Tarea 1 – Estructuras Algebraicas

Profesor: Pedro Montero, Ayudante: Mateo Hidalgo

Departamento de Matemática, Universidad Técnica Federico Santa María

Fecha de entrega:[1] Hasta el Miércoles 24 de Abril de 2024 a las 23h59.

Esta Tarea puede ser realizada en grupos de 1 o 2 personas, y se debe indicar el nombre de cada integrante.

1. **Generalidades sobre grupos (10 pts).** Sea G un grupo arbitrario.
   (a) Sea $g \in G$. Pruebe que la función $\iota_g : G \to G,\ x \mapsto gxg^{-1}$ es un automorfismo de G.
   (b) Pruebe que $\iota : G \to \mathrm{Aut}(G),\ g \mapsto \iota_g$ es un morfismo de grupos y pruebe que $\ker(\iota) = Z(G)$.

2. **Espacios vectoriales cocientes (15 pts).** Sea k un cuerpo y V un k-espacio vectorial de dimensión finita. Sea $W \subseteq V$ un sub-espacio vectorial.
   (a) Pruebe que el grupo abeliano cociente V/W puede ser dotado de estructura de k-espacio vectorial.
   (b) Pruebe que $\dim_k(V/W) = \dim_k(V) - \dim_k(W)$.
   (c) Deducir, usando el Teorema del Isomorfismo de Noether, el Teorema del Rango: *Toda aplicación lineal $f : V_1 \to V_2$ entre k-espacios vectoriales de dimensión finita cumple que* $\dim_k(V_1) = \dim_k \ker(f) + \mathrm{rg}(f)$.

3. **Acción del grupo ortogonal en $\mathbb{R}^n$ (20 pts).** Considere la acción natural del grupo ortogonal $\mathrm{O}_n(\mathbb{R})$ en el espacio vectorial $\mathbb{R}^n$ dada por $(A, v) \mapsto Av$ para toda $A \in \mathrm{O}_n(\mathbb{R})$ y todo $v \in \mathbb{R}^n$.
   (a) Pruebe que la acción anterior es fiel.
   (b) Sea G es un grupo arbitrario actuando sobre un conjunto no-vacío X. Pruebe que para x, y en X con $y = g \cdot x$ para cierto $g \in G$ se tiene que $G_y = gG_xg^{-1}$.
   (c) Pruebe que si $v \neq 0$ es un vector no-nulo, entonces el estabilizador $\mathrm{O}_n(\mathbb{R})_v$ es isomorfo a $\mathrm{O}_{n-1}(\mathbb{R})$.

   Indicación: Notar que v y $w := \|v\|e_n$ están en la misma órbita de la acción, y usar (b).

   (d) Deducir que $\mathrm{O}_n(\mathbb{R})/\mathrm{O}_n(\mathbb{R})_v$ está en biyección con la esfera $\mathbb{S}^{n-1}(r) \subseteq \mathbb{R}^n$ de radio $r = \|v\|$.

4. **Clases de conjugación (5 pts).** Describir **todas** las clases de conjugación del grupo $\mathrm{GL}_2(\mathbb{C})$.

   Indicación: Se requiere el Teorema de la forma canónica de Jordan.

5. **Teoremas de Sylow (10 pts).**
   (a) Sea $p \geq 2$ un número primo y sea $n \geq 1$. Determine el orden de los grupos $\mathrm{GL}_n(\mathbb{F}_p)$ y $\mathrm{SL}_n(\mathbb{F}_p)$. Considere el subgrupo $T_n(\mathbb{F}_p) \leq \mathrm{GL}_n(\mathbb{F}_p)$ dado por las matrices triangulares superiores con 1 en la diagonal (i.e., $A = (a_{ij}) \in T_n(\mathbb{F}_p)$ si $a_{ii} = 1$ para todo $i \in \{1, \ldots, n\}$ y si $a_{ij} = 0$ para todo $i > j$) y pruebe que es un p-subgroup de Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$. ¿Es $T_n(\mathbb{F}_p)$ un p-subgrupo de Sylow de $\mathrm{SL}_n(\mathbb{F}_p)$?
   (b) Demuestre que todo grupo G de orden 10,000,000 **no** es simple.

