Tarea 1 Estructuras Algebraicas

Pedro Montero

Departamento de Matemática, Universidad Técnica Federico Santa María

En cada sección, debe **escoger solamente un ejercicio** (a, b, c o d) para resolver.

1. **Grupos, sub-grupos y generadores (10 pts).**

   (a) Sea k un cuerpo y $n \geq 1$. Determinar el centro del grupo $\mathrm{GL}_n(k)$.

   (b) Sea $n \geq 3$. Determinar el centro del grupo diedral D_n de $2n$ elementos.

   (c) Sea $f : G \to G'$ un morfismo de grupos y sea $x \in G$ un elemento de orden finito. Probar que $f(x)$ es de orden finito y que dicho orden divide al orden de x.

   (d) Probar que **no** existe $f : (\mathbb{Q}, +) \twoheadrightarrow (\mathbb{Q}^{>0}, \times)$ morfismo de grupos sobreyectivo.

2. **Clases laterales y sub-grupos normales (10 pts).**

   (a) Sea G un grupo finito. Probar que si H es un subgrupo de G y si K es un subgrupo de H, entonces

   $$[G : K] = [G : H][H : K].$$

   (b) Sea G un grupo finitamente generado y sea $H \leq G$ un subgrupo de índice finito. Probar que H es finitamente generado.
   Indicación: Si $a_1, \ldots, a_m \in G$ son generadores, y si $g_1 H, \ldots, g_n H$ son todas las clases laterales izquierdas, donde $g_1 = e$, probar que el conjunto finito $H \cap \{g_i^{-1} a_k g_j,\ 1 \leq k \leq m, 1 \leq i, j \leq m\}$ genera H.

   (c) Probar que $|\,\mathrm{SL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-2})p^{n-1}$.
   Indicación: Primero determinar el valor de $|\,\mathrm{GL}_n(\mathbb{F}_p)|$ y luego utilizar el Teorema de Lagrange.

   (d) Sea G un grupo y sean $H \trianglelefteq G,\ K \trianglelefteq G$ subgrupos normales. Probar que si $HK = G$ y $H \cap K = \{e\}$, entonces G es isomorfo a $H \times K$.

3. **Acciones de grupos (10 pts).**

   (a) Sea S un subconjunto (no necesariamente un subgrupo) no-vacío de un grupo finito G, y recordemos que $N_G(S) := \{g \in G \mid gSg^{-1} = S\}$ y $C_G(S) := \{g \in G \mid \forall s \in S, gsg^{-1} = s\}$ denotan el normalizador y centralizador de S en G, respectivamente. Probar que $N_G(S) \leq G$ es un subgrupo y que $C_G(S) \trianglelefteq N_G(S)$ es un subgrupo normal.

   (b) Sea G un grupo finito. Probar que elementos conjugados de G tienen el mismo orden. ¿Es cierto que si dos elementos de un grupo G tienen el mismo orden entonces son conjugados?

   (c) Sea G un grupo finito y sea p el número primo más pequeño que divide $|G|$. Probar que todo subgrupo de G de índice p es normal en G.
   Indicación: Sea $H \leq G$ con $[G : H] = p$. Considerar la acción de G en $X := G/H$ por multiplicación izquierda, y probar que la restricción a H induce una acción de H sobre el conjunto $\widetilde{X} := X \setminus \{H\}$. Probar que esta última acción es trivial y deducir a partir de esto que H es normal.

   (d) Sea G un grupo finito actuando fiel y transitivamente sobre un conjunto finito X, tal que $\mathrm{card}(X) = p$ es un número primo. Sea $H \trianglelefteq G$ un subgrupo normal tal que $H \neq \{e\}$, probar que H actúa transitivamente en X.

4. **p-grupos y Teorema de Sylow (10 pts).**

   (a) Sean p y q números primos y sea G un grupo de orden pq. Probar que G **no** es simple.

   (b) Probar que **no** existen grupos simples de orden 1,000,000.

   (c) Sea G un grupo finito y sea H un subgrupo de G. Sea p un número primo que divide el orden de H. Probar que el número de p-subgrupos de Sylow de H es menor o igual al número de p-subgrupos de Sylow de G.
   Indicación: Probar que un p-subgrupo de Sylow de G contiene a lo más un p-subgrupo de Sylow de H.

