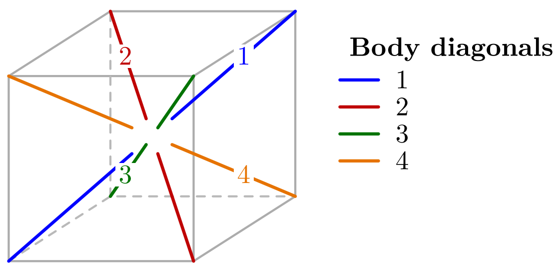
MAT205 Assignment 1 Solution Manual

Problem 1. The Rotation Group of a Cube

Problem.

Let G be the group of orientation-preserving rotations of a cube.



the four body diagonals

a. The cube has four body diagonals, labeled $1, 2, 3, 4$ in the figure. Show that every rotation of the cube permutes these four diagonals. Hence define a homomorphism

$$\varphi : G \to S_4.$$

b. Prove that φ is injective.

c. Prove that φ is surjective by showing that every transposition $(ij) \in S_4$ lies in $\operatorname{im} \varphi$.

Hint: put the cube at the vertices $(\pm 1, \pm 1, \pm 1)$, and label the body diagonals by

$$D_1 = \{\pm(1,1,1)\}, \quad D_2 = \{\pm(-1,1,1)\}, \quad D_3 = \{\pm(-1,-1,1)\}, \quad D_4 = \{\pm(1,-1,1)\}.$$

Use half-turns around axes through the midpoints of suitable pairs of opposite edges.

Conclude that

$$G \cong S_4.$$

d. Use Sylow theory to determine the possible values of n_3 and n_2, the numbers of Sylow 3- and Sylow 2-subgroups of G. Then use the geometry of the cube, or the identification $G \cong S_4$, to determine the actual values of n_3 and n_2.

e. Explain geometrically what one Sylow 3-subgroup represents. Explain geometrically what one Sylow 2-subgroup represents.

f. Put the cube at the vertices $(\pm 1, \pm 1, \pm 1)$, and consider the four vertices

$$T = \{(1,1,1),\ (-1,-1,1),\ (-1,1,-1),\ (1,-1,-1)\}.$$

Show that T is a regular tetrahedron inscribed in the cube. Let

$$K = \{g \in G : g(T) = T\}.$$

Prove that, under the isomorphism $G \cong S_4$, the subgroup K corresponds to A_4.

Now let $V = \mathbb{R}^3$, with the cube centered at the origin, and define

$$V^K = \{v \in V : k(v) = v \text{ for every } k \in K\}.$$

Compute V^K. In your answer, distinguish between preserving the tetrahedron T setwise and fixing vectors in V pointwise.

g. Let $V_4 = \{1, (12)(34), (13)(24), (14)(23)\} \leq S_4$. Use the chain

$$1 \triangleleft C_2 \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$$

to find the composition factors of G.

h. Decide whether G is solvable. Decide whether G is nilpotent. Justify both answers using the criteria from the lectures.

Solution.

a. A rotation sends vertices of the cube to vertices of the cube, and it sends opposite vertices to opposite vertices. Therefore it sends each body diagonal to another body diagonal. Thus each $g \in G$ gives a permutation of the set $\{1, 2, 3, 4\}$ of body diagonals.

Define

$$\varphi(g) = \text{the permutation of the four body diagonals induced by } g.$$

If $g, h \in G$, then the rotation gh acts on the diagonals by first applying h and then applying g. Hence

$$\varphi(gh) = \varphi(g)\varphi(h),$$

so $\varphi : G \to S_4$ is a group homomorphism.

b. Suppose $g \in \ker\varphi$. Then g fixes each of the four body diagonals as a set. A nonidentity rotation of a cube has one of three axis types: opposite faces, opposite vertices, or opposite edges. A face-axis rotation moves all four body diagonals; a vertex-axis rotation fixes one body diagonal and cycles the other three; an edge-axis half-turn swaps the body diagonals in pairs. Hence no nonidentity rotation fixes all four body diagonals. Therefore g is the identity rotation, so $\ker\varphi = 1$ and φ is injective.

c. We prove surjectivity directly by putting all transpositions in the image.

Put the cube at the vertices $(\pm1, \pm1, \pm1)$. Let

$$v_1 = (1, 1, 1), \quad v_2 = (-1, 1, 1), \quad v_3 = (-1, -1, 1), \quad v_4 = (1, -1, 1),$$

so the four body diagonals are $D_i = \{\pm v_i\}$.

