UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Dado $K \subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K \subseteq A_n$.
2. Sea $(G, \cdot)$ un grupo finito y abeliano, si $d \mid \#G$ entonces existe $a \in G$ tal que $O(a) = d$.
3. Sea $(G, \cdot)$ un grupo y H_1, H_2 subgrupos de G tales que $H_1 \lhd H_2$ y que $H_2 \lhd G$ entonces $H_1 \lhd G$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = D_3 \times D_4 \times D_5$ y $H = S_5 \times C_2 \times C_2$.

1. Determinar si G y H son o no son grupos isomorfos.
2. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si $\mathrm{car}(R) = n > 0$, entonces $\mathrm{car}(R \times R \times R) = n^3$.
2. Si R es un D.I.P., entonces R/I es D.I.P.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[i] = \{a + bi\,;\, a, b \in \mathbb{Z}\}$, el anillo de los enteros de Gauss, consideramos el ideal $I = (1 + 7i)$ y el anillo cociente $A = \mathbb{Z}[i]/I$.

1. Probar que $i+I = 7+I$ y deducir que para todo elemento $a+bi$ de $\mathbb{Z}[i]$ existe $k \in \mathbb{Z}$ tal que $(a+bi)+I = k+I$.
2. Construye un homomorfismo de anillos $\Psi : \mathbb{Z} \to A$ sobreyectivo.
3. Encuentra un valor de $n \in \mathbb{N}$ tal que $\mathbb{Z}/n\mathbb{Z} \approx A$. ¿Es A un cuerpo?

Esquema de una solución de la versión A del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Dado $K \subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K \subseteq A_n$.

   Solución: Verdadera. Tenemos que $\#K = 2k+1$ con $k \in \mathbb{Z}$, por el Corolario 1.5.1.a), para todo $\alpha \in K$ tenemos que $O(\alpha) \mid 2k+1$. Por la Proposición 1.3.6.2, $\alpha^{2k+1} = id$. Luego $\alpha^{2k}\alpha = 1$ y deducimos que $\alpha = \alpha^{-2k} = (\alpha^{-k})^2$. Por consiguiente, tanto si $\beta = \alpha^{-k}$ es una permutación par como si β es impar, β^2 es par. En consecuencia, $\alpha = \beta^2 \in A_n$ y concluimos que $K \subseteq A_n$.

2. Sea $(G, \cdot)$ un grupo finito y abeliano, si $d \mid \#G$ entonces existe $a \in G$ tal que $O(a) = d$.

   Solución: Falsa. Basta considerar $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ que es un grupo finito y abeliano. Tenemos que $\#G = 4$, pero $O((0,0)) = 1$ y $O((0,1)) = O((1,0)) = O((1,1)) = 2$, es decir, no existe $a \in G$ con $O(a) = 4$.

3. Sea $(G, \cdot)$ un grupo y H_1, H_2 subgrupos de G tales que $H_1 \lhd H_2$ y que $H_2 \lhd G$ entonces $H_1 \lhd G$.

   Solución: Falsa. Con la notación del **E156**, basta considerar $G = D_4$, $H_1 = \{id, b\} = \langle b \rangle$ y $H_2 = \{id, b, a^2, a^2b\} = \langle a, b \rangle$. Sabemos que $\#H_1 = 2$, $\#H_2 = 4$ y que $\#D_4 = 8$. Por el Teorema de Lagrange, se tiene que $\#(H_2 : H_1) = 2$ y $\#(D_4 : H_2) = 2$. Por el **E167**, concluimos que $H_1 \lhd H_2$ y que $H_2 \lhd D_4$. Finalmente, observamos que $aH_1 = \{a, ab\}$ y que $H_1 a = \{a, ba\}$ y, por el **E156**, sabemos $ba = a^3b$ y que $a^3b \neq ab$. Por consiguiente, $aH_1 \neq H_1 a$ y concluimos que H_1 no es normal en D_4.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = D_3 \times D_4 \times D_5$ y $H = S_5 \times C_2 \times C_2$.

Solución: Lema Auxiliar. Dados tres grupos finitos A, B, C, y tres elementos $a \in A$, $b \in B$, $c \in C$ se tiene que el orden de (a, b, c) como elemento del grupo producto $A \times B \times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a,b,c)) = m.c.m.\{O(a), O(b), O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b), O(c)\}$, por la definición del grupo producto tenemos que $(a,b,c)^m = (a^m, b^m, c^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$, $b^m = 1_B$ y $c^m = 1_C$, luego $(a,b,c)^m = 1_{A\times B\times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a,b,c)) \mid m$. Por otra parte, si $O((a,b,c)) = t$ como $(a,b,c)^t = 1_{A\times B\times C}$ se tiene que $a^t = 1_A$, $b^t = 1_B$ y $c^t = 1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$, $O(b) \mid t$ y $O(c) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Determinar si G y H son o no son grupos isomorfos.

   Solución: Observamos que $\#G = \#H = 480$, por tanto, no podemos emplear el cardinal para determinar si son isomorfos o no. Por tanto, con la notación del **E156**, si consideramos el elemento $x = ((123), (1234), (12345))$ de G por el Lema Auxiliar $O(x) = 60$. Por otro lado, empleando la descomposición en ciclos disjuntos (**Cor. 1.4.1.**), comprobamos que los posibles órdenes de los elementos de S_5 son $\{1,2,3,4,5,6\}$. Por el Lema Auxiliar, los posibles órdenes de los elementos de H son $\{1,2,3,4,5,6,10\}$. Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y G no son isomorfos porque en G hay un elemento de orden 60 y en H no.

2. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.

   Solución: Por la Proposición 1.6.2, como $\mathbb{Z}/3\mathbb{Z} = \langle 1 \rangle$ es cíclico f queda completamente determinado por $f(1)$. Además por la Proposición 1.6.2. sabemos que $O(f(1)) \mid 3$ y que para cada $b \in G$ con $O(b) \mid 3$ existe un único homomorfismo $f_b : \mathbb{Z}/3\mathbb{Z} \to G$ tal que $f(1) = b$. Por consiguiente determinar los homomorfismos equivale a determinar los elementos $b \in G$ con $O(b) \in \{1, 3\}$.
   Observamos que $O(b) = 1$ si y sólo si $b = 1_G$. Empleando el **E156**, vemos que el posible orden de los elementos de D_3 es $\{1,2,3\}$ de los elementos de D_4 es $\{1,2,4\}$ y de D_5 es $\{1,2,5\}$. Por tanto, por el Lema Auxiliar, deducimos que los elementos de orden 3 de G son $((123), id, id)$ y $((132), id, id)$. Por consiguiente, hay tres homomorfismos de grupos $\mathbb{Z}/3\mathbb{Z}$ en G determinados por $f_1(1) = (id, id, id)$, $f_2(1) = ((123), id, id)$ y $f_3(1) = ((132), id, id)$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si $\mathrm{car}(R) = n > 0$, entonces $\mathrm{car}(R \times R \times R) = n^3$.

   Solución: Falso. Por el **Ejemplo II.4.8**, sabemos que $(R,+,\cdot) = (\mathbb{Z}/3\mathbb{Z},+,\cdot)$ es un dominio. Como los dominios son anillos unitarios, por el **Teorema.II.3.18**, $\mathrm{car}(\mathbb{Z}/3\mathbb{Z}) = O(1_{\mathbb{Z}/3\mathbb{Z}}) = 3$. Como en el anillo producto $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ las operaciones se definen componete a componete es un anillo unitario con elemento neutro $(1_{\mathbb{Z}/3\mathbb{Z}}, 1_{\mathbb{Z}/3\mathbb{Z}}, 1_{\mathbb{Z}/3\mathbb{Z}})$. Por el **Teorema.II.3.18**, se tiene que $\mathrm{car}(R \times R \times R) = O((1,1,1)) = 3 \neq 27 = 3^3$.

2. Si R es un D.I.P., entonces R/I es D.I.P.

   Solución: Falso. Basta considerar $(R,+,\cdot) = (\mathbb{Z},+,\cdot)$ e $I = 6\mathbb{Z}$. El anillo cociente R/I es $(\mathbb{Z}/6\mathbb{Z},+,\cdot)$ que no es un dominio porque 6 no es primo (**Ejemplo II.4.8**). En consecuencia R/I no es un dominio de ideales principales (D.I.P.).

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[i] = \{a + bi\,;\, a,b \in \mathbb{Z}\}$, el anillo de los enteros de Gauss, consideramos el ideal $I = \big(1 + 7i\big)$ y el anillo cociente $A = \mathbb{Z}[i]/I$.

1. Probar que $i+I = 7+I$ y deducir que para todo elemento $a+bi$ de $\mathbb{Z}[i]$ existe $k \in \mathbb{Z}$ tal que $(a+bi)+I = k+I$.

   Solución: Observamos que $i - 7 = i(1+7i) \in I$, luego $i + I = 7 + I$. Dado un elemento $a + bi$ de $\mathbb{Z}[i]$ con $a,b \in \mathbb{Z}$, por las propiedades de la suma y el producto en A, se tiene que $(a+bi)+I = (a+I)+(b+I)(7+I) = (a + b7) + I$. En otras palabras, como $a + b7 \in \mathbb{Z}$, queda demostrado el apartado.

2. Construye un homomorfismo de anillos $\Psi : \mathbb{Z} \to A$ sobreyectivo.

   Solución: Basta considerar $\Psi = p \circ f$ donde $f : \mathbb{Z} \to \mathbb{Z}[i]$ es la inyección canónica y $p : \mathbb{Z}[i] \to \mathbb{Z}[i]/I$ es la aplicación de paso al cociente. Como f y p son homomorfismos de anillos, por la **Proposición II.3.3**, Ψ es también un homomorfismo de anillos y está dado por $\Psi(k) = k + I$. Por el apartado anterior, para todo elemento $a + bi$ de $\mathbb{Z}[i]$ existe $k \in \mathbb{Z}$ tal que $(a + bi) + I = k + I$, luego $\Psi(k) = (a + bi) + I$, es decir, Ψ es sobreyectivo.

3. Encuentra un valor de $n \in \mathbb{N}$ tal que $\mathbb{Z}/n\mathbb{Z} \approx A$. ¿Es A un cuerpo?

   Solución: Observamos que dado $k \in \mathbb{Z}$, $k \in \mathrm{Ker}\Psi$ si y solo si $k + I = I$, es decir, si y solo si $k \in I$. Vemos que $k \in I$ si y solo si existen $a,b \in \mathbb{Z}$ con $k = (a + bi)(1 + 7i)$, es decir, si y solo si, existen $a,b \in \mathbb{Z}$, $k = a - 7b$ y $0 = 7a + b$. Deducimos que $k \in \mathrm{Ker}\Psi$ si y solo si existe $a \in \mathbb{Z}$ tal que $k = 50a$, es decir, si y solo si, $k \in 50\mathbb{Z}$, dicho de otro modo, $n = 50$. Como Ψ es sobreyectivo, por **Primer teorema de isomorfía (Teorema II.3.8)**, $\mathbb{Z}/50\mathbb{Z} \approx A$. Por el **Ejemplo II.4.8**, tenemos que $\mathbb{Z}/50\mathbb{Z}$ no es un cuerpo porque 50 no es primo. Deducimos que A tampoco es un cuerpo porque, por ejemplo, la imagen de un divisor de cero no nulo por un isomorfismo es un divisor de cero no nulo. En otras palabras, en A hay divisores de cero no nulos.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo si hay un elemento $a \in G$ de orden 18, entonces hay por lo menos 6 elementos de orden 18.
2. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.
3. Sea $(G,\cdot)$ un grupo no abeliano y $K \lhd G$ un subgrupo no abeliano entonces G/K es no abeliano.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = C_3 \times C_5 \times C_{15}$ y $H = C_9 \times C_{25}$.

1. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.
2. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un D.I.P., entonces cada ideal del anillo cociente R/I es principal.
2. Si R es un D.F.U. y $a, b, c \in R$ con $a \neq 0$, entonces

$$d \text{ es un m.c.d. de } b \text{ y } c \text{ si y solo si } ad \text{ es un m.c.d. de } ab \text{ y } ac.$$

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[x]$, el anillo de los polinomios con coeficientes enteros, consideramos el ideal $I = (10, x-3)$ y el anillo cociente $A = \mathbb{Z}[x]/I$.

1. Probar que $x+I = 3+I$ y deducir que para todo elemento $P(x)$ de $\mathbb{Z}[x]$ existe $k \in \mathbb{Z}$ tal que $P(x)+I = k+I$.
2. Probar que $Q(x) = 6x^3 + 5x^2 + 8x + 12$ es irreducible en $\mathbb{Z}[x]$.
3. Encuentra el inverso de $Q(x) + I$ en A.

Esquema de una solución de la versión B del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo si hay un elemento $a \in G$ de orden 18, entonces hay por lo menos 6 elementos de orden 18.

   Solución: Verdadera. Por la Proposición 1.3.6, $\#(\langle a\rangle) = O(a) = 18$. Por el Teorema 1.3.1.c), en $\langle a\rangle$ hay $\varphi(18)$ elementos de orden 18. Por el **E13**, $\varphi(18) = 18(1/2)(2/3) = 6$ y, como $\langle a\rangle \subseteq G$, concluimos que hay por lo menos 6 elementos de orden 18 en G.

2. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.

   Solución: Falsa. Escribimos α como el producto de ciclos disjuntos $\alpha = (1\,8)(2\,7)(4\,9\,5\,6)$. Por la Proposición 1.4.1, sabemos las permutaciones disjuntas conmutan y se tiene que

   $$\alpha^3 = (1\,8)^3(2\,7)^3(4\,9\,5\,6)^3 = (1\,8)(2\,7)(4\,6\,5\,9).$$

   Finalmente, observamos que $(4\,6\,5\,9) = (4\,9)(4\,5)(4\,6)$. En consecuencia, α^3 descompone como producto de 5 transposiciones y concluimos que es impar y, por tanto, $\alpha^3 \notin A_9$.

3. Sea $(G,\cdot)$ un grupo no abeliano y $K \lhd G$ un subgrupo no abeliano entonces G/K es no abeliano.

   Solución: Falsa. Basta considerar $G = S_4$ y $K = A_4$. Observamos que $(123), (234) \in A_4 \subseteq S_4$ y que $(123)(234) = (12)(34) \neq (13)(24) = (234)(123)$ luego G y K no son abelianos. Por el **E116**, $\#A_4 = 12$ y como $\#S_4 = 24$, por el Teorema de Lagrange, se tiene que $\#(S_4 : A_4) = 2$. Por el **E167**, vemos que $A_4 \lhd S_4$. Como $\#(S_4 : A_4) = \#(S_4/A_4) = 2$, por el Corolario 1.5.1.b), el grupo cociente S_4/A_4 es cíclico y, por tanto, es abeliano.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = C_3 \times C_5 \times C_{15}$ y $H = C_9 \times C_{25}$.

Solución: Lema Auxiliar. Dados tres grupos finitos A, B, C, y tres elementos $a \in A$, $b \in B$,$c \in C$ se tiene que el orden de (a,b,c) como elemento del grupo producto $A \times B \times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a,b,c)) = m.c.m.\{O(a), O(b), O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b), O(c)\}$, por la definición del grupo producto tenemos que $(a,b,c)^m = (a^m, b^m, c^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$, $b^m = 1_B$ y $c^m = 1_C$, luego $(a,b,c)^m = 1_{A\times B\times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a,b,c)) \mid m$. Por otra parte, si $O((a,b,c)) = t$ como $(a,b,c)^t = 1_{A\times B\times C}$ se tiene que $a^t = 1_A$, $b^t = 1_B$ y $c^t = 1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$, $O(b) \mid t$ y $O(c) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

   Solución: Observamos que $\#G = \#H = 225$. Buscamos K con $\#K = 225$ de modo que $K \not\approx H$ y $K \not\approx G$. Consideramos $K := C_9 \times C_5 \times C_5$, cumple que $\#K = 225$. Por el Teorema 1.3.1, sabemos que el orden de los elementos de C_3 es 1 o 3,el orden de los elementos de C_5 es 1 o 5, el orden de los elementos de C_9 es 1, 3 o 9,el orden de los elementos de C_{15} es 1, 3, 5 o 15, y que el orden de los elementos de C_{25} es 1, 5 o 25. Empleando el Lema Auxiliar vemos que:

   - en K no hay ningún elemento de orden 25 pero sí hay elementos de orden 9.
   - en G no hay ningún elemento de orden 25 ni de orden 9.
   - en $C_1 \times C_9 \times C_{25} \approx C_9 \times C_{25} = H$ hay elementos de orden 9 y de orden 25.

   Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y K no son isomorfos y G y K tampoco son isomorfos.

2. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.

Solución: Consideramos $f : G \to G$ dado por $f(a,b,c) = (0,c)$. Comprobamos de forma directa que f es un endomorfismo (proyección), que $\mathrm{Ker} f = C_3 \times C_5 \times \{0\}$ y que $\mathrm{Im} f = \{0\} \times \{0\} \times C_{15}$. Finalmente, demostramos que $\mathrm{Ker} f \approx \mathrm{Im} f \approx C_{15}$, para probar esto se puede ver que ambos grupos son cíclicos de orden 15 y concluir usando la Proposición 1.6.3.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un D.I.P., entonces cada ideal del anillo cociente R/I es principal.

   Solución: Cierto. Consideramos el homomorfismo de anillos sobreyectivo $p : R \to R/I$ de paso al cociente dado por $p(a) = a + I$. Dado L un ideal de R/I, por la **Proposición II.3.4.(vi)**, sabemos que $p^{-1}(L)$ es un ideal de R. Como R es un D.I.P., existe $x \in R$ tal que $\big(x\big) = p^{-1}(L)$.
   Veamos que $L = \big(p(x)\big)$. Como $x \in \big(x\big) = p^{-1}(L)$, se tiene que $p(x) \in L$ luego $\big(p(x)\big) \subseteq L$. Recíprocamente, dado $\ell \in L$ como p es sobreyectiva, existe $y \in R$ tal que $p(y) = \ell$. Por consiguiente, $y \in \big(x\big) = p^{-1}(L)$. Como R es un dominio, $\big(x\big) = \{rx; r \in R\}$, es decir, $y = rx$ para algún $r \in R$. Como p es homomorfismo de anillos, $\ell = p(y) = p(r)p(x)$. Deducimos que $\ell \in \big(p(x)\big)$ y concluimos que $L \subseteq \big(p(x)\big)$. En resumen hemos probado que cada ideal L del anillo cociente R/I está generado por un único elemento, es decir, es principal.

2. Si R es un D.F.U. y $a,b,c \in R$ con $a \neq 0$, entonces

   $$d \text{ es un m.c.d. de } b \text{ y } c \text{ si y solo si } ad \text{ es un m.c.d. de } ab \text{ y } ac.$$

   Solución: Cierto. Supongamos que d es un m.c.d. de b y c. Por (MCD.I), $d \mid b$ y $d \mid c$, luego $ad \mid ab$ y $ad \mid ac$, es decir, ad satisface (MCD.I). Como R es un D.F.U., sabemos que existe x un m.c.d de ab y ac. Como $a \mid ab$ y $a \mid ac$, por (MCD.II), $a \mid x$. Dicho de otro modo, existe $r \in R$ tal que $x = ar$. Por (MCD.I), $x \mid ab$ y $x \mid ac$, luego $ar \mid ab$ y $ar \mid ac$. Como $a \neq 0$ y como R es un dominio, por la Ley de Cancelación, **Teorema.II.4.6**, se tiene que $r \mid b$ y que $r \mid c$. Como d es un m.c.d. de b y c, por (MCD.II), $r \mid d$, luego $x = ar \mid ad$ y como x es un m.c.d de ab y ac concluimos que ad también satisface (MCD.II) para ab y ac. En resumen, ad es un un m.c.d de ab y ac.
   Recíprocamente, supongamos que ad es un m.c.d. de ab y ac. Por (MCD.I), $ad \mid ab$ y $ad \mid ac$, Como $a \neq 0$ y como R es un dominio, por la Ley de Cancelación, **Teorema.II.4.6**, se tiene que $d \mid b$ y $d \mid c$, es decir, d satisface (MCD.I). Si $s \mid b$ y $s \mid c$, tenemos que $as \mid ab$ y $as \mid ac$. Por (MCD.II), $as \mid ad$ y de nuevo por la Ley de Cancelación $s \mid d$, es decir, d satisface (MCD.II).

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[x]$, el anillo de los polinomios con coeficientes enteros, consideramos el ideal $I = (10, x-3)$ y el anillo cociente $A = \mathbb{Z}[x]/I$.

1. Probar que $x+I = 3+I$ y deducir que para todo elemento $P(x)$ de $\mathbb{Z}[x]$ existe $k \in \mathbb{Z}$ tal que $P(x)+I = k+I$.

   Solución: Observamos que $x - 3 \in I$, luego $x + I = 3 + I$. Dado un elemento $P(x) = \sum_{j=0}^{n} a_j x^j$ de $\mathbb{Z}[x]$, por las propiedades de la suma y el producto en A, se tiene que $P(x) + I = (\sum_{j=0}^{n} a_j x^j) + I = \sum_{j=0}^{n} \big((a_j + I)(x+I)^j\big) = \sum_{j=0}^{n} \big((a_j + I)(3+I)^j\big) = P(3) + I$. Como $P(3) \in \mathbb{Z}$, queda demostrado el apartado.

2. Probar que $Q(x) = 6x^3 + 5x^2 + 8x + 12$ es irreducible en $\mathbb{Z}[x]$.

   Solución: El polinomio $Q(x)$ es primitivo en $\mathbb{Z}[x]$ y consideramos su clase módulo 5, es decir, el polinomio $\overline{Q(x)} = x^3 + 3x + 2$ de $(\mathbb{Z}/5\mathbb{Z})[x]$. Comprobamos que $\overline{Q(x)}$ no tiene raíces en $\mathbb{Z}/5\mathbb{Z}$ porque $\overline{Q(0)} = 2$, $\overline{Q(1)} = \overline{Q(2)} = 1$, $\overline{Q(3)} = \overline{Q(4)} = 3$. Por consiguiente, por el **Ejercicio A.44**, como $\mathrm{gr}(\overline{Q(x)}) = 3$ y como $\mathbb{Z}/5\mathbb{Z}$ es un cuerpo (**Ejemplo II.4.8**), tenemos que $\overline{Q(x)}$ es irreducible en $(\mathbb{Z}/5\mathbb{Z})[x]$. Finalmente, por el **Criterio de irreducibilidad módulo 5 (Problema A.64)**, concluimos que $Q(x)$ es irreducible en $\mathbb{Z}[x]$.

3. Encuentra el inverso de $Q(x) + I$ en A.

   Solución: Por el primer apartado sabemos que $Q(x) + I = Q(3) + I = 243 + I$. Como $10 \in I$, $243 - 3 = 240 \in I$, luego $Q(x) + I = 3 + I$. Finalmente, observamos que $(3+I)(7+I) = (21+I) = 1 + I$ porque $21 - 1 = 20 \in I$. En consecuencia, $(Q(x) + I)^{-1} = (7 + I)$.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo si $\#G=\infty$ entonces existe $a\in G$ tal que $O(a)=\infty$.
2. Sea $(G,\cdot)$ un grupo $K\lhd G$ un subgrupo y $a\in G$. Si $O(aK)=n\in\mathbb{N}$, entonces $a^n=1_G$.
3. En D_{37} consideramos el subgrupo R de las rotaciones entonces $R\lhd D_{37}$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G=S_4$ y $H=D_4\times\mathbb{Z}/3\mathbb{Z}$.

