2024/10/16 MATH3301 Tutorial 7

1.(a) Proof: For all 3-cycle $(r,s,i) \in S_n$,

$(r,s,i) = (r,i)(r,s)$ is the product of 2 transpositions,

so $(r,s,i) \in A_n$ as 2 is even.

(b) Proof: For all product $(a,b)(c,d)$ of 2 transpositions:

Case 1: If $(a,b) = (c,d)$, then $(a,b)(c,d) = e$ is generated by S.

Case 2: If $a = c$ and $b \neq d$, then $(a,b)(a,d) = (a,d,b)$ is generated by S.

Case 3: If $(a,b),(c,d)$ are disjoint, then $(a,b)(c,d) = (c,a,d)(a,b,c)$ is generated by S

This implies a generator $T = \{(a,b)(c,d) \in A_n : (a,b),(c,d) \text{ are transpositions}\}$ of A_n is generated by S, so A_n is generated by S.

(c) Proof: For all 3-cycle $(a,b,c) \in A_n$,

Case 1: If $r = a$ and $s = b$, then $(a,b,c) = (r,s,c)$ is generated by R.

Case 2: If $r = a$ and $s \neq b, c$, then $(a,b,c) = (r,s,c)^{-1}(r,s,b)(r,s,c)$ is generated by R.

Case 3: If $r \neq a,b,c$ and $s \neq a,b,c$, then

$(a,b,c) = (r,a,b)(r,b,c) = (r,s,b)^{-1}(r,s,a)(r,s,b)(r,s,c)^{-1}(r,s,b)(r,s,c)$

is generated by R.

This implies a generator S of A_n is generated by R, so A_n is generated by R.

(d) Proof: Assume that N contains a 3-cycle $(r,s,j) \in A_n$.

For all 3-cycle $(r,s,i) \in A_n$:

Case 1: If $i = j$, then $(r,s,i) = (r,s,j) \in N$.

Case 2: If $i \neq j$, then $(r,s,i) = [(r,s)(i,j)](r,s,j)[(r,s)(i,j)]^{-1} \in N$.

This implies N contains a generator R of A_n, so $N = A_n$

2.(a) Proof. Since $\mu, (a_1, \cdots, a_r)$ are disjoint, $\mu, (a_1, \cdots, a_3)$ are disjoint,

so $\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1} = (a_1, \cdots, a_r)^{-1}\mu^{-1}(a_1, a_2, a_3)\mu(a_1, \cdots, a_r)(a_1, a_2, a_3)^{-1}$

$= (a_1, \cdots, a_r)^{-1}\mu^{-1}\mu(a_1, a_2, a_3)(a_1, \cdots, a_r)(a_1, a_2, a_3)^{-1}$

$= (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3)(a_1, \cdots, a_r)(a_1, a_2, a_3)^{-1} = \nu$

For all $3 < k < r$:

$\nu a_k = (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3)(a_1, \cdots, a_r)(a_1, a_2, a_3)^{-1} a_k$

$= (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3)(a_1, \cdots, a_r) a_k$

$= (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3) a_{k+1} = (a_1, \cdots, a_r)^{-1} a_{k+1} = a_k$

It remains to investigate a_1, a_2, a_3, a_r:

$\nu a_1 = (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3)(a_1, \cdots, a_r)(a_1, a_2, a_3)^{-1} a_1$

$= (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3)(a_1, \cdots, a_r) a_3$

$= (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3) a_4 = (a_1, \cdots, a_r)^{-1} a_4 = a_3$

$\nu a_2 = (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3)(a_1, \cdots, a_r)(a_1, a_2, a_3)^{-1} a_2$

$= (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3)(a_1, \cdots, a_r) a_1$

$= (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3) a_2 = (a_1, \cdots, a_r)^{-1} a_3 = a_2$

$\nu a_3 = (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3)(a_1, \cdots, a_r)(a_1, a_2, a_3)^{-1} a_3$

$= (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3)(a_1, \cdots, a_r) a_2$

$= (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3) a_3 = (a_1, \cdots, a_r)^{-1} a_1 = a_r$