For a nonzero vector u, the half-turn around the axis $\mathbb{R}u$ is

$$R_u(w) = 2\frac{w \cdot u}{u \cdot u}u - w.$$

This is orientation-preserving: it fixes the line $\mathbb{R}u$ and acts as -1 on the perpendicular plane $u^\perp$, so its eigenvalues are $1, -1, -1$ and its determinant is 1. For the six choices of u below, the line $\mathbb{R}u$ passes through the midpoints of a pair of opposite edges of the cube, so R_u is a rotation of the cube. Now compute its effect on the four chosen representatives v_1, v_2, v_3, v_4:

u	$R_u(x, y, z)$	$(R_u(v_1), R_u(v_2), R_u(v_3), R_u(v_4))$
$(0, 1, 1)$	$(-x, z, y)$	$(v_2, v_1, -v_3, -v_4)$
$(1, 1, 0)$	$(y, x, -z)$	$(-v_3, -v_2, -v_1, -v_4)$
$(1, 0, 1)$	$(z, -y, x)$	$(v_4, -v_2, -v_3, v_1)$
$(1, 0, -1)$	$(-z, -y, -x)$	$(-v_1, v_3, v_2, -v_4)$
$(1, -1, 0)$	$(-y, -x, -z)$	$(-v_1, -v_4, -v_3, -v_2)$
$(0, 1, -1)$	$(-x, -z, -y)$	$(-v_1, -v_2, v_4, v_3)$

Since $D_i = \{\pm v_i\}$, a minus sign does not change the diagonal. Therefore these six rotations induce

$$(12), \quad (13), \quad (14), \quad (23), \quad (24), \quad (34),$$

respectively, on the set $\{D_1, D_2, D_3, D_4\}$. Thus every transposition of the four body diagonals belongs to $\operatorname{im}\varphi$.

The transpositions generate S_4, so φ is surjective. Together with injectivity from part (b), φ is an isomorphism. Hence

$$G \cong S_4.$$

d. Since $G \cong S_4$, we have $|G| = |S_4| = 24 = 2^3 \cdot 3$. Sylow's theorems give

$$n_3 \mid 8, \qquad n_3 \equiv 1 \pmod{3}.$$

Thus

$$n_3 = 1 \text{ or } 4.$$

Also

$$n_2 \mid 3, \qquad n_2 \equiv 1 \pmod{2},$$

so

$$n_2 = 1 \text{ or } 3.$$

In S_4, a Sylow 3-subgroup is generated by a 3-cycle. There are 8 different 3-cycles, and each subgroup of order 3 contains two nonidentity 3-cycles. Hence

$$n_3 = \frac{8}{2} = 4.$$

A Sylow 2-subgroup has order 8. In the cube, choosing a pair of opposite faces gives the rotations preserving the axis through their centers. These form a subgroup isomorphic to D_4 of order 8. There are 3 pairs of opposite faces, hence

$$n_2 = 3.$$

e. A Sylow 3-subgroup is generated by a $120°$ rotation around a body diagonal. Geometrically, it is the rotational symmetry group around a vertex-opposite-vertex axis.

A Sylow 2-subgroup is the order-8 rotation subgroup preserving a chosen pair of opposite faces. It acts on one of those square faces as the symmetry group generated by quarter-turns and half-turns, and is isomorphic to D_4 in the convention $|D_4| = 8$.

f. The six distances between distinct vertices of T are all equal: for example,

$$\|(1,1,1) - (-1,-1,1)\| = \|(1,1,1) - (-1,1,-1)\| = \|(1,1,1) - (1,-1,-1)\| = 2\sqrt{2},$$

and the same calculation holds for the other pairs. Thus T is a regular tetrahedron inscribed in the cube.

The cube vertices split into two complementary tetrahedra:

$$T = \{(x,y,z) : xyz = 1\}, \qquad T' = \{(x,y,z) : xyz = -1\}.$$

A cube rotation permutes the four body diagonals. Each body diagonal contains exactly one vertex of T and one vertex of T'. Hence a rotation preserving T induces a permutation of the four vertices of T.

The orientation-preserving rotation group of a regular tetrahedron acts on its four vertices as A_4. Therefore the subgroup

$$K = \{g \in G : g(T) = T\}$$

is the tetrahedral rotation subgroup and corresponds to A_4 under $G \cong S_4$. Equivalently, the odd permutations in S_4 swap the two complementary tetrahedra T and T', while the even permutations preserve each one.

Now compute V^K. The subgroup $K \cong A_4$ contains the normal Klein four subgroup

$$V_4 = \{1, (12)(34), (13)(24), (14)(23)\},$$

which geometrically is the identity together with the three $180°$ rotations around the three face axes. Their fixed axes are the three coordinate axes, and the intersection of those three axes is $\{0\}$. Hence

$$V^K \subseteq V^{V_4} = \{0\}.$$

So

$$V^K = \{0\}.$$

This is the important distinction: K preserves the tetrahedron T setwise, but it fixes no nonzero vector in $\mathbb{R}^3$ pointwise.

