

**Problem 1:**

Let  $G$  be a group, and let  $a, b \in G$  with  $|a| = m$ ,  $|b| = n$ .

Part a:

First, if  $m \mid k$ , then  $m = lk$  for some  $l \in \mathbb{Z}$ . So  $a^k = a^{lm} = (a^m)^l = e^l = e$ .

Next, if  $m \nmid k$ , then  $k = lm + j$  for some  $l \in \mathbb{Z}$ ,  $j \in \mathbb{N}$  with  $0 < j < m$ . So  $a^k = a^{lm+j} = a^{lm}a^j = a^j \neq e$ . ( $a^j \neq e$  for any  $j$  between 0 and  $m$  (exclusive), because otherwise the order of  $a$  would be less than  $m$ , which is against our assumptions.)

So  $m \mid k$  if and only if  $a^k = e$ .

Part b:

Let  $ab = ba$ , and  $\langle a \rangle \cap \langle b \rangle = \{e\}$ .

First,  $|ab| \leq \text{lcm}(m, n)$ :

Then  $(ab)^{\text{lcm}(m, n)} = a^{\text{lcm}(m, n)}b^{\text{lcm}(m, n)} = ee = e$ .

So  $\text{lcm}(m, n)$  is a positive number with the property  $(ab)^{\text{lcm}(m, n)} = e$ ;  $\text{lcm}(m, n)$  is greater than or equal to the order of  $ab$ . (So  $|ab| \leq \text{lcm}(m, n)$ ).

Next,  $|ab| \geq \text{lcm}(m, n)$ :

Let  $r \in \mathbb{N}$  be such that  $(ab)^r = e$ .

Then  $(ab)^r = a^r b^r = e$ . To rewrite this, we know that  $a^r = b^{-r}$ . Now, because  $\langle a \rangle \cap \langle b \rangle = \{e\}$ , we know that  $a^s = b^t$  for any  $s, t \in \mathbb{Z}$  implies that  $a^s = b^t = e$ . By the earlier problem, this means that  $m \mid r$  and  $n \mid -r$  (or equivalently,  $n \mid r$ ).

So by elementary number theory, this means that  $\text{lcm}(m, n) \mid r$ . So  $r \geq \text{lcm}(m, n)$  if  $(ab)^r = e$  and  $r \geq 1$ .

So by the squeeze theorem,  $|ab| = \text{lcm}(m, n)$ .

**Problem 2:**

Consider  $\delta = (1\ 2\ \dots\ n)$ .

From theorem 4.9a, we know that the number of conjugacy classes of  $\delta$  is equal to  $[G : C(x)]$ .

From theorem 5.6, we know that every  $n$ -cycle is conjugate to  $\delta$ . There are  $(n-1)!$   $n$ -cycles in  $S_n$ :

We know that there are  $n!$  elements of  $S_n$ . Pick an element of  $S_n$ ...call it  $\sigma$ . Now, write the cycle  $(\sigma(1)\ \sigma(2)\ \sigma(3)\ \dots\ \sigma(n))$ . This cycle is equivalent to  $n$  other cycles, each given by

$$\begin{aligned}
&(\sigma(2) \sigma(3) \sigma(4) \dots \sigma(n) \sigma(1)) \\
&(\sigma(3) \sigma(4) \sigma(5) \dots \sigma(n) \sigma(1) \sigma(2)) \\
&\dots \\
&(\sigma(n) \sigma(1) \sigma(2) \dots \sigma(n-1)).
\end{aligned}$$

So there are  $n!/n = (n-1)!$  different  $n$ -cycles in  $S_n$

So  $[G : C(x)] = (n-1)!$ . So  $|C(x)| = n$ .

Now, there are  $n$  elements of the form  $\delta^i$ ; we know from class that an  $n$ -cycle has order  $n$ , so  $|\{\delta^i : i \in \mathbb{Z}\}| = |\langle \delta \rangle| = n$ .

Each element of the form  $\delta^i$  commutes with  $\delta$  trivially.

So the only elements that commute with  $\delta$  are the elements of the form  $\delta^i$ ; there are  $n$  of them, and there can only be  $n$  different elements that commute with  $\delta$ .

### Problem 3:

The following proof is constructive; it mimicks a selection sort. I attempt to illustrate the proof using crayon, as the proof is nigh-illegible otherwise.

Define  $s = (1 \ 2)$  and  $r = (1 \ 2 \ 3 \dots n)$ . (“swap” and “rotation”).

