Certamen 1 – Estructuras Algebraicas

Profesor: Pedro Montero, Ayudante: Mateo Hidalgo

Departamento de Matemática, Universidad Técnica Federico Santa María

Problema A (25 puntos)

Sea $n \in \mathbf{N}^{\geq 2}$ fijo. El objetivo de este problema es estudiar propiedades de la **función Φ de Euler**. Para ello, puede utilizar directamente el hecho que si $a \in \{0, 1 \ldots, n-1\}$ entonces $\operatorname{ord}([a]_n) = \frac{n}{\operatorname{mcd}(a,n)}$ es el orden de $[a]_n \in \mathbf{Z}/n\mathbf{Z}$ y que $[a]_n \in (\mathbf{Z}/n\mathbf{Z})^\times$ si y sólo si $\operatorname{mcd}(a,n) = 1$, así como el siguiente hecho[1]

> **Teorema Chino del Resto:** Dado $n \in \mathbf{N}^{\geq 2}$, donde $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ descomposición en factores primos, hay un isomorfismo **de anillos** $f : \mathbf{Z}/n\mathbf{Z} \xrightarrow{\sim} (\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z}) \times \cdots \times (\mathbf{Z}/p_r^{\alpha_r}\mathbf{Z})$.

Definimos la función $\Phi : \mathbf{N}^{\geq 1} \to \mathbf{N}^{\geq 1}$ como $\Phi(1) := 1$ y para $n \geq 2$ como $\Phi(n) := |(\mathbf{Z}/n\mathbf{Z})^\times|$, es decir, es el orden del **grupo de unidades** $G_n = (\mathbf{Z}/n\mathbf{Z})^\times$ del anillo $(\mathbf{Z}/n\mathbf{Z}, +, \cdot)$ de enteros módulo n.

1. (**5 pts**) Pruebe que $\Phi(n) = \Phi(p_1^{\alpha_1}) \cdots \Phi(p_r^{\alpha_r})$, donde $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ descomposición en factores primos.
2. (**10 pts**) Pruebe que si p y q son dos números primos distintos, entonces $\Phi(pq) = (p-1)(q-1)$.

Recuerde que $\operatorname{Aut}(\mathbf{Z}/n\mathbf{Z}) = \{f : \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ automorfismo de grupo$\}$ es el grupo de automorfismos de $\mathbf{Z}/n\mathbf{Z}$. Considere el morfismo de grupos[2] $\psi : (\mathbf{Z}/n\mathbf{Z})^\times \to \operatorname{Aut}(\mathbf{Z}/n\mathbf{Z})$, $[m]_n \mapsto f_m$, donde $f_m : \mathbf{Z}/n\mathbf{Z} \xrightarrow{\sim} \mathbf{Z}/n\mathbf{Z}$ es el automorfismo dado por $f_m([a]_n) := [ma]_n$.

3. (**10 pts**) Pruebe que ψ es un **isomorfismo de grupos**.

   Indicación: Para la sobreyectividad, puede ser útil recordar que $\mathbf{Z}/n\mathbf{Z}$ es un grupo cíclico para probar que dado $f \in \operatorname{Aut}(\mathbf{Z}/n\mathbf{Z})$ se tiene que $f = f_m$. Luego, debe justificar adecuadamente que $[m]_n \in (\mathbf{Z}/n\mathbf{Z})^\times$

Problema B (55 puntos)

El objetivo de este problema es clasificar todos los grupos finitos de orden 255. Para esto, comenzaremos por estudiar la noción de *producto semi-directo* de grupos.

Sean G y H dos grupos y sea $\varphi : H \to \operatorname{Aut}(G)$ un morfismo de grupos. Denotamos $G \rtimes_\varphi H$ al conjunto $G \times H$ dotado de la ley de composición interna definida por $(g_1, h_1) \rtimes_\varphi (g_2, h_2) := (g_1 \cdot \varphi(h_1)(g_2), h_1 h_2)$. Puede usar el siguiente resultado sin demostración.

> **Hecho:** El conjunto $G \rtimes_\varphi H$ junto con la ley de composición interna antes definida es un grupo, llamado el producto semi-directo de H por G respecto a φ. En particular, se verifica que para todo $(g, h) \in G \rtimes_\varphi H$ se tiene que[3] $(g,h)^{-1} = (\varphi(h^{-1})(g^{-1}), h^{-1})$.

Note que, en particular, si $\varphi : H \to \operatorname{Aut}(G)$, $h \mapsto \operatorname{Id}_G$ es el **morfismo trivial** entonces $G \rtimes_\varphi H \cong G \times H$.

