Guía de Ejercicios y tarea 1.
Álgebra I, primer semestre 2018

Entregue resueltos cuatro de los ejercicios que le parezcan más interesantes el miércoles 21 de marzo.

1. Sea G un grupo (no necesariamente finito) y $H \leq K \leq G$.
   Demuestre que $[G : H] = [G : K][K : H]$.

2. Sea p un número primo y G un grupo con $|G| = p^\alpha$ para algun entero positivo α. Demuestre que todo subgrupo H de G con $[G : H] = p$ es normal en G. Deduzca que cada grupo G de orden p^2 tiene un subgrupo normal de orden p. Deduzca además que entonces G es abeliano.

3. Sea G grupo, $S \subseteq G$ y $g \in G$. Pruebe que
   $$g\ N_G(S)\ g^{-1} = N_G(gSg^{-1}) \quad \text{y} \quad g\ C_G(S)\ g^{-1} = C_G(gSg^{-1}).$$

4. Pruebe que $Z(S_n) = \{e\}$ para todo $n \geq 3$.

5. Sea σ la permutación en S_n ($n \geq 4$) dada por $\sigma = (1\ 2)(3\ 4)$. Demuestre que $|C_{S_n}(\sigma)| = 8(n-4)!$.

6. Sea $\sigma = (1\ 2\ 3\ 4\ 5)$ en S_5. En cada uno de los casos siguientes encuentre un elemento $\tau \in S_5$ tal que
   $$i)\ \ \tau\sigma\tau^{-1} = \sigma^2, \quad ii)\ \ \tau\sigma\tau^{-1} = \sigma^{-1}, \quad iii)\ \ \tau\sigma\tau^{-1} = \sigma^{-2}.$$

7. Sea $G = GL_2(\mathbb{C})$ y $H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{C}, ad \neq 0 \right\}$. Pruebe que cada elemento de G es conjugado a algún elemento de H y deduzca que G es la unión de los conjugados de H. (Sug.: Muestre que cada matriz en G tiene un vector propio.)

8. Sean p, q números primos con $p < q$. Pruebe que todo grupo no abeliano G de orden pq tiene un subgrupo no-normal de índice q, y que existe un homomorfismo inyectivo de G en S_q.

   Sea $\sigma = (1\ 2\ \ldots\ q)$ en S_q. Demuestre además que G es isomorfo a un subgrupo de $N_{S_q}(<\sigma>)$.

9. ¿Qué relación hay entre Stab_x y Stab_y si $x, y \in S$ pertenecen a la misma órbita?

10. Una permutación $\sigma \in S_n$ se puede escribir como producto de ciclos disjuntos. ¿Cómo se relaciona esto con acciones? (Piense en la acción del grupo cíclico generado por σ sobre el conjunto $\{1, 2, \ldots, n\}$.)

11. Sea $\mathrm{GL}(n,\mathbb{Z})$ el conjunto de matrices $n \times n$ con determinante ± 1 y coeficientes en $\mathbb{Z}$.

    a) Demuestre que $\mathrm{GL}(n,\mathbb{Z})$ es un grupo bajo la multiplicación de matrices.

    b) Demuestre que $\mathrm{GL}(n,\mathbb{Z})$ es infinito si $n \geq 2$.

    c) Para $\sigma \in S_n$ defina la matrix $P(\sigma)$ como la matriz en la base usual $e_1, e_2, \ldots, e_n$ de $\mathbb{R}^n$ que representa la única función $\mathbb{R}$-lineal $L_\sigma : \mathbb{R}^n \to \mathbb{R}^n$ que cumple $L_\sigma(e_i) = e_{\sigma(i)}$. Demuestre que $P(\sigma) \in \mathrm{GL}(n,\mathbb{Z})$ y que $\sigma \to P(\sigma)$ es un homomorfismo de S_n a $\mathrm{GL}(n,\mathbb{Z})$.

    d) Sea $A_n \subset S_n$ definido como $A_n := \ker(\det \circ P)$, donde det es el determinante. Demuestre que S_n/A_n tiene dos elementos si $n \geq 2$.

12. Las clases de conjugación de G son las órbitas bajo la acción de conjugación (es decir, $S = G$ y $g \cdot x := gxg^{-1}$). Calcule explícitamente todas las clases de conjugación de S_3, S_4 y A_5. Conjeture una generalización para las clases de conjugación de S_n y A_n.

13. Sea $G := \mathrm{GL}(n,\mathbb{R})$ el grupo de matrices invertibles de tamaño $n \times n$ con coeficientes reales y $S := \mathbb{R}^n$, con la acción $g \cdot v := gv$ (multiplicación de matriz $n \times n$ por una matriz $n \times 1$). Describa todas las órbitas. Ahora sea S el conjunto de las matrices de $n \times m$ y haga lo mismo.

