KTH Teknikvetenskap

SF2729 Groups and Rings
Suggested solutions to midterm exam
Tuesday, March 15, 2011

---

(1) a) Show that there are exactly two non-isomorphic group structures on a set of four elements directly from basic properties of groups. **(2)**

b) Draw the Cayley digraph of the symmetric group S_3 using the generators $(1\,2\,3)$ and $(2\,3)$. **(2)**

c) The group of upper-triangular invertible matrices of the field $\mathbb{Z}_3$ with three elements has order 12 as well as the dihedral group D_6 given by the symmetries of a regular hexagon. Show that they are isomorphic. (Recall that the field $\mathbb{Z}_3$ can be seen as the integers modulo 3, i.e., with the usual addition and multiplication of residue classes.) **(2)**

SOLUTION

a). Assume that G is a group of order 4. Let a be a non-unit of G. Then G is cyclic if a has order 4 and there is only one cyclic group of order four up to isomorphic.

By Lagrange's theorem, we know that the order of a has to be a divisor of 4, but we can also exclude the possibility of $a^3 = e$ in the following more elementary way. If $a^3 = e$, we have that a generates a cyclic subgroup of order 3 leaving just one element outside. This is impossible, since the 3×3- subtable of the group table given by the subgroup already contains the elements of the subgroup in each row and each column, forcing the fourth element to be in the last column all the time, violating the condition that each element occurs only once in each row and column.

If $a^2 = e$, we have to have that $ab = c = ba$, if the other two non-units are b and c, since a is not a unit and we cannot have $ab = e$ or $ab = a$, since there is a unique inverse to a and since b is not a unit. Now we can fill in all the other entries of the group table using the property that each element occurs exactly once in each row and column.

b). Let $a = (1\,2\,3)$ and $b = (2\,3)$. We can write all the elements as in S_3 as $a^{e_2}b^{e_1}$, where the exponents satisfy $0 \leq e_1 \leq 1$ and $0 \leq e_2 \leq 2$. ($a^0b^0 = Id$, $a^1b^0 = (1\,2,\,3)$, $a^2b^0 = (1\,3\,2)$, $a^0b^1 = (2\,3)$, $a^1b^1 = (1\,2)$, $a^2b^1 = (1\,3)$) The Cayley digraph will be two directed cycles of length three corresponding to multiplication by a joined by double arrows corresponding to multiplication by b.

The digraph can be seen as

$$\begin{array}{ccccccc} a^0 & \longrightarrow & a^1 & \longrightarrow & a^2 & \longrightarrow & a^3 = e \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ a^0 b & \longleftarrow & a^1 b & \longleftarrow & a^2 b & \longleftarrow & a^3 b = e \end{array}$$

where the left and right ends are to be identified. Horisontal arrows correspond to multiplication by a and vertical arrows to multiplication by b, where we use that $ba = a^{-1}b$.

c). We need to find a matrix of multiplicative order 6, which we can do by seeing that it should be a matrix which is not diagonalizable and with eigenvalues of order 2, i.e., $2 = -1$. Hence we have two choices

$$r = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \quad \text{or} \quad r = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}.$$

Now the rotations of the hexagon should correspond to powers of r and the reflections to the remaining 6 matrices, which we can get from the powers of r by multiplying by one matrix of determinant 2.

Now, we can check that we get all 12 invertible matrices as

$$\begin{aligned} r^0 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & r^1 &= \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}, & r^2 &= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \\ r^3 &= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, & r^4 &= \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, & r^5 &= \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \end{aligned}$$

and

$$\begin{aligned} sr^0 &= \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, & sr^1 &= \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}, & sr^2 &= \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \\ sr^3 &= \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, & sr^4 &= \begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix}, & sr^5 &= \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}, \end{aligned}$$

where we have used

$$s = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

---

(2) Let $G = \mathrm{Sl}_2(\mathbb{Z})$ be the group of integer matrices of size 2×2 with determinant one.

a) Show that G acts on $\mathbb{Z}^2$ seen as 1×2-matrices by matrix multiplication by the inverse on the right, i.e., by $A.\begin{pmatrix} m & n \end{pmatrix} = \begin{pmatrix} m & n \end{pmatrix} A^{-1}$. **(2)**

b) Determine the stabilizer[1], G_x, where $x = \begin{pmatrix} 1 & 2 \end{pmatrix}$. **(4)**

---

[1] called *isotropy subgroup* in the text-book.

SOLUTION

a). We have that the inverse of an integer matrix of determinant one is again an integer matrix since the inverse equals the adjoint matrix in this case. Hence $\begin{pmatrix} m & n \end{pmatrix} A^{-1}$ is an integer vector.

We now check that $e = \mathrm{I}_2$ acts trivially since

$$\begin{pmatrix} m & n \end{pmatrix} I_2^{-1} = \begin{pmatrix} m & n \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} m & n \end{pmatrix}$$

for all $(m, n) \in \mathbb{Z}^2$.

