

Partial Solutions to Homework 6 for MATH 336

11D # 2

We will first show that if f is 1-1, then $\ker f = \{e_G\}$. So suppose that f is 1-1. Let $g \in G$ be any element in $\ker f$. Then by definition of the kernel, $f(g) = e_{G'}$, and by a property of group homomorphisms, $f(e_G) = e_{G'}$. But $f(g) = f(e_G)$ implies that $g = e_G$ since f is 1-1. Therefore, $\ker f = \{e_G\}$.

Next let $\ker f = \{e_G\}$, and we will show that f is 1-1. Consider any $a, b \in G$ such that $f(a) = f(b)$. Then as proven at the top of pg. 187 by properties of group homomorphisms, $f(a)^{-1} = f(a^{-1})$. Then

$$\begin{aligned} f(a) &= f(b) \\ f(a)^{-1}f(a) &= f(a)^{-1}f(b) \\ e_{G'} &= f(a^{-1})f(b) \\ e_{G'} &= f(a^{-1}b) \quad \text{because } f \text{ is a group homomorphism} \end{aligned}$$

Therefore, by definition of the kernel, $a^{-1}b \in \ker f$. Since $\ker f = \{e_G\}$, this implies that $a^{-1}b = e_G$, or $a = b$ since inverses are unique in groups. Therefore, f is 1-1.

11E #2

A group homomorphism from U_5 to S_4 is just a function from the set $U_5 = \{[1]_5, [2]_5, [3]_5, [4]_5\}$ to the set of permutations S_4 . By Cayley's theorem, the function that maps $[a]_5 \in U_5$ to the permutation that takes $[b]_5$ to $[a]_5[b]_5 = [ab]_5$ is a group homomorphism. So let f be that map, and we will now define it explicitly. $f([2]_5)$ maps to the permutation that takes $[1]_5$ to $[2]_5[1]_5 = [2]_5$, $[2]_5$ to $[2]_5[2]_5 = [4]_5$, $[3]_5$ to $[2]_5[3]_5 = [1]_5$, and $[4]_5$ to $[2]_5[4]_5 = [3]_5$. This is the permutation $(1, 2, 3, 4) \rightarrow (2, 4, 1, 3)$, or in cyclic notation, (1243) .

Repeating this process, we see that

$$\begin{aligned} f([1]_5) &= (1, 2, 3, 4) \rightarrow (1, 2, 3, 4) \\ f([2]_5) &= (1, 2, 3, 4) \rightarrow (2, 4, 1, 3) \\ f([3]_5) &= (1, 2, 3, 4) \rightarrow (3, 1, 4, 2) \\ f([4]_5) &= (1, 2, 3, 4) \rightarrow (4, 3, 2, 1). \end{aligned}$$

f is a group homomorphism by Cayley's theorem.

Coding Supplement, 1.7

Let C be a code that contains $\mathbf{0}$ and \mathbf{u} . Then $d(C) \leq d(\mathbf{0}, \mathbf{u}) = w(\mathbf{u})$, where $w(\mathbf{u})$ is the weight of \mathbf{u} , or the number of 1's in \mathbf{u} . By theorem 1.3.6 we can detect at most $d(C) - 1$ errors. Since $d(C) - 1 \leq w(\mathbf{u}) - 1 < w(\mathbf{u})$, we cannot detect \mathbf{u} if it occurs as an error.