Chapter 1

Groups

1.1 Semigroups, monoids and groups

Exercise 1.1.1. Give examples other than those in the text of semigroups and monoids that are not groups.

Answer. Semigroup: $(\mathbf{Z}_+, +)$
Monoid: $(\mathbf{Z}_+, \times)$

Exercise 1.1.2. Let G be a group (written additively), S a nonempty set, and $M(S, G)$ the set of all functions $f : S \to G$. Define addition in $M(S, G)$ as follows: $(f + g) : S \to G$ is given by $s \to f(s) + g(s) \in G$. Prove that $M(S, G)$ is a group, which is abelian if G is.

Answer. Firstly we check $M(S, G)$ is a group

1. $f + g : s \mapsto f(s) + g(s) \in G$, so $f + g \in M(S, G)$
2. $(f + g) + h : s \mapsto (f(s) + g(s)) + h(s)$, G is a group, so $s \mapsto (f(s) + g(s)) + h(s) \Leftrightarrow s \mapsto f(s) + (g(s) + h(s))$, $(f + g) + h = f + (g + h)$.
3. Take the unit element as $e' : s \mapsto e$. $f + e' : s \mapsto f(s) + e'(s) = f(s) + e = f(s)$, so $f + e' = f$. Similarly, $e' + f = f$.
4. For any $f \in M(S, G)$, take $f^{-1} : s \mapsto (f(s))^{-1}$, whence $f(s) + (f(s))^{-1} = (f(s))^{-1} + f(s) = e$.

In conclusion, $M(S, G)$ is a group. If G is abelian $f + g : s \mapsto f(s) + g(s) = g(s) + f(s)$, $f + g = g + f$, so $M(S, G)$ is abelian.

Exercise 1.1.3. Is it true that a semigroup which has a left identity element and in which every element has a right inverse (see Proposition 1.3) is a group?

Answer. If e is the left identity, $\forall a \in A, ea = a$ and $\forall a \in A, \exists a^{-1} s.t. aa^{-1} = e$. We have proved that if $cc = c$, then $c = e$.

$$(a^{-1}a)(a^{-1}a) = a^{-1}(aa^{-1})a = a^{-1}(ea) = a^{-1}a \Rightarrow a^{-1}a = e$$

a^{-1} is also the left inverse. $ae = a(a^{-1}a) = (aa^{-1})a = ea = a$, e is also the right identity.

Exercise 1.1.4. Write out a multiplication table for the group D_4^*.

Answer. $D_4^* = \{R, R^2, R^3, I, T_x, T_y, T_{13}, T_{24}\}$

	I	R	R^2	R^3	T_x	T_y	T_{13}	T_{24}
I	I	R	R^2	R^3	T_x	T_y	T_{13}	T_{24}
R	R	R^2	R^3	I	T_{13}	T_{24}	T_y	T_x
R^2	R^2	R^3	I	R	T_y	T_x	T_{24}	T_{13}
R^3	R^3	I	R	R^2	T_{24}	T_{13}	T_x	T_y
T_x	T_x	T_{24}	T_y	T_{13}	I	R^2	R^3	R
T_y	T_y	T_{13}	T_x	T_{24}	R^2	I	R	R^3
T_{13}	T_{13}	T_y	T_{24}	T_x	R^3	R	I	R^2
T_{24}	T_{24}	T_x	T_{13}	T_y	R	R^3	R^2	I

Exercise 1.1.5. Prove that the symmetric group on n letters, S_n, has ordrer $n!$.

Answer. For a set A whose order is n, we prove there's $n!$ different bijections by induction

1. For $n = 1$, trivial.
2. Assume $n = k$, there's $k!$ bijections. For $n = k + 1$, fix one element in A, and take $a \mapsto a$, there's k free elements, so there's $k! \cdot (k + 1)$ bijections in total.

By induction, we get the result.

Exercise 1.1.6. Write out an addition table for $Z_2 \oplus Z_2$. $Z_2 \oplus Z_2$ is called the Klein four group.

Answer. $Z_2 = \{1, 0\}$, $Z_2 \oplus Z_2 = \{(1,1), (1,0), (0,1), (0,0)\}$

	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$
$(1,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(1,0)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(0,1)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Exercise 1.1.7. If p is prime, then the nonzero elements of Z_p form a group of order $p-1$ under multiplication. Show that this statement is false if p is not prime.

Answer. For the set $Z_p\backslash\{\bar{0}\}$

1. $Z_p\backslash\{\bar{0}\}$ is obviously associative and communicative.
2. Take $\bar{1}$ as the identity element, $\forall \bar{a} \in Z_p\backslash\{\bar{0}\}, \bar{1} \times \bar{a} = \bar{a}$.
3. We prove there is a unique element $a^{-1} \in Z_p\backslash\{\bar{0}\} s.t. aa^{-1} = \bar{1}$. Assume there exists $\bar{b}, \bar{c}$ and $\bar{a} \cdot \bar{b} = \bar{k}, \bar{a} \cdot \bar{c} = \bar{k}$, then $a(b-c) \equiv 0 \mod p$. p is a prime, so $lcm(p,a) = 1, lcm(p, b-c) = 1$, so $\bar{b} = \bar{c}$. There is at most one element s.t. $\bar{a}\bar{b} = \bar{k}$. Take $\bar{b} = \bar{1}, \bar{2}, \ldots p \bar{-} 1$, $\bar{k}$ travels through $\bar{b} = \bar{1}, \bar{2}, \ldots p \bar{-} 1$. There exists an element $\bar{b} \in Z_p\backslash\{\bar{0}\}, \bar{a}\bar{b} = \bar{1}$.

$Z_p\backslash\{\bar{0}\}$ is a group. If p is not a prime, the inverse element is not always unique. Take $a|p$, there's more than one inverse element in $Z_p\backslash\{\bar{0}\}$.

Exercise 1.1.8. (a) The relation given by $a \sim b \Leftrightarrow a - b \in \mathbf{Z}$ is a congruence relation on the additive group $\mathbf{Q}$ [see Theorem 1.5].
(b) The set $\mathbf{Q}/\mathbf{Z}$ of equivalence classes is an infinite abelian group.

Answer. (a) For group $(\mathbf{Q}, +)$, $a_1 \sim b_1 \Leftrightarrow a_1 - b_1 = k_1 \in \mathbf{Z}$, $a_2 \sim b_2 \Leftrightarrow a_2 - b_2 = k_2 \in \mathbf{Z}$, so $(a_1+a_2)-(b_1+b_2) = ((k_1+b_1)+(k_2+b_2))-(b_1+b_2) = k_1 + k_2 \in \mathbf{Z}$. $a \sim b$ is a congruence relation.

(b) 1 if $a + b \geq 1$, $\bar{a} + \bar{b} = a + \bar{b} - 1$. If $a + b < 1$, $\bar{a} + \bar{b} = a \bar{+} b$.
2 $\mathbf{Q}/\mathbf{Z}$ is obviously associative and communicative.
3 Take the identity element as $\bar{0}$, $\bar{0} + \bar{a} = \bar{a}$.
4 If $\bar{a} \neq 0$, take $(\bar{a})^{-1} = 1 \bar{-} a$, then $\bar{a} + 1 \bar{-} a = \bar{0}$
so $\mathbf{Q}/\mathbf{Z}$ is a abelian group. (Infinite remains to be certified)

Exercise 1.1.9. Let p be a fixed prime. Let R_p be the set of all those rational numbers whose denominator is relatively prime to p. Let R^p be the set of rationals whose denominator is a power of $p (p^i, i > 0)$. Prove that both R_p and R^p are abelian groups under ordinary addition of rationals.

Answer. Trivial.

Exercise 1.1.10. Let p be a prime and let $Z(p^\infty)$ be the following subset of the group $\mathbf{Q}/\mathbf{Z}$:

$$Z(p^\infty) = \{a\bar{/}b \in \mathbf{Q}/\mathbf{Z} | a, b \in \mathbf{Z} \text{ and } b = p^i \text{ for some } i \geq 0\}$$

Show that $Z(p^\infty)$ is an infinite group under the addition operation of $\mathbf{Q}/\mathbf{Z}$.

Answer. $Z(p^\infty) = \{a\bar{/}b | a, b \in \mathbf{Z}, b = p^i, i \geq 0\}$. Take $a = \frac{\bar{a_1}}{b_1}$, $b = \frac{\bar{a_2}}{b_2}$. $b^{-1} = \frac{b_2 \bar{-} a_2}{b_2}$

$$\begin{aligned} a + b^{-1} = \frac{\bar{a_1}}{b_1} + \frac{b_2 \bar{-} a_2}{b_2} &= \frac{\bar{a_1}}{p^{s_1}} + \frac{p^{s_2} \bar{-} a_2}{p^{s_2}} \\ &= \frac{a_1 \cdot p^{s_2} + p^{\bar{s_1}}(p^{s_2} - a_2)}{p^{s_1+s_2}} \in Z(p^\infty) \end{aligned}$$

Therefore, $Z(p^\infty)$ is a subgroup of $\mathbf{Q}/\mathbf{Z}$. $\frac{1}{p^i} \in Z(p^\infty)$ for any $i \in \mathbf{Z}$, so $Z(p^\infty)$ is infinite, $\mathbf{Q}/\mathbf{Z}$ is also infinite.

Exercise 1.1.11. The following conditions on a group G are equivalent:

i G is abelian;
ii $(ab)^2 = a^2b^2$ for all $a, b \in G$;
iii $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$;
iv $(ab)^n = a^nb^n$ for all $n \in \mathbf{Z}$ and all $a, b \in G$;
v $(ab)^n = a^nb^n$ for three consecutive integers n and all $a, b \in G$. Show that v⇒ i is false if 'three' is replaced by 'two'.

Answer. i⇔ iii: $((ab)b^{-1})a^{-1} = (ab)(b^{-1}a^{-1}) = e$, so $(ab)^{-1} = b^{-1}a^{-1}$. If iii, $b^{-1}a^{-1} = a^{-1}b^{-1}$ for any $a, b \in G$, G is abelian. If i, G is abelian, $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$.
iv ⇒ v, iv⇒ ii and i⇒ iv are trivial.
ii⇒ i:

$$(ab)(ab) = aabb \Rightarrow a^{-1}(ab)^2b^{-1} = a^{-1}aabbb^{-1} = ba = ab$$

so G is abelian.

v $\Rightarrow$ i: $a^n b^n = (ab)^n$, $a^{n-1}b^{n-1} = (ab)^{n-1}$, $a^{n+1}b^{n+1} = (ab)^{n+1}$.

$$(b^{-1})^n(a^{-1})^n = ((ab)^n)^{-1} = ((ab)^{-1})^n$$

$$((ab)^{-1})^n(ab)^{n+1} = (b^{-1})^n ab^{n+1}$$

$$((ab)^{-1})^n(ab)^{n-1} = b^{-1}a^{-1} = (b^{-1})^n a^{-1}b^{n-1}$$

$$a = (b^{-1})^n ab^n \qquad b^{-1}a^{-1}b = (b^{-1})^n a^{-1}b^n$$

So $a^{-1} = b^{-1}a^{-1}b$, which means G is abelian.
If "three" is replaced by "two": $a^n b^n = (ab)^n$, $a^{n+1}b^{n+1} = (ab)^{n+1}$.

$$(b^{-1})^n(a^{-1})^n = ((ab)^{-1})^n \qquad a = (b^{-1})^n ab^n$$

For the group $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, taking any $a \in S_3$, we can check that $a^6 = (1)$. If $n = 6$, then $a = (b^{-1})^n ab^n$ for any $a, b \in S_3$. But S_3 is nonabelian.

Exercise 1.1.12. If G is a group, $a, b \in G$ and $bab^{-1} = a^r$ for some $r \in \mathbf{N}$, then $b^j ab^{-j} = a^{r^j}$ for all $j \in \mathbf{N}$.

Answer. $bab^{-1} = a^r$. We prove it by induction. For $j = 1$, its always true. Assume $j = k$ the equation is correct, $b^k ab^{-k} = a^{r^k}$. $ba^{r^k}b^{-1} = (a^{r^k})^{r=a^{r^{k+1}}}$. For $j = k + 1$, it's also true.

Exercise 1.1.13. If $a^2 = e$ for all elements a of a group G, then G is abelian.

Answer.

$$a^2 = e \Rightarrow a^2a^{-1} = ea^{-1} = a(aa^{-1}) = ae \Rightarrow a = a^{-1}$$

$$ab = a^{-1}b^{-1} = (ab)^{-1} = (ba)^{-1}$$

So $ab = ba \forall a, b \in G$. G is abelian.

Exercise 1.1.14. If G is a finite group of even order, then G contains an element $a \neq e$ such that $a^2 = e$.

Answer. Suppose not. $\forall a \neq e, aa \neq e \Leftrightarrow a \neq a^{-1}$. We can classify the group into some subsets. $G = \bigcup_{a \neq e} \{a, a^{-1}\} \cup \{e\}$. Notice that $\{a, a^{-1}\} \cap \{b, b^{-1}\} = \varnothing$ if $a \neq b$, so $|G| = 2n + 1$, That's contradictory!

Exercise 1.1.15. Let G be a nonempty finite set with an associative binary operation such that for all $a, b, c \in G$, $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$. Then G is a group. Show that this conclusion may be false if G is finite.

Answer. G is a semigroup. Fix $a \in G$ and take b travels through all elements in G, then ab travels through all elements in G.
There exists an element e_1 s.t. $ae_1 = a \forall a \in G$. Similarly, we can find e_2 s.t. $e_2 a = a \forall a \in G$. $e_2 e_1 = e_1 = e_2 = e$. e is the identity element of G. Easily, we can find that $\forall a \in G, \exists! a^{-1} \in G$ s.t. $a^{-1}a = aa^{-1} = e$ because $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$.
G is a group. If G is infinite, G may not be a group, for example: $(Z_+, \times)$.

