Certamen 1 Estructuras Algebraicas

Profesor: Pedro Montero, Ayudante: Cristóbal Montecino
Departamento de Matemática, Universidad Técnica Federico Santa María

Problema 1 (30 puntos)

Sea G un grupo arbitrario. Decimos que un subgrupo H de G verifica la propiedad $\mathscr{P}$ (dentro de G) si para **todo** automorfismo $\varphi : G \xrightarrow{\sim} G$ se cumple que $\varphi(H) = H$.

(a) Probar que si H satisface la propiedad $\mathscr{P}$, entonces $H \trianglelefteq G$ es un sub-grupo normal de G.

Solución: Sabemos que para todo $g \in G$ la conjugación $\varphi_g : G \xrightarrow{\sim} G,\ x \mapsto gxg^{-1}$ es un automorfismo de G. En particular, si H satisface la propiedad $\mathscr{P}$ entonces $\varphi_g(H) = H$ para todo $g \in G$ y por ende $\varphi_g(h) = ghg^{-1} \in H$ para todo $g \in G$ y todo $h \in H$. Luego, $H \trianglelefteq G$ es un sub-grupo normal.

(b) Probar que el grupo de Klein $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ posee un sub-grupo normal que **no** verifica la propiedad $\mathscr{P}$.

Solución: Dado que $G = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ es un grupo abeliano, tenemos que **todo** sub-grupo de G es normal. Por otra parte, si consideramos $H = \langle([1]_2, [0]_2)\rangle \cong \mathbf{Z}/2\mathbf{Z}$ y $\varphi : G \xrightarrow{\sim} G,\ ([x]_2, [y]_2) \mapsto ([y]_2, [x]_2)$, tenemos que $\varphi(H) \not\subseteq H$ y luego H **no** verifica la propiedad $\mathscr{P}$.

(c) Sea H un sub-grupo de G que verifica la propiedad $\mathscr{P}$ dentro de G, y sea K un sub-grupo de H que verifica la propiedad $\mathscr{P}$ dentro de H. Probar que K verifica la propiedad $\mathscr{P}$ dentro de G.

Solución: Sea $\varphi : G \xrightarrow{\sim} G$ un automorfismo de G. Dado que H verifica la propiedad $\mathscr{P}$ dentro G, tenemos que $\varphi(H) = H$ y luego la restricción $\varphi|_H : H \xrightarrow{\sim} H$ define un automorfismo de H (i.e., $\varphi|_H \in \mathrm{Aut}(H)$). Dado que K verifica la propiedad $\mathscr{P}$ dentro de H, sabemos que $\varphi|_H(K) = K$ y luego $\varphi(K) = K$, probando así lo pedido.

Cultura general: Un sub-grupo H que verifica la propiedad $\mathscr{P}$ es llamado un sub-grupo **característico** de G.

Problema 2 (30 puntos)

El objetivo de este problema es estudiar grupos abelianos finitamente generados.

(a) Clasificar todos los grupos abelianos de orden 500 módulo isomorfismo.

Indicación: Notar que si $1 < d_1 \mid d_2 \mid \cdots \mid d_s$ *entonces* d_1^s *divide al producto* $d_1 \cdots d_s$.

Solución: El teorema de estructura de grupos abelianos finitamente generados implica que todo grupo abeliano G con $|G| = 500$ puede escribirse de manera única como

$$G \cong \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z},$$

para únicos enteros positivos (factores invariantes) $1 < d_1 \mid d_2 \mid \cdots \mid d_s$ tales que $d_1 \cdots d_s = 500 = 2^2 5^3$. En particular, gracias a la indicación tenemos que d_1^s divide $2^2 5^3$ y por ende $s \leq 3$. Basta analizar todos los casos posibles:

- ✓ $s = 1$: Obtenemos $G_1 = \mathbf{Z}/500\mathbf{Z}$.
- ✓ $s = 2$ y d_1^2 divide 500: Si $d_1 = 2$, obtenemos que $G_2 = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/250\mathbf{Z}$. Si $d_1 = 5$, obtenemos que $G_3 = \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/100\mathbf{Z}$. Si $d_1 = 10$, obtenemos que $G_4 = \mathbf{Z}/10\mathbf{Z} \times \mathbf{Z}/50\mathbf{Z}$.
- ✓ $s = 3$ y d_1^3 divide 500: Necesariamente $d_1 = 5$. Repitiendo el mismo tipo de análisis para grupos abelianos de orden 100 (y restringiéndonos al caso de **dos** factores invariantes d_2 y d_3, que sean divisibles por $d_1 = 5$), o bien chequeando los posibles factores de $100 = 2^2 5^2$ divisibles por $d_1 = 5$, obtenemos $G_5 = (\mathbf{Z}/5\mathbf{Z})^2 \times \mathbf{Z}/20\mathbf{Z}$ o bien $G_6 = \mathbf{Z}/5\mathbf{Z} \times (\mathbf{Z}/10\mathbf{Z})^2$.