   (d) Sea G un grupo finito y $H \trianglelefteq G$ un subgrupo normal. Sea p un número primo que divide el orden de G/H. Probar que para todo p-subgrupo de Sylow S de G, la imagen de S por la proyección canónica $\pi : G \twoheadrightarrow G/H$ es un p-subgrupo de Sylow de G/H.

5. **Teorema chino del resto (10 pts).**

(a) Supongamos que tenemos un número desconocido N de objetos, con $N \leq 100$. Si los contamos en grupos de a 3 sobran 2, si los contamos en grupos de a 5 sobran 3, y si los contamos en grupos de a 7 sobran 2. ¿Cuántos objetos hay?

(b) Sean $n, m \in \mathbb{N}^{\geq 1}$ dos enteros positivos arbitrarios (no necesariamente primos entre sí), y consideremos el morfismo de grupos

$$\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z},\ x \mapsto ([x]_n, [x]_m).$$

Determinar $\ker(\varphi)$ y el orden del grupo cociente $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})/\operatorname{Im}(\varphi)$.

(c) Demostrar usando el Teorema chino del resto[1] que $n^7 \equiv n \mod 42$ para todo $n \in \mathbb{Z}$.
Indicación (pequeño teorema de Fermat): Probar (e.g. usando el Teorema de Lagrange) que si p es un número primo, entonces $n^{p-1} \equiv 1 \mod p$ para todo $n \in \mathbb{Z}$, pues $\mathbb{F}_p^\times$ es un grupo con $p-1$ elementos.

(d) Utilizar el Teorema chino del resto para calcular los últimos dos dígitos de 74^{540}.

6. **Grupos abelianos finitamente generados (10 pts).**

(a) Probar que los grupos $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ y $\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ son isomorfos.

(b) Determinar todos los grupos abelianos de orden 360.

(c) Se define el **exponente** de un grupo finito como el mínimo común múltiplo de los órdenes de sus elementos. Probar que si G es un grupo abeliano finito, entonces existe un elemento de G cuyo orden es igual al exponente de G.

(d) Sea G un subgrupo finito de $\mathrm{GL}_n(\mathbb{Q})$, y definamos

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

Probar que H es un grupo libre y finitamente generado.

7. **Grupos simples y series de composición (10 pts).**

(a) Sea G un grupo abeliano finitamente generado (no necesariamente finito). Probar que G es simple si y sólo si $G \cong \mathbb{Z}/p\mathbb{Z}$ para cierto primo p.

(b) Decimos que un grupo finito G es **resoluble** si los factores simples de G son grupos abelianos[2]. Probar que si $|G| = pq$ es producto de dos números primos p y q, entonces G es resoluble.

(c) Sea G un grupo finito y $H \trianglelefteq G$ un subgrupo normal. Probar que G admite una serie de composición

$$G =: G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_r = \{e\}$$

tal que $H = G_i$ para cierto $i \in \{0, \ldots, r\}$.
Indicación: Probar que si $K \trianglelefteq L \trianglelefteq G/H$, entonces $\pi^{-1}(L)/\pi^{-1}(K) \cong L/K$, donde $\pi : G \to G/H$ es la proyección al cociente. Para esto último, determinar el kernel de la composición $\pi^{-1}(L) \twoheadrightarrow L \twoheadrightarrow L/K$.

(d) Sea $n \in \mathbb{N}^{\geq 1}$ un entero. Describir todas las series de composición (módulo equivalencia) de $\mathbb{Z}/n\mathbb{Z}$.

Finalmente, debe **escoger sólamente un problema** (A, B o C) para resolver.

Problema A (30 pts).

El objetivo de este problema es utilizar la fórmula de clases para contar objetos. Más precisamente, consideremos el conjunto X cuyos elementos son collares de 9 perlas, de las cuales 4 son azules, 3 son blancas y 2 son rojas.

Supongamos que cada collar en X forma un polígono regular de 9 lados, cuyos vértices $v_1, \ldots, v_9$ corresponden a las perlas. Decimos que dos collares son equivalentes si podemos obtener uno a partir de otro efectuando simetrías del polígono regular que forman, i.e., X está dotado de una acción del grupo diedral[3] D_9. El objetivo de este problema es determinar todos los posibles collares no-equivalentes, i.e., el cardinal de X/G (que denotaremos $|X/G|$).