Exercise 1.1.16. Let $a_1, a_2, \ldots$ be a sequence of elements in a semigroup G. Then there exists a unique function $\Psi : \mathbf{N}^* \to G$ such that $\Psi(1) = a_1, \Psi(2) = a_1 a_2, \Psi(3) = (a_1 a_2)a_3$ and for $n \geq 1$, $\Psi(n + 1) = (\Psi(n))a_{n+1}$. Note that $\Psi(n)$ is precisely the standard n product $\prod_{i=1}^{n} a_i$.

Answer. Applying the Recursion Theorem with $a = a_1, S = G$ and $f_n : G \to G$ given by $x \mapsto x a_{n+2}$ yields a function $\phi : \mathbf{N} \to G$. Let $\Psi = \phi\theta$, where $\theta : \mathbf{N}^* \to \mathbf{N}$ is given by $k \mapsto k - 1$.

1.2 Homomorphisms and subgroups

Exercise 1.2.1. If $f : G \to H$ is a homomorphism of groups, then $f(e_G) = e_H$ and $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$. Show by example that the first conclusion may be false if G, H are monoids that are not groups.

Answer. For example, $(\mathbf{Z}_+, +)$ and $(\mathbf{N}, \times)$ are monoids. Denote $f : \mathbf{Z}_+ \to \mathbf{N}$ as $f(x) = 0 \forall x \in \mathbf{Z}_+$. f is a homomorphism satisfies those conditions.

Exercise 1.2.2. A group G is abelian if and only if the map $G \to G$ given by $x \mapsto x^{-1}$ is automorphism.

Answer. If G is abelian, $f(x) = x^{-1}$ is a monomorphism and epimorphism. $f(a)f(b) = a^{-1}b^{-1} = (ab)^{-1} = f(ab)$
If $f(x) = x^{-1}$ is a isomorphism, $f(a)f(b) = a^{-1}b^{-1} = f(ab) = (ab)^{-1} = b^{-1}a^{-1} \forall a, b \in G$, so G is abelian.

Exercise 1.2.3. Let Q_8 be the group(under ordinary matrix multiplication) generated by complex matrices $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, where $i^2 = -1$. Show that Q_8 is a nonabelian group of order 8. Q_8 is called the quaternion group.

Answer. The multiply operation is associative by the difinition. $A^4 = B^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$ which is the identity element.

$$A^{-1} = A^3 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \in G \qquad B^{-1} = B^3 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \in G$$

So $\forall A^i B^j \in G$, $(A^i B^j)^{-1} \in G$. G is a group. Now we examine the order of G is 8.

$$BA = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

$$A^3 B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix}$$

So $BA = A^3B$. Take $X = A^{s_1}B^{s_2}A^{s_3}B^{s_4}\dots A^{s_{2n-1}}B^{s_{2n}} = A^{s_1}B^{s_2-1}A^3B$ $A^{s_3-1}B^{s_4}\dots A^{s_{2n-1}}B^{s_{2n}} = \dots$ In finite steps , we can change it into $X = A^aB^b$. $A^4 = B^4 = I$, so we only consider $1 \le a, b \le 4$. $A^2 = B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, we list all: $Q_8 = \{A, A^2, B, BA, AB, A^2B, AB^2, I\}$. The order of Q_8 is 8.

Exercise 1.2.4. Let H be the group(under ordinary matrix multiplication) of real matrices generated by $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Show that H is a nonabelian group of order 8 which is not isomorphic to the quaternion group, but is isomorphic to the group D_4^*.

Answer. $C^4D^2 = I, DC = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = C^3D$.Similarly, we can prove H is a nonabelian group of order 8. $H = \{C, C^2, C^3, I, D, CD, C^2D, C^3D\}$
Assume $G \cong H$ and the isomorphism is f, Let $f(D) = X$, $f(D^2) = X^2 = f(I) = I$, so $X^2 = I$. But $f^{-1}(I) = I \Rightarrow X \neq I \Rightarrow X = AB$ or $X = A^2$ or $X = B^2$.
If $X = A^2$, consider $f(C) = Y, f(C^2D) = Z$, we have $(Y, Z) = (B^2, AB)$ or $(Y, Z) = (AB, B^2)$. $f(C^2D) = f(C^2)f(D) \Leftrightarrow Z = XY$. That's contradictory!
If $X = B^2$, the proof is similar.
If $X = AB$, $(Y, Z) = (A, B)$ or $(Y, Z) = (B, A)$. That's contradictory! So f doesn't exist. G is not isomorphic to H.
Now we prove $H \cong D_4^*$. For any point $(x, y)^T$ inside the square

$$T_x = (x, -y)^T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}(x, y)^T = CD(x, y)^T$$

$$T_y = (-x, y)^T = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}(x, y)^T = C^3D(x, y)^T$$

$$T_{13} = (-y, x)^T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}(x, y)^T = C^3(x, y)^T$$

$$T_{24} = (y, -x)^T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}(x, y)^T = C(x, y)^T$$

so $D_4^* = \langle T_x, T_y, T_{13}, T_{24}\rangle = H = \langle C, D\rangle$.

Exercise 1.2.5. Let S be a nonempty subset of a group G and define a relation on G by $a \sim b$ if and only if $ab^{-1} \in S$. Show that $\sim$ is an equivalence relation if and only if S is a subgroup of G.

Answer. If $\sim$ is a equivalence relation

1. $a \sim b \Rightarrow b \sim a$;
2. $a \sim a$;
3. $a \sim b, b \sim c \Rightarrow a \sim c$.

$2 \Leftrightarrow aa^{-1} = e \in S$. $1 \Rightarrow a \sim e \Rightarrow e \sim a \forall a \in S$, so $ae^{-1} = a \in S, ea^{-1} = a^{-1} \in S$. If $a, b \in S, b^{-1} \in S$, so $ae^{-1} \in S, e(b^{-1})^{-1} \in S$. By 3, $a \sim e, e \sim b^{-1} \Rightarrow a \sim b^{-1} \Rightarrow ab \in S$. S is a subgroup of G.
If S is a subgroup of G

1. $aa^{-1} \in S \Rightarrow a \sim a$;
2. $ab^{-1} \in S \Rightarrow (ab^{-1})^{-1} = ba^{-1} \in S \Rightarrow (a \sim b \Rightarrow b \sim a)$;
3. $ab^{-1} \in S, bc^{-1} \in S \Rightarrow (ab^{-1})(bc^{-1}) = ac^{-1} \in S$, which means $a \sim b, b \sim c \Rightarrow a \sim c$

In conclusion, $\sim$ is a equivalence relation.

Exercise 1.2.6. A nonempty finte subset of a group is s subgroup if and only if it is closed under the product in G.

Answer. $\Rightarrow$: Trivial.
$\Leftarrow$: S is apparently associative. $\forall a, b \in S, ab \in S$. S is a finite set, so there exists $m > n \in \mathbf{N}$ s.t. $a^m = a^n$.

Exercise 1.2.7. If n is a fixed integer, then $\{kn | n \in \mathbf{Z}\} \subset \mathbf{Z}$ is an additive subgroup of $\mathbf{Z}$, which is isomorphic to $\mathbf{Z}$.

Answer. Denote $Z^n = \{kn | k \in \mathbf{Z}\}$. We can easily check that Z^n is a subgroup of $\mathbf{Z}$. Now we build a isomorphism between Z^n and $\mathbf{Z}$. Take $f : Z^n \to \mathbf{Z}$ as $f(kn) = k$, $f^{-1}(n) = kn$. f is a bijection so Z^n and $\mathbf{Z}$ are isomorphism.

Exercise 1.2.8. The set $\{\sigma \in S_n | \sigma(n) = n\}$ is a subgroup of S_n which is isomorphic to S_{n-1}.

Answer. Denote $S_n^{(n)} = \{\sigma \in S_n | \sigma(n) = n\}$. $\forall \sigma_1, \sigma_2 \in S_n^{(n)}, \sigma_1\sigma_2(n) = \sigma_1(\sigma_2(n)) = \sigma_1(n) = n$, so $\sigma_1\sigma_2 \in S_n^{(n)}$. By the above exercise, $S_n^{(n)}$ is a subgroup of S_n. Now we build an isomorphism between $S_n^{(n)}$ and S_{n-1}. Take $f : S_{n-1} \to S_n^{(n)}$ as $f(\sigma) = \sigma'$, where $\sigma'(x) = \begin{cases} n, & x = n \\ \sigma(n), & x \neq n \end{cases}$. $\sigma' \in S_n^{(n)}$ and f is a bijection, so $S_{n-1} \cong S_n^{(n)}$.

Exercise 1.2.9. Let $f : G \to H$ be a homomorphism of groups, A a subgroup of G, and B a subgroup of H.
(a) Ker$f$ and $f^{-1}(B)$ are subgroups of G.
(b) $f(A)$ is a subgroup of H.

Answer. (a) f is a homomorphism, so $f(e) = e', e \in \text{Ker}f$. $\forall a \in \text{Ker}f$, $f(aa^{-1}) = f(a)f(a^{-1}) = e'$, so $f(a^{-1}) = f(a)^{-1} = e'^{-1} = e'$. $\forall a, b \in \text{Ker}f, f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e' \Rightarrow ab^{-1} \in \text{Ker}f$, which means Ker$f$ is a subgroup of G. The proof of $f^{-1}(B)$ is a subgroup of G is similar.
(b) f is a homomorphism, $f(e) = e'$. $\forall a, b \in A, ab^{-1} \in A$, so $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} \in f(A)$, $f(A)$ is a subgroup of H.

Exercise 1.2.10. List all subgroups of $Z_2 \oplus Z_2$. Is $Z_2 \oplus Z_2$ isomorphic to Z_4?

Answer. $Z_2 \oplus Z_2$: $\{\{(1,1),(1,0),(0,1),(0,0)\},\{(1,1),(0,0)\},\{(0,0)\},$
$\{(1,0),(0,0)\},\{(0,1),(0,0)\},\{(0,1),(1,0),(0,0)\}\}$.
Z_4: $\{\{\bar{0},\bar{1},\bar{2},\bar{3}\},\{\bar{0},\bar{2}\},\{\bar{0}\}\}$.
Z_4 and $Z_2 \oplus Z_2$ are not isomorphic because they have different subgroups.

Exercise 1.2.11. If G is a subgroup, then $C = \{a \in G | ax = xa \text{ for all } x \in G\}$ is a abelian subgroup of G. C is called the center of G.

Answer. Take $a, b \in C, ab = ba$, C is communicative. $\forall a, b \in C, x \in G$, $b^{-1} \in G$, so $ab^{-1} = b^{-1}a$.

$$ax = axbb^{-1} = abxb^{-1} = baxb^{-1} = bxab^{=1} = abb^{-1}x = bab^{-1}x$$

so $b^{-1}ax = ab^{-1}x = xab^{-1}$, $ab^{-1} \in C$, C is a subgroup of G.

Exercise 1.2.12. The group D_4^* is not cyclic, but can be generated by two elements. The same is true of S_n(nontrivial). What is the minimal number of generators of the additive group $\mathbf{Z} \oplus \mathbf{Z}$?

Answer. $\mathbf{Z} \oplus \mathbf{Z} = \{(a, b) | a \in \mathbf{Z}, b \in \mathbf{Z}\} = \langle (0, 0), (1, 0), (0, 1) \rangle$. We can easily check the spanning set is the minimal.

Exercise 1.2.13. If $G = \langle a \rangle$ is a cyclic group and H is any group, then every homomorphism $f : G \to H$ is completely determined by the element $f(a) \in H$.

Answer. $\forall x \in G$, there exist $m \in \mathbf{N}$ s.t. $x = a^m$, so $f(x) = f(a^m) = f(a)^m \Rightarrow \mathrm{Im} f = \langle f(a) \rangle$. $f : a^m \mapsto f(a)^m \forall m \in \mathbf{N}$. f is completely determined by $f(a) \in H$.

Exercise 1.2.14. The following cyclic subgroups are all isomorphic: the multiplication group $\langle i \rangle$ in $\mathbf{C}$, the additive group $\mathbf{Z_4}$ and the subgroup $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \right\rangle$ of S_4.

Answer. $\langle i \rangle = \{i, -1, -i, 1\}$, $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$,
$\langle (1234) \rangle = \{(1234), (13)(24), (1432), (1)\}$. Denote $f : \langle i \rangle \to Z_4$ as $f(i) = \bar{i}$, $g : Z_4 \to \langle (1234) \rangle$ as $g(i) = (1234)$. From the exercise above we know f and g aer homomorphisms, and they are bijections, so $\langle i \rangle \cong Z_4 \cong \langle (1234) \rangle$.

Exercise 1.2.15. Let G be a group and Aut$G$ is the set of all automorphisms of G.
(a) Aut$G$ is a group with composition of functions as binary operation.
(b) Aut$\mathbf{Z} \cong Z_2$ and Aut$Z_6 \cong Z_2$; Aut$Z_8 \cong Z_2 \oplus Z_2$; Aut$Z_p \cong Z_{p-1}$ (p prime).
(c) What is Aut$\mathrm{Z_n}$ for arbitrary $n \in \mathbf{N}^*$?

Answer. We only prove the third question.
For $\bar{a} \in Z_n$, the order of $\bar{a}$ is $|\bar{a}| = \frac{n}{(n,a)}$. When $(n, a) = 1$, $\bar{a}$ is a generator of Z_n. Denote Euler function as $\varphi(x)$ and $Z_n^* = \{\bar{a} \in Z_n | (a, n) = 1\}$, then $|Z_n^*| = \varphi(n)$. For $\sigma \in \mathrm{Aut}Z_n$, σ is completely determined by $\sigma(\bar{1}) = \bar{a}$, and we denote σ as σ_a. For $\sigma_a, \sigma_b \in \mathrm{Aut}Z_n$, $\sigma_a(\sigma_b(\bar{1})) = \sigma_a(\bar{b}) = \bar{ab} = \sigma_{ab}(\bar{1})$. We have proved $\mathrm{Aut}Z_n \cong Z_n^*$.
Now we give out a lemma to show the structure of Z_n^*.

