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

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

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 $\mathrm{Im}(\phi) = G$.
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 $i = 1, 2, \ldots, t$.
Then we have

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

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

$$G = \langle g_1, g_2, \ldots, g_t \rangle.$$

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

(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 $G = \langle g_1, g_2, \ldots, g_n \rangle$.
Define

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

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

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

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 possible subgroups of $\mathbb{Z}$ are $\{0\}$ and $n\mathbb{Z}$ 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 identity vector and $n_i \in \mathbb{Z}, n_i \geq 1$ for $i = 1, 2, \ldots, t$.((there are many others, like $\langle(1, 1, \ldots, 1)\rangle$)
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

$$\phi(h) = g_1 h_1 + \ldots + g_t h_t.$$

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

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

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

Also,

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

Thus,

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

Since $a, b \in \mathbb{Z}$ and $a,\ b$ are relatively prime, $\mathrm{lcm}(a, b) = ab$.
So (need detailed proof here.)

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

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

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

$\square$

(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,

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

$\square$