14. Sea $G := \mathrm{GL}(n,\mathbb{C})$ el grupo de matrices invertibles de tamaño $n \times n$ con coeficientes en $\mathbb{C}$, $S := \mathrm{M}_n(\mathbb{C})$ el conjunto de matrices complejas $n \times n$, con la acción $g \cdot m = gmg^{-1}$. Encuentre funciones invariantes interesantes. (Una función $f : S \to \mathbb{C}$ es invariante por la acción de G si $f(g \cdot x) = f(x)$ para todo $x \in S$ y todo $g \in G$. Lo mínimo para ser interesante es que no sea constante.) ¿Sus funciones f_i alcanzan a separar las órbitas? (Es decir $f_i(x) = f_i(y)$ para todas las funciones f_i implica que $x = g \cdot y$ para algún $g \in G$.)

15. Sea $H \subset G$ un subgrupo *sin torsión* (es decir, $h^k \neq e$ para todo $k \in \mathbb{N}$ y todo $h \in H,\ h \neq e$) con G/H finito, de cardinalidad n. Sea $T \subset G$ un grupo finito de orden m. Demuestre que $n \geq m$. Demuestre además que m divide n. (Sugerencia: Piense en la acción de T sobre (G/H)).

16. Sea $H \subset G$ un subgrupo con G/H finito. Demuestre que existe un subgrupo $N \subset H$ con G/N finito y N normal en G. (Sugerencia: Piense en el homomorfismo de G en $\mathrm{Biy}(G/H)$ dado por la acción de G sobre G/H).

Guía de Ejercicios y tarea 2.
Álgebra I, primer semestre 2018

Entregue resueltos los 5 ejercicios marcados con * el miércoles 3 de abril. De los demás ejercicios, indique cuáles no pudo resolver.

1. Sea G un grupo de orden p^n. Demuestre que para todo natural $t \in \mathbb{N}$ con $t \leq n$ existe un subgrupo de G de orden p^t y existe un grupo cociente G/H de orden p^t.

2. Demuestre que el subgrupo de las matrices extrictamente triangulares superior en $\mathrm{GL}_n(\mathbb{F}_q)$ es un p-subgrupo de Sylow de tal grupo.

   NOTA. $\mathrm{GL}_n(\mathbb{F}_q)$ denota las matrices $n \times n$ invertibles con coeficientes a_{ij} en el cuerpo finito $\mathbb{F}_q$ de $q = p^m$ elementos. Estrictamente triangular superior significa que $a_{ii} = 1$, y $a_{ij} = 0$ si $i > j$.

3. Sea S un p-Sylow de G y $N \lhd G$. Demuestre que $N \cap S$ es un p-Sylow de N.

4. Sea $f : G \to H$ un epimorfismo de grupos finitos.

   a) Si S es un p-Sylow de G, demuestre que $f(S)$ es un p-Sylow de H.

   b) Si Q es un p-Sylow de H, demuestre que $Q = f(P)$ para algún p-Sylow S de G.

5. Sea S un p-Sylow de G. Demuestre que $N_G\big(N_G(S)\big) = N_G(S)$.

6. *Sea G un grupo de orden 231. Demuestre que hay un sólo 11-Sylow y que está en el centro de G.

7. Un grupo tiene orden $3^2 5^2$. ¿Qué puede decir sobre sus subgrupos de Sylow?

8. Sea G un grupo de orden 385. Demuestre que G tiene un único 11-Sylow y que su 7-Sylow está contenido en el centro de G.

9. * Sea $|G| = pqr$ donde p, q y r son primos. Demuestre que G no es simple.

10. Sea G un grupo de orden 105. Pruebe que si G tiene un 3-subgrupo de Sylow normal, entonces G es abeliano.

11. * Demuestre que para cualquier entero $n > 1$ hay una sucesión exacta de grupos abelianos $1 \to \mathbb{Z}/n\mathbb{Z} \xrightarrow{f} \mathbb{Z}/n^2\mathbb{Z} \xrightarrow{g} \mathbb{Z}/n\mathbb{Z} \to 1$ no escindida. Aquí f y g son homomorfismos que debe definir.