The four vertices

$$(1,1,1), \quad (-1,-1,1), \quad (-1,1,-1), \quad (1,-1,-1)$$

are therefore the geometric source of the subgroup A_4 appearing in the composition series below.

g. Under $G \cong S_4$, use

$$1 \lhd C_2 \lhd V_4 \lhd A_4 \lhd S_4.$$

The successive quotients are

$$C_2/1 \cong \mathbb{Z}_2, \qquad V_4/C_2 \cong \mathbb{Z}_2, \qquad A_4/V_4 \cong \mathbb{Z}_3, \qquad S_4/A_4 \cong \mathbb{Z}_2.$$

All four factors are simple. Therefore the composition factors of G are

$$\mathbb{Z}_2, \quad \mathbb{Z}_2, \quad \mathbb{Z}_3, \quad \mathbb{Z}_2.$$

h. The group G is solvable because it has a subnormal series whose factors are abelian, namely the chain in part (g).

The group G is not nilpotent. For a finite group, nilpotent is equivalent to every Sylow subgroup being normal. But $n_3 = 4$, so the Sylow 3-subgroups are not unique and therefore not normal.

Problem 2. Automorphisms of Finite Abelian Groups

Problem.

Let p be a prime. The first nontrivial example is

$$A = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_p.$$

Write $A = \langle e_1 \rangle \oplus \langle e_2 \rangle$, where $|e_1| = p^2$ and $|e_2| = p$.

$$\begin{tikzcd}
A \arrow[r, dashed, "\text{quotient}"] \arrow[d] & A/pA \cong \mathbb{Z}_p^2 \\
A[p] = \{a \in A : pa = 0\} \cong \mathbb{Z}_p^2 \arrow[d] & \\
pA \cong \mathbb{Z}_p \arrow[d] & \\
0 &
\end{tikzcd}$$

a. Compute pA, $A[p]$, and A/pA explicitly in terms of e_1, e_2.

b. Prove that pA and $A[p]$ are characteristic subgroups of A. Explain why every automorphism of A must preserve the filtration

$$0 \subset pA \subset A[p] \subset A.$$

c. Show that every endomorphism $f : A \to A$ has the form

$$f(e_1) = ae_1 + be_2, \qquad f(e_2) = pce_1 + de_2,$$

where $a \in \mathbb{Z}/p^2\mathbb{Z}$ and $b, c, d \in \mathbb{F}_p$.

d. Prove that f is an automorphism if and only if

$$a \in (\mathbb{Z}/p^2\mathbb{Z})^\times, \qquad d \in \mathbb{F}_p^\times.$$

e. Deduce that

$$|\operatorname{Aut}(A)| = p^3(p-1)^2.$$

f. Now let

$$B = \mathbb{Z}_{p^{\lambda_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\lambda_r}}, \qquad \lambda_1 \geq \cdots \geq \lambda_r.$$

Explain why every subgroup $p^k B$ is characteristic. State the general principle suggested by parts (a)–(e): an automorphism of a finite abelian p-group is an invertible endomorphism whose matrix entries respect the p-power filtration.

g. Finally let M be any finite abelian group with primary decomposition

$$M = \bigoplus_p M_p, \qquad M_p = \{m \in M : p^k m = 0 \text{ for some } k \geq 1\}.$$

Prove that each M_p is characteristic and conclude that

$$\operatorname{Aut}(M) \cong \prod_p \operatorname{Aut}(M_p).$$

Solution.

a. Since e_1 has order p^2 and e_2 has order p,

$$pA = \langle pe_1 \rangle \cong \mathbb{Z}_p.$$

The elements killed by p are precisely

$$A[p] = \langle pe_1, e_2 \rangle \cong \mathbb{Z}_p \oplus \mathbb{Z}_p.$$

Also

$$A/pA \cong \langle e_1 + pA \rangle \oplus \langle e_2 + pA \rangle \cong \mathbb{Z}_p \oplus \mathbb{Z}_p.$$

b. The subgroup pA is the image of the intrinsic map

$$A \to A, \qquad x \mapsto px.$$

If $\alpha \in \operatorname{Aut}(A)$, then

$$\alpha(px) = p\alpha(x),$$

so $\alpha(pA) = pA$. Thus pA is characteristic.

