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 commutative.
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 commutative.

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 $\mathbf{Q}/\mathbf{Z}$:

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

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

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

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

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$\Rightarrow$ i is false if 'three' is replaced by 'two'.

Answer. i$\Leftrightarrow$ 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 $\Rightarrow$ v, iv$\Rightarrow$ ii and i$\Rightarrow$ iv are trivial.
ii$\Rightarrow$ 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. $G = \bigcup\limits_{a \neq e} \{a, a^{-1}\} \cup \{e\}$. 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 commutative. $\forall a, b \in C, x \in G$, $b^{-1} \in G$, 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 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 $x \in$ 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 $S(d) = \{\bar{a} \in Z_p^* | \mathrm{ord}_p(a) = d\}$. $S(d)$ 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 $k = 1, 2, \ldots, d-1$, $\mathrm{ord}_p(\overline{a^k}) = \left|a^k\right| = \frac{d}{(d,k)} = d \Leftrightarrow (d,k) = 1$. 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 $(a \mod p^s) \mapsto (a \mod p^t)$. 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, $\mathrm{Ker} f_{3,1} = \left\langle p \bar{+} 1_{p^3} \right\rangle \cong Z_{p^2}$, 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 $a \in g_{k,1}^{-1}(x)$, $g_{k,1}^{-1}(x) = a\text{Ker}f_{k,1}$, and $a^{p-1} \in g_{k,1}^{-1}(x^{p-1}) = g_{k,1}^{-1}(\bar{1}_p) = \text{Ker}f_{k,1}$. If $a^{p-1} \notin \text{Ker}f_{k,2}$, then $\left|a^{p-1}\right| = p^{k-1}$. If $a^{p-1} \in \text{Ker}f_{k,2}$, $\forall h \in \text{Ker}f_{k,1}, h \notin \text{Ker}f_{k,2}$. Since $(ah)^{p-1} = (a^{p-1}h^p)h^{-1}$, $(ah)^{p-1} \in \text{Ker}f_{k,1}, (ah)^{p-1} \notin \text{Ker}f_{k,2}$, whence $\left|(ah)^{p-1}\right| = p^{k-1}$, $Z_{p^k}^* \cong Z_{(p-1)p^{k-1}}$.
If $p = 2$, $Z_{2^k}^* = \text{Ker}f_{k,1} \cong Z_{2^{k-2}} \oplus Z_2$.
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 $\mathbf{Q/Z}$ is generated by the set $\{1/\bar{p}^n|n \in \mathbf{N}^*\}$.

Answer. We prove that $\left\langle \bigcup_{n=1}^{\infty} \frac{1}{p^n} \right\rangle \cong Z(p^\infty)$. $\forall x \in Z(p^\infty), x = \frac{\bar{a}}{b} = \frac{\bar{a}}{p^k}$. Expand a as $a = \sum_{i=0}^{k-1} p^i a_i$, where $a_i = 1, 2, \dots n-1$. $x = \frac{\bar{a}}{b} = \sum_{i=0}^{k-1} \frac{\bar{a_i}}{p^{k-i}} = \sum_{i=1}^{k} \frac{a_{\bar{k}-i}}{p^i}$. Denote $f : \left\langle \bigcup_{n=1}^{\infty} \frac{1}{p^n} \right\rangle \to Z(p^\infty)$ as $f(\sum_{i=1}^{n} \frac{a_i}{p^i}) = \sum_{i=1}^{n^{-}} \frac{a_i}{p^i}$. 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, $H_1, H_2, \dots H_n$ are n subgroups. $\left\langle \bigcup_{i=1}^{n} H_i \right\rangle = \{\prod_{i=1}^{n} h_i | h_i \in H_i, i = 1, 2, \dots n\}$. 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 $\bigcup\limits_{i\in I} H_i \neq \left\langle \bigcup\limits_{i\in I} H_i \right\rangle$.

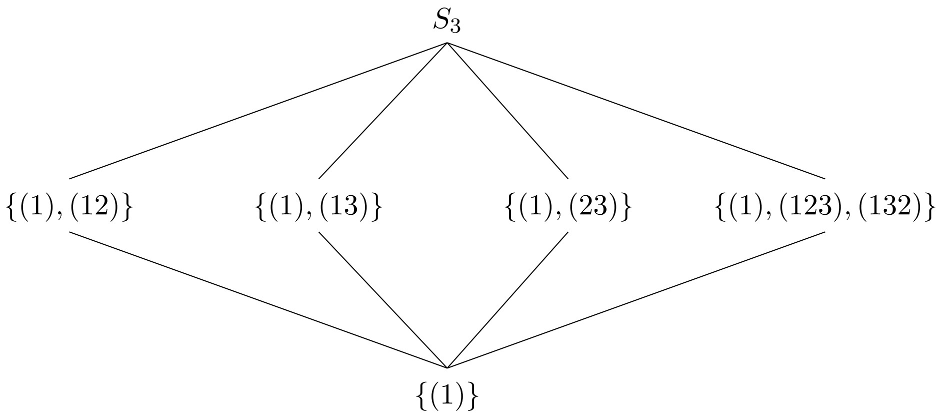
Answer. I didn't find a sufficient and necessary condition for this question, just choose one as you like:)

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}.

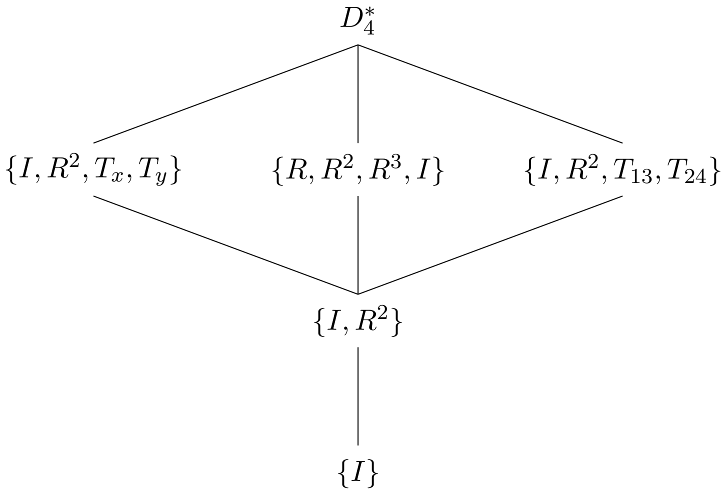
Answer.

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



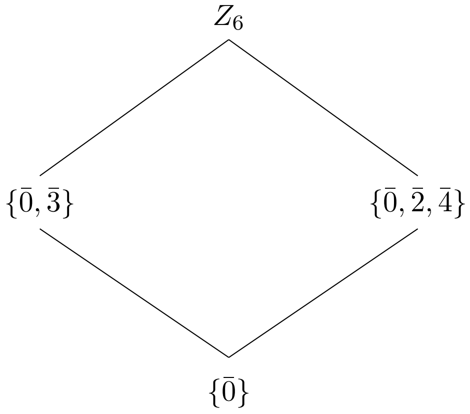
The Hasse figure of the lattice of S_3

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

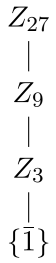


The Hasse figure of the lattice of D_4^*

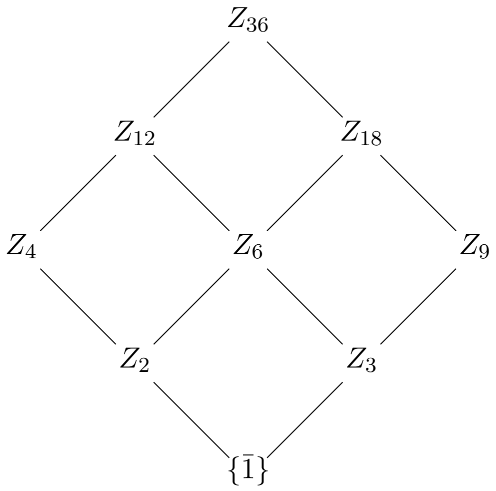
$Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.



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 $\overline{1/p^k}$, 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 $C_n = \left\langle \bar{1/p^n} \right\rangle$ $(n = 1, 2, \dots)$. 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 $a \in G$, $(\bigcap\limits_i H_i)a = \bigcap\limits_i H_i a$.

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

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 $|S| \mid |G| = p$. 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 commutative. 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 $p^k m$, 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 $HK < G$, $|HK| = p^k n$, $n|m$. 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 $x \in K\backslash H$. $K \bigcup\limits_{i\in I} Ha_i$, $\forall h_i \in H$ 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. $xn_1 = h_2n_2 = h_2an_1$. So $a = n_2n_1^{-1} \in N$, $a \in K \cap N = H \cap N \Rightarrow a \in H, x \in H$. 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) $ba = a^3 b = a^{-1} b$; (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 $\forall a \in G$, $aN_ia^{-1} = \{an_ia^{-1} | n_i \in N_i\} = N_i$. $\forall x = ana^{-1} \in a(\bigcap\limits_{i\in I} N_i)a^{-1}$, $n \in N_i \Rightarrow x \in a(\bigcap\limits_{i\in I} N_i)a^{-1} \subset \bigcap\limits_{i\in I} aN_ia^{-1} = \bigcap\limits_{i\in I} N_i$. $\bigcap\limits_{i\in I} N_i$ 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 $a_2b_2^{-1} \in N$, $a_1N = Na_1 = Nb_1 \Rightarrow a_1Nb_1^{-1} = N$. So $a_1a_2b_1^{-1}b_2^{-1} = (a_1a_2)(b_1b_2)^{-1} \in N$. Similarly, $(a_1a_2)^{-1}(b_1b_2) \in N$. 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 $a_1a_2 \equiv b_1b_2 \mod N$. 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 $a_2b_2^{-1}$, $a_2 \equiv b_2 \mod N$. $\forall a_1 \in G$ and $\forall b_1 \equiv a_1 \mod N$, $a_1nb_1^{-1} = a_1a_2b_2^{-1}b_1^{-1} \in N$. Take $b_1 = a_1$ and n varies in N, $a_1na_1^{-1} \in N \Rightarrow a_1Na_1^{-1} \subset N$. 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. $\forall a \in G$, $aNa^{-1} \subset N$. $\forall a_1, b_1, a_2, b_2 \in G$, $a_1b_1^{-1} \in N$, $a_2b_2^{-1} \in N$. $a_1a_2(b_1b_2)^{-1} = a_1a_2b_2^{-1}b_1^{-1}$, denote $n = a_2b_2^{-1} \in N$, $a_1a_2b_2^{-1}b_1^{-1} = a_1nb_1^{-1} \in a_1Nb_1^{-1}$. $\forall n \in N$, there exists $n' = b_1^{-1}a_1, n' \in N$ s.t. $a_1n = b_1n'$. So $a_1nb_1^{-1} = b_1n'b_1^{-1} \in b_1Nb_1^{-1} \subset N$. That means $(a_1a_2)(b_1b_2)^{-1} \in N$, $a \sim b$ 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. $H < G$, $aHa^{-1} = \{aha^{-1} | h \in H\}$. $\forall x, y \in aHa^{-1}$, $x = ah_1a^{-1}$, $y = ah_2a^{-1}$. $y^{-1} = ah_2^{-1}a^{-1}$, $xy = ah_1h_2^{-1}a^{-1} \in aHa^{-1}$, so $aHa^{-1} < G$.
Take $f : H \to aHa^{-1}$ as $f(h) = aha^{-1}$. If $f(h_1) = f(h_2) = ah_1a^{-1} = ah_2a^{-1}$, then $h_1 = h_2$, so f is an injection. f is a surjection because $\forall x \in aHa^{-1}$, $f(a^{-1}xa) = x$, $a^{-1}xa \in H$. 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 commutative 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 commutative.

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 $K \ntriangleleft D_4^*$.

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

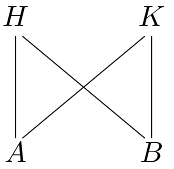
$$a = b_1^{n_1} b_2^{n_2} \cdots b_t^{n_t} \quad \text{where } b_i \in H \text{ or } b_i \in K, i = 1, 2, \ldots, t$$

so $x^{-1}ax = x^{-1}b_1^{n_1} \cdots b_t^{n_t} x = (x^{-1}b_1 x)^{n_1}(x^{-1}b_2 x)^{n_2} \cdots (x^{-1}b_t x)^{n_t}$.
$H \lhd G$, $K \lhd G$, so $x^{-1}b_i x \in H \vee K, i = 1, 2, \ldots, t$ and

$$x^{-1}ax = (x^{-1}b_1 x)^{n_1}(x^{-1}b_2 x)^{n_2} \cdots (x^{-1}b_t x)^{n_t} \in H \vee K$$

$H \vee K \lhd G$.

(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 $g_1 \in G_1$, $g_2 \in G_2$. $x^{-1} = (g_1^{-1}, g_2^{-1})$, $x^{-1}ax = (g_1^{-1}n_1 g_1, g_2^{-1}n_2 g_2)$. $N_1 \lhd G_1$, $N_2 \lhd G_2$, so $g_1^{-1}n_1 g_1 \in N_1$, $g_2^{-1}n_2 g_2 \in N_2$. $x^{-1}ax \in (N_1 \times N_2)$. Thus $(N_1 \times N_2) \lhd (G_1 \times G_2)$.
Assume $G_1 = \bigcup\limits_{i \in I} N_1 a_i$, $G_2 = \bigcup\limits_{j \in J} N_2 b_j$. Then $G_1 \times G_2 = \bigcup\limits_{i \in I} N_1 a_i \times \bigcup\limits_{j \in J} N_2 b_j$.
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 $(G_1/N_1) \times (G_2/N_2)$.

$$f : N_1 a_i \times N_2 b_j \mapsto (a_i, b_j)$$

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

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 $G = \bigcup\limits_{i \in I} N a_i$, 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) $\langle km \rangle \lhd \langle k \rangle$, $\langle k \rangle = \bigcup\limits_{i \in I} (\langle km \rangle + a_i)$. 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 $y = \sum\limits_{i=1}^{m} \frac{a_i}{p^{n+i}}$, $x = \sum\limits_{i=1}^{m} (\frac{a_i}{p^{n+i}} + H) \in \langle A \rangle$. 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

$$(\tau(a_1)\tau(a_2)\cdots\tau(a_n)) = (a_1a_4a_5\cdots a_na_3a_2)$$

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 $(12)(35) \in N$, $(12)(35)(12)(34) = (345) \in N$. 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 $x = j_k \in J$, $\tau^{-1}(x) = i_k$, $\sigma\tau^{-1}(x) = i_{3k-4[\frac{k}{2}]-1}$, $\tau\sigma\tau^{-1}(x) = (\tau(i_i)\tau(i_2))(\tau(i_3)\tau(i_4)) \in N$. 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 $a = f(x^ny^m)$, 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 $m' \equiv m \mod 2$, $n' \equiv n \mod 2$. $D_n = \{e, a, a^2, \dots, a^{n-1}, b, ba, \dots, ba^{n-1}\}$. $|D_n| = 2n$. 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 $ba^i, i = 1, \dots, n$. 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 $S \ntriangleleft D_n$ for all $k = 1, 2, \dots, n$.
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 $S \ntriangleleft D_n$ for all $k = 1, 2, \dots, n$.
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 $S = \left\langle a^d, ba^r\right\rangle$, 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, $S = \left\langle a^d, ba^r\right\rangle$.
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 $A_i = (\cos\frac{2\pi i}{n}, \sin\frac{2\pi i}{n})^t$, $i = 1, 2, \dots, n$. 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 $\varphi : f \mapsto (1 i\, 2 i{-}1\, 3 i{-}2 \cdots)$. If $f(A_2) = A_{i-1}$, similarly, we can also prove $f(A_k) = A_{i+1-k}$. φ can be defined as $\varphi : f \mapsto (1 i)(2\, i-1)(3\, i-2)\cdots$. 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 $x(A_2) = A_{i+1}$, $x(A_k) = A_{i-1+k} = \alpha^{i-1}A_k$, $k = 1, 2, \dots, n$. 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, $D_n^* \cong \langle f, g\rangle \cong D_n$.

1.7 Categories: products, coproducts, and free objects

Exercise 1.7.1. A *pointed set* is a pair (S, x) with S a set and $x \in S$. A morphism of pointed sets $(S, x) \to (S', x')$ is a triple (f, x, x'), where $S \to S'$ is a function such that $f(x) = x'$. Show that pointed sets form a category.

Answer. Let $\mathcal{S}$ be the category and 4 objects of $\mathcal{S}$ are (A, a), (B, b), (C, c), (D, d). f, g and h are morphisms defined by $f : A \to B$, $g : B \to C$, $h : C \to D$ with $f(a) = b$, $g(b) = c$, $h(c) = d$.

$$\begin{tikzcd}
(A,a) \arrow[r, "f"] & (B,b) \arrow[r, "g"] & (C,c) \arrow[r, "h"] & (D,d)
\end{tikzcd}$$

category $\mathcal{S}$

$$\hom(A, B) \times \hom(B, C) \to \hom(A, C)$$

because $g \circ f : A \to C$ with $g(f(a)) = g(b) = c = g \circ f(a)$. Similarly, $(h \circ g) \circ f = h \circ (g \circ f)$ with $(h \circ g) \circ f(a) = h \circ (g \circ f)(a) = d$. Take 1_B consist of those functions $i : B \to B$ with $i(b) = b$. Then $1_B \circ f = f$ and $g \circ 1_B = g$. So $\mathcal{S}$ is a category.

Exercise 1.7.2. If $f : A \to B$ is an equivalence in a category $\mathcal{C}$ and $g : B \to A$ is the morphism such that $g \circ f = 1_A$, $f \circ g = 1_B$, show that g is unique.

Answer. Assume there exist g and g' satisfies the condition.

$$\begin{tikzcd}
A \arrow[r, shift left, "f"] & B \arrow[l, shift left, "g"]
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, shift left, "f"] & B \arrow[l, shift left, "g'"]
\end{tikzcd}$$

So $g' \circ (f \circ g) = g' \circ 1_B = g' = (g' \circ f) \circ g = 1_A \circ g = g$.

Exercise 1.7.3. In the category $\mathcal{G}$ of groups, show that the group $G_1 \times G_2$ together with the homomorphisms $\pi_1 : G_1 \times G_2 \to G_1$ and $\pi_2 : G_1 \times G_2 \to G_2$ is a product for $\{G_1, G_2\}$.

Answer. Take $\tau_1 : G_1 \to G_1 \times G_2$ as $\tau_1(g_1) = (g_1, e)$; $\tau_2 : G_2 \to G_1 \times G_2$ as $\tau_2(g_2) = (e, g_2)$; $\pi_1 : G_1 \times G_2 \to G_1$ as $\pi_1(g_1, g_2) = g_1$; $\pi_2 : G_1 \times G_2 \to G_2$ as $\pi_2(g_1, g_2) = g_2$. Then

$$\begin{tikzcd}
G_1 \arrow[r, shift right, "\tau_1"'] & G_1 \times G_2 \arrow[l, shift right, "\pi_1"'] \arrow[r, shift left, "\pi_2"] & G_2 \arrow[l, shift left, "\tau_2"]
\end{tikzcd}$$

For any object B such that

$$\begin{tikzcd}
G_1 & B \arrow[l, "\varphi_1"'] \arrow[r, "\varphi_2"] & G_2
\end{tikzcd}$$

For any $x \in B$, define $f : B \to G_1 \times G_2$ as $f(x) = (\varphi_1(x), \varphi_2(x))$. Then $\pi_1(f(x)) = \varphi_1(x)$, $\pi_1 \circ f = \varphi_1$, $\pi_2(f(x)) = \varphi_2(x)$, $\pi_2 \circ f = \varphi_2$. Thus

$$\begin{tikzcd}
 & B \arrow[dl, "\varphi_1"'] \arrow[d, "f"'] \arrow[dr, "\varphi_2"] & \\
G_1 \arrow[r, shift right, "\tau_1"'] & G_1 \times G_2 \arrow[l, shift right, "\pi_1"'] \arrow[r, shift left, "\pi_2"] & G_2 \arrow[l, shift left, "\tau_2"]
\end{tikzcd}$$

Next we verify the uniqueness. If there exist f and f' satisfies the condition,

$$\pi_1(f(x)) = \pi_1(f'(x)) = \varphi_1(x)$$

$$\pi_2(f(x)) = \pi_2(f'(x)) = \varphi_2(x)$$

Thus $f(x) = f'(x)$ for all $x \in B$, so $f = f'$.

Exercise 1.7.4. In the category $\mathcal{A}$ of abelian groups, show that the group $A_1 \times A_2$ together with the morphisms $\tau_1 : A_1 \to A_1 \times A_2$ and $\tau_2 : A_2 \to A_1 \times A_2$ is a coproduct of $\{A_1, A_2\}$.

Answer. Take $\tau_1 : A_1 \to A_1 \times A_2$ as $\tau_1(a_1) = (a_1, e)$; $\tau_2 : A_2 \to A_1 \times A_2$ as $\tau_2(a_2) = (e, a_2)$; $\pi_1 : A_1 \times A_2 \to A_1$ as $\pi_1(a_1, a_2) = a_1$; $\pi_2 : A_1 \times A_2 \to A_2$ as $\pi_2(a_1, a_2) = a_2$. Then

$$\begin{tikzcd}
A_1 \arrow[r, shift right, "\tau_1"'] & A_1 \times A_2 \arrow[l, shift right, "\pi_1"'] \arrow[r, shift left, "\pi_2"] & A_2 \arrow[l, shift left, "\tau_2"]
\end{tikzcd}$$

For any object B such that

$$\begin{tikzcd}
A_1 \arrow[r, "\varphi_1"] & B & A_2 \arrow[l, "\varphi_2"']
\end{tikzcd}$$

For any $(a_1, a_2) \in A_1 \times A_2$, define $f : A_1 \times A_2 \to B$ as $f(a_1, a_2) = \varphi_1(a_1)\varphi_2(a_2)$. Then $f(\tau_1(a_1)) = f(a_1, e) = \varphi_1(a_1)e = \varphi_1(a_1)$, $f \circ \tau_1 = \varphi_1$, $f(\tau_2(a_2)) = f(e, a_2) = e\varphi_2(a_2) = \varphi_2(a_2)$, $f \circ \tau_2 = \varphi_2$.

$$\begin{tikzcd}
 & B & \\
A_1 \arrow[ur, "\varphi_1"] \arrow[r, shift right, "\tau_1"'] & A_1 \times A_2 \arrow[u, "f"] \arrow[l, shift right, "\pi_1"'] \arrow[r, shift left, "\pi_2"] & A_2 \arrow[ul, "\varphi_2"'] \arrow[l, shift left, "\tau_2"]
\end{tikzcd}$$

Next we verify the uniqueness. If there exist f and f' satisfies the condition,

$$f(\tau_1(a_1)) = f'(\tau_1(a_1)) = f(a_1, e) = f'(a_1, e)$$

$$f(\tau_2(a_2)) = f'(\tau_2(a_2)) = f(e, a_2) = f'(e, a_2)$$

$$\begin{aligned} f(\tau_1(a_1), \tau_2(a_2)) &= f(\tau_1(a_1))f(\tau_2(a_2)) \\ =&f'(\tau_1(a_1), \tau_2(a_2)) = f'(\tau_1(a_1))f'(\tau_2(a_2)) \end{aligned}$$

so $f = f'$.

Exercise 1.7.5. Every family $\{A_i | i \in I\}$ in the category of sets has a coproduct.

Answer. We examine $\dot{\bigcup} A_i = \{(a, i) \in (\cup A_i) \times I | a \in A_i\}$ which satisfies the condition. Define the morphism $\pi_i : A_i \to \dot{\bigcup} A_i$ as $\pi_i(a) = (a, i)$. For any B such that $\exists \varphi_i : A_i \to B$.

$$\begin{tikzcd}
 & & B & \\
A_1 \arrow[urr, "\varphi_1"] & A_2 \arrow[ur, "\varphi_2"] & \cdots & A_n \arrow[ul, "\varphi_n"']
\end{tikzcd}$$

$\varphi(a) = x \in B$. Take $\varphi(a,i) = \varphi_i(a)$ defined on the subset of $\cup A_i \times I$, we can verify that the domain of φ is $\dot{\bigcup} A_i$. Then take $f = \varphi$, $f(\pi_i(a)) = \varphi_i(a)$, $f \circ \pi_i = \varphi_i$.
The uniqueness is obvious.

Exercise 1.7.6. (a) Show that in the category $\mathcal{S}_*$ of pointed sets product always exist; describe them.

(b) Show that in $\mathcal{S}_*$ every family of objects has a coproduct, describe the coproduct.

