,$$

impossible.

(b) Check which of the groups up to order 10 have "minimal centralisers".

15. Find all group homomorphisms $f\colon Q_8 \to \mathbb{Z}_4$.

Solution: We work with the presentation

$$Q_8 = \langle i, j \,|\, i^2 = j^2, i^4, iji^{-1} = j^{-1} \rangle \tag{1.2}$$

By the last relation we must have

$$f(iji^{-1}) = f(i) + f(j) - f(i) = f(j) = f(j^{-1}) = -f(j) \ ,$$

which forces $f(j) = 0$ or 2. The last relation is equivalent to $iji^{-1}j^3 = j^2 = i^2$, hence $ji^{-1}j^{-1} = i$. Thus the same calculation as before, with i interchanged with j, gives $f(i) = 0$ or 2. Thus wem have the four homomorphisms $f_{a,b}$, $a, b = 0, 2$ given by

$$f_{a,b}(i^\alpha j^\beta) = a\alpha + b\beta \mod 4 \ .$$

16. Recall the classification theorem for finite abelian groups: For every finite abelian group G there are natural numbers $a_1, a_2, \ldots a_k$ so that $a_i | a_{i+1}$ for all $i = 1, \ldots, i-1$ and an isomorphism

$$G \cong \mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times \cdots \times \mathbb{Z}_{a_k}$$

The factors $\mathbb{Z}_{a_j}$ and also the numbers a_j are the **invariant factors** of G.

There also are prime powers $p_i^{a_i}$, so that

$$G \cong \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_r^{a_r}} \ .$$

The p_i here are primes but need not be pairwise different. The factors $\mathbb{Z}_{p_i^{a_i}}$ in this decomposition are the **elementary divisors** of the group G.

Make a list of products of cyclic groups, giving the decomposition in invariant factors and the elementary divisors for every abelian group of order 900.

Solution: $900 = 2^2 \times 3^2 \times 5^2$. Thus the abelian groups of order 900 are isomorphic to the following.

$$\begin{aligned}
\mathbb{Z}_{900} &\cong \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_{25} \\
\mathbb{Z}_2 \times \mathbb{Z}_{450} &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{25} \\
\mathbb{Z}_3 \times \mathbb{Z}_{300} &\cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \\
\mathbb{Z}_5 \times \mathbb{Z}_{180} &\cong \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
\mathbb{Z}_6 \times \mathbb{Z}_{150} &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \\
\mathbb{Z}_{10} \times \mathbb{Z}_{90} &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
\mathbb{Z}_{15} \times \mathbb{Z}_{60} &\cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
\mathbb{Z}_{30} \times \mathbb{Z}_{30} &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5
\end{aligned}$$

2 Topics for Review

1. Group Axioms, neutral element, inverse element.
2. Order of a group, order of an element of a group, cyclic groups

3. Subgroups, subgroup generated by a set, Cosets
   Lagrange's Theorem

4. Normal subgroups, quotient group, group homomorphisms
   Isomorphism Theorem

5. conjugacy classes, centraliser, center of a group,
   Class Equation

6. Groups of order ≤ 12

7. Symmetric groups, Computations in symmetric groups: cycle decompositions, transpositions, sign, order of elements, conjugacy classes in terms of cycle type

8. Abelian groups, Classification of finitely generated abelian groups, Torsion subgroup, Elementary factors, Invariant factors.

3 Some more problems

1. Write down a list of permutations on $\{1, 2, 3, 4, 5, 6, 7\}$ so that every conjugacy class contains exactly one element from your list. Write your permutations as product of disjoint cycles. Also find the order and the sign of each of your permutations, and say how many elements are in its conjugacy class

   Solution: Permutations are conjugate if the cycles in their disjoint cycle decomposition have the same lenghts. Thus Every element of S_7 is conjugate to one of

π	$\lvert\pi\rvert$	sgnπ
()	1	1
(12)	2	-1
(12)(34)	2	1
(12)(34)(56)	2	-1
(567)	3	1
(12)(567)	6	-1
(12)(34)(567)	6	1
(123)(567)	3	1
(1234)(56)	4	1
(1234)(567)	12	-1
(12345)(67)	10	-1
(123456)	6	-1
(1234567)	7	1

2. Let $\omega \in S_{12}$ be the permutation

$$\omega = \begin{pmatrix} 123456789abc \\ 2468ac31579b \end{pmatrix}$$

   where $a = 10, b = 11, c = 12$.

