1 Groups
1.4 The Sylow theorem

1. If $a \in G$ with $ord(a) = 5$, then $< a >$ is a Sylow 5-subgroup of group G whose order is 20. Since $5k + 1|4$, $k = 0$, then G has a unique Sylow 5-subgroup, thus all elements of order 5 in G are contained in $< a >$, hence there are 4 elements of order 5 in G.

2. It is obvious that $< \sigma >$ is a subgroup of S_p. Since $|S_p| = p!$ and $| < \sigma > | = p$, $| < \sigma > |||S_p|$. Moreover, $(p, (p-1)!) = 1$, therefore $p^2 \nmid p!$. Hence $< \sigma >$ is a Sylow p-subgroup of S_p.

3. For any Sylow p-subgroup Q of G, then there are $a \in G$ such that $a^{-1}Pa = Q$, thus $Q = aPa^{-1} \subseteq aHa^{-1} \subseteq H$.

4. $|S_5| = 120 = 2^3 \times 3 \times 5$. Since all Sylow 3-subgroups of S_5 are cyclic groups, consider $< \sigma >$s which is generated by a 3-cycle acts on the set $\{1, 2, 3, 4, 5\}$, then there are 1 element or 3 elements contained in the orbit $< \sigma > \cdot a$ and there are only one orbit contains 3 elements, therefore $\sigma = (i, j, k)$ for some $1 \leq i, j, k \leq 5$.

   Since $|S_4| = 24 = 8 \times 3$, $2l + 1|3$, then $l = 0, 1$, thus there are 1 or 3 Sylow 2-subgroup of S_4. $K = \{(1), (12)(34), (13)(24), (14)(23)\}$ is a subgroup with order 4 of S_4, then

   $$< K \cup \{(12)\} >= \{(1), (12)(34), (13)(24), (14)(23), (12), (34), (1324), (1423)\},$$

   $$< K \cup \{(13)\} >= \{(1), (12)(34), (13)(24), (14)(23), (24), (13), (1234), (1432)\},$$

   $$< K \cup \{(14)\} >= \{(1), (12)(34), (13)(24), (14)(23), (14), (23), (1342), (1243)\}$$

   are subgroups of order 8, therefore these three subgroups are all Sylow 2-subgroups of S_4. For S_5, since $2k + 1|3 \times 5$, $k = 0, 1, 2, 7$, then then there are 1, 3,5 or 15 Sylow 2-subgroups. In the above three Sylow 2-subgroups, substitute 1,2,3,4 with 5 respectively, then we get another 12 Sylow 2-subgroups of S_5. Hence there are 15 Sylow 2-subgroups of S_5.

   Similarly, Sylow 3-subgroups of S_4 are generated by (i, j, k) for some $1 \leq i, j, k \leq 4$, therefore there are 4 Sylow 3-subgroups.

   For S_3, there are 3 Sylow 2-subgroups:$< (12) >, < (13) >, < (23) >$,and unique Sylow 3-subgroup:$< (123) >$.

5. (a) For $ord(G) = 12 = 2^2 \times 3$, since $3k + 1|4$, $k = 0, 1$. If $k = 0$, then there are only one Sylow 3-subgroup P, thus $P = a^{-1}Pa$ for any $a \in G$. If $k = 1$, then there are 4 Sylow 3-subgroup. Since there are 8 elements of order 3, there are 4 elements at most contained in Sylow 2-subgroup, thus there are only one Sylow 2-subgroup Q, hence $Q = a^{-1}Qa$ for any $a \in G$.

   (b) For $ord(G) = 28 = 2^2 \times 7$, since $7k + 1|4$, $k = 0$, then there are only one Sylow 7-subgroup P, thus $P = a^{-1}Pa$ for any $a \in G$.

(c) For $ord(G) = 56 = 2^3 \times 7$, since $7k+1|8$, $k = 0, 1$. If $k = 0$, then there are only one Sylow 7-subgroup P, thus $P = a^{-1}Pa$ for any $a \in G$. If $k = 1$, then there are 8 Sylow 7-subgroup. Since there are 48 elements of order 7, there are 8 elements at most contained in Sylow 2-subgroup, thus there are only one Sylow 2-subgroup Q, hence $Q = a^{-1}Qa$ for any $a \in G$.