12. Sea $1 \to X \xrightarrow{f} \Gamma \xrightarrow{g} H \to 1$ una sucesión exacta de grupos. Demuestre:

    a) Existe una función (no necesariamente un homomorfismo) $s : H \to \Gamma$ tal que $g \circ s = \mathrm{Id}_H$. Tal función se llama una sección (de g).

    b) Demuestre que si h_1, $h_2 \in H$, existe $x \in X$ con $s(h_1h_2) = f(x)s(h_1)s(h_2)$. Demuestre que este x está únicamente determinado por h_1, h_2 y la sección s.

    c) Demuestre que si $H \cong \mathbb{Z}$, entonces s se puede elegir para que sea homomorfismo. Demuestre lo mismo si $H \cong \mathbb{Z}^n$.

    d) Fijemos una sección s de g. Demuestre que todo $\gamma \in \Gamma$ se escribe en forma única como $\gamma = f(x)s(h)$, con $x \in X$, $h \in H$.

    e) Demuestre que si s_1 y s_2 son dos secciones de g, entonces $s_1(h)s_2(h)^{-1} \in \mathrm{Im}(f)$ para todo $h \in H$.

    f) Sea s una sección de g. Demuestre entonces que para todo $h \in H$ y todo $x \in X$ existe un $\tilde{x} \in X$ tal que $s(h)f(x)s(h)^{-1} = f(\tilde{x})$.

13. * Suponga que $1 \to X \xrightarrow{f} \Gamma \xrightarrow{g} H \to 1$ es una sucesión exacta de grupos y que existe un homomorfismo $T : \Gamma \to X$ tal que $T\big(f(x)\big) = x$ para todo $x \in X$. Demuestre que $\Gamma \cong X \times H$ y que la sucesión es escindida.

14. * Suponga que $1 \to X \xrightarrow{f} \Gamma \xrightarrow{g} H \to 1$ es una sucesión exacta de grupos abelianos y que la sucesión es escindida. Demuestre que $\Gamma \cong X \times H$. ¿Qué pasa si Γ no es abeliano?

15. Considere el siguiente diagrama conmutativo de grupos abelianos, donde f_1, f_2, f_4 y f_5 son isomorfismos y ambas sucesiones horizontales son exactas (Todas las funciones son homomorfismos).

$$\begin{tikzcd}
A_1 \arrow[r] \arrow[d, "f_1"] & A_2 \arrow[r] \arrow[d, "f_2"] & A_3 \arrow[r] \arrow[d, "f_3"] & A_4 \arrow[r] \arrow[d, "f_4"] & A_5 \arrow[d, "f_5"] \\
B_1 \arrow[r] & B_2 \arrow[r] & B_3 \arrow[r] & B_4 \arrow[r] & B_5
\end{tikzcd}$$

    Demuestre que f_3 es isomorfismo. Este resultado de contagio de isomorfismos se llama el Lema Quíntuple (5-Lemma).

16. Demuestre que la sucesión exacta de grupos abelianos $A \to B \to C$ siempre se puede completar a una sucesión exacta $0 \to K \to A \to B \to C \to D \to 0$.

Guía de Ejercicios y tarea 3.
Álgebra I, primer semestre 2018

Entregue resueltos los 5 ejercicios marcados con * el miércoles 18 de abril. De los demás ejercicios, indique cuáles no pudo resolver.

1. * Exhiba un subgrupo de $Q_8 \times C_4$ que no sea normal (note que todo subgrupo de cada factor es normal).

2. * Para cada una de las siguientes, muestre un grupo que satisfaga las propiedades indicadas:

   a) Un grupo infinito en que todos los elementos tengan orden 1 o 2.

   b) Un grupo infinito en que cada elemento tenga orden finito y que para cada entero positivo n contenga un elemento de orden n.

   c) Un grupo no abeliano con un elemento de orden infinito y uno de orden 2.

   d) Un grupo G tal que todo grupo finito sea isomorfo a un subgrupo de G.

   e) Un grupo no trivial G tal que $G \cong G \times G$.

3. Sea G el grupo multiplicativo de las matrices de 2 por 2 con coeficientes en $\mathbb{R}$ y determinante 1. Muestre que las matrices en G

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

   tienen orden 4 y 3 respectivamente, pero que la matriz ab tiene orden infinito.

   ¿Puede encontrar un grupo con elementos a, b, ambos de orden infinito tal que $b \neq a^{-1}$ y ab sea de orden finito?

4. Sea G el grupo multiplicativo de las matrices de 2 por 2 con coeficientes en $\mathbb{R}$ y determinante 1. ¿Para qué valores de n existe $g \in G$ de orden n?

5. Sea G el grupo multiplicativo de las matrices de 2 por 2 con coeficientes en $\mathbb{Z}$ y determinante 1. ¿Para qué valores de n existe $g \in G$ de orden n?

6. * Demuestre que el grupo multiplicativo $(\mathbb{Z}/p^n\mathbb{Z})^*$ es cíclico para todo $n \in \mathbb{N}$ cuando p es un primo impar, pero que $(\mathbb{Z}/2^n\mathbb{Z})^*$ no es cíclico si $n \geq 3$.