$\nu a_r = (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3)(a_1, \cdots, a_r)(a_1, a_2, a_3)^{-1} a_r$

$= (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3)(a_1, \cdots, a_r) a_r$

$= (a_1, \cdots, a_r)^{-1}(a_1, a_2, a_3) a_1 = (a_1, \cdots, a_r)^{-1} a_2 = a_1$

Hence, $\nu = (a_1, a_3, a_r)$ is a 3-cycle, it remains to prove $\nu \in N$:

$$\sigma \in N \Rightarrow \left.\begin{cases} \text{(i) } \sigma^{-1} \in N \\ \text{(ii) } \underset{A_n}{(a_1, a_2, a_3)}\ \underset{N}{\sigma}\ \underset{A_n}{(a_1, a_2, a_3)^{-1}} \in N \end{cases}\right\} \Rightarrow \nu = \sigma^{-1}[(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}] \in N.$$

(b) Proof: $\sigma = \mu(a_4,a_5,a_6)(a_1,a_2,a_3)$, where $\mu, (a_1,a_2,a_3), (a_4,a_5,a_6)$ are mutually disjoint.

Since $\mu, (a_1,a_2,a_3), (a_4,a_5,a_6)$ are mutually disjoint, $\mu, (a_1,a_2,a_4)$ are disjoint,

so $\sigma^{-1}(a_1,a_2,a_4)\sigma(a_1,a_2,a_4)^{-1} = (a_1,a_2,a_3)^{-1}(a_4,a_5,a_6)^{-1}\mu^{-1}(a_1,a_2,a_4)\mu(a_4,a_5,a_6)(a_1,a_2,a_3)(a_1,a_2,a_4)^{-1} = (a_1,a_2,a_3)^{-1}(a_4,a_5,a_6)^{-1}\mu^{-1}\mu(a_1,a_2,a_4)(a_4,a_5,a_6)(a_1,a_2,a_3)(a_1,a_2,a_4)^{-1} = (a_1,a_2,a_3)^{-1}(a_4,a_5,a_6)^{-1}(a_1,a_2,a_4)(a_4,a_5,a_6)(a_1,a_2,a_3)(a_1,a_2,a_4)^{-1} = \nu$

Each factor is disjoint with μ, so ν is disjoint with μ.

According to my permutation calculator:

$$\nu = (a_1,a_3,a_2)(a_4,a_6,a_5)(a_1,a_2,a_4)(a_4,a_5,a_6)(a_1,a_2,a_3)(a_1,a_4,a_2)$$
$$= (a_1,a_4,a_2,a_6,a_3) \text{ is a cycle of length } 5$$

It remains to prove $\nu \in N$:

$$\sigma \in N \Rightarrow \left\{\begin{array}{l} (i)\ \sigma^{-1} \in N \\ (ii)\ \underset{A_n}{(a_1,a_2,a_4)}\underset{N}{\sigma}\underset{A_n}{(a_1,a_2,a_4)^{-1}} \in N \end{array}\right\} \Rightarrow \nu = \sigma^{-1}[(a_1,a_2,a_4)\sigma(a_1,a_2,a_4)^{-1}] \in N$$

(c) Proof: Assume that $\mu = (a_4,a_5)(a_6,a_7)$, where $(a_1,a_2,a_3), (a_4,a_5), (a_6,a_7)$ are mutually disjoint

$$\sigma^2 = [\mu(a_1,a_2,a_3)]^2 = [(a_4,a_5)(a_6,a_7)(a_1,a_2,a_3)]^2 = (a_4,a_5)^2(a_6,a_7)^2(a_1,a_2,a_3)^2$$
$= (a_1,a_3,a_2)$ is a 3-cycle, and $\sigma \in N \Rightarrow \sigma^2 \in N$

(d) Proof: $\sigma = \mu(a_3,a_4)(a_1,a_2)$, where $\mu, (a_3,a_4), (a_1,a_2)$ are mutually disjoint.