Let  $\sigma \in S_n$ . Then for each  $m \in \{1, 2, \dots, n\}$ :

Define  $\alpha_0 = (1)$ . Determine  $\sigma(1)$ . Consider  $r^{-(\sigma(1)-1)}$ .

Define  $\alpha_1 = r^{-\sigma(1)-1}$ . From the above diagram, it is clear that  $\alpha_1(1) =$

$\sigma(1)$ . Now, determine  $\alpha_1(\sigma(2))$ . Define  $\beta_2 = r^{-(\alpha_1(\sigma(2))-1)}$ . (Look at the picture)

Define  $\gamma_2 = (rs)^{\beta_2\alpha_1\sigma(2)-\beta_2\alpha_1\sigma(1)-1}$ . (Seriously, just look at the pictures)

Now define  $\alpha_2 = \gamma_2\beta_2\alpha_1$ . Now,  $\alpha_2(1) = \sigma(1)$  and  $\alpha_2(2) = \sigma(2)$ , as is clear from the illustrations.

We iterate to completion: for each  $n \in \mathbb{N}$  we can define  $\alpha_n = \gamma_n\beta_n\alpha_{n-1}$  recursively, where  $\beta_n = r^{-(\alpha_{n-1}(\sigma(n))-(n-1))}$  and  $\gamma_n = (rs)^{\beta_n\alpha_{n-1}\sigma(n)-\beta_n\alpha_{n-1}\sigma(n-1)-(n-1)}$ . From the below illustrations, it should be clear that for each  $n$ ,  $\alpha_n(x) = \sigma(x)$  for all  $x \leq n$ .

So we have constructed  $\alpha_n = \sigma$ , with  $\alpha_n$  a product of  $r$ ,  $s$ , and their inverses. Thus,  $\sigma \in \langle (1\ 2), (1\ 2\ 3 \dots n) \rangle$  for all  $\sigma \in S_n$

In other words,  $S_n \subset \langle (1\ 2), (1\ 2\ 3 \dots n) \rangle$ , which implies that  $S_n = \langle (1\ 2), (1\ 2\ 3 \dots n) \rangle$  (because subgroups generated by elements are still subgroups.)

**Problem 4:**

Let  $p$  be a prime number and let  $H < S_p$  contain a transposition and act transitively on  $\{1, \dots, p\}$ .

From the earlier homework,  $H$  has an element with no fixed point (it acts transitively on a finite set).

This means that  $H$  contains a  $p$ -cycle:

By the class equation and transitivity,  $p = \sum [H : H_{x_i}]$ . Now, this means that there is one stabilizer of any given  $x_i$ ; if  $[H : H_{x_i}] = 1$  for any given element, it is that for all elements (because  $p$  is prime). This would mean that for all  $x_i$ ,  $H = H_{x_i}$ ; that is, the entire group stabilizes every element, which contradicts transitivity.

Moreover, this means that  $[H : H_{x_i}] = p$ , which implies that  $|H| = p|H_{x_i}|$ . So  $p \mid |H|$ . Thus,  $H$  has a subgroup of order  $p$ . So  $H$  has an element of order  $p$ , by Cauchy's Theorem. We know that an element of  $S_p$  of order  $p$  is a  $p$ -cycle. So  $H$  has a  $p$ -cycle.

This means that  $H$  contains a transposition and a  $p$ -cycle; by a quick adaptation of the above problem (it is a bit more than a simple relabeling...but the proof can somewhat clearly be reworked to get the desired result), this means that  $H = S_p$ .

**Problem 5:**

This is given as an exercise in Hungerford: out of a sense of honesty, I must admit that I ran across this in the book, instead of coming up with it independently.

Consider  $H = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ .

First,  $H \leq G$ ;

We apply the subgroup criterion, and proceed by exhaustion. (In the below, I freely use the facts that 2-cycles are their own inverse and that disjoint cycles commute).

