MATH 8510, Abstract Algebra I
Fall 2016
Exercises 8-1
Name: Shuai Wei
Collaborator: Xiaoyuan Liu, Daozhou Zhu

Exercise 1 (UMP: Universal Mapping Property)**.** Let $(G, +)$ be an abelian group and let $g_1, \ldots, g_t \in G$. For $i = 1, \ldots, t$ let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{Z}^t$ be the "ith standard basis vector".

(a) Prove that there exists a unique abelian group homomorphism $\phi \colon \mathbb{Z}^t \to G$ such that $\phi(e_i) = g_i$ for $i = 1, \ldots, t$.

Proof. Let $z_i \in \mathbb{Z}$ for $i = 1, \ldots, t$.
Define ϕ as

$$\phi : \mathbb{Z}^t \to G$$
$$(z_1, \ldots, z_t) \mapsto \sum_{i=1}^{t} z_i g_i$$

For $i = 1, \ldots, t$, $z_i \in \mathbb{Z}$ and $g_i \in (G, +)$, so $z_i g_i \in G$.
Then

$$\sum_{i=1}^{t} z_i g_i \in G.$$

So ϕ is well-defined.
At first, we verify that for $i = 1, \ldots, t$,

$$\phi(e_i) = 0g_1 + ...0g_{i-1} + 1g_i + 0g_{i+1} + \ldots + 0g_t = g_i.$$

We then show ϕ is a homomorphism.
Let $x = (x_1, x_2, \ldots, x_t), y = (y_1, y_2, \ldots, y_t) \in \mathbb{Z}^t$, where $x_i, y_i \in \mathbb{Z}$ for i $= 1, 2, \ldots, t$.
Since G is abelian,

$$\begin{aligned}
\phi(x + y) &= \phi((x_1 + y_1, x_2 + y_2, \ldots, x_t + y_t)) \\
&= \sum_{i=1}^{t} (x_i + y_i) g_i \\
&= \sum_{i=1}^{t} x_i g_i + \sum_{i=1}^{t} y_i g_i \\
&= \phi(x) + \phi(y).
\end{aligned}$$

So ϕ is a homomorphism.
Suppose there exists another abelian group homomorphism $\varphi \colon \mathbb{Z}^t \to G$ such that

$$\varphi(e_i) = g_i, \text{ for } i = 1, \ldots, t.$$

Let $z = (z_1, z_2, \ldots, z_t) \in \mathbb{Z}^t$, then $z_i \in \mathbb{Z}$ for $i = 1, 2, \ldots, t$.
Then

$$z = \sum_{i=1}^{t} z_i e_i.$$

Since ϕ and φ are homomorphisms,

$$\begin{aligned}\phi(z) &= \sum_{i=1}^{t} z_i g_i \\ &= \sum_{i=1}^{t} z_i \varphi(e_i) \\ &= \sum_{i=1}^{t} \varphi(z_i e_i) \\ &= \varphi(z)\end{aligned}$$

Since $z \in \mathbb{Z}^t$ is arbitrary, $\phi = \varphi$.
Thus, such abelian group homomorphism is unique.

□

(b) Prove that $\mathrm{Im}(\phi) = \langle g_1, \ldots, g_t \rangle$. In particular, ϕ is surjective if and only if $G = \langle g_1, \ldots, g_t \rangle$.

Proof. Let $z = (z_1, z_2, \ldots, z_t) \in \mathbb{Z}^t$, then $z_i \in \mathbb{Z}$ for $i = 1, 2, \ldots, t$.
Then

$$z = \sum_{i=1}^{t} z_i e_i.$$

By the definition of ϕ,

$$\phi(z) = \sum_{i=1}^{t} z_i g_i \in \langle g_1, g_2, \ldots, g_t \rangle,$$

so

$$\mathrm{Im}(\phi) \subset \langle g_1, g_2, \ldots, g_t \rangle.$$

On the other hand, let $x \in \langle g_1, g_2, \ldots, g_t \rangle$, then $\exists\ x_1, x_2, \ldots, x_t \in \mathbb{Z}$ such that