Since $\mu, (a_3,a_4), (a_1,a_2)$ are mutually disjoint, $\mu, (a_1,a_2,a_3)$ are disjoint,

so $\sigma^{-1}(a_1,a_2,a_3)\sigma(a_1,a_2,a_3)^{-1} = (a_1,a_2)^{-1}(a_3,a_4)^{-1}\mu^{-1}(a_1,a_2,a_3)\mu(a_3,a_4)(a_1,a_2)(a_1,a_2,a_3)^{-1}$

$= (a_1,a_2)^{-1}(a_3,a_4)^{-1}\mu^{-1}\mu(a_1,a_2,a_3)(a_3,a_4)(a_1,a_2)(a_1,a_2,a_3)^{-1}$

$= (a_1,a_2)^{-1}(a_3,a_4)^{-1}(a_1,a_2,a_3)(a_3,a_4)(a_1,a_2)(a_1,a_2,a_3)^{-1} = \nu$

Each factor is disjoint with μ, so ν is disjoint with μ

According to my permutation calculator:

$$\nu = (a_1,a_2)(a_3,a_4)(a_1,a_2,a_3)(a_3,a_4)(a_1,a_2)(a_1,a_3,a_2)$$
$= (a_1,a_3)(a_2,a_4)$ is the product of two disjoint 2-cycles.

It remains to prove $\nu \in N$

$$\sigma\in N \Rightarrow \left.\begin{cases}(i)\ \sigma^{-1}\in N\\ (ii)\ \underset{A_n}{(a_1,a_2,a_3)}\,\underset{N}{\sigma}\,\underset{A_n}{(a_1,a_2,a_3)^{-1}}\in N\end{cases}\right\}\Rightarrow \nu=\sigma^{-1}[(a_1,a_2,a_3)\sigma(a_1,a_2,a_3)^{-1}]\in N$$

$\beta\alpha=(a_1,a_3,i)(a_1,a_3)(a_2,a_4)=(a_1,i)(a_2,a_4)$

is the product of two disjoint 2-cycles

$(\beta\alpha)^2=[(a_1,i)(a_2,a_4)]^2=(a_1,i)^2(a_2,a_4)^2=e$

Note that $\beta^3=e$, so $\beta^{-1}\alpha\beta\alpha=\beta(\beta\alpha)^2=\beta$.

3.(a) $|A_3|=3$ prime, so A_3 has no nontrivial proper (normal) subgroup.

$|A_4|=12$. Consider $K_4=\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$.

$\circ$ +	e (0,0)	$(1,2)(3,4)$ (0,1)	$(1,3)(2,4)$ (1,0)	$(1,4)(2,3)$ (1,1)
e (0,0)	e (0,0)	$(1,2)(3,4)$ (0,1)	$(1,3)(2,4)$ (1,0)	$(1,4)(2,3)$ (1,1)
$(1,2)(3,4)$ (0,1)	$(1,2)(3,4)$ (0,1)	e (0,0)	$(1,4)(2,3)$ (1,1)	$(1,3)(2,4)$ (1,0)
$(1,3)(2,4)$ (1,0)	$(1,3)(2,4)$ (1,0)	$(1,4)(2,3)$ (1,1)	e (0,0)	$(1,2)(3,4)$ (0,1)
$(1,4)(2,3)$ (1,1)	$(1,4)(2,3)$ (1,1)	$(1,3)(2,4)$ (1,0)	$(1,2)(3,4)$ (0,1)	e (0,0)

This implies $K_4\cong\mathbb{Z}_2\times\mathbb{Z}_2$, so $\{e\}\neq K_4$ is a group with $K_4\subsetneq A_4$, $K_4\lneq A_4$

$eK_4=K_4e=\{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$

$(1,2,3)K_4=K_4(1,2,3)=\{(1,2,3),(1,3,4),(2,4,3),(1,4,2)\}$

$(1,3,2)K_4=K_4(1,3,2)=\{(1,3,2),(2,3,4),(1,2,4),(1,4,3)\}$

Hence, K_4 is a nontrivial proper normal subgroup of A_4.

Date / /

(b) Proof: Assume to the contrary that A_n has a nontrivial proper normal subgroup N.

