Zhengdong Zhang
Email: zhengz@uoregon.edu
Course: MATH 647 - Abstract Algebra
Instructor: Dr.Victor Ostrik

Homework - Week 8
ID: 952091294
Term: Fall 2024
Due Date: 27^{th} November, 2024

Problem 6.3.5
Let $\sigma \in S_n$ be written as a product of disjoint cycles:

$$\sigma = (a_1 \dots a_s)(b_1 \dots b_t) \cdots$$

(a) Write σ^{-1} as a product of disjoint cycles.

(b) Deduce that σ and σ^{-1} are conjuagte in S_n.

(c) Deduce the stronger statement, that there is $\tau \in S_n$ with $\tau(n) = n$ and $\sigma^{-1} = \tau\sigma\tau^{-1}$.

Solution:

(a) Consider

$$\sigma^{-1} = (a_s\ a_{s-1} \dots a_1)(b_t\ b_{t-1} \dots) \cdots$$

To see that it is indeed the inverse, we only need to show that each of the disjoint cycles is the inverse, namely: for any $1 \leq i \leq s$(assume $a_{1-1} = a_s$ and $a_{s+1} = a_1$), we know that $(a_1 \dots a_s)(a_s \dots a_1)$ sends

$$a_i \xrightarrow{(a_s \dots a_1)} a_{i-1} \xrightarrow{(a_1 \dots a_s)} a_i.$$

Similar for $(a_s \dots a_1)(a_1 \dots a_s)$, which sends a_i to a_{i+1}, then back to a_i.

(b) Note that σ and σ^{-1} have the same cycle type, by Theorem 6.3.4, they belong to the same conjugacy class in S_n.

(c) We first prove this for disjoint cycles. Without loss of generality, assume $\sigma = (a_1 \dots a_s)$ and $a_s = n$. We know that $\sigma^{-1} = (a_s \dots a_1)$. Rewrite $(a_s \dots a_1) = (a_{s-1}a_{s-2} \dots a_1 a_s)$ and consider $\tau \in S_n$ with $\tau(a_i) = a_{s-i}$ for $1 \leq i \leq s-1$, $\tau(a_s) = a_s$ and τ fixes any other elements in $\{1, 2, \dots, n\} \setminus \{a_1, \dots, a_s\}$. By Lemma 6.3.3, we have

$$\tau\sigma\tau^{-1} = (\tau a_1 \dots \tau a_s) = (a_{s-1}a_{s-2} \dots a_1 a_s) = \sigma^{-1}$$

If σ is a product of disjoint cycles, note that in our construction τ only permutes elements in one disjoint cycles, so the above conclusion is also valid for σ.

Problem 6.3.6
Let $x \in S_n$ be of cycle type $(\lambda_1, \lambda_2, \dots, \lambda_l)$. What is the order of x?

Solution: Let $a_1, a_2, \dots, a_s$ be distinct elements in $\{1, 2, \dots, n\}$. Let

$$\sigma = (a_1 \dots a_s)$$

be a n-cycle in S_n.
Claim: The order of σ in S_n is equal to s.
Proof: We have $\sigma(a_i) = a_{i+1}$. So we have $\sigma^s(a_i) = a_{i+s}$. Here we assume for any integer k, $a_{i+k} = a_j$ if $i + k \equiv j (\text{mod } s)$ and $a_0 = a_s$. So $a_{i+s} = a_i$ and for any $1 \leq k \leq s-1$, $\sigma^k(a_i) = a_{i+k} \neq a_i$. ■ Let $x \in S_n$ be of cycle type $(\lambda_1, \ldots, \lambda_l)$. So the order of x is the least common multiple $lcd(\lambda_1, \ldots, \lambda_l)$.

Problem 6.3.7
The center of S_n is trivial for $n \geq 3$.

Solution: Let $\sigma \in S_n$ which is not the identity. We want to show that there exists some $\tau \in S_n$ such that $\tau\sigma\tau^{-1} \neq \sigma$. Decompose σ into disjoint cycles and first suppose this decomposition contains a s-cycle $(x_1 \ldots x_s)$ for $s \geq 3$, where $x_1, \ldots, x_s$ are different elements in $\{1, 2, \ldots, n\}$. Consider the transposition $\tau = (a_1 a_2) \in S_n$. By Lemma 6.3.3, $\tau(x_1 \ldots x_s)\tau^{-1} = (x_2 x_1 x_3 \ldots x_s)$. Note that $s \geq 3$, so $(x_1 x_2 x_3 \ldots x_s)$ and $(x_2 x_1 x_3 \ldots x_s)$ are different elements in S_n. This implies that the conjugate of τ changes one of the disjoint cycles in σ, so we have $\tau\sigma\tau^{-1} \neq \sigma$.