En conclusión, existen 6 grupos abelianos no-isomorfos de orden 500.

(b) En cada grupo obtenido en el item (a), determinar (módulo isomorfismo) todos los 2-subgrupos de Sylow.

Indicación: Puede utilizar el teorema chino del resto adecuadamente para simplificar cálculos.

Solución: Sabemos que si G un grupo abeliano finito, entonces el **único** 2-subgrupo de Sylow de G está dado por el subgrupo de 2-torsión dado por

$$T_2(G) := \left\{ g \in G \text{ tal que existe } n \in \mathbf{N}^{\geq 1} \text{ con } 2^n g \overset{\text{def}}{=} \sum_{j=1}^{2^n} g = 0 \right\}.$$

En otras palabras, el subgrupo de elementos cuyo orden es una potencia de 2. Para calcular $T_2(G)$ en cada caso del ítem (a), utilizamos el teorema chino del resto:

- ✓ $G_1 \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/25\mathbf{Z}$ y luego $T_2(G_1) \cong \mathbf{Z}/4\mathbf{Z}$.
- ✓ $G_2 \cong (\mathbf{Z}/2\mathbf{Z})^2 \times \mathbf{Z}/125\mathbf{Z}$ y luego $T_2(G_2) \cong (\mathbf{Z}/2\mathbf{Z})^2$.
- ✓ $G_3 \cong \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/25\mathbf{Z}$ y luego $T_2(G_3) \cong \mathbf{Z}/4\mathbf{Z}$.
- ✓ $G_4 \cong (\mathbf{Z}/2\mathbf{Z})^2 \times \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/25\mathbf{Z}$ y luego $T_2(G_4) \cong (\mathbf{Z}/2\mathbf{Z})^2$.
- ✓ $G_5 \cong (\mathbf{Z}/5\mathbf{Z})^3 \times \mathbf{Z}/4\mathbf{Z}$ y luego $T_2(G_5) \cong \mathbf{Z}/4\mathbf{Z}$.
- ✓ $G_6 \cong (\mathbf{Z}/5\mathbf{Z})^3 \times (\mathbf{Z}/2\mathbf{Z})^2$ y luego $T_2(G_6) \cong (\mathbf{Z}/2\mathbf{Z})^2$.

(c) Sea G un subgrupo finito de $\mathrm{GL}_n(\mathbf{Q})$, y consideremos el subgrupo de $(\mathbf{Q}^n, +)$ dado por

$$H := \{Av,\ A \in G \text{ y } v \in \mathbf{Z}^n\} \subseteq \mathbf{Q}^n.$$

Probar que H es un grupo libre finitamente generado.

Indicación: Primero pruebe que es finitamente generado, y luego que es libre.

Solución: El grupo abeliano H está generado por los elementos de la forma Ae_i, donde $(e_1, \ldots, e_n)$ es la base canónica de $\mathbf{Z}^n$ y A es un elemento del grupo *finito* G. Luego, H es finitamente generado. El teorema de estructura de grupos abelianos finitamente generados implica que

$$H \cong \mathbf{Z}^r \times \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z},$$

para únicos enteros $r \in \mathbf{N}$ (rango) y $1 < d_1 \mid d_2 \mid \cdots \mid d_s$ (factores invariantes). Sin embargo, como H es subgrupo de $(\mathbf{Q}^n, +)$, no puede contener elementos no-nulos de orden finito. En otras palabras, $s = 0$ y luego $H \cong \mathbf{Z}^r$ es libre finitamente generado.

Problema 3 (40 puntos)

El objetivo de este problema es estudiar una representación explícita del grupo simétrico S_3, así como también su representación dual.

