Universidad de la República - Facultad de Ingeniería - IMERL.
Matemática Discreta 2, semipresencial

Solución de la segunda prueba práctica- 30 de octubre de 2017.

Ejercicio 1.

a. i) Por ser F homomorfismo tenemos que $F(e_G) = e_K$ y entonces $e_K \in \mathrm{Im}(F)$ (pues $e_G \in G$).

ii) Si $k \in \mathrm{Im}(F)$, existe $g \in G$ tal que $F(g) = k$. Por ser F homomorfismo tenemos que $F(g^{-1}) = F(g)^{-1} = k^{-1}$ y entonces $k^{-1} \in \mathrm{Im}(F)$ (pues $g^{-1} \in G$).

iii) Si $k, \ell \in \mathrm{Im}(F)$, existen $g, h \in G$ tales que $F(g) = k$ y $F(h) = \ell$. Por ser F homomorfismo tenemos que $F(gh) = F(g)F(h) = k\ell$ y entonces $k\ell \in \mathrm{Im}(F)$ (pues $gh \in G$).

Entonces $\mathrm{Im}(F)$ es un subgrupo de K.

b. i) Al ser F no trivial tenemos que $|\mathrm{Im}(F)| \neq 1$ y por el Teorema de órdenes tenemos que $6 = |S_3| = |\mathrm{Ker}(F)||\mathrm{Im}(F)|$ por lo que $|\mathrm{Im}(F)| = 2,\ 3,\ $ o 6. . Por otro lado como $\mathrm{Im}(F) < K$, por el Teorema de Lagrange tenemos que $|\mathrm{Im}(F)| \mid |K|$ y como $3 \nmid |K|$ entonces $|\mathrm{Im}(F)| \neq 3,\ 6$. Por lo tanto $|\mathrm{Im}(F)| = 2$ y luego $|\mathrm{Ker}(F)| = 3$. Como $\mathrm{Ker}(F) < S_3$ y el único subgrupo de S_3 con 3 elementos es $\langle\sigma_1\rangle = \{Id,\ \sigma_1,\ \sigma_2\} = \langle\sigma_2\rangle$, tenemos que $\mathrm{Ker}(F) = \{Id,\ \sigma_1,\ \sigma_2\}$.

ii) Como $\mathrm{Im}(F)$ es un subgrupo de K con 2 elementos, entonces $\mathrm{Im}(F) = \{e_K,\ k\}$ para algún $k \in K$, $k \neq e_K$; es decir que $F(x) = e_k$ o k para todo $x \in S_3$. Como $\tau_i \notin \mathrm{Ker}(F)$, $F(\tau_i) \neq e_K$ y entonces $F(\tau_i) = k$ para todo $i = 1, 2, 3$.

iii) Como en $K = \mathbb{Z}_4$ (con la suma), $o(\overline{1}) = o(\overline{3}) = 4$ y $o(\overline{2}) = 2$, el único subgrupo de $\mathbb{Z}_4$ con dos elementos es $\{\overline{0}, \overline{2}\}$. Entonces $\mathrm{Im}(F) = \{\overline{0}, \overline{2}\}$ y por las antes anteriores (tomando $k = \overline{2}$) tenemos que $F(Id) = F(\sigma_1) = F(\sigma_2) = e_K = \overline{0}$ y $F(\tau_i) = k = \overline{2}$ para $i = 1, 2, 3$.

Ejercicio 2. Utilizaremos la siguiente propiedad: $g^n = e \Leftrightarrow o(g) \mid n$.

a. Como $g^{110} = e$ tenemos que $o(g) \mid 110$ y por lo tanto $o(g) \in \{1,\ 2,\ 5,\ 10,\ 11,\ 22,\ 55,\ 110\}$. Como $g^{55} \neq e$ sabemos que $o(g) \nmid 55$; es decir $o(g) \notin \{1,\ 5,\ 11,\ 55\}$. De forma análoga obtenemos que $o(g)$ no divide ni a 10 ni a 22 por lo que la única posibilidad restante es que $o(g) = 110$.