Answer. (a) Define $\otimes$ as an operator between points and other elements in the pointed set. $\forall a \in A_i$, $a \otimes a_i = a_1 \times a = a$. For a family of sets with their points $\{(A_i, a_i | i \in I)\}$, consider $(A_1, A_2, \cdots, A_n) = \{(a'_1, a'_2, \cdots, a'_n)\}$. Define morphisms $\pi_i(a) = (a_1, a_2, \cdots, a, \cdots, a_n)$, $\pi_i : A_i \to (A_1, A_2, \cdots, A_n)$.

$$\begin{tikzcd}
 & (A_1, A_2, \cdots, A_n) & & \\
A_1 \arrow[ur, "\pi_1"] & A_2 \arrow[u, "\pi_2"] & \cdots & A_n \arrow[ull, "\pi_n"']
\end{tikzcd}$$

For any B such that $\exists \varphi_i : A_i \to B$.

$$\begin{tikzcd}
 & B & & \\
A_1 \arrow[ur, "\varphi_1"] & A_2 \arrow[u, "\varphi_2"] & \cdots & A_n \arrow[ull, "\varphi_n"']
\end{tikzcd}$$

Take $f : (A_1, A_2, \cdots, A_n) \to B$ as

$$f(a'_1, a'_2, \cdots, a'_n) = \varphi_1(a'_1) \otimes \varphi_2(a'_2) \otimes \cdots \otimes \varphi(a'_n)$$

Then $f \circ \pi_i(a) = f(a_1, a_2, \cdots, a, \cdots, a_n) = \varphi_1(a_1) \otimes \cdots \otimes \varphi_i(a) \otimes \cdots \otimes \varphi_n(a_n) = \varphi_i(a)$. So $f \circ \pi_i = \varphi_i$.
Next we verify the uniqueness. If there exist f and f' satisfies the condition. Then $\exists i \in I$ and $a \in A_i$ s.t. $f(a_1, a_2, \cdots, a, \cdots, a_n) \neq f'(a_1, a_2, \cdots, a, \cdots, a_n)$. But $f(\pi_i(a)) = f'(\pi_i(a))$, so $f = f'$.

(b) The proof is similar to **Exercise 1.7.5**.

Exercise 1.7.7. Let F be a free object on a set $X(i : X \to F)$ in a concrete category $\mathcal{C}$. If $\mathcal{C}$ contains an object whose underlying set has at least two elements in it, then i is an injective map of sets.

Answer. Assume $A \in \text{obj}(\mathcal{C})$, A has at least two elements and $X \xrightarrow{f} A$. $X \xrightarrow{i} F$ and F is free on X, so there exists a morphism $\bar{f}$ s.t. $F \xrightarrow{\bar{f}} A$. If $|X| = 1$, i must be injective. For $|X| \geq 2$. Suppose i is not injective. Take $x_1, x_2 \in X$ and $i(x_1) = i(x_2) \in F$, $f(x_1) = a_1$, $f(x_2) = a_2$. $\bar{f}(i(x_1)) = \bar{f}(i(x_2)) = f(x_1) = f(x_2) = a_1 = a_2$. That means all the elements in A are identical. That's contradictory to the assumption.

Exercise 1.7.8. Suppose X is a set and F is a free object on X (with $i : X \to F$) in the category of groups. Prove that $i(X)$ is a set of generators for the group F.

Answer. Assume G the subgroup of F is the group generated by $i(X)$. Since $X \xrightarrow{i} G$ and $X \xrightarrow{i} F$, we can obtain unique morphism φ such that $F \xrightarrow{\varphi} G$ and $\varphi \circ i = i$.
Consider morphism $1_F : F \to F$ which is the identical homomorphism. F is free so 1_F is the unique homomorphism. Take $\subset: G \to F$ as a morphism defined as $\forall g \in G$, $\subset (g) = g$. Then

$$\begin{tikzcd}
 & G \arrow[dr, "\subset", sloped] & \\
X \arrow[ur, "i", sloped] \arrow[r, "i"] & F \arrow[u, "\varphi"] \arrow[r, "1_F"] & F
\end{tikzcd}$$

$\subset \circ \varphi \circ i = 1_F \circ i = i$ so $\subset \circ \varphi = 1_F$. Thus $\subset$ is an epimorphism, $F \subset G$. So $F = G$ can be generated by $i(X)$.

1.8 Direct products and direct sums

Exercise 1.8.1. S_3 is not the direct product of any family of its proper subgroups. The same is true of $Z_{p^n}(p$ prime, $n \geq 1)$ and $\mathbb{Z}$.

Answer. We list all the subgroups of S_3: $\{(1),(12)\}$, $\{(1),(13)\}$, $\{(1),(23)\}$, $\{(1),(123),(132)\}$. Only $\{(1),(123),(132)\}$ is normal, so S_3 isn't an direct product of any family of its proper subgroups.
For Z_{p^n}, $Z_{p^i} \lhd Z_{p^n}$ for all $i = 1, 2, \ldots, n-1$ but $Z_{p^i} \cap Z_{p^j} \neq \{e\}$. So Z_{p^n} isn't an direct product of any family of its proper subgroups.
For $\mathbf{Z}$. $\forall N_1 \lhd \mathbf{Z}$, $N_2 \lhd \mathbf{Z}$, we have $N_1 = \langle a_1 \rangle$ and $N_2 = \langle a_2 \rangle$. Thus, $N_1 \cap N_2 = \langle a_1 a_2 \rangle \neq \{e\}$. So $\mathbf{Z}$ isn't an direct product of any family of its proper subgroups.

Exercise 1.8.2. Give an example of groups H_i, K_i such that $H_1 \times H_2 \cong K_1 \times K_2$ and no H_i is isomorphic to any K_j.

Answer. Take $H_1 \cong K_1 \times K_2$, $H_2 = \{e\}$. We verify that $H_1 \times H_2 \cong K_1 \times K_2$. There exists $f : H_1 \to K_1 \times H_2$ which is an isomorphism. There exists canonical projection $\pi_1 : H_1 \times H_2 \to H_1$ and π_1 is an epimorphism. Ker$\pi_1 = \{(e_1, e_2)\}$ thus π_1 is also a monomorphism. Therefore $\bar{f} = f \circ \pi_1$ is a well defined isomorphism. $H_1 \times H_2 \cong K_1 \times K_2$ but neither H_1 nor H_2 are isomorphic to any K_i, $i = 1, 2$.

Exercise 1.8.3. Let G be and (additive) abelian group with subgroups H and K. Show that $G \cong H \oplus K$ if and only if there are homomorphisms

$$\begin{tikzcd} H \arrow[r, shift right, "\tau_1"'] & G \arrow[l, shift right, "\pi_1"'] \arrow[r, shift left, "\pi_2"] & K \arrow[l, shift left, "\tau_2"] \end{tikzcd}$$

such that $\pi_1\tau_1 = 1_H$, $\pi_2\tau_2 = 1_K$, $\pi_1\tau_2 = 0$ and $\pi_2\tau_1 = 0$, where 0 is the map sending every element onto the zero (identity) element, and $\tau_1\pi_1(x) + \tau_2\pi_2(x) = x$ for all $x \in G$.

Answer. If $G \cong H \oplus K$. Denote $f : G \to H \oplus K$ which is a isomorphism. Then there are canonical products π_1', π_2', τ_1', τ_2'.

$$\begin{tikzcd}
H \arrow[r, shift right, "\tau_1'"'] & H \oplus K \arrow[l, shift right, "\pi_1'"'] \arrow[r, shift left, "\pi_2'"] & K \arrow[l, shift left, "\tau_2'"]
\end{tikzcd}$$

Thus

$$\begin{tikzcd}
& G \arrow[dl, dashed, shift right, "\pi_1"'] \arrow[d, shift left, "f^{-1}"] \arrow[dr, dashed, shift left, "\pi_2"] & \\
H \arrow[ur, dashed, shift right, "\tau_1"'] \arrow[r, shift right, "\tau_1'"'] & H \oplus K \arrow[u, shift left, "f"] \arrow[l, shift right, "\pi_1'"'] \arrow[r, shift left, "\pi_2'"] & K \arrow[ul, dashed, shift left, "\tau_2"] \arrow[l, shift left, "\tau_2'"]
\end{tikzcd}$$

Take $\tau_1 = f \circ \tau_1'$, $\tau_2 = f \circ \tau_2'$, $\pi_1 = \pi_1' \circ f^{-1}$, $\pi_2 = \pi_2' \circ f^{-1}$.

$$\pi_1\tau_1 = \pi_1' f^{-1} f \tau_1' = \pi_1'\tau_1' = 1_H$$

$$\pi_2\tau_2 = \pi_2' f^{-1} f \tau_2' = \pi_2'\tau_2' = 1_K$$

$$\pi_1\tau_2 = \pi_1' f^{-1} f \tau_2' = \pi_1'\tau_2' = 0$$

$$\pi_2\tau_1 = \pi_2' f^{-1} f \tau_1' = \pi_2'\tau_1' = 0$$

$\forall x \in G$, $x = hk$ where $h \in H$ and $k \in K$.

$$\begin{aligned}
\tau_1\pi_1(x) + \tau_2\pi_2(x) &= f(\tau_1'\pi_1'(h,k)) + f(\tau_2'\pi_2(h,k)) \\
&= f(\tau_1'(h)) + f(\tau_2'(k)) \\
&= f(h,e) + f(e,k) \\
&= f(h+e, e+k) = f(h,k) \\
&= x
\end{aligned}$$

If there exist π_1, π_2, τ_1, τ_2 satisfies the condition. There are canonical projections π_1', π_2', τ_1', τ_2' between H and $H \oplus K$, K and $H \oplus K$.

$$\begin{tikzcd}
& G \arrow[dl, shift right, "\pi_1"'] \arrow[d, dashed, shift left, "f^{-1}"] \arrow[dr, shift left, "\pi_2"] & \\
H \arrow[ur, shift right, "\tau_1"'] \arrow[r, shift right, "\tau_1'"'] & H \oplus K \arrow[u, dashed, shift left, "f"] \arrow[l, shift right, "\pi_1'"'] \arrow[r, shift left, "\pi_2'"] & K \arrow[ul, shift left, "\tau_2"] \arrow[l, shift left, "\tau_2'"]
\end{tikzcd}$$

For $f = \tau_1'\pi_1 + \tau_2'\pi_2$ which is a well defined homomorphism. $\forall h \in H$ and $k \in K$, $\tau_1'(h) + \tau_2'(k) = (h, k) \in H \oplus K$. Thus $f(x) = (e_1, e_2)$ if and only if $\pi_1(x) = e_1$ and $\pi_2(x) = e_2$. $\tau_1\pi_1(x) + \tau_2\pi_2(x) = \tau_1(e_1) + \tau_2(e_2) = e = x$. Thus Ker$f = \{e\}$. f is a monomorphism. $\forall (h, k) \in H \oplus K$, take $x = \tau_1(h) + \tau_2(k) \in G$, then

$$\begin{aligned} f(x) &= \tau_1'\pi_1\tau_1(h) + \tau_1'\pi_1\tau_2(h) + \tau_2'\pi_2\tau_1(k) + \tau_2'\pi_2\tau_1(k) \\ &= \tau_1'(h) + \tau_2'(k) = (h, k) \in H \oplus K \end{aligned}$$

f is a epimorphism. Thus $G \cong H \oplus K$.

Exercise 1.8.4. Give an example to show that the weak direct product is not a coproduct in the category of all groups.

Answer. Consider S_3 and $S_3 \times S_3$.

$$\begin{tikzcd}
 & S_3 \times S_2 \\
S_3 \arrow[ur] \arrow[r] & S_3 \times S_3 \arrow[u, dashed]
\end{tikzcd}$$

Since there doesn't exist homomorphism $S_3 \to S_2$, there is no homomorphism $S_3 \times S_3 \to S_3 \times S_2$.

Exercise 1.8.5. Let G, H be finite cyclic groups. Then $G \times H$ is cyclic if and only if $(|G|, |H|) = 1$.

Answer. Assume $|G| = m$, $|H| = n$, then $G \cong Z_m$, $H \cong Z_n$ and $G \times H \cong Z_m \oplus Z_n$.
If$(|G|, |H|) = 1$. Consider $(x_1, x_2) \in Z_m \oplus Z_n$. By *Chinese Remainder Theorem*, there exists x such that $a \equiv x \mod \operatorname{lcm}(m, n)$ and $a \equiv x_1 \mod m$, $a \equiv x_2 \mod n$. Thus, $a(1, 1) = (x_1, x_2)$. $Z_m \oplus Z_n < \langle (1, 1) \rangle$. $\langle (1, 1) \rangle < Z_m \oplus Z_n$ is trivial. So $Z_m \oplus Z_n = \langle (1, 1) \rangle \cong G \times H$ is cyclic.
If $G \times H$ is cyclic. Assume $l = \gcd(m, n)$ and there exist x such that $x_1 \equiv x \mod m$, $x_2 \equiv x \mod n$. Take $x_1 \not\equiv x_2 \mod l$, it can be chosen properly. Consider $(x_1, x_2) \in Z_m \oplus Z_n$, $x = k_1 m + x_1 = k_2 n + x_2 \Rightarrow x_1 \equiv x_2 \mod l$. That's contradictory!

Exercise 1.8.6. Every finitely generated abelian group $G \neq \langle e \rangle$ in which every element (except e) has order p (p prime) is isomorphic to $Z_p \oplus Z_p \oplus \cdots \oplus Z_p(n$ summands) for some $n \geq 1$.

Answer. Assume $\{a_1, a_2, \ldots, a_n\}$ generates G. $|a_i| = p$ for $i = 1, 2, \ldots, n$ so $\langle a_i \rangle \cong Z_p$. Now we show that $G = \prod\limits_{i=1}^{n}{}^{w} \langle a_i \rangle \cong \sum\limits_{i=1}^{n} Z_p$. $G = \langle a_1, a_2, \ldots, a_n \rangle$ and $\langle a_1 \rangle \lhd G$ for $i = 1, 2, \ldots, n$. If exist $\langle a_i \rangle$ s.t. $\prod\limits_{j=1, j\neq i}^{n} \langle a_j \rangle \cap \langle a_i \rangle \neq \{e\}$. Then there exists $a_i^{s_i} = a_1^{s_1} \cdots a_{i-1}^{s_{i-1}} a_{i+1}^{s_{i+1}} \cdots a_n^{s_n}$. $(s_i, p) = 1$ so $\exists 1 \leq t_i \leq p-1$ such that $s_i t_i \equiv 1 \mod p$. So $a_i^{s_i t_i} = a_1^{s_1 t_i} \cdots a_{i-1}^{s_{i-1} t_i} a_{i+1}^{s_{i+1} t_i} \cdots a_n^{s_n t_i} = a_i$. $\{a_1, a_2, \ldots, a_n\}$ can generate G. That's contradictory! So $\prod\limits_{j=1, j\neq i}^{n} \langle a_j \rangle \cap \langle a_i \rangle = \{e\}$, which means $G = \prod\limits_{i=1}^{n}{}^{w} \langle a_i \rangle \cong \sum\limits_{i=1}^{n} Z_p$.

Exercise 1.8.7. Let H, K, N be nontrivial normal subgroups of a group G and suppose $G = H \times K$. Prove that N is in the center of G or N intersects one of H, K nontrivially. Give examples to show that both possibilities can actually occur when G is nonabelian.

Answer. If $N \cap H = N \cap K = \{e\}$. $G = HK$. $\forall h \in H$ and $k \in K$, since $H \cap K = \{e\}$, $hk = kh$. For any $hk \in N$, and $h_1 \in H \subset HK$, $h_1^{-1} h k h_1 = h_1^{-1} h h_1 k \in N$. Assume $h' = h_1^{-1} h_1 \in H$, $h'k \in N$. Thus $h'^{-1} k^{-1} k h = h'^{-1} h \in N$. So $h'^{-1} h = e$, $h = h'$, h is in the center $C(H)$ of group H. Similarly, $k \in C(K)$ which is the center of K. Then $\forall hk \in N$ and $h_1 k_1 \in G$, $k_1^{-1} h_1^{-1} h k h_1 k_1 = h_1^{-1} h h_1 k_1^{-1} k k_1 = hk$. $N \subset N(G)$.
For $N \cup H \neq \varnothing$, the example can be trivial: $N < H$ and $N \lhd G$. There's many cyclic group satisfy the condition.
For $N \subset C(G)$. Take $G = D_4^* \times D_4^*$, $H = D_4^* \times \{I\}$, $K = \{I\} \times D_4^*$. $\{I, R^2\}$ is normal in D_4^*. Denote N is the subgroup $\{(I, I), (R^2, R^2)\}$. We can verify that N satisfies the condition.

Exercise 1.8.8. Corollary 8.7 is false if one of the N_i is not normal.

Answer. Consider $N_1, N_2, \ldots, N_n$ are all finite. WLOG, assume N_1 is not normal. $G = \left\langle \bigcup\limits_{i=1}^{n} N_i \cup N_1 \right\rangle$ and $N_1N_2\cdots N_n \subset G$. Denote $A = N_2N_3\cdots N_n$. Then $\exists a \in A$ such that $a^{-1}na = n' \notin N_1$. Thus $n'a \in G$ but $n'a \notin N_1N_2\cdots N_n$ so $|G| > |N_1N_2\cdots N_n| = |N_1| \times |N_2| \times \cdots \times |N_n| = |N_1 \times N_2 \times \cdots \times N_n|$.

Exercise 1.8.9. If a group G is the (internal) direct product of its subgroups H, K, then $H \cong G/K$ and $G/H \cong K$.

Answer. $H \cap K = \{e\}$. $G = H \times K = HK$. Thus $HK/H \cong K/(K \cap H) = K$, $HK/K \cong H/(K \cap H) = H$.

Exercise 1.8.10. If $\{G_i | i \in I\}$ is a family of groups, then $\prod^w G_i$ is the internal weak product its subgroups $\{\tau_i(G_i) | i \in I\}$.

Answer. Take $\tau_i(g) = (e_1, e_2, \ldots, g, \ldots, e_n)$, $g \in G_i.\tau_i(G_i)$. $\tau_i(G_i)$ is normal in $\prod\limits_{i\in I}{}^w G_i$. $\tau_i(G_i) \cap \tau_j(G_j) = \{(e_1, e_2, \ldots, e_n)\}$ which is the identity element in $\prod\limits_{i\in I}{}^w G_i$. $\forall (g_1, g_2, \ldots, g_n) \in \prod\limits_{i\in I}{}^w G_i$, we have

$$(g_1, g_2, \ldots, g_n) = (g_1, e_2, \ldots, e_n)(e_1, g_2, \ldots, e_n)\cdots(e_1, e_2, \ldots, g_n)$$

Thus $\prod\limits_{i\in I}{}^w G_i \subset \left\langle \bigcup\limits_{i\in I}{}^w \tau_i(G_i) \right\rangle$ and

$$\left\langle \bigcup_{i\in I}{}^w \tau_i(G_i) \right\rangle = \tau_1(G_1)\tau_2(G_2)\cdots\tau_n(G_n) \subset \prod_{i\in I}{}^w G_i$$

Therefore $\prod\limits_{i\in I}{}^w G_i$ is the direct product of $\tau_i(G_i)$.

Exercise 1.8.11. Let $\{N_i | i \in I\}$ be a family of subgroups of a group G. Then G is the internal weak product of $\{N_i | i \in I\}$if and only if:

(i) $a_i a_j = a_j a_i$ for all $i \neq j$ and $a_i \in N_i$, $a_j \in N_j$;

(ii) every nonidentity element of G is uniquely a product $a_{i_1} \cdots a_{i_n}$, where $i_i, \ldots, i_n$ are distinct elements of I and $e \neq a_{i_k} \in N_{i_k}$ for each k.

Answer. Trivial.

Exercise 1.8.12. A normal subgroup H of a group G is said to be a **direct factor** (**direct summand** if G is additive abelian) if there exists a (normal) subgroup K of G such that $G = H \times K$.

(a) If H is a direct factor of K and K is a direct factor of G, then H is normal in G.

(b) If H is a direct factor of G, then every homomorphism $H \to G$ may be extended to an endomorphism $G \to G$. However, a monomorphism $H \to G$ need not be extendible to and automorphism $G \to G$.

Answer. (a) $G = K \times K' = (H \times H') \times K'$. So $\forall g \in G$, $g = hh'k'$ with $h \in H$, $h' \in H'$ and $k' \in K'$. $\forall h_1 \in H$ and $g \in G$, $g^{-1}h_1g = k'^{-1}h'^{-1}h^{-1}h_1hh'k' = (h^{-1}h_1h)(h'^{-1}h')(k'^{-1}k') = h^{-1}h_1h \in H$. Thus $H \lhd G$.

(b) If $G = H \times K$. For a homomorphism $f : H \to G$, we construct a homomorphism $\bar{f} : G \to G$, $\forall g \in G$,g can be uniquely written as $g = hk$ where $h \in H$, $k \in K$. Take $\tau(g) = h$ which is a homomorphism $\tau : G \to H$. We can get $\bar{f} = f \circ \tau : G \to G$ is a endomorphism but it needn't to be a automorphism.

Exercise 1.8.13. Let $\{G_i | i \in I\}$ be a family of groups and $J \subset I$. The map $\alpha : \prod\limits_{j \in J} G_j \to \prod\limits_{i \in I} G_i$ given by $\{a_j\} \mapsto \{b_i\}$, where $b_j = a_j$ for $j \in J$ and $b_i = e_i$(identity in G_i) for $i \notin J$, is a monomorphism of groups and $\prod\limits_{i \in I} G_i / \alpha(\prod\limits_{j \in J} G_j) \cong \prod\limits_{i \in I - J} G_i$.

Answer. Define a map $\beta : \prod\limits_{i \in I} G_i \to \prod\limits_{i \in I - J} G_i$ given by $\{a_i\} \mapsto \{b_i\}$ and for those $i \in I - J$, $\exists b_i \in \{b_i\}$ s.t. $a_i = b_i$. Thus $\beta(\{a_i\})\beta(\{a'_i\}) = \beta(\{a_ia'_i\})$, β is a well defined homomorphism. Ker$\beta = \{\{a_i\} \in \prod\limits_{i \in I} G_i | a_i = e_i \text{ for } i \in I - J\} = \alpha(\prod\limits_{j \in J} G_j)$. We verify β is a epimorphism. $\forall \{b_i\} \in \prod\limits_{i \in I - J} G_i$, take

$\{a_i\} \in \prod\limits_{i\in I} G_i$ where $a_i = b_i$ for $i \in I - J$. Then $\beta(\{a_i\}) = \{b_i\}$. Thus β is an isomorphism, $\mathrm{Im}\beta = \prod\limits_{i\in I-J} G_i \cong \prod\limits_{i\in I} G_i/\alpha(\prod\limits_{j\in J}(G_j))$.

Exercise 1.8.14. For $i = 1, 2$ let $H_i \lhd G_i$ and give examples to show that each of the following statements may be false:
(a) $G_1 \cong G_2$ and $H_1 \cong H_2 \Rightarrow G_1/H_1 \cong G_2/H_2$.
(b) $G_1 \cong G_2$ and $G_1/H_1 \cong G_2/H_2 \Rightarrow H_1 \cong H_2$.
(c) $H_1 \cong H_2$ and $G_1/H_1 \cong G_2/H_2 \Rightarrow G_1 \cong G_2$.

Answer. (a) Take $G_1 = G_2 = Z_2 \times Z_4$, $H_1 = Z_2 \times \{\bar{0}\}$, $H_2 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{2})\}$.
(b) Take $G_1 = G_2 = Z_2 \times Z_4$, $H_1 = \{\bar{0}\} \times Z_4$, $H_2 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{0}, \bar{2}), (\bar{1}, \bar{2})\}$.
(c) Take $H_1 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{2})\}$, $H_2 = Z_2$ and $G_1 = Z_2 \times Z_4$, $G_2 = Z_2 \times K_4$.

1.9 Free groups, free products, generators and relations

Exercise 1.9.1. Every nonidentity elements in a free group F has a infinite order.