1. Determinar todos los homomorfismos de grupos de $f:\mathbb{Z}/3\mathbb{Z}\to G$.
2. Determinar si G y H son o no son grupos isomorfos.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I\subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si $\mathrm{car}(R)=n>0$ y R es un cuerpo, entonces $\#R<\infty$.
2. Si R es un dominio, entonces $\#R\neq 21$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En el anillo de los polinomios con coeficientes racionales, $\mathbb{Q}[x]$, consideramos: $P_1(x)=(3/4)x^7+36x-18$ y $P_2(x)=(4/3)x^3+4x^2-(40/3)x-32$ de $\mathbb{Q}[x]$.

1. Probar que $P_1(x)$ es irreducible en $\mathbb{Q}[x]$ y que $P_2(x)$ no es irreducible en $\mathbb{Q}[x]$.
2. Determinar si $R_1=\mathbb{Q}[x]/(P_1(x))$ y $R_2=\mathbb{Q}[x]/(P_2(x))$ son o no son cuerpos.
3. Encuentra en R_1 el inverso de $((x-2)/200)+(P_1(x))$.

Esquema de una solución de la versión C del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo si $\#G=\infty$ entonces existe $a\in G$ tal que $O(a)=\infty$.

   Solución: Falsa. Tenemos que $(\mathbb{Q},+)$ es un grupo abeliano, luego $\mathbb{Z}\lhd\mathbb{Q}$. Por el Teorema 1.5.6, $(\mathbb{Q}/\mathbb{Z},+)$ es un grupo. Dado un elemento $a+\mathbb{Z}\in\mathbb{Q}/\mathbb{Z}$, existen $p\in\mathbb{Z}$ y $q\in\mathbb{N}$ tales que $a=p/q$. Observamos que $q(a+\mathbb{Z})=q(p/q+\mathbb{Z})=p+\mathbb{Z}=0+\mathbb{Z}$ y concluimos que $O(a+\mathbb{Z})<\infty$. Dados dos elementos distintos $r,s\in[0,1)\cap\mathbb{Q}$ tenemos que $r-s\notin\mathbb{Z}$, luego $r+\mathbb{Z}\neq s+\mathbb{Z}$. En otras palabras, cada elemento de $[0,1)\cap\mathbb{Q}$ define una clase distinta en $\mathbb{Q}/\mathbb{Z}$. Por la Propiedad de Densidad, $\#([0,1)\cap\mathbb{Q})=\infty$, luego $\#(\mathbb{Q}/\mathbb{Z})=\infty$ (Alternativa ver **E82**).

2. Sea $(G,\cdot)$ un grupo $K\lhd G$ un subgrupo y $a\in G$. Si $O(aK)=n\in\mathbb{N}$, entonces $a^n=1_G$.

   Solución: Falsa. Basta considerar $(G,\cdot)=(\mathbb{Z},+)$, $K=3\mathbb{Z}$ y $a=2$. Como $(\mathbb{Z},+)$ es abeliano tenemos que $3\mathbb{Z}\lhd\mathbb{Z}$ y $O(2+3\mathbb{Z})=3$ pero $3\cdot 2=6\neq 0$.

3. En D_{37} consideramos el subgrupo R de las rotaciones entonces $R\lhd D_{37}$.

   Solución: Verdadera. Por el **E156**, sabemos que $\#R=37$ y que $\#D_{37}=2\cdot 37=74$. Por el Teorema de Lagrange, $\#(D_{37}:R)=2$. Por el **E167**, concluimos que $R\lhd D_{37}$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G=S_4$ y $H=D_4\times\mathbb{Z}/3\mathbb{Z}$.

Solución: Lema Auxiliar. Dados dos grupos finitos A,B, y dos elementos $a\in A$, $b\in B$, se tiene que el orden de (a,b) como elemento del grupo producto $A\times B$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a,b))=m.c.m.\{O(a),O(b)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m=m.c.m.\{O(a),O(b)\}$, por la definición del grupo producto tenemos que $(a,b)^m=(a^m,b^m)$. Por la Proposición 1.3.6.2, $a^m=1_A$ y $b^m=1_B$, luego $(a,b)^m=1_{A\times B}$ y, de nuevo la Proposición 1.3.6.2, $O((a,b))\mid m$. Por otra parte, si $O((a,b))=t$ como $(a,b)^t=1_{A\times B}$ se tiene que $a^t=1_A$ y $b^t=1_B$. En consecuencia, por Proposición 1.3.6.2, $O(a)\mid t$ y $O(b)\mid t$, luego $m\mid t$ y concluimos que $t=m$. □

1. Determinar todos los homomorfismos de grupos de $f:\mathbb{Z}/3\mathbb{Z}\to G$.

   Solución: Por la Proposición 1.6.2, como $\mathbb{Z}/3\mathbb{Z}=\langle 1\rangle$ es cíclico f queda completamente determinado por $f(1)$. Además por la Proposición 1.6.2. sabemos que $O(f(1))\mid 3$ y que para cada $b\in G$ con $O(b)\mid 3$ existe un único homomorfismo $f_b:\mathbb{Z}/3\mathbb{Z}\to G$ tal que $f(1)=b$. Por consiguiente determinar los homomorfismos equivale a determinar los elementos $b\in G$ con $O(b)\in\{1,3\}$.
   Observamos que $O(b)=1$ si y sólo si $b=1_G$. Empleando la descomposición en ciclos disjuntos de los elementos de S_4 (**Cor. 1.4.1.**), vemos que los elementos de orden 3 de S_4 son necesariamente ciclos de longitud 3. Por consiguiente, hay 9 homomorfismos de grupos $\mathbb{Z}/3\mathbb{Z}$ en G determinados por $f_1(1)=id$, $f_2(1)=(123)$, $f_3(1)=(132)$, $f_4(1)=(124)$, $f_5(1)=(142)$, $f_6(1)=(134)$, $f_7(1)=(143)$, $f_8(1)=(234)$ y $f_9(1)=(243)$.

2. Determinar si G y H son o no son grupos isomorfos.

   Solución: Observamos que $\#G=\#H=24$, por tanto, no podemos emplear el cardinal para determinar si son isomorfos o no. Por tanto, con la notación del **E156**, si consideramos el elemento $x=((1234),1)$ de H por el Lema Auxiliar $O(x)=12$. Por otro lado, empleando la descomposición en ciclos disjuntos (**Cor. 1.4.1.**), comprobamos que los posibles órdenes de los elementos de $G=S_4$ son $\{1,2,3,4\}$. Deducimos ni de orden 49 de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y G no son isomorfos porque en H hay un elemento de orden 12 y en G no.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si $\mathrm{car}(R) = n > 0$ y R es un cuerpo, entonces $\#R < \infty$.

   Solución: Falso. Por el **Ejemplo II.4.8**, sabemos que $(\mathbb{Z}/3\mathbb{Z},+,\cdot)$ es un dominio. Como los dominios son anillos unitarios, por el **Teorema.II.3.18**, $\mathrm{car}(\mathbb{Z}/3\mathbb{Z}) = O(1_{\mathbb{Z}/3\mathbb{Z}}) = 3$. Por **Ejercicio.A.29**, sabemos que $(\mathbb{Z}/3\mathbb{Z}[x],+,\cdot)$ es un dominio. Por el **Ejercicio.A.24**, sabemos que la característica de $\mathbb{Z}/3\mathbb{Z}[x]$ es la misma que la de $\mathbb{Z}/3\mathbb{Z}[x]$, es decir, $\mathrm{car}(\mathbb{Z}/3\mathbb{Z}[x]) = \mathrm{car}(\mathbb{Z}/3\mathbb{Z}) = 3$. Por el **Ejercicio.A.26**, la característica de $\mathbb{Z}/3\mathbb{Z}[x]$ coincide con la característica de su cuerpo de fracciones $F(\mathbb{Z}/3\mathbb{Z}[x]) = \mathbb{Z}/3\mathbb{Z}(x)$. Finalmente, como $\mathbb{Z}/3\mathbb{Z}[x]$ tiene infinitos elementos, concluimos que $R = \mathbb{Z}/3\mathbb{Z}(x)$ es un cuerpo con infinitos elementos y con $\mathrm{car}(R) = 3 > 0$.

2. Si R es un dominio, entonces $\#R \neq 21$.

   Solución: Cierto. Razonamos por reducción al absurdo y suponemos que $\#R = 21$. Como R es un dominio, por (D.II) es un anillo unitario. Por el **Teorema II.3.18**, se tiene que $\mathrm{car}(R) = O(1_R)$. Por el **Teorema de Lagrange**, $O(1_R) \mid \#R = 21$, luego $O(1_R)$ es $1, 3, 7$ o 21. Por el **Corolario II.4.9**, tenemos que $\mathrm{car}(R) = p$ con p primo. Por tanto, tenemos dos opciones:
   (A) $\mathrm{car}(R) = O(1_R) = 7$. Por la definición de característica, $7x = 0$ para todo $x \in R$, luego $O(x) \mid 7$ para todo $x \in R$. Por el **Teorema de Cauchy para grupos Abelianos**, como $3 \mid \#R$, existe un elemento $r \in R$ con $O(r) = 3$, contradiciendo que $O(r) \mid 7$.
   (B) $\mathrm{car}(R) = O(1_R) = 3$, razonando como en el caso (A) llegamos a contradicción.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En el anillo de los polinomios con coeficientes racionales, $\mathbb{Q}[x]$, consideramos: $P_1(x) = (3/4)x^7 + 36x - 18$ y $P_2(x) = (4/3)x^3 + 4x^2 - (40/3)x - 32$ de $\mathbb{Q}[x]$.

1. Probar que $P_1(x)$ es irreducible en $\mathbb{Q}[x]$ y que $P_2(x)$ no es irreducible en $\mathbb{Q}[x]$.

   Solución: Observamos que podemos escribir $P_1(x) = (3/4)(x^7 + 48x - 24)$ y también que $P_2(x) = (4/3)(x^3 + 3x^2 - 10x - 24)$. Como $Q_1(x) = x^7 + 48x - 24$ es primitivo, por el **Ejercicio A.57**, sabemos que $P_1(x)$ es irreducible en $\mathbb{Q}[x]$ si y solo si $Q_1(x)$ es irreducible en $\mathbb{Z}[x]$. Aplicando el **Criterio de Eisenstein (Problema A.66)** a $Q_1(x)$ para $p = 3$, vemos que $Q_1(x)$ es irreducible en $\mathbb{Z}[x]$. Por el **Teorema de la raíz racional (Ejercicio A.70)**, sabemos que las posibles raíces racionales de $Q_2(x) = x^3 + 3x^2 - 10x - 24$ son divisores de 24. Comprobamos que $-2, 3, -4$ son raíces de $Q_2(x)$ y, en consecuencia, también son raíces de $P_2(x)$. Por el **Ejercicio A. 44**, concluimos que $P_2(x)$ no es irreducible.

2. Determinar si $R_1 = \mathbb{Q}[x]/(P_1(x))$ y $R_2 = \mathbb{Q}[x]/(P_2(x))$ son o no son cuerpos.

   Solución: Por el **Ejercicio A.48** y el apartado 1, R_1 es un cuerpo y R_2 no es un cuerpo.

3. Encuentra en R_1 el inverso de $((x-2)/200) + (P_1(x))$.

   Solución: Mediante el Algoritmo de Euclides calculamos el m.c.d. y los enteros de la identidad de Bezout de $P(x) = (1/200)(x-2)$ y $P_1(x)$, vemos que

   $$\begin{aligned} P_1(x) &= (1)P_1(x) + (0)P(x), \\ P(x) &= (0)P_1(x) + (1)P(x), \\ 150 &= (1)P_1(x) + ((-150)(x^6 + 2x^5 + 4x^4 + 8x^3 + 16x^2 + 32x + 112))P(x). \end{aligned}$$

   En consecuencia, tomando clases módulo $I = (P_1(x))$ en la última igualdad tenemos que

   $$1 + I = (-x^6 - 2x^5 - 4x^4 - 8x^3 - 16x^2 - 32x - 112 + I)(P(x) + I).$$

   En otras palabras, El inverso de $P(x) + I$ en R_1 es $-x^6 - 2x^5 - 4x^4 - 8x^3 - 16x^2 - 32x - 112 + I$.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo $K \lhd G$ un subgrupo y $x, y \in G$. Si $O(x) = O(y) < \infty$, entonces $O(xK) = O(yK)$.
2. Sea $(G,\cdot)$ un grupo si $a, b \in G$ son tales que $O(a) < \infty$ y $O(b) < \infty$, entonces $O(ab) < \infty$.
3. Dado $K \subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K \subseteq A_n$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ y $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times D_7$.

1. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.
2. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio y todo ideal de R distinto de R es primo, entonces R es un cuerpo.
2. Existe R es no conmutativo de modo que se satisface la siguiente propiedad:
   para todos $r, s, t \in R$ con $r \neq 0$ si $rs = tr$, entonces $s = t$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Recordamos que el anillo $\mathbb{C}[x,y]$ se define como $\mathbb{C}[x]([y])$

1. Probar que $x^2 + y^2 - 4$ es un elemento irreducible de $\mathbb{C}[x,y]$.
2. Probar que $\mathbb{C}[x,y]/(x^2 + y^2 - 4)$ es un dominio.
3. Si $I = (x^2 + y^2 - 4)$, probar que $(x + iy) + I \in U(\mathbb{C}[x,y]/I)$.

Esquema de una solución de la versión D del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo $K \lhd G$ un subgrupo y $x, y \in G$. Si $O(x) = O(y) < \infty$, entonces $O(xK) = O(yK)$.

   Solución: Falsa. Basta considerar como grupo $(G,\cdot)$ el grupo producto $(\mathbb{Z}/6\mathbb{Z},+) \times (\mathbb{Z}/6\mathbb{Z},+)$, $K = \langle (2,3)\rangle$, $x = (1,0)$ e $y = (0,1)$. Como G es abeliano se tiene que $K \lhd G$. Observamos que $O(x) = 6$ porque $n(1,0) = (n\,(\text{mód}\,6), 0)$ para todo $n \in \mathbb{N}$. Como 6 es el menor natural n tal que $n \equiv 0(\text{ mód}\,6)$, deducimos que $O(x) = 6$. Análogamente vemos que $O(y) = 6$. Mediante un cálculo directo comprobamos que

   $$K = \{(0,0),(2,3),(4,0),(0,3),(2,0),(4,3)\},$$
   $$x + K = \{(1,0),(3,3),(5,0),(1,3),(3,0),(5,3)\}, \qquad y + K = \{(0,1),(2,4),(4,1),(0,4),(2,1),(4,4)\}.$$

   Observamos que $x + K \neq K$, $y + K \neq K$, $2(x + K) = (2,0) + K = K$ y que

   $$2(y + K) = (0,2) + K = \{(0,2),(2,5),(4,2),(0,5),(2,2),(4,5)\}, \qquad 3(y + K) = (0,3) + K = K.$$

   Por consiguiente, concluimos que $O(x + K) = 2 \neq 3 = O(y + K)$.

2. Sea $(G,\cdot)$ un grupo si $a, b \in G$ son tales que $O(a) < \infty$ y $O(b) < \infty$, entonces $O(ab) < \infty$.

   Solución: Falsa. Consideremos como grupo G, el grupo lineal $(GL(2,\mathbb{R}),\cdot)$ de las matrices 2×2 invertibles con coeficientes en $\mathbb{R}$ y tomamos

   $$A := \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \qquad B := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

   Observamos que $A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id$, $B^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id$, $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Por tanto, deducimos que $O(A) = 2$ y $O(B) = 2$. Sin embargo, probamos por inducción que para todo $n \in \mathbb{N}$ se tiene que $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ y concluimos que $O(AB) = \infty$. (Alternativa ver **E78**).

3. Dado $K \subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K \subseteq A_n$.

   Solución: Verdadera. Tenemos que $\#K = 2k + 1$ con $k \in \mathbb{Z}$, por el Corolario 1.5.1.a), para todo $\alpha \in K$ tenemos que $O(\alpha) \mid 2k + 1$. Por la Proposición 1.3.6.2, $\alpha^{2k+1} = id$. Luego $\alpha^{2k}\alpha = 1$ y deducimos que $\alpha = \alpha^{-2k} = (\alpha^{-k})^2$. Por consiguiente, tanto si $\beta = \alpha^{-k}$ es una permutación par como si β es impar, β^2 es par. En consecuencia, $\alpha = \beta^2 \in A_n$ y concluimos que $K \subseteq A_n$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ y $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times D_7$.

Solución: Lema Auxiliar. Dados tres grupos finitos A, B, C, y tres elementos $a \in A$, $b \in B$,$c \in C$ se tiene que el orden de (a,b,c) como elemento del grupo producto $A \times B \times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a,b,c)) = m.c.m.\{O(a), O(b), O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b), O(c)\}$, por la definición del grupo producto tenemos que $(a,b,c)^m = (a^m, b^m, c^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$, $b^m = 1_B$ y $c^m = 1_C$, luego $(a,b,c)^m = 1_{A\times B\times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a,b,c)) \mid m$. Por otra parte, si $O((a,b,c)) = t$ como $(a,b,c)^t = 1_{A\times B\times C}$ se tiene que $a^t = 1_A$, $b^t = 1_B$ y $c^t = 1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$, $O(b) \mid t$ y $O(c) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

   Solución: Observamos que $\#G = \#H = 196$. Buscamos K con $\#K = 196$ de modo que $K \not\approx H$ y $K \not\approx G$. Consideramos $K := \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, cumple que $\#K = 196$. Por el Teorema 1.3.1, sabemos que el orden de los elementos de $\mathbb{Z}/2\mathbb{Z}$ es 1 o 2, el orden de los elementos de $\mathbb{Z}/4\mathbb{Z}$ es 1, 2 o 4, el orden de los elementos de $\mathbb{Z}/7\mathbb{Z}$ es 1 o 7, el orden de los elementos de $\mathbb{Z}/14\mathbb{Z}$ es 1, 2, 7 o 14. Por otro lado, por el **E156**, comprobamos que los posibles órdenes de los elementos de D_7 son $\{1,2,7\}$. Empleando el Lema Auxiliar vemos que:

- en K hay elementos de orden 4.
- en $\mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \approx G$ no hay ningún elemento de orden 4.
- en H no hay ningún elemento de orden 4.

Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, G y K no son isomorfos y H y K tampoco son isomorfos.

2. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.

   Solución: Consideramos $f : G \to G$ dado por $f(a, b) = (0, b)$. Comprobamos de forma directa que f es un endomorfismo (proyección), que $\mathrm{Ker} f = \mathbb{Z}/14\mathbb{Z} \times \{0\}$ y que $\mathrm{Im} f = \{0\} \times \mathbb{Z}/14\mathbb{Z}$. Demostramos que $\mathrm{Ker} f \approx \mathrm{Im} f \approx \mathbb{Z}/14\mathbb{Z}$, para probar esto se puede ver que ambos grupos son cíclicos de orden 15 y concluir usando la Proposición 1.6.3.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio y todo ideal de R distinto de R es primo, entonces R es un cuerpo.

   Solución: Cierto. Como R es dominio se satisfacen (F.I) y (F.II) basta comprobar que se satisface (F.III), es decir, que $U(R) = R\backslash\{0_R\}$. Como R es un dominio por (D.III), se tiene que $U(R) \subseteq R\backslash\{0_R\}$. Veamos ahora que se cumple la contención contraria. Dado $x \in R\backslash\{0_R\}$ consideremos el ideal $J_1 = (x)$.
   Si $J_1 \subsetneq R$, consideramos el ideal $J_2 = (x^2)$. Como $x^2 \in J_1$ y $J_1 \subsetneq R$, se tiene que $J_2 \subseteq J_1 \subsetneq R$. Por hipótesis, J_2 es primo. Como $x \cdot x = x^2 \in J_2$, tenemos que $x \in J_2$. Por consiguiente, existe $r \in R$ tal que $x = rx^2$ y por la Ley de Cancelación, **Teorema.II.4.6**, $1_R = rx$. Por tanto, $1_R \in J_1$ y tenemos que $J_1 = R$ contradiciendo nuestra suposición.
   Si $J_1 = R$, entonces $1_R \in (x)$, luego existe $u \in R$ tal que $1_R = ux$, es decir, $x \in U(R)$ y concluimos que R es un cuerpo.

2. Existe R es no conmutativo de modo que se satisface la siguiente propiedad:
   para todos $r, s, t \in R$ con $r \neq 0$ si $rs = tr$, entonces $s = t$.

   Solución: Falso. Veamos que si R satisface esta propiedad, entonces R debe ser conmutativo. Dados $x, y \in R$, si $x = 0$ o $y = 0$, por la **Proposición.II.1.9**, $xy = 0_R = yx$. Supongamos que $x \neq 0$ y que $y \neq 0$. Tomamos $s = yx$, $t = xy$ y $r = x$, como por la propiedad asocitiva se tiene que $rs = x(yx) = (xy)x = tr$, aplicando la propiedad, dado que $r = x \neq 0$, concluimos que $yx = s = t = xy$. En consecuencia, hemos visto que R es conmutativo. En resumen, R no puede satisfacer la propiedad y al mismo tiempo ser no conmutativo.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Recordamos que el anillo $\mathbb{C}[x, y]$ se define como $\mathbb{C}[x]([y])$

1. Probar que $x^2 + y^2 - 4$ es un elemento irreducible de $\mathbb{C}[x, y]$.

   Solución: Sabemos que $\mathbb{C}[x, y] = (\mathbb{C}[x])([y])$ como $\mathbb{C}$ es un cuerpo $\mathbb{C}[x]$ es un D.E. y por los **Teoremas II.5.27** y **II.5.22** $\mathbb{C}[x]$ es un D.F.U. Observamos que podemos escribir $P(x, y) = x^2 + y^2 - 4 = a_2(x)y^2 + a_1(x)y + a_0(x)$ con $a_2(x) = 1$, $a_1(x)$ y $a_0(x) = x^2 - 4 = (x + 2)(x - 2)$ que es un polinomio primitivo de $(\mathbb{C}[x])([y])$. Por el **Ejercicio A.43**, tenemos que $x - 2$ es un elemento irreducible de $\mathbb{C}[x]$. Aplicando el **Criterio de Eisenstein (Ejercicio A.66)** a $P(x, y)$ para $p = x - 2$ deducimos que $x^2 + y^2 - 4$ es un elemento irreducible de $\mathbb{C}[x, y]$.

2. Probar que $\mathbb{C}[x, y]/(x^2 + y^2 - 4)$ es un dominio.

   Solución: En el apartado anterior hemos visto que $\mathbb{C}[x]$ es un D.F.U., por el **Problema A.60**, $\mathbb{C}[x, y]$ es un D.F.U.. Por el apartado anterior sabemos que $P(x, y)$ es irreducible, luego por la **Proposición II.5.10**, $P(x, y)$ es primo. Por la **Proposición II.5.6**, $(P(x, y))$ es un ideal primo. Por el **Proposición II.4.14**, $\mathbb{C}[x, y]/(x^2 + y^2 - 4)$ es un dominio.

3. Si $I = (x^2 + y^2 - 4)$, probar que $(x + iy) + I \in U(\mathbb{C}[x, y]/I)$.

   Solución: Basta observar que, por la definición de la suma y el producto en $\mathbb{C}[x, y]/I$ y como $4 + I = x^2 + y^2 + I$, tenemos que $((x + iy) + I)((1/4)(x - iy) + I) = (1/4)(x^2 + y^2) + I = 1 + I$.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo $K \lhd G$ un subgrupo. Si $Z(G) = \{z \in G\,;\, zx = xz \text{ para todo } x \in G\}$, entonces $K \subseteq Z(G)$.
2. Sea $(G,\cdot)$ un grupo abeliano y $a, b \in G$ elementos de orden finito, entonces $O(ab)$ es el $m.c.m(O(a), O(b))$.
3. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = D_3 \times D_4 \times D_5$ y $H = S_5 \times C_2 \times C_2$.

1. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.
2. Determinar si G y H son o no son grupos isomorfos.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio, S es un dominio, $f : S \to R$ es un homomorfismo de anillos e I es maximal en R, entonces $f^{-1}(I)$ es maximal en S.
2. Si $\text{car}(R) = n > 0$, entonces $\text{car}(R \times R \times R) = n^3$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Consideramos el dominio $\mathbb{Z}[\sqrt{15}] = \{a + b\sqrt{15}\,;\, a, b \in \mathbb{Z}\}$.

1. Probar que $7 + 2\sqrt{15}$ es irreducible en $\mathbb{Z}[\sqrt{15}]$.
2. Demuestra que $4 + \sqrt{15}$ es una unidad en $\mathbb{Z}[\sqrt{15}]$ y dar 6 divisores diferentes de 1 en $\mathbb{Z}[\sqrt{15}]$.
3. Probar que $\mathbb{Z}[\sqrt{15}]$ y que $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3}\,;\, a, b \in \mathbb{Z}\}$ no son anillos isomorfos.

Esquema de una solución de la versión E del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo $K \lhd G$ un subgrupo. Si $Z(G) = \{z \in G\,;\, zx = xz \text{ para todo } x \in G\}$, entonces $K \subseteq Z(G)$.

   Solución: Falsa. Con la notación del **E156**, basta considerar $G = D_4$, $K = \langle a\rangle$. Sabemos que $\#K = 4$ y que $\#D_4 = 8$. Por el Teorema de Lagrange, se tiene que $\#(D_4 : K) = 2$ y, por **E167**, concluimos que $K \lhd D_4$. Comprobamos empleando las propiedades del **E156** que $Z(D_4) = \langle a^2\rangle = \{1, a^2\}$, luego $K \not\subseteq Z(D_4)$.

2. Sea $(G,\cdot)$ un grupo abeliano y $a, b \in G$ elementos de orden finito, entonces $O(ab)$ es el $m.c.m(O(a), O(b))$.

   Solución: Falsa. Basta considerar en el grupo $(\mathbb{Z}/12\mathbb{Z}, +)$ los elementos $a = 2$ y $b = 4$, tenemos que $O(a) = 6$ y $O(b) = 3$. Observamos que $m.c.m(O(a), O(b)) = 6$ pero tenemos que $a + b = 6$ y $O(a + b) = O(6) = 2$.

3. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.

   Solución: Falsa. Escribimos α como el producto de ciclos disjuntos $\alpha = (1\,8)(2\,7)(4\,9\,5\,6)$. Por la Proposición 1.4.1, sabemos las permutaciones disjuntas conmutan y se tiene que

   $$\alpha^3 = (1\,8)^3(2\,7)^3(4\,9\,5\,6)^3 = (1\,8)(2\,7)(4\,6\,5\,9).$$

   Finalmente, observamos que $(4\,6\,5\,9) = (4\,9)(4\,5)(4\,6)$. En consecuencia, α^3 descompone como producto de 5 transposiciones y concluimos que es impar y, por tanto, $\alpha^3 \notin A_9$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = D_3 \times D_4 \times D_5$ y $H = S_5 \times C_2 \times C_2$.

Solución: Lema Auxiliar. Dados tres grupos finitos A, B, C, y tres elementos $a \in A$, $b \in B$, $c \in C$ se tiene que el orden de (a, b, c) como elemento del grupo producto $A \times B \times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a, b, c)) = m.c.m.\{O(a), O(b), O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b), O(c)\}$, por la definición del grupo producto tenemos que $(a, b, c)^m = (a^m, b^m, c^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$, $b^m = 1_B$ y $c^m = 1_C$, luego $(a, b, c)^m = 1_{A\times B\times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a, b, c)) \mid m$. Por otra parte, si $O((a, b, c)) = t$ como $(a, b, c)^t = 1_{A\times B\times C}$ se tiene que $a^t = 1_A$, $b^t = 1_B$ y $c^t = 1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$, $O(b) \mid t$ y $O(c) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.

   Solución: Por la Proposición 1.6.2, como $\mathbb{Z}/3\mathbb{Z} = \langle 1\rangle$ es cíclico f queda completamente determinado por $f(1)$. Además por la Proposición 1.6.2. sabemos que $O(f(1)) \mid 3$ y que para cada $b \in G$ con $O(b) \mid 3$ existe un único homomorfismo $f_b : \mathbb{Z}/3\mathbb{Z} \to G$ tal que $f(1) = b$. Por consiguiente determinar los homomorfismos equivale a determinar los elementos $b \in G$ con $O(b) \in \{1, 3\}$.
   Observamos que $O(b) = 1$ si y sólo si $b = 1_G$. Empleando el **E156**, vemos que el posible orden de los elementos de D_3 es $\{1, 2, 3\}$ de los elementos de D_4 es $\{1, 2, 4\}$ y de D_5 es $\{1, 2, 5\}$. Por tanto, por el Lema Auxiliar, deducimos que los elementos de orden 3 de G son $((123), id, id)$ y $((132), id, id)$. Por consiguiente, hay tres homomorfismos de grupos $\mathbb{Z}/3\mathbb{Z}$ en G determinados por $f_1(1) = (id, id, id)$, $f_2(1) = ((123), id, id)$ y $f_3(1) = ((132), id, id)$.

2. Determinar si G y H son o no son grupos isomorfos.

   Solución: Observamos que $\#G = \#H = 480$, por tanto, no podemos emplear el cardinal para determinar si son isomorfos o no. Por tanto, con la notación del **E156**, si consideramos el elemento $x = ((123), (1234), (12345))$ de G por el Lema Auxiliar $O(x) = 60$. Por otro lado, empleando la descomposición en ciclos disjuntos (**Cor. 1.4.1.**), comprobamos que los posibles órdenes de los elementos de S_5 son $\{1, 2, 3, 4, 5, 6\}$. Por el Lema Auxiliar, los posibles órdenes de los elementos de H son $\{1, 2, 3, 4, 5, 6, 10\}$. Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y G no son isomorfos porque en G hay un elemento de orden 60 y en H no.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio, S es un dominio, $f : S \to R$ es un homomorfismo de anillos e I es maximal en R, entonces $f^{-1}(I)$ es maximal en S.

   Solución: Falso. Basta considerar $S = \mathbb{Z}$, $R = \mathbb{Q}$ y $f : \mathbb{Z} \to \mathbb{Q}$ la inclusión canónica dada por $f(m) = m$ para todo $m \in \mathbb{Z}$ que es un homomorfismo de anillos. El ideal $I = (0)$ es maximal en $\mathbb{Q}$, porque $I \neq \mathbb{Q}$ (M.I) y si J es otro ideal con $I \subsetneq J$, existe $q \in J$ con $q \neq 0$, luego $1 = q^{-1}q \in J$ y por tanto, $J = \mathbb{Q}$, es decir, se satisface (M.II). Sin embargo, $f^{-1}(I) = (0)$ que no es un ideal maximal de $\mathbb{Z}$ porque, por ejemplo, $(0) \subsetneq (2) \subsetneq \mathbb{Z}$.

2. Si $\mathrm{car}(R) = n > 0$, entonces $\mathrm{car}(R \times R \times R) = n^3$.

   Solución: Falso. Por el **Ejemplo II.4.8**, sabemos que $(R,+,\cdot) = (\mathbb{Z}/3\mathbb{Z},+,\cdot)$ es un dominio. Como los dominios son anillos unitarios, por el **Teorema.II.3.18**, $\mathrm{car}(\mathbb{Z}/3\mathbb{Z}) = O(1_{\mathbb{Z}/3\mathbb{Z}}) = 3$. Como en el anillo producto $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ las operaciones se definen componete a componete es un anillo unitario con elemento neutro $(1_{\mathbb{Z}/3\mathbb{Z}}, 1_{\mathbb{Z}/3\mathbb{Z}}, 1_{\mathbb{Z}/3\mathbb{Z}})$. Por el **Teorema.II.3.18**, se tiene que $\mathrm{car}(R \times R \times R) = O((1,1,1)) = 3 \neq 27 = 3^3$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Consideramos el dominio $\mathbb{Z}[\sqrt{15}] = \{a + b\sqrt{15}\,;\, a,b \in \mathbb{Z}\}$.

1. Probar que $7 + 2\sqrt{15}$ es irreducible en $\mathbb{Z}[\sqrt{15}]$.

   Solución: Emplearemos las propiedades de la función $N(a + b\sqrt{15}) = a^2 - b^2 15$ del **E460**. Se tiene que $N(7 + 2\sqrt{15}) = -11$. Como -11 es primo en $\mathbb{Z}$, por la propiedad (IV), $7 + 2\sqrt{15}$ es irreducible en $\mathbb{Z}[\sqrt{15}]$.

2. Demuestra que $4 + \sqrt{15}$ es una unidad en $\mathbb{Z}[\sqrt{15}]$ y dar 6 divisores diferentes de 1 en $\mathbb{Z}[\sqrt{15}]$.

   Solución: Con la notación del primer apartado $N(4 + \sqrt{15}) = 16 - 15 = 1$ y, por el **E460**, $u = 4 + \sqrt{15}$ es una unidad en $\mathbb{Z}[\sqrt{15}]$. Observamos que u^n para $n \in \mathbb{N}$ es una unidad porque $N(u^n) = (N(u))^n = 1$. Comprobamos que $u^2 = 31 + 8\sqrt{15}$ y que $u^3 = 244 + 63\sqrt{15}$ y tenemos seis divisores diferentes de 1 en $\mathbb{Z}[\sqrt{15}]$: u, $u^{-1} = 4 - \sqrt{15}$, u^2, $u^{-2} = 31 - 8\sqrt{15}$, u^3 y $u^{-3} = 244 - 63\sqrt{15}$.

3. Probar que $\mathbb{Z}[\sqrt{15}]$ y que $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3}\,;\, a,b \in \mathbb{Z}\}$ no son anillos isomorfos.

   Solución: Razonamos por reducción al absurdo y suponemos que existe $\psi : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}[\sqrt{15}]$ un isomorfismo de anillos. Como ψ es un isomorfismo podemos probar que $\psi(1) = 1$. En consecuencia, por (HA.I), $\psi(3) = \psi(1+1+1) = \psi(1) + \psi(1) + \psi(1) = 3$. Por otro lado, por (HA.II), $\psi(3) = \psi(\sqrt{3}\sqrt{3}) = (\psi(\sqrt{3}))^2$. En resumen, deberían existir $a,b \in \mathbb{Z}$ tales que $(a + b\sqrt{15})^2 = (\psi(\sqrt{3}))^2 = \psi(3) = 3$. Reescribiendo, esta igualdad existirían $a,b \in \mathbb{Z}$ tales que $a^2 + b^2 15 + 2ab\sqrt{15} = 3$. Igualando términos, tenemos dos opciones o $a = 0$ y $b^2 5 = 1$ (imposible) o $b = 0$ y $a^2 = 3$ (imposible) porque $a,b \in \mathbb{Z}$.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo y H_1, H_2 subgrupos de G tales que $H_1 \lhd H_2$ y que $H_2 \lhd G$ entonces $H_1 \lhd G$.
2. Sea $(G,\cdot)$ un grupo si $x,y,z \in G$ entonces $O(xyz) = O(zyx)$.
3. En D_{37} consideramos el subgrupo R de las rotaciones entonces $R \lhd D_{37}$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = C_3 \times C_5 \times C_{15}$ y $H = C_9 \times C_{25}$.

1. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.
2. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si $r,s \in R$ entonces $(r+s)^2 = r^2 + 2rs + s^2$.
2. Si R es un D.F.U. y $a,b,c \in R$ con $a \neq 0$, entonces

   d es un m.c.d. de b y c si y solo si ad es un m.c.d. de ab y ac.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[i] = \{a+bi\,;\, a,b \in \mathbb{Z}\}$, el anillo de los enteros de Gauss, consideramos el ideal $I = (1+7i)$ y el anillo cociente $A = \mathbb{Z}[i]/I$.