The subgroup $A[p]$ is the kernel of the same map $x \mapsto px$. If $x \in A[p]$, then

$$p\alpha(x) = \alpha(px) = \alpha(0) = 0,$$

so $\alpha(x) \in A[p]$. Since α is bijective, $\alpha(A[p]) = A[p]$. Thus $A[p]$ is characteristic.

Therefore every automorphism preserves

$$0 \subset pA \subset A[p] \subset A.$$

c. The image of e_1 can be any element of A, so it has the form

$$f(e_1) = ae_1 + be_2$$

with $a \in \mathbb{Z}/p^2\mathbb{Z}$ and $b \in \mathbb{F}_p$.

The image of e_2 must have order dividing p, because $pe_2 = 0$. Therefore $f(e_2) \in A[p] = \langle pe_1, e_2 \rangle$, so

$$f(e_2) = pce_1 + de_2$$

with $c, d \in \mathbb{F}_p$.

Thus, using columns for the images of e_1, e_2, the corresponding matrix has the form

$$\begin{pmatrix} a & pc \\ b & d \end{pmatrix}.$$

d. The induced map on A/pA has basis $e_1 + pA, e_2 + pA$ and matrix

$$\begin{pmatrix} \bar{a} & 0 \\ b & d \end{pmatrix}$$

over $\mathbb{F}_p$, where $\bar{a}$ is the reduction of a modulo p. If f is an automorphism, this induced map must be invertible. Hence $\bar{a} \neq 0$ and $d \neq 0$, which means

$$a \in (\mathbb{Z}/p^2\mathbb{Z})^\times, \qquad d \in \mathbb{F}_p^\times.$$

Conversely, suppose a is a unit modulo p^2 and $d \neq 0$. If $f(x) = 0$, write

$$x = ue_1 + ve_2.$$

Reducing $f(x) = 0$ modulo pA gives

$$\bar{a}\,\bar{u} = 0, \qquad b\bar{u} + dv = 0$$

in $\mathbb{F}_p$. Since $\bar{a} \neq 0$ and $d \neq 0$, we get $\bar{u} = 0$ and $v = 0$. Thus $u = pu'$ for some $u' \in \mathbb{F}_p$, so $x = u'pe_1$ lies in pA.

On pA, the map sends

$$pe_1 \mapsto pf(e_1) = p(ae_1 + be_2) = a\,pe_1.$$

Since a is a unit modulo p, this is an automorphism of pA. Hence $x = 0$. So f is injective, and because A is finite, f is an automorphism.

Thus

$$f \in \operatorname{Aut}(A) \iff a \in (\mathbb{Z}/p^2\mathbb{Z})^\times, \quad d \in \mathbb{F}_p^\times.$$

e. There are

$$|(\mathbb{Z}/p^2\mathbb{Z})^\times| = p^2 - p = p(p-1)$$

choices for a, p choices for b, p choices for c, and $p-1$ choices for d. Therefore

$$|\operatorname{Aut}(A)| = p(p-1) \cdot p \cdot p \cdot (p-1) = p^3(p-1)^2.$$

f. For any $k \geq 0$, the subgroup p^kB is the image of the intrinsic endomorphism

$$B \to B, \qquad x \mapsto p^kx.$$

Every automorphism commutes with multiplication by p^k, so it preserves the image p^kB. Hence p^kB is characteristic.

The principle is: a finite abelian p-group carries a natural p-power filtration

$$B \supset pB \supset p^2 B \supset \cdots ,$$

and automorphisms must preserve this filtration. In a basis adapted to the cyclic summands, an endomorphism is represented by a matrix whose entries satisfy divisibility conditions forced by the orders of the generators. It is an automorphism exactly when the induced maps on the relevant finite layers are invertible.

g. For each prime p,

$$M_p = \{m \in M : p^k m = 0 \text{ for some } k \geq 1\}$$

is defined intrinsically from the group structure. If $\alpha \in \mathrm{Aut}(M)$ and $m \in M_p$, then $p^k m = 0$ for some k, so

$$p^k \alpha(m) = \alpha(p^k m) = 0.$$

Thus $\alpha(m) \in M_p$. Since α is bijective, $\alpha(M_p) = M_p$. Therefore each M_p is characteristic.

Because every automorphism preserves each primary component, restriction gives a homomorphism

$$\mathrm{Aut}(M) \to \prod_p \mathrm{Aut}(M_p).$$

It is injective because an automorphism of $M = \bigoplus_p M_p$ is determined by its restrictions to the direct summands. It is surjective because any tuple of automorphisms $\alpha_p \in \mathrm{Aut}(M_p)$ defines an automorphism of M by acting as α_p on the p-primary component. Hence

$$\mathrm{Aut}(M) \cong \prod_p \mathrm{Aut}(M_p).$$