Answer. Define the length of a word $x = a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_n^{\lambda_n}$ is n and denote it as $len(x)$. Assume $len(x) = n$ for some $n \in F$ and $len(1) = 0$, we prove that $len(x^m) \geq n \forall m \geq 1$.
Let k be the largest integer such that $a_{n-j}^{\lambda_{n-j}} = a_n^{-\lambda_j}$ for $j = 0, 1, \ldots, k-1$. If $k > \left[\frac{n}{2}\right]$. For even k, $a_{\frac{n}{2}}^{\lambda_{\frac{n}{2}}} = a_{\frac{n}{2}+1}^{-(\lambda_{\frac{n}{2}+1})}$, $a_{\frac{n}{2}-1}^{\lambda_{\frac{n}{2}-1}} = a_{\frac{n}{2}+2}^{-(\lambda_{\frac{n}{2}+2})}$, $\cdots$ which means $x = a_1^{\lambda_1} a_2^{\lambda_2} \cdots a_n^{\lambda_n} = 1$. For odd k, $a_{\left[\frac{n}{2}\right]+1}^{\lambda_{\left[\frac{n}{2}\right]+1}} = a_{\left[\frac{n}{2}\right]+1}^{-(\lambda_{\left[\frac{n}{2}\right]+1})}$, which is contradictory to x is reduced. So $k \leq \left[\frac{n}{2}\right]$.
Divide $x = x_1 x_2 x_3$ where $x_1 = a_1^{\lambda_1} \cdots a_k^{\lambda_k}$, $x_2 = a_{k+1}^{\lambda_{k+1}} \cdots a_{n-k}^{\lambda_{n-k}}$, $x_3 = a_{n-k+1}^{\lambda_{n-k+1}} \cdots a_n^{\lambda_n}$. $x_3 x_1 = 1$. So $len(x) = len(x_1) + len(x_2) + len(x_3) = n$. $x^m = x_1 x_2 x_3 x_1 x_2 x_3 \cdots x_1 x_2 x_3 = x_1 x_2^m x_3$. $len(x^m) = len(x_1) + m \cdot len(x_2) + len(x_3) \geq n$. So $\forall m \geq 1$, $x^m \neq 1$, $|x|$ is infinite.

Exercise 1.9.2. Show that the free group on the set $\{a\}$ is an infinite cyclic group, and hence isomorphic to $\mathbf{Z}$.

Answer. $F(\{a\}) = \langle a \rangle$ and thus it's a infinite cyclic group. $F(\{a\}) \cong \mathbf{Z}$.

Exercise 1.9.3. Let F be a free group and let N be the subgroup generated by the set $\{x^n | x \in F, n \text{ a fixed integer}\}$. Show that $N \lhd F$.

Exercise 1.9.4. Let F be the free group on the set X, and let $Y \subset H$. If H is the smallest normal subgroup of F containin Y, then F/H is a free group.

Exercise 1.9.5. The group defined by generators a, b and relations $a^8 = b^2a^4 = ab^{-1}ab = e$ has order at most 16.

Exercise 1.9.6. The cyclic group of order 6 is the group defined by generators a, b and relations $a^2 = b^3 = a^{-1}b^{-1}ab = e$.

Exercise 1.9.7. Show that the group defined by generators a, b and relations $a^2 = e$, $b^3 = e$ is infinite and nonabelian.

Exercise 1.9.8. The group defined by generators a, b and relations $a^n = e(3 \leq n \in \mathbf{N}^*)$, $b^2 = e$ and $abab = e$ is the dihedral group D_n.

Exercise 1.9.9. The group defined by the generator b and $b^m = e(m \in \mathbf{N}^*)$ is the cyclic group Z_m.

Exercise 1.9.10. The operation of free product is commutative and associative: for any groups A, B, C, $A * B \cong B * A$ and $A * (B * C) \cong (A * B) * C$.

Exercise 1.9.11. If N is normal subgroup of $A * B$ generated by A, then $(A * B)/N \cong B$.

Exercise 1.9.12. If G and H each have more than one element, then $G * H$ is an infinite group with center $\langle e \rangle$.

Exercise 1.9.13. A free group is a free product of infinite cyclic groups.

Exercise 1.9.14. If G is the group defined by generators a, b and relations $a^2 = e$, $b^3 = e$, then $G \cong Z_2 * Z_3$.

Exercise 1.9.15. If $f : G_1 \to G_2$ and $g : H_1 \to H_2$ are homomorphisms of groups, then there is a unique homomorphism $h : G_1 * H_1 \to G_2 H_2$ such that $h|G_1 = f$ and $h|H_1 = g$.

Chapter 2

The structure of groups

Chapter 3

Rings

3.1 Rings and homomorphisms

Exercise 3.1.1. (a) Let G be an (additive) abelian group. Define an operation of multiplication in G by $ab = 0$ (for all $a, b \in G$). Then G is a ring.

(b) Let S be the set of all subsets of some fixed set U. For $A, B \in S$, define $A + B = (A - B) \cup (B - A)$ and $AB = A \cap B$. Then S is a ring. Is S commutative? Does it have an identity?

Answer. (a) $\forall a, b \in G$, $ab = 0 \in G$, so G is a monoid under multiplication, thus G is a ring.

(b) $A \subset U$, $B \subset U$, so $A - B \subset U$, $B - A \subset U$. Thus $A + B = B + A = (A - B) \cup (B - A) \subset U$. Take $\varnothing$ is the identity under addition and $U - A$ as the inverse of A, S is abelian group under the addition. $AB = A \cap B \subset U$, $AB = A \cap B = B \cap A = BA \in S$. So S is a commutative ring. $\forall A \in S$, $A \cap U = AU = A$ is the identity of the ring S.

Exercise 3.1.2. Let $\{R_i | i \in I\}$ be a family of rings with identity. Make the direct sum of abelian groups $\sum\limits_{i \in I} R_i$ into a ring by defining multiplication coordinatewise. Does $\sum\limits_{i \in I} R_i$ have identity?

Answer. Take $1_{R_i} \in R_i$ is the identity for $i = 1, 2, \ldots, n$. $\forall (a_1, a_2, \ldots, a_n) \in \sum\limits_{i \in I} R_i$

$$\begin{aligned}&(a_1, a_2, \ldots, a_n)(1_{R_1}, 1_{R_2}, \ldots, 1_{R_n})\\ =&(1_{R_1}, 1_{R_2}, \ldots, 1_{R_n})(a_1, a_2, \ldots, a_n)\\ =&(a_1, a_2, \ldots, a_n)\end{aligned}$$

is the identity.

Exercise 3.1.3. A ring R such that $a^2 = a$ for all $a \in R$ is called **Boolean ring**. Prove that every Boolean ring R is commutative and $a + a = 0$ for all $a \in R$.

Answer. $\forall a \in R$, $(a+a)^2 = a^2 + 2a + a^2 = a + 2a + a = 2a$, so $a + a = 0$. $\forall a, b \in R$, $(a+b)^2 = a^2 + b^2 + ab + ba = a + b = a + b + ba + ab$, so $ab + ba = 0 \Rightarrow ab = -ab = -ba$, $ab = ba$. Thus R is commutative.

Exercise 3.1.4. Let R be a ring and S a nonempty set. Then the group $M(S, R)$ is a ring with multiplication defined as follows: the product of $f, g \in M(S, R)$ is the function $S \to R$ given by $s \mapsto f(s)g(s)$.

Answer. We only need to check $M(S, R)$ is a monoid under multiplication, which means $\forall f, g \in M(S, R)$, $fg \in M(S, R)$. $\forall a \in S$, $fg(a) = f(a)g(a)$. Since $f(a) \in R$, $g(a) \in R$, $f(a)g(a) \in R$, $fg : S \to G$ is a well defined function. $fg \in M(S, R)$. $M(S, R)$ is a ring.

Exercise 3.1.5. If A is the abelian group $\mathbf{Z} \oplus \mathbf{Z}$, then End$A$ is a noncommutative ring.

Answer. We only need to verify that End$A$ is not commutative. Take $f, g \in \text{End}A$, $f : (x_1, x_2) \mapsto (x_1 \mod 2, x_2 \mod 2)$, $g : (x_1, x_2) \mapsto (x_1 \mod 3, x_2 \mod 3)$. Then $gf(3, 3) = (1, 1)$, $fg(3, 3) = (0, 0)$. Thus End$A$ is not commutative.

Exercise 3.1.6. A finite ring with more than one element and no zero divisors is a division ring.

Answer. For any disjoint $a, b, c \in R$, $ab \neq ac$, otherwise $a(b - c) = 0$, $b - c$ is a zero divisor. So ax are different for different $x \in R$. $|\{ax|x \in R\}| = |R|$ and $\{ax|x \in R\} \subset R$. Thus $\{ax|x \in R\} = R$ which means $\exists a^{-1} \in R$ s.t. $aa^{-1} = R$. Similarly, a is also left invertable and R is a division ring.

Exercise 3.1.7. Let R be a ring withe more than one element such that for each nonzero $a \in R$ there is a unique $b \in R$ such that $aba = a$. Prove:
(a) R has no zero divisors.

(b) $bab = b$.
(c) R has an identity.
(d) R is a division ring.

Answer. (a) If x is a zero divisor of a. WLOG, assume $ax = 0$, $axa \neq a$ so $b \neq x$. But $axa + aba = a(x + b)a = a$ which is contradictory to the uniqueness.
(b) $aba = a \Rightarrow abab = ab$, $a(bab - b) = 0$ and $a \neq 0$, so $bab - b =$, $bab = b$.
(c) Assume $c = ab$, $abab = ab \Rightarrow c^2 = c$. $\forall x \in R$, $xc^2 = xc \Rightarrow (xc - x)c = 0$ and $c \neq 0$, so $xc = x$ for any $x \in R$. Similarly, $cx = x$ for all $x \in R$, c is the identity of R.
(d) $\forall a, b \in R$, $aba = a \cdot 1_R = 1_R \cdot a$. So $a(ba - 1_R) = (ab - 1_R)a = 0$, $ba = ab = 1_R$. That means a, b are all units, so R is a division ring.

Exercise 3.1.8. Let R be the set of all 2×2 matrices over the complex field $\mathbf{C}$ of the form

$$\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$$

where $\bar{z}, \bar{w}$ are the complex conjugates of z and w respectively. Then R is a division ring that is isomorphic to the division ring K of real quaternions.

Answer. Define $f : K \to R$ with $f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $f(i) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $f(j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $f(k) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Assume $z = a + bi$, $w = c + di$.

$$\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Define

$$f(\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}) = af(1) + bf(i) + cf(j) + df(k)$$

$f(xy) = f(x)f(y)$ and f is a isomorphism, so $R \cong K$.

Exercise 3.1.9. (a) The subset $G = \{1, -1, i, -i, j, -j, k, -k\}$ of the division ring K of real quaternions forms a group under multiplication.

(b) G is isomorphic to the quaternion group.

(c) What is the difference between the ring K and the group $\mathbf{R}(G)(\mathbf{R}$ the field of real numbers)?

Answer. (a) Trivial.

(b) Define $f : G \to Q_8$ given by $f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $f(i) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $f(j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $f(k) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. We can verify that f is a isomorphism, $G \cong Q_8$.

(c) $R(G)$ is a free abelian group while K is not free on G.

Exercise 3.1.10. Let k, n be integers such that $0 \leq k \leq n$ and $\binom{n}{k}$ the binomial coefficient $n!/(n-k)!k!$, where $0! = 1$ and for $n > 0$, $n! = n(n-1)(n-2)\cdots 2 \cdot 1$.

(a) $\binom{n}{k} = \binom{n}{n-k}$

(b) $\binom{n}{k} < \binom{n}{k+1}$ for $k+1 \leq n/2$.

(c) $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ for $k < n$.

(d) $\binom{n}{k}$ is an integer.

(e) if p is prime and $1 \leq k \leq p^n - 1$, then $\binom{p^n}{k}$ is divisible by p.

(a) $\binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{n!}{(n-(n-k))!(n-k)!} = \binom{n}{n-k}$.

(b) $\binom{n}{k} = \frac{n!}{(n-k)!k!}$, $\binom{n}{k+1} = \frac{n!}{(n-k-1)!(k+1)!}$, since $k+1 \leq n-k$ when $k+1 \leq \frac{n}{2}$, then $\binom{n}{k} < \binom{n}{k+1}$.

(c) $\binom{n}{k} + \binom{n}{k+1} = \frac{n!}{(n-k)!k!} + \frac{n!}{(n-k-1)!(k+1)!} = \frac{(n+1)!}{(n-k)!(k+1)!} = \binom{n+1}{k+1}$.

(d) $\binom{n}{k}$ is an integer can be easily solved by induction and (c).

(e) $\mathrm{ord}_p(p^n!) = \sum\limits_{i=1}^{\infty} \left[\frac{p^n}{p^i}\right] = \sum\limits_{i=0}^{n-1} p^i$. $\mathrm{ord}_p(k!) = \sum\limits_{i=1}^{\infty} \left[\frac{k}{p^i}\right]$, $\mathrm{ord}_p((p^n-k)!) = \sum\limits_{i=1}^{\infty} \left[\frac{p^n-k}{p^i}\right]$. $\forall i \in \mathbf{N}$, $\left[\frac{p^n-k}{p^i}\right] + \left[\frac{k}{p^i}\right] \leq \left[\frac{p^n}{p^i}\right]$, the equality holds if and only if $\frac{p^n-k}{p^i}, \frac{k}{p^i} \in \mathbf{Z}$. And $\left[\frac{p^n-k}{p^n}\right] = 0$, $\left[\frac{k}{p^n}\right] = 0$. So $\mathrm{ord}_p((\binom{p^n}{k})) = \mathrm{ord}_p(p^n!) - \mathrm{ord}_p((n-k)!) - \mathrm{ord}_p(k!) \geq 1$. $p|\binom{p^n}{k}$.

Exercise 3.1.11. Let R be a commutative ring with identity of prime characteristic p. If $a, b \in R$, then $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$ for all integers $n \geq 0$.

Answer. $(a \pm b)^{p^n} = \sum\limits_{i=0}^{p^n} \binom{p^n}{i}(\pm a)^i b^{p^n-i}$. From **Exercise 3.1.10**, $p|\binom{p^n}{i}$ for all $i = 1, 2, \ldots, n-1$, so $\binom{p^n}{i}a^i b^{p^n-i} = 0$ for $i = 1, 2, \ldots, n-1$. Thus $\sum\limits_{i=0}^{p^n} \binom{p^n}{i}(\pm a)^i b^{p^n-i} = a^{p^n} \pm b^{p^n} = (a \pm b)^{p^n}$.

Exercise 3.1.12. An element of a ring is **nilpotent** if $a^n = 0$ for some n. Prove that in a commutative ring $a + b$ is nilpotent if a and b are. Show that this result may be false if R is not commutative.

Answer. Assume $a^m = 0$, $b^n = 0$. For $(a+b)^{m+n} = \sum\limits_{i=1}^{m+n} \binom{m+n}{i} a^i b^{m+n-i}$. If $i \geq m$, $a^i b^{m+n-i} = 0b^{m+n-i} = 0$; if $i \leq m$, $m+n-i \geq n$ so $a^i b^{m+n-i} = a^i 0 = 0$. Thus $a^i b^{m+n-i} = 0$ for all $i = 1, 2, \ldots, m+n$. $a+b$ is also nilpotent. For the 2×2 matrix ring. $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ are nilpotent, but $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is not nilpotent.

Exercise 3.1.13. In a ring R the following conditions are equivalent.
(a) R has no nonzero nilpotent elements.
(b) If $a \in R$ and $a^2 = 0$, then $a = 0$.

Answer. (a)$Rightarrow$(b): Trivial.
(b)$Rightarrow$(a): If $\exists a \in R$, $a^n = 0$ for some n and $a \neq 0$. Assume $n = 2^m \cdot k$ and k is a odd integer. Then $(a^{k \cdot 2^{m-1}})^2 = 0 \Rightarrow a^{k \cdot 2^{m-1}} = 0 \Rightarrow \cdots \Rightarrow a^k = 0$. $a^k \cdot a^{k+1} = 0$ and $2|k+1$, we can continue this step until $\frac{k+1}{2} \geq k$ which means $k = 1$. So $a = 0$.

Exercise 3.1.14. Let R be a commutative ring with identity and prime characteristic p. The map $R \to R$ given by $r \mapsto r^p$ is a homomorphism of rings called the Frobenius homomorphism.

Answer. $\forall a, b \in R$, $pa = pb = 0$ and the map $f : r \mapsto r^p$. $f(a+b) = (a+b)^p = \sum\limits_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$. Since p is a prime so $p \mid p!$ and $p \nmid i!(p-i)!$, $p \mid \binom{p}{i}$ for $i = 1, 2, \ldots, p-1$. So $f(a+b) = a^p + b^p = f(a) + f(b)$, $f(ab) = (ab)^p = a^p b^p = f(a)f(b)$, f is a homomorphism of rings.

Exercise 3.1.15. (a) Give an example of nonzero homomorphism $f : R \to S$ of rings with the identity such that $f(1_R) \neq 1_S$.

(b) If $f : R \to S$ is an epimorphism of rings with identity, then $f(1_R) = 1_S$.

(c) If $f : R \to S$ is a homomorphism of rings with identity and u is a unit in R such that $f(u)$ is a unit in S, then $f(1_R) = 1_S$ and $f(u^{-1}) = f(u)^{-1}$.

Answer. (a) For $f : Z_2 \to Z_6$ defined by $f(0) = 0$, $f(1) = 3$. f is a homomorphism of ring which satisfies the condition.

(b) $\forall s \in S$, $\exists r \in R$ such that $f(r) = s$, so $f(r)f(1_R) = f(1_R)f(r) = f(r) = s$, so $f(1_R) = 1_S$ is the identity of S.

(c) $f(u)f(u^{-1}) = f(u^{-1})f(u) = f(1_R)$. $\exists s \in S$ such that $f(u)s = sf(u) = 1_S$, $sf(u)f(u^{-1}) = sf(1_R) = f(u^{-1})$, $sf(1_R)f(u) = f(u^{-1})f(u) = f(1_R) = sf(u) = 1_S$. Thus $f(u^{-1} = s)$, $f(u^{-1}) = f(u)^{-1}$.

Exercise 3.1.16. Let $f : R \to S$ be a homomorphism of rings such that $f(r) \neq 0$ for some nonzero $r \in R$. If R has an identity and S has no zero divisors, then S is a ring with identity $f(1_R)$.

Answer. $f(1_R)f(1_R) = f(1_R)$, so $f(1_R)(f(1_R) - 1_S) = 0 \Rightarrow f(1_R) = 1_S$.

Exercise 3.1.17. (a) If R is a ring, then so is R^{op} is defined as follows. The underlying set of R^{op} is precisely R and addition in R^{op} coincides with addition in R. Multiplication in R^{op}, denoted $\circ$, is defined by $a \circ b = ba$, where ba is the product in R. R^{op} is called the **opposite ring** of R.

(b) R has identity if and only if R^{op} does.

(c) R is a division ring if and only if R^{op} is.

(d) $(R^{op})^{op} = R$.

(e) If S is a ring, then $R \cong S$ if and only if $R^{op} \cong S^{op}$.

Answer. (a) Trivial.

(b) If 1_R is the identity of R. Take $1_{R^{op}} = 1_R$ then $\forall a \in R^{op}$, $1_{R^{op}} \circ a = a1_R = a = 1_R a = a \circ 1_{R^{op}}$. So $1_{R^{op}}$ is the identity of R^{op}.

(c) $\forall a \in R^{op}$, take $a^{-1} \in R$, $a^{-1} \circ a = aa^{-1} = 1_R = a^{-1}a = a \circ a^{-1}$. So a is a unit, R^{op} is a division ring.

(d) Denote $*$ is the multiplication in $(R^{op})^{op}$.

$$a * b = b \circ a = ab \in R$$

The multiplications are identical. The underlying set and addition of R and $(R^{op})^{op}$ are identical. So $R = (R^{op})^{op}$.

(e) If $R \cong S$, there exists isomorphism $f : R \to S$. We verify that $f' R^{op} \to S^{op}$ defined by $f' = f$ is an isomorphism. $f' = f$ is obviously a bijection. $f'(a) \circ f'(b) = f(b)f(a) = f(ba) = f'(a \circ b)$. f' is a well defined homomorphism, so $R^{op} \cong S^{op}$.

Exercise 3.1.18. Let $\mathbf{Q}$ be the field of rational numbers and R any ring. If $f, g : \mathbf{Q} \to R$ are homomorphisms of rings such that $f|\mathbf{Z} = g|\mathbf{Z}$, then $f = g$.

Answer. $f(n) = g(n)$ for $n \in \mathbf{Z}$. $g(n)g(\frac{1}{n}) = g(1) \Rightarrow f(n)g(\frac{1}{n}) = g(1) = f(1)$, so $f(\frac{1}{n})f(n)g(\frac{1}{n}) = g(\frac{1}{n}) = f(\frac{1}{n})$ for all $n \in \mathbf{Z}$. Thus $f = g$.

3.2 Ideals

Exercise 3.2.1. The set of all nilpotent elements in a commutative ring forms an ideal.

Answer. Assume the set is I, then $\forall a, b \in I$, $a^m = b^n = 0$, $(a+b)^{m+n} = 0$ and $(ab)^{mn} = 0$ so $a+b \in I$, $ab \in I$. I is a subring. $\forall x \in R$, $(xa)^m = x^m a^m = 0$, $(ax)^m = a^m x^m = 0$, so $xa \in I$ and $ax \in I$, I is an ideal.

Exercise 3.2.2. Let I be an ideal in a commutative ring R and let $\mathrm{Rad}I = \{r \in R | r^n \in I \text{ for some } n\}$. Show that $\mathrm{Rad}I$ is an ideal.

Answer. $\mathrm{Rad}I$ is a ring since R is a commutative ring. For $r \in \mathrm{Rad}I$ and $\forall x \in R$, $(xr)^n = x^n r^n \in I$ so $xr \in \mathrm{Rad}I$, $(rx)^n = r^n x^n \in I$ so $rx \in \mathrm{Rad}I$. Thus $\mathrm{Rad}I$ is an ideal.

Exercise 3.2.3. If R is a ring and $a \in R$, then $J = \{r \in R | ra = 0\}$ is a left ideal and $K = \{r \in R | ar = 0\}$ is a right ideal in R.

Answer. J is a subring of R. For $r \in J$ and $\forall x \in R$, $(xr)a = x(ra) = 0$ so $xr \in J$, J is a left ideal. Similarly, I is a right ideal.

Exercise 3.2.4. If I is a left ideal of R, then $A(I) = \{r \in R | rx = 0 \text{ for every } x \in I\}$ is an ideal in R.

Answer. For any $a, b \in A(I)$, we have $ab \in A(I)$ and $a+b \in A(I)$. For $r \in A(I)$ and $\forall x \in R$, $(xr)x' = x(rx') = 0$ for every $x' \in I$, so $xr \in A(I)$. $(rx)x' = r(xx')$, $xx' \in I$ so $rxx' = 0$, $rx \in A(I)$. Thus $A(I)$ is an ideal of R.

Exercise 3.2.5. If I is an ideal in a ring R, let $[R : I] = \{r \in R | xr \in I \text{ for every } x \in R\}$. Prove that $[R : I]$ is an ideal of R which contains I.

Answer. I is a subring of R so $[R : I]$ is also a subring of R. For $r \in [R : I]$ and $x, x' \in R$, $x'xr = (x'x)r \in I$ so $xr \in [R : I]$, $x'rx = (x'r)x \in I$ so $rx \in [R : I]$. $[R : I]$ is an ideal of R. Since $\forall r \in I$, $xr \in I$ and $rx \in I$, $I \subset [R : I]$.

Exercise 3.2.6. (a) The center of the ring S of all 2×2 matrices over a field F consists of all matrices of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$.

(b) Then center of S is not an ideal in S.

(c) What is the center of the ring of all $n \times n$ matrices over a division ring?

Answer. (a) $\forall x \in M_F(2, 2)$, $x = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$

$$x \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} x = \begin{pmatrix} ax_1 & ax_2 \\ ax_3 & ax_4 \end{pmatrix}$$

so $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in C(M_F(2, 2))$.

$\forall \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in C(M_F(2, 2))$, take $\begin{pmatrix} 0 & 1_F \\ 0 & 0 \end{pmatrix} \in M_F(2, 2)$

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} 1_F & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ a_3 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1_F & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ 0 & 0 \end{pmatrix}$$

so $a_2 = a_3 = 0$.

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} 0 & 1_F \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a_1 \\ 0 & a_3 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1_F \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} a_3 & a_4 \\ 0 & 0 \end{pmatrix}$$

so $a_1 = a_4$. All the elements of $C(M_F(2, 2))$ has the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$.

(b) For $c \in C(S)$. If S is not commutative, $\forall x, x' \in R$, we need $xc \in C(S) \Rightarrow x'xc = xcx' = xx'c$, however, this may not always true.

(c) By multiplying $\begin{pmatrix} 1_F & & \\ & \ddots & \\ & & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & & & \\ & 1_F & & \\ & & \ddots & \\ & & & 0 \end{pmatrix}$, $\dots$, $\begin{pmatrix} 0 & & \\ & \ddots & \\ & & 1_F \end{pmatrix}$, we can have $C(M_F(2,2))$ consist of all the elements in the form of $a\begin{pmatrix} 1_F & & & \\ & 1_F & & \\ & & \ddots & \\ & & & 1_F \end{pmatrix}$.