Now assume the decomposition of σ only contains 2-cycles. If $\sigma = (ij)$ is a transposition, since $n \geq 3$, there exists $1 \leq k \leq n$ with $k \neq i$ and $k \neq j$. Consider $\tau = (ik)$, we have

$$\tau\sigma\tau^{-1} = (\tau(i)\tau(j)) = (kj) \neq (ij).$$

Now suppose the decomposition of σ contains at least two disjoint 2-cycles $(ij)(kl)$ for differen i, j, k, l. Consider $\tau = (jk)$. We have

$$\tau(ij)(kl)\tau^{-1} = (ik)(jl) \neq (ij)(kl).$$

we are done.

Problem 6.4.1
The *Klein four-group*

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

Prove that V_4 is a normal subgroup of A_4. In particular, A_4 is not simple.

Solution: Write $a = (12)(34)$, $b = (13)(23)$ and $c = (14)(23)$. We have

$$ab = ba = c, bc = cb = a, ac = ca = b, a^2 = b^2 = c^2 = 1.$$

So this is a subgroup of S_4. Moreover, note that sgn(a) =sgn(b) =sgn$(c) = 1$, so V_4 is a subgroup of A_4. Given any $\tau \in A_4$, by Lemma 6.3.3, $\tau a \tau^{-1}$ has the same cycle type $(2, 2)$, and V_4 contains all the elements of cycle type $(2, 2)$ in S_4, so $\tau a \tau^{-1} \in V_4$. Similar for b and c. This shows that $\tau V_4 \tau^{-1} = V_4$. V_4 is a normal subgroup of A_4. And we know that $|A_4| = |S_4|/2 = 12$, so A_4 is not simple.

Problem 6.4.2
Show that
$$S_4 > A_4 > V_4 > C_2 > \{1\}$$
is a Jordan-Hölder series of S_4. What are the Jordan-Hölder factors?

Solution: Use the same notation for Exercise 6.4.1. We know that $[S_4 : A_4] = 2$ and any index 2 subroup is normal, so A_4 is normal in S_4. We have proved in Exercise 6.4.1 that V_4 is normal in A_4. Note that $V_4 = \{1, a, b, c, \}$ is abelian and $C_2 = \langle a \rangle = \langle b \rangle = \langle c \rangle$ is a subrgoup, so it is automatically normal in V_4.

Use the presentation of V_4
$$V_4 = \langle\langle a, b, c \,|\, a^2 = b^2 = c^2 = 1, ab = ba = c, ac = ca = b, bc = cb = a\rangle\rangle.$$
and assume $C_2 = \langle a \rangle$. The quotient group V_4/C_2 consists of two cosets C_2 and bC_2, thus $V_4/C_2 \cong C_2$ is simple. Note that $|A_4| = 12$ and $|V_4| = 4$, so the quotient group $|A_4/V_4| = \frac{|A_4|}{|V_4|} = 3$. The only order 3 group is cyclic group C_3 and it is simple. Similarly, we have $|S_4/A_4| = \frac{|S_4|}{|A_4|} = 2$ and the only group of order 2 is the cyclic group C_2, so $S_4/A_4 \cong C_2$ is simple. This proves that
$$S_4 > A_4 > V_4 > C_2 > \{1\}$$
is a Jordan-Hölder series of S_4.

Problem 6.4.10
Any finite group is isomorphic to a subgroup of A_n for some n.

Solution: By Theorem 6.3.1, any finite group is isomorphic to a subgroup of S_n for some n. If we could show that any symmetric group S_n is isomrphic to a subgroup of A_m for some m, then we are done. By Lemma 4.3.11, the symmetric group S_n is generated by the set
$$\{(12), (23), \ldots, (n-1\ n)\}\,.$$
Consider a subgroup G of S_{n+2} generated by the following elements
$$\{(12)(n+1\ n+2), (23)(n+1\ n+2), \ldots, (n-1\ n)(n+1\ n+2)\}$$
Note that for any $1 \leq i \leq n-1$, $(i\, i{+}1)$ and $(n{+}1\ n{+}2)$ are disjoint, so $\mathrm{sgn}((i\, i{+}1)(n{+}1\ n{+}2)) = 1$. Thus G is a subgroup of A_{n+2} and we have a group homomorphism $f : S_n \to G$ sending $\sigma \in S_n$ to $\sigma(n+1\ n+2)$ if σ is odd and to σ if σ is even. This is also an isomorphism because f is injective and every element in G is a product of its generating set.

Problem 6.4.11
Find the smallest n such that A_n contains a subgroup of order 15.