7. Sea $\mathbb{Q}$ el grupo aditivo de los números racionales y $p \in \mathbb{Z}$ un número primo. Definimos el subconjunto $\mathbb{Z}(p^\infty)$ del grupo cociente $\mathbb{Q}/\mathbb{Z}$ como sigue:

$$\mathbb{Z}(p^\infty) = \left\{ \overline{\left(\frac{a}{b}\right)} \in \mathbb{Q}/\mathbb{Z} \mid a, b \in \mathbb{Z},\ b = p^i \text{ algún } i \geq 0 \right\}.$$

   Pruebe que $\mathbb{Z}(p^\infty)$ es un grupo infinito respecto de la adición en $\mathbb{Q}/\mathbb{Z}$.

8. Sea H un subgrupo de $\mathbb{Z}(p^\infty)$

   a) Cada elemento de $\mathbb{Z}(p^\infty)$ tiene orden finito p^n para algún $n \geq 0$.

   b) Si al menos un elemento de H tiene orden p^k y ningún elemento de H tiene orden mayor a p^k, entonces H es el grupo cíclico generado por $\overline{1/p^k}$. En particular $H \cong \mathbb{Z}/p^k\mathbb{Z}$.

   c) Si no existe una cota superior al orden de los elementos en H, entonces $H = \mathbb{Z}(p^\infty)$.

   d) Los únicos subgrupos propios de $\mathbb{Z}(p^\infty)$ son los grupos finito cíclicos $C_n = \left\langle \overline{1/p^k} \right\rangle$, $n = 1, 2, \ldots$. Además $\{0\} < C_1 < C_2 < C_3 < \ldots$

9. Sea C_n un grupo cíclico de orden n y para cada entero a defina

$$\sigma_a : C_n \to C_n, \qquad \sigma_a(x) = x^a \text{ para cada } x \in C_n.$$

   a) Pruebe que σ_a es un automorfismo de C_n si y solo si a y n son relativamente primos.

   b) Pruebe que $\sigma_a = \sigma_b$ si y solo si $a \equiv b \pmod{n}$.

   c) Demuestre que cada automorfismo de C_n es igual a σ_a para algún entero a.

   d) Demuestre que $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduzca que el grupo de automorfismos de C_n es isomorfo a $(\mathbb{Z}/n\mathbb{Z})^*$.

10. * Considere un grupo cíclico K, un grupo cualquiera H y φ_1, φ_2 homomorfismos de K en $\mathrm{Aut}(H)$ tal que $\varphi_1(K)$ y $\varphi_2(K)$ son subgrupos conjugados de $\mathrm{Aut}(H)$. Demuestre, construyendo un isomorfismo explícito, que $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$.

11. * Construya un grupo no abeliano de orden 75. Clasifique todos los grupos de orden 75 (hay 3). Ayuda: Use el ejercicio 10 para mostrar que el grupo no abeliano es único. Este método se puede generalizar para grupos de orden pq^2 donde $p < q$ y p no divide a $q - 1$.

Tarea 4.
Álgebra I, primer semestre 2018

El objetivo de esta tarea es usar SAGE para obtener información sobre algunos grupos finitos. Concretamente, se pide hacer una lista de todos los subgrupos de S_7 (grupo de permutaciones de 7 elementos) sin repetir grupos isomorfos. Para identificar un grupo que no conozca, puede usar su G.id() que consiste de un par de números, el orden y su posición en la lista de grupos de ese orden que almacena GAP. Esto se puede hacer para grupos de orden menor a 2000.

Para cada grupo determine si es cíclico, abeliano, nilpotente, supersoluble, soluble. Para los grupos nilpotentes encuentre sus series centrales ascendente y descendente. Para los grupos supersolubles, encuentre una serie normal de composicin. Para los grupos solubles, encuentre su serie derivada. Para el resto encuentre una serie de composicin.

Determine si en alguno de los grupos encontrados, el subgrupo conmutador G contiene elementos que no sean conmutadores.

Encuentre una presentación minimal para cada uno de los grupos listados (con el mínimo nmero de generadores.)

El resultado lo puede entregar por mail como archivo sws (sage) o pdf, incluyendo las explicaciones necesarias en cualquiera de los dos casos. La fecha de entrega no está predefinida por las dificultades técnicas que puedan surgir, pero sugiero el 7 de mayo en forma tentativa.

Guía de Ejercicios y tarea 5.
Álgebra I, primer semestre 2018

Entregue resueltos los 4 ejercicios marcados con * el lunes 14 de mayo. De los demás ejercicios, indique cuáles no ha podido resolver.

