Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos y Teoría de Galois
Primer Semestre 2020

Soluciones - Práctico 2

1. (a) $\mathbb{Z}_4 \to < 2 > \to < 0 >$

   (b) $\mathbb{Z}_5 \to < 0 >$

   (c)
$$\begin{tikzcd} & < 3 > \arrow[dr] & \\ \mathbb{Z}_6 \arrow[ur] \arrow[dr] & & < 0 > \\ & < 2 > \arrow[ur] & \end{tikzcd}$$

   (d) $\mathbb{Z}_8 \to < 2 > \to < 4 > \to < 0 >$

   (e)
$$\begin{tikzcd} & < (1,0) > \arrow[dr] & \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \arrow[ur] \arrow[r] \arrow[dr] & < (0,1) > \arrow[r] & < 0 > \\ & < (1,1) > \arrow[ur] & \end{tikzcd}$$
   $\mathbb{Z}_4$ y $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ no son isomorfos porque el primero es cíclico, mientras que el segundo no.

2. - $HK < G \Longleftrightarrow HK = KH$

     $\Rightarrow$) Sea $hk \in HK$. Como es subgrupo, $(hk)^{-1} \in HK$. Pero $(hk)^{-1} = k^{-1}h^{-1} \in KH$. Finalmente, como todo elemento de HK es opuesto de algún otro elemento, se deduce que $HK \subset KH$. Para la otra inclusión, tomar $kh \in KH$, entonces $kh = (h^{-1}k^{-1})^{-1}$, que es el inverso de un elemento de HK. Por tanto, $KH \subset HK$.

     $\Leftarrow$)$e \in HK$, veamos que es cerrado por la operación del grupo. Si $hk, h'k' \in HK$, entonces $hkh'k' = hh''k''k' \in HK$, donde usamos que $kh' = h''k''$ por ser iguales $HK = KH$. Por tanto $hkh'k' \in HK$

   - Probar que $HK \subset KH \Rightarrow HK = KH$

     Sea $kh \in KH$. Entonces $h^{-1}k^{-1} \in HK \subset KH$. Esto implica que KH es cerrado bajo la operación del grupo, es decir, es subgrupo (el neutro pertence). Entonces de la parte anterior tenemos que $HK = KH$.

3. Ejercicio de Entrega

4. Por ejercicio 8 del práctico 1, $|gf| = |g||f|$. Además,

$$< f, g >= \{f^a g^b : 0 \leq a \leq |f| . 0 \leq b \leq |g|\} \tag{1}$$

   que tiene a lo sumo $|g||f|$ elementos; luego $< fg > \subset < f, g >$ y ambos tienen la misma cantidad de elementos. Por tanto fg genera $< f, g >$

5. (a) $G_0 < G \times F$, $F_0 < G \times F$ trivial de las definiciones. Los mapas $\phi_G : G \to G_0, g \mapsto (g, 1)$ y $\phi_F : F \to F_0, f \mapsto (f, 1)$ son los isomorfismos buscados, y las propiedades $G_0 \cap F_0 = \{1\}, G_0 F_0 = G \times F$ son inmediatas.

   (b) Como $G = HK$, ϕ es sobreyectiva. Para probar inyectividad: $hk = h'k' \Leftrightarrow h'^{-1}h = k'k^{-1} \Leftrightarrow h'^{-1}h, k'k^{-1} \in H \cap K = \{1\}$, por tanto $h = h'.k = k'$.

6. Ídem a ejercicio 4. Usamos $(1, 1, 1, ..., 1)$ como generador.

7. $\phi \in Aut(G) \Leftrightarrow G$ abeliano

   $fg = \phi(f^{-1})\phi(g^{-1}) = \phi(f^{-1}g^{-1}) = gf$, por tanto G abeliano.

8. Sea g tal que $G =< g >$. Consideremos $< \phi(g) >< G$. Como ϕ morfismo, $\phi(< g >) =< \phi(g) >$, por tanto la ecuación anterior resulta $\phi(G) < G$. Al ser automorfismo, es sobreyectiva; luego $\phi(G) = G$. Esto implica que $\phi(g)$ es generador.

   Recíprocamente, sea f otro generador. Definimos $\phi(1) = 1, \phi(g) = f$, y se cumplen las ecuaciones. anteriores.

9.
   - $Aut\mathbb{Z} \simeq \mathbb{Z}_2$: sea $\phi \in Aut\mathbb{Z}$. Por ejercicio anterior, $\phi(1)$ debe ser generador. Como los únicos generadores son $1, -1$ tenemos dos posibilidades. Basta ver que $\phi(1) = -1$ da lugar a un morfismo, y esto último es claro por el ejercicio 7.
   - $Aut\mathbb{Z}_n = \mathbb{Z}_n^\times$: $\phi(1)$ debe ser generador (pues 1 lo es), así que $\phi(1) = r$, con r coprimo con n (pues son números para los que el conjunto $\{r, 2r, 3r, ...nr\}$ es un conjunto completo de restos para n). Notemos por ϕ_r al morfismo que asocia $\phi(1) = r$. Entoces, veamos que $\phi_r \mapsto r \in \mathbb{Z}_n^\times$ es un morfismo biyectivo:
     - $\phi_1(1) = 1$, así que es la identidad: $\phi_1(n) = n\phi_1(1) = n$.
     - $\phi_r(\phi_s(1)) = \phi_r(s) = rs = \phi_{rs}(1)$, pues recordar que si r, s son coprimos con n, entonces rs también lo es.