1. Probar que $i+I = 7+I$ y deducir que para todo elemento $a+bi$ de $\mathbb{Z}[i]$ existe $k \in \mathbb{Z}$ tal que $(a+bi)+I = k+I$.
2. Construye un homomorfismo de anillos $\Psi : \mathbb{Z} \to A$ sobreyectivo.
3. Encuentra un valor de $n \in \mathbb{N}$ tal que $\mathbb{Z}/n\mathbb{Z} \approx A$. ¿Es A un cuerpo?

Esquema de una solución de la versión F del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo y H_1, H_2 subgrupos de G tales que $H_1 \lhd H_2$ y que $H_2 \lhd G$ entonces $H_1 \lhd G$.

   Solución: Falsa. Con la notación del **E156**, basta considerar $G = D_4$, $H_1 = \{id, b\} = \langle b\rangle$ y $H_2 = \{id, b, a^2, a^2b\} = \langle a, b\rangle$. Sabemos que $\#H_1 = 2$, $\#H_2 = 4$ y que $\#D_4 = 8$. Por el Teorema de Lagrange, se tiene que $\#(H_2 : H_1) = 2$ y $\#(D_4 : H_2) = 2$. Por el **E167**, concluimos que $H_1 \lhd H_2$ y que $H_2 \lhd D_4$. Finalmente, observamos que $aH_1 = \{a, ab\}$ y que $H_1a = \{a, ba\}$ y, por el **E156**, sabemos $ba = a^3b$ y que $a^3b \neq ab$. Por consiguiente, $aH_1 \neq H_1a$ y concluimos que H_1 no es normal en D_4.

2. Sea $(G,\cdot)$ un grupo si $x, y, z \in G$ entonces $O(xyz) = O(zyx)$.

   Solución: Falsa. Basta considerar $G = Q_8$ (ver **E64**) y tomar $x = i$, $y = j$ y $z = k$ tenemos que $xyz = ijk = kk = -1$ luego $O(xyz) = 2$ pero $zyx = kji = k(-k) = 1$ luego $O(zyx) = 1$.

3. En D_{37} consideramos el subgrupo R de las rotaciones entonces $R \lhd D_{37}$.

   Solución: Verdadera. Por el **E156**, sabemos que $\#R = 37$ y que $\#D_{37} = 2 \cdot 37 = 74$. Por el Teorema de Lagrange, $\#(D_{37} : R) = 2$. Por el **E167**, concluimos que $R \lhd D_{37}$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = C_3 \times C_5 \times C_{15}$ y $H = C_9 \times C_{25}$.

Solución: Lema Auxiliar. Dados tres grupos finitos A, B, C, y tres elementos $a \in A$, $b \in B$,$c \in C$ se tiene que el orden de (a, b, c) como elemento del grupo producto $A \times B \times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a, b, c)) = m.c.m.\{O(a), O(b), O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b), O(c)\}$, por la definición del grupo producto tenemos que $(a, b, c)^m = (a^m, b^m, c^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$, $b^m = 1_B$ y $c^m = 1_C$, luego $(a, b, c)^m = 1_{A\times B\times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a, b, c)) \mid m$. Por otra parte, si $O((a, b, c)) = t$ como $(a, b, c)^t = 1_{A\times B\times C}$ se tiene que $a^t = 1_A$, $b^t = 1_B$ y $c^t = 1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$, $O(b) \mid t$ y $O(c) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.

   Solución: Consideramos $f : G \to G$ dado por $f(a, b, c) = (0, c)$. Comprobamos de forma directa que f es un endomorfismo (proyección), que $\mathrm{Ker} f = C_3 \times C_5 \times \{0\}$ y que $\mathrm{Im} f = \{0\} \times \{0\} \times C_{15}$. Finalmente, demostramos que $\mathrm{Ker} f \approx \mathrm{Im} f \approx C_{15}$, para probar esto se puede ver que ambos grupos son cíclicos de orden 15 y concluir usando la Proposición 1.6.3.

2. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

   Solución: Observamos que $\#G = \#H = 225$. Buscamos K con $\#K = 225$ de modo que $K \not\approx H$ y $K \not\approx G$. Consideramos $K := C_9 \times C_5 \times C_5$, cumple que $\#K = 225$. Por el Teorema 1.3.1, sabemos que el orden de los elementos de C_3 es 1 o 3,el orden de los elementos de C_5 es 1 o 5, el orden de los elementos de C_9 es 1, 3 o 9,el orden de los elementos de C_{15} es 1, 3, 5 o 15, y que el orden de los elementos de C_{25} es 1, 5 o 25. Empleando el Lema Auxiliar vemos que:

   - en K no hay ningún elemento de orden 25 pero sí hay elementos de orden 9.
   - en G no hay ningún elemento de orden 25 ni de orden 9.
   - en $C_1 \times C_9 \times C_{25} \approx C_9 \times C_{25} = H$ hay elementos de orden 9 y de orden 25.

   Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y K no son isomorfos y G y K tampoco son isomorfos.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si $r, s \in R$ entonces $(r+s)^2 = r^2 + 2rs + s^2$.

   Solución: Falso. Basta considerar R el anillo de las matrices 2×2 con coeficientes en $\mathbb{R}$, es decir, $(\mathrm{Mat}_{2\times 2}(\mathbb{R}), +, \cdot)$ y tomar $r = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ y $s = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Observamos que

   $$r^2 + 2rs + s^2 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}^2 + 2\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix},$$

   pero $(r+s)^2 = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix}$.

2. Si R es un D.F.U. y $a, b, c \in R$ con $a \neq 0$, entonces

   $$d \text{ es un m.c.d. de } b \text{ y } c \text{ si y solo si } ad \text{ es un m.c.d. de } ab \text{ y } ac.$$

   Solución: Cierto. Supongamos que d es un m.c.d. de b y c. Por (MCD.I), $d \mid b$ y $d \mid c$, luego $ad \mid ab$ y $ad \mid ac$, es decir, ad satisface (MCD.I). Como R es un D.F.U., sabemos que existe x un m.c.d de ab y ac. Como $a \mid ab$ y $a \mid ac$, por (MCD.II), $a \mid x$. Dicho de otro modo, existe $r \in R$ tal que $x = ar$. Por (MCD.I), $x \mid ab$ y $x \mid ac$, luego $ar \mid ab$ y $ar \mid ac$. Como $a \neq 0$ y como R es un dominio, por la Ley de Cancelación, **Teorema.II.4.6**, se tiene que $r \mid b$ y que $r \mid c$. Como d es un m.c.d. de b y c, por (MCD.II), $r \mid d$, luego $x = ar \mid ad$ y como x es un m.c.d de ab y ac concluimos que ad también satisface (MCD.II) para ab y ac. En resumen, ad es un un m.c.d de ab y ac.
   Recíprocamente, supongamos que ad es un m.c.d. de ab y ac. Por (MCD.I), $ad \mid ab$ y $ad \mid ac$, Como $a \neq 0$ y como R es un dominio, por la Ley de Cancelación, **Teorema.II.4.6**, se tiene que $d \mid b$ y $d \mid c$, es decir, d satisface (MCD.I). Si $s \mid b$ y $s \mid c$, tenemos que $as \mid ab$ y $as \mid ac$. Por (MCD.II), $as \mid ad$ y de nuevo por la Ley de Cancelación $s \mid d$, es decir, d satisface (MCD.II).

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[i] = \{a + bi\,;\, a, b \in \mathbb{Z}\}$, el anillo de los enteros de Gauss, consideramos el ideal $I = (1 + 7i)$ y el anillo cociente $A = \mathbb{Z}[i]/I$.

1. Probar que $i+I = 7+I$ y deducir que para todo elemento $a+bi$ de $\mathbb{Z}[i]$ existe $k \in \mathbb{Z}$ tal que $(a+bi)+I = k+I$.

   Solución: Observamos que $i - 7 = i(1 + 7i) \in I$, luego $i + I = 7 + I$. Dado un elemento $a + bi$ de $\mathbb{Z}[i]$ con $a, b \in \mathbb{Z}$, por las propiedades de la suma y el producto en A, se tiene que $(a+bi)+I = (a+I)+(b+I)(7+I) = (a + b7) + I$. En otras palabras, como $a + b7 \in \mathbb{Z}$, queda demostrado el apartado.

2. Construye un homomorfismo de anillos $\Psi : \mathbb{Z} \to A$ sobreyectivo.

   Solución: Basta considerar $\Psi = p \circ f$ donde $f : \mathbb{Z} \to \mathbb{Z}[i]$ es la inyección canónica y $p : \mathbb{Z}[i] \to \mathbb{Z}[i]/I$ es la aplicación de paso al cociente. Como f y p son homomorfismos de anillos, por la **Proposición II.3.3**, Ψ es también un homomorfismo de anillos y está dado por $\Psi(k) = k + I$. Por el apartado anterior, para todo elemento $a + bi$ de $\mathbb{Z}[i]$ existe $k \in \mathbb{Z}$ tal que $(a + bi) + I = k + I$, luego $\Psi(k) = (a + bi) + I$, es decir, Ψ es sobreyectivo.

3. Encuentra un valor de $n \in \mathbb{N}$ tal que $\mathbb{Z}/n\mathbb{Z} \approx A$. ¿Es A un cuerpo?

   Solución: Observamos que dado $k \in \mathbb{Z}$, $k \in \mathrm{Ker}\Psi$ si y solo si $k + I = I$, es decir, si y solo si $k \in I$. Vemos que $k \in I$ si y solo si existen $a, b \in \mathbb{Z}$ con $k = (a + bi)(1 + 7i)$, es decir, si y solo si, existen $a, b \in \mathbb{Z}$, $k = a - 7b$ y $0 = 7a + b$. Deducimos que $k \in \mathrm{Ker}\Psi$ si y solo si existe $a \in \mathbb{Z}$ tal que $k = 50a$, es decir, si y solo si, $k \in 50\mathbb{Z}$, dicho de otro modo, $n = 50$. Como Ψ es sobreyectivo, por **Primer teorema de isomorfía (Teorema II.3.8)**, $\mathbb{Z}/50\mathbb{Z} \approx A$. Por el **Ejemplo II.4.8**, tenemos que $\mathbb{Z}/50\mathbb{Z}$ no es un cuerpo porque 50 no es primo. Deducimos que A tampoco es un cuerpo porque, por ejemplo, la imagen de un divisor de cero no nulo por un isomorfismo es un divisor de cero no nulo. En otras palabras, en A hay divisores de cero no nulos.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo si $x,y,z\in G$ entonces $O(xyz)=O(yzx)$.
2. Dado $K\subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K\subseteq A_n$.
3. Sea $(G,\cdot)$ un grupo no abeliano y $K\lhd G$ un subgrupo no abeliano entonces G/K es no abeliano.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G=S_4$ y $H=D_4\times\mathbb{Z}/3\mathbb{Z}$.

1. Determinar todos los homomorfismos de grupos de $f:\mathbb{Z}/3\mathbb{Z}\to G$.
2. Determinar si G y H son o no son grupos isomorfos.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I\subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio, entonces $\#R\neq 21$.
2. Si R es un D.I.P., entonces R/I es D.I.P.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[x]$, el anillo de los polinomios con coeficientes enteros, consideramos el ideal $I=(10,x-3)$ y el anillo cociente $A=\mathbb{Z}[x]/I$.

1. Probar que $x+I=3+I$ y deducir que para todo elemento $P(x)$ de $\mathbb{Z}[x]$ existe $k\in\mathbb{Z}$ tal que $P(x)+I=k+I$.
2. Probar que $Q(x)=6x^3+5x^2+8x+12$ es irreducible en $\mathbb{Z}[x]$.
3. Encuentra el inverso de $Q(x)+I$ en A.

Esquema de una solución de la versión G del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo si $x,y,z\in G$ entonces $O(xyz)=O(yzx)$.

   Solución: Verdadera. Observamos que $xyz=x(yzx)x^{-1}$, luego aplicando el **E75.(iii)**, deducimos que $O(yzx)=O(x(yzx)x^{-1})=O(xyz)$.