Exercise 3.2.7. (a) A ring R with identity is a division ring if and only if R has no proper left ideals.

(b) If S is a ring (possibly without identity) with no proper left ideals, then either $S^2 = 0$ or S is a division ring.

Answer. (a) Suppose not. I is an ideal in R. $\forall r \in I$, take $r^{-1} \in R$, then $1_R \in I$ so $I = R$ is not a proper ideal.

(b) $I = \{a \in S | Sa = 0\}$ is a left ideal since $\forall x, x' \in S$, $x'(xs) = (x'x)s = 0$, $xs \in I$. Thus $I = 0$ or $I = S$. If $I = S$, then $S^2 = 0$. If $I = 0$, we prove S has no zero divisor.

For the set $I' = \{r \in S | rb = 0\}$, $I' \subset I$. I' is a subring of S, and I' is also a left ideal of S. So $I' = 0$, b has no left zero divisors. $\forall a \in S$, Sa is a left ideal of S. $Sa \neq 0$ so $Sa = S$. Thus, $\exists 1_S \in S$, such that $1_S a = a$. Since $s_1 - s_2$ has no left zero divisor, $as_1 = as_2 \Rightarrow s_1 = s_2$. So $aS = S$. For all $s \in S$, $\exists s'$ s.t. $s = as'$ so $\forall s \in S$, $1_S \cdot s = 1_S as' = as' = s$. $aS = S$ so $\exists 1'_S \in S$, $a1'_S = a$. Similarly, $\forall s \in S$, $s1_S = s$. Then $1_S 1'_S = 1_S = 1'_S$ so S has identity. Since $Sa = aS = S$, we can have S is a division ring.

Exercise 3.2.8. Let R be a ring with identity and S the ring of all $n \times n$ matrices over R. J is an ideals of S if and only if J is the ring of all $n \times n$ matrices over I for some ideal I in R.

Answer. If J is an ideal. Denote $E_{r,s}$ as the matrix which has 1_R as the r column and s row. Then $\forall A = (a_{ij})$, $E_{p,r} A E_{s,q}$ is a matrix with a_{rs} in the p column and q row. So for $A \in J$ $(aE_{p,r})A(bE_{s,q})$ is the matrix with $aa_{rs}b$

in the p column and q row. $aa_{rs}b \in I$. Then because of closure we know J contains all $n \times n$ matrices over I.
If J consists of all $n \times n$ matrices over I, the proof is trivial.

Exercise 3.2.9. Let S be the ring of all $n \times n$ matrices over a division ring D.
(a) S has no proper ideals (that is, 0 is the maximal ideal).
(b) S has zero divisors. Consequently, (i) $S \cong S/0$ is not a division ring and (ii) 0 is a prime ideal which does not satisfy condition (1) of Theorem 2.15.

Answer. (a) J is an ideal of S so J consists of all $n \times n$ matrices over I where I is an ideal of D. From **Exercise 3.2.7**, D has no proper ideal so $I = 0 \Rightarrow J = 0$.
(b) For $A = (a_{ij})$ with $a_{ri} = 0$ for $i = 1, 2 \cdots$ and other entries doesn't equals to zero, we have $E_{1r}A = 0$. S has no zero divisors.

Exercise 3.2.10. (a) Show that $\mathbf{Z}$ is a principal ideal ring.
(b) Every homomorphic image of a principal ideal ring is also a principal ideal ring.
(c) Z_m is a principal ideal ring for every $m > 0$.

Answer. (a) For any ideal I in $\mathbf{Z}$, I is a subring so $I = m\mathbf{Z}$ where $m \in \mathbf{Z}$. $m\mathbf{Z} = (m)$ is a principal ideal so $\mathbf{Z}$ is a PID.
(b) For $f : R \to S$ with $f(r) = s$ and R is a principal ideal ring. Consider $f : R \to \text{Im}f \subset S$. For any ideal $J \subset \text{Im}f$, $f^{-1}(J)$ is an ideal since $\forall a \in f^{-1}(J)$ and $r \in R$, $f(ar) = f(a)f(r) \in J \Rightarrow ar \in f^{-1}(J)$. $f^{-1}(J)$ is a principal ideal, assume $f^{-1}(J) = (a)$. Then $\forall r \in R$, $ar \in (a)$, $ra \in (a)$. $f(ar) = f(a)f(r) \in J$ and $f(ra) = f(r)f(a) \in J$ since $f(a) \in J$ and $f(r) \in S$. So $(f(a)) \subset J$. $J = f((a)) = \{f(ra + as + na + \sum_{i=1}^{m} r_i a s_i) | r, s, r_i, s_i \in R, n \in \mathbf{Z}\} = \{f(r)f(a) + f(a)f(s) + nf(a) + \sum_{i=1}^{m} f(r_i)f(a_i)f(s_i) | r, s, r_i, s_i \in R, n \in \mathbf{Z}\} \subset (f(a))$. So $J = (f(a))$ is a principal ideal. The image of a principal ideal ring is also a principal ideal ring.

Exercise 3.2.11. If N is the ideal of all nilpotent elements in a commutative ring R, then R/N is a ring with no nonzero nilpotent elements.

Answer. Suppose not. $\exists r \in R$, $r \notin N$, $(r+N)^n = 0$ for some $n \in \mathbf{N}$.

$$(r+N)^n = r^n + N = N \Rightarrow r^n \in N$$

so for some $m \in \mathbf{N}$, $r^{nm} = 0 \Rightarrow r \in N$. That's contradictory!

Exercise 3.2.12. Let R be a ring without identity and with no zero divisors. Let S be the ring whose additive group is $R \times \mathbf{Z}$ as in the proof of Theorem 1.10. Let $A = \{(r,n) \in S | rx + nx = 0 \text{ for every } x \in R\}$.
(a) A is an ideal in S.
(b) S/A has an identity and contains a subring isomorphic to R.
(c) S/A has no zero divisors.

Answer. (a) For $(r,n),(r',n') \in S$, $(r'+r)x + (n'+j)x = rx + nx + r'x + n'x = 0$, so $(r+r', n+n') \in A$. $(r,n)(r'n') = (rr' + nr' + n'r, nn')$, $rr'x + n'rx + nr'x + nn'x = r(r'x + n'x) + n(r'x + n'x) = 0$, so $(r,n)(r',n') \in A$. A is a subring of $R \times \mathbf{Z}$. $\forall (r_1, n_1) \in R \times \mathbf{Z}$, $(r_1,n_1)(r,n) = (r_1 r + n r_1 + n_1 r, n n_1) \Rightarrow r_1 r x + n r_1 x + n_1 r x + n n_1 x = r_1(rx + nx) + n_1(rx + nx) = 0 \Rightarrow (r_1, n_1)(r,n) \in A$. A is an ideal of $R \times \mathbf{Z}$.

(b) Take $0_R \in R$ and $(0_R, 1) \in S$. Then $(0_R, 1) + A$ is an identity of S/A.

$$\forall (r,n) \in S, \quad (r,n)(0_R,1) = (0_R,1)(r,n) = (r,n)$$

(c) For any $(r,n),(s,m)$ satisfy that $(r,n)(s,m) \in A$, we prove that $(r,n) \in A$ or $(s,m) \in A$. Suppose $sx + mx \neq 0$, $r(sx+mx) + n(sx+mx) = 0 \Rightarrow (sx+mx)r(sx+mx) + n(sx+mx)^2 = 0 \Rightarrow ((sx+mx)r + n(sx+mx))(sx+mx) = 0 \Rightarrow (sx+mx)r + n(sx+mx) = 0$. For any $x \in R$, $(sx+mx)rx + n(sx+mx)x = 0 \Rightarrow (sx+mx)(rx+nx) = 0 \Rightarrow rx+nx = 0$, so $(r,n) \in A$. S/A has no divisor.

Exercise 3.2.13. Let $f : R \to S$ be a homomorphism of rings, I and ideal in R, and J an ideal in S.

(a) $f^{-1}(J)$ is and ideal in R that contains Ker$f$.

(b) If f is an epimorphism, then $f(I)$ is an ideal in S. If f is not surjective, $f(I)$ need not be an ideal.

Answer. (a) $\forall a \in f^{-1}(J)$ and $r \in R$, $f(ar) = f(a)f(r) \in J \Rightarrow ar \in J$. Similarly, $ra \in J$, $f^{-1}(J)$ is an ideal. Ker$f \subset f^{-1}(J)$ since $0_S \in J$.

(b) $\forall b \in f(I)$ and $s \in S$, f is a epimorphism so $s = f(r)$, $b = f(a)$ for some $r, a \in R$. $sb = f(r)f(a) = f(ar)$, $ar \in I \Rightarrow sb \in f(I)$, similarly $bs \in f(I)$. $f(I)$ is an ideal.

If f is not surjective. Take $Z[x]$ and $\mathbf{Z}$ which is a subring but not an ideal in $Z[x]$. $\mathbf{Z}$ is an ideal of itself, $f = 1_{\mathbf{Z}}$ satisfies the condition.

Exercise 3.2.14. If P is an ideal in a not necessarily commutative ring R, then the following conditions are equivalent.

(a) P is a prime ideal.

(b) If $r, s \in R$ are such that $rRs \subset R$, then $r \in P$ or $s \in P$.

(c) If (r) and (s) are principal ideals of R such that $(r)(s) \subset P$, then $r \in P$ or $s \in P$.

(d) If U and V are right ideals in R such that $UV \subset R$, then $U \subset R$ or $V \subset R$.

(e) If U and V are left ideals in R such that $UV \subset R$, then $U \subset R$ or $V \subset R$.

Exercise 3.2.15. The set consisting of zero and all zero divisors in a commutative ring with identity contains at least one prime ideal.

Answer. Denote $S = R - Z$. $\forall a, b \in S$, we prove that $ab \in S$. Suppose $\exists (ab)c = 0$ for some $c \in R$, a, b are not zero divisors so $abc = b(ac) = a(bc) = 0$, so $ac = 0$, $bc = 0 \Rightarrow c = 0$, so ab is not a zero divisor. Thus $Z = R - S$ contains an prime ideal.

Exercise 3.2.16. Let R be a commutative ring with identity and suppose that the ideal A of R is contained in a finite union of prime ideals $P_1 \cup \cdots \cup P_n$. Show that $A \subset P_i$ for some i.

Answer. Suppose not. We choose the smallest I such that for all $i \in I$, $P_i \cap A \neq \varnothing$ and $A \cap P_i \not\subset \bigcup\limits_{j \neq i} P_j$ for any $i \in I$. So $\exists a_i \in (A \cap P_i) - (\bigcup\limits_{j \neq i} P_j)$, $\forall i \in I$. Take $x = a_1 + a_2 a_3 \cdots a_n$, $x \in A$ since $a_i \in A$ for all $i \in I$. And $x \notin P_i$ for $i = 2, 3, \ldots, n$ since $a_1 \notin P_i$, $i = 2, 3, \ldots, n$. $x \notin P_1$ since P_1 is prime and $a_2, \ldots, a_n \notin P_1$. So $x \notin \bigcup\limits_{j \neq i} P_j$, which is contradictory!

Exercise 3.2.17. Let $f : R \to S$ be an epimorphism of rings with kernel K.

(a) If P is a prime ideal in R that contains K, then $f(P)$ is a prime ideal in S.

(b) If Q is a prime ideal in S, then $f^{-1}(Q)$ is a prime ideal in R that contains K.

(c) There is a one-to-one correspondence between the set of all prime ideals in R that contain K and the set of all prime ideals in S, given by $P \mapsto f(P)$.

(d) If I is an ideal in a ring R, then every prime ideal in R/I is of the form P/I, where P is a prime ideal in R that contains I.

Answer. (a) From **Exercise 3.2.13** we know $f(P)$ is an ideal. $\forall x, y \in f(P)$, $\exists a.b \in R$, $x = f(a)$, $y = f(b)$ and $a, b \notin P$. Assume $\exists p \in P$ such that $f(ab) = f(p)$, then $f(ab - p) = 0$, $ab - p \in \text{Ker} f \subset P \Rightarrow ab \in P$. That's contradictory to $a, b \notin P$ so $xy \notin f(P)$. $f(P)$ is prime.

(b) From **Exercise 3.2.13**, $f^{-1}(Q)$ is an ideal. Take $g : S \to S/Q$ and $gf : R \to S/Q$. By the Theorem of homomorphism, $R/f^{-1}(Q) \cong S/Q$ is a ring without divisor, so $f^{-1}(Q)$ is prime.

(c) From (a), (b), f is a one-to-one map between prime ideals given by $P \mapsto f(P)$.

(d) Consider the homomorphism $f : R \to R/I$. For any prime ideal $P \subset R$ and $f(P)$ is an prime ideal in R, $\text{Ker} f = I$ so for prime ideals $I \subset P \subset R$. P can have one to one correspondence with $f(P) = P/I \subset R/I$. So all the prime ideals has the form P/I.

Exercise 3.2.18. An ideal $M \neq R$ in a commutative ring R with identity is maximal if and only if for every $r \in R - M$, there exists $x \in R$ such that $1_R - rx \in M$.

Answer. If M is maximal, then M is prime. So $rR + M = R$, $r(R - M) + M = R$ and $r(R - M) \cap M = \varnothing$. Take $1_R \in R$ we have $x \in R - M$, $1_R - xr \in M$. If $\forall r \in R - M$, $\exists x \in R$ such that $1_R - rx \in M$. Suppose $M \subset I \subset R$ where I is an ideal, $I \neq R$ so $1_R \notin R$. Take $r \in I - M \subset R - M$, then $\forall x \in R$, $rx \in I$, so $1_R - rx \notin I$ thus $1_R - rx \notin M$. That's contradictory!

Exercise 3.2.19. The ring E of even integers contains a maximal ideal M such that E/M is not a field.

Answer. $E = 2\mathbf{Z}$ and M is a maximal ideal in E and for any subring of E has the form $wn\mathbf{Z}$ where $n \in \mathbf{Z}$. $2n\mathbf{Z}$ is an ideal in $2\mathbf{Z}$. Take $n = 15$, $(2, 15) = 1$ so $2\mathbf{Z}/30\mathbf{Z} \cong \mathbf{Z}/15\mathbf{Z}$ which is not a field since $3 \cdot 5 = 0$ is a zero divisor.

Exercise 3.2.20. In the ring $\mathbf{Z}$ the following conditions on a nonzero ideal I are equivalent: (i) I is prime; (ii) I is maximal; (iii) $I = (p)$ with p prime.

Answer. $\mathbf{Z}$ is an integer domain so (ii)$\Rightarrow$(i).
(i)$\Rightarrow$(iii): Trivial.
(iii)$\Rightarrow$(ii): For any $n \notin (p)$, we have $p \nmid n$ thus $\exists x, y \in \mathbf{Z}$ such that $px + my = 1$. Consider an ideal I and $(p) \subset I$, $n \in I$, then $1 \in I$ so $I = \mathbf{Z}$ which means (p) is maximal.

Exercise 3.2.21. Determine all prime and maximal ideals in the ring Z_m.

Answer. $Z_m^2 = Z_m$ so every maximal ideal is prime in Z_m. $Z_m \cong \mathbf{Z}/m\mathbf{Z}$ via $\varphi : \bar{x} \mapsto mz + x$. From **Exercise 3.2.17**, all the prime ideals in $\mathbf{Z}/m\mathbf{Z}$ are $P/m\mathbf{Z}$, where P is a prime ideal contains $m\mathbf{Z} = (m)$.
If m is prime, (m) is prime, too. So no such ideal exist.
If $m = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$ where p_i are primes, then $(p_1), (p_2), \ldots, (p_n)$ are prime ideals and $f((\bar{p_i})) = (p_i)/m\mathbf{Z}$ are prime ideals. So all the prime ideals in Z_m are $(\bar{p_i})$, $i, 1, 2, \ldots, n$.

Exercise 3.2.22. (a) If $R_1, \ldots, R_n$ are rings with identity and I is an ideal in $R_1 \times \cdots \times R_n$, then $I = A_1 \times \cdots \times A_m$, where each A_i is an ideal in R_i.

(b) Show that the conclusion of (a) need not hold if the rings R_i do not have identities.

Exercise 3.2.23. An element e in a ring R is said to be **idempotent** if $e^2 = e$. An element of the center of the ring R is said to be central. If e is a central idempotent in a ring R with identity, then

(a) $1_R - e$ is a central idempotent;

(b) eR and $(1_R - e)R$ are ideals in R such that $R = eR \times (1_R - e)R$.

Answer. (a) $(1_R - e)^2 = 1_R - 2e + e^2 = 1_R - 2e + e = 1_R - e$. $\forall x \in R$, $ex = xe$ so $(1_R - e)x = x - ex = x - xe = x(1_R - e)$. $1_R - e$ is a central idempotent.

(b) $eR \cup (1_R - e)R \subset R$ so $\langle eR \cap (1_R - e)R\rangle \subset R$. $R = eR + (1_R - e)R$ so $R \subset \langle eR \cap (1_R - e)R\rangle$. So $R = \langle eR \cap (1_R - e)R\rangle$. $\langle eR\rangle = eR$ and $\langle (1_R - e)R\rangle = (1_R - e)R$ so $\langle eR\rangle \cap \langle (1_R - e)R\rangle = 0$. Thus $R = eR \times (1_R - e)R$.

Exercise 3.2.24. Idempotent elements $e_1, \ldots, e_n$ in a ring R are said to be **orthogonal** if $e_ie_j = 0$ for $i \neq j$. If $R, R_1, \ldots, R_n$ are rings with identity, then the following conditions are equivalent:

(a) $R \cong R_1 \times \cdots \times R_n$.

(b) R contains a set of orthogonal central idempotents $\{e_1, \ldots, e_n\}$ such that $e_1 + e_2 + \cdots + e_n = 1_R$ and $e_iR \cong R$ for each i.

(c) R is the internal direct product $R = A_1 \times \cdots \times A_n$ where each A_i is an ideal of R such that $A_i \cong R_i$.

Answer. Assume $f : R_1 \times \cdots \times R_n \to R$ is an isomorphism.

(a)⇒(b): Denote $\bar{e_1} = (1_R, 0, \ldots, 0)$, $\bar{e_2} = (0, 1_R, \ldots, 0)$, $\ldots$, $\bar{e_n} = (0, 0, \ldots, 1_R)$. They are orthogonal central idempotent in $S = R_1 \times \cdots \times R_n$ and $f(\bar{e_n}) = e_n$, $e_1 + e_2 + \cdots + e_n = 1_S$, $\sum\limits_{i=1}^{n} e_iS = S$.

Take $\varphi_i : (r_1, r_2, \dots, r_i, \dots, r_n) \mapsto r_i$. Then φ_i is a well defined isomorphism between e_iS and R_i. $e_iR \cong \bar{e}_iS \cong R_i$.
(b)⇒(c): Take $A_i = e_iR$, then $A_i \cong R_i$. We need to prove $R = e_iR \times e_2R \times \cdots \times e_nR$. $e_iR \cap (e_1R + e_2R + \cdots + e_{i-1}R + e_{i+1}R + \cdots + e_nR) = 0$ since $e_ix_i = e_1x_1 + e_2x_2 + \cdots + e_{i-1}x_{i-1} + e_{i+1}x_{i+1} + \cdots + e_nx_n \Rightarrow e_i^2x_i = 0$. $R = 1_RR = \sum\limits_{i=1}^{n} e_iR$ so $R = e_iR \times e_2R \times \cdots \times e_nR$.
(c)⇒(a): Trivial.

Exercise 3.2.25. If $m \in \mathbf{Z}$ has a prime decomposition $m = p_1^{k_1} \cdots p_t^{k_t}(k_i > 0$; p_i distinct primes), then there is an isomorphism of rings $Z_m \cong Z_{p_1^{k_1}} \times \cdots \times Z_{p_t^{k_t}}$.

Answer. For any $m \in \mathbf{Z}$, $\mathbf{Z}/m\mathbf{Z} \cong Z_m$. $p_1^{k_1}\mathbf{Z} \cap \cdots \cap p_t^{k_t}\mathbf{Z} = m\mathbf{Z}$. So $\exists \varphi : Z_m \mapsto Z_{p_i^{k_1}} \times \cdots \times Z_{p_t^{k_t}}$. $\forall i, j \in I$, $p_i^{k_i} \in p_i^{k_i}\mathbf{Z}$ and $p_j^{k_j} \in p_j^{k_j}\mathbf{Z}$, $\exists x, y \in \mathbf{Z}$ such that $xp_i^{k_i} + yp_j^{k_j} = 1 \in \mathbf{Z}$. So $p_i^{k_i}\mathbf{Z} + p_j^{k_j}\mathbf{Z} = \mathbf{Z}$, φ is an isomorphism so $Z_m \cong Z_{p_1^{k_1}} \times \cdots \times Z_{p_t^{k_t}}$.

Exercise 3.2.26. If $R = \mathbf{Z}$, $A_1 = (6)$ and $A_2 = (4)$, then the map $\theta : R/A_1 \cap A_2 \to R_1/A_1 \times R_2/A_2$ of Corollary 2.27 is not surjective.

Answer. $R/(A_1 \cap A_2) = Z_{12}$, $R/A_1 = Z_6$ and $R/A_2 = Z_4$. $|Z_6 \times Z_4| = |Z_6| \times |Z_4| = 24$ but $|Z_{12}| = 12$, so θ is surjective.

3.3 Factorization in commutative rings

Exercise 3.3.1. A nonzero ideal in a principal ideal domain is maximal if and only if it is prime.

Answer. For PID R, $R^2 = R$ so every maximal ideal is prime. If $I = (p) \neq 0$ is prime in R, then p is prime so p is irreducible and (p) is maximal.

Exercise 3.3.2. An integral domain R is unique factorization domain if and only if every non zero prime ideal in R contains a nonzero principal ideal that is prime.

Answer. Suppose R is a unique factorization domain and $P \neq 0$ is a prime ideal. Let $x \in P$ be a nonzero nonunit. Then x can be factored into $x = p_1 p_2 \cdots p_n$ a product of prime elements. Then $x \in P$ implies $p_i \in P$ for some i, so $(p_i) \subset P$.
Conversely, assume that each nonzero prime ideal of R contains a principal prime ideal.

Lemma. *Let R be a commutative ring and $S \subset R \backslash \{0\}$ a multiplicatively closed subset containing 1_R. Let $\mathcal{I}_S$ be the set of ideals of R which are disjoint from S. Then*
(a) $\mathcal{I}_S$ is nonempty.
(b) Every element of $\mathcal{I}_S$ is contained in a maximal element oof $\mathcal{I}_S$.
(c) Every maximal element of $\mathcal{I}_S$ is prime.

Here's the proof of the lemma:
(a) Trivial.
(b) Let $I \in \mathcal{I}_S$. Consider the subposet P_I of $\mathcal{I}_S$ consisting of ideals which contain I. Since $I \in P_I$, P_I is nonempty; moreover, any chain in P_I has an upper bound,namely the union of all of its elements. Therefore by Zorn's lemma, P_I has a maximal element of $\mathcal{I}_S$, which is clearly also a maximal element of $\mathcal{I}_S$.
(c) Let I be a maximal element of $\mathcal{I}_S$; suppose that $x, y \in R$ are such that $xy \in I$. If x is not in I, then $\langle I, x \rangle \supsetneq I$ and therefore contains an element s_1 of S, say

$$s_1 = i_1 + ax$$

Similarly, if y is not in I, then we get an element s_2 of S of the form

$$s_2 = i_2 + by$$

But then

$$s_1s_2 = i_1i_2 + (by)i_1 + (ax)i_2 + (ab)xy \in I \cap S$$

a contradiction!

A multiplicative subset S is saturated if for all $x \in S$ and $y \in R$, if $y \mid x$ then $y \in S$. We define the saturation $\bar{S}$ of a multiplicatively closed subset S to be the intersection of all saturated multiplicatively closed subsets containing S. Let S be the set of units of R together with all product of prime elements. One checks easily that S is saturated multiplicative subset. We should show that $S = \frac{R}{\setminus}\{0\}$. Suppose then for a contradiction that there exists a nonzero nonunit $x \in R\setminus S$. Then saturation of S implies that $S \cap (x) = \varnothing$, and then there exists a prime ideal P contains x and disjoint from S. But by the hypothesis, P contains a prime element p, contradictting its disjointness from S.

