Answer sheet 2 - Yiwei Yang 2018533218

1. a) $|G| = 1$, the case is trivial group

   b) Assume $|G| > 1$ then there's $a \in G$, but all groups have inverses so $a^{-1} \in G$, which indicates that $|G| \geq 3$, but the case would be abelian so there should be another element $b \in G$ and also, it's inverse, and we have that $|G| \geq 5$.

   c) We have that $ab \in G$. So that we may give one of the following:

   1) $ab = a$ or $ab = b$ which indicates that they can be eliminated as they imply that either a or b are identity or inverse

   3) $ab = e$ or $ab = a^{-1}$ or $ab = b^{-1}$ which indicates that they can be eliminated for that $aba = a^2b = e$ with left and right a multiplication on $ab = a^{-1}$.

   So that $ab = ba$ for the elements which clearly aren't abelian.

   Thus $|G| \geq 6 \square$

2. a.

   First denote $\tau = (1\ 2\ \ldots n)$ and $\tau = (1\ 2)$. The transposition of the denoted form $(k\ k+1), \forall k \in \mathbb{N}$ by the following steps leads to $(k\ k+1)$

   1. shift the numbers up $k-1$ and k will be at place 1. this manifest the permutation $\sigma^{-(k-1)}$
   2. swap k and $k+1$, which manifest the transposition τ
   3. move the number back $k-1$, and the permutation is σ^{k-1}.

   By another way, we can show that $(k+1\ k+2) = \tau(k\ k+1)\tau^{-1}$. with induction from above process. Take first item as 1 we get $(1\ k+1) = (1\ k)(k\ k+1)(1\ k)$. To generalize the case 1, we have $(m\ k) = (1\ m)(1\ k)(1\ m)$

   Thus the group generated by σ and τ can include all transpostion and can generate $\mathfrak{S}_r \square$

   b. Without loss of generality, let $\tau = (0\ 1)$, denote $\sigma = (0\ 1..p)$ we have $\sigma^1\tau\sigma^{-1} = (0\ 1\ ..p)(0\ 1)(p\ ..\ 1\ 0) = (1\ 2)$

   By induction, we have $\sigma^k\tau\sigma^{-k} = \sigma\left(\sigma^{k-1}\tau\sigma^{-k+1}\right)\sigma^{-1} = (k+1\ k+2)$

   Thus $(01), (12), \ldots, (p-1\ p)$ are generated by $\{\tau, \sigma\}$. Let $(x\ y)$ be a transposition and $(x\ x+1)(x+1\ x+2)..(y-1\ y) = (x\ y)$ and $(x\ y)$ is generated by $\{\tau, \sigma\}$. So that it generate $\mathfrak{S}_r$.

3. a.

   Since an exchange of adjacent elements only changes the order of these two elements and does not change the relative position between the remaining elements and the exchanged elements, an exchange can only make the inverse order number +1 or -1. With the goal of ascending arrangement as the exchange, as long as the sequence does not reach ascending arrangement, there exist two adjacent elements that form an inverse order pair (which can be proved by contradiction), so there exists an exchange of adjacent elements so that the number of inverse order is always -1. Therefore, under the condition that only adjacent elements can be exchanged, the number of inverse order is equal to the minimum number of exchanges required for a sequence to become ascending. which is $l(\tau) = inv(\tau)$.

   b.

   The inverse number is

```
(3,1),(3,2)
(4,1),(4,2)
(5,1),(5,2)
```

The process is listed below

```
3 4 1 5 2  <- (3 4 5 1 2)o(3 4)
3 1 4 5 2  <- (3 4 1 5 2)o(2 3)
1 3 4 5 2  <- (3 1 4 5 2)o(1 2)
1 3 4 2 5  <- (1 3 4 5 2)o(3 4)
1 3 2 4 5  <- (1 3 4 2 5)o(2 3)
1 2 3 4 5  <- (1 3 2 4 5)o(1 2)
```

4. Take any $(k\ k+1)$-type permutation τ, $Sign(\tau) = 1$. (There is only one inverse order pair).

   Take any (k k+1)-type permutation η, then $Sign(\tau\sigma) = Sign(\sigma) + 1 = Sign(\tau) + Sign(\sigma)$. A number pair (i, j), which is not simultaneously the inverse order pair of $\tau\sigma$ and σ when and only when $\{\sigma(i), \sigma(j)\} = \{k, k+1\}$. Thus the inverse order pairs of σ and $\tau\sigma$ differ by 1 and therefore have opposite signs.

   Take any given substitution τ, written as a product of $(k\ k+1)-$type pairs of permutations, and repeatedly using the above equation, it is known that $Sign(\tau)$ is equal to the number of permutations modulo 2 remainder used when writing τ as a product of (k k+1)-type pairs of permutations.

   If the permutation is written as a rotation product, $Sign$ is equal to the number of rotations of even length mod 2 remainder. This means that the parity of k does not depend on the choice. □

5. a.

   Let X be a 1 x n matrix $(1, 1...1)$. Observe that $XA = X$

   It is then straightforward to prove the following facts, using only what you know about matrix multiplication.

   1. If $XA = X$ and $XB = X$ for some 2×2 matrices A and B then also $X(AB) = X$
   2. If $XA = X$ then also $X = XA^{-1}$.

      These facts immediately imply that G is a subgroup of the group of invertible $n \times n$ matrices.□

   b.

   If G has elements of order 3, let $|x| = 3$, then $<x>$ is a subgroup of index 2, a regular subgroup. $G/<x> \cong \mathbb{Z}_2$

   Take $y \notin <x>$, the order of $|y|$ is divisible by 2, and by assumption we know that $|y| = 2$. $<x, y>$ is at least a group of order 6, so $< x, y >= G$, $yxy = x$ or $yxy = x^2$, both of which give $\mathbb{Z}_6$ or S_3, respectively. if the elements of G are all of order 2, then G is commutative group, taking the element x of order 2, $G/<x>$ is of order 3, so G has elements of order divisible by 3, a contradiction.

   Thus $|S| = 3$ □