1. (**10 pts**) Probar que[4] $G \times \{e_H\} \trianglelefteq G \rtimes_\varphi H$, y que el cociente de $G \rtimes_\varphi H$ por $G \times \{e_H\}$ es isomorfo a H.

   Indicación: Es útil notar que $\varphi(e_H) = \operatorname{Id}_G$ y luego $\varphi(e_H)(g) = g$ para todo $g \in G$. Para el último isomorfismo, pruebe que la función $\psi : G \rtimes_\varphi H \to H$, $(g,h) \mapsto h$ es un morfismo de grupos.

2. (**10 pts**) Supongamos que G es un grupo y N y H son sub-grupos de G tales que $N \cap H = \{e\}$, $NH = G$ y $N \trianglelefteq G$. Considere el morfismo de grupos[5] $\varphi : H \to \operatorname{Aut}(N)$ dada por $h \mapsto \varphi_h$, con $\varphi_h(n) = hnh^{-1}$. Probar que en este caso la función $f : N \rtimes_\varphi H \to G$, $(n,h) \mapsto nh$ es un **morfismo de grupos** y es **biyectivo**.

En lo que sigue, utilizaremos lo anterior y los resultados vistos en clases para obtener la clasificación completa de grupos de orden 255. Para ello, puede usar el siguiente resultado (ver Problema A):

> Sea n un número entero positvo. Entonces $\operatorname{Aut}(\mathbf{Z}/n\mathbf{Z}) \cong (\mathbf{Z}/n\mathbf{Z})^\times$. En particular, si p y q son primos distintos, entonces $\operatorname{Aut}(\mathbf{Z}/pq\mathbf{Z}) \cong (\mathbf{Z}/(p-1)\mathbf{Z}) \times (\mathbf{Z}/(q-1)\mathbf{Z})$.

[1] La demostración hecha en clases para el caso de grupos se adapta de manera literal para el caso de anillos.

[2] No es necesario que pruebe que es un morfismo.

[3] Puesto que $(\varphi(h^{-1})(g^{-1}), h^{-1}) \cdot (g,h) \overset{\text{def}}{=} (\varphi(h^{-1})(g^{-1})\varphi(h^{-1})(g), h^{-1}h) = (\varphi(h^{-1})(g^{-1}g), e_H) = (\varphi(h^{-1})(e_G), e_H) = (e_G, e_H)$.

[4] No es necesario probar que es un subgrupo, debe probar que es un subgrupo **normal**.

[5] Bien definido, dado que $N \trianglelefteq G$.

En todo lo que sigue, consideremos G un grupo finito de orden $255 = 3 \cdot 5 \cdot 17$.

3. (**10 pts**) Sea $n_p \in \mathbf{N}$ el número de p-subgrupos de Sylow de G. Probar que $n_{17} = 1$, y que además necesariamente $n_3 = 1$ o bien $n_5 = 1$ (i.e., es **imposible que** $n_3 > 1$ y $n_5 > 1$ **simultaneamente**).

   Indicación: $5 \cdot 17 = 85 = 28 \cdot 3 + 1$ *y* $3 \cdot 17 = 51 = 10 \cdot 5 + 1$.

4. (**10 pts**) Suponga que $n_3 = 1$. Sean R el **único** 3-Sylow de G, sea S el **único** 17-Sylow de G, y sea T **alguno** de los posibles 5-Sylow de G. Probar que:

   (a) $R \times S \cong RS$ y que $RS \trianglelefteq G$.

   (b) $RS \cap T = \{e\}$ es la identidad de G.

   (c) $RST = G$.

   Indicación: Recuerde que en la Ayudantía 4 se discutió que si G es un grupo y H, K son subgrupos normales de G tales que $H \cap K = \{e\}$, entonces $HK \cong H \times K$. Justifique adecuadamente que puede usar este resultado. Para probar que $RS \trianglelefteq G$, puede notar que si $g \in G$ y $h \in RS$ entonces $\mathrm{ord}(ghg^{-1}) = \mathrm{ord}(h)$.

5. (**10 pts**) Probar, usando (2), que $G \cong RS \rtimes_\varphi T$ para algún $\varphi : T \to \mathrm{Aut}(RS)$. Deducir que φ es trivial.

   Indicación: Para la trivialidad de φ, calcule el orden de $\mathrm{Aut}(RS)$ *y note que (por Teorema de Lagrange) si $f : G_1 \to G_2$ morfismo entre grupos finitos entonces* $|\mathrm{Im}(f)|$ *divide* $|G_2|$.

6. (**5 pts**) Concluir que G es un grupo cíclico, i.e., $G \cong \mathbf{Z}/255\mathbf{Z}$.