Exercise 3.3.3. Let R be the subring $\{a + b\sqrt{10} | a, b \in \mathbf{Z}\}$ of the field of real numbers

(a) The map $N : R \to Z$ given by $a + b\sqrt{10} \mapsto (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$ is such that $N(uv) = N(u)N(v)$ for all $u, v \in R$ and $N(u) = 0$ if and only if $u = 0$.

(b) u is a unit in R if and only if $N(u) = \pm 1$.

(c) $2, 3, 4 + \sqrt{10}$ and $4 - \sqrt{10}$ are irreducible elements of R.

(d) $2, 3, 4 + \sqrt{10}$ and $4 - \sqrt{10}$ are not prime elements of R.

Answer. (a) Assume $u = a_1 + b_1\sqrt{10}$, $v = a_2 + b_2\sqrt{10}$.

$$\begin{aligned} N(uv) &= N(a_1a_2 + 10b_1b_2 + (a_1b_2 + a_2b_1)\sqrt{10}) \\ &= (a_1a_1 + 10b_1b_2)^2 - 10(a_1b_2 + a_2b_1)^2 \\ &= a_1^2a_2^2 + 100b_1^2b_2^2 - 10a_1^2b_2^2 - 10a_2^2b_1^2 \end{aligned}$$

$$N(u)N(v) = (a_1^2 - 10b_1^2)(a_2^2 - 10b_2^2) = N(uv)$$

(b) If u is a unit of R, $N(uu^{-1}) = N(1) = N(u)N(u^{-1}) = 1$. $N(u)$ and $N(u^{-1}) \in \mathbf{Z}$ so $N(u) = \pm 1$.

(c) Suppose $4 + \sqrt{10} = (a_1 + b_1\sqrt{10})(a_2 + b_2\sqrt{10})$ where $N(a_1 + b_1\sqrt{10})$, $N(a_2 + b_2\sqrt{10}) \neq \pm 1$. $N(4 + \sqrt{10}) = 6 = N(a_1 + b_1\sqrt{10})N(a_2 + b_2\sqrt{10})$

so $N(a_1+b_1\sqrt{10}) = \pm 2$ and $N(a_2+b_2\sqrt{10}) = \pm 3$. WLOG, assume $N(a_1+b_1\sqrt{10}) = 2$ and $N(a_2+b_2\sqrt{10}) = 3$.

$$a_1^2 = 10b_1^2 + 2 \Rightarrow a_1^2 \equiv 2 \mod 10$$

$$a_2^2 = 10b_2^2 + 3 \Rightarrow a_2^2 \equiv 3 \mod 10$$

This can't be true! So $4+\sqrt{10}$ is irreducible. Similarly, 2,3,$4-\sqrt{10}$ is irreducible.

(d) $3 \cdot 2 = (4+\sqrt{10})(4-\sqrt{10}) - 6$, But none of these four numbers divide another.

Exercise 3.3.4. Show that in the integral domain of **Exercise 3.3.3** every element can be factored into a product of irreducibles, but this factorization need not be unique.

Answer. Suppose a can be factored into $a_1a_2\cdots a_n\cdots$ which may not be finite. We only need to prove there are finite a_i are irreducible. $N(a) = N(a_1)N(a_2)\cdots N(a_n)\cdots = k \in \mathbf{Z}$. Assume $k = k_1k_2\cdots k_m$ and for irreducible a_i, $N(a_i) \neq \pm 1$, so there are at most m a_i irreducible. Thus a can be factored into a product of irreducibles.

Exercise 3.3.5. Let R be a principal ideal domain.

(a) Every proper ideal is a product $P_1P_2\cdots P_n$ of maximal ideals, which are unique ly determined up to order.

(b) An ideal P in R is said to be primary if $ab \in P$ and $a \notin P$ imply $b^n \in P$ for some n. Show that P is primary if and only if for some n, $P = (p^n)$ where $p \in R$ is prime or $p = 0$.

(c) If $P_1, P_2, \ldots, P_n$ are primary ideals such that $P_i = (p_i^{n_i})$ and the p_i are distinct primes, then $P_1P_2\cdots P_n = P_1 \cap P_2 \cap \cdots \cap P_n$.

(d) Every proper ideal in R can be expressed (uniquely up to order) as the intersection of a finite number of primary ideals.

Answer. (a) For any ideal (a), a can be factored into irreducible product $a_1a_2\cdots a_n$. (a_i) are maximal in R and $(a) = (a_1)(a_2)\cdots(a_n)$.

(b) If $P = (p^n)$. For any $ab \in P$, $ab = p^n x$ for some $x \in R$ and $n \in \mathbf{Z}$. R is a UFD so $p \mid a$ or $p \mid b$ so $b^n \in P$. Conversely, $\forall P = (k)$ we prove $k = p^t$ for some prime p and $t \in \mathbf{Z}$. For any $ab = kx$, assume $a = a_1^1 \cdots a_m^{p_m}$, $b = a_1^{q_1} \cdots a_m^{q_m}$ and $k = a_1^{s_1} \cdots a_m^{s_m}$, p_i, q_i, s_i are all nonnegative integers. We prove that for all but one i, $s_i = 0$. Take $p_i = 0$ for $i = 1, 2, \ldots, m-1$, $p_m = s_m$, $q_i = s_i$ for $i = 1, 2, \ldots, m-1$, $q_m = 0$, then $ab = k \in (k)$ but a, a^n, b, $b^n \notin (k)$ for all $n \in \mathbf{Z}$. So $k = a_i^{s_i}$ for some $s_i \in \mathbf{Z}$, $(k) = (a_i^{s_i})$, a_i prime.

(c) $P_1 P_2 \cdots P_n \subset P_1 \cap P_2 \cap \cdots \cap P_n$ is trivial.
For any $a \in P_1 \cap \cdots \cap P_n$, $p_i^{n_i} | a$, $\forall i = 1, 2, \ldots, n$. $p_i^{n_i} \neq p_j^{n_j}$ so $a = p_1^{n_1} x_1 \Rightarrow p_2^{n_2} | x_2 \Rightarrow a = p_1^{n_1} p_2^{n_2} x_2 \cdots \Rightarrow a = p_1^{n_1} p_2^{n_2} \cdots p_n^{n_n} x_n \in P_1 P_2 \cdots P_n$. So $P_1 P_2 \cdots P_n \subset P_1 \cap P_2 \cap \cdots \cap P_n$, $P_1 \cdots P_n = P_1 \cap \cdots \cap P_n$.

(d) For any ideal $(a) \subset R$, $(a) = P_1 P_2 \cdots P_n$ which is the product of maximal ideals. So we can express (a) as the product of $p_i' = (p_i^{s_i})$ since n is finite. $(a) = P_1' P_2' \cdots P_m' = P_1' \cap P_2' \cap \cdots \cap P_m'$.

Exercise 3.3.6. (a) If a and n are integers, $n > 0$, then there exist integers q and r such that $a = qn + r$, where $|r| \leq n/2$.

(b) The Gaussian integers $\mathbf{Z}[i]$ form a Euclidean domain with $\varphi(a + bi) = a^2 + b^2$.

Answer. (a) Trivial.

(b) For $a_1 + b_1 i$, $a_2 + b_2 i \in \mathbf{Z}[i]$

$$\begin{aligned}
\varphi(a_1 + b_1 i)(a_2 + b_2 i) &= \varphi((a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i) \\
&= (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + a_2 b_1)^2 \\
&= (a_1 a_2)^2 + (b_1 b_2)^2 + (a_1 b_2)^2 + (a_2 b_1)^2 \\
&= (a_1^2 + b_1^2)(a_2^2 + b_2^2) \\
&= \varphi(a_1 + b_1 i) \varphi(a_2 + b_2 i)
\end{aligned}$$

For any $x \in \mathbf{Z}$, and $y = a + bi \in \mathbf{Z}[i]$, from (a) $a = q_1 x + r_1$, $b = q_2 x + r_2$ with $|r_1| \leq \frac{x}{2}$, $|r_2| \leq \frac{x}{2}$. Let $q = q_1 + q_2 i$, $r = r_1 + r_2 i$, then $y = qx + r$ with $r = 0$ or $\varphi(r) = r_1^2 + r_2^2 < \varphi(x)$. $\forall x = c + di \neq 0$, take $\bar{x} = c - di$, then there are q, $r_0 \in \mathbf{Z}[i]$ such that $y\bar{x} = qx\bar{x} + r_0$ with $r_0 = 0$ or $\varphi(r_0) < \varphi(x\bar{x})$. Let $r = y - qx$, then $y = qx + r$ and $r = 0$ or $\varphi(r) < \varphi(x)$.

Exercise 3.3.7. What are the units in the ring of Gaussian integers $\mathbf{Z}[i]$?

Answer. From **Exercise 3.3.6**, we proved that $\varphi(a+bi) = a^2+b^2$ satisfies that $\forall u, v \in \mathbf{Z}[i]$, $\varphi(uv) = \varphi(u)\varphi(v)$. So if there exist $u^{-1} = c+di$ such that $uu^{-1} = 1$, then $\varphi(u)\varphi(u^{-1}) = 1$ which means $(a^2+b^2)(c^2+d^2) = 1$. So $u = \pm 1$ or $\pm i$.

Exercise 3.3.8. Let R be the following subring of the complex numbers: $R = \{a + b(1+\sqrt{19}i)/2 | a, b \in \mathbf{Z}\}$. The R is a principal ideal domain that is not a Euclidean domain.

Answer. Take $\varphi(a + b(1+\sqrt{19}i)/2) = a^2 + ab + 5b^{p2}$. Denote $\tilde{R}$ as the collection of units in R together with 0. An element $u \in R - \tilde{R}$ is called a universal side divisor if for every $x \in R$ there is some $z \in \tilde{R}$ such that u divides $x - z$ in R.

Let R be an integral domain that is not a field, if R is a Euclidean domain then there are universal side divisors in R. Since $\varphi(R) \subset \mathbf{N}$ has a lower bound, we can choose $u \in R - \tilde{R}$ such that $\varphi(u)$ minimizes. Then $\forall x = qu + r$, $r = 0$ or $\varphi(r) < \varphi(u)$ so $r \in \tilde{R}$. Hence u is a universal side divisor in R. Now we prove $R = \mathbf{Z}[(1+\sqrt{19}i)/2]$ is not a Euclidean domain by showing R contains no universal side divisor. The units in R are only ± 1 so $\tilde{R} = \{\pm 1, 0\}$. $\forall a + b(1+\sqrt{19}i)/2 \in \mathbf{Z}[(1+\sqrt{19}i)/2] \backslash \mathbf{Z}$, $\varphi(a+b(1+\sqrt{19}i)/2) = a^2 + ab + 5b^2 \geq 5$. So the smallest nonzero value of $\varphi(x)$ is 1 and 4. Take $x = 2$ in the definition of universal side divisor, u must divide 2 or 3. If $2 = ab$, then $4 = \varphi(a)\varphi(b)$ so the only divisor of 2 are ± 1, ± 2. Similarly the only divisor of 2 are ± 1, ± 3. So the value of u should be ± 2 or ± 3. Take $x = (1+\sqrt{19}i)/2$ and it's easy to check that none of x, $x \pm 1$ are divisible by ± 2, ± 3. Thus none of these is a universal side divisor.

Next we prove R is a principal ideal domain. Define φ' to be a Dedekind-Hasse norm if φ' is a positive norm and for every nonzero $a, b \in R$ either $a \in (b)$ or there exist $s, t \in R$ with $0 < \varphi'(sa - tb) < \varphi'(b)$.

For any principal ideal domain R, R has a Dedekind-Hasse norm. Let I be an nonzero ideal in R and b be a nonzero element of I with $\varphi'(b)$ minimal. Suppose a is any nonzero elements in I, so the ideal (a, b) is contained in I. Then the Dedekind-Hasse condition on φ' and the minimality of b implies that $a \in (b)$, so $I = (b)$ is principal.

We prove $R = \mathbf{Z}[(1+\sqrt{19}i)/2]$ has a Dedekind-Hasse norm φ. Suppose α, β are nonzero elements of R and $a/\beta \notin R$. We should show that there are elements $s, t \in R$ with $0 < \varphi(s\alpha - t\beta) < \varphi(\beta)$, which is equivalent to $0 < \varphi(\frac{\alpha}{\beta}s - t) < 1$. Assume $\frac{\alpha}{\beta} = \frac{a+b\sqrt{19}i}{c} \in \mathbf{Q}[\sqrt{19}i]$ with integers a, b, c having no common divisor and with $c > 1$. Since a, b, c have no common divisor there are integers x, y, z with $ax+by+ca = 1$. Write $ay-19bx = cq+r$ for some quatient q and remainder r with $|r| \leq c/2$ and let $s = y + x\sqrt{19}i$ and $t = q - z\sqrt{19}i$. Then

$$0 < \varphi(\frac{\alpha}{\beta}s - t) = \frac{(ay - 19bx - cq)^2 + 19(ax + by + cz)^2}{c^2} < \frac{1}{4} + \frac{19}{c^2}$$

so when $c \geq 5$ then condition is satisfied.
Suppose $c = 2$. Then one of a, b is even and the other is odd, and then $s = 1$ and $t = \frac{(a-1)+b\sqrt{19}i}{2}$ are elements of R satisfying the condition.
Suppose $c = 3$. The integer a^2+19b^2 is not divisible by 3. Assume $a^2+19b^2 = 3q + r$ with $r = 1$ or $r = 2$. Then $s = a - b\sqrt{19}i$ and $t = q$ satisfies the condition.
Suppose $c = 4$ so a and b are not both even. If one of a, b is even and the other is odd, then $a^2 + 19b^2$ is odd, so we can write $a^2 + 19b^2 = 4q + r$ for some $q, r \in \mathbf{Z}$ and $0 < r < 4$. Then $s = a - b\sqrt{19}i$ and $t = q$ satisfies the condition. If a and b are both odd, then $a^2 + 19b^2 \equiv 4 \mod 8$, so we have $a^2 + 19b^2 = 8q + 4$ for some $q \in \mathbf{Z}$. Then $s = (a - b\sqrt{19}i)/2$ and $t = q$ are elements in R satisfying the condition.

Exercise 3.3.9. Let R be a unique factorization domain and d a nonzero element of R. There are only a finite number of distinct principal ideals that contain the ideal (d).

Answer. Assume $d = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$. For some k satisfies that $(d) \subset (k)$, we have $k \mid d$. So $kx = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$ for $x \in \mathbf{R}$. Thus $k = p_1^{t_1} \cdots p_n^{t_n}$, where $t_i \leq s_i$, whence the choices of k are finite.

Exercise 3.3.10. If R is a unique factorization domain and $a, b \in R$ are relatively prime and $a \mid bc$, then $a \mid c$.

Answer. Assume $d = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$, $a|bc \Rightarrow ax = bc$ for some $x \in R$. a, b are relatively prime so for any prime ideal (p_i), $p_i \nmid b$, $c \in (p_i)$. Assume $p_i c_1 = c$, $p_i a_1 = a$, then $c_1 b = a_1 x$. Similarly, $c \in (p_i)$, we can continue this step so $c \in (p_i^{s_i})$. $c \in (a) = (p_1^{s_1})(p_2^{s_2}) \cdots (p_n^{s_n})$.

Exercise 3.3.11. Let R be a Euclidean ring and $a \in R$. Then a is a unit in R if and only if $\varphi(a) = \varphi(1_R)$.

Answer. If a is a unit, then $\exists a^{-1} \in R$, $aa^{-1} = 1_R$. $a = a \cdot 1_R$ so $\varphi(1_R) < \varphi(a \cdot 1_R) = \varphi(a)$, $\varphi(a) \leq \varphi(aa^{-1}) = \varphi(1_R)$ so $\varphi(a) = \varphi(1_R)$.
If $\varphi(a) = \varphi(1_R)$, $\forall x \in R\backslash\{0\}$, $x = x \cdot 1_R$ so $\varphi(x) \geq \varphi(1_R)$. Assume $1_R = qa + r$, $\varphi(r) \geq \varphi(a)$ for all $r \in R\backslash\{0\}$. So $r = 0$, $1_R = qa$, a is a unit.

Exercise 3.3.12. Every nonempty set of elements (possibly infinite) in a commutative principal ideal ring with identity has a greatest common divisor.

Answer. Denote $S = \{(a) | \bigcup_{i \in I} (a_i) \subset (a)\}$. S is nonempty since $R \in S$. For finite I, the conclusion is trivial. For infinite I. Assume $(d) = \bigcap_{A \in S} A$ which is a well defined ideal. $\bigcap_{i \in I} (a_i) \subset (d)$ so $(a_i) \subset (d) \Rightarrow d \mid a_i$ for all $i \in I$. And $\forall c \mid a_i$ for all $i \in I$, $(c) \subset S$ so $(d) \subset (c)$, $c \mid d$. d is the greatest common divisor of $\{a_i | i \in I\}$.

Exercise 3.3.13. Let R be a Euclidean domain with associated function $\varphi : R - \{0\} \to \mathbf{N}$. If $a, b \in R$ and $b \neq 0$, here is a method for finding the greatest common divisor of a and b. By repeated use of Definition 3.8(ii) we have:

$$\begin{gathered}
a = q_0 b + r_1, \quad \text{with} \quad r_1 = 0 \quad \text{or} \quad \varphi(r_1) < \varphi(b); \\
b = q_1 r_1 + r_2, \quad \text{with} \quad r_2 = 0 \quad \text{or} \quad \varphi(r_2) < \varphi(1); \\
r_1 = q_2 r_2 + r_3, \quad \text{with} \quad r_3 = 0 \quad \text{or} \quad \varphi(r_3) < \varphi(2); \\
\vdots \\
r_k = q_{k+1} r_{k+1} + r_{k+2}, \quad \text{with} \quad r_{k+2} = 0 \quad \text{or} \quad \varphi(r_{k+2}) < \varphi(k+1); \\
\vdots
\end{gathered}$$

Let $r_0 = b$ and let n be the least integer such that $r_{n+1} = 0$ (such an n exists since the $\varphi(r_k)$ form a strictly decreasing squence of nonnegative integers). Show that r_n is the greatest common divisor a and b.

Answer. $r_n$exists since $\varphi(r_i)$ decreases. $r_n \mid a$ and $r_n \mid b$ is simple. We prove $(a)+(b)=(r_n)$. $r_n \mid a$, $r_n \mid b$ so $(a) \subset (r_n)$, $(b) \subset (r_n) \Rightarrow (a)+(b) \subset (r_n)$. We use induction to prove $(r_n) \subset (a)+(b)$: 1. For $i=1$, $a=q_0b+r \Rightarrow r_1=a-q_0b \in (a)+(b)$. 2. Assume for $i \leq m$, $(r_i) \subset (a)+(b)$, $r_{m-1}=q_mr_m+r_{m-1} \Rightarrow r_{m+1}=r_{m-1}-q_mr_m \in (r_m)+(r_{m-1}) \subset (a)+(b)$. So $(r_n) \subset (a)+(b)$. r_n is the greatest common divisor of a and b.

3.4 Rings of quotients and localization

Exercise 3.4.1. Determine the complete ring of quotients of the ring Z_n for each $n \geq 2$.

Answer. For the complete multiplicative subset S of Z_n, $S = \{\bar{x} | (x, n) = 1\}$ so the complete ring of quotient is $S^{-1}Z_n$.

Exercise 3.4.2. Let S be a multiplicative subset of a commutative ring R with identity and let T be a multiplicative subset of the ring $S^{-1}R$. Let $S_* = \{r \in R | r/s \in T \text{ for some } s \in S\}$. Then S_* is a multiplicative subset of R and there is a ring isomorphism $S_*^{-1}R \cong T^{-1}(S^{-1}R)$.

Answer. For any r_1/s_1 , $r_2/s_2 \in T$. $r_1r_2/s_1s_2 \in T$. And there exists a monomorphism $\varphi : S_* \to T$ given by $\varphi : r \mapsto r/s$ for some $s \in S$ by the definition of S_*. So $\forall r_1, r_2 \in S_*$, $\exists \varphi(r_1)\varphi(r_2) = r_1r_2/s_1s_2 \in T$, thus $r_1r_2 \in S_*$. S_* is a multiplicative subset.
Next we prove $S_*^{-1}R \cong T^{-1}(S^{-1}R)$. $\forall s \in S_*$ and $r \in R$, $sr \in S_*$ since if there exists some $s' \in S$, $s/s' \in T$ then $sr/s'r = s/s' \in T$. For any $(r/s)/(r'/s') \in T^{-1}(S^{-1}R)$ where $r \in R$ and $s \in S$, $r'/s' \in T$, we construct a map $\varphi : T^{-1}(S^{-1}R) \to S_*^{-1}R$ given by $\varphi : (r/s)/(r'/s') \mapsto rs'/sr'$. φ is well defined since $rs' \in R$ and $sr' \in S_*$. Now we check φ is an isomorphism. $\forall (r_1/s_1)/(r_1'/s_1'), (r_2/s_2)/(r_2'/s_2') \in T^{-1}(S^{-1}R)$

$$\begin{aligned}
&\varphi((r_1/s_1)/(r_1'/s_1') + (r_2/s_2)/(r_2'/s_2'))\\
=&\varphi(((r_1/s_1)(r_2'/s_2') + (r_2/s_2)(r_1'/s_1'))/((r_1'/s_1')/(r_2'/s_{2'})))\\
=&\varphi((r_1r_2'/s_1s_2' + r_2r_1'/s_2s_1')/(r_1'r_2'/s_1's_2'))\\
=&\varphi(((r_1r_2's_2s_1' + r_2r_1's_1s_2')/s_1s_2s_1's_2')/(r_1'r_2'/s_1's_2'))\\
=&(((r_1r_2's_2s_1' + r_2r_1's_1s_2')s_1's_2')/s_1s_2s_1's_2'r_1'r_2')\\
=&((r_1r_2's_2s_1' + r_2r_1's_1s_2')/s_1s_2r_1'r_2')\\
=&(r_1s_1')/(r_1's_1) + (r_2s_2')/(r_2's_2)\\
=&\varphi((r_1/s_1)/(r_1'/s_1/)) + \varphi((r_2/s_2)/(r_1'/s_2'))
\end{aligned}$$

The conservation of multiplication is trivial. φ is a homomorphism and φ is obviously injective, so $\left|T^{-1}(S^{-1}R)\right| \leq \left|S^{-1}R\right|$.
Take $\tau : S_*^{-1}R \to T^{-1}(S^{-1}R)$ given by $\tau : r/s \mapsto (r/s')/(s/s')$. Similarly, τ is injective so $|S_*R| \leq \left|T^{-1}(S^{-1}R)\right|$. φ is isomorphism and $S_*^{-1}R \cong T^{-1}(S^{-1}R)$.

Exercise 3.4.3. (a) The set E of positive even integers is a multiplicative subset of $\mathbf{Z}$ such that $E^{-1}(\mathbf{Z})$ is field of rational numbers.

(b) State and prove condition(s) on a multiplicative subset of S of $\mathbf{Z}$ which insure that $S^{-1}\mathbf{Z}$ is a field of rationals.

Answer. (a) Trivial.

(b) Assume the primes $p \in \mathbf{Z}$ forms a set P. For any multiplicative subset S and $x \in S$ then $\{x^n | n \in \mathbf{Z}\} \subset S$. If $\forall p \in P$, $\exists x \in S$ such that $p \mid x$, we prove $S^{-1}\mathbf{Z}$ forms the field of rationals. For any $p/q \in \mathbf{Q}$, $q = q_1^{t_1} q_2^{t_2} \cdots q_n^{t_n}$ and for any q_i there exists $x_1 \in S$, $x_1 = a_i q_i$. Take $x = a_1^{t_1} q_1^{t_1} \cdots a_n^{t_n} q_n^{t_n}$ and $y = a_1^{t_1} \cdots a_n^{t_n} p$. Then $y/x = p/q$, $y/x \in S^{-1}\mathbf{Z}$. So $S^{-1}\mathbf{Z}$ forms the field of rationals.

For any other multiplicative subset S, assume $p \in P$ and $\forall x \in S$, $p \nmid x$ then $\forall y/x \in S^{-1}\mathbf{Z}$, $yp - x \neq 0$ so $1/p \notin S^{-1}\mathbf{Z}$, $S^{-1}\mathbf{Z}$ isn't the rational field.

Exercise 3.4.4. If $S = \{2, 4\}$ and $R = Z_6$, then $S^{-1}R$ is isomorphic to the field Z_3. Consequently, the converse of Theorem 4.3(ii) is false.

Answer. $S^{-1}Z_6 = \{1/3, 2/3, 3/3\}$ so $S^{-1}Z_6 \cong Z_3$ is a integral domain. However, Z_6 has no zero divisor.

Exercise 3.4.5. Let R be an integral domain with quotient field F. If T is an integral domain such that $R \subset T \subset F$, then F is (isomorphic to) the quotient field of T.