(a) Sea G un grupo finito arbitrario y $\rho_V : G \to \mathrm{GL}(V)$, $g \mapsto \rho_g$ una representación. Recordemos que la **representación dual** de ρ_V está dada por[1]

$$\rho_{V^*} : G \longrightarrow \mathrm{GL}(V^*),\ g \mapsto \rho_{V^*}(g) := {}^t\rho_g^{-1}.$$

Sea $W \subseteq V$ un sub-espacio G-invariante respecto a ρ_V. Probar que el sub-espacio[2]

$$W^\circ := \{\ell \in V^* \text{ tal que } \ell(w) = 0 \text{ para todo } w \in W\}$$

es un sub-espacio G-invariante respecto a ρ_{V^*}. Deducir que ρ_V irreducible si y sólo si ρ_{V^*} es irreducible.

Solución: Sea $W \subseteq V$ un sub-espacio G-invariante respecto a ρ_V, i.e., $\rho_g(w) \in W$ para todo $w \in W$ y todo $g \in G$. Para probar que $W^\circ \subseteq V^*$ es G-invariante respecto a ρ_{V^*} consideremos $\ell \in W^\circ$ y $g \in G$ arbitrarios y calculamos

$$\rho_{V^*,g}(\ell) \overset{\text{def}}{=} {}^t\rho_g^{-1}(\ell) \overset{\text{def}}{=} \ell \circ \rho_g^{-1} = \ell \circ \rho_{g^{-1}},$$

por lo que $(\rho_{V^*,g}(\ell))(w) = \ell(\rho_{g^{-1}}(w)) = 0$, puesto que $\rho_{g^{-1}}(w)) \in W$ y $\ell \in W^\circ$. En otras palabras, $\rho_{V^*,g}(\ell) \in W^\circ$ para todo $\ell \in W^\circ$ y todo $g \in G$, i.e., $W^\circ \subseteq V^*$ es G-invariante respecto a ρ_{V^*}. Recíprocamente, por dualidad, tenemos que si $W^\circ \subseteq V^*$ es G-invariante respecto a ρ_{V^*} entonces $(W^\circ)^\circ = W$ es un sub-espacio G-invariante respecto a ρ_V.

---

[1] Recordemos que si $u : V \to V$ es una aplicación lineal, entonces la aplicación transpuesta ${}^tu : V^* \to V^*$ está definida por ${}^tu(\ell) := \ell \circ u$ para todo $\ell \in V^*$, i.e., ${}^tu(\ell)(v) = \ell(u(v))$ para todo $\ell \in V^*$ y todo $v \in V$. Ver también aquí.

[2] Puede usar directamente, sin demostración, el hecho que $\dim_{\mathbf{C}}(W) + \dim_{\mathbf{C}}(W^\circ) = \dim_{\mathbf{C}}(V) = \dim_{\mathbf{C}}(V^*)$ y que $(W^\circ)^\circ = W$ si identificamos V y con su bidual V^{**}. Ver aquí para más detalles.

Finalmente, ρ_V es irreducible si y sólo si todo sub-espacio $W \subseteq V$ que es G-invariante cumple $W = \{0\}$ o bien $W = V$. Equivalentemente, W verifica $\dim_{\mathbf{C}}(W) = 0$ o bien $\dim_{\mathbf{C}}(W) = \dim_{\mathbf{C}}(V)$. Esto último equivale a su vez a que $\dim_{\mathbf{C}}(W^\circ) = \dim_{\mathbf{C}}(V^*)$ o bien $\dim_{\mathbf{C}}(W^\circ) = 0$, respectivamente. Así, concluímos que ρ_V irreducible si y sólo si ρ_{V^*} es irreducible.

(b) En todo lo que sigue, consideremos $G = S_3$. Sea

$$V := \{(x_1, x_2, x_3) \in \mathbf{C}^3 \text{ tal que } x_1 + x_2 + x_3 = 0\} \cong \mathbf{C}^2$$

con base $e_1 = (1, -1, 0)$ y $e_2 = (0, 1, -1)$, y sea $\rho_V = \rho : S_3 \to \mathrm{GL}(V) \cong \mathrm{GL}_2(\mathbf{C})$, $\sigma \mapsto \rho_\sigma$ la representación dada por $\rho_\sigma(x_1, x_2, x_3) := (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$. Demuestre que ρ es una representación irreducible.

Indicación: Para calcular $\langle \chi, \chi \rangle$, notar que el valor de $\chi(\sigma)$ sólo depende de la clase de conjugación de σ. Además, puede usar la representación de permutación $\rho_{\text{perm}} = \rho_{\text{trivial}} \oplus \rho_V$ o bien usar la base (e_1, e_2).