$$x = \sum_{i=1}^{t} g_i x_i.$$

Let $y = (x_1, x_2, ..., x_t)$, then

$$x = \phi(y) = \sum_{i=1}^{t} x_i g_i \in \mathrm{Im}(\phi).$$

So

$$\langle g_1, g_2, \ldots, g_t \rangle \subset \mathrm{Im}(\phi).$$

Thus,

$$\mathrm{Im}(\phi) = \langle g_1, g_2, \ldots, g_t \rangle.$$

Then we show the second statement.
"$\Leftarrow$". Assume $G = \langle g_1, g_2, \ldots, g_t \rangle$.
Since $\mathrm{Im}(\phi) = G$, ϕ is surjective.
"$\Rightarrow$". Assume ϕ is surjective.
We show it by contradiction.
Suppose $\exists\ g \in G$ but $g \notin \langle g_1, g_2, \ldots, g_t \rangle$.
By the assumption that ϕ is surjective,
so $\exists\ f \in \mathbb{Z}^t$ such that $\phi(f) = g$, where $f = (f_1, f_2, \ldots, f_t)$ and $f_i \in \mathbb{Z}$ for

$i = 1, 2, \dots, t$.
Then we have

$$g = \phi(f) = \sum_{i=1}^{t} g_i f_i \in \langle g_1, g_2, \dots, g_t \rangle,$$

which is contradicted by the other assumption that $g \notin \langle g_1, g_2, \dots, g_t \rangle$.
Thus, if $g \in G$, then $g \in \langle g_1, g_2, \dots, g_t \rangle$.
Namely, $G \subset \langle g_1, g_2, \dots, g_t \rangle = \mathrm{Im}(\phi)$.
Besides, $\mathrm{Im}(\phi) \subset G$ by the definition of ϕ.
Therefore,

$$G = \mathrm{Im}(\phi) = \langle g_1, g_2, \dots, g_t \rangle.$$

In summary, ϕ is surjective if and only if $G = \langle g_1, \dots, g_t \rangle$. □

(c) Prove that the following conditions are equivalent.
  (i) G is finitely generated.
  (ii) There is an integer $t \geq 0$ and an epimorphism $\phi \colon \mathbb{Z}^t \to G$.
  (iii) There is an integer $t \geq 0$ and a subgroup $K \leq \mathbb{Z}^t$ such that $G \cong \mathbb{Z}^t / K$.

Proof. "(i)$\Rightarrow$ (ii)".
Let $G = \langle g_1, g_2, \dots, g_n \rangle$.
Define

$$\phi : \mathbb{Z}^t \to G$$
$$(z_1, \dots, z_t) \mapsto \sum_{i=1}^{t} z_i g_i$$

Then by part (a), we have ϕ is a homomorphism.
Besides, since G is finitely generated, by part (b), ϕ is surjective.
So ϕ is an epimorphism.
Thus, there is an integer $t = n$ and an epimorphism $\phi : \mathbb{Z}^t \to G$.
"(ii) $\Rightarrow$ (iii)".
Since ϕ is epimorphism, it is a homomorphism.
So by the First Isomorphism Theorem, we have

$$\mathrm{Im}(\mathbb{Z}_t) \cong \mathbb{Z}_t / \operatorname{Ker} \mathbb{Z}_t.$$

Since ϕ is epimorphism, it is surjective.
So

$$\mathrm{Im}(\mathbb{Z}_t) = G.$$

Then

$$G \cong \mathbb{Z}_t / \operatorname{Ker} \mathbb{Z}_t.$$

Thus, there exists $t \in \mathbb{N}$ and a subgroup $K = \operatorname{Ker} \mathbb{Z}_t \leq \mathbb{Z}_t$ such that $G \cong \mathbb{Z}_t / K$.
"(iii) $\Rightarrow$ (ii)".
Since the possilbe subgroups of $\mathbb{Z}$ are $\{0\}$ and $\mathbb{Z}_n$ for $n \in \mathbb{N}$ and $n \geq 1$, it is obvious $K = \{e_{\mathbb{Z}^t}\}$ and $(n_1\mathbb{Z}) \times (n_2\mathbb{Z}) \times \ldots \times (n_t\mathbb{Z})$ are the possible subgroup of $\mathbb{Z}^t$, where $e_{\mathbb{Z}^t}$ is a t-dimensional zero vector and $n_i \in \mathbb{Z}, n_i \geq 1$ for $i = 1, 2, \dots, t$.
We will show it by the following two cases.