Answer. Consider T_i which is a PID satisfying $R \subset T_i \subset F$, T_i forms a category with the inclusion map as morphisms. T_i' is the quotient field of T_i so $R \subset T_i' \Rightarrow R \subset F \subset T_i'$ (up to isomorphic). $R \subset T_j \subset F \subset T_i'$ for all i, j thus $T_i' \subset T_j'$. Similarly $T_j' \subset T_i'$ so all the T_i' are universal under the inclusion map. Thus F is isomorphic to the quotient field of T.

Exercise 3.4.6. Let S be a multiplicative subset of an integral domain R such that $0 \notin S$. If R is a principal ideal domain, then so is $S^{-1}R$.

Answer. Actually this is true if and only if $1_R \in S$. For any ideal $J \subset S^{-1}R$, there exists ideal $I \subset R$ and $\varphi_S(I) = J$, $J = S^{-1}I = S^{-1}(a)$ for some $a \in R$. Since $1_R \in S$, $a/1_R \in S^{-1}(a)$. So $\forall s \in S$, $1_R/s$ is a unit of $S^{-1}(a)$, so $S^{-1}(a) = (a/1_R)$ is a principal ideal. Thus the multiplicative subset of R is a principal ideal domain.

Exercise 3.4.7. Let R_1 and R_2 be integral domains with quotient fields F_1 and F_2 respectively. If $f : R_1 \to R_2$ is an isomorphism, then f extends to an isomorphism $F_1 \cong F_2$.

Answer. For $f : R_1 \to R_2$, and the inclusion map $\subset R_2 \to F_2$, $\subset \circ f = R_1 \to F_2$ so there exists $\subset \bar{} \circ f : F_1 \to F_2$ which is a well defined homomorphism of rings. $\subset \bar{} \circ f|R_1 = f$, $\subset \bar{} \circ f$ is a monomorphism so $|F_1| \leq |F_2|$. Similarly, $|F_2| \leq |F_1|$ so $\subset \bar{} \circ f$ is an isomorphism and $F_1 \cong F_2$.

Exercise 3.4.8. Let R be a commutative ring with identity, I an ideal of R and $\pi : R \to R/I$ the canonical projection.

(a) If S is a multiplicative subset of R, then $\pi S = \pi(S)$ is a multiplicative subset of R/I.

(b) The mapping $\theta : S^{-1}R \to (\pi S)^{-1}(R/I)$ given by $r/s \mapsto \pi(r)/\pi(s)$ is a well-defined function.

(c) θ is a ring epimorphism with kernel $S^{-1}I$ and hence induces a ring isomorphism $S^{-1}R/S^{-1}I \cong (\pi S)^{-1}(R/I)$.

Answer. (a) For any $a, b \in S$, $\pi(a) = a + I$, $\pi(b) = b + I$, $\pi(a)\pi(b) = ab + I = \pi(ab) \in \pi S$, so πS is a multiplicative subset of R/I.

(b) If $r_1/s_1 = r_2/s_2$ then $x(r_1s_2 - r_2s_1) = 0$ for some $x \in S$.

$$\theta(r_1/s_1) = \pi(r_1)/\pi(s_1) = (r_1 + I)/(s_1 + I)$$

$$\theta(r_2/s_2) = \pi(r_2)/\pi(s_2) = (r_2 + I)/(s_2 + I)$$

$$\begin{aligned}&(x + I)((r_1 + I)(s_2 + I) - (r_2 + I)(s_1 + I))\\ =&(xr_1s_2 + I) - (xr_2s_1 + I)\\ =&x(r_1s_2 - r_2s_1) + I\\ =&I\end{aligned}$$

so $\theta(r_1/s_1) = \theta(r_2/s_2)$, θ is well-defined.

(c) π is a homomorphism and so is θ. θ is obviously an epimorphism and $\forall r/s \in S^{-1}I$, $\theta(r/s) = \pi(r)/\pi(s)$. $\pi(r) = I$ so $\theta(r/s) \in (\pi S)^{-1}I$, $S^{-1}I \subset \text{Ker}\theta$. For any $r/s \notin S^{-1}I$, $\theta(r/s) = (r+I)/(s+I) \neq I$, so $\text{Ker}\theta \subset S^{-1}I$. $\text{Ker}\theta = S^{-1}I$, $S^{-1}R/\text{Ker}\theta \cong \text{Im}\theta \Rightarrow S^{-1}R/S^{-1}I \cong (\pi S)^{-1}(R/I)$.

Exercise 3.4.9. Let S be a multiplicative subset of a commutative ring R with identity. If I is an ideal in R, then $S^{-1}(\text{Rad}I) = \text{Rad}(S^{-1}I)$.

Answer. $\text{Rad}I = \{r | r^n \in I \text{ for some } n\}$. For any $r/s \in S^{-1}\text{Rad}I$, $(r/s)^n = r^n/s^n \in S^{-1}I$ so $S^{-1}\text{Rad}I \subset \text{Rad}(S^{-1}I)$.
For any $a/b \in \text{Rad}(S^{-1}I)$, $b \in S$ then $a^n b' - b^n a' = 0$ with $a' \in I$ and $b' \in S$. $(ab')^n = (b')^{n-1} b^n a' \in I$ so $a/b = ab'/bb' \in S^{-1}(\text{Rad}I)$. Thus $S^{-1}(\text{Rad}I) \subset \text{Rad}(S^{-1}I)$. So $S^{-1}(\text{Rad}I) = \text{Rad}(S^{-1}I)$.

Exercise 3.4.10. Let R be an integral domain and for each maximal ideal M, consider R_M as a subring of the quotient field of R. Show that $\cap R_M = R$, where the intersection is taken over all maximal ideals M of R.

Answer. M is maximal so $1_R \in R - M$, which means $R \subset R_M$ for any M. So $R \subset \cap R_M$.
Denote R' as the quotient field of R. For any M maximal, $R_M \subset R'$. For any $x \in R' - R$, we prove there exists M maximal and $x \notin R_M$. Take $A = \{a | ax \in R\}$, A is an ideal of R. So $\exists A \subset M$ with M maximal. If $x \in R - M$, $x = r/s$, so $xs = r \in R$, $s \in I \subset M$. That's contradictory! Thus $\cap R_M \subset R$, $R = \cap R_M$.

Exercise 3.4.11. Let p be a prime in $\mathbf{Z}$l then (p) is a prime ideal. What can be said about the relationship of Z_p and the localization $Z_{(p)}$?

Answer. Z_p can be embedded into $\mathbf{Z}_{(p)}$ since $Z_p \subset \mathbf{Z} \subset (p)_{(p)} \subset \mathbf{Z}_{(p)}$.

Exercise 3.4.12. A commutative ring with identity is local if and only if for all $r, s \in R$, $r + s = 1_R$ implies r or s is a unit.

Answer. If R is local, $r + s = 1_R \Rightarrow (r) + (s) = R$. R has unique maximal ideal M so $(r) \subset M$, $(s) \subset M$, $(r) + (s) = R \subset M$. That's contradictory! So $(r) = R$ or $(s) = R$, r or s is a unit.
Conversely, if there exist M_1, M_2 are maximal ideals. $M_1 + M_2 = R$ so $\exists r \in M$, $s \in M_2$ such that $r + s = 1_R$. WLOG assume r is unit, $R = (r) \subset M_1$, that's contradictory! So R is local.

Exercise 3.4.13. The ring R consisting of all rational numbers with denominators not divisible by some (fixed) prime p is a local ring.

Answer. Denote the set of primes in the question as P. Then (P) is a prime ideal in $\mathbf{Z}$. So $S = \mathbf{Z} = (P)$ is multiplicative subset. We prove $R = \mathbf{Z}_{(P)}$. $\forall r/s \in \mathbf{Z}_{(p)}$, $r \in \mathbf{Z}$ and $s \notin (P)$ so $r/s \in R$. Thus $\mathbf{Z}_{(P)} \subset R$. Conversely, $\forall r/s \in R$, suppose $s = p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n}$, $\forall p \in P$, $p \nmid s$ so $(p_i) \not\subset$ for all $i = 1, 2, \ldots, n$. Thus $(p_i) \subset S$ so $s \in S$, $r/s \in \mathbf{Z}_{(P)}$. $\mathbf{Z}_{(P)} = R$ is a lcoal ring.

Exercise 3.4.14. If M is a maximal ideal in a commutative ring R with identity and n is a positive integer, then the ring R/M^n has a unique prime ideal and therefore is local.

Answer. Consider the homomorphism $f : R \to R/M^n$. For any prime ideal $I \subset R/M^n$, $J = f^{-1}(I)$ is a prime ideal contains M^n. $M^n \subset P \Rightarrow M \subset P$, since M is maximal, $P = M$ so the only prime ideal in R/M^n is R/M.

Exercise 3.4.15. In a commutative ring R with identity the following conditionns are equivalent: (i) R has a unique prime ideal; (ii) every nonunit is nilpotent; (iii) R has a minimal prime ideal which contains all zero divisors, and all nonunits of R are zero divisors.

Answer. We first prove a lemma:

Lemma. *For an ideal $I \subset R$,* $\mathrm{Rad} I = \bigcap\limits_{I \subset P_i} P_i$ *where P_i are prime ideals.*

Proof of the lemma: $\forall a \in \mathrm{Rad} I$, $a^n \in I$ for some n, so $\forall I \subset P_i$ with P_i prime. $a^n \in P_i \Rightarrow a \in P_i$ so $\mathrm{Rad} I \subset \bigcap\limits_{I \subset P_i} P_i$.

Conversely $\forall a \notin \mathrm{Rad} I$, we only need to find $I \subset P_i$ and $a \notin P_i$. Take $A = \{J | a^n \in J \, \forall n \in \mathbf{N}\}$. A has maximal element under $\subset$ by Zorn's lemma. Denote the maximal element as P. $\forall x, y \in R$ and $x \notin P$, $y \notin P$. Then $\exists m, n \in \mathbf{N}$, $a^n \in (x) + P$, $a^m \in (y) + P$, so $a^{m+n} \in (xy) + P \Rightarrow xy \notin P$. Thus P is prime. That's contradictory! So $\bigcap\limits_{I \in P_i} P_i \subset \mathrm{Rad} I$. The lemma has been proved.

(i)$\Rightarrow$(ii): $0 \in P$ where P is the unique prime ideal, so $P = \{a | a^n = 0 \text{ for some } n\}$. For any nonunit a, $(a) \subset M = P$ so $a \in P$, there exists $n \in \mathbf{N}$ such that $a^n = 0$.

(ii)$\Rightarrow$(i): Denote N as the ideal contains all the nilpotent elements. Take $\varphi : R \to R/N$. For any unit u, $\varphi(u)$ is also a unit. So R/N is a field, N is maximal in R. For any prime ideal P, $N \subset P$ from the lemma. Thus N is the only prime ideal.

(ii)$\Rightarrow$(iii): Denote N as the ideal contains all the nilpotent elements. All nilpotent elements are zero divisors by the definition. N is prime and minimal is the direct corollary of the lemma.

(iii)$\Rightarrow$(ii): Denote I as the minimal prime ideal and N as the ideal contains all the nilpotent elements. Then $N \subset I$. Since all then nonunits are zero divisors, we have N itself a prime ideal. So $N = I$.

Exercise 3.4.16. Every nonzero homomorphic image of a local ring is local.

Answer. Suppse L is a local ring and $\varphi : L \to R$ is a ring of rings. Then φ is an one-to-one correspondence between ideals in L and ideals in R. For the maximal ideal M in L, $\varphi(M) \subsetneq R$, so $\varphi(M)$ contains all the proper ideals in R. R is a local ring.

3.5 Rings of polynomials and formal power series

Exercise 3.5.1. (a) If $\varphi : R \to S$ is a homomorphism of rings, then the map $\bar{\varphi} : R[[x]] \to S[[x]]$ given by $\bar{\varphi}(\sum a_i x^i) = \sum \varphi(a_i)x^i$ is a homomorphism of rings such that $\bar{\varphi}(R[x]) \subset S[x]$.

(b) $\bar{\varphi}$ is a monomorphism if and only if $u\varphi$ is. In this case $\bar{\varphi} : R[x] \to S[x]$ is also a monomorphism.

(c) Extend the results of (a) and (b) to the polynomial rings $R[x_1, \dots, x_n]$, $S[x_1, \dots, x_n]$.

Answer. (a) It's easy to show $\bar{\varphi}(\sum a_i x^i)\bar{\varphi}(\sum b_i x^i) = \bar{\varphi}(\sum c_i)x^i$, $c_n = \sum\limits_{j=0}^{n} a_j b_{n-j}$ and $\bar{\varphi}(\sum a_i x^i) + \bar{\varphi}(\sum b_i x^i) = \bar{\varphi}(\sum(a_i + b_b)x^i)$. $\forall f(x) = \sum\limits_{i=0}^{n} a_i x^i \in R[x]$, $\bar{\varphi}(f(x)) = \bar{\varphi}(\sum\limits_{i=0}^{n} a_i x^i) = \sum\limits_{i=0}^{n} \varphi(a_i)x^i \in S[x]$. So $\bar{\varphi}(R[x]) \subset S[x]$.

(b) If φ is monomorphism [epimorphism], it's easy to show that $\bar{\varphi}$ is also monomorphism [epimorphism].

Conversely, if $\bar{\varphi}$ is monomorphism, take $a_i \in R[[x]]$, then $\bar{\varphi}(a_i) = \varphi(a_i)$, φ is also a monomorphism.

Similarly, φ is epimorphism if $\bar{\varphi}$ is.

(c) It's trivial to since $R[x] \subset R[[x]]$, $S[x] \subset S[[x]]$.

Exercise 3.5.2. Let $\mathrm{Mat}_n R$ be the ring of $n \times n$ matrices over a ring R. Then for each $n \geq 1$:

(a) $(\mathrm{Mat}_n R)[x] \cong \mathrm{Mat}_n R[x]$.

(b) $(\mathrm{Mat}_n R)[[x]] \cong \mathrm{Mat}_n R[[x]]$.

Answer. (a) Take $x = (p_{ij}(x)) \in \mathrm{Mat}_n R[x]$, $p_{ij}(x) = \sum\limits_{k=0}^{n_{ij}} a_{ijk}x^k$. Take $n = \max\limits_{0<i,j\leq n} n_{ij}$, and for those $n \geq k > n_{ij}$, take $a_{ijk} = 0$. Denote $X_k = (a_{ijk})$, $x' = \sum\limits_{i=0}^{n} X_i x^i \in (\mathrm{Mat}_n R)[x]$. We prove $\varphi : x \mapsto x'$ is an isomorphism between rings.

For $x, x' \in \mathrm{Mat}_n R[x]$, $x = (p_{ij}(x))$, $x' = (p'_{ij}(x))$, $p_{ij}(x) = \sum\limits_{k=0}^{n_{ij}} a_{ijk}x^k$,

$p'_{ij}(x) = \sum\limits_{k=0}^{n_{ij}} a'_{ijk}x^k$.

$$\begin{aligned}
\varphi(x+x') &= \varphi(p_{ij}(x) + p'_{ij}(x)) \\
&= \begin{pmatrix} a_{110}+a'_{110} & \cdots & \\ \vdots & \ddots & \\ & & a_{nn0}+a'_{nn0} \end{pmatrix} \\
&+ \begin{pmatrix} a_{111}+a'_{111} & \cdots & \\ \vdots & \ddots & \\ & & a_{nn1}+a'_{nn1} \end{pmatrix} x + \cdots \\
&= \varphi(x) + \varphi(x')
\end{aligned}$$

$$\varphi(xx') = \varphi((p_{ij}(x))(p'_{ij}(x))) = \varphi((\sum_{k=1}^{n} p_{ik}(x)p'_{kj}(x)))$$

$$\begin{aligned}
\sum_{k=1}^{n} p_{ik}(x)p'_{kj}(x) &= \sum_{k=1}^{n}(\sum_{m=0}^{n_{ik}} a_{ikm}x^m)(\sum_{m=0}^{n'_{kj}} a'_{kjm}x^m) \\
&= \sum_{w}\sum_{k=1}^{n}\sum_{m=1}^{w} a_{ikm}a'_{kj(w-m)}x^w
\end{aligned}$$

so

$$\begin{aligned}
\varphi(xx') &= \varphi((\sum_{w}\sum_{k=1}^{n}\sum_{m=1}^{w} a_{ikm}a'_{kj(w-m)}x^w)) \\
&= \sum_{w}(\sum_{k=1}^{n}\sum_{m=1}^{w} a_{ikm}a_{kj(w-m)})x^w \\
\varphi(x)\varphi(x') &= (\sum_{w}(a_{ijw})x^w)(\sum_{w}(a'_{ijw})x^w) \\
&= \sum_{w}(\sum_{k=1}^{n}\sum_{m=1}^{w} a_{ikm}a_{kj(w-m)})x^w
\end{aligned}$$

so $\varphi(xx') = \varphi(x)\varphi(x')$, φ is a well defined homomorphism. Ker$\varphi = 0$ so φ is a monomorphism. For any $\sum\limits_{w}(a_{ijw})x^w \in \mathrm{Mar}_n R[x]$, $\exists(\sum\limits_{w} a_{ijw}x^w) \in (\mathrm{Mat}_n R)[x]$ s.t. $\varphi(\sum\limits_{w} a_{ijw}x^w = \sum\limits_{w}(a_{ijw})x^w)$. So φ is an epimorphism.

Exercise 3.5.3. Let R be a ring and G an infinte multiplicative cyclic group with generator denoted x. Is the group ring $R(G)$ isomorphic to the polynomial ring in one indeterminate over R?

Answer. $R(G)$ is not isomorphic to $R[x]$ since there's no isomorphic image of $rx^{-1} \in R(G)$ in $R[x]$.

Exercise 3.5.4. (a) Let S be a nonempty set and let N^S be the set of all functions $\varphi : S \to \mathbf{N}$ such that $\varphi(s) \neq 0$ for at most a finite number of elements $s \in S$. Then $\mathbf{N}^S$ is a multiplicative abelian monoid with prooduct defined by

$$(\varphi\psi)(s) = \varphi(s) + \psi(s)\, (\varphi, \psi \in \mathbf{N}^S; s \in S)$$

The identity element in $\mathbf{N}^S$ is the zero function.

(b) For each $x \in S$ and $i \in \mathbf{N}$ let $x^i \in \mathbf{N}^S$ be defined by $x^i(x) = i$ and $x^i(s) = 0$ for $s \neq x$. If $\varphi \in \mathbf{N}^S$ and $x_1, \ldots, x_n$ are the only elements of S such that $\varphi(x_i) \neq 0$, then in $\mathbf{N}^S$, $\varphi = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$, where $i_j = \varphi(x_j)$.

(c) If R is a ring with identity let $R[S]$ be the set of all functions $f : \mathbf{N}^S \to R$ such that $f(\varphi) \neq 0$ for at most a finite number of $\varphi \in \mathbf{N}^S$. Then $R[S]$ is a ring with identity, where addition and multiplication are defined as follows:

$$(f+g)(\varphi) = f(\varphi) + g(\varphi)\, (f, g \in R[S]; \varphi \in \mathbf{N}^S)$$

$$(fg)(\varphi) = \sum f(\theta)g(\zeta)\, (f, g \in R[S]; \theta, \zeta, \varphi \in \mathbf{N}^S)$$

where teh sum is over all pairs (θ, ζ) such that $\theta\zeta = \varphi$. $R[S]$ is called the ring of polynomials in S over R.

(d) For each $\varphi = x_1^{i_1} \cdots x_n^{i_n} \in \mathbf{N}^S$ and each $r \in R$ we denote by $rx_1^{i_1} \cdots x_n^{i_n}$ the function $\mathbf{N}^S \to R$ which is r at φ and 0 elsewhere. Then every nonzero element f of $R[S]$ can be written in the form $\int = \sum\limits_{i=0}^{m} r_i x_1^{k_{i1}} x_2^{k_{i2}} \cdots x_n^{k_{in}}$ with the $r_i \in R$, $x_i \in S$ and $k_{ij} \in \mathbf{N}$ all uniquely determined.

(e) If S is finite of cardinality n, then $R[S] \cong R[x_1, \ldots, x_n]$.

(f) State and prove an analogue of Theorem 5.5 for $R[S]$.

Answer. (a) $\varphi\psi = \varphi + \psi : S \to \mathbf{N}$ so $\varphi\psi \in \mathbf{N}^S$. For any $\varphi \in \mathbf{N}^S$, $\varphi 0 = 0\varphi = \varphi + 0 = 0 + \varphi = \varphi$. So $\mathbf{N}^S$ is a monoid.

(b) For any $\varphi \in \mathbf{N}^S$, $x_1, x_2, \ldots, x_n$ are the only element s.t. $\varphi(x_i) \neq 0$. We prove it has the form $\varphi = x_1^{i_1} \cdots x_n^{i_n}$. Suppose $\varphi(x_j) = i_j$. Take $\varphi_1 = \varphi - x_n$ then $x_1, x_2, \ldots, x_{n-1}$ are the only element s.t. $\varphi_1(x_i) \neq 0$. Continue this step, we can have $\varphi_{n-1} = x_i^{i_1}$ and $\varphi_n = 0$. Thus $\varphi = x_1^{i_1} + \cdots + x_n^{i_n} = x_1^{i_1} \cdots x_n^{i_n}$.

(c) $f + g(\varphi) = f(\varphi) + g(\varphi)$, $f + g : \mathbf{N}^S \to R$ and for at most finite $\varphi \in \mathbf{N}^S$, $f(\varphi) \neq 0$, so $f + g \in \mathbf{N}^S$.

$(fg)(\varphi) = \sum f(\theta)g(\zeta)$, so $fg\mathbf{N}^S \to R$. Suppose $\mathbf{N}_f^S$, $\mathbf{N}_g^S$ are the set such that $f(\mathbf{N}_f^S) = 0$, $g(\mathbf{N}_g^S) = 0$. Take $\mathbf{N}_{fg}^S = \mathbf{N}_f^S \cup \mathbf{N}_g^S$, then $\mathbf{N}_{fg}^S$ is also finite. For all $\theta, \zeta \notin \mathbf{N}_{fg}^S$, $(fg)(\varphi) = 0$. So $fg \in R[S]$.

Take the 0 element of f in $R[S]$ as $0(\varphi) = 0_R$ for any $\varphi \in \mathbf{N}^S$ and the inverse element of f in $R[S]$ as $f^{-1}(\varphi) = -f(\varphi)$ for any $\varphi \in \mathbf{N}^S$. Thus $R[S]$ is a ring.

(d) The proof is similar to (b).

(e) First we prove $\mathbf{N}^S \cong \mathbf{N}^n$. Assume $S = \{x_1, x_2, \ldots, x_n\}$. We can write every $\varphi \in \mathbf{N}^S$ into $x_{n_1}^{i_{n_1}} \cdots x_{n_m}^{i_{n_m}}$ and extend it to $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ by taking $i_j = 0$ if $j \neq n_1, n_2, \ldots, n_m$. Then the map $\sigma : \mathbf{N}^S \to \mathbf{N}^n$ given by $\sigma : x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \mapsto (i_1, i_2, \ldots, i_n)$ is a well defined isomorphism so $\mathbf{N}^S \cong \mathbf{N}^n$.

For any $f \in R[x_1, x_2, \ldots, x_n]$. f can be expressed as $f = \sum a_{k_1 k_2 \cdots k_n} x_1^{k_1} \cdots x_n^{k_n}$. Take $\tau : R[x_1, x_2, \ldots, x_n] \to R[S]$ given by $\tau : f \mapsto \sum a_{k_1 \cdots k_n} \sigma^{-1}(k_1, k_2, \ldots, k_n)$. It's easy to show that τ is an isomorphism.

(f) Let R and X be commutative rings with identity and $\varphi : R \to X$ a homomorphism of rings such that $\varphi(1_R) = 1_X$. If $x_1, x_2, \ldots, x_n \in S$, there is a unique homomorphism of rings $\bar{\varphi} : R[S] \to X$ such that $\bar{\varphi}|R = \varphi$, $|S| = n$ and $\varphi(s_i) = x_i$ for $i = 1, 2, \ldots, n$. The proof is quite simple since there exists $\tau : R[x_1, \ldots, x_n] \to R[S]$ an isomorphism.

Exercise 3.5.5. Let R and S be rings with identity, $\varphi : R \to S$ a homomorphism of rings with $\varphi(1_R) = 1_S$, and $s_1, s_2, \ldots, s_n \in S$ such that $s_i s_j = s_j s_i$ for all i, j and $\varphi(r)s_i = s_i\varphi(r)$ for all $r \in R$ and all i. Then there is a unique homomorphism $\bar{\varphi} : R[x_1, \ldots, x_n] \to S$ such that $\bar{\varphi}|R = \varphi$ and $\varphi(\bar{x_i}) = s_i$. This property completely determines $R[x_1, \ldots, x_n]$ up to isomorphism.