Problema C (20 puntos)

El objetivo de este problema es resolver algunos ejercicios propuestos en clases.

1. (**10 pts**) Sea A un anillo y sea $I \subseteq A$ un ideal. Pruebe que el conjunto

$$\sqrt{I} := \{a \in A,\ a^n \in I \text{ para algún } n \geq 1\}$$

   es un ideal de A. Demuestre, usando los resultados vistos en clase, que si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ es la descomposición prima de $n \in \mathbf{N}^{\geq 1}$ y $I_n = n\mathbf{Z}$ ideal de $\mathbf{Z}$, entonces $\sqrt{I_n} = p_1 \cdots p_r \mathbf{Z}$.

   Indicación: Si lo desea, puede usar sin demostración el hecho que $p_1\mathbf{Z} \cap \cdots \cap p_r\mathbf{Z} = p_1 \cdots p_r\mathbf{Z}$.

2. (**10 pts**) Sea $\mathbf{F}_2 = (\mathbf{Z}/2\mathbf{Z}, +, \cdot)$ el cuerpo de dos elementos. Pruebe que $P = X^2 - X - 1$ es un elemento irreducible[6] del anillo $\mathbf{F}_2[X]$ y deduzca que el anillo cociente $K = \mathbf{F}_2[X]/\langle X^2 - X - 1\rangle$ es un cuerpo de 4 elementos. Escriba explícitamente la tabla de multiplicar del cuerpo K.

   Indicación: Justifique, tal como se hizo en clases, que los elementos de K son de la forma $\{0, 1, \alpha, 1 + \alpha\}$.

Mini-Bonus (3 puntos)

Clasifique, salvo isomorfismo, todos los grupos abelianos de orden $2024 = 2^3 \cdot 11 \cdot 23$.

[6] Recuerde que si k es un cuerpo, entonces $k[X]^\times = k^\times$ son los polinomios constantes no-nulos.

Bonus (7 puntos)

El objetivo de este problema es estudiar una acción explícita de un grupo finito G sobre un anillo A, y analizar el anillo de invariantes A^G. Más precisamente, consideremos el anillo $\mathbf{C}[X,Y]$ de polinomios en dos variables con coeficientes en $\mathbf{C}$ y considere la acción de $G = \mathbf{Z}/2\mathbf{Z}$ dada por $[1]_2 \cdot X := -X$ y $[1]_2 \cdot Y := -Y$.

(B1) **(2 pts)** Demuestre que el conjunto de puntos fijos $\mathbf{C}[X,Y]^{\mathbf{Z}/2\mathbf{Z}}$ es un sub-anillo de $\mathbf{C}[X,Y]$.

(B2) **(2 pts)** Pruebe la igualdad $\mathbf{C}[X,Y]^{\mathbf{Z}/2\mathbf{Z}} = \mathbf{C}[X^2, XY, Y^2]$, donde el término a la derecha es el sub-anillo de polinomios en las variables X^2, XY, Y^2.

Indicación: $P \in \mathbf{C}[X,Y]^{\mathbf{Z}/2\mathbf{Z}}$ *si y sólo si* $P(X,Y) = P(-X,-Y)$*, donde* $P = \sum_{i,j} a_{ij} X^i Y^j$.

(B3) **(3 pts)** Pruebe que hay un isomorfismo de anillos $\mathbf{C}[U,V,W]/\langle UW - V^2\rangle \cong \mathbf{C}[X,Y]^{\mathbf{Z}/2\mathbf{Z}}$.

Cultura general: Geométricamente, el Problema Bonus nos está diciendo que el cociente de la variedad álgebraica afín $\mathbf{C}^2$ por la acción del grupo $G = \mathbf{Z}/2\mathbf{Z}$ es la variedad algebraica afín

$$\mathbf{C}^2/G \cong \{(u,v,w) \in \mathbf{C}^3,\ uw = v^2\}.$$

A diferencia del plano afín $\mathbf{C}^2$, donde todo punto posee un plano tangente, el cociente $\mathbf{C}^2/G$ cumple que el punto $(u_0, v_0, w_0) = (0,0,0)$ **no posee un plano tangente** (pues la función $f(u,v,w) = uw - v^2$ tiene gradiente nulo en dicho punto), i.e., $(0,0,0) \in \mathbf{C}^2/G$ es un **punto singular**.

El estudio de cocientes de variedades algebraicas afines por grupos finitos fue la motivación original de David Hilbert para demostrar el **Teorema de la base de Hilbert** (visto en clases). De manera más general, la Teoría Geométrica de Inviariantes (GIT, en inglés) creada por David Mumford en 1965 busca estudiar cocientes en geometría por grupos más generales (no necesariamente finitos).