(1) Let $K = \{e_{\mathbb{Z}^t}\}$.
Then
$$G \cong \mathbb{Z}^t/K \cong \mathbb{Z}^t.$$
Define
$$\phi : \mathbb{Z}^t \to G$$
$$(z_1, \ldots, z_t) \mapsto \sum_{i=1}^{t} z_i g_i$$
Then ϕ is an isomorphism, and then it is an epimorphism.
By part (b), we have G is finitely generated.

(2) Let $K = (n_1\mathbb{Z}) \times (n_2\mathbb{Z}) \times \ldots \times (n_t\mathbb{Z})$.
Then $\mathbb{Z}^t/K = (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \ldots \times (\mathbb{Z}/n_t\mathbb{Z})$.
So $|\mathbb{Z}^t/K| = n_1 n_2 \ldots n_t$.
Since
$$G \cong \mathbb{Z}^t/K$$
$$|G| = n_1 n_2 \ldots n_t < \infty.$$
So G is finitely generated.

Thus, G is finitely generated if there is an integer $t \geq 0$ and a subgroup $K \leq \mathbb{Z}^t$ such that $G \cong \mathbb{Z}^t/K$. □

(d) Let $s \leq t$ and let $n_1, \ldots, n_s \in \mathbb{Z}$. Prove that there is an isomorphism
$$\mathbb{Z}^t/\langle n_1 e_1, \ldots, n_s e_s\rangle \cong (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_s\mathbb{Z}) \times \mathbb{Z}^{t-s}.$$

Proof. Let $G = (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_s\mathbb{Z}) \times \mathbb{Z}^{t-s}$.
Let $g_i = (\bar{0}, \ldots, \bar{0}, \bar{1}, \bar{0}, \ldots, \bar{0}, 0, \ldots, 0) \in \mathbb{Z}^t$ be the ith basis vetor with the i-th element $\bar{1}$ for $1 \leq i \leq s$.
Let $g_i = (\bar{0}, \ldots, \bar{0}, 0, \ldots, 0, 1, 0, \ldots, 1)$ be the ith basis vector with the i-th element 1 for $s+1 \leq i \leq t$.
Then it is obvious that $G = \langle g_1, \ldots, g_s, g_{s+1}, \ldots, g_t\rangle$.
Define ϕ as
$$\phi : \mathbb{Z}^t \to G$$
$$(z_1, \ldots, z_t) \mapsto \sum_{i=1}^{t} z_i g_i$$
So by part (a), ϕ is a homomorphism.
Since G is finitely generated, by part (b),
$$\mathrm{Im}(\phi) = G.$$
Next we show
$$\mathrm{Ker}(\phi) = \langle n_1 e_1, \ldots, n_s e_s\rangle.$$
$\forall h = (h_1, \ldots, h_t) \in \mathbb{Z}_t$, where $h_i \in \mathbb{Z}$ for $i = 1, 2, \ldots, t$, we have
$$\phi(h) = g_1 h_1 + \ldots + g_t h_t.$$

$$\begin{aligned}
h \in \operatorname{Ker}(\phi) &\Leftrightarrow \phi(h) = e_G = (\bar{0}, \ldots, \bar{0}, 0, \ldots, 0) \\
&\Leftrightarrow g_1 h_1 + \ldots + g_t h_t = (\bar{0}, \ldots, \bar{0}, 0, \ldots, 0) \\
&\Leftrightarrow (\bar{h_1}, \ldots, \bar{h_s}, h_{s+1}, \ldots, h_t) = (\bar{0}, \ldots, \bar{0}, 0, \ldots, 0) \\
&\Leftrightarrow h_1 \in (n_1\mathbb{Z}), \ldots, h_s \in (n_s\mathbb{Z}), h_{s+1} = 0, \ldots, h_t = 0 \\
&\Leftrightarrow h \in \langle n_1 e_1, \ldots, n_s e_s \rangle.
\end{aligned}$$

Thus,

$$\operatorname{Ker}(\phi) = \langle n_1 e_1, \ldots, n_s e_s \rangle.$$

By the First Isomorphism Theorem, we have

$$\mathbb{Z}^t / \langle n_1 e_1, \ldots, n_s e_s \rangle \cong (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_s\mathbb{Z}) \times \mathbb{Z}^{t-s}.$$

□

Exercise 2. (a) Let $a, b \in \mathbb{Z}^+$ be relatively prime. Use Exercise 5-1#3 to prove that $\mathbb{Z}/(ab)\mathbb{Z} \cong (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$.