Answer. $S' = \langle \varphi(R) \cup \{s_1, s_2, \ldots, s_n\} \rangle$ is a commutative ring. So applying Theorem 5.5. on S', we can get the unique homomorphism $\bar{\varphi}$:

$R[xt_1, x_2, \ldots, x_n] \to S'$, so $\bar{\varphi} : R[x_1, \ldots, x_n] \to S$ is also a homomorphism. The proof of the second statement is exactly the same as Theorem 5.5.

Exercise 3.5.6. (a) If R is the ring of all 2×2 matrices over $\mathbf{Z}$, then for any $A \in R$,

$$(x + A)(x - A) = x^2 - A^2 \in R[x]$$

(b) There exist $C, A \in R$ such that $(C + A)(C - A) \neq C^2 - A^2$. Therefore, Corollary 5.6 is false if the rings involved are not commutative.

Answer. (a) For any $A \in R$, $x + A$, $x - A$, $(x + A)(x - A)$, $x^2 - A^2 \in R[x]$. $(x + A)(x - A) = x^2 + Ax - xA + A^2$. Since $Ax = xA$, $(x + A)(A + x) = x^2 - A^2$.

(b) Take $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, then $CA = \begin{pmatrix} 1 & 1 \\ 3 & 3 \end{pmatrix}$, $AC = \begin{pmatrix} 3 & 1 \\ 3 & 1 \end{pmatrix}$. So $AC \neq CA$, $(C + A)(C - A) \neq C^2 - A^2$. Corollary 5.6 is false in R.

Exercise 3.5.7. If R is a commutative ring with identity and $f = a_n x^n + \cdots + a_0$ is a zero divisor in $R[x]$, then there exists a nonzero $b \in R$ such that $ba_n = ba_{n-1} = \cdots = ba_0 = 0$.

Answer. Assume $g = b_m x^m + \cdots + b_0$ and $fg = 0$, $fg = a_n b_m x^{m+n} + (a_n b_{m-1} + a_{n-1} b_m) x^{m+n-1} + \cdots + a_0 b_0 = 0$. So for any $k = 0, 1, \ldots, m + n$, $\sum\limits_{i+j=k} a_i b_j = 0$. Take $b'_1 = b_n$, and then $a_n b'_1 = 0$, $a_n b_{m-1} + a_{n-1} b_m = 0 \Rightarrow a_n b_{m-1} b'_1 + a_{n-1} b_m b'_1 = 0$. Take $b_2 = b_m b'_1$, we have $a_n b'_2 = a_{n-1} b'_2 = 0$. $a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m = 0$, take $b'_3 = b_m b'_1$, we have $a_m b'_3 = a_{n-1} b'_3 = a_n b'_3 = 0$. Continue this step and we have $a_n b'_n = a_{n-1} b'_n = \cdots = a_0 b'_n = 0$. That's the b we want.

Exercise 3.5.8. (a) The polynomial $x + 1$ is a unit in the power series ring $\mathbf{Z}[[x]]$, but is not a unit in $\mathbf{Z}[x]$.

(b) $x^2 + 3x + 2$ is irreducible in $\mathbf{Z}[[x]]$, but not in $\mathbf{Z}[x]$.

Answer. (a) Take $(x+1)^{-1} = 1 - x + x^2 - x^3 + \cdots \in \mathbf{Z}[[x]]$. $(1 - x + x^2 - x^3 + \cdots)(x+1) = (x+1)(1 - x + x^2 - x^3 + \cdots) = (1 - x + x^2 - x^3 + \cdots) + (x - x^2 + x^3 - \cdots) = 1$. So $x+1$ is a unit in $\mathbf{Z}[[x]]$. For any $f = \sum\limits_{i=0}^{n} a_i x^i \in \mathbf{Z}[x]$, $(x+1)f = a_n x^{n+1} + \sum\limits_{i=1}^{n}(a_i + a_{i-1})x^i + a_0$, $a_n \neq 0$ so $(x+1)f \neq 1$. $x+1$ is not a unit.

(b) $x^2+3x+2 = (x+2)(x+1)$ and $x+2, x+1 \in \mathbf{Z}[x]$, so x^2+3x+2 is not irreducible in $\mathbf{Z}[x]$. x^2+3x+2 itself is a unit in $\mathbf{Z}[x]$ so if $x^2+3x+2 = ab$, a,b must be units. Thus x^2+3x+2 is irreducible in $\mathbf{Z}[[x]]$.

Exercise 3.5.9. If F is a field, then (x) is a maximal ideal in $F[x]$, but it is not the only maximal ideal.

Answer. Suppose not. $(x) \subset I \subset F[x]$ with $I \neq F[x]$. (x) contains all polynomials which have zero constant term. For any $p(x) = \sum\limits_{i=0}^{n} a_i x^i \in I$, $a_0 \neq 0$, $p(x) \notin (x)$. There exists $q(x) = \sum\limits_{i=0}^{n} a'_i x_i$ with $a'_i = a_i$ for $i = 1, 2, \ldots, n$ and $a_0 = 0$, $q(x) \in (x) \subset I$. Thus $a_0 = p(x) - q(x) \in I$, a_0 is a unit so $I = F$. That's contradictory! (x) is a maximal ideal.
Consider $(x+1) \subset F[x]$. $F[x]$ is a UFD since F is. For any $f \in (x+1)$, $f = (x+1)g$. For any $h \in F[x] \backslash (x+1)$, $h = (x+1)k + r$, where $\deg r < \deg(x+1) = 1$. So r is a unit in $F[x]$, which means $(h) + (x+1) = F[x]$. $(x+1)$ is maximal in $F[x]$.

Exercise 3.5.10. (a) If F is a field then every nonzero element of $F[[x]]$ is of the form $x^k u$ with $u \in F[[x]]$ a unit.

(b) $F[[x]]$ is a principal ideal domain whose only ideals are 0, $F[[x]] = (1_F) = (x^0)$ and (x^k) for each $k \geq 1$.

Answer. (a) For any nonzero element f in $F[[x]]$, $f = (a_0, a_1, \ldots)$, we can find the minimal k such that $a_k \neq 0$. $f = \sum\limits_{i=0}^{\infty} a_i x^i = x^k g$, $g = \sum\limits_{i=0}^{\infty} a_{i+k} x^i$ which has nonzero constant term thus a unit. So $f = x^k g$.

(b) For any ideal $I \subset F[[x]]$ and $a \in I$, $a = x^k u$, u a unit, we construct $\varphi : I \to \mathbf{N}$ given by $\varphi(a) = k$, $\varphi(I) \subset \mathbf{N}$, take $a \in I$ minimize $\varphi(a)$.

Assume $a = x^k u$, then $(a) = (x^k) \subset I$. For any $a' = x^{k'} u' \in I$, $k' > k$, $a' = x^k(x^{k'-k}u') \in (x^k)$. So $I \subset (x^k)$. This also shows that the only ideals are (x^k) for $k \in \mathbf{N}$.

Exercise 3.5.11. Let $\mathcal{C}$ be the category with objects all commutative rings with identity and morphisms all ring homomorphism $f : R \to S$ such that $f(1_R) = 1_S$. Then the polynomial ring $\mathbf{Z}[x_1, \ldots, x_n]$ is a free object on the set $\{x_1, \ldots, x_n\}$ in the category $\mathcal{C}$.

Answer. Denote $X = \{x_1, x_2, \ldots, x_n\}$. For any object R in $\mathcal{C}$, there exists a map $f : \mathbf{Z} \to R$ given by $f : n \mapsto n \cdot 1_R$ is a homomorphism of rings. If there exist $i : X \to R$ given by $i(x_i) = r_i \in R$. Applying Theorem 5.5 there exists $\bar{f} : \mathbf{Z}[x_1, x_2, \ldots, x_n] \to R$ and $\bar{f}|\mathbf{Z} = f$, $\bar{f}(x_i) = r_i$ so $\bar{f}i = f$. Thus $\mathbf{Z}[x_1, x_2, \ldots, x_n]$ is free over X.

3.6 Factorization in polynomial rings

Exercise 3.6.1. (a) If D is an integral domain and c is an irreducible element in D, then $D[x]$ is not a principal ideal domain.

(b) $\mathbf{Z}[x]$ is not a principal ideal domain.

(c) If F is a field and $n \geq 2$, then $F[x_1, \ldots, x_n]$ is not a principal ideal domain.

Exercise 3.6.2. If F is a field and $f, g \in F[x]$ with $\deg n \geq 1$, then there exist unique polynomials $f_0, f_1, \ldots, f_r \in F[x]$ such that $\deg f_i < degg$ for all i and

$$f = f_0 + f_1 g + f_2 g^2 + \cdots + f_r g^r$$

Exercise 3.6.3. Let f be a field of positive degree over an integral domain D.

(a) If $\mathrm{char} D = 0$, then $f' \neq 0$.

(b) If $\mathrm{char} D = p \neq 0$, then $f' = 0$ if and only if f is a polynomial in x^p(that is, $f = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots + a_{jp} x^{jp}$).

Exercise 3.6.4. If D is a unique factorization domain, $a \in D$ and $f \in D[x]$, then $C(af)$ and $aC(f)$ are associates in D.

Exercise 3.6.5. Let R be a commutative ring with identity and $f = \sum\limits_{i=0}^{n} a_i x^i \in R[x]$. Then f is a unit in $R[x]$ if and only if a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent elements of R.

Exercise 3.6.6. Let $p \in \mathbf{Z}$ be prime; let F be a field and let $c \in F$. Then $x^p - c$ is irreducible in $F[x]$ if and only if $x^p - c$ has no root in F.

Exercise 3.6.7. If $f = \sum a_i x^i \in \mathbf{Z}[x]$ and p prime, let $\bar{f} = \sum \bar{a}_i x^i \in Z_p[x]$, where $\bar{a}$ is the image of a under the canonical epimorphism $\mathbf{Z} \to Z_p$.

(a) If f is monic and $\bar{f}$ is irreducible in $Z_p[x]$ for some p, then f is irreducible in $\mathbf{Z}[x]$.

(b) Given an example to show that (a) may be false if f is not monic.

(c) Extend (a) to polynomials over a unique factorization domain.

Exercise 3.6.8. (a) Let $c \in F$, where F is a field of characteristic p (p prime). Then $x^p - x - c$ is irreducible in $F[x]$ if and only if $x^p - x - c$ has no root in F.

(b) If $\mathrm{char}F = 0$, part (a) is false.

Exercise 3.6.9. Let $f = \sum\limits_{i=0} a_i x^i \in \mathbf{Z}[x]$ have degree n. Suppose that for some $k(0 < k < n)$ and some prime p: $p \nmid a_n$; $p \nmid a_k$; $p \mid a_i$ for all $0 \leq i \leq k-1$; and $p^2 \nmid a_0$. Show that f has a factor g of degree at least k that is irreducible in $\mathbf{Z}[x]$.

Exercise 3.6.10. (a) Let D be an integral domain and $c \in D$. Let $f(x) = \sum\limits_{i=0}^{n} a_i x^2 \in D[x]$ and $f(x-c) = \sum\limits_{i=0}^{n} a_i (x-c)^i \in D[x]$. Then $f(x)$ is irreducible in $D[x]$ if and only if $f(x-c)$ is irreducible.

(b) For each prime p, the **cyclotomic polynomial** $f = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbf{Z}[x]$.

Exercise 3.6.11. If $c_0, c_1, \ldots, c_n$ are distinct elements of an integral domain D and $d_0, \ldots, d_n$ are any elements of D, then there is at most one polynomial f of degree $\leq n$ in $D[x]$ such that $f(c_i) = d_i$ for $i = 0, 1, \ldots, n$.

Exercise 3.6.12. *Lagrange's Interpolation Formula.* If F is a field, a_0, a_1,…, a_n are distinct elements of F and $c_0, c_1, \ldots, c_n$ are any elements of F, then

$$f(x) = \sum_{i=0}^{n} \frac{(x-a_0)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)}{(a_i-a_n)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n)} c_i$$

is the unique polynomial of degree $\leq n$ in $F[x]$ such that $f(a_i) = c_i$ for all i.

Exercise 3.6.13. Let D be a unique factorization domain with a finite number of units and quotient field F. If $f \in D[x]$ has degree n and $c_0, c_1, \ldots, c_n$ are $n+1$ distinct elements of D, then f is completely determined by $f(c_0), f(c_1), \ldots, f(c_n)$ according to **Exercise 3.6.11**. Here is **Kronecker's Method** for finding all the irreducible factors of f in $D[x]$.

(a) It suffices to find only those factors g of degree at most $n/2$.

(b) If g is a factor of f, then $g(c)$ is a factor of $f(c)$ for all $c \in D$.

(c) Let m be the largest integer $\leq n/2$ and choose distinct elements c_0, c_1, …, $c_m \in D$. Choose d_0, d_i, …, $d_m \in D$ such that d_i is a factor of $f(c_i)$ in D for all i. Use **Exercise 3.6.12** to construct a polynomial $g \in F[x]$ such that $g(c_i) = d$ for all i; it is unique by **Exercise 3.6.11**.

(d) Check to see if the polynomial g of part (c) is a factor of f in $F[x]$. If not, make a new choise of $d_0, \ldots, d_m$ and repeat part (c).

(e) After a finite number of steps, all the (irreducible) factors of f in $F[x]$ will have been found. If $g \in F[x]$ is such a factor (of positive degree) then choose $r \in D$ such that $rg \in D[x]$. Then $rg = C(rg)g_1$ with $g_1 \in D[x]$ primitive and irreducible in $F[x]$. By Lemma 6.13, g_1 is an irreducible factor of f in $D[x]$. Proceed in this manner to obtain all the nonconstant irreducible factors of f; the constants are then easily found.

Exercise 3.6.14. Let R be a commutative ring with identity and $c, b \in R$ with c a unit.

(a) Show that the assignment $x \mapsto cx + b$ induces a unique automorphism of $R[x]$ that is the identity of R. What is its inverse?

(b) If D is an integral domain, then show that every automorphism of $D[x]$ that is the identity on D is of the type described in (a).

Exercise 3.6.15. If F is a field, then x and y are relatively prime in the polynomial domain $F[x, y]$, but $F[x, y] = (1_F) \supsetneqq (x) + (y)$.

Exercise 3.6.16. Let $f = a_n x^n + \cdots + a_0$ be a polynomial over the field $\mathbf{R}$ of real numbers and let $\varphi = |a_n| \, x^n + \cdots + |a_0| \in \mathbf{R}[x]$.

(a) IF $|u| \leq d$, then $|f(u)| \leq \varphi(d)$.

(b) Given $a, c \in \mathbf{R}$ with $c > 0$ there exists $M \in \mathbf{R}$ such that $|f(a + h) - f(a)| \leq M \, |h|$ for all $h \in \mathbf{R}$ with $|h| \leq c$.

(c) (Intermediate Value Theorem) If $a < b$ and $f(a) < d < f(b)$, then there exists $c \in \mathbf{R}$ such that $a < c < b$ and $f(c) = d$.

(d) Every polynomial g of odd degree in $\mathbf{R}[x]$ has a real root.

Chapter 4

Modules

4.1 Modules, homomorphisms and exact sequences

Exercise 4.1.1. If A is an abelian group and $n > 0$ an integer such that $na = 0$ for all $a \in A$, then A is a unitary Z_n-module, with the action of Z_n on A given by $\bar{k}a = ka$, where $k \in \mathbf{Z}$ and $k \mapsto \bar{k} \in Z_n$ under the canonical projection $\mathbf{Z} \to Z_n$.

Answer. $\bar{k}, \bar{l} \in Z_n$, $k, l \in \mathbf{Z}$ and $a, b \in A$, $(\bar{k} + \bar{l})a = (k + l)a = ka + la = \bar{k}a + \bar{l}a$, $\bar{k}(a + B) = k(a + b) = ka + kb = \bar{k}a + \bar{k}b$. Assume $\bar{k}l = kl \mod n = t$, $\bar{k}l = ta = k(la) = \bar{k}(\bar{l}a)$ since $kl = t + sn, s \in \mathbf{N}$. So A is a Z_n-module.

Exercise 4.1.2. Let $f : A \to B$ be an R-module homomorphism.

(a) f is a monomorphism if and only if for every pair of R-module homomorphisms $g, h : D \to A$ such that $fg = fh$, we have $g = h$.

(b) f is an epimorphism if and only if for every pair of R-module homomorphisms $k, t : B \to A$ such that $kf = tf$, we have $k = t$.

Answer. (a) If f is a monomorphism, $f(a) = f(b)$ if and only if $a = b$, so $fg(a) = fh(a)\, \forall a \in D \Rightarrow g(a) = h(a)\, \forall a \in D$, whence $g = h$.
Conversely. Take $D = \mathrm{Ker} f$ and $g : a \mapsto a \in A$, $h : a \mapsto 0 \in A$. Then $\forall a \in D$, $fg(a) = fh(a) = 0 \in B$. This means $D = \{0\}$, so f is a monomorphism.

(b) If f is an epimorphism. $\forall b \in B$, there is $a \in A$ such that $f(a) = b$. So $gf(a) = hf(a) \Rightarrow g(b) = f(b)\, \forall b \in B$, $g = h$.
Conversely. Take $k : b \mapsto b + \mathrm{Im} f$ and $t : b \mapsto - \in B/\mathrm{Im} f$. $\forall a \in A$, $f(a) \in \mathrm{Im} f$ so $kf(a) = \mathrm{Im} f = tf(a) \Rightarrow k = t$. So $\mathrm{Im} f = B$, f is an epimorphism.

Exercise 4.1.3. Let I be a left ideal of a ring R and A an R-module.

(a) If S is a nonempty subset of A, then $IS = \{\sum\limits_{i=1}^{n} r_i a_i | n \in \mathbf{N}^*; r_i \in I; a_i \in S\}$ is a submodule of A. Note that if $S = \{a\}$, then $IS = Ia = \{ra | r \in I\}$.

(b) If I is a two-sided ideal, then A/IA is an R/I-module with the action of R/I given by $(r + I)(a + IA) = ra + IA$.

Answer. (a) For any $x \in IS$, $x = \sum\limits_{i=1}^{n} r_i a_i$ so $rx = r\sum\limits_{i=1}^{n} r_i a_i = \sum\limits_{i=1}^{n}(rr_i)a_i \in IS$. For any $x, y \in IS$, $x = \sum\limits_{i=1}^{n} r_i a_i$, $y = \sum\limits_{i=1}^{n'} r'_i a'_i$. Then $x + y = x = \sum\limits_{i=1}^{n} r_i a_i + \sum\limits_{i=1}^{n'} r'_i a'_i \in IS$. IS is a submodule of A.

(b) For any $r+I \in R/I$, and $a+IA = A/IA$. $(r+I)(a++IA) = ra+IA \in A/IA$ since $ra \in A$. $\forall r_1, r_2 \in R$, $a_1, a_2 \in A$.

$$\begin{aligned}((r_1 + I) + (r_2 + I))(a + IA) &= (r_1 + r_2 + I)(a + IA)\\ &= (r_1 a + r_2 a + IA)\\ &= (r_1 a + IA) + (r_2 a + IA)\end{aligned}$$

$$\begin{aligned}(r + I)((a_1 + IA) + (a_2 + IA)) &= (r + I)(a_1 + a_2 + IA)\\ &= ra_1 + ra_2 + IA\\ &= (ra_1 + IA) + (ra_2 + IA)\end{aligned}$$

$$\begin{aligned}(r_1 + I)(r_2 + I)(a + IA) &= r_1 r_2 a + IA\\ &= r_1(r_2 a) + IA\\ &= (r_1 + I)(r_2 a + I)\end{aligned}$$

so A/IA is a submodule of R/I.

Exercise 4.1.4. If R has identity, then every unitary cyclic R-module is isomorphic to an R-module of the form R/J, where J is a left ideal of R.

Answer. The cyclic unitary module generated by a is Ra. We only need to prove $J = \{r | ra = 0 \in Ra\}$ is an left ideal of R. $\forall r' \in R$ and $r \in J$, $r'ra = r'(ra) = r'0 = 0 \in Ra$ so $r'r \in J$. J is a left ideal of R. Thus $Ra \cong R/J$.

Exercise 4.1.5. If R has identity, then a nonzero unitary R-module A is **simple** if its only submodules are 0 and A.

(a) Every simple R-module is cyclic.

(b) If A is simple every R-module endomorphism is either the zero map of and isomorphism.

Answer. (a) Trivial.

(b) For and endomorphism f, Imf is a submodule of A, so f is a zero map or an isomorphism.

Exercise 4.1.6. A finitely generated R-module need not to be finitely generated as an an abelian group.

Answer. For the polynomial ring with degree less than 3. $\mathrm{Q}_2[x]$ is finitely generated Q-module. But $\mathrm{Q} \subset \mathrm{Q}_2[x]$, $\mathrm{Q}_2[x]$ is not finitely generated abelian group since Q is not finitely generated.

Exercise 4.1.7. (a) If A and B are R-modules, then the set $\mathrm{Hom}_R(A, B)$ of all R-module homomorphisms $A \to B$ is an abelian group with $f + g$ given on $a \in A$ by $(f + g)(a) = f(a) + g(a) \in B$. The identity element is the zero map.

(b) $\mathrm{Hom}_R(A, B)$ is a ring with identity, where multiplication is composition of functions. $\mathrm{Hom}_R(A, B)$ is called the **endomorphism ring** of A.

(c) A is a left $\mathrm{Hom}_R(A, A)$-module with fa defined to be

$$f(a)(a \in A), f \in \mathrm{Hom}_R(A, A)$$

Answer. (a) For any $f, g \in \mathrm{Hom}_R(A, B)$, $f+g := (f+g)(a) = f(a)+g(a) \in B$ and $f+g = g+f$. Take the 0 element as the zero map and the inverse element of f as $-f : a \mapsto -f(a)$. We have $\mathrm{Hom}_R(A, B)$ an abelian group.

(b) $\mathrm{Hom}_R(A, A)$ is an abelian group. $\forall f, g, h \in \mathrm{Hom}_R(A, A)$,

$$(fg)h = (f \circ h) \circ h = f \circ g \circ h = f \circ (g \circ h) = f(gh)$$

$$f \circ (g + h)(a) = f(g(a) + h(a)) = f(g(a)) + f(h(a))$$

so $f(g + h) = fg + fh$.

$$(f + g) \circ h(a) = (f + g)(h(a)) = f(h(a)) + g(h(a))$$

so $(f+g)h = fh+gh$. $\mathrm{Hom}_R(A, A)$ is a ring and the identity is 1_A map.

(c) $\forall a \in A$ and $f\mathrm{Hom}_R(A, A)$, $fa = f(a) \in A$. For all $a, b \in A$, $f, g \in \mathrm{Hom}_R(A, A)$,

$$(f + g)a = f(a) + g(a) = fa + ga$$

$$f(a + b) = f(a) + f(b) = fa + fb$$

$$(fg)a = f(g(a)) = f(ga)$$

so A is a $\mathrm{Hom}_R(A, A)$-module.

Exercise 4.1.8. Prove that the obvious analogues of Theorem I.8.10 and Corollary I.8.11 are valid for R-modules.

Answer. Let $\{f_i : G_i \to H_i | i \in I\}$ be a family of homomorphisms of R-module. Let $f : \bigoplus\limits_{i\in I}$ be the map $\bigoplus\limits_{i\in I} G_i \to \bigoplus\limits_{i\in I} H_i$ given by $\{a_i\} \mapsto \{f_i(a_i)\}$. Then f is a homomorphism of R-modules such that $f(\bigoplus\limits_{i\in I}) \subset \bigoplus\limits_{i\in I} H_i$, $\mathrm{Ker}f = \bigoplus\limits_{i\in I} \mathrm{Ker}f_i$ and $\mathrm{Im}f = \bigoplus\limits_{i\in I} f_i$.