Take $\sigma \in N \setminus \{e\}$, and factorize σ into disjoint cycles.

$$\sigma = \sigma_n \sigma_{n-1} \cdots \sigma_2 \sigma_1$$

According to 2(a) and 1(d), the decomposition contains no cycle of length $r>3$.

According to 2(b), the decomposition contains at most one 3-cycle.

According to 2(d), the decomposition contains at most one 2-cycle.

Now $\sigma = (1,2)$ (contradiction)

or $\sigma = (1,2,3)$ (contradiction)

or $\sigma = (1,2)(3,4,5)$ (contradiction)

Hence, our assumption is false, and we've proven that A_n is simple.

4. (a) $\mathbb{Z}_{40}$ (or $\mathbb{Z}_8 \times \mathbb{Z}_5$, they are the same group)

(b) $(\mathbb{Z}_4 \times \mathbb{Z}_2) \times \mathbb{Z}_5$ and $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_5$.

(c) $(\mathbb{Z}_4 \times \mathbb{Z}_2) \times \mathbb{Z}_5$ and $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_5$

5. (a) False. Consider the simple group $A_n (n \geq 5)$,

it has a nontrivial proper subgroup $\{e, (1,2)(3,4)\}$

(b) True. If a group has no nontrivial proper subgroup,

then it has no nontrivial proper normal subgroup, so it is simple.

(c) True. In an Abelian group, every subgroup is normal,

so the Abelian group has no nontrivial proper normal subgroup

implies it has no nontrivial proper subgroup.

As a consequence, this group is cyclic of prime order.

(d) True. In $\mathbb{Z}_{40}$, $[5]_{40}$ has order 8

(e) True. In an Abelian group of order $40 = 2^3 \cdot 5$, 2, 5 are two prime factors of 40,

so there exist g_2, g_5 with $\mathrm{ord}(g_2) = 2$ and $\mathrm{ord}(g_5) = 5$. Now $\mathrm{ord}(g_2 g_5) = 10 = \mathrm{l.c.m.}(2,5)$.

6.(a) Proof: Do prime factorization:

$G = [p_1 \text{ part}] \times [p_2 \text{ part}] \times \cdots \times [p_\ell \text{ part}]$

$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_\ell^{\alpha_\ell}$

$d = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_\ell^{\beta_\ell}$

$\beta_1 \le \alpha_1 \Rightarrow [p_1 \text{ part}]$ has a subgroup H_1 of order $p_1^{\beta_1}$

$\beta_2 \le \alpha_2 \Rightarrow [p_2 \text{ part}]$ has a subgroup H_2 of order $p_2^{\beta_2}$

$\vdots \qquad \vdots$

$\beta_\ell \le \alpha_\ell \Rightarrow [p_\ell \text{ part}]$ has a subgroup H_ℓ of order $p_\ell^{\beta_\ell}$

It suffices to take $H = H_1 \times H_2 \times \cdots \times H_\ell$

(b) Consider the group $\mathbb{Z}_4 \times \mathbb{Z}_2$ with order 8.

$(2\mathbb{Z}_4) \times \mathbb{Z}_2$ and $\mathbb{Z}_4 \times (0\mathbb{Z}_2)$ are two subgroups of $\mathbb{Z}_4 \times \mathbb{Z}_2$ of order 4.

Notice that $(2\mathbb{Z}_4) \times \mathbb{Z}_2$ doesn't have an element of order 4

and $\mathbb{Z}_4 \times (0\mathbb{Z}_2)$ has an element $([1]_4, [0]_2)$ of order 4

so $(2\mathbb{Z}_4) \times \mathbb{Z}_2 \not\cong \mathbb{Z}_4 \times (0\mathbb{Z}_2)$.

(c) If d has a prime factor p with multiplicity $\alpha \ge 2$,

then take $[\underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{\alpha \text{ copies}}] \times$ [The remaining parts] and we are done.

If d has no prime factor p with multiplicity $\alpha \ge 2$,

then by Cauchy Theorem and Chinese Remainder Theorem,

we can find $g = g_1 g_2 \cdots g_n$ with order d.

Date /