Proof. Since $(\mathbb{Z}, +)$ is abelian and $a\mathbb{Z} \leq \mathbb{Z}$ and $b\mathbb{Z} \leq \mathbb{Z}$,

$$a\mathbb{Z} \trianglelefteq \mathbb{Z} \text{ and } b\mathbb{Z} \trianglelefteq \mathbb{Z}.$$

Since a and b are relatively prime, $(a, b) = 1$.
Then $\exists\ x, y \in \mathbb{Z}$ such that

$$ax + by = 1.$$

Let $z \in \mathbb{Z}$, then

$$a(xz) + b(yz) = z$$

Since $x, y, z \in \mathbb{Z}$, $xz, yz \in \mathbb{Z}$.
Then $a(xz) \in a\mathbb{Z}$,and $b(yz) \in b\mathbb{Z}$.
Then

$$z \in a\mathbb{Z} + b\mathbb{Z}.$$

So

$$\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}.$$

Besides,

$$a\mathbb{Z} + b\mathbb{Z} \subset \mathbb{Z}.$$

Thus,

$$\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}.$$

Since $a, b \in \mathbb{Z}$, $\operatorname{lcm}(a, b) = ab$.
So

$$(a\mathbb{Z}) \cap (b\mathbb{Z}) = (ab)\mathbb{Z}.$$

Therefore, according to the conclusion from the Exercise 5-1#3,
we have

$$\mathbb{Z}/(ab)\mathbb{Z} \cong (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}).$$

□

(b) Let $m \in \mathbb{Z}^+$, let $p_1, \ldots, p_m$ be distinct prime numbers, and let $e_1, \ldots, e_m \in \mathbb{Z}^{\geq 0}$. Prove that $\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^m \mathbb{Z}/p_i^{e_i}\mathbb{Z}$.

Proof. We will show it by induction.

(1) Basic step: when $m = 1$, $n = p_1^{e_1}$,
then it is obvious that

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z}.$$

(2) Inductive step: assume when $m = k$, we have $n = \prod_{i=1}^{k} p_i^{e_i}$ and

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{k} \mathbb{Z}/p_i^{e_i}\mathbb{Z}.$$

Let p_{k+1} be a prime such that $p_1, ..., p_k, p_{k+1}$ are distinct and $e_{k+1} \in \mathbb{Z}^{\geq 0}$.
Then $\prod_{i=1}^{k} p_i^{e_i}$ and $p_{k+1}^{e_{k+1}}$ are relatively primes.
According to the conclusion from part (a), we have

$$\mathbb{Z}/\left(\left(\prod_{i=1}^{k} p_i^{e_i}\right) p_{k+1}^{e_{k+1}}\right)\mathbb{Z} \cong \left(\mathbb{Z}/\left(\prod_{i=1}^{k} p_i^{e_i}\right)\mathbb{Z}\right) \times \left(\mathbb{Z}/p_{k+1}^{e_{k+1}}\mathbb{Z}\right).$$

Namely,

$$\mathbb{Z}/\left(\left(\prod_{i=1}^{k+1} p_i^{e_i}\right)\right)\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z}) \times \left(\mathbb{Z}/p_{k+1}^{e_{k+1}}\mathbb{Z}\right).$$

By the inductive assumption, we know

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{k} \mathbb{Z}/p_i^{e_i}\mathbb{Z}.$$

So

$$\mathbb{Z}/\left(\left(\prod_{i=1}^{k+1} p_i^{e_i}\right)\right)\mathbb{Z} \cong \left(\prod_{i=1}^{k} \mathbb{Z}/p_i^{e_i}\mathbb{Z}\right) \times \left(\mathbb{Z}/p_{k+1}^{e_{k+1}}\mathbb{Z}\right).$$

Namely,

$$\mathbb{Z}/\left(\left(\prod_{i=1}^{k+1} p_i^{e_i}\right)\right)\mathbb{Z} \cong \left(\prod_{i=1}^{k+1} \mathbb{Z}/p_i^{e_i}\mathbb{Z}\right).$$

Thus, the assumption also holds for $m = k + 1$.

Therefore,

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{m} \mathbb{Z}/p_i^{e_i}\mathbb{Z}.$$

$\square$

Exercise 3 (5.2)**.** Write a list of the non-isomorphic abelian groups of order 270 in terms of their elementary divisor decompositions. For each group in this list, write its invariant factor decomposition.