For any $a_i, b_i \in H_i$ with $i \in I$, $f(\{a_i\}) = \{f_i(a_i)\}$, $f(\{b_i\}) = \{f_i(b_i)\}$ and $f(\{a_ib_i\}) = \{f_i(a_ib_i)\} = \{f_i(a_i)f_i(b_i)\} = \{f(a_i)\}\{f(b_i)\} = f(\{a_i\})f(\{b_i\})$. For any $r \in R$, $f(\{ra_i\}) = \{f_i(ra_i)\} = \{rf_i(a_i)\} = r\{f_i(a_i)\} = rf(\{a_i\})$. Hence f is a well defined homomorphism of R-modules. $\{0\} \in \bigoplus\limits_{i\in I} H_i$ is the zero element of $\bigoplus\limits_{i\in I} H_i$, so $\forall\{a_i\} \in \mathrm{Ker}f$, $f_i(a_i) = 0$. Thus $\mathrm{Ker}f = \bigoplus\limits_{i\in I} \mathrm{Ker}f_i$. The analogue of Corollary I.8.11 is the obvious corollary of the theorem above.

Exercise 4.1.9. If $f : A \to A$ is an R-module homomorphism such that $ff = f$, then

$$A = \mathrm{Ker}f \oplus \mathrm{Im}f$$

Answer. For the theorem of homomorphisms, $\mathrm{Im}f \cong A/\mathrm{Ker}f$. Suppose $\mathrm{Ker}f \cap \mathrm{Im}f \neq \{0\}$, $a \in \mathrm{Ker}f \cap \mathrm{Im}f$. $a = f(b)$, $f(a) = f(f(b)) = f(b) = a = 0$, that's contradictory! So $\mathrm{Ker}f \cap \mathrm{Im}f = \{0\}$. $A = \mathrm{Ker}f \oplus \mathrm{Im}f$.

Exercise 4.1.10. Let $A, A_1, \ldots, A_n$ be R-modules. Then $A \cong A_1 \oplus \cdots \oplus A_n$ if and only if for each $i = 1, 2, \ldots, n$ there is an R-module homomorphism $\varphi_i : A \to A$ such that $\mathrm{Im}\varphi_i \cong A_i$; $\varphi_i\varphi_j$ for $i \neq j$; and $\varphi_1 + \varphi_2 + \cdots + \varphi_n = 1_A$.

Answer. If $A \cong A_1 \oplus \cdots \oplus A_n$. Let π_i, τ_i be as in Theorem 1.14. Define $\varphi_i = \tau_i\pi_i$. Then $\varphi_i\varphi_j = 0$ for $i \neq j$ and $\sum\limits_{i=1}^{n} = 1_A$. $\mathrm{Im}\varphi_i \cong \pi_i(\tau_i(A_i)) = 1_{A_i}(A_i) = A_i$.
Conversely. If exist φ_i, $i \in I$ satisfies those conditions. $\varphi_i(\varphi_1 + \cdots + \varphi_n) = \varphi_i$, $\varphi_i\varphi_j = 0$ for $i \neq j$, so $\varphi_i\varphi_i = \varphi_i$. Let $\psi_i = \varphi_i|\mathrm{Im}\varphi_i : \mathrm{Im}\varphi_i \to A$. Then $\varphi_i\psi_i = 1_{\mathrm{Im}\varphi_i}$ since $\forall\varphi_i(a) \in \mathrm{Im}\varphi_i$, $\varphi_i\psi_i(\varphi_i(a)) = \varphi_i(a)$. $\varphi_i\psi_j = 0$ if $i \neq j$. $\sum\limits_{i=1}^{n} \psi_i\varphi_i = 1_A$ since $\sum\limits_{i=1}^{n} \varphi_i = \sum\limits_{i=1}^{n} \varphi_i\varphi_i = 1_A$. From Theorem 1.14, $A \cong \bigoplus\limits_{i=1}^{n} \mathrm{Im}\varphi_i$.

Exercise 4.1.11. (a) If A is a module over a commutative ring R and $a \in A$, then $\mathcal{O}_a = \{r \in R | ra = 0\}$ is an ideal of R. If $\mathcal{O}_a \neq 0$, a is said to be a **torsion element** of A.

(b) if R is an integral domain, then the set $T(A)$ of all torsion elements of A.($T(A)$ is called the **torsion submodule**.)

(c) Show that (b) may be false for a commutative ring R, which is not an integral domain.
In (d) - (f) R is an integral domain.

(d) If $f : A \to B$ is an R-module homomorphism, then $f(T(A)) \subset T(B)$; hence the restriction f_T of f to $T(A)$ is an R-module homomorphism $T(A) \to T(B)$.

(e) If $0 \to A \xrightarrow{f} B \xrightarrow{g} C$ is an exact sequence of R-module, then so is $0 \to T(A) \xrightarrow{f_T} T(B) \xrightarrow{g_T} T(C)$.

(f) If $g : B \to C$ is an R-module epimorphism, then $g_T : T(B) \to T(C)$ need not be an epimorphism.

Answer. (a) Trivial.

(b) For any $a, b \in T(A)$ and $r_1, r_2 \in R$ such that $r_1a = r_2b = 0$, $r_1r_2(a+b) = r_2(r_1a) + r_1(r_2b) = 0 \Rightarrow a + b \in T(A)$. $\forall r \in R$, $r_1ra = r(r_1a) = 0 \Rightarrow ra \in T(A)$. $T(A)$ is a submodule of A.

(c) Take $R = Z_6 = \{0, 1, 2, 3, 4, 5\}$. R itself is an R-module and $2, 3 \in T(R)$, but $2 + 3 = 5 \notin T(R)$ since $5x = 0$ if and only if $x = 0$.

(d) We only need to check $\forall a \in T(A)$, $f(a) \in T(B)$. There exist $r \in R$ s.t. $ra = 0$, so $f(ra) = rf(a) = f(0) = 0$ so $f(a) \in T(B)$, $f(T(A)) \subset T(B)$.

(e) If $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is an exact sequence. $f(A) = \text{Ker}g$, $fg_T(a) = 0 \Rightarrow g_T f_T(a) = 0$. Hence $0 \to T(A) \xrightarrow{f_T} T(B) \xrightarrow{g_T} T(C) \to 0$ is an exact sequence.

(f) $\mathbf{Z}$ itself is a $\mathbf{Z}$-module. Z_6 is a $\mathbf{Z}$-module as the multiplication given by $a \cdot \bar{b} = \bar{ab}$, $\mathbf{Z}$ has the torsion submodule. $\{0\}$ and Z_6 has the torsion submodule $\{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$ which means $f : \mathbf{Z} \to Z_6$ cannot form an epimorphism $f_T : T(\mathbf{Z}) \to T(Z_6)$.

Exercise 4.1.12. (The Five Lemma). Let

$$\begin{tikzcd}
A_1 \arrow[r] \arrow[d, "\alpha_1"'] & A_2 \arrow[r] \arrow[d, "\alpha_2"'] & A_3 \arrow[r] \arrow[d, "\alpha_3"'] & A_4 \arrow[r] \arrow[d, "\alpha_4"'] & A_5 \arrow[d, "\alpha_5"'] \\
B_1 \arrow[r] & B_2 \arrow[r] & B_3 \arrow[r] & B_4 \arrow[r] & B_5
\end{tikzcd}$$

be a commutative diagram of R-module homomorphisms, with exact rows. Prove that:

(a) α_1 an epimorphism and α_2, α_4 monomorphisms $\Rightarrow$ α_3 is a monomorphism;

(b) α_5 a monomorphism and α_2, α_4 epimorphisms $\Rightarrow$ α_3 is an epimorphism.

Answer. Denote all the homomorphisms as following.

$$\begin{tikzcd}
A_1 \arrow[r, "f_1"] \arrow[d, "\alpha_1"'] & A_2 \arrow[r, "f_2"] \arrow[d, "\alpha_2"'] & A_3 \arrow[r, "f_3"] \arrow[d, "\alpha_3"'] & A_4 \arrow[r, "f_4"] \arrow[d, "\alpha_4"'] & A_5 \arrow[d, "\alpha_5"'] \\
B_1 \arrow[r, "g_1"] & B_2 \arrow[r, "g_2"] & B_3 \arrow[r, "g_3"] & B_4 \arrow[r, "g_4"] & B_5
\end{tikzcd}$$

(a) For any $a \in A_3$, $\alpha_3(a) = 0$, we need to show that $a = 0$. $g_3\alpha_3(a) = \alpha_4 f_3(a) = 0$, since α_4 is monomorphism, $f_3(a) = 0$. So $a \in \text{Ker}f_3 \Rightarrow a \in \text{Im}f_2$. There's $a' \in A_2$, $f_2(a') = a$, $\alpha_3 f_2(a') = 0 = g_2\alpha_2(a')$. So $\alpha_2(a') \in \text{Ker}g_2 = \text{Im}g_1$. There is $b'' \in B_1$, $g_1(b'') = \alpha_2(a')$. α_1 is epimorphism so $\exists a'' \in A_1$, $b'' = \alpha_1(a'')$, so $g_1\alpha_1(a'') = \alpha_2 f_1(a'') = \alpha_2(a')$. α_2 is monomorphism so $f_1(a'') = a' \in \text{Ker}f_2 \Rightarrow a = f_2(a') = 0$.

(b) For any $b \in B_3$, we need to show that $b \in \text{Im}\alpha_3$. $g_3(b) \in B_4$, $g_3(b) = \alpha_4(a')$ for $a' \in A_4$ since α_4 is epimorphism. $g_4\alpha_4(a') = g_4g_3(b) = 0 = \alpha_5 f_4(a')$. $f_4 a' = 0$ cince α_5 is monomorphism. So there is $a \in A_3$, $f_3(a) = a'$, $\alpha_4 f_3(a) = g_3\alpha_3(a) = \alpha_4(a') = g_3(b)$. $g_3(b - \alpha_3(a)) = 0 \Rightarrow b - \alpha_3(a) \in \text{Ker}g_3 = \text{Im}g_2$. There's $b' \in B_2$, $g_2(b') = -b + \alpha_3(a)$. α_2 is epimorphism so $\exists a'' \in A_2$, $\alpha_2(a'') = b'$. Consider $\alpha_3(a - f_2(a'')) = \alpha_3(a) - \alpha_3 f_2(a'') = -g_2\alpha_2(a'') + \alpha_3(a'') = b$. Thus $b \in \text{Im}\alpha_3$, whence α_3 is epimorphism.

Exercise 4.1.13. (a) If $0 \to A \to B \xrightarrow{f} C \to 0$ and $0 \to C \xrightarrow{g} D \to D \to E \to 0$ are short exact sequences of modules, then the sequence $0 \to A \to B \xrightarrow{gf} D \to E \to 0$ is exact.

(b) Show that every exact sequence may be obtained by splicing together suitable short exact sequences as in (a).

Answer. (a) The commutative diagram

$$\begin{tikzcd}
 & & & C \arrow[rd, "g"] & & & \\
0 \arrow[r] & A \arrow[r, "k"] & B \arrow[ru, "f"] \arrow[rr, "gf"'] & & D \arrow[r, "l"] & E \arrow[r] & 0
\end{tikzcd}$$

For any $a \in A$, $k(a) \in \text{Ker}f \Rightarrow fk(a) = 0$. g is monomorphism so $\text{Ker}g = 0$. Since $gfk(a) = 0$, $\text{Im}k \subset \text{Ker}gf$. $\text{Ker}g = 0 \Rightarrow gf(a) = 0$ if and only if $f(a) = 0$. $\text{Ker}gf \subset \text{Im}k$. $\text{Im}gf = \text{Im}g$ since f is epimorphism. So $\text{Im}gf = \text{Ker}l$. $0 \to A \to B \xrightarrow{gf} D \to E \to 0$ is an exact sequence.

(b) For any finite exact sequence $A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} A_n$. We can add head and tail into it and form

$$0 \to \text{Coker}f_1 \to A_1 \xrightarrow{f_1}\to A_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} A_n \to \text{Coim}f_{n-1} \to 0$$

For any exact sequence which has fragment

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$

Consider

$$\begin{tikzcd}
 & & \mathrm{Im} g \arrow[dr, "\subset"] & & \\
A \arrow[r, "f"] & B \arrow[ur, "g"] \arrow[rr, "g"] & & C \arrow[r, "h"] & D
\end{tikzcd}$$

$\subset$ is the inclusion map. We can split into $A \xrightarrow{f} B \xrightarrow{g} \mathrm{Im} g \to 0$ and $0 \to \mathrm{Im} g \xrightarrow{\subset} C \xrightarrow{h} D$. This provides us a way to split an exact sequence into short exact sequences.

Exercise 4.1.14. Show that isomorphism of short exact sequences is an equivalence relation.

Answer. We check isomorphism of short exact sequence is equivalence relation. $a = 0 \to A_1 \to B_1 \to C_1 \to 0$, $b = 0 \to A_2 \to B_2 \to C_2 \to 0$ and $c = 0 \to A_3 \to B_3 \to C_3 \to 0$.

1. The commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r] \arrow[d, "1_{A_1}"'] & B_1 \arrow[r] \arrow[d, "1_{B_1}"'] & C_1 \arrow[r] \arrow[d, "1_{C_1}"'] & 0 \\
0 \arrow[r] & A_1 \arrow[r] & B_1 \arrow[r] & C_1 \arrow[r] & 0
\end{tikzcd}$$

shows that $a \sim a$ since 1_{A_1}, 1_{B_1} and 1_{C_1} are isomorphisms.

2. If

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r] \arrow[d, "f"'] & B_1 \arrow[r] \arrow[d, "g"'] & C_1 \arrow[r] \arrow[d, "h"'] & 0 \\
0 \arrow[r] & A_2 \arrow[r] & B_2 \arrow[r] & C_2 \arrow[r] & 0
\end{tikzcd}$$

then we have

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r] \arrow[d, "f^{-1}"'] & B_1 \arrow[r] \arrow[d, "g^{-1}"'] & C_1 \arrow[r] \arrow[d, "h^{-1}"'] & 0 \\
0 \arrow[r] & A_2 \arrow[r] & B_2 \arrow[r] & C_2 \arrow[r] & 0
\end{tikzcd}$$

is also commutative. So $a \sim b \Leftrightarrow b \sim a$.

3. If

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r] \arrow[d, "f_1"'] & B_1 \arrow[r] \arrow[d, "g_1"'] & C_1 \arrow[r] \arrow[d, "h_1"'] & 0 \\
0 \arrow[r] & A_2 \arrow[r] & B_2 \arrow[r] & C_2 \arrow[r] & 0
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[r] & A_2 \arrow[r] \arrow[d, "f_2"'] & B_2 \arrow[r] \arrow[d, "g_2"'] & C_2 \arrow[r] \arrow[d, "h_2"'] & 0 \\
0 \arrow[r] & A_3 \arrow[r] & B_3 \arrow[r] & C_3 \arrow[r] & 0
\end{tikzcd}$$

are commutative. Then

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r] \arrow[d, "f_2f_1"'] & B_1 \arrow[r] \arrow[d, "g_2g_1"'] & C_1 \arrow[r] \arrow[d, "h_2h_1"'] & 0 \\
0 \arrow[r] & A_3 \arrow[r] & B_3 \arrow[r] & C_3 \arrow[r] & 0
\end{tikzcd}$$

is also commutative. So $a \sim b, b \sim c \Rightarrow a \sim c$.

Exercise 4.1.15. If $f : A \to B$ and $g : B \to A$ are R-module homomorphisms such that $gf = 1_A$, then $B = \text{Im}f \oplus \text{Ker}g$.

Answer. $gf = 1_A$ so f is monomorphism and g is epimorphism. So $B/\text{Ker}g \cong \text{Im}g = A \cong A/0 \cong \text{Im}f$. $\text{Ker}g \cap \text{Im}0 = \{0\}$ since $g(\text{Im}f) = A$. Thus $B = \text{Ker}g \oplus \text{Im}f$.

Exercise 4.1.16. Let R be a ring and R^{op} its opposite ring. If A is a left R-module, then A is a right R^{op}-module such that $ra = ar$ for all $a \in A, 4 \in R, r \in R^{op}$.

Answer. Trivial.

Exercise 4.1.17. (a) If R has an identity and A is an R-module, then there are submodules B and C of A such that B is unitary, $RC = 0$ and $A = B \oplus C$.

(b) Let A_1 be another R-module, with $A_1 = B_1 \oplus C_1$ (B_1 unitary, $RC = 0$), If $f : A \to A_1$ is an R-module homomorphism then $f(B) \subset B_1$ and $f(C) \subset C_1$.

(c) If the map f of part (b) is an epimorphism, then so are $f|B : B \to B_1$ and $f|C : C \to C_1$.

Answer. (a) Let $B = \{1_R a | a \in A\}$, $C = \{a \in A | 1_R a = 0\}$. Then B is unitary since $1_R(1_R a) = 1_R a$. $RC = 0$ since $ra = (r1_R)a = r(1_R a) = 0 \forall a \in C$. And $\forall a \in A$, $1_R(a - 1_R a) = 0 \Rightarrow a - 1_R a \in C$. So $A = \subset B \oplus C$. Obviously $B \oplus C \subset A$, $A = B \oplus C$.

(b) For any $x = b_1 + c_1 \in A_1$, $1_R x = 1_R(b_1 + c_1) = 1_R b_1$, B_1 is the maximal unitary submodule and B_1 contains all unitary elements. $f(B)$ is also unitary since $f(b) = f(1_R b) = 1_R f(b)$ for any $b \in B$. $f(B) \subset B_1$.
C_1 contains all elements $x \in A_1$ s.t. $Rx = 0$. Since $Rf(c) = f(Rc) = 0$ for all $c \in C$, we have $f(C) \subset C_1$.

(c) For any $b' \in B'$, we have $f(x) = b'$ since f is epimorphism. Assume $x = b + c$ with $b \in B$ and $c \in C$. $f(x) = f(1_R(b + c)) = f(1_R b) = 1_R f(b) = f(b)$. So $\exists b \in B$, $f(b) = b'$. $f|B$ is epimorphism. For any $c' \in C$, we have $f(y) = c$. Assume $y = a + d$ with $a \in B$ and $d \in C$. $f(y) = f(1_R(a + d)) = f(1_R a) = 0$, so $1_R f(a) = 0 \Rightarrow a = 0$. Thus $\exists y = d \in C$, $f(d) = c'$. $f|C$ is epimorphism.

Exercise 4.1.18. Let R be a ring without identity. Embed R in a ring S with identity and charateristic zero as in the proof of Theorem III.1.10. Identify R with its image in S.

(a) Show that every element of S may be uniquely expressed in the form $r1_S + n1_S (r \in R, n \in \mathbf{Z})$.

(b) If A is an R-module and $a \in A$, show that there is a unique R-module homomorphism $f : S \to A$ such that $f(1_S) = a$.

Answer. (a) Trivial since $S = R \times \mathbf{Z}$.

(b) $S = R1_S \oplus \mathbf{Z}1_S$. Let $f(r1_S + n1_S) = ra + na$, then $f(1_S) = a$ and f is a well defined homomorphism of modules. If there exists another g s.t.

$g(1_S) = a$, $\forall r1_S + n1_S \in S$, $g(r1_S + n1_S) = rg(1_S) + ng(1_S) = ra + na = f(r1_S + n1_S)$. So $g = f$.

4.2 Free modules and vector spaces

Exercise 4.2.1. (a) A set of vectors $\{x_1, \cdots x_n\}$ in a vector space V over a division ring R is linearly dependent if and only if some x_k is a linear combination of the preceding x_i.

(b) If $\{x_1, x_2, x_3\}$ is a linearly independent subset of V, then the set $\{x_1 + x_2, x_2 + x_3, x_3 + x_1\}$ is linearly independent if and only if $\mathrm{Char}R \neq 2$.

Exercise 4.2.2. Let R be any ring (possibly without identity) and X a nonempty set. In this exercise an R-module F is called a **free module on** X if F is a free object on X in the category of all left R-modules. Thus by Definition I.7.7m F is the free module on X if there is a function $\tau : X \to F$ such that for any left R-module A and function $f : X \to A$ there is a unique R-module homomorphism $\bar{f} : F \to A$ with $\bar{f}\tau = f$.

(a) Let $\{X_i | i \in I\}$ be a collection of mutually disjoint sets and for each $i \in I$, suppose F_i is a free module on X_i, with $\tau_i : X_i \to F_i$. Let $X = \bigcup\limits_{i \in I} X_i$ and $F = \sum\limits_{i \in I} F_i$, with $\phi_i : F_i \to F$ the canonical injection. Define $\tau : X \to F$ by $\tau(x) = \phi_i \tau_i(x)$ for $x \in X_i$. Prove that F is a free module on X.

(b) Assume R has an identity. Let the abelian group $\mathbf{Z}$ be given trivial R-module structure ($rm = 0$ for all $r \in R, m \in \mathbf{Z}$), so that $R \oplus \mathbf{Z}$ is an R-module with $r(r', m) = (rr', 0)$ for all $r, r' \in R$, $m \in \mathbf{Z}$. If X is any one element set, $X = \{t\}$, let $\tau : X \to R \oplus \mathbf{Z}$ be given by $\tau(t) = (1_R, 1)$. Prove that $R \oplus \mathbf{Z}$ is a free module on X.

(c) If R is an arbitrary ring and X is any set, then there exists a free module on X.

Exercise 4.2.3. Let R be any ring (possibly without indentity) and F a free R-module on the set X, with $\tau X :\to F$, as in **Exercise 4.2.2**. Show that $\tau(X)$ is a set of generators of the R-module F.

Exercise 4.2.4. Let R be a principal ideal domain, A a unitary left R-module, and $p \in R$ a prime (= irreducible). Let $pA = \{pa | a \in A\}$ and $A[p] = \{a \in A | pa = 0\}$.

(a) $R/(p)$ is a field.

(b) pA and $A[p]$ are submodules of A.
(c) A/pA is a vector space over $R/(p)$, with $(r+(p))(a+pA) = ra+pA$.
(d) $A[p]$ is a vector space over $R/(p)$, with $(r+(p))a = ra$.

Exercise 4.2.5. Let V be a vector space over a division ring D and S the set of all subspaces of V, partiallly ordered by set theoretic inclusion.
(a) S is a complete lattice.
(b) S is a complemented lattice; that is, for each $V_1 \in S$ there exists $V_2 \in S$ such that $V = V_1 + V_2$ and $V_1 \cap V_2 = 0$, so that $V = V_1 \oplus V_2$.
(c) S is modular lattice; that is, if $V_1, V_2, V_3 \in S$ and $V_3 \subset V_1$, then

$$V_1 \cap (V_2 + V_3) = (V_1 \cap V_2) + V_3$$

Exercise 4.2.6. Let $\mathbf{R}$ and $\mathbf{C}$ be the fields of real and complex numbers respetively.
(a) $\dim_{\mathbf{R}}\mathbf{C}$ and $\dim_{\mathbf{R}}\mathbf{R} = 1$.
(b) There is no field K such that $\mathbf{R} \subset K\mathbf{C}$.

Exercise 4.2.7. If G is a nontrivial group that is not cyclic of order 2, then G has a nonidentity automorphism.

Exercise 4.2.8. If V is a finite dimensional vector space and V^m is the vector space

$$V \oplus V \oplus \cdots \oplus V \text{ (m summands)}$$

then for each $m \geq 1$, V^m is finite dimensional and $\dim V^m = m(\dim V)$.

Exercise 4.2.9. If F_1 and F_2 are free modules over a ring with the invariant dimension property, then $\operatorname{rank}(F_1 \oplus F_2) = \operatorname{rank} F_1 + \operatorname{rank} F_2$.

Exercise 4.2.10. Let R be a ring with no zero divisors such that for all $r, s \in R$ there exists $a, b \in R$, not both zero, with $ar + bs = 0$.
(a) If $R = K \oplus L$, then $K = 0$ or $L = 0$.
(b) If R has an identity, then R has the invariant dimension property.

Exercise 4.2.11. Let F be a free module of infinite rank α over a ring R that has the invariant dimension property. For each cardinal β such that $0 \leq \beta \leq \alpha$, F has infinitely many proper free submodules of rank β.

Exercise 4.2.12. If F is a free module ober a ring with indentity such that F has a basis of finite cardinality $n \geq 1$ and another basis of cardinality $n+1$, then F has a basis of cardinality m for every $m \geq n(m \in \mathbf{N}^*)$.

Exercise 4.2.13. Let K be a ring with identity and F a free K-module with an infinite demumerable basis $\{e_1, e_2, \ldots\}$. Then $R = \mathrm{Hom}_K(F, F)$ is a ring by **Exercise 4.1.7**. If n is any positive integer, then the free left R-module R has a basis of n elementsl that is, as an R-module, $R \cong R \oplus \cdots \oplus R$ for any finite number of summands.

Exercise 4.2.14. Let $f : V \to V'$ be a linear transformation of finite dimensional vector space V and V' such that $\dim V = \dim V'$. Then the following conditions are equivalent: (i) f is an isomorphism; (ii) f is an epimorphisml f is a monomorphism.

Exercise 4.2.15. Let R be a ring with identity. Show that R is not a free module on any set in the category of all R-modules.