1. Sea G un grupo finito actuando sobre un conjunto finito X, y definamos para cada $g \in G$ el conjunto

$$\mathrm{Fix}(g) := \{x \in X \mid g \cdot x = x\},$$

[1] Recordar que si n y m son primos entre sí, entonces hay un isomorfismo **de anillos** $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n$.

[2] En particular, ellos deben ser necesariamente grupos cíclicos de orden primo.

[3] Generado por la rotación r de $\frac{2\pi}{9}$ en torno al centro del collar, y por la reflexión s respecto al eje formado por el centro del collar y el vértice v_1.

cuyo cardinal denotaremos $|\operatorname{Fix}(g)|$. Probar que

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|.$$

Indicación: Considerar el conjunto $Y := \{(g, x) \in G \times X \mid g \cdot x = x\}$ *y calcular su cardinal de dos formas diferentes. Más precisamente, probar que el cardinal de* Y *está dado por* $\sum_{g \in G} |\operatorname{Fix}(g)|$ *y por* $\sum_{x \in X} |G_x|$.

2. En el contexto del enunciado, calcular $|\operatorname{Fix}(g)|$ para cada $g \in D_9$.
Indicación: Tratar por separado el caso $g = r^k$ *según si* k *es relativamente primo a* 9 *o no. Probar que si* $g = r^k s$ *entonces* $|\operatorname{Fix}(g)| = 12$.

3. Probar que el cardinal de X es 1260 y deducir que hay exactamente 76 collares no-equivalentes en X.

Problema B (30 pts).

El objetivo de este problema es estudiar en detalle algunas propiedades del **producto semi-directo**, definido de la manera siguiente: 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 $(g_1, h_1) \rtimes_\varphi (g_2, h_2) := (g_1 \cdot \varphi(h_1)(g_2), h_1 h_2)$.

1. Demostrar que $G \rtimes_\varphi H$ es un grupo, llamado el producto semi-directo de H por G respecto a φ.

2. Probar que $G \times \{e_H\} \trianglelefteq G \rtimes_\varphi H$ y que $\{e_G\} \times H \leq G \rtimes_\varphi H$.

3. Probar que el cociente de $G \rtimes_\varphi H$ por $G \times \{e_H\}$ es isomorfo a H.

Problema C (30 pts).

Sea k un cuerpo. El objetivo de este ejercicio es probar todo subgrupo finito G del grupo (abeliano) multiplicativo $k^\times$ es necesariamente cíclico. Para esto, podremos usar directamente (sin demostración) el hecho que la ecuación $x^n = 1$ posee a lo más n soluciones en k.

Sea $G \leq k^\times$ un subgrupo finito, y denotemos por $g \in G$ un elemento de orden maximal $\operatorname{ord}(g) = d$.

1. Sea h un elemento arbitrario de G y sea $e = \operatorname{ord}(h)$. Supongamos que e **no** divide a d y consideremos $q = p^\alpha$ una potencia de un número primo que divida a e pero no divida a d. Si denotamos por r al orden del elemento $x := gh^{e/q} \in G$, probar que q divide a $\operatorname{mcm}(d, r)$, probar que r es divisible por $\operatorname{mcm}(d, r)$, y obtener una contradicción.
Indicación: Calcular $(h^{er/q})^{d/\operatorname{mcd}(d,r)}$. *Recordar que* $\operatorname{mcd}(d, r) = dr/\operatorname{mcm}(d, r)$.

2. Deducir del punto anterior que e divide a d y que g genera a G. En particular, $G \cong \mathbb{Z}/d\mathbb{Z}$.

3. Usar lo anterior para probar que $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ y que todo subgrupo finito del círculo unitario complejo $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ es cíclico.

Bonus (20 puntos): El objetivo de este problema es caracterizar los números primos que pueden escribirse como suma de dos cuadrados. Notamos que $2 = 1^2 + 1^2$, por lo que consideramos números primos $p \geq 3$ de aquí en adelante.

(i) Probar que si $p = x^2 + y^2$ para ciertos $x, y \in \mathbb{Z}$ entonces $p \equiv 1 \mod 4$.