1. Sea A un anillo con unidad.

   Un homomorfismo de grupos abelianos $f : A^n \to A^n$ (donde A^n es un grupo bajo la operación de suma cordenada por coordenada) se dice un A-endomorfismo (derecho) ssi $f(va) = f(v)a$ para todo $a \in A$ y todo $v \in A^n$. Aquí si $v = (v_1, \ldots, v_n)$, definimos $va = (v_1 a, \ldots, v_n a)$. El conjunto de estos A-endomorfismos los denotaremos $\mathrm{End}_A(A^n)$.

   a) Demuestre que $\mathrm{End}_A(A^n)$ es un anillo (con unidad, por supuesto) donde la "multiplicación" es composición de funciones.

   b) Demuestre que $\mathrm{End}_A(A^n)$ es isomorfo al anillo $M_n(A)$ de matrices $n \times n$ con coeficientes en A.

2. Sea A el conjunto de funciones continuas de $[0,1]$ a $\mathbb{R}$, con su estructura natural de anillo y sea $x_0 \in [0,1]$. Demuestre que $I_{x_0} := \big\{ f \in A \big| \, f(x_0) = 0 \big\}$ es un ideal maximal de A. *Sugerencia.* Encuentre un homomorfismo epiyectivo de A a $\mathbb{R}$.

En lo que sigue, todos los anillos se suponen conmutativos con 1.

3. * Sea $f : A \to B$ un homomorfismo unitario de anillos (e.d. $f(1_A) = 1_B$) y $\mathfrak{b} \subset B$ un ideal de B. Demuestre que $f^{-1}(\mathfrak{b})$ es un ideal de A. Demuestre mediante un ejemplo que si $\mathfrak{a} \subset A$ es un ideal de A, entonces $f(\mathfrak{a})$ no es necesariamente un ideal de B. De hecho, demuestre que esta propiedad se cumple para todo ideal de A ssi f es epiyectivo.

4. Sea $f : A \to B$ un homomorfismo unitario de anillos y $\mathfrak{p} \subset B$ un ideal primo de B. Demuestre que $f^{-1}(\mathfrak{p})$ es un ideal primo de A. ¿Es cierta la aseveración anterior si cambiamos "primo" por "maximal"?

5. Demuestre que las operaciones de intersección, suma y producto de ideales (de un mismo anillo) tienen las siguientes propiedades.

   a) $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$, $\quad \mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$, $\quad \mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$, $\quad A\mathfrak{a} = \mathfrak{a}$, $\quad \{0\} + \mathfrak{a} = \mathfrak{a}$. ¿Por qué el conjunto de ideales NO es un anillo bajo las operaciones de suma y producto?

   b) $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$, $\qquad (\mathfrak{a}+\mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a} \cap \mathfrak{b}$.

   c) $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$ si $\mathfrak{a} + \mathfrak{b} = A$.

6. * Para $\mathfrak{a}$ un ideal de A, se define su radical
$$r(\mathfrak{a}) := \left\{ b \in A \middle| \, b^n \in \mathfrak{a} \text{ para algún } n \in \mathbb{N} \right\}.$$
Demuestre que $r(\mathfrak{a})$ es ideal de A y que es igual a la intersección de todos los ideales primos $\mathfrak{p}$ de A tales que $\mathfrak{a} \subset \mathfrak{p}$ (piense en el caso $\mathfrak{a} = \{0\}$ y después en el anillo $A/\mathfrak{a}$).

7. Sea $\mathfrak{a}$ un ideal de A y $\mathfrak{p}_1, \ldots \mathfrak{p}_\mathfrak{n}$ ideales primos de A. Demuestre que $\mathfrak{a} \subset \bigcup_{i=1}^{n} \mathfrak{p}_i$ ssi $\mathfrak{a} \subset \mathfrak{p}_i$ para algún i.

8. Demuestre que todo dominio de integridad finito con más de un elemento es un cuerpo.

9. Sea $r \in A$ nilpotente (e.d. $r^n = 0$ para algún entero positivo n). Demuestre que $1 \pm r \in A^*$, es decir, son unidades (escriba los inversos explicitamente).

10. * El radical de Jacobson J_A se define como la intersección de todos los ideales maximales de A. Demuestre que $x \in J_A$ si y sólo si $1 - xy \in A^*$ para todo $y \in A$. Ayuda: $p \Leftrightarrow q$ es equivalente con $\neg p \Leftrightarrow \neg q$

11. Demuestre que los anillos $2\mathbb{Z}$ y $3\mathbb{Z}$ no son isomorfos.

12. Demuestre que $\mathbb{Z}[x]$ no es isomorfo a $\mathbb{Q}[x]$.

13. Describa todos los homomorfismos de anillos de $\mathbb{Z} \times \mathbb{Z}$ a $\mathbb{Z}$. En cada caso determine el núcleo y la imagen.

14. Sea $R = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Z}\}$. Demuestre que la función $\varphi : R \to \mathbb{Z} \times \mathbb{Z}$ definida por $\varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) = (a, c)$ es un epimorfismo y describa el núcleo.