Solution:

Claim: If a group G has order 15, then G must be isomorphic to the cyclic group C_{15}.
Proof: By Cauchy's theorem, G must have an element a of order 3 and an element b of 5. Consider the cyclic subgroup generated by a and b. The index of $\langle b \rangle$ in G is 3, which is the smallest prime dividing 15, so $\langle b \rangle$ is normal in G. Since 3 and 5 are coprime, $\langle a \rangle \cap \langle b \rangle = \{1\}$. We know that $\mathrm{Aut}(\langle b \rangle) = C_4$. Consider a group homomorphism $\phi : \langle a \rangle \cong C_3 \to C_4$. Since 3 and 4 are also coprime, ϕ can only be the trivial map. G can only be $C_3 \times C_5 \cong C_{15}$. ■

A_n having a subrgoup isomorphic to C_{15} is equivalent to have an element of order 15. Consider $x \in S_n$ with the cycle type $(5, 3)$. It has order 15 and is an even permutation, so $x \in A_8$. The smallest possible n is 8.

Problem 6.5.7(Isometries)
Let E be the Euclidean space $\mathbb{R}^n$ with the standard scalar product. A distance preserving bijection of E is called an *isometry* of E.

1. The isometries of E form a group denoted by $ISO(E)$.
2. $AO(E)$ is a subgroup of $ISO(E)$.
3. If $f \in ISO(E)$ preserves zero, i.e. $f(0) = 0$, then f preserves the scalar product, i.e. $(f(v)|f(w)) = (v|w)$ for all $v, w \in E$.
4. An isometry of E preserving zero is a linear map.
5. $AO(E) = ISO(E)$.

Solution: Write $d : E \times E \to \mathbb{R}_{\geq 0},\ d(x, y) = |x - y|$ as the distance function on E.

1. Let $f, g \in ISO(E)$. For any $a, b \in E$, we have
$$d((f \circ g)(a), (f \circ g)(b)) = d(g(a), g(b)) = d(a, b).$$
So $(f \circ g) \in ISO(E)$. The identify function is the identity element in $ISO(E)$. $ISO(E)$ is indeed a group.

2. For any $x \in E$, write x as a vector and we know that $|x|^2 = x^T \cdot x$. Suppose $A \in O(E)$ is an orthogonal transformation. We have
$$(Ax)^T (Ax) = x^T (A^T A) x = |x|^2.$$
This implies that $d(Ax, 0) = d(x, 0)$. For any $x, y \in E$, we have
$$d(Ax, Ay) = |Ax - Ay| = |A(x - y)| = d(A(x - y), 0) = d(x - y, 0) = d(x, y).$$
Moreover, for any $x, y, z \in E$, we have
$$d(x - z, y - z) = |(x - z) - (y - z)| = |x - y| = d(x, y).$$
So both $O(E)$ and $T(E)$ are a subgroup of $ISO(E)$. We have $AO(E) = O(E)T(E) < ISO(E)$.

3. For any vector $v \in E$, we have

$$|f(v)| = d(f(v), 0) = d(f(v), f(0)) = d(v, 0) = |v|$$

since $f \in ISO(E)$ is an isometry and $f(0) = 0$. For any $v, w \in E$, f is an isometry impiles that

$$\begin{aligned} |f(v) - f(w)|^2 &= |v - w|^2 \\ (f(v)^T - f(w)^T) \cdot (f(v) - f(w)) &= (v^T - w^T) \cdot (v - w) \\ |f(v)|^2 + |f(w)|^2 - (f(v)^T f(w) + f(w)^T f(v)) &= |v|^2 + |w|^2 - (v^T w + w^T v) \\ f(v)^T f(w) + f(w)^T f(v) &= v^T w + w^T v \end{aligned}$$

Note that $2(f(v)|f(w)) = f(v)^T f(w) + f(w)^T f(v)$ and $2(v|w) = v^T w + w^T v$. So we have $(f(v)|f(w)) = (v|w)$.

4. Let $v, w \in E$ and c_1, c_2 be scalars. Then we have

$$\begin{aligned} |f(c_1 v + c_2 w) - c_1 f(v) - c_2 f(w)|^2 =& |f(c_1 v + c_2 w)|^2 + |c_1 f(v) + c_2 f(w)|^2 \\ & - 2(f(c_1 v + c_2 w)|c_1 f(v) + c_2 f(w)) \\ =& |c_1 v|^2 + |c_2 w|^2 + |c_1|^2 |f(v)|^2 + |c_2|^2 |f(w)|^2 + 4|c_1 c_2|(f(v)|f(w)) \\ & - 2(c_1(c_1 v + c_2 w)|v) + c_2(c_1 v + c_2(w)|w) \\ =& 2|c_1|^2 |v|^2 + 2|c_2|^2 |w|^2 + 4|c_1 c_2|(v|w) \\ & - 2(|c_1|^2 (v|v)^2 + |c_2|^2 (w|w)^2 + 2|c_1 c_2|(v|w)) \\ =& 0. \end{aligned}$$

This shows that

$$f(c_1 v + c_2 w) = c_1 f(v) + c_2 f(w).$$

We can conlude that f is linear.

