MATH 8510, Abstract Algebra I
Fall 2016
Exercises 3-2
Due date Thu 08 Sep 4:00PM

Exercise 1 (2.3.18–19 +5ϵ)**.** Let G be a group, and let $g \in G$.

(a) Prove that there exists a unique group homomorphism $f_g\colon \mathbb{Z} \to G$ such that $f_g(1) = g$.

Proof. Define

$$\begin{aligned} f_g : \mathbb{Z} &\to G \\ n &\mapsto g^n \end{aligned}$$

Then f_g is a homomorphism since $\forall m, n \in \mathbb{Z}, f_g(m+n) = g^{m+n} = g^m g^n = f_g(m) f_g(n)$ and also satisfies $f_g(1) = g$.
So there exists a group homomorphism $f_g\colon \mathbb{Z} \to G$ such that $f_g(1) = g$.
Next we show it is unique.
Assume there exists another homomorphism h_g differing from f_g such that $h_g(1) = g$.

(a) If $n > 0$, $h_g(n) = h_g(\sum_{i=1}^n 1) = \prod_{i=1}^n h_g(1) = \prod_{i=1}^n g = g^n$ since h_g is homomorphism.
(b) If $n < 0$, then $-n > 0$ and $h_g(n) = h_g(-(-n)) = (h_g(-n))^{-1} = (g^{-n})^{-1} = g^n$ since h_g is homomorphism.
(c) If $n = 0$, then $h_g(0) = h_g(n-n) = h_g(n) h_g(-n) = g^n g^{-n} = g^0 = f_g(0)$.

So $h_g(n) = g^n = f_g(n), \forall n \in \mathbb{Z}$.
Thus, $f_g = h_g$, which is contradicted by the assumption.
Hence, such group homomorphism is unique. □

(b) Prove that $\operatorname{Im}(f_g) = \langle g \rangle$.

Proof.
$\operatorname{Im}(f_g) = \{g^n | n \in \mathbb{Z}\} \subset G$.
So $g^n \in G, \forall n \in \mathbb{Z}$.
Thus, $\langle g \rangle = \{g^n \in G | n \in \mathbb{Z}\} = \{g^n | n \in \mathbb{Z}\} = \operatorname{Im}(f_g)$. □

(c) Prove that f_g is a monomorphism if and only if $|g| = \infty$.

Proof.

(a) Assume f_g is a monomorphism, then f_g is 1-1 since f_g is homomorphism.
Then $\infty = |\mathbb{Z}| = |\operatorname{Im}(f_g)| = |\langle g \rangle| = |g|$.
So $|g| = \infty$.
(b) Assume $|g| = \infty$.
Suppose f_g is not a monomorphism, then f_g is not 1-1.
So $\exists\, m, n \in \mathbb{Z}$ with $m > n$ such that $f_g(m) = g^m = g^n = f_g(n)$.
Then $g^{m-n} = e_G$.
So $|g| = |\langle g \rangle| \leq m - n < \infty$ since $0 < m - n < \infty$.
It is a contradion since $|g| = \infty$ by assumption.
So f_g is a monomorphism.

□

(d) Assume that $|g| = n < \infty$.

(1) Prove that $\text{Ker}(f_g) = n\mathbb{Z} := \{nm \in \mathbb{Z} \mid m \in \mathbb{Z}\}$.

Proof.
$f_g(n\mathbb{Z}) = g^{n\mathbb{Z}} = g^0 = e_G$ since $|g| = n$.
So $n\mathbb{Z} \in \text{Ker}(f_g)$. Moreover, for other $k = 1, 2, ...n-1$, $g^{k+n\mathbb{Z}} = g^k \neq e_G$ since $|g| = n$.
Thus, $\text{Ker}(f_g) = n\mathbb{Z}$. $\square$

(2) Prove that there is a unique group monomorphism $\phi_g \colon \mathbb{Z}/n\mathbb{Z} \to G$ such that $\phi_g(\bar{1}) = g$.

Proof.
Define

$$\begin{aligned} \phi_g : \mathbb{Z}/n\mathbb{Z} &\to G \\ \bar{m} &\mapsto g^m \end{aligned}$$

Then $\phi_g(\bar{1}) = g^1 = g$.
We first show ϕ_g is well defined.
Let $p = m + n\mathbb{Z}$ and $q = m + l\mathbb{Z}$, where $m, n, l \in \mathbb{Z}$.
So $\phi_g(p) = g^{m+n\mathbb{Z}} = g^m = g^{m+l\mathbb{Z}} = \phi_g(q)$ since $|g| = n$.
So it is well defined.
Next, we show it is a homomorphism.
$\forall \bar{p}, \bar{q} \in \mathbb{Z}/n\mathbb{Z}, \phi_g(\overline{p}\overline{q}) = \phi_g(\overline{pq}) = g^{pq} = g^p g^q = \phi_g(\bar{p})\phi_g(\bar{q})$.
Then we show ϕ_g is 1-1.
Let $g^{\bar{p}} = g^{\bar{q}}$, then $g^{\bar{p}-\bar{q}} = e^G$.
Then $\bar{p} - \bar{q} \in \text{Ker}(f_g)$.
So $\bar{p} - \bar{q} = n\mathbb{Z} = \bar{0}$.
Thus $\bar{p} = \bar{q}$.
As aresult, it is a group monomorphism.
Suppose there exists another group monomorphism $h_g \colon \mathbb{Z}/n\mathbb{Z} \to G$ such that $h_g(\bar{1}) = g$.
Then when $1 < k \leq n-1, h_g(\bar{k}) = h_g(\sum_{i=1}^{k} \bar{1}) = \prod_{i=1}^{k} h_g(\bar{1}) = g^k$ since h_g is a monomorphism.
Besides, $h_g(\bar{0}) = h_g(\bar{n}) = (h_g(\bar{1}))^n = g^n = e_G = \phi_g(\bar{0})$.
So $\phi_g(\bar{k}) = h_g(\bar{k})$ for all $0 \leq k \leq n-1$.
Therefore, $\phi_g = h_g$.
We conclude that such a group monomorphism is unique. $\square$

(3) Prove that $\text{Im}(\phi_g) = \langle g \rangle$.

Proof.
$\text{Im}(\phi_g) = \{g^n | n = 0, 1, 2, ...n-1\} = \{e_G, g, g^2, ..., g^{n-1}\}$
$\langle g \rangle = \{e_G, g, g^2, ..., g^{n-1}\}$ since $|g| = n$.
So $\text{Im}(\phi_g) = \langle g \rangle$. $\square$

(4) We say that a diagram of group homomorphisms

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[dr, "\alpha'"'] & B \arrow[d, "\beta"] \\ & C \end{tikzcd}$$

"commutes" when $\beta \circ \alpha = \alpha'$. Let $\pi \colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the canonical epimorphism, and prove that the following diagram commutes.

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\pi"] \arrow[dr, "f_g"'] & \mathbb{Z}/n\mathbb{Z} \arrow[d, "\phi_g"] \\ & G \end{tikzcd}$$

Proof.
$\forall m \in \mathbb{Z}$, $\phi_g\pi(m) = \phi_g(\bar{m}) = g^m$.
On the other hand, $\forall m \in \mathbb{Z}$, $f_g(m) = g^m$.
Namely, $\forall m \in \mathbb{Z}$, $\phi_g\pi(m) = f_g(m)$.
So $\phi_g\pi = f_g$.
Thus, the diagram commutes. □

Exercise 2. In your free time, read the statements of the exercises from Section 2.3.