(a) Write ω as a product of disjoint cycles, as a product of (not necessarily disjoint) transpositions, and as a product of (not necessarily disjoint) 3-cycles, if possible.

Solution:

$$\begin{aligned}\omega &= (1248)(36cb95a7)\\ &= (12)(14)(18)(36)(3c)(3b)(39)(35)(3a)(37)\\ &= (124)(18)(83)(83)(36)(3cb)(395)(3a7)\\ &= (124)(183)(836)(3cb)(395)(3a7)\end{aligned}$$

(b) What is the order of ω?

Solution: $|\omega| = 8$, the least common multiple of the cycle length.

(c) How many elements of S_{12} are conjugate to ω? What is the order of the centraliser $C(\omega)$ of ω? Find a set of generators of $C(\omega)$.

Solution: A permutation is conjugate to ω if and only if it splits into disjoint cycles as ω does, i.e. one cycle of length 8 and a cycle disjoint from this of length 4. Thus we need to count the elements of cycle type $(8, 4)$. Choosing such a permutation first involves choosing 8 elements out of 12 giving $\binom{12}{8} = \binom{12}{4}$ possibilities. Fixing such a choice, for instance

$$(12345678)(9abc)$$

we need to count the different 8-cycles on the elments $\{12345678\}$ times the number of different 4-cycles on $\{9abc\}$. Now observe that there are 8! different ways to write 8-cycles on the elements $\{12345678\}$. However **cyclic** permutations of these digits give the same permuation, e.g.

$$(12345678) = (23456781) = \cdots = (81234567)\ .$$

This gives $\frac{8!}{8} = 7!$ different (as permutation) 8-cycles. Similarly, there are $\frac{4!}{4} = 3!$ different 4-cycles on a fixed set of 4 digits. Thus

$$\left|\omega^{S_{12}}\right| = \binom{12}{8} \times 7! \times 3! = \frac{12!}{4 \times 8}$$

By the orbit stabiliser theorem, the order of the centraliser is

$$|C(\omega)| = 4 \times 8$$

and the centraliser is generated by two elements,

$$C(\omega) = \langle (1248), (36cb95a7) \rangle$$

3. Recall that every permutation $\pi \in S_n$ on $\{1, 2, \ldots, n\}$ is a product of (not necessarily disjoint) transpositions. If the number of transpositions in such a product representing π is k, then we say the sign of π is $(-1)^k$. Show that

$$\mathrm{sgn}\pi = \prod_{0<i<j<n+1} \frac{\pi i - \pi j}{i - j}\ . \tag{3.1}$$

Solution: The product on the right hand of (3.1) is ± 1 because the numerators and the donominators exhaust all the differences $i - j$ of all the 2-sets $\{i, j\} \subset \{1, \ldots, n\}$, only possibly with the

wrong sign in the numerator. We show that the right hand side of (3.1) is multiplcative. To this end, let $\omega, \sigma \in S_n$. Then

$$\prod_{0<i<j<n+1} \frac{(\omega\sigma)i - (\omega\sigma)j}{i-j} = \prod_{0<i<j<n+1} \frac{(\omega\sigma)i - (\omega\sigma)j}{\sigma i - \sigma j} \quad \frac{\sigma i - \sigma j}{i-j}$$
$$= \prod_{0<k<l<n+1} \frac{\omega k - \omega l}{k-l} \prod_{0<i<j<n+1} \frac{\sigma i - \sigma j}{i-j} \ .$$

Clearly (3.1) holds for transpositions, and since both sides of (3.1) are multiplicative, (3.1) holds for all permutations. A consequence of this is that the parity (even or odd) of the number of transpositions in a product representing a permutaion $\pi \in S_n$ is determined by π.