Lemma. *If $n = st, (s, t) = 1$, then $Z_n^* \cong Z_s^* \oplus Z_t^*$.*

The proof of this lemma is quite simple. Consider the mappping $f^* : Z_n^* \to Z_s^* \oplus Z_t^*$ which is defined by $(x \mod n) \mapsto (x \mod s, x \mod t)$. Since for any $a, b \in Z_n^*$, $f^*(a)f^*(b) = (a \mod s, a \mod t)(b \mod s, b \mod t) = (ab \mod s, ab \mod t) = f^*(ab)$, f^* is a well defined homomorphism. For $x \in \mathrm{Ker}f^*$, $x \equiv 1 \mod s$, $x \equiv 1 \mod t$, so $x \equiv 1 \mod [s, t]$, $x \equiv 1 \mod n$, f^* is a monomorphism. Since $|f^*(Z_n^*)| = |Z_n| = \varphi(n) = \varphi(s)\varphi(t) = |Z_s^* \oplus Z_t^*|$, f^* is a epimorphism. $Z_n^* \cong Z_s^* \oplus Z_t^*$
For $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, $Z_n^* \cong Z^*_{p_1^{k_1}} \oplus Z^*_{p_2^{k_2}} \oplus \cdots \oplus Z^*_{p_m^{k_m}}$. Now we consider the structure of $Z^*_{p^k}$.
For $p = 2$, $Z_2^* \cong Z_1$, $Z_4^* \cong Z_2$, $Z^*_{2^k} \cong Z_2 \oplus Z_{2^{k-2}}$.
For other odd prime p, $Z^*_{p^k} \cong Z_{(p-1)p^{k-1}}$.
In order to prove the result, we need the Lagrange theorem in number theory.

Lemma (Lagrange)**.** *$f(x) \in Z[n]$, $f(x) \equiv k$ has at most n solutions when* mod p*, where p is an odd prime.*

We use induction to prove the lemma.
1. $n = 1$, the proof the trivial.
2. Assume for $n \leq m - 1$ the lemma is correct, and for $n = m$, $f(x) \equiv k$ has $m + 1$ solutions. $f(x) - f(x_{m+1}) = (x - x_{m+1})g(x) \equiv 0 \mod p$. Take $x = x_i, i = 1, 2, \ldots, m$, $(x_i - x_{m+1})g(x_i) \equiv 0 \mod p$, $x_i \neq x_{m+1}$, so $g(x_i) \equiv 0 \mod p$, That's contradictory to the induction assumptions!

The lemma is proved.
Come back to the original question. Firstly, we consider $k = 1$ and p is an odd prime. For any factor d of $p-1$, denote $S(d) = \{\bar{a} \in Z_p^* | \mathrm{ord}_p(a) = d\}$. $S(d)$ forms a partition of Z_p^*. If $S(d) \neq \varnothing$, there exists $\bar{a} \in S(d)$ and $a^d \equiv 1 \mod p$. By Largrange theorem, $a^d \equiv 1 \mod p$ has at most d solutions. Notice that $\{1, a, a^2, \ldots, a^{d-1}\}$ are the solutions of the equation, $a^i \not\equiv a^j \mod p$, whence $S(d) \subset \langle \bar{a} \rangle$. For $k = 1, 2, \ldots, d-1$, $\mathrm{ord}_p(\bar{a^k}) = \left|a^k\right| = \frac{d}{(d,k)} = d \Leftrightarrow (d, k) = 1$. Thus $|S(d)| = \varphi(d)$.
From $Z_p^* = \bigcup_{d|p-1} S(d)$, we get

$$p - 1 = \left|Z_p^*\right| = \sum_{d|p-1} |S(d)| \leq \sum_{d|p-1} \varphi(d) = p - 1$$

If $d|p-1$, $|S(d)| = \varphi(d)$. Particularly, when $d = p-1$, $|S(p-1)| = \varphi(p-1) \neq 0$, Z_p^* has a element of order $p-1$, Z_p^* is a cyclic group.
Secondly, we consider $k \geq 2$. Take $a \in \mathbf{Z}$ and $\bar{a}$ is the class of $x \equiv a \mod p^k$. For $s \geq t$, we have a group homomorphism $f_{s,t} : Z_{p^s}^* \to Z_{p^t}^*$ which is defined by $(a \mod p^s) \mapsto (a \mod p^t)$. Since $a \equiv b \mod p^s \Rightarrow a \equiv b \mod p^t$, f is well defined. $\mathrm{Ker} f_{s,t} = \{up^t + 1 \mod p^s | u = 0, 1, \ldots, p^{s-t} - 1\}$. If $2t \geq s$, since $(up^t + 1)(vp^t + 1) \equiv uvp^{2t} + (u + v)p^t + 1 \equiv (u + v)p^t + 1 \mod p^s$, $\mathrm{Ker} f_{s,t} \cong Z_{p^{s-t}}$ is a cyclic group. There exists a isomorphism $g_{s,t} : Z_{p^s}^* / \mathrm{Ker} f_{s,t} \to Z_{p^t}^*$.

$$\{\bar{1}_{p^k}\} = \mathrm{Ker} f_{k,k} < \mathrm{Ker} f_{k,k-1} < \cdots < \mathrm{Ker} f_{k,1} < Z_{p^k}^*$$

Lemma. *Suppose $i \geq 2$, $\bar{a}_{p^k} \in \mathrm{Ker} f_{k,i}$, but $\bar{a}_{p^k} \notin \mathrm{Ker} f_{k,i+1}$, then $\bar{a}_{p^k}^p \in \mathrm{Ker} f_{k,i+1}$ and $\bar{a}_{p^k}^p \notin \mathrm{Ker} f_{k,i+2}$.*

This lemma can be proved by LTE. Here we use the language in group theory to prove it. $f_{k,i+2}(\bar{a}_{p^k}) = \bar{a}_{p^{i+2}}$, $\bar{a}_{p^{i+2}} \in f_{k,i+2}(\mathrm{Ker} f_{k,i}) = \mathrm{Ker} f_{i+2,i}$. $\mathrm{Ker} f_{i+2,i} \cong Z_{p^2}$ since $2i \geq i + 2$. $\bar{a}_{p^{i+2}} \notin f_{k,i+2}(\mathrm{Ker} f_{k,i+1}) = \mathrm{Ker} f_{i+2,i+1} \cong Z_p$. $\mathrm{Ker} f_{i+2,i+1}$ contains all the elements whose order is p in $\mathrm{Ker} f_{i+2,i}$, so $\left|\bar{a}_{p^{i+2}}\right| = p^2$. $\bar{a}_{p^{i+2}}^p \in \mathrm{Ker} f_{i+2,i+1}$, $\bar{a}_{p^{i+2}}^p \notin \mathrm{Ker} f_{i+2,i+2}$, $\bar{a}_{p^k}^p \in g_{k,i+2}^{-1}(\bar{a}_{p^{i+2}}^p) \subset g_{k,i+2}^{-1}(\mathrm{Ker} f_{i+2,i+1}) = \mathrm{Ker} f_{k,i+1}$, $\bar{a}_{p^k}^p \notin g_{k,i+2}^{-1}(\mathrm{Ker} f_{i+2,i+2}) = \mathrm{Ker} f_{k,i+2}$.
For $i = 1$, if p is an odd prime, $\mathrm{Ker} f_{3,1} = \left\langle p \dot{+} 1_{p^3} \right\rangle \cong Z_{p^2}$, if $p = 2$, $\mathrm{Ker} f_{3,1} = \{\bar{1}_8, \bar{3}_8, \bar{5}_8, \bar{7}_8\} \cong Z_2 \oplus Z_2$. Thus, for $\bar{a}_{p^k} \in \mathrm{Ker} f_{k,2}, \bar{a}_{p^k} \notin \mathrm{Ker} f_{k,3}$, using the lemma above for several times, we get $\bar{a}_{p^k}^{p^{k-2}} \in \mathrm{Ker} f_{k,2}, \bar{a}_{p^k}^{p^{k-3}} \notin \mathrm{Ker} f_{k,k}$, $\left|\bar{a}_{p^k}\right| = p^{k-2}$, $\mathrm{Ker} f_{k,2} \cong Z_{p^{k-2}}$.
If p is an odd prime, we can further obtain $\mathrm{Ker} f_{k,1} \cong Z_{p^{k-1}}$.

Suppose x is a generator of Z_p^*, assume $a \in g_{k,1}^{-1}(x)$, $g_{k,1}^{-1}(x) = a\mathrm{Ker}f_{k,1}$, and $a^{p-1} \in g_{k,1}^{-1}(x^{p-1}) = g_{k,1}^{-1}(\bar{1}_p) = \mathrm{Ker}f_{k,1}$. If $a^{p-1} \notin \mathrm{Ker}f_{k,2}$, then $\left|a^{p-1}\right| = p^{k-1}$. If $a^{p-1} \in \mathrm{Ker}f_{k,2}$, $\forall h \in \mathrm{Ker}f_{k,1}, h \notin \mathrm{Ker}f_{k,2}$. Since $(ah)^{p-1} = (a^{p-1}h^p)h^{-1}$, $(ah)^{p-1} \in \mathrm{Ker}f_{k,1}, (ah)^{p-1} \notin \mathrm{Ker}f_{k,2}$, whence $\left|(ah)^{p-1}\right| = p^{k-1}$, $Z_{p^k}^* \cong Z_{(p-1)p^{k-1}}$.
If $p = 2$, $Z_{2^k}^* = \mathrm{Ker}f_{k,1} \cong Z_{2^{k-2}} \oplus Z_2$.
For Aut$\mathbf{Z}$, assume there exist $f \neq 1_G, -1_G$, $f \in \mathbf{AutZ}$. WLOG, $f(1) = x \neq \pm 1, f(-1) = y$. $f(1)+f(-1) = f(0) = x+y = 0$. Assume $af(1)+bf(-1) = f(a-b) = 1 = (a-b)x$, since $x \neq \pm 1$, there is a contradiction. Aut$\mathbf{Z} \cong Z_2$.

Exercise 1.2.16. For each prime p the additive subgroup $Z(p^\infty)$ of $\mathbf{Q}/\mathbf{Z}$ is generated by the set $\{\bar{1/p^n} | n \in \mathbf{N}^*\}$.

Answer. We prove that $\left\langle \bigcup_{n=1}^{\infty} \frac{\bar{1}}{p^n} \right\rangle \cong Z(p^\infty)$. $\forall x \in Z(p^\infty), x = \frac{\bar{a}}{b} = \frac{\bar{a}}{p^k}$. Expand a as $a = \sum_{i=0}^{k-1} p^i a_i$, where $a_i = 1, 2, \ldots n-1$. $x = \frac{\bar{a}}{b} = \sum_{i=0}^{k-1} \frac{\bar{a_i}}{p^{k-i}} = \sum_{i=1}^{k} \frac{\bar{a_{k-i}}}{p^i}$. Denote $f : \left\langle \bigcup_{n=1}^{\infty} \frac{1}{p^n} \right\rangle \to Z(p^\infty)$ as $f(\sum_{i=1}^{n} \frac{a_i}{p^i}) = \sum_{i=1}^{n} \frac{\bar{a_i}}{p^i}$. f is an isomorphism because every $x \in Z(p^\infty)$ can be written in such form.

Exercise 1.2.17. Let G be an abelian group and let H, K be subgroups of G. Show that the join $H \vee K$ is the set $\{ab | a \in H, b \in K\}$. Extend this result to any finite number of subgroups of G.

Answer. $H \vee K = \langle H \cup K \rangle, I = \{ab | a \in H, b \in K\}$. G is abelian so I is a subgroup of G. $H < I, K < I, (H \cup K) \subset I$. $\langle H \cup K \rangle \subset I \Rightarrow \langle H \cup K \rangle$.
For any $ab \in I$, $a \in H$, $b \in K$, we prove that ab is contained in any subgroup which contains $H \cup K$.
Assume $(H \cup K) \subset J$, so $a \in J, b \in J \Rightarrow ab \in J$, which means $I \subset H \vee K$. $\langle H \cup K \rangle = I$.
G is abelian group, $H_1, H_2, \ldots H_n$ are n subgroups. $\left\langle \bigcup_{i=1}^{n} H_i \right\rangle = \{\prod_{i=1}^{n} h_i | h_i \in H_i, i = 1, 2, \ldots n\}$. This proposition can be proved by induction.

Exercise 1.2.18. 1. Let G be a group and $\{H_i | i \in I\}$ a family of subgroups. State and prove a condition that will imply that $\bigcup_{i\in I} H_i$ is a subgroup, that is $\bigcup_{i\in I} H_i = \left\langle \bigcup_{i\in I} H_i \right\rangle$.

2. Given an example of a group G and a family of subgroups $\{H_i | i \in I\}$ such that $\bigcup_{i\in I} H_i \neq \left\langle \bigcup_{i\in I} H_i \right\rangle$.

