1(a). Let $k$ be the first position not occupied by the correct card. Thus positions $1, 2, \ldots, k - 1$ are occupied by cards $1, 2, \ldots, k - 1$, but card $k$ is in position $j$ for some $j > k$. If $k \geq 51$, we’re done: all but the last two cards are in correct position. Thus suppose $k < 51$. Then there is some number $i > 51$ different from $k$ and $j$. If we now apply the cyclic permutation $(j \ k \ i)$, the first $k$ cards will now be in correct position.

We can repeat the process until all the cards are correct or until only the last two are incorrect.

1(b). The 3-cycles are all even permutations, so they are contained in $A_n$. Thus $H \subset A_n$ (since $H$ is the smallest subgroup containing all the 3-cycles.) We will prove that every element of $A_n$ can be written as a product of 3-cycles, i.e. that $A_n \subset H$. Consequently $H = A_n$, which has index 2 in $S_n$.

Method 1 (using part (a).) The argument in part (a) applies to decks of any size. Let $\sigma \in S_n$. Then by part (a), there is a product $\tau$ of 3-cycles such that

\[(*) \quad \tau \sigma = (n-1 \ n) \quad \text{or} \quad \tau \sigma = 1\]

Each 3 cycle is an even permutation, so $\tau$ is an even permutation. Thus $\tau \sigma$ is even if $\sigma$ is even and odd if $\sigma$ is odd. Hence by $(*)$:

$$\sigma = \begin{cases} \tau^{-1}(n-1 \ n) & \text{if } \sigma \text{ is odd, and} \\ \tau^{-1} & \text{if } \sigma \text{ is even.} \end{cases}$$

Since $\tau$ is a product of 3-cycles, it (and its inverse) belongs to $H$. Thus if $\sigma$ is even, $\sigma = \tau^{-1}$ belongs to $H$. □

Method 2: Any element $\sigma$ of $A_n$ can be written as a product of an even number of transpositions:

$$\sigma = T_1 T_2 \ldots T_{2k-2} T_{2k} = (T_1 T_2)(T_3 T_4) \ldots (T_{2k-1} T_k).$$

Thus if we can show that the product of any pair of transpositions must be in $H$, then $\sigma$ must be in $H$.

Thus consider such a product $\rho = (a \ b)(c \ d)$.

Case 1: $a$ and $b$ are the same as $c$ and $d$. Then $\rho = 1$, which is certainly in $H$.

Case 2: $(a \ b)$ and $(c \ d)$ have one element in common. Then $\rho$ is itself a 3-cycle and therefore is in $H$. For example $(1 \ 2)(2 \ 3) = (1 \ 2 \ 3)$. In general $(x \ y)(y \ z) = (x \ y \ z)$ if $x$, $y$, and $z$ are all different.

Case 3: $a$, $b$, $c$, and $d$ are all different. Then

$$(a \ b)(c \ d) = (a \ b \ c)(b \ c \ d)$$

□
2(a). This was done in class Wed. . It’s also in the text (section 4.3, p. 126, proposition 11) about conjugates in the symmetric group.

2(b). Let $H$ be a normal subgroup that contains a 3-cycle. By 2(a), it contains every 3-cycle. Hence by problem 1, it contains all of $A_n$. (The problem had a misprint. It should say “...then it contains all of $A_n$”, not “...then it is all of $A_n$”.)

(Note: $|A_n|$ divides $|H|$, which divides $|S_n|$. Since $|A_n|$ is $\frac{1}{2} |S_n|$, this means $|H| = |A_n|$ or $|H| = |S_n|$. Thus $H = A_n$ or $H = S_n$.)

3(a). Claim: $G$ cannot have two distinct subgroups, each of order $p$. For suppose $H$ and $K$ are such subgroups. Then $H \cap K$ is a subgroup of $H$ and is not equal to it, so $|H \cap K|$ divides, but is not equal to, $|H| = p$. Thus $|H \cap K| = 1$, so

$$|HK| = \frac{|H||K|}{|H \cap K|} = p^2$$

But $HK$ is a subgroup (since $G$ is abelian), so $HK$ should divide $|G| = pq$ by Lagrange’s theorem. Since $p^2$ does not divide $pq$, there cannot be two such subgroups $H$ and $K$.

In other words, if $G$ has a subgroup of order $p$, then every element of order $p$ must belong to it. Consequently $G$ can have at most $p-1$ elements of order $p$. Likewise it can have at most $q-1$ elements of order $q$. By Lagrange, every element must have order 1, $p$, $q$, or $pq$. The identity is the only element of order 1, so $G$ has at most $1 + (p-1) + (q-1) = p + q - 1$ elements of order $\neq pq$. Since $p + q - 1 < pq$, $G$ must have an element of order $pq$. $\square$

(Why is $p + q - 1 < pq$? Well, if $p + q - 1 \geq pq$, then (subtracting $p$ from both sides) $q - 1 \geq p(q - 1) \geq (p - 1)(q - 1)$. But $p$ and $q$ are primes and are therefore $\geq 2$.)

3(b).

**Lemma.** . If $a$ and $b$ are elements of a group that have relatively prime orders and that commute, then $|ab| = |a||b|$.

**Proof.** Let $A$ and $B$ be the subgroups generated by $a$ and $b$, respectively. Then by Lagrange, $A \cap B$ must be $\{1\}$.

Now suppose $(ab)^r = 1$. Then (since $a$ and $b$ commute) $a^r b^r = 1$, so $a^r = b^{-r}$.

Since $a^r \in A$ and $b^{-r} \in B$, $a^r = b^{-r}$ must be in $A \cap B = \{1\}$, so

$$a^r = b^{-r} = 1.$$ 

Thus $|a|$ divides $r$ and $|b|$ divides $r$. Since $|a|$ and $|b|$ are relatively prime, $|a||b|$ must divide $r$. Conversely, if $|a||b|$ divides $s$, then $a^s = 1$ and $b^{-s} = 1$, so $(ab)^s = a^s b^s = 1$.

Thus $|ab| = |a||b|$. $\square$

Now (to prove the statement in the problem), let $x$ be any element of $G$. If $X = \langle x \rangle$ is all of $G$, we are done. If not, there is an element $y \in G \setminus X$. Let $Y = \langle y \rangle$.
Then

\[(*) \quad |XY| = \frac{|X||Y|}{|X \cap Y|} = |X| - \frac{|Y|}{|X \cap Y|}.\]

This is bigger than \(|X|\), so

\[\frac{|Y|}{|X \cap Y|} > 1.\]

Also \(XY = YX\) (since \(G\) is abelian), so \(XY\) is a subgroup, so by Lagrange, \((*)\) divides \(|G|\), and since \(|G|\) has no repeated prime factors, \(\frac{|Y|}{|X \cap Y|}\) must have a prime factor \(p\) that does not divide \(|X|\). Thus \(|Y| = |y| = mp\) for some \(m\).

Let \(z = y^m\). Note that the order of \(z\) is \(p\).

By the lemma, \(|xz| = |x||z| > |x|\).

We have shown: if \(x \in G\) has order \(|x| < |G|\), then there is another element \(x' (= xz)\) of greater order. Since there are only finitely many elements of \(G\), there must be one of largest order, and that order must be \(|G|\). \(\square\)