b. Tenemos que $h^n = e \Leftrightarrow 5 \mid n$ y que $k^n = e \Leftrightarrow 22 \mid n$. Al ser G abeliano tenemos que $(hk)^n = h^n k^n$ para todo $n \in \mathbb{Z}$. Y entonces si $5 =\mid n$, $(hk)^n = h^n k^n = e \cdot k^n = k^n$ por lo que $(hk)^{110} = k^{110} = e$ (pues 22 divide a 110), $(hk)^{10} = k^{10} \neq e$ pues $22 \nmid 10$ y $(hk)^{55} = k^{55} \neq e$ pues $22 \nmid 55$. Por último $(hk)^{22} = h^{22}k^{22} = h^{22} \neq e$ (pues $5 \nmid 22$). Utilizando la parte anterior concluìmos que $o(hk) = 110$.

c. Sea $G = U(121)$; tenemos que $|G| = \varphi(121) = 11(10) = 110$ y como para todo $g \in G$, $o(g) \mid |G|$ tenemos que $o(g) \mid 110$.

i) Cuando escribo $a \equiv b$ me refiero a $a \equiv b \pmod{121}$. Como $2^7 = 128 \equiv 7$, $2^{10} = 2^7 2^3 \equiv 7(8) \equiv 56 \not\equiv 1$, $2^{11} \equiv (56)2 = 112 \equiv (-9)$ y $2^{22} \equiv (-9)^2 = 81 \equiv -40 \not\equiv 11$, tenemos que $o(\overline{2}) = 55$ o 110. Como que $2^{55} = (2^{22})^2 2^{11} \equiv (-40)^2(-9) \equiv (360)(-40) \equiv (-3)(-40) = 120 \equiv -1 \not\equiv 1$ concluímos (usando la parte a)) que $o(\overline{2}) = 110$.
Ahora como $\overline{119} = \overline{-2}$ y $(-2)^{55} = -(2^{55}) \equiv -(-1) = 1$ tenemos que $o(\overline{-2}) \mid 55$. De forma similar tememos que $(-2)^{11} \equiv -112 \equiv 9 \not\equiv 1$ y $(-2)^5 = -32 \not\equiv 1$, por lo que $o(\overline{-2}) = 55$. Otro argumento es: $-2 = (-1)(2) \equiv 2^{55}2 = 2^{56}$ y por la propiedad del orden de una potencia tenemos que $o(2^{56}) = \dfrac{o(2)}{\mathrm{mcd}(56, o(2))} = \dfrac{110}{2} = 55$.
Como $3^4 = 9^2 = 81 \equiv -40$, $3^5 \equiv -120 \equiv 1$ por lo que $o(\overline{3}) \mid 5$ y como $o(\overline{3}) \neq 1$ obtenemos que $o(\overline{3}) = 5$.

ii) Como $o(\overline{2}) = 110$, el subgrupo $\langle\overline{2}\rangle$ tiene cardinal 110 ($= |G|$), por lo que $\langle\overline{2}\rangle = G$.

iii) Al ser $G = \langle\overline{2}\rangle = \{\overline{2}^m : m \in \mathbb{Z}\}$ cada homomorfismo $F : G \to \mathbb{Z}_{20}$ queda determinado por $F(\overline{2}) = \overline{k} \in \mathbb{Z}_{20}$ tal que o$(\overline{k}) \mid o(\overline{2})$ (pues luego F en los elementos de G es $F(\overline{2}^m) = \underbrace{F(\overline{2}) + \cdots + F(\overline{2})}_{m \text{ veces}} = \underbrace{\overline{k} + \cdots + \overline{k}}_{m \text{ veces}} = \overline{mk}$. Resta entonces hallar todos los $\overline{k} \in \mathbb{Z}_{20}$ tales que $10 \mid o(\overline{k})$. Como en $\mathbb{Z}_{20}$ la operación es la suma, tenemos $10 \mid o(\overline{k}) \Leftrightarrow 10k \equiv 0 \pmod{20}$, y por la cancelativa, esto es equivalente a que $k \equiv 0 \pmod{2}$ (es decir a que k sea par). Por lo tanto hay 10 posibles $\overline{k}$ que son $\overline{k} = \overline{2i}$ para $i \in \{0, 1, \cdots, 9\}$.