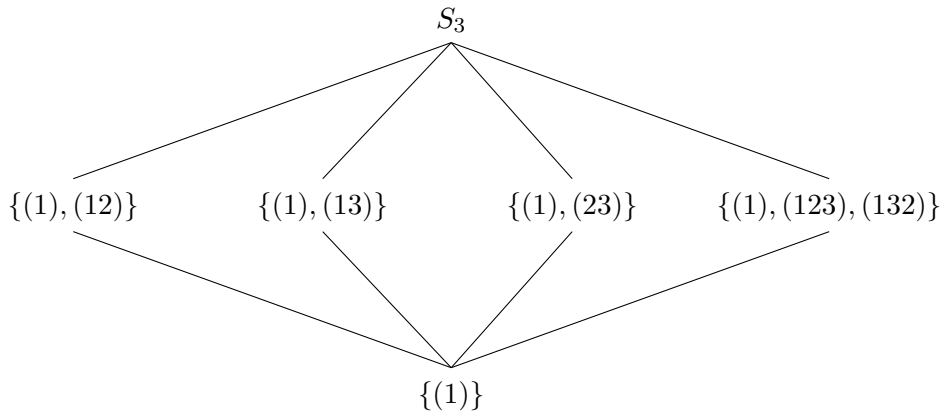
Answer. I didn't find a sufficient and necessary condition for this question, just choose one as you like:)

Exercise 1.2.19. 1. The set of all subgroups of a group G, partially ordered by set theoretic inclusion, forms a complete lattice in which the g.l.b of $\{H_i | i \in I\}$ is $\bigcap_{i\in I} H_i$ and the l.u.b is $\left\langle \bigcap_{i\in I} H_i \right\rangle$.

2. Exhibit the lattice of subgroups of the groups S_3, D_4^*, Z_6, Z_{27} and Z_{36}.

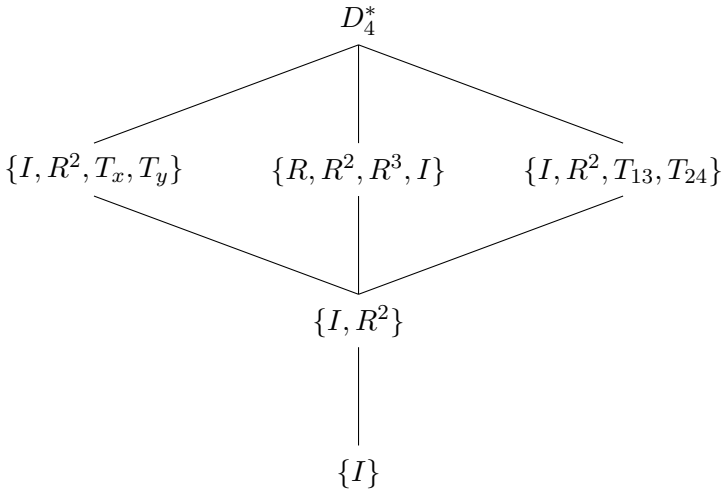
Answer. 1. The subset relation $<$ forms a partially ordered relation. By the difinition of $\left\langle \bigcup_{i\in I} H_i \right\rangle$, $\left\langle \bigcup_{i\in I} H_i \right\rangle$ is the smallest set contains $\bigcup_{i\in I} H_i$, so it's lup. For glb, we know that $\bigcap_{i\in I} H_i \subset H_i \ \forall i \in I$, and $\forall H \supset \bigcap_{i\in I} H_i$, there exists $x \in H, x \notin H_j \ j \in I$, so $\bigcap_{i\in I}$ is glb.

2. $S_3 = \{(1), (12), (13), (23), (123), (132)\}$.



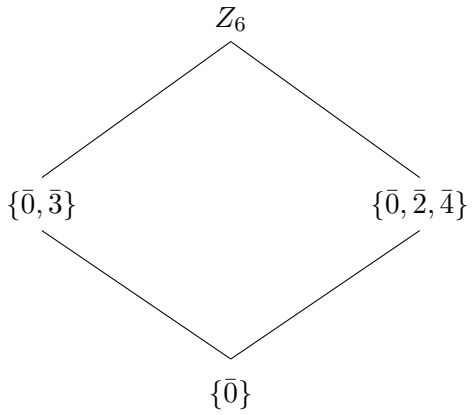
The Hasse figure of the lattice of S_3

$D_4^* = \{R, R^2, R^3, I, T_x, T_y, T_{13}, T_{24}\}$.

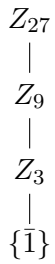


The Hasse figure of the lattice of D_4^*

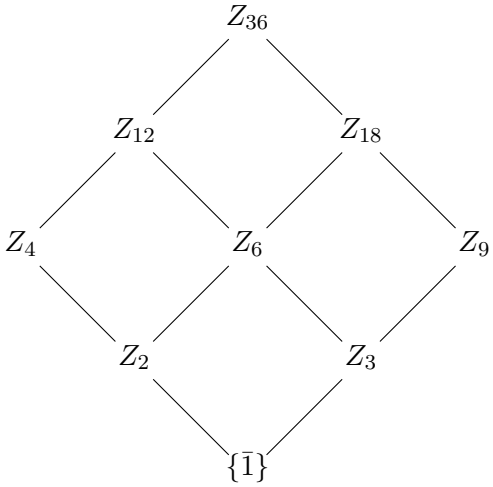
$Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.



The Hasse figure of the lattice of Z_6



The Hasse figure of the lattice of Z_{27}



The Hasse figure of the lattice of Z_{36}

1.3 Cyclic groups

Exercise 1.3.1. Let a, b be elements of group G. Show that $|a| = \left|a^{-1}\right|$; $|ab| = |ba|$, and $|a| = \left|cac^{-1}\right|$ for all $c \in G$.

Answer. We only consider that $|a|, |b|, |c|$ are finite. Assume $a^k = e$, $(ab)^m = e$, $(ac^{-1})^n = e$, $kmn \neq 0$. $a^k \cdot (a^{-1})^k = e$, so k sialso the order of a^{-1}, $\left|a^{-1}\right| = k$. $(ab)^m = e = a(ba)^{m-1}b \Rightarrow (ba)^{m-1} = a^{-1}b^{-1}$, $(ba)^m = a^{-1}b^{-1}ba = e$. m is the order of ba. $(cac^{-1})^r = cac^{-1}cac^{-1}\cdots cac^{-1} = ca^nc^{-1} = e$, so $a^n = e$, whence $n = k$.

Exercise 1.3.2. Let G be an abelian group containing elements a and b of orders m and n respectively. Show that G contains an element whose order is the least commom multiple of m and n.

Answer. If $(m, n) = 1$, we know that $\forall a^i, i = 1, 2, \ldots, m$, $b^j, j = 1, 2, \ldots, n$, $a^ib^j \neq e$, since if $a^i = b^j$, $\left|a^i\right| = n = \left|b^{-j}\right| = \left|b^j\right| = m$. G is abelian, so $(ab)^k = a^kb^k \Rightarrow |ab| = mn = [m, n]$.
If $m|n$ or $n|m$, then a or b is the element we want. We consider $m \nmid n$ and $n \nmid m$. Factorise $n = p_1^{t_1}p_2^{t_2}\cdots p_l^{t_l}$, $m = p_1^{s_1}p_2^{s_2}\cdots p_l^{s_l}$, where $p_1, \cdots, p_l$ are primes and $t_1, \cdots, t_l, s_1, \cdots, s_l \geq 0$. We can choose a new arrangement of $p_1, \cdots, p_l$ and make $t_1 \geq s_1$, $t_2 \geq s_2$, $\ldots$, $t_i \geq s_i$, $t_{i+1} < s_{i+1}$, $\ldots$, $t_l < s_l$.

$$(m, n) = p_1^{s_1}\cdots p_i^{s_i}p_{i+1}^{t_{i+1}}\cdots p_l^{t_l}, [m, n] = p_1^{t_1}\cdots p_i^{t_i}p_{i+1}^{s_{i+1}}\cdots p_l^{s_l}$$

Take $x = a^{p_{i+1}^{s_{i+1}}\cdots p_l^{s_l}}$, $y = b^{p_1^{t_1}\cdots p_i^{t_i}}$, then $|x| = p_1^{t_1}\cdots p_i^{t_i}$, $|y| = p_{i+1}^{s_{i+1}}\cdots p_l^{s_l}$. Thus $(x, y) = 1$, the order of xy is $|x| \cdot |y| = p_1^{t_1}\cdots p_i^{t_i}p_{i+1}^{s_{i+1}}\cdots p_l^{s_l} = [m, n]$.

Exercise 1.3.3. Let G be an abelian group of order pq, with $(p, q) = 1$. Assume there exist $a, b \in G$ such that $|a| = p, |b| = q$ and show that G is cyclic.

Answer. From **Exercise 1.3.2** we know $a^ib^j \neq e$ for $i < p$, $j < q$. $|G| = pq$ for all a^ib^j and a^mb^n with $i \neq m$, $b \neq n$, $a^ib^j \neq a^mb^n$. So G can be generated by ab. G is cyclic.

Exercise 1.3.4. If $f : G \to H$ is a homomorphism, $a \in G$, and $f(a)$ has finte order in H, then $|a|$ is infinite or $|f(a)|$ divides $|a|$.

Answer. Assume $|f(a)| = n$, $|a| = m$, and $n \nmid m$. Trivially, $m \geq n$. Assume $\gcd(m, n) = k \leq n$. $a^m = e \Rightarrow f(a)^m = e' = f(a)^n$. By Bezout theorem $\exists x, y \in \mathbf{Z}$ s.t. $f(a)^{mx+ny} = f(a)^k = e'$, $k \leq n$, that's contradictory!

Exercise 1.3.5. Let G be the multiplicative group of all nonsingular 2×2 matrices with rational entries. Show that $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$has order 4 and $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$has order 3, but ab has infinite order. Conversely, show that the additive group $Z_2 \oplus \mathbf{Z}$ contains nonzero elements a, b of infinite order such that $a + b$ has finite order.

Answer. The verification of $|a| = 4$ and $|b| = 3$ is trivial. $ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $\det(ab = \lambda I) = 0 \Rightarrow \lambda_1 = \lambda_2 = 1$. ab is not diagnizable. By induction, we have $(ab)^n = \begin{pmatrix} 1 & 2^{n-1} \\ 0 & 1 \end{pmatrix}$ which means (ab) has infinite order.
For $a = (\bar{0}, 1), b = (\bar{0}, -1) \in Z_2 \oplus \mathbf{Z}$, a, b have infinite order, but $a+b = (\bar{0}, 0)$ has finite order 1.

Exercise 1.3.6. If G is a cyclic group of order n and $k|n$, then G has exactly one subgroup of order k.

Answer. Assume $a^n = e$, $mk = n$, we verify that $\langle a^m \rangle$ is a subgroup of order k. $\forall x, y \in \mathbf{Z}_+$, $a^{xm} \cdot a^{-ym} = a^{(x-y)m} \in \langle a^m \rangle$, so $\langle a^m \rangle$ is a subgroup. $a^{km} = e$, $a^{sm} \neq e$ for $s < k$, so $|\langle a^m \rangle| = k$.

Exercise 1.3.7. Let p be prime and H a subgroup of $Z(p^\infty)$.
(a) Every element of $Z(p^\infty)$ has finite order p^n for some $n \geq 0$.
(b) If at least one element of H has order p^k and no element of H has order greater than p^k, then H is the cyclic subgroup generated by $1/\bar{p}^k$, whence $H \cong Z_{p^k}$.

(c) If there is no upper bound on the orders of elements of H, then $H = Z(p^\infty)$.
(d) The only proper subgroups of $Z(p^\infty)$ are the finite cyclic groups $C_n = \left\langle 1/p^n \right\rangle$ $(n = 1, 2, \dots)$. Futhermore, $\langle 0 \rangle = C_0 < C_1 < C_2 < C_3 < \cdots$.
(e) Let $x_1, x_2, \dots$ be elements of an abelian group G such that $|x_1| = p, px_2 = x_1, px_3 = x_2, \dots, px_{n+1} = x_n, \dots$. The subgroup generated by the $x_i (i \geq 1)$ is isomorphic to $Z(p^\infty)$.

Answer. (a) $\forall x \in Z(p^\infty)$, $x = \frac{a}{p^n}$ where $a < p^n$, $p \nmid a$. p is a prime, so $\gcd(p, a) = 1$. $m \cdot a | p^n \Rightarrow m = p^n$. Thus $m \cdot \frac{a}{p^n} = e$, p^n is the smallest number satisfies it. $\frac{a}{p^n}$ has order p^n.
(b) For all $x \in Z(p^\infty)$, if x has order smaller than p^k, x must have the form $x = \frac{a}{p^i} (i \leq k)$, $(p, a) = 1$, so $x \in \left\langle \frac{1}{p^k} \right\rangle$. If not, assume $x = \frac{a}{p^i} (i > k)$, then $p^k \cdot x = \frac{a}{p^{i-k}} \neq 1$.
(c) Assume not, $H < Z(p^\infty)$, $H \neq Z(p^\infty)$. There exist $y \in H$ s.t. y has order $p^m, m \geq n$. $y = \frac{b}{p^m}$, $(p, b) = 1$, so there exists $b^{-1} \in \{1, 2, \dots, p-1\}$, $bb^{-1} \equiv 1 \mod p^m$. But $ab^{-1}p^{m-n}y = \frac{a}{p^n} = x \in H$, that's contradictory! Conversely, $H = Z(p^\infty)$.
(d) From (b), we know that if there's least upper bound p^n for elements in a subgroup S, then $S = C_n$.

$$\langle 0 \rangle = C_0 < C_1 < C_2 < C_3 < \cdots < Z(p^\infty)$$

is easy to verify.
(e) We can verify that $f : x_i \mapsto \frac{\bar{1}}{p^i}$ is a well defined isomorphism. $f(e) = f(px_1) = 1$, $f(px_{i+1}) = f(x_i) = \frac{1}{p^i} = p \cdot \frac{1}{p^{i+1}}$. f is obviously a bijection, so $H \cong Z(p^\infty)$.

Exercise 1.3.8. A group that has only a finite number of subgroups must be finite.

Answer. Suppose not. If the order of all subgroups are finite, G must be finite. So there exists a infinite subgroup $H < G$. $\forall a \in G$, if $\forall n \in \mathbf{N}$, $a^n \neq e$. then we can construct infinte subgroups $\langle a \rangle$, $\left\langle a^2 \right\rangle$, $\left\langle a^3 \right\rangle \dots$. If $\forall a \in G$, $\exists n \in \mathbf{N}$, $a^n = e$, so $\langle a \rangle$ is a proper subgroup of G, we can take $b \in G \ni \langle a \rangle$ to construct another subgroup. By induction, there are infinte subgroups in G. That's contradictory, so G must be finite.