4. Prove the

Theorem 3.2 (Correspondence Theorem) *Let G be a group and $N \lhd G$ be a normal subgroup. Then the map assigning to a subgroup H of G containing N the quotient H/N is a bijection*

$$\phi\colon \{H \mid G > H > N\} \xrightarrow{H \mapsto H/N} \{Q \mid G/N > Q\} \ .$$

Solution: The inverse map is given by taking the inverse image under the quotient map $\pi\colon G \to G/N$, i.e. $\pi(g) = gN$. Thus, for $Q < G/N$ we only need to check that

$$\pi^{-1}(Q) = \{g \in G \mid \pi g \in Q\}$$

is a subgroup of G containing N. To this end, let $Q < G/N$. Then

$$\pi^{-1}(Q) = \{g \in G \mid gN \in Q\}$$

is not empty. Since $N \lhd G$ we have $gN = Ng$ for all $g \in G$. If $x, y \in \pi^{-1}(Q)$, i.e. $xN, yN \in Q$ then

$$(xy^{-1})N = (xN)(y^{-1}N) = (xN)(yN)^{-1} \in Q$$

because $Q < G/N$.

5. If G is a group and $\phi \in \mathrm{Aut}\,(G)$ (an **automorphism of** G, i.e. an isomorphism $G \xrightarrow[\cong]{\phi} G$), then the fixed point set of ϕ,

$$\mathrm{Fix}\,(\phi) = \{x \in G \mid \phi(x) = x\} < G$$

is a subgroup of G.

(a) Find an example of a group G and a subgroup $H < G$ that is **not** the fixed group of some automorphism of G.

Solution: Let $H = 2\mathbb{Z} < \mathbb{Z} = G$. Since $\mathrm{Aut}\,(\mathbb{Z}) = \{\mathrm{id}, -\mathrm{id} : x \mapsto -x\}$, an automorphism fixing H must be id, but $\mathrm{Fix}\,(\mathrm{id}) = \mathbb{Z}$.

(b) Which subgroups of $G = \mathbb{Z} \times \mathbb{Z}$ are fixed groups of suitable automorphisms?

Solution: If $x \in G \setminus H$ and $\lambda x \in H$ for some $\lambda \in \mathbb{Z}$, then every automorphism of G fixing λx must also fix x. Thus a fixed group H must have the property that

$$\lambda x \in H \quad \Longrightarrow \quad x \in H \ .$$

Thus, besides the trivial cases $H = 0$ and $H = G$, the only fixed groups are of the form

$$H = \langle (a, b) \rangle \quad \text{with} \quad \gcd(a, b) = 1 \ .$$

(c) Is the fixed group of an automorphism necessarily a normal subgroup?

Solution: No. For a counterexample, consider the automorphism c of S_3 given by conjugation with (12). The fixed group of c is the centraliser of (12), i.e. the group generated by (12). This is not normal. For instance

$$(23)(12)(23) = (13) \notin \langle (12) \rangle \ .$$

6. Make a list of products of cyclic groups so that every abelian group of order 2024 is isomorphic to exactly one product in your list. Write each group in your list with as few factors as possible, and then with factors as small as possible.

Solution: Since

$$2024 = 2^3 \times 11 \times 23$$

there are 3 isomorphism typse of abelian groups of that order:

(a) $\mathbb{Z}_8 \times \mathbb{Z}_{11} \times \mathbb{Z}_{23} \cong \mathbb{Z}_{2024}$

(b) $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{11} \times \mathbb{Z}_{23} \cong \mathbb{Z}_2 \times \mathbb{Z}_{1012} \cong \mathbb{Z}_4 \times \mathbb{Z}_{506}$.

(c) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{11} \times \mathbb{Z}_{23} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{506}$

7. Define the dihedral group D_8 of order 8. Find all group homomorphisms $D_8 \to S_3$. How many are there?

Solution: A 3-cycle in S_3 can not be in the image of such a group homomorphism f, because the elements x of D_8 have order 1, 2 or 4, hence $f(x)$ cannot have order 3. Since S_3 is generated by any two transpositions, there can at most be one transposition in the image of f. Thus we are left with determining all group homomorphisms

$$f_{a,b} \colon D_8 = \left\langle i, c \,\middle|\, i^4, c^2, cic = i^{-1} \right\rangle \xrightarrow[c \mapsto b]{i \mapsto a} \mathbb{Z}_2$$

where $a, b \in \mathbb{Z}_2$ need to be so that

$$4a = 0, \ 2b = 0, \ 2b + a = -a \ .$$

Since this is true for any choice of a, b there are 10 group homomorphisms $D_8 \to S_3$, all of the form

$$f(z) = \tau^{f_{a,b}(z)} \quad \text{with} \quad \tau = (12), (13), (23) \quad \text{and} \quad a, b \in \mathbb{Z}_2 \ .$$

