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

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

1. 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].
2. The set $\mathbf{Q}/\mathbf{Z}$ of equivalence classes is an infinite abelian group.

Answer.

1. 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.
2. 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 ⇒ 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. $G = \bigcup\limits_{a \neq e} \{a, a^{-1}\} \cup \{e\}$. Notice that $\{a, a^{-1}\} \cap \{b, b^{-1}\} = \oslash$ 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 $x \to x a_{n+2}$ yields a function $\phi : \mathbf{N} \to G$. Let $\Psi = \phi\theta$, where $\theta : \mathbf{N}^* \to \mathbf{N}$ is given by $k \to k - 1$.

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 $x \to x^{-1}$ 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: $Q_8 = \{A, A^2, B, B^2, AB, A^2B, AB^2, I\}$. 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.

1. $\mathrm{Ker} f$ and $f^{-1}(B)$ are subgroups of G.
2. $f(A)$ is a subgroup of H.

Answer.

1. f is a homomorphism, so $f(e) = e', e \in \mathrm{Ker} f$. $\forall a \in \mathrm{Ker} f$, $f(aa^{-1}) = f(a)f(a^{-1}) = e'$, so $f(a^{-1}) = f(a)^{-1} = e'^{-1} = e'$. $\forall a, b \in \mathrm{Ker} f, f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e' \Rightarrow ab^{-1} \in \mathrm{Ker} f$, which means $\mathrm{Ker} f$ is a subgroup of G. The proof of $f^{-1}(B)$ is a subgroup of G is similar.
2. 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 $C = \{a \in G | ax = xa$ 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 $f(x) = f(a^m) = f(a)^m \Rightarrow \text{Im} f = \langle f(a) \rangle$. $f : a^m \to f(a)^m \forall m \in \mathbf{N}$. 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.

1. Aut$G$ is a group with composition of functions as binary operation.
2. 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).
3. What is $\mathrm{AutZ_n}$ 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 $\sigma \in \text{Aut}Z_n$, σ is completely determined by $\sigma(\bar{1}) = \bar{a}$, and we denote σ as σ_a. For $\sigma_a, \sigma_b \in \text{Aut}Z_n$, $\sigma_a(\sigma_b(\bar{1})) = \sigma_a(\bar{b}) = \overline{ab} = \sigma_{ab}(\bar{1})$. We have proved 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 $(x \mod n) \to (x \mod s, x \mod t)$. 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 $x \in$ Kerf^*, $x \equiv 1 \mod s$, $x \equiv 1 \mod t$, 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 $S(d) = \{\bar{a} \in Z_p^* | \text{ord}_p(a) = d\}$. $S(d)$ forms a partition of Z_p^*. If $S(d) \neq \emptyset$, 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 $\{1, a, a^2, \dots, a^{d-1}\}$ are the solutions of the equation, $a^i \not\equiv a^j \mod p$, whence $S(d) \subset \langle \bar{a} \rangle$. For $k = 1, 2, \dots, d-1$, $\text{ord}_p(\bar{a^k}) = \left|a^k\right| = \frac{d}{(d,k)} = d \Leftrightarrow (d, k) = 1$. Thus $|S(d)| = \varphi(d)$.
From $Z_p^* = \bigcup\limits_{d|p-1} S(d)$, 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 $(a \mod p^s) \to (a \mod p^t)$. Since $a \equiv b \mod p^s \Rightarrow a \equiv b \mod p^t$, f is well defined. $\text{Ker} f_{s,t} = \{up^t + 1 \mod p^s | u = 0, 1, \dots, p^{s-t} - 1\}$. If $2t \geq s$, since $(up^t + 1)(vp^t + 1) \equiv uvp^{2t} + (u + v)p^t + 1 \equiv (u + v)p^t + 1 \mod p^s$, $\text{Ker} f_{s,t} \cong Z_{p^{s-t}}$ is a cyclic group. There exists a isomorphism $g_{s,t} : Z_{p^s}^* / \text{Ker} f_{s,t} \to Z_{p^t}^*$.

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

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

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

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 $\{\overline{1/p^n}|n \in \mathbf{N}^*\}$.

Answer. We prove that $\left\langle \bigcup\limits_{n=1}^{\infty} \frac{1}{p^n} \right\rangle \cong Z(p^\infty)$. $\forall x \in Z(p^\infty), x = \frac{\bar{a}}{b} = \frac{\bar{a}}{p^k}$. Expand a as $a = \sum\limits_{i=0}^{k-1} p^i a_i$, where $a_i = 1, 2, \ldots n-1$. $x = \frac{\bar{a}}{b} = \sum\limits_{i=0}^{k-1} \frac{\bar{a_i}}{p^{k-i}} = \sum\limits_{i=1}^{k} \overline{\frac{a_{k-i}}{p^i}}$. Denote $f : \left\langle \bigcup\limits_{n=1}^{\infty} \frac{1}{p^n} \right\rangle \to Z(p^\infty)$ as $f(\sum\limits_{i=1}^{n} \frac{a_i}{p^i}) = \overline{\sum\limits_{i=1}^{n} \frac{a_i}{p^i}}$. 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. $\left\langle \bigcup\limits_{i=1}^{n} H_i \right\rangle = \{\prod\limits_{i=1}^{n} h_i | h_i \in H_i, i = 1, 2, \ldots n\}$. 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 $\bigcup\limits_{i\in I} H_i$ is a subgroup, that is $\bigcup\limits_{i\in I} H_i = \left\langle \bigcup\limits_{i\in I} H_i \right\rangle$.
2. Given an example of a group G and a family of subgroups $\{H_i | i \in I\}$ such that $\bigcup\limits_{i\in I} H_i \neq \left\langle \bigcup\limits_{i\in I} H_i \right\rangle$.