Exercise 1.3.9. If G is an abelian group, then the set T of all elements of G with finite order is a subgroup of G.

Answer. We can easily verify that $\forall a, b \in S$, $|a| = m$, $|b| = n$ and $\left|ab^{-1}\right| \leq mn$ is finite. T is a subgroup of G.

Exercise 1.3.10. An infinite group is cyclic if and only if it is isomorphic to each of its proper subgroups.

Answer. If G is cyclic, $G \cong \mathbf{Z}$, $S < G$. For any subgroup of $\mathbf{Z}$, it has the form $\{na\}, a \in \mathbf{Z}$. We can construct a isomorphism $f : n \mapsto na$, so $S \cong \{na\} \Rightarrow G \cong S$.
If $\forall S < G$, $G \cong S$ and $|G| = |S|$ is finite. We prove there exists $S < G$ s.t. $|S| = \aleph_0$. Take $a \in G$ and $S = \{na | n \in \mathbf{Z}\}$, S is a subgroup. If there exists $ma = 0$, S must be finite, contradictory! Thus, $S \cong \mathbf{Z} \cong G$. G is a infinite cyclic group.

1.4 Cosets and counting

Exercise 1.4.1. Let G be a group and $\{H_i | i \in I\}$ a family of subgroups. Then for any $a \in G$, $(\bigcap_i H_i)a = \bigcap_i H_i a$.

Answer. $\bigcap_i H_i$ is a subgroup of G. Take $x \in \bigcap_i H_i$, $x \in H_i$, $\forall i \in I$. Then $xa \in H_i a$, $\forall i \in I$, so $xa \in \bigcap_i (H_i a)$. Thus, $(\bigcap_i H_i)a = \bigcap_i (H_i a)$.

Exercise 1.4.2. (a) Let H be the cyclic subgroup (of order 2) of S_3 generated by $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Then no left cosets of H (except H itself) is also a right coset. There exists $a \in S_3$ such that $aH \cap Ha = \{a\}$.

(b) If K is the cyclic subgroup (of order 3) of S_3 generated by $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, then every left coset of K is also a right coset of K.

Answer. (a) $H = \{(12), (1)\}$. $S_3 = \{(12), (13), (23), (1), (123), (132)\}$. For $a \in H$, $aH = Ha = H$.
$a = (13)$, $aH = \{(13), (123)\}$, $Ha = \{(13), (132)\}$.
$a = (23)$, $aH = \{(23), (132)\}$, $Ha = \{(23), (123)\}$.
$a = (123)$, $aH = \{(123), (23)\}$, $Ha = \{(132), (13)\}$.
$a = (132)$, $aH = \{(132), (13)\}$, $Ha = \{(123), (23)\}$.
(b) $K = \{(123), (132), (1)\}$. For $a \in K$, $aK = Ka = K$.
$a = (12)$, $aK = Ka = \{(12), (23), (13)\}$.
$a = (13)$, $aK = Ka = \{(12), (23), (13)\}$.
$a = (23)$, $aK = Ka = \{(12), (23), (13)\}$.

Exercise 1.4.3. The following conditions on a finite group G are equivalent.
(i) $|G|$ is prime.
(ii) $G \neq \langle e \rangle$ and G has no proper subgroups.
(iii) $G \cong Z_p$ for some prime p.

Answer. (i)⇒(ii): If there exists $S < G$, $S \neq G$, then $|S| \,|\, |G| = p$. That's contradictory!
(ii)⇒(iii): $\forall a \in G$, take $S = \{na | n = 1, 2, \ldots, p\}$. If there exists $ma = na, (1 \leq m < n \leq p)$, $(n - m)a = 0$. So there exists subgroup S, and $|S| = n - m < p$. That's contradictory! So $S < G$, $|S| = |G| \Rightarrow S = G \cong Z_p$.

(iii)⇒(i): Trivial.

Exercise 1.4.4. Let a be an integer and p be a prime such that $p \nmid a$. Then $a^{p-1} \equiv 1 \mod p$.

Answer. $(Z_p\backslash\{\bar{0}\}, \times)$ is a group of order $p-1$. From **Exercise 1.1.7**, we know that $\forall \bar{a} \in Z_p\backslash\{\bar{0}\}$ and $b \in Z_p\backslash\{\bar{0}\}$, taking different $\bar{b}$ we will have different $\bar{ab} \in Z_p\backslash\{\bar{0}\}$. $\bar{ab}$ travels through all the elements in $Z_p\backslash\{\bar{0}\}$. So

$$\prod_{i=1}^{p-1}(\bar{i}\cdot\bar{a}) = \prod_{i=1}^{p-1}\bar{i}$$

By the definition of $Z_p\backslash\{\bar{0}\}$, $Z_p\backslash\{\bar{0}\}$ is communicative. So

$$(\bar{a})^{p-1}(\prod_{i=1}^{p-1}\bar{i}) = \prod_{i=1}^{p-1}\bar{i} \Rightarrow (\bar{a})^{p-1} = \bar{1}$$

Exercise 1.4.5. Prove that there are only two distinct groups of order 4 (up to isomorphism), namely Z_4 and $Z_2 \oplus Z_2$.

Answer. The only cyclic group of order 4 is Z_4. For a group G of order 4 which is not cyclic, $\forall a \in G$, $a \neq e$, if $|a| = 2$, $G \cong Z_2 \oplus Z_2$. If there exists $a \in G$, $|a| = 4$, $G \cong Z_4$. If there exists $a \in G$, $|a| = 3$, denote $a^2 = b, a^3 = e$. Then $b^2 = a^4 = a$, $\{e, a, b\} < G$, which is contradictory to the Largrange theorem.

Exercise 1.4.6. Let H, K be subgroups of a group G. Then HK is a subgroup of G if and only if $HK = KH$.

Answer. If $HK = KH$, for $a_1b_1, a_2b_2 \in HK$,

$$(a_1b_1)(a_2b_2)^{-1} = (a_1b_1)(b_2^{-1}a_2^{-1}) = (a_1b_1)(a_3b_3)$$

since $b_2^{-1}a_2^{-1} \in KH = HK$, there exists $b_2^{-1}a_2^{-1} = a_3b_3$.

$$(a_1b_1)(a_3b_3) = a_1(b_1a_3)b_3 = a_1a_4b_4b_3$$

since $b_1a_3 \in KH = HK$, there exists $b_1a_3 = a_4b_4$. $(a_1b_1)(a_2b_2)^{-1} = a_1a_4b_4b_3 = a_5b_5 \in HK$. Thus HK is a subgroup of G.
If HK is a subgroup of G, $\forall b_1a_1 \in KH$, there exists $(a_1^{-1}b_1^{-1}) \in HK$ s.t. $b_1a_1 = (a_1^{-1}b_1^{-1})^{-1} \in HK$. So $KH \subset HK$. $\forall a_1b_1 \in HK$, $(a_1b_1)^{-1} = b_1^{-1}a_1^{-1} \in HK$, so $\exists a_2b_2 \in HK$ s.t. $b_1^{-1}a_1^{-1} = a_2b_2$. $a_1b_1 = b_2^{-1}a_2^{-1} \in KH$. So $HK \subset KH$. Thus $HK = KH$.

Exercise 1.4.7. Let G be a group of order p^km, with p prime and $(p, m) = 1$. Let H be a subgroup of order p^k and K a subgroup of order p^d, with $0 < d \leq k$ and $K \not\subset H$. Show that HK is not a subgroup of G.

Answer. Assume $HK < G$, $|HK| = p^kn$, $n|m$. We can get $[HK : H] = n = [K : K \cap H]$. $[K : K \cap H]\,|p^k \Rightarrow n|p^k$. That's contradictory to $(m, p^k) = 1$.

Exercise 1.4.8. If H and K are subgroups of finite index of a group G such that $[G : H]$ and $[G : K]$ are relatively prime, then $G = HK$.

Answer. Assume $[G : H] = m$, $[G : K] = n$, $(m, n) = 1$. Then $|H| = np$, $|K| = mp$. $H \cap K < H$, $H \cap K < G \Rightarrow |H \cap K|\,|p$.

$$[G : H] = m \geq [K : H \cap K] = \frac{|K|}{|H \cap K|} \geq m$$

Thus $[G : H] = [K : H \cap K] = m$, $G = HK$.

Exercise 1.4.9. If H, K and N are subgroups of a group G such that $H < N$, then $HK \cap N = H(K \cap N)$.

Answer. $\forall x = hk \in HK \cap N$, $\exists h_1^{-1} \in H$ s.t. $h_1^{-1}hk \in K \cap N$. $H < N$ so $\forall h_1^{-1} \in H, h_1^{-1}hk \in N$. Take $h_1^{-1} = h^{-1}$, $h_1^{-1}hk = k \in K$. So $HK \cap N \subset H(K \cap N)$.
$\forall x = hk \in H(K \cap N)$ where $h \in H$, $k \in K \cap N$. $hk \in HK, h, k \in N \Rightarrow hk \in N$. So $H(K \cap N) \subset HK \cap N$.
Thus, $HK \cap N = H(K \cap N)$.

Exercise 1.4.10. Let H, K, N be subgroups of a group G such that $H < K$, $H \cap N = K \cap N$, and $HN = KN$. Show that $H = K$.

Answer. Assume there exists $x \in K \backslash H$. $K \bigcup_{i \in I} Ha_i$, $\forall h_i \in H$ there exists $a \in K$ s.t. $x = h_1 a$. Take $n_1 \in N$. Since $HN = KN$, $xn_1 \in HN$, there exists $h_2 \in H$, $n_2 \in N$ s.t. $xn_1 = h_2 n_2 = h_2 a n_1$. So $a = n_2 n_1^{-1} \in N$, $a \in K \cap N = H \cap N \Rightarrow a \in H, x \in H$. That's contradictory!

Exercise 1.4.11. Let G be a group of order $2n$; then G contains an element of order 2. If n is odd and G abelian, there is only one element of order 2.

Answer. The proof of the first part is exactly the same as **Exercise 1.1.14**. Assume there exists $a, b \in G$, $a^2 = b^2 = e$. We can check $H = \{e, a, b, ab\}$ is a subgroup of G. $|H| \,|G| \Rightarrow 4|2n \Rightarrow 2|n$, which is contradictory to n is odd. So there's only one element a s.t. $a^2 = e$.

Exercise 1.4.12. If H and K are subgroups of a group G, then $[H \vee K : H]$ $\geq [K : H \cap K]$.

Answer. The question is a direct corollary of Proposition 4.8.

Exercise 1.4.13. If $p > q$ are primes, a group of order pq has at most one subgroup of order p.

Answer. $H \cap K < H$, $H \cap K < K$, $H \neq K \neq H \cap K$. $|H \cap K| \,|p$ and $|H \cap K| \neq q$, so $H \cap K = \{e\}$. From **Exercise 1.3.12**,

$$[H \vee K : H] \geq [K : K \cap H] = p$$

$$|H \vee K| = |H| \cdot [H \vee K : H] \geq p^2$$

But $H \vee K \in G$, $|H \vee K| \leq pq < p^2$. That's contradictory!

Exercise 1.4.14. Let G be a group and $a, b \in G$ such that (i) $|a| = 4 = |b|$; (ii) $a^2 = b^2$; (iii) $ba = a^3b = a^{-1}b$; (iv) $a \neq b$; (v) $G = \langle a, b \rangle$. Show that $|G| = 8$ and $G \cong Q_8$.

Answer. The proof is exactly the same as **Exercise 1.2.3**.

1.5 Normality, quotient groups, and homomorphisms

Exercise 1.5.1. If N is a subgroup of index 2 in a group G, then N is normal in G.

Answer. $\forall a \in G \backslash N$, $G = N \cup Na = N \cup aN$ and $N \cap Na = \varnothing$, $N \cap aN = \varnothing$. So $\forall x \in Na$, $x \in G \backslash N \Rightarrow x \in aN$, $Na \subset aN$. Similarly, $aN \subset Na$, whence $Na = aN$, $N \lhd G$.

Exercise 1.5.2. If $\{N_i | i \in I\}$ is a family of normal subgroups of a group G, then $\bigcap\limits_{i \in I} N_i$ is a normal subgroup of G.

Answer. $\bigcap\limits_{i \in I} N_i$ is a subgroup of G. $N_i (i \in I)$ are normal subgroups of G, so $\forall a \in G$, $aN_i a^{-1} = \{an_i a^{-1} | n_i \in N_i\} = N_i$. $\forall x = ana^{-1} \in a(\bigcap\limits_{i \in I} N_i)a^{-1}$, $n \in N_i \Rightarrow x \in a(\bigcap\limits_{i \in I} N_i)a^{-1} \subset \bigcap\limits_{i \in I} aN_i a^{-1} = \bigcap\limits_{i \in I} N_i$. $\bigcap\limits_{i \in I} N_i$ are normal subgroup of G.

Exercise 1.5.3. Let N be a subgroup of a group G. N is normal in G if and only if (right) congruence modulo N is a congruence relation on G.