Solution:

Let G be an abelian group of order 270.

$$270 = 2 \times 3^3 \times 5.$$

Since $3 = 3$, $3 = 1 + 2$ and $3 = 1 + 1 + 1$, we have 3 non-isomorphic abelian groups of order 270 and they are

$$\begin{gathered}(\mathbb{Z}/27\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z});\\ (\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z});\\ (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}).\end{gathered}$$

Next we compute their invariant factor decomposition.

(1)

$$(\mathbb{Z}/27\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/270\mathbb{Z}$$

(2)

$$\begin{aligned}(\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) &\cong (\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})\\ &\cong (\mathbb{Z}/90\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})\end{aligned}$$

(3)

$$\begin{aligned}&(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})\\ &\cong (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})\\ &\cong (\mathbb{Z}/30\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})\end{aligned}$$

Exercise 4 (5.4.11)**.** Let H and K be characteristic subgroups of a group G such that $H \cap K = \{e\}$ and $G = HK$. Prove that $\mathrm{Aut}(G) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$.

Proof. Since H and K be characteristic subgroups of a group G,

$$H \trianglelefteq G \text{ and } K \trianglelefteq G.$$

Besides,

$$H \cap K = \{e\}.$$

Then by Theorem 5.4, we have

$$H \times K \cong HK = G.$$

Let $\sigma \in \mathrm{Aut}(H)$ and $\tau \in \mathrm{Aut}(K)$.
Define $\sigma \times \tau$ as

$$\begin{aligned}\sigma \times \tau : H \times K &\to H \times K\\ (h, k) &\mapsto (\sigma(h), \tau(k))\end{aligned}$$

Then we show $\sigma \times \tau \in \mathrm{Aut}(H \times K)$.
Let $(h_1, k_1), (h_2, k_2) \in H \times K$.

Since $\sigma \in \text{Aut}(H)$, and $\tau \in \text{Aut}(K)$, σ, τ are homomorphisms.

$$\begin{aligned}\sigma \times \tau\left((h_1,k_1)(h_2,k_2)\right) &= \sigma \times \tau(h_1h_2, k_1k_2)\\ &= (\sigma(h_1h_2), \tau(k_1k_2))\\ &= (\sigma(h_1)\sigma(h_2), \tau(k_1)\tau(k_2))\\ &= (\sigma(h_1), \tau(k_1))\left(\sigma(h_2), \tau(k_2)\right)\\ &= (\sigma \times \tau(h_1,k_1))\left(\sigma \times \tau(h_2,k_2)\right),\end{aligned}$$

Therefore, $\sigma \times \tau$ is a homomorphism.
Let $(h,k) \in H \times K$ where $h \in H, k \in K$.
Since $\sigma \in \text{Aut}(H)$, and $\tau \in \text{Aut}(K)$, σ and τ are isomomorphsims.
So $\sigma(h) = e_G$ and $\tau(k) = e_G$ if and only if $h = e_G$ and $k = e_G$.

$$\begin{aligned}(h,k) \in \text{Ker}(\sigma \times \tau) &\Leftrightarrow \sigma \times \tau(h,k) = (e_G, e_G)\\ &\Leftrightarrow (\sigma(h), \tau(k)) = (e_G, e_G)\\ &\Leftrightarrow \sigma(h) = e_G \text{ and } \tau(k) = e_G\\ &\Leftrightarrow h = e_G \text{ and } k = e_G\\ &\Leftrightarrow (h,k) = (e_G, e_G),\end{aligned}$$

so

$$\text{Ker}(\sigma \times \tau) = (e_G, e_G).$$

So $\sigma \times \tau$ is 1-1.
Let $(h^{'}, k^{'}) \in (H, K)$, where $h \in H, k \in K$.
We have shown before that $\sigma^{-1} \in \text{Aut}(H)$ and $\tau^{-1} \in \text{Aut}(K)$ when $\sigma \in \text{Aut}(H)$ and $\tau \in \text{Aut}(K)$.
Then $\sigma^{-1}(h^{'}) \in H$ and $\tau^{-1}(k^{'}) \in K$.
So

$$\left(\sigma^{-1}(h^{'}), \tau^{-1}(k^{'})\right) \in H \times K.$$

Since by the definition of $\sigma \times \tau$,

$$\sigma \times \tau\left(\sigma^{-1}(h^{'}), \tau^{-1}(k^{'})\right) = (h^{'}, k^{'}),$$