Nombre completo y ROL USM:

Pauta Certamen 1 – Estructuras Algebraicas

Profesor: Pedro Montero, Ayudante: Mateo Hidalgo

Departamento de Matemática, Universidad Técnica Federico Santa María

Problema A (25 puntos)

1. Dado que f es un isomorifsmo de **anillos**, induce un isomorfismo entre los grupos de unidades (visto en clases) $(\mathbf{Z}/n\mathbf{Z})^\times \xrightarrow{\sim} (\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/p_r^{\alpha_r}\mathbf{Z})^\times$ y luego sus órdenes son iguales.

2. $\mathbf{Z}/p\mathbf{Z} \overset{\text{def}}{=} \mathbf{F}_p$ es un cuerpo, i.e., $\mathbf{F}_p^\times = \mathbf{F}_p \setminus \{0\}$ tiene $p-1$ elementos, i.e., $\Phi(p) = p-1$. Concluímos por (1).

3. **Inyectividad:** $\psi(m) = \mathrm{Id}$ si y sólo si $[a]_n = [ma]_n$ para todo $[a]_n \in \mathbf{Z}/n\mathbf{Z}$. Si $[a]_n = [1]_n$ obtenemos $[m]_n = [1]_n$. **Sobreyectividad:** como $\mathbf{Z}/n\mathbf{Z}$ es cíclico, todo automorfismo f está determinado por $f([1]_n) =: [m]_n$, i.e., $f = f_m$. Como f automorfismo, $[m]_n$ tiene orden n y luego $\mathrm{mcd}(m,n) = 1$, i.e., $[m]_n \in (\mathbf{Z}/n\mathbf{Z})^\times$.

Problema B (55 puntos)

1. Consideramos la función $\psi : G \rtimes_\varphi H \to H,\ (g,h) \mapsto h$, la cual es **sobreyectiva** y verifica que $\psi((g_1,h_1) \rtimes_\varphi (g_2,h_2)) \overset{\text{def}}{=} \psi(g_1 \cdot \varphi(h_1)(g_2), h_1h_2) = h_1h_2 \overset{\text{def}}{=} \psi(g_1,h_1)\psi(g_2,h_2)$, i.e., es un **morfismo de grupos**. Para determinar su kernel, notamos que si $g \in G$ y $h \in H$ entonces $\psi(g,h) = e_H$ si y sólo si $h = e_H$ y luego $\ker(\psi) = G \times \{e_H\}$ es un **subgrupo normal**[1]. Luego, el Teorema del isomorfismo de Noether implica que ψ induce un isomorfismo $\hat{\psi} : G \rtimes_\varphi H/\ker(\psi) = (G \rtimes_\varphi H)/(G \times \{e_H\}) \xrightarrow{\sim} \mathrm{Im}(\psi) = H$.

2. Sea $f : N \rtimes_\varphi H \to G,\ (n,h) \mapsto nh$. Dados $n, n' \in N$ y $h, h' \in H$, tenemos que $f(n,h)f(n',h') = nhn'h'$. Por otra parte, $f((n,h) \rtimes_\varphi (n',h')) \overset{\text{def}}{=} f(n\varphi(h)(n'), hh') \overset{\text{def}}{=} f(nhn'h^{-1}, hh') = nhn'h^{-1}hh' = nhn'h'$, i.e., f es un morfismo de grupos. La hipótesis $NH = G$ asegura que f es sobreyectivo y la hipótesis $N \cap H = \{e\}$ asegura que $\ker(f) = \{e\}$ (pues $nh = e_H$ equivale a $n = h^{-1} \in N \cap H$). Así, f es un isomorfismo.

3. Por el Teorema de Sylow, $n_{17} \equiv 1 \mod 17$ y divide $3 \cdot 5 = 15$, i.e., $n_{17} = 1$. Del mismo modo, $n_3 \equiv 1 \mod 3$ (resp. $n_5 \equiv 1 \mod 5$) y divide a $5 \cdot 17 = 85$ (resp. $3 \cdot 17 = 51$), i.e., $n_3 \in \{1, 85\}$ y $n_5 \in \{1, 51\}$. No es posible $n_3 = 85$ y $n_5 = 51$, pues habría más de 255 elementos (e.g. al menos $85 \cdot 2$ de orden 3 y $51 \cdot 4$ de orden 5).