$$\begin{aligned}
(1)(1)^{-1} &= (1) \\
(1)((1\ 2)(3\ 4))^{-1} &= (3\ 4)(1\ 2) = (1\ 2)(3\ 4) \\
(1)((1\ 3)(2\ 4))^{-1} &= (2\ 4)(1\ 3) = (1\ 3)(2\ 4) \\
(1)((1\ 4)(2\ 3))^{-1} &= (2\ 3)(1\ 4) = (1\ 4)(2\ 3) \\
(1\ 2)(3\ 4)(1)^{-1} &= (1\ 2)(3\ 4) \\
(1\ 2)(3\ 4)((1\ 2)(3\ 4))^{-1} &= (1) \\
(1\ 2)(3\ 4)((1\ 3)(2\ 4))^{-1} &= (1\ 2)(3\ 4)(2\ 4)(1\ 3) = (1\ 4)(2\ 3) \\
(1\ 2)(3\ 4)((1\ 4)(2\ 3))^{-1} &= (1\ 2)(3\ 4)(2\ 3)(1\ 4) = (1\ 3)(2\ 4) \\
(1\ 3)(2\ 4)(1)^{-1} &= (1\ 3)(2\ 4) \\
(1\ 3)(2\ 4)((1\ 2)(3\ 4))^{-1} &= (1\ 3)(2\ 4)(3\ 4)(1\ 2) = (1\ 4)(2\ 3) \\
(1\ 3)(2\ 4)((1\ 3)(2\ 4))^{-1} &= (1) \\
(1\ 3)(2\ 4)((1\ 4)(2\ 3))^{-1} &= (1\ 3)(2\ 4)(2\ 3)(1\ 4) = (1\ 2)(3\ 4) \\
(1\ 4)(2\ 3)(1)^{-1} &= (1\ 4)(2\ 3) \\
(1\ 4)(2\ 3)((1\ 2)(3\ 4))^{-1} &= (1\ 4)(2\ 3)(3\ 4)(1\ 2) = (1\ 3)(2\ 4) \\
(1\ 4)(2\ 3)((1\ 3)(2\ 4))^{-1} &= (1\ 4)(2\ 3)(2\ 4)(1\ 3) = (1\ 2)(3\ 4) \\
(1\ 4)(2\ 3)((1\ 4)(2\ 3))^{-1} &= (1)
\end{aligned}$$

Next,  $H \trianglelefteq S_4$ ;

Recall that two elements of  $S_4$  are conjugate if and only if their cycle decomposition has the same cycle type. Note that  $H$  contains all of the elements of  $S_4$  composed of a product of two disjoint 2-cycles.

So an element is conjugate to an element of  $H$  if and only if it is in  $H$ . That is,  $ghg^{-1} \in H$  for all  $g \in G$ ,  $h \in H$ .

Thus,  $H \trianglelefteq S_4$ . (And so,  $H \trianglelefteq A_4$ ).

### Problem 6:

Note: I adapt the proof in Hungerford to fit my needs for this problem.

We know from class that for  $n \geq 5$ ,  $A_n$  is simple.

Let  $N \trianglelefteq S_n$ , with  $n \geq 5$ , with  $N$  nontrivial.

Then either  $N$  contains a 3-cycle,  $N$  contains an element  $\sigma$  with its cycle decomposition having a cycle of length  $r \geq 4$ ,  $N$  contains an element  $\sigma$  with its cycle decomposition having at least two cycles of length 3,  $N$  contains an element  $\sigma$  that is a product of one 3-cycle and some 2-cycles, or every element of  $N$  is a product of disjoint 2-cycles.

Case 1: If  $N$  contains a 3-cycle, then  $N$  contains  $A_n$ ; this implies that either  $N = A_n$  or  $N = S_n$ .

Case 2: If  $N$  contains an element  $\sigma$  with its cycle decomposition having a cycle of length  $r \geq 4$ , then  $\sigma = (a_1 a_2 \dots a_r) \tau$  for some  $\tau$  disjoint from the first cycle. Let  $\delta = (a_1 a_2 a_3)$ . Then  $\sigma^{-1}(\delta \sigma \delta^{-1}) \in N$  by normality. But

$$\sigma^{-1}(\delta \sigma \delta^{-1}) = \tau^{-1}(a_1 a_r a_{r-1} \dots a_2)(a_1 a_2 a_3)(a_1 a_2 a_3 \dots a_r) \tau(a_1 a_3 a_2) = (a_1 a_3 a_r) \in N.$$

So  $N$  has a 3-cycle, and we regress to the first case.

Case 3: If  $N$  contains an element  $\sigma$  with its cycle decomposition having at least two cycles of length 3, then  $\sigma = (a_1 a_2 a_3)(a_4 a_5 a_6) \tau$  with  $\tau$  disjoint from the first two cycles. Let  $\delta = (a_1 a_2 a_4)$ . Then, as above,

$$\sigma^{-1}(\delta \sigma \delta^{-1}) = \tau^{-1}(a_4 a_6 a_5)(a_1 a_3 a_2)(a_1 a_2 a_4)(a_1 a_2 a_3)(a_4 a_5 a_6) \tau(a_1 a_4 a_2) = (a_1 a_4 a_2 a_6 a_3) \in N.$$

And so we regress to the second case.

