1 Groups
1.3 The action of a group on a set

1. (1) It is obvious that $G^S \neq \emptyset$. For any $f_1, f_2, f_3 \in G^S$ and any $s \in S$, $((f_1f_2)f_3)(s) = (f_1f_2)(s)f_3(s) = f_1(s)f_2(s)f_3(s) = (f_1(f_2f_3))(s)$, therefore $(f_1f_2)f_3 = f_1(f_2f_3)$. Define $h(s) = e$ where e is the identity of G, then $(hf)(s) = ef(s) = f(s) = (fh)(s)$, therefore h is an identity of G^S. Define $g(s) = f(s)^{-1}$, then $(gf)(s) = g(s)f(s) = e = (fg)(s)$, therefore f is invertible. Hence G^S is a group.

   (2) For all $f \in G^S$ and $h_1, h_2 \in H$, for any $s \in S$, since S is an H-set, $(ef)(s) = f(e^{-1}s) = f(s)$ and $((h_1h_2)f)(s) = f((h_1h_2)^{-1}(s)) = f({h_2}^{-1}({h_1}^{-1}s)) = (h_2f)(h-1^{-1}s) = (h_1(h_2f))(s)$, therefore $ef = f$ and $(h_1h_2)f = h_1(h_2f)$. Hence G^S is an H-set.

2. For any $a \in C_G(H)$, $ha = ah$ for any $h \in H$, then $a^{-1}ha = h$, therefore $a \in N_G(H)$. Hence $C_G(H) \subseteq N_G(H) \subseteq G$. For any $a, b \in C_G(H)$, $(a^{-1}b)h(a^{-1}b) = b^{-1}aha^{-1}b = h$, therefore $C_G(H)$ is a subgroup of $N_G(H)$ and G. For any $a, b \in N_G(H)$, $(a^{-1}b)H(a^{-1}b) = b^{-1}aHa^{-1}b = H$, therefore $N_G(H)$ is a subgroup of G.

3. Assume $A \in C(SL(n, \mathbb{P}))$, then $E_{i,j}(\lambda)A = AE_{i,j}(\lambda)$, therefore the i_{th} row of $E_{i,j}(\lambda)A$ is $a_{i,1} + \lambda a_{j,1}, ..., a_{i,n} + \lambda a_{j,n}$, but the i_{th} row of $AE_{i,j}(\lambda)$ is $a_{i,1}, ..., a_{i,i-1}, a_{i,j} + \lambda a_{i,i}, ..., a_{i,n}$, when $\lambda \neq 0$, then $\lambda a_{j,1} = 0, ..., a_{i,j} + \lambda a_{j,j} = a_{i,j} + \lambda a_{i,i}, ..., \lambda a_{j,1} = 0$, therefore $a_{jk} = 0$ where $k \neq j$ and $a_{i,i} = a_{j,j}$. For the arbitrary of A, therefore A is a diagonal matrix. Hence $C(SL(n, \mathbb{P})) = \{aE | a^n = 1\}$. Since $C(SL(n, \mathbb{P})) \subseteq C(GL(n, \mathbb{P}))$, $C(GL(n, \mathbb{P})) \subseteq \{aE | a \in \mathbb{P}*\}$, while $\{aE | a \in \mathbb{P}*\} \subseteq C(GL(n, \mathbb{P}))$, hence $C(GL(n, \mathbb{P})) = \{aE | a \in \mathbb{P}*\}$.

4. $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, it is obvious that $\{\pm 1\} \subseteq C(Q_8)$. While $(\pm i)j \neq j(\pm i)$, therefore $\pm i \notin C(Q_8)$. Similarly, $\pm j, \pm k \notin C(Q_8)$. Hence $C(Q_8) = \{\pm 1\}$.

5. Define $\varphi : \{hK | h \in H\} \to \{h(H \cap K) | h \in H\}$, $\varphi(hK) = h(H \cap K)$, if $h_1 = h_2k$, then $k = {h_2}^{-1}h_1 \in H \cap K$, therefore $h_1(H \cap K) = h_2(H \cap K)$, this means that φ is well defined. It is obvious that φ is surjective. If $h_1(H \cap K) = h_2(H \cap K)$, then ${h_1}^{-1}h_2 \in H \cap K$, therefore ${h_1}^{-1}h_2 \in K$, thus $h_1K = h_2K$, this means that φ is injective. Hence $|\{hK | h \in H\}| = |\{h(H \cap K) | h | inH\}| \leq [G : K]$ where $|\{hK | h \in H\}|$ is the number of the left coset of HK. Similarly, $|\{Hk | k \in K\}| = |K/H \cap K| \leq [G : H]$. In addition, $[G : H][H : H \cap K] = [G : H \cap K] = [G : K][K : H \cap K]$, since $([G : H], [G : K]) = 1$, $[G : H] || \{Hk | k \in K\}|$, but $|\{Hk | k \in K\}| \leq [G : H] < \infty$, therefore $\{Hk | k \in K\} = G/H$. For any $g \in G$, $g \in Hk$ for some $k \in K$, thus $G \subseteq HK \subseteq G$, hence $G = HK$.

6. $C_G(a) = \{b \in G | ba = ab\} = \{b \in G | bab^{-1} = a\} = G_a$. When $|G| < \infty$, according to Proposition 1.3.5, $|G| = |G \cdot a||G_a| = |G \cdot a||C_G(a)|$ for

any $a \in G$, therefore $|G \cdot a| = \frac{|G|}{|C_G(a)|}$. According to Theorem 1.2.3, $S_n \cdot (i_1, ..., i_k) = \{\sigma(i_1, ..., i_k)\sigma^{-1} | \sigma \in S_n\} = (\sigma(i_1), ..., \sigma(i_k) | \sigma \in S_n)$, take $(j_1, ..., j_k)$ a arrange of any k numbers from $1, ..., n$, construct $\sigma \in S_n$ such that $\sigma(i_t) = j_t, (t = 1, ..., k)$, then $(j_1, ..., j_k) = \sigma(i_1, ..., i_k)\sigma^{-1}$. Hence the conjugacy class of k-cyclic $(i_1, ..., i_k)$ in S_n is all k-cyclic $(j_1, ..., j_k)$ in S_n.

7. For any resolution $n = n_1 + n_2 + ... + n_k$ where $n_1 \geq n_2 \geq ... \geq n_k \geq 1$. Take $\sigma_{n_1,n_2,...,n_k} = (1, 2, ..., n_1)(n_1+1, ..., n_1+n_2)...(n_1+n_2+...+n_{k-1}+1, ..., n_1+n_2+...+n_k)$ is a product of $n_1, n_2, ..., n_k$-cyclic, since for any $\tau \in S_n$, $\tau\sigma_{n_1,n_2,...,n_k}\tau^{-1} = \tau(1, 2, ..., n_1)\tau^{-1}\tau(n_1+1, ..., n_1+n_2)\tau^{-1}...\tau(n_1+n_2+...+n_{k-1}+1, ..., n_1+n_2+...+n_k)\tau^{-1}$ is still a product of $n_1, n_2, ..., n_k$-cyclic. Moreover, any a product of $n_1, n_2, ..., n_k$-cyclic is conjugate with $\sigma_{n_1,n_2,...,n_k}$. Hence the class number of S_n is the resolution number of n.

8. Considering $G \times G \to G$, $(g, h) \to ghg^{-1}$.

   (1) $|G| = \sum_{i=1}^{n} |\overline{x_i}| = \sum_{i=1}^{n} \frac{|G|}{|C_G(x_i)|} = \sum_{i=1}^{n} [G : C_G(x_i)]$.

   (2) $|\{gKg^{-1} | g \in G\}| = |G \cdot K| = \frac{|G|}{|G_K|} = \frac{|G|}{|N_G(K)|} = [G : N_G(K)]$.

9. Considering $G \times G \to G$, $(g, h) \to ghg^{-1}$, then $|G \cdot g| = 1 \Leftrightarrow G \cdot g = \{aga^{-1} | a \in G\} = \{g\} \Leftrightarrow g \in C(G)$, therefore $p^n = |G| = \sum_{i=1}^{r} |G \cdot g_i| + |C(G)|$ where $|C(G| > 1$. Moreover, $|G \cdot g_i| = \frac{|G|}{|G_{g_i}|}$, thus $p | C(G)$, but $C(G) \leq G$, hence $|C(G)| = p^s$ where $s \geq 1$. Similarly, $|S| = \sum_{i=1}^{r} |G \cdot x_i| + |\{x \in S | gx = xforanyg \in G\}$ where $|G \cdot x_i| = p^{n_i}, n_i \geq 1$, $p \nmid \{x \in S | gx = xforanyg \in G\}$ for $p \nmid |S|$, hence $\{x \in S | gx = xforanyg \in G\} \neq \emptyset$, i.e. there is an element $x \in S$ such that $gx = x$ for any $g \in G$.

10. Consider $A = \{(g, x) | gx = x\} \subseteq G \times X$

    (a) For any given $g \in G$, $X^g = \{(g, x) | gx = x, x \in X\}$, thus $|A| = \sum_{g \in G} |X^g|$. While for any given $x \in X$, $G_x = \{(g, x) | gx = x, g \in G\}$, thus $|A| = \sum_{x \in X} |G_x|$. Hence $\sum_{g \in G} |X^g| = \sum_{x \in X} |G_x|$.

    (b) Since $|G_x| = \frac{|G|}{|G \cdot x|}$, $\sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|G \cdot x| = |G| \cdot \sum_{x \in X} \frac{1}{|G \cdot x|}}$. If $x \in G \cdot x_i$, then $|G \cdot x| = |G \cdot x_i|$, hence $\sum_{g \in G} |X^g| = \sum_{x \in X} |G_x| = |G|(numberoforbits)$.

11. $B \backslash GL(n, \mathbb{P})/B = \{BAB | A \in GL(n, \mathbb{P})\}$, $C := \{BAB | A \in W\}$, it is obvious that $C \subseteq B \backslash GL(n, \mathbb{P})/B$. Since $GL(n, \mathbb{P})$ is generated by $d_j(\mu), T_{i,j}(\lambda)$, we only need to consider $BT_{i,j}(\lambda)B$ and $Bd_j(\mu))B$. In addition, $BT_{i,j}(\lambda)B \subseteq BEB$ and $Bd_j(\mu))B \subseteq BEB$, therefore $B \backslash GL(n, \mathbb{P})/B \subseteq C$. Hence $B \backslash GL(n, \mathbb{P})/B = \{BAB | A \in W\}$.

12. For any $g \in G$, $H \times HgH \to HgH$, $(h, agb) \to hagb$ and $H \times HgH \to HgH$, $(h, agb) \to agbh^{-1}$, then $HgH = \cup_{i=1}^{s} Hgy_i = \cup_{i=1}^{s} x_i gH$, take $z_i = x_i g y_i$, then $HgH = \cup_{i=1}^{s} Hz_i = \cup_{i=1}^{s} z_i H$. Hence there is a subset $\{z_1, ..., z_r\}$ of G such that $H \backslash G = \cup_{g \in G} HgH = \{Hz_1, ..., Hz_r\}$ and $G/H = \cup_{g \in G} HgH = \{z_1 H, ..., z_r H\}$.

13. Suppose $G/H = \{g_iH | i \in I\}$ and if $i, i' \in I$, $g_iH \neq g'_iH$, suppose $H/K = \{h_jK | j \in J\}$ and if $j, j' \in J$, $h_jK \neq h'_jK$. Considering $X = \{g_ih_jK | (i,j) \in I \times J\}$, then for any $g \in G$, $gH = g_iH$ for some $i \in I$, thus ${g_i}^{-1}g \in H$, then there exists $j \in J$ such that ${g_i}^{-1}gK = h_jK$, therefore $gK = g_ih_jK$, this means $G/K \subseteq X$, hence $G/K = X$. If $g_ih_jK = g'_ih'_jK$, then $g_ih_j = g'_ih'_jk, k \in K \subseteq H$, thus $g'_ig_i = (h'_jk){h_j}^{-1} \in H$, then $g'_iH = g_iH$, therefore $i = i'$. When $i = i'$, $h_jK = h'_jK$ for $g_ih_jK = g'_ih'_jK$, then $j = j'$. Hence the element in X is differ from each other, then $[G : K] = |X| = |I \times J| = |I||J| = [G : H]H : K$.

14. (1) It is obvious that $G \neq \emptyset$. For any $(g_1, g_2), (h_1, h_2), (f_1, f_2) \in G$, $((g_1, g_2)(h_1, h_2))(f_1, f_2) = (g_1h_1, g_2h_2)(f_1, f_2) = (g_1h_1f_1, g_2h_2f_2) = (g_1, g_2)((h_1, h_2)(f_1, f_2))$; $(g_1, g_2)(e_1, e_2) = (g_1, g_2) = (e_1, e_2)(g_1, g_2)$ where e_1, e_2 is the identity of $GL(m, \mathbb{P}), GL(n, \mathbb{P})$ respectively; and $(g_1, g_2)({g_1}^{-1}, {g_2}^{-1}) = (e_1, e_2) = ({g_1}^{-1}, {g_2}^{-1})(g_1, g_2)$. Hence G is a group.

    (2) Since any $A \in GL(m, \mathbb{P}), B \in GL(n, \mathbb{P})$ is similar to a diagonal matrix, $X = \cap_{A \in Z} G \cdot A$ where $Z = \{(g_1, g_2) | g_1 \in \{e_{11}, ..., \sum_{i=1}^m e_{ii}\}, g_2 \in \{e_{11}, ..., \sum_{i=1}^n e_{ii}\}\}$.

15. Suppose $X = \{x_1, x_2, x_3, x_4, x_5\}$, and $G \cdot x_1 = \{x_1, x_2, x_3\}$, $G \cdot x_4 = \{x_4, x_5\}$. Define $\varphi : G \to S_5$, for any $g \in G$, if $\{gx_1, .., gx_5\} = \{x_{i_1}, ..., x_{i_5}\}$, i.e. $gx_k = x_{i_k}, k = 1, ..., 5$,then $\varphi(g) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_1 & i_2 & i_3 & i_4 & i_5 \end{pmatrix} \in S_5$. If $gx_k = g'x_k, k = 1, 2, ..., 5$, then $g^{-1}g'x_k = x_k, k = 1, 2, ..., 5$, thus $g^{-1}g' = e$, then $g = g'$, i.e. φ is injective. It is easy to verify $\varphi(gg') = \varphi(g)\varphi(g')$, therefore we can consider G as a subgroup of S_5, then $G_{x_1} \leq G \leq S_5, G_{x_4} \leq G \leq S_5$, $[G : G_{x_1}] = |G \cdot x_1| = 3, [G : G_{x_4}] = 2$, $120 = [S_5 : G][G : G_{x_1}]|G_{x_1}|$. In addition, $G \cdot x_1 = \{x_1, x_2, x_3\}$, then $\varphi(G) = \{1, 2, 3\}$, therefore G is a subgroup of S_3 which is generated by $\{(12), (13), (23), (1), (123), (132)\}$, while $<(12)>, <(13)>, <(23)>, <(132)>, s_3, <(1)>$ is all subgroups of S_3 and $G \cdot x_1 = \{x_1, x_2, x_3\}$, therefore $G \cdot x_1 = S_3 or <(123)>$. Considering $G \cdot x_4 = \{x_4, x_5\}$, then G contains generator (45), hence there are two possibility:$<(123), (45)> \simeq \mathbb{Z}_3 \times \mathbb{Z}_2$ and $<S_3 \cup (45)> \simeq S_3 \times S_2$.

16. If G is a finite group, it is obvious that G has finitely many subgroups.Conversely, suppose A is consist of all subgroups of G, consider $\varphi : G \times A \to A, (g, H) \to gHg^{-1}$, then $\varphi : G \to Sym(A)$, thus $|Im\varphi| \leq N!$ where N is the cardinal number of A, while $Ker\varphi = \{g \in G | \varphi(g) = id_A\}$ is a subgroup of G. Since $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ for any $g_1, g_2 \in G$, then φ induces a monomorphism $\overline{\varphi} : \{gKer\varphi | g \in G\} \to Sym(A)$, therefore $[G : Ker\varphi] \leq N!$. We proof $Ker\varphi$ is finite as follow. It is obvious that $Ker\varphi$ only has finite subgroup, and for any $a, b \in Ker\varphi$, since $a < b > a^{-1} = < b >$, $aba^{-1} = b^r$ for some r. For any $a \in Ker\varphi, |a| < n$, take $a_1 \neq e$, If $< a_1 > \neq Ker\varphi$, take $a_2 \in Ker\varphi \backslash < a_1 >$, then $< a_1 > \subsetneqq < a_1, a_2 >$.

If $Ker\varphi \neq < a_1, a_2 >$, take $a_3 \in Ker\varphi$, repeat the above process, then there exists n such that $Ker\varphi =< a_1, a_2, ..., a_n >$. By induction on n to verify $Ker\varphi$ is finite. $n = 1$, the claim is true. If it is true for $n = k$, for $n = k + 1$, since $a_n a_i {a_n}^{-1} = {a_i}^{r_i}$, $a_n a_i = {a_i}^{r_i} a_n$, then $< a_1, a_2, ..., a_n >= \{a{a_n}^k | a \in < a_1, ..., a_{n-1} >, 0 \leq k \leq |a_n| < \infty\}$, thus $| < a_1, ..., a_n > | \leq | < a_1, .., a_{n-1} > | \cdot |a_n| < \infty$, then $|G| = [G : Ker\varphi]|Ker\varphi|$. Hence G is a finite group.

17. Suppose $\sigma = (456)(567)(671)(123)(234)(456)$, then $\sigma(1) = 2, \sigma(2) = 7$, and $\sigma(7) = 1, \sigma(3) = 5, \sigma(5) = 6, \sigma(6) = 3, \sigma(4) = 4$, therefore $\sigma = (127)(356)$.

18. If $(\varepsilon_1, ..., \varepsilon_n) = (e_1, ..., e_n)M$ where $M = (a_{ij}) \in GL(n, \mathbb{C})$ and $M^{-1} = (b_{ij})$, suppose $(\varepsilon_1*, ..., \varepsilon_n*) = (e_1*, ..., e_n*)(c_{ij})$, $(c_{ij})^{-1} = (d_{ij})$, then $\varepsilon_i * (\varepsilon_j) = (\sum_{k=1}^{n} c_{ki} e_k *)(\sum_{l=1}^{n} a_{lj} el) = \sum_{k=1}^{n} c_{ki} a_{kj} = \delta_{ij}$, thus $(c_{ij})^T M = E$, i.e. $(c_{ij}) = (M^{-1})^T$, then

$$\begin{aligned} \sum_{i=1}^{n} \varepsilon_i * (g\varepsilon_i) &= \sum_{i=1}^{n} (\sum_{k=1}^{n} c_{ki} e_k *)(g \sum_{l=1}^{n} a_{li} e_l) \\ &= \sum_{i=1}^{n} \sum_{k=1}^{n} \sum_{l=1}^{n} c_{ki} a_{li} e_k * g e_i \\ &= \sum_{k=1}^{n} e_k * (g e_k) \end{aligned} \tag{1}$$

Hence $r_M(g) = \sum_{i=1}^{n} e *_i (ge_i)$ is independent of choice of basis. Given $g \in G$, suppose $g(e_1, .., e_n) = (e_1, ., e_n)(x_{ij})$, then $r_M(g) = \sum_{k=1}^{n} x_{kk} = tr((x_{ij}))$. For any $h \in G$, if $h(e_1, ..., e_n) = (e_1, ..., e_n)N$, then $(h^{-1}gh)(e_1, ..., e_n) = (e_1, ..., e_n)(N^{-1}(x_{ij})N)$, therefore $r_M(h^{-1}gh) = tr(N^{-1}(x_{ij})N) = tr((x_{ij})) = r_M(g)$.

19. According to the definition, $L_g : V \to V$, $(g, v) \to g \cdot v$, is a linear map. $e \cdot v = v$, if $g, h \in G$, then $v = \sum k_i e_{g_i}$, thus $g(hv) = \sum k_i e_{g(hg_i)} = \sum k_i e_{(gh)g_i} = (gh) \cdot v$, hence V is a linear representation of G. $\overline{(1)} = \{(1)\}$, $\overline{(12)} = \{(12), (23), (13)\}$, $\overline{(123)} = \{(123), (132)\}$ are all conjugacy classes of S_3, then

	$\overline{(1)}$	$\overline{(12)}$	$\overline{(123)}$
r_V	6	0	0

, hence

$$r_V(g) = \sum_{i=1}^{6} e_i * (g e_{g_i}) = \sum_{i=1}^{6} e_i * (e_{gg_i}) = \begin{cases} 6 & g = id \\ 0 & g \neq id \end{cases}$$