Solución: Sabemos que ρ_V es irreducible si y sólo si $\langle \chi_V, \chi_V \rangle = 1$. Además, $\chi = \chi_V$ es una función central, i.e., el valor $\chi(\sigma)$ sólo depende de la clase de conjugación de $\sigma \in S_3$. Por otro lado, sabemos que hay exactamente 3 clases de conjugación en S_3 (que corresponden a particiones del entero 3):

$$e = \{\mathrm{Id}\},\ t = \{(1,2), (1,3), (2,3)\} \text{ y } c = \{(2,3,1), (3,1,2)\},$$

donde $\chi(e) = \dim_{\mathbf{C}}(V) = 2$. Luego, basta calcular $\chi(t) = \chi((1,2))$ y $\chi(c) = \chi((2,3,1))$ para determinar el caracter χ:

- ✓ $\sigma = (1,2)$: Considerando la base (e_1, e_2), notamos que $\rho_\sigma(e_1) = (-1, 1, 0) = e_1$ y $\rho_\sigma(e_2) = (1, 0, -1) = e_1 + e_2$. Luego,
$$R_\sigma = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$
y por ende $\chi(t) = \mathrm{tr}(R_\sigma) = 0$. Alternativamente, considerando $\rho_{\text{perm}} = \rho_{\text{trivial}} \oplus \rho_V$, tenemos que $\chi_{\text{perm}} = \chi_{\text{trivial}} + \chi_V = 1 + \chi$. Dado que $\chi_{\text{perm}}(t) = 1$, tenemos que $\chi(t) = 0$.
- ✓ $\sigma = (2,3,1)$: Considerando la base (e_1, e_2), notamos que $\rho_\sigma(e_1) = (0, 1, -1) = e_1$ y $\rho_\sigma(e_2) = (-1, 0, 1) = -e_1 - e_2$. Luego,
$$R_\sigma = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$
y por ende $\chi(c) = \mathrm{tr}(R_\sigma) = -1$. Alternativamente, considerando $\rho_{\text{perm}} = \rho_{\text{trivial}} \oplus \rho_V$, tenemos que $\chi_{\text{perm}} = \chi_{\text{trivial}} + \chi_V = 1 + \chi$. Dado que $\chi_{\text{perm}}(c) = 0$, tenemos que $\chi(c) = -1$.

Finalmente, calculamos

$$\langle \chi, \chi \rangle \overset{\text{def}}{=} \frac{1}{|S_3|} \sum_{\sigma \in S_3} \chi(\sigma)\overline{\chi(\sigma)} = \frac{1}{6} \sum_{\sigma \in S_3} |\chi(\sigma)|^2 = \frac{1}{6}(2^2 + 3 \cdot 0^2 + 2 \cdot (-1)^2) = 1.$$

Así, tenemos que ρ_V es irreducible.

(c) ¿Es ρ_V isomorfa a su representación dual ρ_{V^*}?

Solución: Los cálculos del ítem (b) implican que $\chi_{V^*} = \overline{\chi_V} = \chi_V$ pues $\chi_V(\sigma) \in \mathbf{R}$ para todo $\sigma \in S_3$. Por otra parte, sabemos que $\chi_{V^*} = \chi_V$ si y sólo si $\rho_{V^*} \cong \rho_V$.

(d) Sea $V_0 := V \otimes V$, ¿Cuántas veces aparece ρ_V en ρ_{V_0}?. En otras palabras, si

$$V_0 \cong W_1 \oplus \cdots \oplus W_m$$

es la descomposición en sub-representaciones irreducibles, ¿cuántos W_i tales que $W_i \cong V$ aparecen?.

Solución: Sabemos que la representación irreducible ρ_V aparece exactamente $\langle \chi_{V_0}, \chi_V \rangle$ veces en V_0. Además, sabemos que $\chi_{V_0} \overset{\text{def}}{=} \chi_{V \otimes V} = \chi_V^2$, por lo que calculamos

$$\langle \chi_{V_0}, \chi_V \rangle \overset{\text{def}}{=} \frac{1}{|S_3|} \sum_{\sigma \in S_3} \chi_V^2(\sigma)\overline{\chi_V(\sigma)} = \frac{1}{6} \sum_{\sigma \in S_3} \chi_V^3(\sigma) = \frac{1}{6}(2^3 + 3 \cdot 0^3 + 2 \cdot (-1)^3) = 1,$$

y concluímos así que existe exactamente **un** W_i tal que $W_i \cong V$.