8. Let M be a set, $p \in M$, and let G be a group acting on M, so that the stabiliser G_p of p is a normal subgroup of G. Show that for all $g \in G$ we have

$$G_{gp} = G_p \ .$$

Solution: This is immediate from the definition of the stabiliser subgroup,

$$G_p = \{ g \in G \,|\, gp = p \} \ .$$

$$\begin{aligned} G_{gp} &= \{ x \in G \,|\, xgp = gp \} \\ &= \left\{ x \in G \,\middle|\, g^{-1}xgp = p \right\} \\ &= \left\{ gyg^{-1} \,\middle|\, y \in G, \ yp = p \right\} \\ &= gG_pg^{-1} \\ &= G_p \end{aligned}$$

if $G_p \lhd G$.

9. Find a group G as small as possible that contains two isomorphic subgroups $H < G > K$, $H \cong K$ but so that there is no automorphism of G mapping H to K.

   Solution: Such a group G cannot be cyclic, and it can also not be $\mathbb{Z}_2 \times \mathbb{Z}_2$, so G must have at least order 6. $G = \mathbb{Z}_2 \times \mathbb{Z}_4$, $H = \langle (1,0) \rangle$, $K = \langle (0,2) \rangle$. Both groups H, K have order two, hence $H \cong \mathbb{Z}_2 \cong K$. If $\phi \in \mathrm{Aut}\,(G)$ were so that $\phi(K) = H$, hence $\phi((0,2)) = (1,0)$, then $y = \phi(0,1)$ must be so that $2y = (1,0)$. But the group G has no such element y since for all $(\alpha, \beta) \in G$ we have $2(\alpha, \beta) = (0, *)$.

10. For all groups G of order ≤ 8 find $n(G) \in \mathbb{N}$ as small as possible and an injective group homomorphism $G \hookrightarrow S_{n(G)}$.

    Hint: Every group of order ≤ 8 is isomorphic to one of

$$1,\ \mathbb{Z}_2,\ \mathbb{Z}_3, \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_5,\ \mathbb{Z}_6,\ S_3,\ \mathbb{Z}_7, \mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ D_8,\ Q_8 \tag{3.3}$$

    Solution: (sketch, some cases) The cyclic groups of prime order p have $n(\mathbb{Z}_p) = p$, because we always must have $|G| \,\big|\, n(G)!$. The injective homomorphis in this case maps a generator of $\mathbb{Z}_p$ to a p-cycle,

$$\mathbb{Z}_p \xrightarrow{1 \mapsto (123\cdots p)} S_p$$

    and $n(\mathbb{Z}_p) = p$.

    The group $\mathbb{Z}_4$ cannot be mapped injectively to S_3 because S_3 has no element of order 4. Thus

$$\mathbb{Z}_4 \xrightarrow{1 \mapsto (1234)} S_4$$

    and $n(\mathbb{Z}_4) = 4$.

    The group $\mathbb{Z}_6$ cannot be mapped injectively to S_4, because S_4 has no element of order 6. However, S_5 has an element of order 6 and we can map

$$\mathbb{Z}_6 \xrightarrow{1 \mapsto (123)(45)} S_5$$

    hence $n(\mathbb{Z}_6) = 5$.

    Clearly $n(S_k) = S_k$ for all $k \in \mathbb{N}$.

    Since $8 = 2^3$, and the order of a permutation is the least common multiple of the cycle lengths in its disjoint cycle decomposition, no element of S_7 has order 8. An embedding as required is therefore

$$\mathbb{Z}_8 \xrightarrow{1 \mapsto (12345678)} S_8$$

    and $n(\mathbb{Z}_8) = 8$.

    Similarly

$$\mathbb{Z}_4 \times \mathbb{Z}_2 \xrightarrow{(i,j) \mapsto (1234)^i (56)^j} S_6$$

    $n(\mathbb{Z}_4 \times \mathbb{Z}_2) = 6$.

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \xrightarrow{(i,j,k) \mapsto (12)^i (34)^j (56)^k} S_6$$

    $n(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) = 6$.

    The dihedral group D_8 of order 8 cannot be injectively mapped to S_3, but

$$D_8 = \left\langle i, c \,\middle|\, i^4, c^2, cic = i^{-1} \right\rangle \xrightarrow{i \mapsto (1234), c \mapsto (24)} S_4$$

is an injective group homomorphism. Thus $n(D_8) = 4$.