15. Describa todos los homomorfismos de anillos de $\mathbb{Z}$ a $\mathbb{Z}/30\mathbb{Z}$. En cada caso determine el núcleo y la imagen.

16. * Describa todos los homomorfismos de anillos de $\mathbb{Z}/20\mathbb{Z}$ a $\mathbb{Z}/30\mathbb{Z}$. En cada caso determine el núcleo y la imagen.

17. Demuestre que $\mathbb{C}$ es isomorfo a un subanillo de $M_2(\mathbb{R})$.

18. Un anillo A se dice Booleano si $a^2 = a$ para todo $a \in A$. Demuestre que todo anillo Booleano es conmutativo.

19. Sea X un conjunto no vacío y $\mathcal{P}(X)$ el conjunto de todos los subconjuntos de X. Defina suma y producto en $\mathcal{P}(X)$ como
$$A + B = (A - B) \cup (B - A), \qquad AB = A \cap B.$$
Demuestre que con esas operaciones $\mathcal{P}(X)$ es un anillo Booleano con uno.

Guía de Ejercicios y tarea 6.
Álgebra I, primer semestre 2018

Entregue resueltos los 4 ejercicios marcados con * el miércoles 23 de mayo.

1. Sea R un DFU y d un elemento en $R - \{0\}$. Demuestre que el ideal (d) esta contenido en un número finito de ideales principales de R.

2. Sea A un DIP y $\mathfrak{p}$ un ideal primo distinto de $\{0\}$ y de A. Demuestre que $\mathfrak{p}$ es un ideal maximal.

3. Dado anillos A_1 y A_2, defina su suma directa $A = A_1 \oplus A_2$.

   a) Demuestre que existen elementos e_1, $e_2 \in A$ tales que
   $$e_1^2 = e_1, \quad e_2^2 = e_2, \quad e_1e_2 = 0_A, \quad e_1 + e_2 = 1_A. \qquad (*)$$

   b) Para $i = 1$ e $i = 2$, pongamos $B_i = e_iA = \left\{b \in A \middle| b = e_ia,\ a \in A\right\}$. Demuestre que B_i es un anillo y es isomorfo a A_i.

   c) Describa todos los ideales de A en términos de los de A_1 y A_2.

   d) Describa todos los ideales primos de A en términos de los de A_1 y A_2.

4. Sea A un anillo que contiene elementos e_1 y e_2 con las propiedades $(*)$ del ejercicio anterior. Demuestre que A es isomorfo como anillo a $B_1 \oplus B_2$, con B_i como en el ejercicio anterior.

5. Demuestre que $\mathbb{Z}[i]$ es un dominio euclideano.

6. * Demuestre que $\mathbb{Z}[\omega]$, donde $\omega = \frac{-1+i\sqrt{3}}{2}$, es un dominio euclideano. Para ello defina $N(a+b\omega) = a^2 - ab + b^2$. Ayuda: Observe que puede dividir en $\mathbb{Q}[\omega] \subseteq \mathbb{C}$ usando que $\overline{\omega} = \omega^2 = -1 - \omega$.

7. Sea F un cuerpo. Demuestre que el anillo $F[x_1, \ldots, x_n]$ de polinomios en n variables no es un dominio de ideales principales si $n > 1$.

8. * Demuestre que $Z[\sqrt{-2}] := \left\{a + bi\sqrt{2} \in \mathbb{C} \middle| a, b \in \mathbb{Z}\right\}$ es DFU, pero $Z[i\sqrt{14}]$ no lo es.

9. * Sea $B = \mathbb{R}[X, Y]$, el anillo de polinomios reales en dos variables, y sea $I \subset B$ el ideal principal generado por $(X^2 - Y^3)$. Para $\alpha \in B$, denotaremos por $\bar{\alpha}$ su clase en el anillo cuociente $A = B/I$.

   a) Defina el grado de un elemento no nulo de B y demuestre que tiene las propiedades usuales (grado de un producto es suma de los grados de los factores, grado de una suma es a lo más el máximo de los grados de los sumandos).

b) Demuestre que I es un ideal primo de B.

c) Demuestre que $\bar{X}$ y $\bar{Y}$ son elementos irreducibles de A y que no son asociados (es decir, uno no es una unidad por el otro),

d) Demuestre que A es un dominio, pero no es de factorización única.