Answer. If $N \lhd G$. $\forall a, b \in G$, $ab^{-1} \in N \Leftrightarrow a^{-1}b \in N$. If $a_1 \equiv b_1 \mod N$, $a_2 \equiv b_2 \mod N$, then $a_2 b_2^{-1} \in N$, $a_1 N = N a_1 = N b_1 \Rightarrow a_1 N b_1^{-1} = N$. So $a_1 a_2 b_1^{-1} b_2^{-1} = (a_1 a_2)(b_1 b_2)^{-1} \in N$. Similarly, $(a_1 a_2)^{-1}(b_1 b_2) \in N$. Congruence modulo N is a congruence relation.
If congruence modulo N is a congruence relation. $\forall a_1 \equiv b_1 \mod N$, $a_2 \equiv b_2 \mod N$, we will have $a_1 a_2 \equiv b_1 b_2 \mod N$. Take $n \in N$ and fix $a_2 \in G$, define $b_2 = n^{-1} a_2$. Then $\forall n \in N$, n can be expressed as $a_2 b_2^{-1}$, $a_2 \equiv b_2 \mod N$. $\forall a_1 \in G$ and $\forall b_1 \equiv a_1 \mod N$, $a_1 n b_1^{-1} = a_1 a_2 b_2^{-1} b_1^{-1} \in N$. Take $b_1 = a_1$ and n varies in N, $a_1 n a_1^{-1} \in N \Rightarrow a_1 N a_1^{-1} \subset N$. Thus $N \lhd G$.

Exercise 1.5.4. Let $\sim$ be an equivalence relation on a group G and let $N = \{a \in G | a \sim e\}$. Then $\sim$ is a congruence relation on G if and only if N is a normal subgroup of G and $\sim$ is congruence modulo N.

Answer. If $G \lhd N$ and $\sim$ is congruence modulo N. $\forall a \in G$, $aNa^{-1} \subset N$. $\forall a_1, b_1, a_2, b_2 \in G$, $a_1 b_1^{-1} \in N$, $a_2 b_2^{-1} \in N$. $a_1 a_2 (b_1 b_2)^{-1} = a_1 a_2 b_2^{-1} b_1^{-1}$, denote $n = a_2 b_2^{-1} \in N$, $a_1 a_2 b_2^{-1} b_1^{-1} = a_1 n b_1^{-1} \in a_1 N b_1^{-1}$. $\forall n \in N$, there exists $n' = b_1^{-1} a_1, n' \in N$ s.t. $a_1 n = b_1 n'$. So $a_1 n b_1^{-1} = b_1 n' b_1^{-1} \in b_1 N b_1^{-1} \subset N$. That means $(a_1 a_2)(b_1 b_2)^{-1} \in N$, $a \sim b$ is a congruence relation.
If $a \sim b$ is a congruence relation. We first prove N is a subgroup of G. $\forall a \in N$, $a \sim e$, $a^{-1} \sim a^{-1} \Rightarrow e \sim a^{-1}$, so $a^{-1} \sim e$, $a^{-1} \in N$. $\forall a, b \in N$, $b^{-1} \sim e$, $a \sim e \Rightarrow ab^{-1} \in e$, thus $N < G$.
$\forall x \in G$, $xN = \{xa | a \sim e\} = \{xa | xa \sim xe\} = \{ax | ax \sim e\} = Nx$, so N is normal in G. $x \sim y \Leftrightarrow y \in xN$. $\sim$ is congruence modulo N.

Exercise 1.5.5. Let $N < S_4$ consist of all those permutations σ such that $\sigma(4) = 4$. Is N normal in S_4?

Answer. $N = \{(1), (12), (13), (23), (123), (132)\}$. Take $a = (14) \in G$, $a^{-1} = (14)$, $a^{-1}(12)a = (24) \notin N$. So N is not normal in S_4.

Exercise 1.5.6. Let $H < G$; then the set aHa^{-1} is a subgroup for each $a \in G$, and $H \cong aHa^{-1}$.

Answer. $H < G$, $aHa^{-1} = \{aha^{-1} | h \in H\}$. $\forall x, y \in aHa^{-1}$, $x = ah_1 a^{-1}$, $y = ah_2 a^{-1}$. $y^{-1} = ah_2^{-1} a^{-1}$, $xy = ah_1 h_2^{-1} a^{-1} \in aHa^{-1}$, so $aHa^{-1} < G$.
Take $f : H \to aHa^{-1}$ as $f(h) = aha^{-1}$. If $f(h_1) = f(h_2) = ah_1 a^{-1} = ah_2 a^{-1}$, then $h_1 = h_2$, so f is an injection. f is a surjection because $\forall x \in aHa^{-1}$, $f(a^{-1} x a) = x$, $a^{-1} x a \in H$. In conclusion, $H \cong aHa^{-1}$.

Exercise 1.5.7. Let G be a finite group and H a subgroup of G of order n. If H is the only subgroup of G of order n, then H is normal in G.

Answer. Applying **Exercise 1.5.6**, $\forall a \in G$, $aHa^{-1} \cong H$. $\left|aHa^{-1}\right| = |H| = n \Rightarrow aHa^{-1} = H$. Whence $H \lhd G$.

Exercise 1.5.8. All subgroups of the quaternion group are normal.

Answer. $Q_8 = \{a, b, a^2, ba, ab, a^2b, ab^2, a^2b^2\}$ where $a^2 = b^2$, $a_1b = ba = a^3b$ and $|a| = |b| = 4$. There are several subgroups $\{a, a^2, ab^2, a^2b^2\}$, $\{b, a^2, a^2b, a^2b^2\}$, $\{ab, a^2b^2\}$, $\{ba, a^2b^2\}$, $\{a^2, a^2b^2\}$. From **Exercise 1.5.1**, we know the first two subgroups are normal in G. For $\{ab, a^2b^2\}$, $\{ba, a^2b^2\}$, $\{a^2, a^2b^2\}$, we can check that ab, ba, a^2 is communicative in G, that is $\forall x \in G$, $xabx^{-1} = ab$, $xbax^{-1} = ba$, $xa^2x^{-1} = a^2$. They are all normal in G.

Exercise 1.5.9. (a) If G is a group, then the center of G is a normal subgroup of G;
(b) the center of S_n is the identity subgroup for all $n > 2$.

Answer. (a) By the definition of center C, $\forall x \in G$ and $a \in C$, $ax = xa$, so $xCx^{-1} = C$. C is normal in G.
(b) $\forall x \in S_n$, x can be expressed as

$$x = (a_1a_2 \cdots a_{i_1})(a_{i_1+1}a_{i_1+2} \cdots a_{i_2}) \cdots (a_{i_{n-1}+1}a_{i_{n-1}+2} \cdots a_{i_n})$$

Those cycles $(a_1a_2 \cdots a_{i_1})$, $(a_{i_1+1}a_{i_1+2} \cdots a_{i_2})$, ..., $(a_{i_{n-1}+1}a_{i_{n-1}+2} \cdots a_{i_n})$ are all disjoint, so they are communicative.
If there exists cycles whose length is longer than 2. WLOG, assume $i_1 > 2$. Take $y = (a_1a_2)$,

$$y^{-1}xy = (a_1a_2)(a_1a_2 \cdots a_{i_1})(a_1a_2) \cdots (a_{i_{n-1}+1}a_{i_{n-1}+2} \cdots a_{i_n})$$

$(a_1a_2)(a_1a_2 \cdots a_{i_i})(a_1a_2) = (a_2a_1a_3 \cdots a_{i_1})$, so $y^{-1}xy \neq x$, $x \notin C$.
If $x = (a_1a_2)(a_3a_4) \cdots (a_{2n-1}a_{2n})$ and $n \geq 2$. Take $y = (a_1a_3)$,

$$\begin{aligned} y^{-1}xy &= (a_1a_3)(a_1a_2)(a_3a_4) \cdots (a_{2n-1}a_{2n})(a_1a_3) \\ &= (a_1a_3)(a_1a_2)(a_3a_4)(a_1a_3) \cdots (a_{2n-1}a_{2n}) \\ &= (a_1a_4)(a_2a_3) \cdots (a_{2n-1}a_{2n}) \\ &\neq x \end{aligned}$$

So $x \notin C$.
If $x = (a_1a_2)$. Take $y = (a_1a_3)$, $y^{-1}xy = (a_2a_3) \neq x$, so $x \notin C$.
In conclusion, $C = \{(1)\}$.

Exercise 1.5.10. Find subgroups H and K of D_4^* such that $H \lhd K$ and $K \lhd D_4^*$, but H is not normal in D_4^*.

Answer. $D_4^* = \{I, R, R^2, R^3, T_x, T_y, T_{13}, T_{24}\}$. Take $K = \{I, R, T_x, T_y\}$, $H = \{I, T_x\}$. We can easily verify that $H \lhd K$ and $K \lhd D_4^*$ but $K \not\lhd D_4^*$.

Exercise 1.5.11. If H is a cyclic subgroup of a group G and H is normal in G, then every subgroup of H is normal in G.

Answer. Assume $K < H \lhd G$, H has the generator a, and K has the generator a^n. Here we used: *Every subgroup of a cyclic group is cyclic.* This can be easily proved by the conclusion $H \cong Z_m$ for some $m \in \mathbf{Z}$. $\forall x \in G$, $h = a^s \in H$, $x^{-1}a^s x = a^t \in H$. Assume $x^{-1}ax = a^m$, then $x^{-1}a^n x = (x^{-1}ax)^n = a^{mn} = a^k$, so $n|k$, $a^k \in K$. $x^{-1}Kx \subset K$, K is normal in G.

Exercise 1.5.12. If H is a normal subgroup of a group G such that H and G/H are finitely generated, then so is G.

Answer. Assume $A = \{a_1, a_2, \ldots, a_m\}$, $B = \{b_1, b_2, \ldots, b_n\}$. $H = \langle A \rangle$, $G/H = \langle \{Hb_i | b_i \in B\} \rangle$. We prove that G can be generated by $A \cup B$. $\forall x \in G$, x is in one of the right cosets of H, $x \in Ha$. $Ha \in G/H$ so $Ha = \prod\limits_{b_i \in B} Hb_i^{s_i} = H(\prod\limits_{b_i \in B} b_i^{s_i})$. Thus $a^{-1}(\prod\limits_{b_i \in B} b_i^{s_i}) = a' \in H$. H is generated by A so $xa^{-1} = \prod\limits_{a_i \in A} a_i^{t_i}$, $a' = \prod\limits_{a_i \in A} a_i^{-r_i}$. Then

$$x = (\prod_{a_i \in A} a_i^{t_i + r_i})(\prod_{b_i \in B} b_i^{s_i}) \in \langle A \cup B \rangle$$

Thus $G \subset \langle A \cup B \rangle$ is finitely generated.

Exercise 1.5.13. (a) Let $H \lhd G$, $K \lhd G$. Show that $H \vee K$ is normal in G.

(b) Prove that the set of all normal subgroups of G forms a complete lattice under inclusion.

Answer. (a) $\forall x \in G$, $a \in H \vee K$, we need to prove $x^{-1}ax \in H \vee K$. $a \in H \vee K$ so a can be expressed as

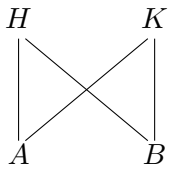
$$a = b_1^{n_1} b_2^{n_2} \cdots b_t^{n_t} \quad \text{where } b_i \in H \text{ or } b_i \in K, i = 1, 2, \ldots, t$$

so $x^{-1}ax = x^{-1}b_1^{n_1} \cdots b_t^{n_t} x = (x^{-1}b_1x)^{n_1}(x^{-1}b_2x)^{n_2} \cdots (x^{-1}b_tx)^{n_t}$. $H \lhd G$, $K \lhd G$, so $x^{-1}b_ix \in H \vee K, i = 1, 2, \ldots, t$ and

$$x^{-1}ax = (x^{-1}b_1x)^{n_1}(x^{-1}b_2x)^{n_2} \cdots (x^{-1}b_tx)^{n_t} \in H \vee K$$

$H \vee K \lhd G$.

(b) Actually, in **Exercise 1.2.19** and (a), we have proved lub exists. Now we only consider glb. For $H \lhd G$, $K \lhd G$. If $H \cap K \lhd G$, then their glb is $H \cap K$. If not, assume there exists $A < H \cap K$, $B < H \cap K$, A, B are both normal in H and K. And there doesn't exists I s.t. $A \lhd I \lhd H$, $A \lhd I \lhd K$, $B \lhd I \lhd H$, $B \lhd I \lhd K$. Just like the figure:



But $A < H \cap K$, $B < H \cap K \Rightarrow A \vee B < H \cap K$. So $A \vee B \lhd H$, $A \vee B \lhd K$. That's contradictory! There is only one lower bound for $\{H, K\}$. Notice that $\{e\} < H \cap K$ so there exists at least one subgroup satisfies the condition. We have proved normality forms a lattice.

Exercise 1.5.14. If $N_1 \lhd G_1$, $N_2 \lhd G_2$ then $(N_1 \times N_2) \lhd (G_1 \times G_2)$ and $(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$.

Answer. Take $a \in (N_1 \times N_2)$, $a = (n_1, n_2)$ where $n_1 \in N_1$, $n_2 \in N_2$. $\forall x \in (G_1 \times G_2)$, $x = (g_1, g_2)$ where $g_1 \in G_1$, $g_2 \in G_2$. $x^{-1} = (g_1^{-1}, g_2^{-1})$, $x^{-1}ax = (g_1^{-1}n_1g_1, g_2^{-1}n_2g_2)$. $N_1 \lhd G_1$, $N_2 \lhd G_2$, so $g_1^{-1}n_1g_1 \in N_1$, $g_2^{-1}n_2g_2 \in N_2$. $x^{-1}ax \in (N_1 \times N_2)$. Thus $(N_1 \times N_2) \lhd (G_1 \times G_2)$.
Assume $G_1 = \bigcup_{i \in I} N_1a_i$, $G_2 = \bigcup_{j \in J} N_2b_j$. Then $G_1 \times G_2 = \bigcup_{i \in I} N_1a_i \times \bigcup_{j \in J} N_2b_j$. Denote $A = \{a_i | i \in I\}$, $B = \{b_j | j \in J\}$. We construct two bijections $(G_1 \times G_2)/(N_1 \times N_2) \to A \times B$ and $(G_1/N_1) \times (G_2/N_2)$.

$$f : N_1a_i \times N_2b_j \mapsto (a_i, b_j)$$

$$g : (N_1 a_i, N_2 b_j) \mapsto (a_i, b_j)$$

Take $h = g^{-1} \circ f$, f, g are bijections, so h is an isomorphism. $(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$.