The quaternion group Q_8 can not be mapped injectively to S_7. One way to see this is to show that there is no faithful action of Q_8 on a set of 7 elements. To this end, let $M = \{1, 2, 3, 4, 5, 6, 7\}$ and assume Q_8 acts faithfully on M. Since the divisors of $8 = |Q_8|$ are $1, 2, 4, 8$, the Q_8 orbits on the set M can have the lengths $1, 2, 4$ only. In particular, stabilisers are non-trivial. Since every non-trivial subgroup of Q_8 contains the center, every stabiliser thus contains the center. Thus the center acts trivially and the action is not faithful.

Thus there is no faithful action of Q_8 on 7 points, hence no injective group homomorphism $Q_8 \hookrightarrow S_7$. The smallest such homomorphism is therefore the left regular representation

$$Q_8 \longrightarrow S_8 = S_{\{1,i,j,k,\}}$$

and $n(Q_8) = 8$.

11. Determine the order of the automorphisms group of $\mathbb{Z}_4 \times \mathbb{Z}_4$.

    Hint: (2×2)-matrices. Reduce mod 2.

    Solution: Automorphisms of $\mathbb{Z}_4 \times \mathbb{Z}_4$ are (2×2)-matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in \mathbb{Z}_4$, with determinant 1 or $-1 = 3$. This is equivalent to the mod 2 reduction of the determinant being 1. Reduction mod 2 maps 16 to 1. Thus $|\mathrm{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_4)| = 16\,|\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)| = 16\,|\mathrm{GL}(\mathbb{Z}_2^2)| = 16 \times 6 = 96$.

4 Some problems using notions not in this course

1. Let $\mathcal{C}$ be the simplicial complex on $X = \{1, 2, 3, 4, 5, 6, 7\}$, so that the set of maximal simplices in $\mathcal{C}$ is

$$\mathcal{C}_{\max} = \{\{1, 2, 3\}, \{2, 3, 4\}, \{3, 4, 5\}, \{4, 5, 6\}, \{5, 6, 7\}, \{6, 7, 1\}, \{7, 1, 2\}\} \ .$$

   (a) Find a set of generators of the automorphim group $\mathrm{Aut}(\mathcal{C}) < S_7$.

   Solution: $z = (1234567) \in \mathrm{Aut}(\mathcal{C})$ and the cyclic group $\mathbb{Z}_7 \cong \langle z \rangle < S_7$ generated by z acts transitively on X. It follows that $\mathrm{Aut}(\mathcal{C})$ is generated by z and any set of generators of the stabiliser $\mathrm{Aut}(\mathcal{C})_1$ of 1.

   In order to determine the stabiliser $\mathrm{Aut}(\mathcal{C})_1$, assume $\pi \in \mathrm{Aut}(\mathcal{C})$, $\pi(1) = 1$. Then π must permute the simplices containing 1, i.e. the sets

$$\{6, 7, 1\}, \{7, 1, 2\}, \{1, 2, 3\} \ .$$

   Since 3 and 6 are the only vertices contained in exactly one of these, there are two cases:

   i. $\underline{\pi(3) = 3}$*:* Then $\pi = \mathrm{id}$
   ii. $\underline{\pi(3) = 6}$*:* Then $\pi(i) = 9 - i$, i.e. $\pi = (27)(36)(45) =: u$

   Thus $\mathrm{Aut}(\mathcal{C}) = \langle z, u \rangle = \langle (1234567), (27)(36)(45) \rangle$.

   (b) Is $\mathrm{Aut}(\mathcal{C})$ abelian? Determine the order of $\mathrm{Aut}(\mathcal{C})$.

   Solution: This group is not abelian, but since

$$uzu^{-1} = uzu = (27)(36)(45)(1234567)(27)(36)(45) = (1765432) = z^{-1}$$

every element is of the form $u^k z^l$, $k, l \in \mathbb{Z}$. Thus

$$\mathrm{Aut}\,(\mathcal{C}) = \left\{ u^k z^l \,\middle|\, k = 0, 1 \ , l = 0, 1, 2, 3, 4, 5, 6 \right\} \cong D_{14} \ .$$

In particular $|\mathrm{Aut}\,(\mathcal{C})| = 14$.