5. We have seen in (2) that $AO(E)$ is a subgroup of $ISO(E)$. Given $f \in ISO(E)$, define a translation $\bar{f} : v \mapsto f(v) - f(0)$. we have $\bar{f}(0) = f(0) - f(0) = 0$. From the previous discussion, we know that $\bar{f}$ is a linear map. Write $\bar{f}$ as a matrix A. For any $x \in E$, we have

$$(Ax)^T (Ax) = x^T (A^T A) x = x^T x.$$

This shows that $A^T A = Id$ and $\bar{f} \in O(E)$. So f can be written as a composition of a translation and an element in $O(E)$. This proves that $ISO(E)$ is contained in $AO(E)$. We can conclude that $ISO(E) = AO(E)$.

Problem 6.6.2(Coxeter presentation of dihedral groups)

$$D_{2n} \cong \langle\langle s_1, s_2 \,|\, s_1^2 = 1, s_2^2 = 1, (s_1 s_2)^n = 1 \rangle\rangle.$$

Solution: In Example 6.6.1, we have already seen that

$$D_{2n} \cong \langle\langle a, b \mid a^n = 1, b^2 = 1, bab = a^{-1} \rangle\rangle.$$

Write

$$\begin{aligned} G_1 &= \langle\langle a, b \mid a^n = 1, b^2 = 1, bab = a^{-1} \rangle\rangle, \\ G_2 &= \langle\langle s_1, s_2 \mid s_1^2 = s_2^2 = 1, (s_1 s_2)^n = 1 \rangle\rangle. \end{aligned}$$

We only need to show that $G_1 \cong G_2$. Consider the following map

$$\begin{aligned} f : G_1 &\to G_2, \\ a &\mapsto s_1 s_2, \\ b &\mapsto s_1. \end{aligned}$$

Note that in G_2, we have

$$\begin{aligned} (s_1 s_2)(s_2 s_1) &= s_1(s_2^2)s_1 = s_1^2 = 1, \\ (s_2 s_1)(s_1 s_2) &= s_2(s_1^2)s_2 = s_2^2 = 1. \end{aligned}$$

We check f to be a well-defined group homomorphism. We have

$$\begin{aligned} f(a)^n &= (s_1 s_2)^n = 1 = f(1) = f(a^n), \\ f(b)^2 &= s_1^2 = 1 = f(b^2), \\ f(b)f(a)f(b) &= s_1(s_1 s_2)s_1 = (s_1^2)s_2 s_1 = (s_1 s_2)^{-1} = f(a^{-1}). \end{aligned}$$

Moreover, f is surjective since $f(b) = s_1$ and $f(ba) = s_2$. For f to be an isomorphism, the only thing left to check is that $|G_2| \geq 2n$.
<u>Claim:</u> The follwoing elements

$$1, s_1, s_1 s_2, s_1 s_2 s_1, s_1 s_2 s_1 s_2, \ldots, \underbrace{s_1 s_2 \cdots s_1 s_2}_{\text{n-1 times}} s_1$$

are different in G_2.
<u>Proof:</u> First we show that none of the nontrivial words as above is equal to 1. Suppose $a = s_1 s_2 \cdots = 1$, if a ends with s_1, then both left and right multiply with s_1, we have

$$s_2 s_1 \cdots s_2 = 1.$$

Now left and right multiply with s_2. Repeat this and it will give us either $s_1 = 1$ or $s_2 = 1$. A contradiction. Suppose two words $a = s_1 s_2 \cdots$ and $b = s_1 s_2 \cdots$ are equal. We are going to show that they must have the same length. Write $a = b$ and left multiply with s_1 and s_2 continously, if a and b have different length, then we have a nontrivial word is equal to 1. It is impossible as we have seen before. ■

Problem 6.6.3
Prove that the group of upperunitriangular 3×3 matrices over $\mathbb{F}_2$ is isomorphic to D_8.

Solution: Write the group of upperunitriangular matrices as G and define

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

Note that $a^4 = 1, b^2 = 1$ and $bab = a^3$. So we have a surjective map $G \twoheadrightarrow D_8$. Since G has 8 elements, same as D_8. So we have $D_8 \cong G$.