MA1214

Introduction to group theory

Prof. Zaitsev

Solutions to Sheet 8

leitner@stp.dias.ie

1. (a) Let $k \in \mathbb{Z}$ and

$$f: \quad \mathbb{Z} \to \mathbb{Z}_n$$
$$a \mapsto f(a) := [ka] .$$

f is a homomorphism: $\forall\, a, b \in \mathbb{Z}$,

$$f(a+b) = [k(a+b)] = [ka+kb] = [ka] + [kb] = f(a) + f(b)$$

(b) Consider the map

$$f: \quad \mathbb{Z}_6 = \{[0],[1],[2],[3],[4],[5]\}\} \to S_3 = \{(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$$
$$[1] \mapsto f([1]) := (1\ 2\ 3) .$$

It is sufficient to show that this prescription of f on $[1] \in \mathbb{Z}_6$ actually defines f on every element of $\mathbb{Z}_6$ (so that there is no choice left):
Since $[1]$ generates $\mathbb{Z}_6$, and since f by assumption is a homorphism, we have for any $[m] \in \mathbb{Z}_6$,

$$f([m]) = f([\underbrace{1+\cdots+1}_{m}]) = f(\underbrace{[1]+\cdots+[1]}_{m}) = \underbrace{f([1]) \circ \cdots \circ f([1])}_{m} = (1\ 2\ 3)^m$$

Thus the specification of f on $[1] \in \mathbb{Z}_6$ determines the map completely.

2. (a) Let

$$f: \quad \mathbb{Z} \to \{3^n | n \in \mathbb{Z}\}$$
$$n \mapsto 3^n .$$

Note that $G_1 = \mathbb{Z}$ is an additive group (the identity in G_1 is $e_1 = 0$), while $G_2 = \{3^n | n \in \mathbb{Z}\}$ is a multiplicative group ($e_2 = 1$).

- f is a homomorphism: $\forall\, n, m \in \mathbb{Z}$,

$$f(n+m) = 3^{n+m} = 3^n \cdot 3^m = f(n) \cdot f(m) .$$

- f is injective: We have

$$3^n = 1\ (= e_2) \quad \Leftrightarrow \quad n = 0\ (= e_1) ,$$

so

$$\ker f = \{0\}$$

- f is surjective: By definition, every element of the group on the r.h.s. is of the form 3^n, for some $n \in \mathbb{Z}$, and thus equal to $f(n)$.

Thus f is an isomorphism.

(b) Let

$$f: \quad \mathbb{Z}\times\mathbb{Z} \to \{2^m 3^n | m, n \in \mathbb{Z}\}$$
$$(m,n) \mapsto 2^m 3^n \,.$$

- f is a homomorphism: $\forall\, m, m', n, n' \in \mathbb{Z}$,

  $$f((m{+}m', n{+}n')) = 2^{m+m'}3^{n+n'} = (2^m 3^n)(2^{m'}3^{n'}) = f((m,n))\cdot f((m',n')).$$

- f is injective:
  $$2^m 3^n = 1 \quad \Leftrightarrow \quad m = n = 0$$
  (we are using unique prime factorization here: powers of 3 cannot be compensated for by powers of 2), so

  $$\ker f = \{(0,0)\}$$

- f is surjective: By definition, every element of the group on the r.h.s. is of the form $2^m 3^n = f((m,n))$ for some $m, n \in \mathbb{Z}$.

Thus f is an isomorphism.

3. (a) Let f, g be group homomorphisms, where $f : G_1 \to G_2$ and $g : G_2 \to G_3$. Here G_1, G_2, G_3 are groups w.r.t. $*_1, *_2, *_3$ respectively. Let $a, b \in G_1$.

$$\begin{aligned}(g \circ f)(a *_1 b) &= g(f(a *_1 b)) \\ &= g(f(a) *_2 f(b)) \\ &= g(f(a)) *_3 g(f(b)) = (g \circ f)(a) *_3 (g \circ f)(b)\end{aligned}$$

(b) Let $G = \langle a \rangle =$ be the cyclic group which as a set equals $\{1, a, a^2, \dots a^n\}$. Let

$$f: \quad G \to H$$
$$a \mapsto f(a)\,.$$

Since f is a group homomorphism, for every $m \in \mathbb{N}_0$, we have

$$f(a^m) = f(\underbrace{a \cdot \ldots \cdot a}_{m}) = \underbrace{f(a) \cdot \ldots \cdot f(a)}_{m} = f(a)^m$$

(here $f(a)^m$ denotes the m-fold composition w.r.t. the group operation in H which we denote by $\cdot$ again). In particular, for $m = 0$,

$$f(e_G) = e_H\,.$$

But $e_G = a^{n+1}$, so

$$e_H = f(e_G) = f(a^{n+1}) = f(a)^{n+1}\,.$$

So the image of G under f is cyclic.