Para probar que todo primo $p \geq 3$ tal que $p \equiv 1 \mod 4$ es necesariamente la suma de dos cuadrados, dividiremos la demostración en dos etapas:

Descenso: Si p divide $x^2 + y^2$ para ciertos $x, y \in \mathbb{Z}$ con $\mathrm{mcd}(x, y) = 1$, entonces $p = u^2 + v^2$ para ciertos enteros $u, v \in \mathbb{Z}$.

Reciprocidad: Si $p \equiv 1 \mod 4$, entonces p divide $x^2 + y^2$ para ciertos $x, y \in \mathbb{Z}$ con $\mathrm{mcd}(x, y) = 1$.

Comencemos por probar la etapa de **descenso**. Para ello, primero veamos que si $N = a^2 + b^2$ con $a, b \in \mathbb{Z}$ tales que $\mathrm{mcd}(a, b) = 1$, y si suponemos que existe un primo $q = x^2 + y^2$ para ciertos $x, y \in \mathbb{Z}$ tal que q divide N, entonces N/q también es suma de dos cuadrados de enteros relativamente primos:

(ii) Probar que $x^2N - a^2q = (xb - ay)(xb + ay)$. En particular, cambiando a por $-a$ si fuese necesario, podemos suponer que q divide $xb - ay$ (i.e., $xb - ay = dq$ para cierto $d \in \mathbb{Z}$). Probar que en tal caso x divide $a + dy$.
Indicación: Como x e y son relativamente primos, x divide $a + dy$ si y sólo si divide $(a + dy)y$.

(iii) Con la notación de (ii), si escribimos $a + dy = cx$ para cierto $c \in \mathbb{Z}$, probar que $b = dx + cy$. Deducir a partir de las dos relaciones anteriores que $N = q(c^2 + d^2)$, y concluir que $\mathrm{mcd}(c, d) = 1$.
Indicación: Recordar que si $z = x + iy, w = c + id \in \mathbb{C}$, entonces la igualdad $|zw|^2 = |z|^2|w|^2$ equivale a $(x^2 + y^2)(c^2 + d^2) = (cx - dy)^2 + (dx + cy)^2$.

Para completar la etapa de descenso, consideremos $p \geq 3$ primo que divida cierto $N = a^2 + b^2$, donde $\mathrm{mcd}(a, b) = 1$:

(iv) Probar que, cambiando N si fuese necesario, podemos suponer que $|a| < p/2$ y $|b| < p/2$, y luego $N < p^2/2$.
Indicación: Si $m \in \mathbb{Z}$ y cambiamos a por $a + mp$ y b por $b + mp$, entonces p sigue dividiendo $a^2 + b^2$ y una elección adecuada de m permite obtener las desigualdades. Si los nuevos a y b no son primos entre sí, considerar a/d y b/d, con $d = \mathrm{mcd}(a, b)$.

(v) Deducir de (iv) que todos los divisores primos q de N, con $q \neq p$, verifican $q < p$. Concluir la etapa de **descenso** utilizando el resultado probado en (ii) y (iii).
Indicación: Si $q < p$ factor primo de $N =: N_0$ fuera suma de dos cuadrados, considerar $N_1 := N/q$. Notar que p divide N_1, y podemos repetir el proceso. Justificar que el descenso se detiene.

Finalmente, para probar la etapa de **reciprocidad**, consideremos $p \geq 3$ primo tal que $p \equiv 1 \mod 4$ y escribamos $p = 4k + 1$:

(vi) Usar el pequeño teorema de Fermat (c.f. Ejercicio 5.(c)) para probar que $(x^{2k} - 1)(x^{2k} + 1) \equiv 0 \mod p$ para todo $x \not\equiv 0 \mod p$. Probar que existe al menos un $x \not\equiv 0 \mod p$ tal que $x^{2k} - 1 \not\equiv 0 \mod p$ y deducir la etapa de **reciprocidad**.
Indicación: En un cuerpo k, la ecuación $x^n = 1$ posee a lo más n soluciones (c.f. Problema C).

En conclusión, un primo $p \geq 3$ es suma de dos cuadrados si y sólo si $p \equiv 1 \mod 4$.