     Entonces el mapa $\phi_r \mapsto r$ es un morfismo. Como la cantidad de elementos de $Aut\mathbb{Z}_n$ es la misma que la de $\mathbb{Z}_n^\times$, tenemos biyectividad.
   - $Aut\mathbb{Z}_5 \simeq \mathbb{Z}_4$: basta ver que $\mathbb{Z}_5^\times \simeq \mathbb{Z}_4$. Para esto, observar que $\mathbb{Z}_5^\times = 1, 2, 3, 4$, es cíclico, generado por el 2. Luego, como todo grupo de orden 4 cíclico es isomorfo a $\mathbb{Z}_4$ (práctico 1), se deduce que $Aut\mathbb{Z}_5 \simeq \mathbb{Z}_4$.
   - $Aut\mathbb{Z}_6 \simeq \mathbb{Z}_2$: $\mathbb{Z}_6^\times = \{1, 5\}$, grupo de orden 2, y por tanto $\mathbb{Z}_2$.
   - $Aut\mathbb{Z}_8 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$: observar que $\mathbb{Z}_8\times = \{1, 3, 5, 7\}$ no es cíclico, así que por la clasificación de grupos de orden 4 debe ser isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

10. Ejercicio de Entrega

11. (a)
    - $\phi : H/H \cap K \to G/K$ tal que $\phi(h(H \cap K)) = hK$ está bien definida. $hK = h'K$ implica que $h^{-1}h' \in K$, entonces $h^{-1}h' \in H \cap K$ y por lo tanto están en la misma coclase en $H/H \cap K$, es decir, $hH \cap K = h'H \cap K$. Esto implica que está bien definida y que es inyectiva.
    - Como la función es inyectiva, entonces $Card(G/K) > Card(H/H \cap K)$, de donde se deduce el resultado.

    (b) Basta probar que el mapa ϕ de la parte anterior es sobreyectivo sii $G = HK$.

    $\Rightarrow$) si ϕ sobreyectivo, entonces toda coclase es acanzada por la imagen de ϕ. Por tanto $G = HK$. $\Leftarrow$) si $G = HK$, cualquier coclase en G/K es de la forma hK, por tanto es alcanzado por ϕ.

12. (a) Tenemos $H \cap K < H, K < G$. Como $[G : K]$ finito, entonces $[H : K \cap H] \leq [G : K]$ finito. Además, $[G : H]$ finito. Luego, $[G : H \cap K]$ finito. Además, $[G : H \cap K] = [G : H][H : H \cap K] \leq [G : H][G : K]$.

    (b) Vale la igualdad si y sólo si (por la parte anterior saturando la igualdad) $[H : K \cap H] = [G : K]$, y esto último por el ejercicio anterior es equivalente a $G = HK$.

(c) $[G:K][K:H\cap K]=[G:H\cap K]=[G:H][H:H\cap K]$, así que $[G:H]$ y $[G:K]$ dividen a $[G:H\cap K]$. Como son coprimos, $[G:H][G:K]|[G:H\cap K]\leq[G:H][G:K]$, por tanto vale la igualdad.

13. Sea G grupo de orden 4, no cíclico. Sea $g\in G$ distinto del neutro. Por el teorema de Lagrange, $|g|=1,2,4$, pues debe ser un divisor positivo de 4. Como el grupo no es cíclico y $g\neq e$, $|g|=2$. Luego, todo elemento no neutro tiene orden 2. Pr ej. 4 del práctico 1, tenemos que el grupo es abeliano. Sea h otro elemento no nulo.

    Entonces, $2=[<h>:<h>\cap<g>]\leq[G:<g>]=2$, así que vale la igualdad, y por el ejercicio anterior $G=<h><g>$.

    Luego, Un grupo de orden 4 no cíclio es isomorfo a $\mathbb{Z}_2\times\mathbb{Z}_2$

14.

$$
\begin{tikzcd}
& <a> \arrow[dr] & & \\
Q \arrow[ur] \arrow[r] \arrow[dr] & <ab> \arrow[r] & <a^2> \arrow[r] & <0> \\
& <b> \arrow[ur] & &
\end{tikzcd}
$$

$$
\begin{tikzcd}
& <\rho> \arrow[dr] & & \\
D_4 \arrow[ur] \arrow[dr] & & <\rho^2> \arrow[dr] & \\
& <\rho^2,\sigma> \arrow[ur] \arrow[dr] & & <0> \\
& & <\sigma> \arrow[ur] &
\end{tikzcd}
$$

15. Consideremos $\phi:\mathcal{M}\to\mathbb{Z}_2$ dada por $\phi(\tau)=0$ si es directa o 1 si no es directa. Este morfismo está bien definido, gracias a las propiedades de las simetrías y la orientación de $\mathbb{R}^2$. Luego, $\hat{\phi}:\mathcal{M}/\mathcal{M}_+\to\mathbb{Z}_2$ es un automorfismo, pues es sobreyectivo y por los teoremas de isomorfismos es biyectivo ($\ker\phi=\mathcal{M}_+$).

    Si $G<\mathcal{M}$, tenemos que $\phi(G)<\mathbb{Z}_2$, de donde salen dos posibilidades:

    - $\phi(G)=0$, entonces $G<\ker\phi=\mathcal{M}_+$.
    - $\phi(G)=\mathbb{Z}_2$, entonces $p\hat{h}i:G/G\cap\mathcal{M}_+\to\mathbb{Z}_2$ es isomorfismo, de donde se deduce $[G:G\cap\mathcal{M}_+]=2$.