$\sigma \times \tau$ is onto.
Therefore,

$$\sigma \times \tau \in \text{Aut}(G).$$

Next we define ϕ as

$$\begin{aligned}\phi : \text{Aut}(H) \times \text{Aut}(K) &\to \text{Aut}(H \times K)\\ (\sigma, \tau) &\mapsto \sigma \times \tau\end{aligned}$$

Since we have show $\sigma \times \tau \in \text{Aut}(H \times K)$, ϕ is well-defined.
Let $(\sigma_1, \tau_1), (\sigma_2, \tau_2) \in \text{Aut}(H) \times \text{Aut}(K)$, where $\sigma_1, \sigma_2 \in \text{Aut}(H)$ and $\tau_1, \tau_2 \in \text{Aut}(K)$.

Let $(h,k) \in H \times K$ where $h \in H, k \in K$.

$$\begin{aligned}
((\sigma_1\sigma_2) \times (\tau_1\tau_2))\,(h,k) &= ((\sigma_1\sigma_2)(h), (\tau_1\tau_2)(k)) \\
&= (\sigma_1(\sigma_2(h)), \tau_1(\tau_2(k))) \\
&= (\sigma_1 \times \tau_1)(\sigma_2(h), \tau_2(k)) \\
&= (\sigma_1 \times \tau_1)\,((\sigma_2 \times \tau_2)(h,k)) \\
&= ((\sigma_1 \times \tau_1)(\sigma_2 \times \tau_2))\,(h,k),
\end{aligned}$$

so

$$(\sigma_1\sigma_2) \times (\tau_1\tau_2) = (\sigma_1 \times \tau_1)(\sigma_2 \times \tau_2)$$

Then

$$\begin{aligned}
\phi\,((\sigma_1,\tau_1)(\sigma_2,\tau_2)) &= \phi(\sigma_1\sigma_2, \tau_1\tau_2) \\
&= (\sigma_1\sigma_2) \times (\tau_1\tau_2) \\
&= (\sigma_1 \times \tau_1)(\sigma_2 \times \tau_2) \\
&= (\phi(\sigma_1,\tau_1))\,(\phi(\sigma_2,\tau_2))\,.
\end{aligned}$$

So ϕ is a homomorphism.
Let $(\sigma,\tau) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$, where $\sigma \in \mathrm{Aut}(H)$ and $\tau \in \mathrm{Aut}(K)$.
Let id_H and id_K be the identity maps of H and K, respectively.
Let $id_{H\times K}$ be the identity map of $\mathrm{Aut}(H \times K)$.

$$\begin{aligned}
(\sigma,\tau) \in \mathrm{Ker}(\phi) &\Leftrightarrow \phi(\sigma,\tau) = id_{H\times K} \\
&\Leftrightarrow \sigma \times \tau = id_{H\times K} \\
&\Leftrightarrow \sigma \times \tau = id_H \times id_K \\
&\Leftrightarrow (\sigma,\tau) = (id_H, id_K)
\end{aligned}$$

So ϕ is 1-1.
Let $\pi \in \mathrm{Aut}(H \times K)$.
Define two maps $\pi_H : H \to H$ and $\pi_K : K \to K$ by $(\pi_H(h), 1) = \pi(h,1)$ and $(1, \pi_K(k)) = \pi(1,k)$.
Repeat the similar processes as previous ones,
we have π_H and π_K are well-defined and $\pi_H \in \mathrm{Aut}(H)$ and $\pi_K \in \mathrm{Aut}(K)$.
Let $(h,k) \in H \times K$ where $h \in H, k \in K$.

$$\begin{aligned}
\pi(h,k) &= \pi((h,1)(1,k)) \\
&= \pi(h,1)\pi(1,k) \\
&= (\pi_H(h), 1)\,(1, \pi_K(k)) \\
&= (\pi_H(h), \pi_K(k)) \\
&= \pi_H \times \pi_K(h,k),
\end{aligned}$$

so $\pi = \pi_H \times \pi_K$.
Thus, ϕ is onto.
As a result,

$$\mathrm{Aut}(H) \times \mathrm{Aut}(K) \cong \mathrm{Aut}(H \times K)$$

Since we have show

$$H \times K \cong G,$$

$$\mathrm{Aut}(G) \cong \mathrm{Aut}(H \times K).$$

Hence,

$$\mathrm{Aut}(G) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$$

□

Use this to prove that if G is a finite abelian group, then $\mathrm{Aut}(G)$ is isomorphic to the direct product of the automorphism groups of its Sylow subgroups.