(d) For $ord(G) = 200 = 2^3 \times 5^2$, since $5k+1|8$, $k = 0$, then there are only one Sylow 5-subgroup P, thus $P = a^{-1}Pa$ for any $a \in G$.

6. $|G| = p^n a$ where $1 < a < p$, then $pk+1|a$, we get $k = 0$, therefore there are only one Sylow p-subgroup H, thus $H = gPg^{-1}$ for any $g \in G$.

7. According to Exercise 1.3.9 $|C(G)| = p^s$ where $1 \leq s \leq 3$. If $ord(C(G) = p^2$, in $G/C(G)$, define $aC(G) \cdot bC(G) = abC(G)$ for any $aC(G), bC(G) \in G/C(G)$, then $G/C(G)$ is a group of order p. Therefore $G/C(G) =< aC(G) >$, then $G = \{a^i b | 0 \leq i \leq p-1, b \in C(G)\}$, while $a^i b \cdot a^j b' = a^{i+j} bb' = a^j b' \cdot a^i b$, thus G is an abelian group, it is contradiction. Hence $|C(G)| = p$, let $G/C(G) = \bar(G)$, then $\bar(G)$ is an abelian group of order p^2. Since $C(G)$ is nontrivial, $|C(\bar(G))| = p^s$ where $s = 1, 2$. If $|C(\bar(G))| = p$, then $\bar(G)$ is an abelian group; if $|C(\bar(G))| = p^2$, then $\bar(G)$ is an abelian group. Thus $abC(G) = aC(G) \cdot bC(G) = bC(G) \cdot aC(G) = baC(G)$, then $aba^{-1}b^{-1} = (ab)(ba)^{-1} \in C(G)$. While G is a nonabelian group, then there exist $a, b \in G$ such that $aba^{-1}b^{-1} \neq e$, hence $C(G) =< aba^{-1}b^{-1} >$.

8. (1) Since $\overline{E_n} := \begin{pmatrix} \bar{1} & & \\ & \ddots & \\ & & \bar{1} \end{pmatrix} \in GL(n, \mathbb{Z}_p)$ and $\overline{E_n} := \begin{pmatrix} \bar{1} & & \\ & \ddots & \\ & & \bar{1} \end{pmatrix} \in SL(n, \mathbb{Z}_p)$, $GL(n, \mathbb{Z}_p) \neq \emptyset \neq SL(n, \mathbb{Z}_p)$. For any $A = (\overline{a_{ij}}), B = (\overline{b_{ij}}), C = (\overline{c_{ij}}) \in GL(n, \mathbb{Z}_p)$, $(AB)C = (\overline{u_{ij}})(\overline{c_{ij}}) = (\overline{d_{ij}})$ where $\overline{u_{ij}} = \sum_{k=1}^{n} \overline{a_{ik} b_{kj}}$ and $\overline{d_{ij}} = \sum_{l=1}^{n} \overline{u_{il} c_{lj}}$, since $\overline{d_{ij}} = \sum_{l=1}^{n} \sum_{k=1}^{n} \overline{a_{ik} b_{kl} c_{lj}} = \sum_{k=1}^{n} \overline{a_{ik}} (\sum_{l=1}^{n} \overline{b_{kl} c_{lj}})$, $(AB)C = A(BC)$. Since $A\overline{E_n} = A = \overline{E_n}A$, $\overline{E_n}$ is the identity of $GL(n, \mathbb{Z}_p)$. Since $|A||A*| = |A|\overline{E_n}$ and $|A| \neq \bar{0}$, $(\frac{1}{|A|}A*)A = \overline{E_n} = A(\frac{1}{|A|}A*)$, moreover $|\frac{1}{|A|}A*| = \frac{1}{|A|} \neq \bar{0}$, thus A is invertible. Hence $GL(n, \mathbb{Z}_p)$ is a group. Similarly, $SL(n, \mathbb{Z}_p)$ is a group.