10. Demuestre que el orden grado-lexicográfico en $K[x_1, \ldots, x_n]$ es un orden monomial.

11. * Usando el orden lexicográfico con $x > y$,

    a) encuentre una base de Groebner para el ideal

    $$I = (2xy^2 + 3x + 4y^2, y^2 - 2y - 2) \leq \mathbb{C}[x, y].$$

    ¿Está $f = 2x^3y^3 + 4y^2$ en este ideal? Determine un conjunto de representantes para $\mathbb{C}[x, y]/I$.

    b) encuentre una base de Groebner para el ideal $J = (x^2+y^2+1, x^2y+2xy+x)$ en $\mathbb{F}_5[x, y]$. Encuentre el conjunto de ceros de este ideal, es decir

    $$\{(x, y) \in \mathbb{F}_5^2 \mid f(x, y) = 0 \forall f \in J\}$$

12. Encuentre un polinomio $f \in \mathbb{Z}[x]$ tal que

    $$\mathbb{Z}[x]/(f) \cong \mathbb{Z} \times \mathbb{Z}$$

    ¿Existe g tal que $\mathbb{Z}[x]/(g) \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$?

Guía de Ejercicios y tarea 7.
Álgebra I, primer semestre 2018

Entregue resueltos los 4 ejercicios marcados con * el miércoles 13 de junio. De los demás ejercicios. En esta guía R es siempre un anillo con unidad, A es un anillo conmutativo con unidad. Un R-módulo se entiende izquierdo. $\mathrm{Hom}_R(X_1, X_2)$ denota el grupo de R-homomorfismos entre los R-módulos X_1 y X_2.

1. Sea $R = \mathrm{End}_K(V)$, con V un espacio vectorial sobre un cuerpo K y base infinita $\{e_1, e_2, \ldots, \}$. Sean α y β las transformaciones lineales de V en V tales que $\alpha(e_{2n}) = e_n$, $\alpha(e_{2n+1}) = 0$, $\beta(e_{2n}) = 0$ y $\beta(e_{2n+1}) = e_n$ para todo $n \geq 0$.

   a) Demuestre que $\{1\}$ y $\{\alpha, \beta\}$ son bases para ${}_RR$

   b) Demuestre que ${}_RR$ tiene una base de cardinalidad m para cualquier entero $m > 0$.

2. Sea M el R-módulo R^n y sean $I_1, I_2, \ldots, I_n$ ideales izq. de R. Demuestre que los siguientes son submódulos de M.

   a) $\{(a_1, a_2, \ldots, a_n) \mid a_j \in I_j\}$

   b) $\{(a_1, a_2, \ldots, a_n) \mid a_j \in R,\ a_1 + a_2 + \ldots + a_n = 0\}$

3. * Sea M un R-módulo. Un elemento $m \in M$ se dice de torsión si $rm = 0$ para algún $r \neq 0$ en R. El conjunto de elementos de torsión se denota

$$\mathrm{Tor}(M) = \{m \in M \mid rm = 0 \text{para algún } r \in R, r \neq 0\}$$

   a) Demuestre que si R es un dominio de integridad, entonces $\mathrm{Tor}(M)$ es un submódulo de M.

   b) Muestre un ejemplo de un anillo R y un R-módulo M tales que $\mathrm{Tor}(M)$ no sea un submódulo. (Considere los elementos de torsión en el R-módulo R.)

   c) Si R tiene divisores de cero, demuestre que todo R-módulo no nulo tiene elementos de torsión no nulos.

4. Sea $F = \mathbb{R}$, $V = \mathbb{R}^2$ y T la transformación lineal de V en V que resulta de la rotación en $\pi/2$ radianes en el sentido del reloj con centro en el origen. Muestre que 0 y V son los únicos submodulos del $F[X]$-módulo V definido por T.

5. * Sea $F = \mathbb{R}$, $V = \mathbb{R}^2$ y T la transformación lineal de V en V que resulta de la proyección en el eje y. Muestre que 0, V, el eje x y el eje y son los únicos submodulos del $F[X]$-módulo V definido por T.

6. Dé un ejemplo explícito de una función de un R-módulo a otro que sea homomorfismo de grupos pero no de R-módulos.

7. Exhiba todos los homomorfismos de $\mathbb{Z}$-módulos de $\mathbb{Z}/30\mathbb{Z}$ en $\mathbb{Z}/21\mathbb{Z}$.

8. Demuestre que $Hom_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n,m)\mathbb{Z}$.

9. Pruebe que $Hom_A(A, A)$ y A son isomorfos como anillos.

10. Describa $\mathrm{Hom}_R(R, X)$ para cualquier R-módulo X. ¿Y $\mathrm{Hom}_R(R^n, X)$?

11. Un R-módulo M se dice módulo de torsión si para cada $m \in M$ existe $r \in R$ no nulo, tal que $rm = 0$ donde r puede depender de m ($M = \mathrm{Tor}(M)$). Demuestre que todo grupo abeliano finito es un $\mathbb{Z}$-módulo de torsión. Dé un ejemplo de un grupo abeliano infinito que sea $\mathbb{Z}$-módulo de torsión.