Case 4: If  $N$  contains an element  $\sigma$  that is a product of one 3-cycle and some 2-cycles, then  $\sigma = (a_1 a_2 a_3) \tau$  where  $\tau$  is disjoint from the first cycle and is a product of disjoint 2-cycles. Then  $\sigma^2 \in N$  and so,

$$\sigma^2 = (a_1 a_2 a_3) \tau (a_1 a_2 a_3) \tau = (a_1 a_3 a_2) \tau^2 = (a_1 a_3 a_2)$$

So we regress to the first case.

Case 5: If every element of  $N$  is a product of disjoint 2-cycles, then consider any  $\sigma \in N$ . If some  $\sigma$  is a 2-cycle, then  $N = S_n$ , by normality of  $N$  and the fact that the 2-cycles generate  $S_n$ . If not, then let  $\sigma = (a_1 a_2)(a_3 a_4) \tau$  where  $\tau$  is disjoint from the first two cycles. Then let  $\delta = (a_1 a_2 a_3)$ . Then as above:

$$\sigma^{-1}(\delta \sigma \delta^{-1}) = \tau^{-1}(a_3 a_4)(a_1 a_2)(a_1 a_2 a_3)(a_1 a_2)(a_3 a_4) \tau(a_1 a_3 a_2) = (a_1 a_3)(a_2 a_4) \in N$$

Define the above permutation to be  $\gamma$ . There's an element,  $a_5$ , distinct from each of  $a_1 \dots a_4$ . Consider  $\lambda = (a_1 a_3 a_5)$ . Now, we know that

$$\gamma^{-1}(\lambda \gamma \lambda^{-1}) = (a_1 a_3)(a_2 a_4)(a_1 a_3 a_5)(a_1 a_3)(a_2 a_4)(a_1 a_5 a_3) = (a_1 a_3 a_5) \in N$$

So we regress to the first case.

That is, in all cases, we have that a nontrivial subgroup of  $S_n$  is either  $A_n$  or  $S_n$ . This satisfies the problem.

**Problem 7:**

Define  $\phi : \text{Aut}(A_4) \rightarrow S_4$  as follows:

Define  $a = (1\ 2\ 3)$ ,  $b = (1\ 2\ 4)$ ,  $c = (1\ 3\ 4)$ , and  $d = (2\ 3\ 4)$ .

Define  $F : \{a, b, c, d\} \rightarrow \{1, 2, 3, 4\}$  by  $F(a) = 1$ ,  $F(b) = 2$ ,  $F(c) = 3$ , and  $F(d) = 4$ . (This is done primarily for convenience. It is rather clear that  $F$  is bijective.)

Then  $\phi(\psi)$  is the transposition naturally given by the way that  $\psi$  permutes these elements. That is,

$$\begin{aligned}\phi(\psi)(1) &= F(\psi(F^{-1}(1))) \\ \phi(\psi)(2) &= F(\psi(F^{-1}(2))) \\ \phi(\psi)(3) &= F(\psi(F^{-1}(3))) \\ \phi(\psi)(4) &= F(\psi(F^{-1}(4)))\end{aligned}$$

First:  $\phi$  is well defined:

If  $\psi \in \text{Aut}(A_4)$ , then  $\psi$  is one-to-one. So each of the expressions in the definition of  $\phi$  is distinct from each other; that is,  $\phi(\psi)$  is a permutation of  $\{1, 2, 3, 4\}$ . That is,  $\phi$  is well-defined.

Next,  $\phi$  is a homomorphism:

Let  $\psi, \chi \in \text{Aut}(A_4)$ . Then:

$$\begin{aligned}\phi(\psi\chi)(n) &= F(\psi\chi(F^{-1}(n))) \\ &= F(\psi(\chi(F^{-1}(n)))) \\ &= F(\psi(F^{-1}(F(\chi(F^{-1}(n)))))) \\ &= \phi(\psi)\phi(\chi)(n)\end{aligned}$$

Last,  $\phi$  is bijective:

First,  $\phi$  is injective:

Let  $\psi, \chi \in \text{Aut}(A_4)$ , with  $\phi(\psi) = \phi(\chi)$ .

Next,  $\phi$  is surjective: