1 Groups

1.2 Subgroups

1. ($\Rightarrow$) Assume that $G =< a >$ is a cyclic group, H is a nontrivial subgroup of G. If $a^n \in H$, then $a^{-n} \in H$. But $a^0 = e$ and H is nontrivial, $\exists$ a minimum positive integer n, s.t., $a^n \in H, \forall a^m \in H, m = kn + r, 0 \leq r \leq n$. From $a^m = a^{kn} \cdot a^r$ we see that $a^r = (a^{kn})^{-1} \cdot a^m \in H$. So $r = 0$ implies that $H =< a^n >$. $(a^n)^s = (a^n)^t \Leftrightarrow a^{ns} = a^{nt} \Leftrightarrow s = t$, hence H is an infinite cyclic group.

   ($\Leftarrow$)$\forall a, b \in G$, $< a, b >= G$, or $< a, b > \subsetneqq G$. If $ab \neq ba$, then $< a, b >= G$ (For $< a, b > \subsetneqq G$ is cyclic). So

   $$a^2b^2 = b^2a^2, ab^2 = b^2a, a^2b = ba^2, ab^3 = b^3a.$$

   Hence we have that

   $$(ab)^2 = abab = ab^{-1}ab^3 = ab^2a = a^2b^2.$$

   So $ab = ba$, hence G is abelian.

   From the fundamental theorem of abelian group, we see that

   $$G \cong \overbrace{\mathbb{Z} \bigoplus \cdots \bigoplus \mathbb{Z}}^{m} \bigoplus \mathbb{Z}_{p_1} \bigoplus \cdots \bigoplus \mathbb{Z}_{p_r}, (m \geq 1, r \geq 0).$$

   If $r > 0$, then $2\mathbb{Z} \bigoplus \mathbb{Z}_p$ is an infinite cyclic group, this is a contradiction. Hence $r \leq 0$, *i.e.* $r = 0$. If $m > 1$, then $2\mathbb{Z} \bigoplus 2\mathbb{Z}$ is an infinite cyclic group. this is also a contradiction. Hence $m \leq 1$, *i.e.* $m = 1$. So $G \cong \mathbb{Z}$, hence G is an infinite cyclic group.

2. According to the definition of G

   $$G = \{a_1^{m_1} a_2^{m_2} \cdots a_n^{m_n} | a_i \in G, 0 \leq m_i \leq |a_i|\}.$$

   Hence $|G| = \displaystyle\prod_{i=1}^{n} |a_i| < \infty$.

3. Let $a_i = \frac{q_i}{p_i}$ and $p = [p_1, \cdots p_n]$ is the LCM.
   Then $pa_i \in \mathbb{Z}$ and $(pa_1, \cdots, pa_n) = q$ is the GCD. So $\exists k_i \in \mathbb{Z}$, *s.t.* $a_i = k_i \frac{q}{p}$. Hence $< a_1, \cdots, a_n > \subset < \frac{q}{p} >$ and $\mu_1 pa_1 + \cdots + \mu_n pa_n = q$. From this we have that $\mu_1 a_1 + \cdots + \mu_n a_n = \frac{q}{p}$, so $< \frac{q}{p} > \subset < a_1, \cdots, a_n >$. Hence $< a_1, \cdots, a_n >=< \frac{q}{p} >$ is the cyclic subgroup of $(\mathbb{Q}, +)$.

4. (a) Let $|a| = k_1$, $|b| = k_2$, $|ab| = t_1$, and $|ba| = t_2$. From $(ab)^{t_1} = e$ we have that $(ba)^{t_1} = a^{-1}(ab)^{t_1}a = e$. So $t_1 | t_2$. Similarly from $(ba)^{t_2} = e$ we have that $(ab)^{t_2} = a(ba)^{t_2}a^{-1} = e$. So $t_2 | t_1$. Hence $t_1 = t_2$.

   (b) When $|ab| = \infty$, if $|ba| = n < \infty$, then $|ab| = n$, this is a contradiction. Hence $|ba| = \infty$.

5. Let $G =< x >$, if $G =< a >$, then $a = x^k$. But $< x^k >=< x >$, so $\exists l$ $s.t.$ $(x^k)^l = x$. Hence $kl = 12n = 1$, $i.e.$ $(k, 12) = 1$, from this we see that $k = 1, 5, 7, 11$. Hence the answer is 4.

6. $H \leqslant G$, $K \leqslant G$, $HK = \{ab|a \in H, b \in K\}$
   ($\Rightarrow$) If HK is a subgroup of G, then $ba = (a^{-1}b^{-1})^{-1} \in HK$. So $KH \subseteq HK$.
   Let $a'b' = (ab)^{-1}$. From $(ab)^{-1} \in HK$ we have that $ab = b'^{-1}a'^{-1} \in KH$, so $HK \subseteq KH$. Hence $HK = KH$.
   ($\Leftarrow$) If $HK = KH$, then $\forall ab \in HK$, $b^{-1}a^{-1} \in KH = HK$ and
   $$(HK)(HK) = H(KH)K = HHKK \subset HK.$$
   So the product of any two elements in HK belongs to HK, and the inverse of any element in HK belongs to HK. Hence HK is a subgroup of G.

7. It is clear that $< (12), (13), \cdots, (1n) >\subseteq S_n$. Since $(1, i)(i, j)(1, i) = (1, j)$, $(i, j) = (1, i)(1, j)(1, i)$. Especially $\sigma_i = (i, i + 1) = (1, i)(1, i + 1)(1, i) \in< (12), \cdots, (1n) >$, so
   $$S_n =< \sigma_1, \cdots, \sigma_n >\subseteq< (12), (13), \cdots, (1n) > .$$
   Hence $S_n =< (12), (13), \cdots, (1n) >$.

8. ($\Rightarrow$) Obviously.
   ($\Leftarrow$) Since
   $$G =< a_1, \cdots, a_n >= \{a_{i_1}^{\varepsilon_{i_1}} a_{i_2}^{\varepsilon_{i_2}} \cdots |a_{i_1} \in \{a_1, \cdots, a_n\}, \varepsilon_i = \pm 1\}$$
   if $a_ia_j = a_ja_i, \forall 1 \leq i, j \leq n$, then
   $$(a_{i_1}^{\varepsilon_{i_1}} a_{i_2}^{\varepsilon_{i_2}} \cdots a_{i_k}^{\varepsilon_{i_k}})(a_{j_1}^{\varepsilon_{j_1}} a_{j_2}^{\varepsilon_{j_2}} \cdots a_{j_l}^{\varepsilon_{j_l}}) = (a_{j_1}^{\varepsilon_{j_1}} a_{j_2}^{\varepsilon_{j_2}} \cdots a_{j_l}^{\varepsilon_{j_l}})(a_{i_1}^{\varepsilon_{i_1}} a_{i_2}^{\varepsilon_{i_2}} \cdots a_{i_k}^{\varepsilon_{i_k}}).$$

9. Computations show that $A^2 = -E$, $A^3 = -A$, $A^4 = E$, $B^2 = -E$, $B^3 = -B$, $B^4 = E$, $A^2B^2 = E$, $A^2B = -B$, $A^3B = -AB$, $AB^2 = -A$, $AB^3 = -AB$. So
   $$\mathbb{Q}_8 = \{E, -E, A, -A, B, -B, AB, -AB\}.$$
   Denote $E = 1, A = i, B = j, AB = k$, then $\mathbb{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

10. Computations show that $A^2 = -E$, $A^3 = -A$, $A^2B = -B$, $A^3B = -AB$, $B^2 = E$, So
    $$D_4^* = \{E, -E, A, -A, B, -B, AB, -AB\}.$$
    Since $AB = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \neq \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = BA = -AB$, hence D_4^* is a noncommutative group of order 8.

11. For any element in $\mathbb{Z}(p^\infty) = \{\frac{a}{p^n} + \mathbb{Z} | a \in \mathbb{Z}, n \in \mathbb{N}\}$, if $a = a_1 p^m, (a_1, p) = 1$, then $\frac{a}{p^n} + \mathbb{Z} = \frac{a_1}{p^{n+m}} + \mathbb{Z}$. Hence we can assume that $(a, p) = 1$. So $\exists u, v \in \mathbb{Z}$, *s.t.* $ua + vp^n = 1$ and

$$\frac{1}{p^n} + \mathbb{Z} = \frac{ua + vp^n}{p^n} + \mathbb{Z} = \frac{ua}{p^n} + \mathbb{Z} = u(\frac{a}{p^n} + \mathbb{Z}).$$

For any subgroup H of $\mathbb{Z}(p^\infty)$, if $\frac{a}{p^n} + \mathbb{Z} \in H, (a,p) = 1$, then $\frac{1}{p^n} + \mathbb{Z} \in H$, hence $H =< \frac{1}{p^{n_i}} + \mathbb{Z} | i \in X >, X \subseteq \mathbb{N}$.
If X is finite, let $n = \max_{i \in X}\{n_i\}$, then $H =< \frac{1}{p^n} + \mathbb{Z} >$, so $|H| = p^n$ and $\forall m < n, < \frac{1}{p^m} + \mathbb{Z} > \subseteq < \frac{1}{p^n} + \mathbb{Z} >$.
If X is infinite, then $\forall n \in \mathbb{N}, \exists m \in X, s.t., n \leq m$.
Since $\frac{1}{p^n} + \mathbb{Z} \in < \frac{1}{p^m} + \mathbb{Z} > \subseteq H$, $\forall n \in N$, $\frac{1}{p^n} + \mathbb{Z} \in H$. Hence

$$\mathbb{Z}(p^\infty) = \{\frac{a}{p^n} + \mathbb{Z} | n \in \mathbb{N}\}.$$

If H, N is finite, then $H =< \frac{1}{p^m} + \mathbb{Z} >, N =< \frac{1}{p^n} + \mathbb{Z} >$. If $m \geq n$, then $H \geq N$. If $m \leq n$, then $H \leq N$. If H is finite, $N = \mathbb{Z}(p^\infty)$, then $H \leq N$. If N is finite, $H = \mathbb{Z}(p^\infty)$, then $N \leq H$. If $H = N = \mathbb{Z}(p^\infty)$, then $H = N$.

12. If $H \subsetneqq G$, then $\exists a \in G$ and $a \notin H$. So $a^{-1} \in G$ and hence $e \in G$. $\forall h \in H, ah \notin H$ (otherwise if $ah \in H$, then $a = ahh^{-1} \in H$. This is a contradiction) so $ah \in < G \backslash H >$ and hence $h = a^{-1}ah \in < G \backslash H >$, then we see that $H \subseteq < G \backslash H >$ and $G \subseteq < G \backslash H >$, hence $G =< G \backslash H >$.

13. From $G = H \bigcup K$ is a group, we have that $H \subseteq K$ or $K \subseteq H$. If $H \neq G$, then $H \subsetneqq G$. Since $G = H \bigcup K$, $K = G$. Similarly if $K \neq G$, then $H = G$.

14. Let

$$A =< \{T_{ij}(\lambda), d_i(\mu) | \lambda, \mu \in \mathbb{P}^*, 1 \leq i \neq j \leq n\} >,$$
$$B =< \{T_{ij}(\lambda) | \lambda \in \mathbb{P}^*, 1 \leq i \neq j \leq n\} > .$$

It is clear that $A \subseteq GL(n, \mathbb{P})$. Next we show the other side. $E(i,j) = d_i(-1)T_{ij}(1)T_{jl}(-1)T_{lj}(1)$, because $E = d_i(1)$ and $\forall Q_i \in GL(n, \mathbb{P})$ can be reduced to E by a sequence of elementary row or column operations, which are generated by $T_{ij}(\lambda), d_i(\mu)$, so $GL(n, \mathbb{P}) \subseteq A$. Hence $A = GL(n, \mathbb{P})$.
Since $|T_{ij}(\lambda)| = 1$, it is clear that $B \subseteq SL(n, \mathbb{P})$.
$\forall Q_i \in SL(n, \mathbb{P})$ can be reduced to E by a sequence of elementary row or column operations, whose determinations are 1. When $|d_i(\mu)| = 1$, $\mu = 1$, *i.e.* $d_i(\mu) = E$. So $SL(n, \mathbb{P}) \subseteq B$, hence $SL(n, \mathbb{P}) = B$.

15. If $c = 0$, then $ad = 1$. So $a = d = 1$ or $a = d = -1$, $\therefore \frac{b}{d} \in \mathbb{Z}$
$\therefore \frac{az+b}{d} = z + \frac{b}{d} = \tau^{\frac{a}{c}}(z)$
If $c \neq 0$ and $d = 0$, then $-bc = 1$. $\therefore \frac{a}{c} \in \mathbb{Z}$, $\therefore \frac{az+b}{cz} = \frac{a}{c} + \frac{b}{c}\frac{1}{z} = \frac{a}{c} - \frac{1}{z} = \tau^{\frac{a}{c}}\sigma(z)$.
If $c \neq 0, d \neq 0$ and $b = 0$, then $\frac{az}{cz+d} = \frac{1}{\frac{cz+d}{az}} = \frac{1}{\frac{c}{a} + \frac{1}{z}} = \sigma\tau^{\frac{c}{d}}\sigma(-z)$.

If $c \neq 0, d \neq 0, b \neq 0$ and $a = 0$, then $\frac{b}{cz+d} = \frac{-1}{z-\frac{d}{b}} = \sigma\tau^{(\frac{-a}{b})}(z)$. If $c \neq 0, d \neq 0, b \neq 0$ and $a \neq 0$, then $\frac{az+b}{cz+d} = \frac{a(z+k_1)+b_1}{c(z+k_1)+d_1} = \frac{ay_1+b_1}{cy_1+d_1} = \frac{a+b_1\frac{1}{y_1}}{c+d_1\frac{1}{y_1}} = \frac{a_1+b_1(\frac{1}{y_1}+k_2)}{c_1+d_1(\frac{1}{y_1}+k_2)} = \frac{a_1+b_1y_2}{c_1+d_1y_2} = \frac{a_1\frac{1}{y_2}+b_1}{c_1\frac{1}{y_2}+d_1} = \frac{a_1(\frac{1}{y_2}+k_3)+b_2}{c_1(\frac{1}{y_2}+k_3)+d_2} = \cdots$.
(Where $d = ck_1 + d_1, d_1 < d$ if $d_1 = 0$, end. $c = d_1k_2 + c_1, c_1 < d_1, d_1 = k_3c_1 + d_2, d_2 < d_1$.) Only if $c_i \neq 0$ or $d_i \neq 0$ end. Keep doing this ,there must be some $i, s.t., d_i = 0$ or $c_i = 0$. If $d_i = 0$, then

$$\frac{az+b}{cz+d} = \tau^{\frac{a_{i-1}}{c_{i-1}}}\sigma\tau^{k_{i-1}}(-\sigma)\cdots\tau^{k_1}(z).$$

If $c_i = 0$, then

$$\frac{az+b}{cz+d} = \tau^{\frac{b_i}{d_i}}\sigma\tau^{k_i}(-\sigma)\cdots\tau^{k_1}(z).$$

16. $\tau\sigma\tau^{-1} = (\tau(1), \tau(2), \cdots, \tau(n)) = (1\ n\ n-1\ n-2\ \cdots\ 2) = \sigma^{n-1}$, $\therefore \tau\sigma = \sigma^{n-1}\tau$, $\therefore \sigma^{i_1}\tau^{i_2}\sigma^{i_3}\tau^{i_4} = \sigma^{i_1}\sigma^{i_3(n-1)^{i_2}}\tau^{i_2+i_4} = \sigma^k\tau^{i_2+i_4} = \sigma^k\tau^l$. $\because \sigma^n = (1)\ \ \therefore 1 \leq k \leq n$. $\because \tau^2 = (1)\ \ \therefore 0 \leq l \leq 1, i.e., l = 0, 1$. $\therefore <\sigma, \tau> = \{\sigma^i\tau^j | 1 \leq i \leq n, j = 0, 1\}$. Hence $| <\sigma, \tau> | = 2n$.

17. (1) If $(m, n) = 1$, then $(ab)^{mn} = l$. $\therefore l | mn$. If $(ab)^l = e$, then $a^l = b^{-l}$. $\therefore (ab)^{ml} = b^{ml} = e, \therefore n | ml$. $(ab)^{nl} = a^{nl} = e, \therefore m | nl$. $\because (m, n) = 1, \therefore n | l$ and $m | l, \therefore mn | l$. Hence $mn = l$.
    (2) If $m = p_1^{s_1}p_2^{s_2}p_3^{s_3}, n = p_1^{t_1}p_2^{t_2}p_3^{t_3}$ and $s_1 \leq t_1, s_2 \geq t_2, s_3 \leq t_3$, then $[m, n] = p_1^{t_1}p_2^{s_2}p_3^{t_3}$. $\therefore |a^{p_1^{s_1}p_3^{s_3}}| = p_2^{s_2}, |b^{p_2^{t_2}}| = p_1^{t_1}p_3^{t_3}$, and $(p_2^{s_2}, p_1^{t_1}p_3^{t_3})$. Hence $|a^{p_1^{s_1}p_3^{s_3}}b^{p_2^{t_2}}| = [m, n]$.

18. Since $a^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $a^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $a^4 = E$ and $b^2 = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$, $b^3 = E$, $|a| = 4$, $|b| = 3$. $ab = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$, therefore $|\lambda E - ab| = \begin{vmatrix} \lambda+1 & -1 \\ 0 & \lambda+1 \end{vmatrix} = \lambda^2 - 1$. If $|ab|$ is finite, then there exists $n \in \mathbb{N}$ such that $(ab)^n = E$, thus $\lambda^2 + 1 | \lambda^n - 1$, it is a contradiction. Hence $|ab|$ is infinite.

19. For any $a, b \in tor(G)$, $|a| = m, |b| = n$, then $(ab)^m n = e$, therefore $ord(ab) | mn$, i.e. $|ab|$ is finite, then $ab \in tor(G)$. Since $(a^{-1})^m = e$, $ord(a^{-1}) | m$, i.e. $|a^{-1}|$ is finite, then $a^{-1} \in tor(G)$. Hence $tor(G)$ is a subgroup of G.

20. According to the definition, $O(n, \mathbb{Z}) = \{A \in GL(n, \mathbb{Z}) | A^TA = E\} = \{A \in GL(n, \mathbb{Z}) | \sum_{j=1}^n a_{ij}{}^2 = 1, \sum_{k=1}^n a_{ki}a_{kj} = 0\} = \{A \in GL(n, \mathbb{Z}) | A = (a_1e_{i_1}, ..., a_ne_{i_n}), a_i \in \{1, -1\}\}$ where $(i_1...i_n)$ is a transposition of $(1...n)$.

21. According to the definition, $S_p(2n, \mathbb{R}) = \{A \in GL(2n, \mathbb{R}) | A^TJA = J$ where $J = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}$, therefore $|A^TJA| = |A||J||A| = |J|$, $|A|^2 = 1$ for $|J| \neq 0$, and $1 = Pf(J) = Pf(A^TJA) = (detA)Pf(J) = detA$.