HW 7 Selected Solutions

Prof. Shahed Sharif

2.59i We showed in class that the order of $b := f(a)$ divides the order of a. Since f is an isomorphism, it is also true that the order of $a = g(b)$ divide the order of b. If the order of either a or b is finite, this implies the orders are equal. If one has infinite order and the other has finite order, this would contradict the previous sentence. Therefore if a has infinite order, so does $f(a)$.

2.68 For $f(x) \in G$, we may write $f(x) = a_0 + a_1x + \cdots + a_nx^n$ for some n, and with $a_i \in \mathbb{Z}$ for all i. Let $p_0, p_1, p_2, \ldots$ be a listing of the prime numbers (for instance, $p_0 = 2$, $p_1 = 3$, $p_2 = 5$, etc; the specific choice doesn't matter). Then any $r \in H$ can be written uniquely as

$$p_0^{e_0} p_1^{e_1} \cdots p_n^{e_n}$$

for some n and with $e_i \in \mathbb{Z}$ for all i; for instance, we have $\frac{12}{25} = 2^2 3^1 5^{-2}$. (This result is an extension of prime factorization from $\mathbb{N}$ to positive rationals.) Define $\varphi : G \to H$ by

$$\varphi(a_0 + a_1x + \cdots + a_nx^n) = p_0^{a_0} p_1^{a_1} \cdots p_n^{a_n}.$$

This is certainly well-defined and surjective.

We show that φ is a homomorphism. For let $f = a_0 + a_1x + \cdots + a_nx^n$ and $g = b_0 + b_1x + \cdots + b_mx^m$. Without loss of generality, $m \le n$. If $m < n$, then define b_i for $m < i \le n$ by $b_i = 0$; this allows us to write $g = b_0 + b_1x + \cdots + b_nx^n$. (For instance, if $f = 1 + x + x^2$ and $g = 2 - 3x$, we have $m = 1 < 2 = n$, so we define $b_2 = 0$, in effect writing $g = 2 - 3x + 0x^2$.)

We then have

$$\begin{aligned}
\varphi(f + g) &= \varphi((a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n) \\
&= p_0^{a_0+b_0} p_1^{a_1+b_1} \cdots p_n^{a_n+b_n} \\
&= p_0^{a_0} p_1^{a_1} \cdots p_n^{a_n} p_0^{b_0} \cdots p_n^{b_n} \\
&= \varphi(f) \cdot \varphi(g).
\end{aligned}$$

Finally, suppose $f \in \ker(\varphi)$; that is, $\varphi(f) = 1$. By the uniqueness of prime factorization of rationals, we must have that the exponents in $1 = p_0^{e_0} \cdots p_n^{e_n}$ are all 0, and hence the coefficients of f are all 0, so that $f = 0$. As $\ker(\varphi)$ is trivial, φ is injective.

The claim follows.

D. We define a map $\varphi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ via $\varphi([x]) = ([x], [x])$. Note that the brackets mean 3 different things; for clarity, we can write this as

$$\varphi([x]_6) = ([x]_2, [x]_3),$$

but I will often omit the subscripts where the reader can deduce them.

We first show that φ is well defined; that is, if $[x]_6 = [y]_6$, then $([x]_2, [x]_3) = ([y]_2, [y]_3)$. Well, $[x]_6 = [y]_6$ means $x \equiv y \pmod 6$, or $6 \mid (x-y)$. But this implies $2 \mid (x-y)$, so $[x]_2 = [y]_2$, and $3 \mid (x-y)$, so $[x]_3 = [y]_3$. Therefore $([x]_2, [x]_3) = ([y]_2, [y]_3)$.

Next we show that φ is a homomorphism. We have

$$\begin{aligned}\varphi([x]+[y]) &= \varphi([x+y]) \\ &= ([x+y],[x+y]) \\ &= ([x]+[y],[x]+[y]) \\ &= ([x],[x]) + ([y],[y]).\end{aligned}$$

Next, we compute $\ker(\varphi)$. We have $\varphi([x]) = (0,0)$ if and only if $[x]_2 = 0$ and $[x]_3 = 0$. The first equality means $x \equiv 0 \pmod 2$, or $2 \mid x$. The second equality means $3 \mid x$. Therefore $6 = \operatorname{lcm}(2,3) \mid 6$, so $x \equiv 0 \pmod 6$, or in other words $[x]_6 = 0$. Thus $\ker(\varphi)$ is trivial, and therefore φ is injective.

Finally, $\#\mathbb{Z}_6 = 6 = 2 \cdot 3 = \#(\mathbb{Z}_2 \times \mathbb{Z}_3)$. By the Pigeonhole Principle, φ is also surjective, and hence bijective. Therefore it is an isomorphism.