12. * Sean M, N y P A-módulos. Demuestre los siguientes isomorfismos de A-módulos:

    a) $Hom_A(M \times N, P) \cong Hom_A(M, P) \times Hom_A(N, P)$
    b) $Hom_A(P, M \times N) \cong Hom_A(P, M) \times Hom_A(P, N)$

13. * Sea R un DIP y sea M un R-módulo anulado por el ideal propio y no nulo (a). Sea $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ su descomposición como producto de potencias de primos diferentes. Sea M_i el anulador de $p_i^{\alpha_i}$ en M, es decir $M_i = \{m \in M \mid p_i^{\alpha_i} m = 0\}$ (llamada componente p_i-primaria de M). Demuestre que
$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_k.$$

14. Muestre que si M es un grupo abeliano finito de orden $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ entonces, considerado como $\mathbb{Z}$-módulo, M es anulado por (a), la componente p_i-primaria de M es el p_i-subgrupo de Sylow de M y M es isomorfo al producto directo de sus subgrupos de Sylow.

15. Sea A una matriz $n \times n$ fija, con coeficientes en $\mathbb{C}$ que usamos para darle a $V = \mathbb{C}^n$ la estructura de $\mathbb{C}[x]$-módulo mediante $xv := A \cdot v$ (multiplicación de matriz por vector columna) para $v \in V$.

    a) Demuestre que V es un módulo de torsión, finitamente generado sobre $\mathbb{C}[x]$. ¿Vale lo mismo si reemplazamos $\mathbb{C}$ por otro cuerpo?
    b) Describa (salvo isomorfismo) todos los módulos de torsión, finitamente generados sobre $\mathbb{C}[x]$. Puede suponer el teorema fundamental del álgebra.
    c) Sin citar ningún teorema de álgebra lineal (por ejemplo, Cayley-Hamilton puede ser un corolario y no debe usarse), demuestre el teorema de Jordan que da una forma canónica de una matriz semejante a A. Identifique claramente la relación entre los valores propios de A y la torsión de V.

Guía de Ejercicios y tarea 8.
Álgebra I, primer semestre 2018

Entregue resueltos 6 de los siguientes ejercicios el miércoles 27 de junio.

1. Sea $\beta' \circ \alpha = \alpha' \circ \beta$ un pushout. Demuestre que si α es inyectivo, entonces α' es inyectivo.
2. Defina pullback de conjuntos y demuestre su existencia y unicidad.
3. Demuestre que cualquier sumando directo de un módulo proyectivo es proyectivo.
4. Demuestre que el producto directo $A = \mathbb{Z} \times \mathbb{Z} \times \dots$ de una cantidad infinita numerable de copias de $\mathbb{Z}$ no es un $\mathbb{Z}$-módulo proyectivo.
5. Encuentre ejemplos de módulos proyectivos que no sean libres.
6. Demuestre que toda suma directa de R-módulos inyectivos es un R-módulo inyectivo.
7. Demuestre que las siguientes condiciones son equivalentes para un R-módulo izquierdo P:

   a) P es proyectivo

   b) $\mathrm{Hom}_R(P, -)$ preserva epimorfismos

   c) $\mathrm{Hom}_R(P, -)$ es exacto
8. Encuentre un ejemplo de un módulo M y una sucesión exacta corta $0 \to A \to B \to C \to 0$ tal que $0 \to \mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B) \to \mathrm{Hom}_R(M, C) \to 0$ no sea exacta.
9. Demuestre que $\mathrm{Hom}_r(-, M)$ es exacto por la izquierda.
10. Enuncie y demuestre una equivalencia similar al ejercicio 7 para módulos inyectivos.
11. Demuestre que $0 \to A \to B \to C$ es exacta si y solo si $0 \to \mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(M, B) \to \mathrm{Hom}_R(M, C)$ es exacta para todo módulo M.
12. Demuestre que $\mathrm{Hom}_R(M, -)$ preserva pullbacks de R-módulos izquierdos.
13. Enuncie y demuestre el efecto que tiene $\mathrm{Hom}_R(-, M)$ sobre los pullbacks de R-módulos izquierdos.
14. Demuestre que $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \cong \mathbb{Z}_d$, donde $d = \mathrm{mcd}(m, n)$.

15. Sea M un R-módulo izquierdo y sea I un ideal de R. Muestre que existe un isomorfismo $R/I \otimes_R M \cong M/IM$ que es natural en M.

16. Demuestre directamente que $- \otimes_R N$ es exacto por la derecha.

17. Demuestre que si M es un R-módulo proyectivo, entonces $- \otimes_R M$ es exacto.

18. Encuentre un homomorfismo inyectivo de grupos abelianos $A \to B$ tal que $\mathbb{Z}_2 \otimes_{\mathbb{Z}} A \to \mathbb{Z}_2 \otimes_{\mathbb{Z}} B$ no sea inyectivo.