2. Dado $K\subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K\subseteq A_n$.

   Solución: Verdadera. Tenemos que $\#K=2k+1$ con $k\in\mathbb{Z}$, por el Corolario 1.5.1.a), para todo $\alpha\in K$ tenemos que $O(\alpha)\mid 2k+1$. Por la Proposición 1.3.6.2, $\alpha^{2k+1}=id$. Luego $\alpha^{2k}\alpha=1$ y deducimos que $\alpha=\alpha^{-2k}=(\alpha^{-k})^2$. Por consiguiente, tanto si $\beta=\alpha^{-k}$ es una permutación par como si β es impar, β^2 es par. En consecuencia, $\alpha=\beta^2\in A_n$ y concluimos que $K\subseteq A_n$.

3. Sea $(G,\cdot)$ un grupo no abeliano y $K\lhd G$ un subgrupo no abeliano entonces G/K es no abeliano.

   Solución: Falsa. Basta considerar $G=S_4$ y $K=A_4$. Observamos que $(123),(234)\in A_4\subseteq S_4$ y que $(123)(234)=(12)(34)\neq(13)(24)=(234)(123)$ luego G y K no son abelianos. Por el **E116**, $\#A_4=12$ y como $\#S_4=24$, por el Teorema de Lagrange, se tiene que $\#(S_4:A_4)=2$. Por el **E167**, vemos que $A_4\lhd S_4$. Como $\#(S_4:A_4)=\#(S_4/A_4)=2$, por el Corolario 1.5.1.b), el grupo cociente S_4/A_4 es cíclico y, por tanto, es abeliano.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G=S_4$ y $H=D_4\times\mathbb{Z}/3\mathbb{Z}$.

Solución: Lema Auxiliar. Dados dos grupos finitos A,B, y dos elementos $a\in A$, $b\in B$, se tiene que el orden de (a,b) como elemento del grupo producto $A\times B$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a,b))=m.c.m.\{O(a),O(b)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m=m.c.m.\{O(a),O(b)\}$, por la definición del grupo producto tenemos que $(a,b)^m=(a^m,b^m)$. Por la Proposición 1.3.6.2, $a^m=1_A$ y $b^m=1_B$, luego $(a,b)^m=1_{A\times B}$ y, de nuevo la Proposición 1.3.6.2, $O((a,b))\mid m$. Por otra parte, si $O((a,b))=t$ como $(a,b)^t=1_{A\times B}$ se tiene que $a^t=1_A$ y $b^t=1_B$. En consecuencia, por Proposición 1.3.6.2, $O(a)\mid t$ y $O(b)\mid t$, luego $m\mid t$ y concluimos que $t=m$. □

1. Determinar todos los homomorfismos de grupos de $f:\mathbb{Z}/3\mathbb{Z}\to G$.

   Solución: Por la Proposición 1.6.2, como $\mathbb{Z}/3\mathbb{Z}=\langle 1\rangle$ es cíclico f queda completamente determinado por $f(1)$. Además por la Proposición 1.6.2. sabemos que $O(f(1))\mid 3$ y que para cada $b\in G$ con $O(b)\mid 3$ existe un único homomorfismo $f_b:\mathbb{Z}/3\mathbb{Z}\to G$ tal que $f(1)=b$. Por consiguiente determinar los homomorfismos equivale a determinar los elementos $b\in G$ con $O(b)\in\{1,3\}$.
   Observamos que $O(b)=1$ si y sólo si $b=1_G$. Empleando la descomposición en ciclos disjuntos de los elementos de S_4 (**Cor. 1.4.1.**), vemos que los elementos de orden 3 de S_4 son necesariamente ciclos de longitud 3. Por consiguiente, hay 9 homomorfismos de grupos $\mathbb{Z}/3\mathbb{Z}$ en G determinados por $f_1(1)=id$, $f_2(1)=(123)$, $f_3(1)=(132)$, $f_4(1)=(124)$, $f_5(1)=(142)$, $f_6(1)=(134)$, $f_7(1)=(143)$, $f_8(1)=(234)$ y $f_9(1)=(243)$.

2. Determinar si G y H son o no son grupos isomorfos.

   Solución: Observamos que $\#G=\#H=24$, por tanto, no podemos emplear el cardinal para determinar si son isomorfos o no. Por tanto, con la notación del **E156**, si consideramos el elemento $x=((1234),1)$ de H por el Lema Auxiliar $O(x)=12$. Por otro lado, empleando la descomposición en ciclos disjuntos (**Cor. 1.4.1.**), comprobamos que los posibles órdenes de los elementos de $G=S_4$ son $\{1,2,3,4\}$. Deducimos ni de orden 49 de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y G no son isomorfos porque en H hay un elemento de orden 12 y en G no.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio, entonces $\#R \neq 21$.

   Solución: Cierto. Razonamos por reducción al absurdo y suponemos que $\#R = 21$. Como R es un dominio, por (D.II) es un anillo unitario. Por el **Teorema II.3.18**, se tiene que $\text{car}(R) = O(1_R)$. Por el **Teorema de Lagrange**, $O(1_R) \mid \#R = 21$, luego $O(1_R)$ es $1, 3, 7$ o 21. Por el **Corolario II.4.9**, tenemos que $\text{car}(R) = p$ con p primo. Por tanto, tenemos dos opciones:
   (A) $\text{car}(R) = O(1_R) = 7$. Por la definición de característica, $7x = 0$ para todo $x \in R$, luego $O(x) \mid 7$ para todo $x \in R$. Por el **Teorema de Cauchy para grupos Abelianos**, como $3 \mid \#R$, existe un elemento $r \in R$ con $O(r) = 3$, contradiciendo que $O(r) \mid 7$.
   (B) $\text{car}(R) = O(1_R) = 3$, razonando como en el caso (A) llegamos a contradicción.

2. Si R es un D.I.P., entonces R/I es D.I.P.

   Solución: Falso. Basta considerar $(R,+,\cdot) = (\mathbb{Z},+,\cdot)$ e $I = 6\mathbb{Z}$. El anillo cociente R/I es $(\mathbb{Z}/6\mathbb{Z},+,\cdot)$ que no es un dominio porque 6 no es primo (**Ejemplo II.4.8**). En consecuencia R/I no es un dominio de ideales principales (D.I.P.).

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[x]$, el anillo de los polinomios con coeficientes enteros, consideramos el ideal $I = (10, x-3)$ y el anillo cociente $A = \mathbb{Z}[x]/I$.

1. Probar que $x+I = 3+I$ y deducir que para todo elemento $P(x)$ de $\mathbb{Z}[x]$ existe $k \in \mathbb{Z}$ tal que $P(x)+I = k+I$.

   Solución: Observamos que $x - 3 \in I$, luego $x + I = 3 + I$. Dado un elemento $P(x) = \sum_{j=0}^{n} a_j x^j$ de $\mathbb{Z}[x]$, por las propiedades de la suma y el producto en A, se tiene que $P(x) + I = (\sum_{j=0}^{n} a_j x^j) + I = \sum_{j=0}^{n} \left((a_j + I)(x + I)^j\right) = \sum_{j=0}^{n} \left((a_j + I)(3 + I)^j\right) = P(3) + I$. Como $P(3) \in \mathbb{Z}$, queda demostrado el apartado.

2. Probar que $Q(x) = 6x^3 + 5x^2 + 8x + 12$ es irreducible en $\mathbb{Z}[x]$.

   Solución: El polinomio $Q(x)$ es primitivo en $\mathbb{Z}[x]$ y consideramos su clase módulo 5, es decir, el polinomio $\overline{Q(x)} = x^3 + 3x + 2$ de $(\mathbb{Z}/5\mathbb{Z})[x]$. Comprobamos que $\overline{Q(x)}$ no tiene raíces en $\mathbb{Z}/5\mathbb{Z}$ porque $\overline{Q(0)} = 2$, $\overline{Q(1)} = \overline{Q(2)} = 1$, $\overline{Q(3)} = \overline{Q(4)} = 3$. Por consiguiente, por el **Ejercicio A.44**, como $\text{gr}(\overline{Q(x)}) = 3$ y como $\mathbb{Z}/5\mathbb{Z}$ es un cuerpo (**Ejemplo II.4.8**), tenemos que $\overline{Q(x)}$ es irreducible en $(\mathbb{Z}/5\mathbb{Z})[x]$. Finalmente, por el **Criterio de irreducibilidad módulo 5 (Problema A.64)**, concluimos que $Q(x)$ es irreducible en $\mathbb{Z}[x]$.

3. Encuentra el inverso de $Q(x) + I$ en A.

   Solución: Por el primer apartado sabemos que $Q(x) + I = Q(3) + I = 243 + I$. Como $10 \in I$, $243 - 3 = 240 \in I$, luego $Q(x) + I = 3 + I$. Finalmente, observamos que $(3 + I)(7 + I) = (21 + I) = 1 + I$ porque $21 - 1 = 20 \in I$. En consecuencia, $(Q(x) + I)^{-1} = (7 + I)$.

UNIVERSIDAD DE CANTABRIA

Examen final
miércoles 3 de junio de 2020
Convocatoria ordinaria

G90 - Estructuras Algebraicas
Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.
2. Sea $(G, \cdot)$ un grupo $K \lhd G$ un subgrupo y $a \in G$. Si $O(aK) = n \in \mathbb{N}$, entonces $a^n = 1_G$.
3. Sea $(G, \cdot)$ un grupo finito y abeliano, si $d \mid \#G$ entonces existe $a \in G$ tal que $O(a) = d$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ y $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times D_7$.

1. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.
2. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio y todo ideal de R distinto de R es primo, entonces R es un cuerpo.
2. Si R es un D.I.P., entonces cada ideal del anillo cociente R/I es principal.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En el anillo de los polinomios con coeficientes racionales, $\mathbb{Q}[x]$, consideramos: $P_1(x) = (3/4)x^7 + 36x - 18$ y $P_2(x) = (4/3)x^3 + 4x^2 - (40/3)x - 32$ de $\mathbb{Q}[x]$.

1. Probar que $P_1(x)$ es irreducible en $\mathbb{Q}[x]$ y que $P_2(x)$ no es irreducible en $\mathbb{Q}[x]$.
2. Determinar si $R_1 = \mathbb{Q}[x]/(P_1(x))$ y $R_2 = \mathbb{Q}[x]/(P_2(x))$ son o no son cuerpos.
3. Encuentra en R_1 el inverso de $((x-2)/200) + (P_1(x))$.

Esquema de una solución de la versión H del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.

   Solución: Falsa. Escribimos α como el producto de ciclos disjuntos $\alpha = (1\,8)(2\,7)(4\,9\,5\,6)$. Por la Proposición 1.4.1, sabemos las permutaciones disjuntas conmutan y se tiene que

   $$\alpha^3 = (1\,8)^3(2\,7)^3(4\,9\,5\,6)^3 = (1\,8)(2\,7)(4\,6\,5\,9).$$

   Finalmente, observamos que $(4\,6\,5\,9) = (4\,9)(4\,5)(4\,6)$. En consecuencia, α^3 descompone como producto de 5 transposiciones y concluimos que es impar y, por tanto, $\alpha^3 \notin A_9$.

2. Sea $(G, \cdot)$ un grupo $K \lhd G$ un subgrupo y $a \in G$. Si $O(aK) = n \in \mathbb{N}$, entonces $a^n = 1_G$.

   Solución: Falsa. Basta considerar $(G, \cdot) = (\mathbb{Z}, +)$, $K = 3\mathbb{Z}$ y $a = 2$. Como $(\mathbb{Z}, +)$ es abeliano tenemos que $3\mathbb{Z} \lhd \mathbb{Z}$ y $O(2 + 3\mathbb{Z}) = 3$ pero $3 \cdot 2 = 6 \neq 0$.

3. Sea $(G, \cdot)$ un grupo finito y abeliano, si $d \mid \#G$ entonces existe $a \in G$ tal que $O(a) = d$.

   Solución: Falsa. Basta considerar $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ que es un grupo finito y abeliano. Tenemos que $\#G = 4$, pero $O((0,0)) = 1$ y $O((0,1)) = O((1,0)) = O((1,1)) = 2$, es decir, no existe $a \in G$ con $O(a) = 4$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ y $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times D_7$.