Exercise 1.5.15. Let $N \lhd G$ and $K \lhd G$. If $N \cap K = \langle e \rangle$ and $N \vee K = G$, then $G/N \cong K$.

Answer. Assume $G = \bigcup_{i \in I} N a_i$, we construct $f : k \to G/N$. We prove that $\forall x, y \in K$, x, y belong to different cosets of N. Suppose not. $\exists x, y \in K$, $x, y \in N a_i$, then $xy^{-1} \in N \Rightarrow x = y$. That's contradictory! So f is a monomorphism.
$G = H \vee K$, so $G = HK$. we can write x as pq, where $p \in H$, $q \in K$. $|G/H| = [G : H] = [HK : H] = [K : K \cap H] = |K|$. f is a epimorphism.
Thus, $G/N \cong K$.

Exercise 1.5.16. If $f : G \to H$ is a homomorphism, H is abelian and N is a subgroup of G containing $\mathrm{Ker} f$, then N is normal in G.

Answer. Assume there exists $x \in G$, $x \notin N$ s.t. $f(x) \in f(N)$. $\exists n \in N$, $f(x) = f(n)$, $f(xn^{-1}) = f(x)f(n)^{-1} = e' \Rightarrow xn^{-1} \in \mathrm{Ker} f \Rightarrow x \in N$. That's contradictory! $\forall x \in G$, $n \in N$, $f(x^{-1}nx) = f(x^{-1})f(n)f(x) = f(n) \in f(N)$, so $x^{-1}nx \in N$. Thus, $N \lhd G$.

Exercise 1.5.17. (a) Consider the subgroups $\langle 6 \rangle$ and $\langle 30 \rangle$ of $\mathbf{Z}$ and show that $\langle 6 \rangle / \langle 30 \rangle \cong Z_5$.
(b) For any $k, m > 0$, $\langle k \rangle / \langle km \rangle \cong Z_m$; in particular, $\mathbf{Z}/\langle m \rangle = \langle 1 \rangle / \langle m \rangle \cong Z_m$.

Answer. (a) $\langle 6 \rangle = \{6n | n \in \mathbf{Z}\}$, $\langle 30 \rangle = \{30n | n \in \mathbf{Z}\}$. So $\langle 6 \rangle / \langle 30 \rangle = \{\langle 30 \rangle, \langle 30 \rangle + 6, \langle 30 \rangle + 12, \langle 30 \rangle + 18, \langle 30 \rangle + 24\} \cong Z_5$
(b) $\langle km \rangle \lhd \langle k \rangle$, $\langle k \rangle = \bigcup_{i \in I} (\langle km \rangle + a_i)$. For $x \in \langle k \rangle$, $x \equiv a_i \mod km$, then $x \in \langle km \rangle + a_i$. $f : \langle k \rangle / \langle km \rangle \to \{a_i | i \in I\}$ defined by $f(\langle km \rangle + a_i) = a_i$ is a bijection. We check that $g : \{a_i | i \in I\} \to Z_m$ is also a bijection. Define

$b_i \equiv \frac{a_i}{k} \mod m$, $g(a_i) = b_i$. If there exists $b_i = b_j$ for $i \neq j$, $a_i \equiv a_j \mod km$. That's contradictory! So g is an injection. g is obviously a surjection, so g is a bijection. Take $h = g \circ f : \langle k \rangle / \langle km \rangle \to Z_m$ is a isomorphism, so $\langle k \rangle / \langle km \rangle \cong Z_m$.

Exercise 1.5.18. If $f : G \to H$ is a homomorphism with kernel N and $K < G$, then prove that $f^{-1}(f(K)) = KN$. Hence $f^{-1}(f(K)) = K$ if and only if $N < K$.

Answer. Take $x \in f^{-1}(f(K))$, then there exists $k \in K$ s.t. $f(x) = f(k)$. $f(xk^{-1}) = f(x)f(k)^{-1} = e' \in f(K) \Rightarrow xk^{-1} \in \text{Ker}f = N$. Thus, $x \in Nk \subset NK$, $f^{-1}(f(K)) \subset NK$.
$\forall x = nk \in NK$, where $n \in N$ and $k \in K$. $f(x) = f(n)f(k) = e'f(k) \in f(K)$, so $NK \subset f^{-1}(f(K))$.
Thus, $f^{-1}(f(K)) = NK$. Hence $f^{-1}(f(K)) = K$ if and only if $N < K$.

Exercise 1.5.19. If $N \lhd G$, $[G : H]$ finite, $H < G$, $|H|$ finite, and $[G : N]$ and $|H|$ are relatively prime, then $H < N$.

Answer. $N \lhd G \Rightarrow NH < G$. By the second isomorphism theorem, $NH/N \cong H/H \cap N \Rightarrow [NH : N] = [H : H \cap N]$. Assume $[G : N] = m$, $|H| = n$, $|G| = mnp$ where $(m, n) = 1$. Then $|N| = np$, $N < NH$, assume $|NH| = knp$, $NH < G \Rightarrow knp|mnp \Rightarrow k|m$. $[NH : N] = [H : H \cap N] = k \Rightarrow k|n$. So $k = 1$, $NH = N$ which means $H < N$.

Exercise 1.5.20. If $N \lhd G$, $|N|$ finite, $H < G$, $[G : N]$ finite, and $[G : H]$ and $|N|$ are relatively prime, then $N < H$.

Answer. $N \lhd G \Rightarrow NH < G$. By the second isomorphism theorem, $NH/N \cong H/H \cap N \Rightarrow [NH : N] = [H : H \cap N]$. Assume $[G : H] = m$, $|N| = n$, $|G| = mnp$ where $(m, n) = 1$. Then $|H| = np$, $H < NH$, assume $|NH| = knp$, $NH < G \Rightarrow knp|mnp \Rightarrow k|m$. $[NH : N] = [H : H \cap N] = kp \Rightarrow kp|np \Rightarrow k|n$. So $k = 1$, $NH = H$ which means $N < H$.

Exercise 1.5.21. If H is a subgroup of $Z(p^\infty)$ and $H \neq Z(p^\infty)$, then $Z(p^\infty)/H \cong Z(p^\infty)$.

Answer. From **Exercise 1.3.7**(b), we know that H has the form $\left\langle \frac{\bar{1}}{p^n} \right\rangle$. Take $x_i = \frac{\bar{1}}{p^{n+i}} + H$, $x_1 = \frac{\bar{1}}{p^{n+1}} + H$.

$$\sum_{m=1}^{p} x_1 = \frac{\bar{p}}{p^{n+1}} + pH = \frac{\bar{1}}{p^n} + H = H$$

$$\sum_{m=1}^{p} x_i = \frac{\bar{p}}{p^{n+i}} + pH = \frac{\bar{1}}{p^{n+i-1}} + H = x_{i-1}$$

Take $A = \{x_i | i \in \mathbf{Z}_+\}$, $\langle A \rangle \cong Z(p^\infty)$ by **Exercise 1.3.7**(e). $\forall x \in \langle A \rangle$, $x \in Z(p^\infty)/H$, so $\langle A \rangle \subset Z(p^\infty)/H$. Take $x \in Z(p^\infty)/H$, $x = y + H$ where $y = \sum_{i=1}^{m} \frac{a_i}{p^{n+i}}$, $x = \sum_{i=1}^{m} (\frac{a_i}{p^{n+i}} + H) \in \langle A \rangle$. Thus, $Z(p^\infty)/H \subset \langle A \rangle$, $\langle A \rangle = Z(p^\infty)/H \cong Z(p^\infty)$.

1.6 Symmetric, alternating, and dihedral groups

Exercise 1.6.1. Find four different subgroups of S_4 that are isomorphic to S_3 and nine isomorphic to S_2.

Answer. $S_4 = \{(1), (12), (13), (14), (23), (24), (34), (123), (124), (132), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23), (1234), (1243), (1324), (1342), (1423), (1432)\}$.
$A_1 = \{(1), (12), (13), (23), (123), (132)\}$;
$A_2 = \{(1), (12), (14), (24), (124), (142)\}$;
$A_3 = \{(1), (13), (14), (34), (134), (143)\}$;
$A_4 = \{(1), (23), (24), (34), (234), (243)\}$;
$A_1 \cong A_2 \cong A_3 \cong A_4$.
$B_1 = \{(1), (12)\}$; $B_2 = \{(1), (13)\}$; $B_3 = \{(1), (14)\}$; $B_4 = \{(1), (23)\}$; $B_5 = \{(1), (24)\}$; $B_6 = \{(1), (34)\}$; $B_7 = \{(1), (12)(34)\}$; $B_8 = \{(1), (13)(24)\}$; $B_9 = \{(14)(23)\}$;
$B_1 \cong B_2 \cong B_3 \cong B_4 \cong B_5 \cong B_6 \cong B_7 \cong B_8 \cong B_9$.

Exercise 1.6.2. (a) S_n is generated by the $n-1$ transpositions (12), (13), (14), ..., $(1n)$.
(b) S_n is generated by the $n-1$ transpositions $(12), (23), (34), \ldots, (n-1\, n)$.

Answer. (a) $\forall x \in S_n$, x can be written as a product of transpositions. Actually, for any transposition (ij), we can obtain it by $(1i)(1j)(1i) = (ij)$. So $x \in \langle (12), (13), \ldots, (1n)\rangle$, $S_n \subset \langle (12), (13), \ldots, (1n)\rangle$.
(b) We can contruct $(1i)$ inductively since $(1i) = (1\, i-1)(i-1\, i)(1\, i-1)$. From (a), we have $\forall x \in S_n$, $x \in \langle (12), (13), \ldots, (1n)\rangle$. Thus $S_n \subset \langle (12), (13), \ldots, (1n)\rangle \subset \langle (12), (23), (34), \ldots, (n-1\, n)\rangle$.

Exercise 1.6.3. If $\sigma = (i_1 i_2 \cdots i_r) \in S_n$ and $\tau \in S_n$, then $\tau\sigma\tau^{-1}$ is the r-cycle $(\tau(i_1)\tau(i_2)\cdots\tau(i_r))$.

Answer. $\sigma(i_n) = i_{n+1}$ for $n = 1, 2, \ldots, r-1$, $\sigma(i_r) = i_1$. Assume $\tau(i_n) = j_n$, $n = 1, 2, \ldots, r-1$ and $I = \{i_n | n = 1, 2, \ldots, r-1\}$, $J = \{j_n | n = 1, 2, \ldots, r-1\}$. For $x \notin J$, $\tau\sigma\tau^{-1}(x) = \tau\tau^{-1}(x) = x$. For $x = j_k \in J$, $\tau^{-1}(x) = i_k$, $\sigma(\tau^{-1}(x)) = i_{k+1}$, $\tau(\sigma(\tau^{-1}(x))) = j_{k+1}$ and $\tau\sigma\tau^{-1}(j_r) = j_1$. Thus $\tau\sigma\tau^{-1} = (\tau(i_1)\tau(i_2)\cdots\tau(i_r))$.

Exercise 1.6.4. (a) S_n is generated by $\sigma_1 = (12)$ and $\tau = (123\cdots n)$.
(b) S_n is generated by (12) and $(23\cdots n)$.

Answer. (a) Denote $\sigma_i = \tau\sigma_{i-1}\tau^{-1}$. Applying **Exercise 1.6.3**, $\sigma_i = (i\, i+1)$. By **Exercise 1.6.2**(b), $S_n \subset \langle (12), (23), (34), \ldots, (n-1\, n)\rangle = \langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1}\rangle \subset \langle \tau, \sigma_1\rangle$. S_n can be generated by τ and σ_1.
(b) Denote $\sigma_1 = (12)$, $\tau = (23\cdots n)$, $\sigma_i = \tau\sigma_{i-1}\tau^{-1}$. Applying **Exercise 1.6.3**,$\sigma_i = (1\, i{+}1)$. By **Exercise 1.6.2**(a), $S_n \subset \langle (12), (13), \ldots, (1n)\rangle = \langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1}\rangle \subset \langle \tau, \sigma_1\rangle$. S_n can be generated by τ and σ_1.

Exercise 1.6.5. Let $\sigma, \tau \in S_n$. If σ is even (odd), then so is $\tau\sigma\tau^{-1}$.

Answer. Assume $\sigma = (x_1x_2)\cdots(x_{2n-1}x_{2n})$, $\tau = (y_1y_2)\cdots(y_{2m-1}y_{2m})$. Then $\tau^{-1} = (y_{2m-1}y_{2m})\cdots(y_1y_2)$. σ is odd (even) if an only if n is odd (even). $\tau\sigma\tau^{-1}$ has $2m+n$ transpositions. We can add $(ij) = (ji) = (1)$ into some segments of $\tau\sigma\tau^{-1}$ without changing it. So $\tau\sigma\tau^{-1}$ is odd (even) if and only if $2m+n$ is odd (even). $2m + n \equiv n \mod 2$ so $\tau\sigma\tau^{-1}$ is odd (even) if and only if σ is odd (even).

Exercise 1.6.6. A_n is the only subgroup of S_n of index 2.