Bonus (20 puntos)

El objetivo de este problema es dar una demostración, usando acciones de grupos, del hecho que si $p \geq 3$ es un número primo con $p \equiv 1 \mod 4$ entonces p es suma de dos cuadrados (cf. Tarea 1). Para esto, consideremos el conjunto finito no-vacío dado por

$$X := \{\mathbf{x} = (x, y, z) \in \mathbf{N}^3 \text{ tal que } x^2 + 4yz = p\},$$

y definamos la función $\varphi : X \to X$ dada por[3]

$$\varphi(x, y, z) := \begin{cases} (x + 2z, z, y - x - z) & \text{si } x < y - z, \\ (2y - x, y, x - y + z) & \text{si } y - z < x < 2y, \\ (x - 2y, x - y + z, y) & \text{si } x > 2y. \end{cases}$$

(a) Probar que $\varphi \circ \varphi = \mathrm{Id}_X$ y probar que φ posee un único punto fijo (i.e., existe un único $\mathbf{x}_0 = (x_0, y_0, z_0)$ tal que $\varphi(\mathbf{x}_0) = \mathbf{x}_0$).

Indicación: Para probar que φ posee un único punto fijo será necesario utilizar el hecho que p es primo y que $p = 4k + 1$ para un único entero $k \in \mathbf{N}^{\geq 1}$.

Solución: Para verificar que para todo $\mathbf{x} = (x, y, z) \in X$ se tiene que $\varphi(\varphi(x, y, z)) = (x, y, z)$ consideramos los 3 casos posibles para la definición de φ:

- ✓ $x < y - z$: En este caso $\varphi(x, y, z) = (a, b, c)$ con $a = x + 2z$, $b = z$ y $c = y - x - z$. Notamos que $a > 2b$ (pues en caso de igualdad, tendríamos que $x = 0$ y luego $p = 4yz$ sería múltiplo de 4) y luego $\varphi(a, b, c) \overset{\text{def}}{=} (a - 2b, a - b + c, b) = (x, y, z)$.
- ✓ $y - z < x < 2y$: En este caso $\varphi(x, y, z) = (a, b, c)$ con $a = 2y - x$, $b = y$ y $c = x - y + z$. Luego, $b - c = 2y - x - z$ y $2b = 2y$, por lo que $b - c < a$ y $a < 2b$ (pues los casos de igualdad quedan excluidos por definición de X, ver el pie de página). Así, $\varphi(a, b, c) \overset{\text{def}}{=} (2b - a, b, a - b + c) = (x, y, z)$.
- ✓ $x > 2y$: En este caso $\varphi(x, y, z) = (a, b, c)$ con $a = x - 2y$, $b = x - y + z$ y $c = y$. Luego, $b - c = x - 2y + z$, por lo que $a < b - c$ (pues en caso de igualdad, tendríamos que $z = 0$ y luego $p = x^2$ no sería primo). Así, $\varphi(a, b, c) \overset{\text{def}}{=} (a + 2c, c, b - a - c) = (x, y, z)$.

Así, concluímos que $\varphi \circ \varphi = \mathrm{Id}_X$.

Para estudiar los puntos fijos de φ consideramos $\mathbf{x} = (x, y, z) \in X$ y notamos que, por definición de φ, si $x < y - x$ (resp. $x > 2y$) y $\varphi(x, y, z) = (x, y, z)$ entonces necesariamente $z = 0$ (resp. $y = 0$), de donde obtendríamos que $p = x^2$ no es número primo. Luego, sólo hay que considerar el caso $y - x < x < 2y$, donde notamos que $(x, y, z) = \varphi(x, y, z) \overset{\text{def}}{=} (2y - x, y, x - y + z)$ equivale a que $x = y$. Finalmente, si $(x, x, z) \in X$ entonces $p = x^2 + 4xz = x(4z + x)$, y esto último equivale a que $x = 1$ y $p = 4z + x = 4z + 1$ (pues p es un número primo). Por otro lado, $p \equiv 1 \mod 4$ implica que existe un único $k \in \mathbf{N}^{\geq 1}$ tal que $p = 4k + 1$ y por ende $\mathbf{x_0} = (1, 1, k) \in X$ es el **único** punto fijo de φ.

(b) Probar que $|X| := \mathrm{card}(X)$ es impar.