For two matrices $A, B \in G$ we have that $(AB)^{-1} = B^{-1}A^{-1}$ which gives us that for an integer vector $\mathbf{x} = (m, n) \in \mathbb{Z}^2$, we get

$$(AB).\mathbf{x} = \mathbf{x}(AB)^{-1} = \mathbf{x}B^{-1}A^{-1} = (\mathbf{x}B^{-1})A^{-1} = A.(B.\mathbf{x}).$$

b). The stabilizer of $(1, 2)$ is given by the matrices with determinant one such that

$$(1, 2)A^{-1} = (1, 2)$$

Since this means that $(1, 2)$ is a left eigenvector of eigenvalue 1, we get that the other eigenvalue must be 1 as well as the product of the eigenvalues equals the determinant. Hence the characteristic equation is $\lambda^2 - 2\lambda + 1 = 0$ and we get that the trace equals 2. Such matrices can be written as $A^{-1} = I + N$, where N is a nilpotent matrix such that $(1, 2)$ is in the left kernel. This means that

$$N = \begin{pmatrix} 2a & 2b \\ -a & -b \end{pmatrix}$$

and $2a - b = 0$, i.e.,

$$A^{-1} = I + a \begin{pmatrix} 2 & 4 \\ -1 & -2 \end{pmatrix}$$

and

$$A = I - a \begin{pmatrix} 2 & 4 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} 1 - 2a & -4a \\ a & 1 + 2a \end{pmatrix}$$

for any integer a.

---

(3) a) Let H be a normal subgroup of a group G. Give the definition of the factor group G/H and prove that this is a well-defined group. **(2)**

b) Let G be the group given by the generators a and b with the relations $a^3 = e$, $b^3 = e$ and $abab = e$, i.e., the factor group of the free group $F[a, b]$ by the smallest normal subgroup containing $\{a^3, b^3, abab\}$. Show that G is isomorphic to the alternating group A_4. **(4)**

SOLUTION

a). The factor group G/H is defined in the following way when $H \leq G$ is a normal subgroup. As a set, G/H is the set of cosets of H in G. with the binary operation given by

$$aH * bH = abH,$$

for a, b in G.

This binary operation is well defined since

$$(aH)(bH) = a(Hb)H = abHH = abH.$$

where we have used that H is normal. The operation is associative since the operation on G is associative,

$$aH * (bH * cH) = aH * (bcH) = a(bc)H = (ab)cH = (abH) * cH = (aH * bH) * cH.$$

and the coset $H = eH$ is a unit since

$$eH * aH = eaH = aH = aeH = aH * eH.$$

The inverse of aH is given by $a^{-1}H$ since

$$aH * a^{-1}H = aa^{-1}H = eH = a^{-1}aH = a^{-1}H * aH.$$

Hence the factor group is in fact a group.

b). In order to find an isomorphism, we need to find which elements of A_4 that correspond to a and b. Since they have order 3, there are eight natural candidates, $(i\,j\,k)$. They come in pairs that form the four subgroups of order 3 together with the unit. We can pick any two from different subgroups, for example $\sigma = (1\,2\,3)$ and $\tau = (2\,3\,4)$. The composition is

$$\sigma\tau = (1\,2\,3)(2\,3\,4) = (1\,2)(3\,4)$$

which has order 2, so we get the relation $\sigma\tau\sigma\tau$. Thus we know that there is a well-defined homomorphism from G to A_4 satisfying $a \mapsto \sigma$ and $b \mapsto \tau$. Since σ and τ generate A_4, this homomorphism is surjective, and it remains to show that it is injective. (We can see that σ and τ must generate A_4 since $\sigma = s_1s_2$ and $\tau = s_2s_3$, which shows that all products of two adjacent transpositions there since $\sigma\tau = s_1s_3$.)

In order to see that the homomorphism is also injective, we may look at the expressions for all the elements of A_4 as products of the generators. We have

$$\begin{array}{llll}
\sigma = (1\,2\,3) & \tau = (2\,3\,4) & \sigma^{-1} = (1\,3\,2) & \tau^{-1} = (2\,4\,3) \\
\sigma\tau = (1\,2)(3\,4) & \tau\sigma = (1\,3)(2\,4) & \sigma^{-1}\tau = (1\,3\,4) & \sigma\tau^{-1} = (1\,2\,4) \\
\tau\sigma^{-1} = (1\,4\,2) & \tau^{-1}\sigma = (1\,4\,3) & &
\end{array}$$

and

$$\sigma\tau^{-1}\sigma = \sigma^{-1}\tau\sigma^{-1} = \tau\sigma^{-1}\tau = \tau^{-1}\sigma\tau^{-1} = (1\,4)(2\,3).$$

In G we have the relation $abab = e$, which we can rewrite as

$$ab = b^{-1}a^{-1}$$

and we can use it together with $a^3 = b^3 = e$ to deduce that

$$\begin{aligned}(a^{-1}b)^3 &= a^2ba^2ba^2b = a(ab)a(ab)a(ab) = a(b^{-1}a^{-1})a(b^{-1}a^{-1})a(b^{-1}a^{-1}) \\ &= ab^{-3}a^{-1} = aa^{-1} = e.\end{aligned}$$

We get from this that $(a^{-1}ba^{-1})(ba^{-1}b) = e$, which implies that

$$ba^{-1}b = (a^{-1}ba^{-1})^{-1} = ab^{-1}a.$$

We can write any element in G as a product of a, b, a^{-1}, b^{-1}, i.e., as

$$a^{i_1}b^{i_2}a^{i_3}\cdots b^{i_k}$$

where $i_j = \pm 1$. If there are two adjacent factors with the same sign of the exponent, we can use the relation $ab = b^{-1}a^{-1}$ to reduce the word to a shorter word. If there are no adjacent factors with the same sign of the exponent, we can use the relation $ba^{-1}b = ab^{-1}a$ to reduce the length of the word. Hence any word of length four or longer can be reduced and the only words that cannot be reduced are the ones listed above written in σ and τ. Thus G is no larger than A_4, which shows that they have to be isomorphic due to the surjective homomorphism $G \to A_4$.