(2) For any $A \in GL(n, \mathbb{Z}_p)$, $A = (\alpha_1, ..., \alpha_n)$ where $\alpha_i \in \mathbb{Z}_p{}^n, 1 \leq i \leq n$, and $\alpha_1, \alpha_2, ..., \alpha_n$ are linear independent. Take $\alpha_1 \neq 0$, then there are $p^n - 1$ choice of α_1. Given α_1, choose α_2 such that α_1, α_2 are independent. While the vector which is linear dependent with α_1 has the formal $k\alpha_1$ where $k \in \mathbb{Z}_p$, there are P choice. Hence there are $p^n - p$ choice of α_2. Repeat this process, if we have selected $\alpha_1, \alpha_2, ..., \alpha_k, (k < n)$, then the vector which is linear dependent with $\alpha_1, ..., \alpha_k$ has the formal $\sum_{i=1}^{k} x_i \alpha_i$ where $x_i \in \mathbb{Z}_p, 1 \leq i \leq k$, there are p^k choice. Thus there are $p^n - p^k$ choice of α_{k+1}. Hence $|GL(n, \mathbb{Z}_p)| = (p^n - 1)(p^n - p)...(p^n - p^{n-1})$.

9. $|UT(n, \mathbb{Z}_p)| = p^{\frac{n(n-1)}{2}}$. Similar to Exercise 1.4.7, we could choose first $n-1$ column vectors of $A \in SL(n, \mathbb{Z}_p)$, and then choose α_n such that $|A| = \bar{1}$. Then the determination is $k, k = 1, 2..., p-1$ if $k\alpha_n$ is substituted for α_n. Hence $(p-1)|SL(n, \mathbb{Z}_p)| = |GL(n, \mathbb{Z}_p)|$, thus $|SL(n, \mathbb{Z}_p)| = \frac{(p^n-1)(p^n-p)...(p^n-p^{n-1})}{p-1} = (p^n-1)...(p^n-p^{n-2})p^{n-1} = p^{\frac{(n-1)n}{2}}(p^n-1)...(p^2-1)$. While $p \nmid p^k - 1$ for $k = 2, ...n$, therefore $UT(n, \mathbb{Z}_p)$ is a Sylow p-subgroup of $SL(n, \mathbb{Z}_p)$. Since $|GL(n, \mathbb{Z}_p)| = (p^n-1)(p^n-p)...(p^n-p^{n-1}) = p^{\frac{(n-1)n}{2}}(p^n-1)...(p^2-1)(p-1)$, $UT(n, \mathbb{Z}_p)$ is a Sylow p-subgroup of $GL(n, \mathbb{Z}_p)$.

10. Since $aN = Na$ for any $a \in G$, $PN = NP \leq G$, we can get $[NP : P] = [N : P \cap N]$. Because $p \nmid [G : P]$ and $[G : P] = [G : NP][NP : P]$, $p \nmid [N : N \cap P]$. While $|P| = [P : N \cap P]|N \cap P|$, hence $|N \cap P| = p^s$. But $|N| = [N : N \cap P]p^s$, $p \nmid [N : N \cap P]$, therefore $N \cap P$ is a Sylow p-subgroup of N. For example, $G = A_{12}, P = \{(1), (12)(34), (13)(24), (14)(23)\}, N =< (123) >$, then $N \cap P = \{(1)\}$ is not a Sylow subgroup.

11. It is obvious that $N_G(N_G(P)) \supseteq N_G(P)$. For any $a \in N_G(N_G(P))$, then $aN_G(P)a^{-1} = N_G(P)$, hence $aPa^{-1} \subseteq aN_G(P)a^{-1} = N_G(P)$. Since P is a Sylow subgroup of G, P is a Sylow subgroup of $N_G(P)$, thus aPa^{-1} is a Sylow subgroup of $N_G(P)$, therefore there exists $b \in N_G(P)$ such that $aPa^{-1} = bPb^{-1} = P$. Whence $a \in N_G(P)$, and $N_G(N_G(P)) = N_G(P)$ for the arbitrary of a.