Indicación: Considerar el 2-grupo $G = \mathbf{Z}/2\mathbf{Z} \cong \langle\varphi\rangle \subseteq \mathrm{Biy}(X)$ que actúa en X vía φ, i.e., $[1]_2 \cdot \mathbf{x} := \varphi(\mathbf{x})$.

Solución: Como G es un 2-grupo que actúa en X vía φ, tenemos que

$$|X^G| \equiv |X| \mod 2.$$

Por otro lado, $|X^G| \overset{\text{def}}{=} \mathrm{card}(\{\mathbf{x} \in X \text{ tal que } \varphi(\mathbf{x}) = \mathbf{x}\}) = 1$, gracias al ítem (a). Luego, $|X| \equiv 1 \mod 2$, i.e., $|X|$ es impar.

(c) Probar que la función $\psi : X \to X$, $(x, y, z) \mapsto (x, z, y)$ posee al menos un punto fijo.

Indicación: Considerar el 2-grupo $H = \mathbf{Z}/2\mathbf{Z} \cong \langle\psi\rangle \subseteq \mathrm{Biy}(X)$ que actúa en X vía ψ, i.e., $[1]_2 \cdot \mathbf{x} := \psi(\mathbf{x})$.

Solución: La función ψ verifica (por definición de X) que $\psi(X) \subseteq X$ y $\psi \circ \psi = \mathrm{Id}_X$. Así, ella define una acción del 2-grupo $H \cong \mathbf{Z}/2\mathbf{Z}$ en X. En particular,

$$|X^H| \equiv |X| \mod 2.$$

Por otro lado, $|X| \equiv 1 \mod 2$ gracias al ítem (b), y luego $|X^H| \overset{\text{def}}{=} \mathrm{card}(\{\mathbf{x} \in X \text{ tal que } \psi(\mathbf{x}) = \mathbf{x}\}) \geq 1$. En otras palabras, ψ posee al menos un punto fijo.

[3] Puede utilizar, sin demostración, el hecho que efectivamente $\varphi(X) \subseteq X$ y que los casos $x = y - z$ o $x = 2y$ no pueden ocurrir pues $p = x^2 + 4yz$ es primo.

(d) Concluir que si $p \equiv 1 \mod 4$ entonces existen $u, v \in \mathbf{N}$ tales que $p = u^2 + v^2$.

Solución: Sea $\mathbf{x}_0 = (x_0, y_0, y_0) \in X$ el punto fijo de ψ obtenido en el ítem (c). Por definición de X, tenemos que $p = x_0^2 + 4y_0^2$. Luego, $p = u^2 + v^2$ con $(u, v) = (x_0, 2y_0) \in \mathbf{N}^2$, demostrando lo pedido.

Cultura general:[4] La demostración presentada en la Tarea 1 es una adaptación de Euler (1747) a ideas de Fermat (1640). La demostración presentada en el Certamen 1 fue descubierta por Zagier (1990).

Mini-bonus (1 punto)

Sea $R = x_1x_2x_3x_4x_5x_6x_7x_8$ un número entero positivo de 8 dígitos, donde $x_i \in \{0, \ldots, 9\}$ es el i-ésimo dígito, y sea

$$V := 3x_1 + 2x_2 + 7x_3 + 6x_4 + 5x_5 + 4x_6 + 3x_7 + 2x_8 \in \mathbf{N}.$$

Consideremos el grupo finito $(\mathbf{Z}/11\mathbf{Z}, +)$, cuyos elementos denotaremos

$$0 := [0]_{11}, 1 := [1]_{11}, \ldots, 9 := [9]_{11}, \mathrm{K} := [10]_{11}.$$

Verificar que si R es el entero positivo formado por los primeros 8 dígitos de su RUT, entonces el dígito verificador (que viene luego del guión) está dado por $[-V]_{11} \in \mathbf{Z}/11\mathbf{Z}$, usando la notación anterior.

Observación: Puede determinar V con una calculadora, pero justifique el cálculo de $[-V]_{11}$.

Solución: Consideremos el RUT de la Universidad, dado por 81.668.700–4. Así, sus primeros 8 dígitos están dados por $R = 81668700$, de donde calculamos $V = 172$. Finalmente, $-V - 4 = -176 = -16 \cdot 11$, de donde comprobamos que $[-V]_{11} = 4$.

[4] Ver el libro «*Primes of the form $x^2 + ny^2$*» por David A. Cox (2013) para una discusión más detallada.