Answer. For any subgroup $N < S_n$ and $[S_n : N] = 2$, we have $N \lhd S_n$.
Assume there exists k-circle $\sigma = (i_1i_2\cdots i_k) \in N$. Then for any other k-circle $(j_1j_2\cdots j_k)$, take $\tau = (i_ij_1)(i_2j_2)\cdots(i_kj_k)$, by **Exercise 1.6.3**, $\tau\sigma\tau^{-1} = (j_1j_2\cdots j_k) \in N$. Thus N contains all the k-circles.
For $n \geq 5$. If there exists 3-circle in N, then all the 3-circles are contained in N, $A_n \subset N \subset S_n \Rightarrow A_n = N$.
If there exists 2-circle in N, then all the 2-circles are contained in N. Notice $(1i)(1j) = (1ij) \in N$ is a 3-circle, so $A_n = N$.
If there only contain x in the form of $(a_ia_2\cdots a_{n_1})(b_1b_2\cdots b_{n_2})\cdots$ where $n_i \geq 4$ and every two circles are disjoint. Take $\tau_i : \{a_i | i = 1, 2, \ldots, n_1\} \to \{a_i | i = 1, 2, \ldots, n_1\}$. We can obtain product of two n_1-circles

$$x^{-1}\tau x\tau^{-1} = (a_1a_2\cdots a_{n_1})(\tau(a_1)\tau(a_2)\cdots\tau(a_n)) \in N$$

By the arbitrariness of τ, take

$$(\tau(a_1)\tau(a_2)\cdots\tau(a_n)) = (a_1a_4a_5\cdots a_na_3a_2)^{-1}$$

then $x^{-1}\tau x\tau^{-1} = (a_1a_3)(a_2a_4)$ is a product of 2-circles. We can take a_1, a_2, a_3, a_4 arbitrarily. WLOG, take $(12)(34) \in N$ and $(12)(35) \in N$, $(12)(34)(12)(35) = (345) \in N$. Then there exists 3-circle in N, $N = A_n$.
In conlusion, when $n \geq 5$, S_n has only one normal subgroup A_n.
For $n = 2, 3, 4$, we can verify it by enumeration.

Exercise 1.6.7. Show that $N = \{(1), (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of S_4 contained in A_4 such that $S_4/N \cong S_3$ and $A_4/N \cong Z_3$.

Answer. Assume $\sigma = (i_1i_2)(i_3i_4) \in N$, $\forall\tau \in S_4$, $\tau(i_n) = j_n$, $J = \{j_n | n = 1, 2, 3, 4\}$. For $x \notin J$, $\tau\sigma\tau^{-1}(x) = \tau\tau^{-1}(x) = x$. For $x = j_k \in J$, $\tau^{-1}(x) = i_k$, $\sigma\tau^{-1}(x) = i_{3k-4\left[\frac{k}{2}\right]-1}$, $\tau\sigma\tau^{-1}(x) = (\tau(i_i)\tau(i_2))(\tau(i_3)\tau(i_4)) \in N$. So $N \lhd S_4$. $S_4/N = \{N, N(12), N(13), N(23), N(123), N(132)\} \cong S_3$. $A_4/N = \{N, N(123), N(132)\} \cong Z_3$.

Exercise 1.6.8. The group A_4 has no subgroup of order 6.

Answer. $|A_4| = 12$, assume there exists $N < A_4$, $|N| = 6$. Then $N \lhd A_4$. From **Exercise 1.6.6**, we know that all 3-circles are contained in N. But there're 8 3-circles in total, so N can't exist.

Exercise 1.6.9. For $n \geq 3$ let G_n be the multiplicaive group of complex matrices generated by $x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $y = \begin{pmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{pmatrix}$, where $i^2 = -1$. Show that $G_n \cong D_n$.

Answer. Take a mapping $f : G_n \to D_n$ as $f(x) = (2\,n)(3\,n-1)\cdots$, $f(y) = (123\cdots n)$. $|f(x)| = |x| = 2$, $|f(y)| = |y| = n$. f is obviously a monomorphism. $\forall a \in D_n$, $a = f(x)^n f(y)^m, m = 1, 2$, then $a = f(x^n y^m)$, f is a epimorphism. Thus $G_n \cong D_n$.

Exercise 1.6.10. Let a be the generator of order n of D_n. Show that $\langle a\rangle \lhd D_n$ and $D_n/\langle a\rangle \cong Z_2$.

Answer. $|\langle a\rangle| = n$, b is the other generator of D_n, $a^n = b^2 = (1)$. $\forall k \in \mathbf{Z}$, $a^k b = ba^{-k}$ can be easily proved by induction. So $\forall x = a^m b^n \in D_n$, $x = a^{m'}b^{n'}$, here $m' \equiv m \mod 2$, $n' \equiv n \mod 2$. $D_n = \{e, a, a^2, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1}\}$. $|D_n| = 2n$. Thus, $\langle a\rangle \lhd D_n$. $D_n/\langle a\rangle = \{\langle a\rangle, \langle a\rangle b\} \cong Z_2$.

Exercise 1.6.11. Find all normal subgroups of D_n.

Answer. The subgroups of $\langle a\rangle$ is always normal in D_n. $\langle a^m\rangle < \langle a\rangle$. $\forall x \in D_n$ and $a^{km} \in \langle a^m\rangle$, $x = a^t$ or $x = ba^t$.

$$x^{-1}a^{km}x = a^{-t}a^{km}a^t = a^{km} \in \langle a^m\rangle$$

or

$$x^{-1}a^{km}x = a^{-t}b^{-1}a^{km}ba^t = a^{-t}ba^{km}ba^t = a^{-t}a^{-km}b^2a^t = a^{-km} \in \langle a^m\rangle$$

so $\langle a^m\rangle \lhd D_n$.
Consider the subgroup S which only contains $ba^i, i = 1, \ldots, n$. Since $ba^i \cdot ba^j = a^{j-i} \in S\,(i \neq j)$, so $S = \{e, ba^k\}$.
If n is odd, take $x = a^{\frac{n-1}{2}} \in D_n$.

$$x^{-1}ba^kx = a^{\frac{1-n}{2}}ba^ka^{\frac{n-1}{2}} = ba^{k+n-1} \notin S$$

so $S \not\lhd D_n$ for all $k = 1, 2, \ldots, n$.
If n is even, take $x = a^{\frac{n-2}{2}} \in D_n$, $n \geq 6$.

$$x^{-1}ba^kx = a^{\frac{2-n}{2}}ba^ka^{\frac{n-2}{2}} = ba^{k+n-2} \notin S$$

so $S \not\lhd D_n$ for all $k = 1, 2, \ldots, n$.
If $n = 2$, all the subgroups are normal since $|D_2| = 4$.
For subgroup S contains both ba^i and a^j. It can be written as $S = \langle a^d, ba^r\rangle$, where $d|n$, $0 \leq r \leq d-1$. If $\exists a^m, a^n \in S$, $(m, n) = d$, then there exist $x, y \in \mathbf{Z}$ s.t. $a^{mx+ny} = a^d \in \mathbf{Z}$. Thus, $S = \langle a^d, ba^r\rangle$.
Take $x = a^{\frac{n-w}{2}}$, then $x^{-1}ba^rx = ba^{r+n-w}$.

If $d \geq 3$, take $w \equiv n \mod 2$, $x^{-1}ba^r x \notin S$.
If $d = 2$, then $n = 2s$ and $S = \{e, a^s, ba^s, b\}$. $Sa^k = \{a^k, a^{s+k}, ba^{s-k}, ba^{-k}\}$, $k = 1, 2, \ldots, s-1$. $ba^k = ba^{-k}$ or $ba^k = ba^{s-k} \Rightarrow k = \frac{s}{2}$. So for $s = 2$, $n = 4$, S is a normal subgroup of D_4.

Exercise 1.6.12. The center of the group D_n is $\langle e \rangle$ if n is odd and isomorphic to Z_2 if n is even.

Answer. If n is odd, C is the center of D_n, $C \lhd D_n \Rightarrow C < \langle a \rangle$. Take $a^d \in C$, $x = ba^m$,

$$x^{-1}ax = a^{-m}b^{-1}a^d ba^m = a^{-m}ba^d ba^m = a^{-d} = a^d$$

so $d = 0$, $C = \{e\}$.
If n is even, $n \geq 6$. C is the center of D_n. $C \lhd D_n \Rightarrow C < \langle a \rangle$ or $C = \{e, ba^k\}$.
If $C = \{e, ba^k\}$, $C \cong Z_2$.
If $C < \langle a \rangle$,take $a^d \in C$, $x = ba^m$,

$$x^{-1}ax = a^{-m}b^{-1}a^d ba^m = a^{-m}ba^d ba^m = a^{-d} = a^d$$

so $d = \frac{n}{2}$ or $d = 0$, $C = \{a^{\frac{n}{2}}, e\} \cong Z_2$.

Exercise 1.6.13. For each $n \geq 3$ let P_n be a regular polygon of n sides (for $n = 3$, P_n is an equilateral triangle; for $n = 4$, a square). A *symmetry* of P_n is a bijection $P_n \to P_n$ that preserves distances and maps adjacent vertices on to adjacent vertices.

(a) The set D_n^* of all symmetries of P_n is a group under the binary operation of composition of functions.

(b) Every $f \in D_n^*$ is completely determined by its actions on the vertices of P_n. Number the vertices consecutively $1, 2, \ldots, n$; then each $f \in D_n^*$ determines a unique permutation σ_f of $\{1, 2, \ldots, n\}$. The assignment $f \mapsto \sigma_f$ defines a monomorphism of groups $\varphi : D_n^* \to S_n$.

(c) D_n^* is generated by f and g, where f is a rotation of $2\pi/n$ degrees about the center of P_n and g is a reflection about the "diameter" through the center and vertex 1.

(d) $\sigma_f = (123 \cdots n)$ and $\sigma_g = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix}$, whence $\mathrm{Im}\varphi = D_n$ and $D_n^* \cong D_n$.

Answer. In the following analysis, all the numbers are $\mod n$.

(a) Consider n points $A_i = (\cos\frac{2\pi i}{n}, \sin\frac{2\pi i}{n})^t$, $i = 1, 2, \ldots, n$. f is the transposition of $A_i \mapsto A_j$ with the consevation of n regular polygon structure. So f must be a bijection. D_n^* is the set of f. By the definition, $D_n^* \subset S_n$. We prove D_n^* is ta subgroup of S_n.

Notice that $A_{i+1} = \begin{pmatrix} \cos\frac{2\pi i}{n} & -\sin\frac{2\pi i}{n} \\ \sin\frac{2\pi i}{n} & \cos\frac{2\pi i}{n} \end{pmatrix} A_i$.

Denote $X = \begin{pmatrix} \cos\frac{2\pi i}{n} & -\sin\frac{2\pi i}{n} \\ \sin\frac{2\pi i}{n} & \cos\frac{2\pi i}{n} \end{pmatrix}$. To construct the polygon, we must have

$$f(A_{i+1}) = \begin{pmatrix} \cos\frac{2\pi i}{n} & -\sin\frac{2\pi i}{n} \\ \sin\frac{2\pi i}{n} & \cos\frac{2\pi i}{n} \end{pmatrix} f(A_i)$$

or

$$f(A_i) = \begin{pmatrix} \cos\frac{2\pi i}{n} & -\sin\frac{2\pi i}{n} \\ \sin\frac{2\pi i}{n} & \cos\frac{2\pi i}{n} \end{pmatrix} f(A_{i+1})$$

We need to verify that $\forall f_1, f_2 \in D_n^*$, $f_1 f_2^{-1} \in D_n^*$. Assume $B_i = f_2(A_i)$, $B_{i+1} = f_2(A_{i+1})$. Then $B_i = XB_{i+1}$ or $B_i = X^{-1}B_{i+1}$. Denote $B_i = A_j$, then $B_{i+1} = A_{j-1}$ or $B_{i+1} = A_{j+1}$. WLOG, assume $B_{i+1} = A_{j+1}$, then $f_1(A_j) = Xf_1(A_{j+1})$ or $f_1(A_j) = X^{-1}f_1(A_{j-1})$. So $f_1 f_2^{-1} \in D_n^*$. D_n^* is a subgroup of S_n.

(b) Assume $A_i = f(A_1)$. If $f(A_2) = A_{i+1}$, since f is a bijection, by induction, we can prove $f(A_k) = A_{k+i-1}$. $\varphi : D_n^* \to S_n$ can be defined as $\varphi : f \mapsto (1i\,2i{-}1\,3i{-}2\cdots)$. If $f(A_2) = A_{i-1}$, similarly, we can also prove $f(A_k) = A_{i+1-k}$. φ can be defined as $\varphi : f \mapsto (1i)(2\,i-1)(3\,i-2)\cdots$. This means f is completely determined by $f(A_1)$ and $f(A_2)$. D_n^* can be embedded into S_n.

(c) Denote $\alpha = \begin{pmatrix} \cos\frac{2\pi i}{n} & -\sin\frac{2\pi i}{n} \\ \sin\frac{2\pi i}{n} & \cos\frac{2\pi i}{n} \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $f : A_i \mapsto \alpha A_i$, $g : A_i \mapsto \beta A_i$. f is the rotation of $\frac{2\pi}{n}$ degrees counter-clockwisely. g is the reflection about x-axis. Now we prove $\forall x \in D_n^*$, x can be factorised into finite product of f and g. From (b), x is fully defined by $x(A_1)$ and $x(A_2)$. Assume $x(A_1) = A_i$.

If $x(A_2) = A_{i+1}$, $x(A_k) = A_{i-1+k} = \alpha^{i-1}A_k$, $k = 1, 2, \ldots, n$. So $x = f^{i-1}$.

If $x(A_2) = A_{i-2}$, $x(A_k) = A_{i+1-k} = \alpha^{i+1}A_{-k} = \alpha^{i+1}\beta A_k$. So $x = f^{i+1}g$. Thus $D_4^* \subset \langle f, g\rangle$.

(d) $\alpha^n = \beta^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. We can easily verify that $|f| = n$ and $|g| = 2$. From **Exercise 1.6.9**, $\langle f, g\rangle \cong D_n$, $|\langle f, g\rangle| = |D_n| = 2n$. From (b), $x \in D_n^*$

if completely determined by $x(A_1)$ and $x(A_2)$. There are $2n$ different ways to obtain $x(A_1)$ and $x(A_2)$. So $|D_n^*| = |\langle f, g\rangle| = 2n$. $D_n^* \subset \langle f, g\rangle$, so $D_n^* = \langle f, g\rangle$. Thus, $D_n^* \cong \langle f, g\rangle \cong D_n$.