6. **Grupos abelianos (10 pts).**
   (a) Demuestre que para todo primo $p \geq 2$ los p-subgrupos de Sylow del grupo producto $G_1 \times G_2$, donde G_1 y G_2 son grupos finitos, son todos de la forma $S_1 \times S_2$ donde $S_1 \leq G_1$ y $S_2 \leq G_2$ son p-subgrupos de Sylow. Utilice lo anterior para determinar, para cada $p \geq 2$ primo, todos los p-subgrupos de Sylow de

   $$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}.$$

   (b) Una expedición de 13 exploradores encuentra un tesoro en una isla, compuesto por monedas de oro idénticas. Al intentar dividir el tesoro entre ellos les sobraron 8 monedas. Dos miembros del grupo contrajeron una enfermedad y fallecieron. Al intentar dividir nuevamente el tesoro, les sobraron 3 monedas. Luego de esto, tres exploradores murieron en un accidente. Después de otro intento fallido, en el que les sobraron 5 monedas, decidieron guardar el tesoro. Tiempo después, se dirijeron a un pueblo de la isla en el que había exactamente 1136 personas viviendo, y decidieron integrarse al pueblo para iniciar una nueva vida. Sin embargo, al intentar distribuir equitativamente el tesoro entre todos los habitantes del pueblo (incluyéndose a ellos), nuevamente les sobraron monedas. ¿Cuántas monedas sobraron?

[1] Factor de retraso: 0.7 por 1 día de retraso, 0.55 por 2 días de retraso, 0.01 por 3 días de retraso.

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

Problema A (30 pts)

El objetivo de este problema es estudiar el grupo de transformaciones afines de $\mathbb{F}_p$. Más precisamente, dado $p \geq 2$ un número primo fijo, definimos G como el grupo de biyecciones $f : \mathbb{F}_p \to \mathbb{F}_p$ de la forma $x \mapsto f(x) = ax + b$ para cierto $a \in \mathbb{F}_p$ y $b \in \mathbb{F}_p$.

(A1) Determinar el orden de G.

(A2) Escribamos $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$, donde $0 = [0]_p, \ldots, p-1 = [p-1]_p$ por abuso de notación. Con la notación anterior, y si pensamos a G como un subgrupo de S_p, ¿cuál es la permutación asociada a la función afín τ dada por $x \mapsto x+1$?

(A3) Determine todos los p-subgrupos de Sylow de G.

(A4) Demostrar que G actúa fielmente sobre $\mathbb{F}_p$.

(A5) Demostrar que G actúa transitivamente sobre $\mathbb{F}_p$.

Problema B (30 pts)

El objetivo de este problema es estudiar cocientes de grupos y consencuencias del Teorema del isomorfismo de Noether. Consideremos G un grupo arbitrario, $K \leq G$ un subgrupo arbitrario, y $H \trianglelefteq G$ un subgrupo normal.

(B1) Sea $p : G \to G/H$ la proyección canónica. Demuestre que las aplicaciones

$$\begin{aligned} \{\text{subgrupos de } G/H\} &\longrightarrow \{\text{subgrupos de } G \text{ que contienen } H\} \\ K' &\longmapsto p^{-1}(K') \\ p(K) &\longleftarrow\!\shortmid K \end{aligned}$$

son biyecciones y son inversas una de la otra. Además, pruebe que K' es un sub-grupo normal de G/H si y solamente si $p^{-1}(K')$ es un sub-grupo normal de G.

(B2) Probar que si $K \trianglelefteq G$ también es un subgrupo normal y si $H \leq K$ entonces hay un isomorfismo

$$(G/H)/(K/H) \cong G/K.$$

(B3) Probar que si $HK := \{hk,\ h \in H \text{ y } k \in K\}$ entonces HK es un subgrupo de G, y probar que $HK = KH$.

(B4) Probar que H es un subgrupo normal de HK.

(B5) Probar que hay un isomorfismo $K/(K \cap H) \cong (HK)/H$.

Bonus (20 puntos extra, opcional)

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 $p \equiv 1 \pmod 4$.

Para probar que todo primo $p \geq 3$ tal que $p \equiv 1 \pmod 4$ 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 $\operatorname{mcd}(x, y) = 1$, entonces $p = u^2 + v^2$ para ciertos enteros $u, v \in \mathbb{Z}$.

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

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 $\operatorname{mcd}(a, b) = 1$, 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 $x^2 N - a^2 q = (xb - ay)(xb + ay)$. 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 $\operatorname{mcd}(c,d)=1$.

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 $\operatorname{mcd}(a,b)=1$:

(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 $d=\operatorname{mcd}(a,b)$.

(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[2] 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: Recuerde que en un cuerpo k, la ecuación $x^n=1$ posee a lo más n soluciones.

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

[2] El pequeño teorema de Fermat afirma que para todo número primo p y todo $n\in\mathbb{Z}$ se tiene que $n^p\equiv n \mod p$.