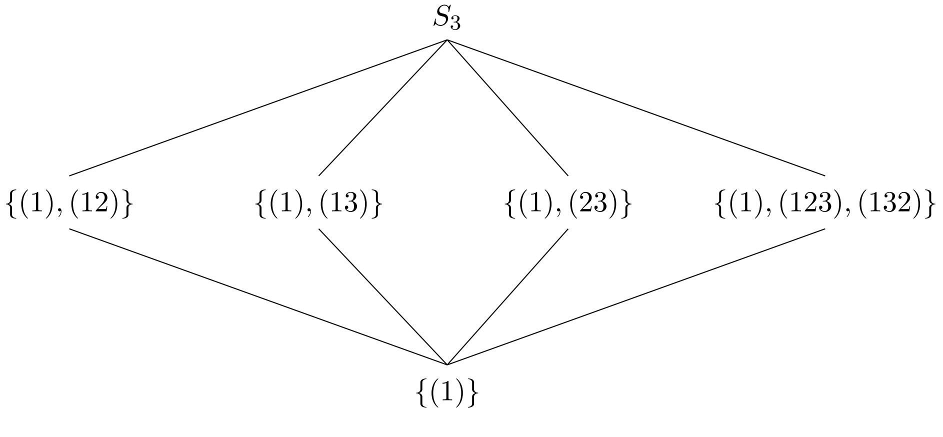
Answer. I didn't find a sufficient and necessary condition for this question, just choose one as you like:)

Exercise 1.2.19.

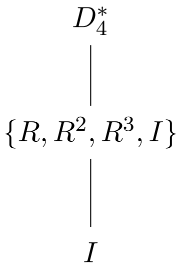
1. The set of all subgroups of a group G, partially ordered by set theoretic inclusion, forms a complete lattice in which the g.l.b of $\{H_i | i \in I\}$ is $\bigcap\limits_{i\in I} H_i$ and the l.u.b is $\left\langle \bigcap\limits_{i\in I} H_i \right\rangle$.
2. Exhibit the lattice of subgroups of the groups S_3, D_4^*, Z_6, Z_{27} and Z_{36}.

Answer.

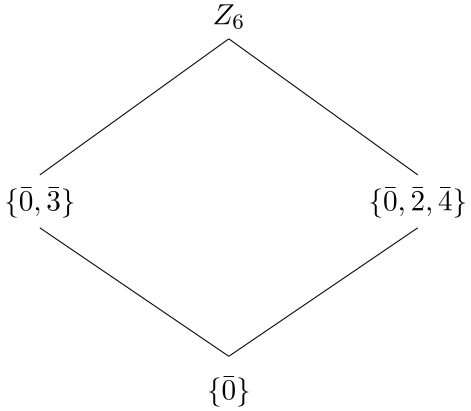
1. The subset relation $<$ forms a partially ordered relation. By the difinition of $\left\langle \bigcup\limits_{i\in I} H_i \right\rangle$, $\left\langle \bigcup\limits_{i\in I} H_i \right\rangle$ is the smallest set contains $\bigcup\limits_{i\in I} H_i$, so it's lup. For glb, we know that $\bigcap\limits_{i\in I} H_i \subset H_i \ \forall i \in I$, and $\forall H \supset \bigcap\limits_{i\in I} H_i$, there exists $x \in H, x \notin H_j \ j \in I$, so $\bigcap\limits_{i\in I}$ is glb.
2. $S_3 = \{(1), (12), (13), (23), (123), (132)\}$.



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



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



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 $c \in G$.

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.

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.

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 $|a|$.

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.

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.

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 $C_n = \left\langle 1\bar{/}p^n \right\rangle$ $(n = 1, 2, \ldots)$. Futhermore, $\langle 0 \rangle = C_0 < C_1 < C_2 < C_3 < \cdots$.

(e) Let $x_1, x_2, \ldots$ be elements of an abelian group G such that $|x_1| = p, px_2 = x_1, px_3 = x_2, \ldots, px_{n+1} = x_n, \ldots$. The subgroup generated by the $x_i (i \geq 1)$ is isomorphic to $Z(p^{\infty})$.

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

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