Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería **Curso 2012**
Instituto de Matemática y Estadística

Solución del segundo parcial

Ejercicio 1.

A. El neutro de $GL_2(\mathbb{R})$ es $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ y pertenece a H. Observar que

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix} = \begin{pmatrix} aa' & ab' + ba' \\ 0 & aa' \end{pmatrix} \quad \text{y si } a = \pm 1 \ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} a & -b \\ 0 & a \end{pmatrix}$$

Entonces si $A, B \in H$ entonces $AB \in H$ y $A^{-1} \in H$ y por lo tanto H es un subgrupo de $GL_2(\mathbb{R})$. Es abeliano porque

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix} = \begin{pmatrix} aa' & ab' + ba' \\ 0 & aa' \end{pmatrix} = \begin{pmatrix} a'a & a'b + b'a \\ 0 & a'a \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

B. Notemos que

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^n = \begin{pmatrix} a^n & na^{n-1}b \\ 0 & a^n \end{pmatrix}$$

Entonces $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ tiene orden 1, $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ tiene orden 2 y el resto tiene orden infinito pues si $b \neq 0$ entonces $na^{n-1}b \neq 0$ para todo $n \in \mathbb{N}$.

C. ($\Rightarrow$) Si φ es inyectivo y $g \in G_1$ tal que $g \neq e_1$, entonces $\varphi(g) \neq \varphi(e_1) = e_2$, luego $g \notin \ker(\varphi)$.
($\Leftarrow$) Recíprocamente si $\varphi(g_1) = \varphi(g_2)$ tenemos que $\varphi(g_1 g_2^{-1}) = e_2$. Por lo tanto $g_1 g_2^{-1} \in \ker(\varphi) = \{e_1\}$. Luego $g_1 g_2^{-1} = e_1$ y resulta que $g_1 = g_2$.

D. Como

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix}\right) = \varphi\begin{pmatrix} aa' & ab' + ba' \\ 0 & aa' \end{pmatrix} = \begin{cases} (\overline{0}, ab' + ba') & \text{si } aa' = 1 \\ (\overline{1}, -ab - ba') & \text{si } aa' = -1 \end{cases}$$

$$\varphi\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \varphi\begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix} = \begin{cases} (\overline{0}, b) + (\overline{0}, b') & \text{si } a = 1 \text{ y } a' = 1 \\ (\overline{0}, b) + (\overline{1}, -b') & \text{si } a = 1 \text{ y } a' = -1 \\ (\overline{1}, -b) + (\overline{0}, b') & \text{si } a = -1 \text{ y } a' = 1 \\ (\overline{1}, -b) + (\overline{1}, -b') & \text{si } a = -1 \text{ y } a' = -1 \end{cases} = \begin{cases} (\overline{0}, ab' + ba') & \text{si } aa' = 1 \\ (\overline{1}, -ab - ba') & \text{si } aa' = -1 \end{cases}$$

entonces φ es un morfismo de grupos. Notemos que $\varphi(A) = (\overline{0}, 0)$ solamente cuando $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, entonces por parte anterior φ es inyectivo. Es fácil ver que φ es sobreyectivo y por lo tanto es un isomorfismo.

Ejercicio 2.

A. Si $\varphi : G_1 \to G_2$ es un homomorfismo de grupos finitos, entonces $|G_1| = |\ker(\varphi)||\operatorname{im}(\varphi)|$.

C. Como el $\operatorname{mcd}(|\mathbb{Z}_{33}|, |G|) = 1$ el único homomorfismo posible es el homomorfismo trivial.

D. Por el teorema de órdenes para homomorfismos de grupos tenemos que $34 = |G| = |\ker(\varphi)||\operatorname{im}(\varphi)|$. Por otro lado $|\operatorname{im}(\varphi)|$ divide a 17 por ser $\operatorname{im}(\varphi)$ un subgrupo de $\mathbb{Z}_{17}$. Como φ es no trivial sabemos que $|\operatorname{im}(\varphi)| \neq 1$ y por lo tanto $|\operatorname{im}(\varphi)| = 17$. Luego $\ker(\varphi)$ es un grupo con 2 elementos.

Ejercicio 3.

A. Verdadera: Consideramos $o(x) = n$ y $o(y) = m$. Como $x * y = y * x$ tenemos que

$$(x * y)^{nm} = x^{nm} * y^{nm} = (x^n)^m * (y^m)^n = e^m * e^n = e$$

entonces $o(x * y) \leq mn$ y por lo tanto es finito.

B. Falsa: Si g es un elemento de orden $n > 1$, g^{-1} también es un elemento de orden n y $o(g * g^{-1}) = o(e) = 1 \neq n$. Por ejemplo considerar $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ en el ejercicio 1.

C. Verdadera: Igual que en la parte A. se prueba que $(x * y)^{nm} = e$. Sea d tal que $(x * y)^d = e$. Observemos que

$$e = (x^d * y^d)^n = x^{dn} * y^{dn} = y^{dn} \qquad e = (x^d * y^d)^m = x^{dm}$$

luego $m|dn$ y $n|dm$. Como $\operatorname{mcd}(n, m) = 1$ entonces por el lema de Euclides $m|d$ y $n|d$, luego como $\operatorname{mcd}(n, m) = 1$, $mn|d$. Concluimos que mn es el menor exponente d para el cual $(x*y)^d = e$ y por lo tanto $o(x * y) = o(x)o(y)$.

Ejercicio 4.

A. Haciendo las cuentas vemos que $2^{35} \equiv 1 (\operatorname{mod} 71)$. Notemos que $2^5 \equiv 32 \not\equiv 1 (\operatorname{mod} 71)$ y $2^7 \equiv 57 \not\equiv 1 (\operatorname{mod} 71)$ entonces el orden de $\overline{2}$ es 35.

B. Como $-\overline{1}$ tiene orden 2 y $\overline{2}$ tiene orden 35, $-\overline{2} = \overline{69}$ tiene orden 70 en $U(71)$ porque $\operatorname{mcd}(2, 35) = 1$. Por lo tanto 69 es raíz primitiva módulo 71.

C. Como $3^{10} \equiv 48 (\operatorname{mod} 71)$ entonces la clave es 48.

D. Notemos que $(-\overline{2})^5 = -\overline{32} = \overline{39} \neq \overline{3}$. Asi que no es posible haber considerado la raíz de la parte [B.]. (En caso de haber encontrado otra raíz en la parte [B.] se tomará en cuenta a esa raíz).