4. Para (a), notamos que podemos usar el resultado de la Ayudantía 4 pues $n_3 = 1$ y $n_{17} = 1$ equivalen a que R y S sean subgrupos normales y pues no tienen elementos no-triviales en común (Teorema de Lagrange). Así, $R \times S \cong RS$. Para la normalidad, notamos que si $g \in G$ y $h \in RS$, entonces $\mathrm{ord}(ghg^{-1}) = \mathrm{ord}(h) \mid 3 \cdot 17$ y por ende (Teorema de Lagrange y unicidad de dichos p-subgrupos de Sylow) necesariamente[2] $ghg^{-1} \in RS$. El mismo argumento anterior implica que $RS \cap T = \{e\}$ (i.e., (b)), y para (c) basta notar que RST tiene al menos 255 elementos y por ende es el grupo total.

5. Por (2), $G \cong RS \rtimes_\varphi T$ para cierto $\varphi : T \to \mathrm{Aut}(RS) \cong \mathrm{Aut}(R \times S) \cong \mathrm{Aut}(\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/17\mathbf{Z}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/16\mathbf{Z}$. Dado que $T \cong \mathbf{Z}/5\mathbf{Z}$, dicho φ es necesariamente trivial (sino 5 dividiría $2 \cdot 16$), y así $G \cong RS \times T$.

6. $G \cong RS \times T \cong R \times S \times T \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/17\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z} \cong \mathbf{Z}/255\mathbf{Z}$ por el Teorema Chino del Resto.

Problema C (20 puntos)

1. Sean $a, b \in \sqrt{I}$ tales que $a^n \in I$ y $b^m \in I$, y sea $c \in A$ arbitrario. Supongamos que $n \leq m$. Entonces, $(ac)^n = a^nc^n \in I$ y luego $ac \in \sqrt{I}$. Además, $(a+b)^{n+m} = \sum_{i=0}^{n+m} \lambda_i a^i b^{n+m-i}$ con $\lambda_i = \binom{n+m}{i} \in \mathbf{Z}$. Si $i \geq n$ entonces $a^i \in I$ y luego $\lambda_i a^i b^{n+m-i} \in I$, mientras que si $i \leq n$ (i.e., $-n \leq -i$) entonces $n+m-i \geq m$ y luego $b^{n+m-i} \in I$ y por ende $\lambda_i a^i b^{n+m-i} \in I$. En cualquier caso, $a+b \in \sqrt{I}$. Por último, tenemos que
$$\sqrt{I_n} = \bigcap_{I_n \subseteq p\mathbf{Z}} p\mathbf{Z} = \bigcap_{p|n \text{ primo}} p\mathbf{Z} = p_1\mathbf{Z} \cap \cdots p_r\mathbf{Z} = p_1 \cdots p_r\mathbf{Z}.$$

2. Un polinomio de grado 2 es irreducible si no tiene raíces. Como $P(0) = P(1) = -1 \neq 0$, tenemos que P es irreducible, y luego K es un cuerpo. Dado que P tiene grado 2, sus elementos son clases de equivalencia de polinomios de la forma $aX + b$ con $a, b \in \mathbf{F}_2$. Si $\alpha := [X] \in K$ entonces $K = \{0, 1, \alpha, 1+\alpha\}$. Dado que 0 y 1 son los neutros aditivos y multiplicativos, los únicos productos no-triviales son $\alpha \cdot \alpha = 1 + \alpha$, $\alpha \cdot (1+\alpha) = \alpha + \alpha^2 = 1 + 2\alpha = 1$ y $(1+\alpha)^2 = 1 + \alpha^2 = 2 + \alpha = \alpha$.

[1] Alternativamente, si $g, g' \in G$ y $h \in H$, entonces $(g,h) \rtimes_\varphi (g', e_H) \rtimes_\varphi (g,h)^{-1} \overset{\text{def}}{=} (g,h) \rtimes_\varphi (g', e_H) \rtimes_\varphi (\varphi(h^{-1})(g^{-1}), h^{-1}) \overset{\text{def}}{=} (g\varphi(h)(g'), h) \rtimes_\varphi (\varphi(h^{-1})(g^{-1}), h^{-1}) \overset{\text{def}}{=} (g\varphi(h)(g')\varphi(h)(\varphi(h^{-1})(g^{-1}), e_H) \overset{\text{def}}{=} (g\varphi(h)(g')g^{-1}, e_H) \in G \times \{e_H\}$, i.e., $G \times \{e_H\}$ normal.

[2] Alternativamente, si $r \in R$ y $s \in S$ entonces $grsg^{-1} = (grg^{-1})(gsg^{-1}) = \tilde{r}\tilde{s} \in RS$ pues R y S son subgrupos normales.