Proof. Let $\{P_i\}_{i=1}^{n}$ be the collection of all the Sylow subgroups of G_n.
Then $G_n = P_1P_2 \dots P_n$.
Since G_n is abelian and $P_i \leq G_n$ for $1 \leq i \leq n$,

$$P_i \trianglelefteq G_n.$$

So the Sylow $|P_i|$-subgroup is unique for $1 \leq i \leq n$.
Thus, $P_i \cap P_j = \{e_{G_n}\}$ for $1 \leq i, j \leq n$ and $i \neq j$.
Besides, by Corollary 4.5.6, P_i is a characteristic subgroup of G_n for $1 \leq i \leq n$.
We will show it by induction.
Basic steps:
When $n = 1$, it is a trivial case since the only Sylow subgroup is G_n and $\mathrm{Aut}(G_n) \cong \mathrm{Aut}(G_n)$.
We have just showed the case for $n = 2$.
Inductive steps:
Assume

$$\mathrm{Aut}(G_n) = \mathrm{Aut}(P_1P_2 \dots P_n) \cong \prod_{i=1}^{n} \mathrm{Aut}(P_i).$$

Let $\{Q_i\}i = 1^{n+1}$ be the collection of all the Sylow subgroups of J_{n+1}.
Then $J_{n+1} = Q_1Q_2 \dots Q_{n+1}$.
Similarly, we have for $i = 1, 2, \dots, n+1$,

$$Q_i \trianglelefteq J_{n+1}.$$

For $1 \leq i, j \leq n+1$ and $i \neq j$,

$$Q_i \cap Q_j = \{e_{J_{n+1}}\}.$$

For $1 \leq i \leq n+1$, Q_i is a characteristic subgroup of J_{n+1}.
Let $J_n = Q_1Q_2 \dots Q_n$.
Then it is obvious that $\{Q_i\}_{i=1}^{n}$ is the collection of all the Sylow subgroups of J_n.
Let $\sigma \in \mathrm{Aut}(J_{n+1})$.
Then for $i = 1, 2, \dots, n$, $\sigma(Q_i) = Q_i$ since Q_i is a characteristic subgroup of J_{n+1}.
Since σ is a homomorphism,

$$\begin{aligned} \sigma(J_n) &= \sigma(Q_1Q_2 \dots Q_n) \\ &= \sigma(Q_1)\sigma(Q_2) \dots \sigma(Q_n) \\ &= Q_1Q_2 \dots Q_n \\ &= J_n. \end{aligned}$$

So J_n is a characteristic subgroup of J_{n+1}.
Since for $1 \leq i, j \leq n+1$ and $i \neq j$,

$$Q_i \cap Q_j = \{e_{J_{n+1}}\},$$

and $J_n = Q_1Q_2 \dots Q_n$, we have

$$J_n \cap Q_{n+1} = \{e_{J_{n+1}}\}.$$

We already have Q_{n+1} is a characteristic subgroup of J_{n+1}.
Besides,

$$J_{n+1} = J_n Q_{n+1}.$$

By the conclusion we just made,

$$\mathrm{Aut}(J_{n+1}) \cong \mathrm{Aut}(J_n) \times \mathrm{Aut}(Q_{n+1}).$$

By the inductive assumption, we have

$$\mathrm{Aut}(J_n) = \mathrm{Aut}(Q_1 Q_2 \dots Q_n) \cong \prod_{i=1}^{n} \mathrm{Aut}(Q_i).$$

Thus,

$$\mathrm{Aut}(J_{n+1}) \cong \left(\prod_{i=1}^{n} \mathrm{Aut}(Q_i) \right) \times \mathrm{Aut}(Q_{n+1}).$$

Namely,

$$\mathrm{Aut}(J_{n+1}) \cong \prod_{i=1}^{n+1} \mathrm{Aut}(Q_i).$$

Thus, the assumption also holds for J_{n+1}.
As a result, if $\{P_i\}_{i=1}^{n}$ is the collection of all the Sylow subgroups of a finite abelian group G, then

$$\mathrm{Aut}(G) \cong \prod_{i=1}^{n} \mathrm{Aut}(P_i).$$

□