Solución: Lema Auxiliar. Dados tres grupos finitos A, B, C, y tres elementos $a \in A$, $b \in B$,$c \in C$ se tiene que el orden de (a, b, c) como elemento del grupo producto $A \times B \times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a, b, c)) = m.c.m.\{O(a), O(b), O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b), O(c)\}$, por la definición del grupo producto tenemos que $(a, b, c)^m = (a^m, b^m, c^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$, $b^m = 1_B$ y $c^m = 1_C$, luego $(a, b, c)^m = 1_{A\times B\times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a, b, c)) \mid m$. Por otra parte, si $O((a, b, c)) = t$ como $(a, b, c)^t = 1_{A\times B\times C}$ se tiene que $a^t = 1_A$, $b^t = 1_B$ y $c^t = 1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$, $O(b) \mid t$ y $O(c) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.

   Solución: Consideramos $f : G \to G$ dado por $f(a, b) = (0, b)$. Comprobamos de forma directa que f es un endomorfismo (proyección), que $\mathrm{Ker} f = \mathbb{Z}/14\mathbb{Z} \times \{0\}$ y que $\mathrm{Im} f = \{0\} \times \mathbb{Z}/14\mathbb{Z}$. Demostramos que $\mathrm{Ker} f \approx \mathrm{Im} f \approx \mathbb{Z}/14\mathbb{Z}$, para probar esto se puede ver que ambos grupos son cíclicos de orden 15 y concluir usando la Proposición 1.6.3.

2. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

   Solución: Observamos que $\#G = \#H = 196$. Buscamos K con $\#K = 196$ de modo que $K \not\approx H$ y $K \not\approx G$. Consideramos $K := \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, cumple que $\#K = 196$. Por el Teorema 1.3.1, sabemos que el orden de los elementos de $\mathbb{Z}/2\mathbb{Z}$ es 1 o 2, el orden de los elementos de $\mathbb{Z}/4\mathbb{Z}$ es 1, 2 o 4, el orden de los elementos de $\mathbb{Z}/7\mathbb{Z}$ es 1 o 7, el orden de los elementos de $\mathbb{Z}/14\mathbb{Z}$ es 1, 2, 7 o 14. Por otro lado, por el **E156**, comprobamos que los posibles órdenes de los elementos de D_7 son $\{1, 2, 7\}$. Empleando el Lema Auxiliar vemos que:

   - en K hay elementos de orden 4.
   - en $\mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \approx G$ no hay ningún elemento de orden 4.
   - en H no hay ningún elemento de orden 4.

   Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, G y K no son isomorfos y H y K tampoco son isomorfos.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio y todo ideal de R distinto de R es primo, entonces R es un cuerpo.

   Solución: Cierto. Como R es dominio se satisfacen (F.I) y (F.II) basta comprobar que se satisface (F.III), es decir, que $U(R) = R\backslash\{0_R\}$. Como R es un dominio por (D.III), se tiene que $U(R) \subseteq R\backslash\{0_R\}$. Veamos ahora que se cumple la contención contraria. Dado $x \in R\backslash\{0_R\}$ consideremos el ideal $J_1 = (x)$.
   Si $J_1 \subsetneq R$, consideramos el ideal $J_2 = (x^2)$. Como $x^2 \in J_1$ y $J_1 \subsetneq R$, se tiene que $J_2 \subseteq J_1 \subsetneq R$. Por hipótesis, J_2 es primo. Como $x \cdot x = x^2 \in J_2$, tenemos que $x \in J_2$. Por consiguiente, existe $r \in R$ tal que $x = rx^2$ y por la Ley de Cancelación, **Teorema.II.4.6**, $1_R = rx$. Por tanto, $1_R \in J_1$ y tenemos que $J_1 = R$ contradiciendo nuestra suposición.
   Si $J_1 = R$, entonces $1_R \in (x)$, luego existe $u \in R$ tal que $1_R = ux$, es decir, $x \in U(R)$ y concluimos que R es un cuerpo.

2. Si R es un D.I.P., entonces cada ideal del anillo cociente R/I es principal.

   Solución: Cierto. Consideramos el homomorfismo de anillos sobreyectivo $p : R \to R/I$ de paso al cociente dado por $p(a) = a + I$. Dado L un ideal de R/I, por la **Proposición II.3.4.(vi)**, sabemos que $p^{-1}(L)$ es un ideal de R. Como R es un D.I.P., existe $x \in R$ tal que $\big(x\big) = p^{-1}(L)$.
   Veamos que $L = \big(p(x)\big)$. Como $x \in \big(x\big) = p^{-1}(L)$, se tiene que $p(x) \in L$ luego $\big(p(x)\big) \subseteq L$. Recíprocamente, dado $\ell \in L$ como p es sobreyectiva, existe $y \in R$ tal que $p(y) = \ell$. Por consiguiente, $y \in \big(x\big) = p^{-1}(L)$. Como R es un dominio, $\big(x\big) = \{rx; r \in R\}$, es decir, $y = rx$ para algún $r \in R$. Como p es homomorfismo de anillos, $\ell = p(y) = p(r)p(x)$. Deducimos que $\ell \in \big(p(x)\big)$ y concluimos que $L \subseteq \big(p(x)\big)$. En resumen hemos probado que cada ideal L del anillo cociente R/I está generado por un único elemento, es decir, es principal.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En el anillo de los polinomios con coeficientes racionales, $\mathbb{Q}[x]$, consideramos: $P_1(x) = (3/4)x^7 + 36x - 18$ y $P_2(x) = (4/3)x^3 + 4x^2 - (40/3)x - 32$ de $\mathbb{Q}[x]$.

1. Probar que $P_1(x)$ es irreducible en $\mathbb{Q}[x]$ y que $P_2(x)$ no es irreducible en $\mathbb{Q}[x]$.

   Solución: Observamos que podemos escribir $P_1(x) = (3/4)(x^7 + 48x - 24)$ y también que $P_2(x) = (4/3)(x^3 + 3x^2 - 10x - 24)$. Como $Q_1(x) = x^7 + 48x - 24$ es primitivo, por el **Ejercicio A.57**, sabemos que $P_1(x)$ es irreducible en $\mathbb{Q}[x]$ si y solo si $Q_1(x)$ es irreducible en $\mathbb{Z}[x]$. Aplicando el **Criterio de Eisenstein (Problema A.66)** a $Q_1(x)$ para $p = 3$, vemos que $Q_1(x)$ es irreducible en $\mathbb{Z}[x]$. Por el **Teorema de la raíz racional (Ejercicio A.70)**, sabemos que las posibles raíces racionales de $Q_2(x) = x^3 + 3x^2 - 10x - 24$ son divisores de 24. Comprobamos que $-2, 3, -4$ son raíces de $Q_2(x)$ y, en consecuencia, también son raíces de $P_2(x)$. Por el **Ejercicio A. 44**, concluimos que $P_2(x)$ no es irreducible.

2. Determinar si $R_1 = \mathbb{Q}[x]/(P_1(x))$ y $R_2 = \mathbb{Q}[x]/(P_2(x))$ son o no son cuerpos.

   Solución: Por el **Ejercicio A.48** y el apartado 1, R_1 es un cuerpo y R_2 no es un cuerpo.

3. Encuentra en R_1 el inverso de $((x-2)/200) + (P_1(x))$.

   Solución: Mediante el Algoritmo de Euclides calculamos el m.c.d. y los enteros de la identidad de Bezout de $P(x) = (1/200)(x-2)$ y $P_1(x)$, vemos que

   $$\begin{aligned} P_1(x) &= (1)P_1(x) + (0)P(x), \\ P(x) &= (0)P_1(x) + (1)P(x), \\ 150 &= (1)P_1(x) + ((-150)(x^6 + 2x^5 + 4x^4 + 8x^3 + 16x^2 + 32x + 112))P(x). \end{aligned}$$

   En consecuencia, tomando clases módulo $I = (P_1(x))$ en la última igualdad tenemos que

   $$1 + I = (-x^6 - 2x^5 - 4x^4 - 8x^3 - 16x^2 - 32x - 112 + I)(P(x) + I).$$

   En otras palabras, El inverso de $P(x) + I$ en R_1 es $-x^6 - 2x^5 - 4x^4 - 8x^3 - 16x^2 - 32x - 112 + I$.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. En D_{37} consideramos el subgrupo R de las rotaciones entonces $R \lhd D_{37}$.
2. Sea $(G, \cdot)$ un grupo si hay un elemento $a \in G$ de orden 18, entonces hay por lo menos 6 elementos de orden 18.
3. Sea $(G, \cdot)$ un grupo $K \lhd G$ un subgrupo y $x, y \in G$. Si $O(x) = O(y) < \infty$, entonces $O(xK) = O(yK)$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = D_3 \times D_4 \times D_5$ y $H = S_5 \times C_2 \times C_2$.

1. Determinar si G y H son o no son grupos isomorfos.
2. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si $\mathrm{car}(R) = n > 0$, entonces $\mathrm{car}(R \times R \times R) = n^3$.
2. Si $\mathrm{car}(R) = n > 0$ y R es un cuerpo, entonces $\#R < \infty$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Recordamos que el anillo $\mathbb{C}[x, y]$ se define como $\mathbb{C}[x]([y])$

1. Probar que $x^2 + y^2 - 4$ es un elemento irreducible de $\mathbb{C}[x, y]$.
2. Probar que $\mathbb{C}[x, y]/(x^2 + y^2 - 4)$ es un dominio.
3. Si $I = (x^2 + y^2 - 4)$, probar que $(x + iy) + I \in U(\mathbb{C}[x, y]/I)$.

Esquema de una solución de la versión I del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. En D_{37} consideramos el subgrupo R de las rotaciones entonces $R \lhd D_{37}$.

   Solución: Verdadera. Por el **E156**, sabemos que $\#R = 37$ y que $\#D_{37} = 2 \cdot 37 = 74$. Por el Teorema de Lagrange, $\#(D_{37} : R) = 2$. Por el **E167**, concluimos que $R \lhd D_{37}$.

2. Sea $(G, \cdot)$ un grupo si hay un elemento $a \in G$ de orden 18, entonces hay por lo menos 6 elementos de orden 18.

   Solución: Verdadera. Por la Proposición 1.3.6, $\#(\langle a \rangle) = O(a) = 18$. Por el Teorema 1.3.1.c), en $\langle a \rangle$ hay $\varphi(18)$ elementos de orden 18. Por el **E13**, $\varphi(18) = 18(1/2)(2/3) = 6$ y, como $\langle a \rangle \subseteq G$, concluimos que hay por lo menos 6 elementos de orden 18 en G.

3. Sea $(G, \cdot)$ un grupo $K \lhd G$ un subgrupo y $x, y \in G$. Si $O(x) = O(y) < \infty$, entonces $O(xK) = O(yK)$.

   Solución: Falsa. Basta considerar como grupo $(G, \cdot)$ el grupo producto $(\mathbb{Z}/6\mathbb{Z}, +) \times (\mathbb{Z}/6\mathbb{Z}, +)$, $K = \langle (2,3) \rangle$, $x = (1,0)$ e $y = (0,1)$. Como G es abeliano se tiene que $K \lhd G$. Observamos que $O(x) = 6$ porque $n(1,0) = (n \,(\text{mód}\, 6), 0)$ para todo $n \in \mathbb{N}$. Como 6 es el menor natural n tal que $n \equiv 0 (\text{mód}\, 6)$, deducimos que $O(x) = 6$. Análogamente vemos que $O(y) = 6$. Mediante un cálculo directo comprobamos que

   $$K = \{(0,0), (2,3), (4,0), (0,3), (2,0), (4,3)\},$$
   $$x + K = \{(1,0), (3,3), (5,0), (1,3), (3,0), (5,3)\}, \qquad y + K = \{(0,1), (2,4), (4,1), (0,4), (2,1), (4,4)\}.$$

   Observamos que $x + K \neq K$, $y + K \neq K$, $2(x + K) = (2,0) + K = K$ y que

   $$2(y + K) = (0,2) + K = \{(0,2), (2,5), (4,2), (0,5), (2,2), (4,5)\}, \qquad 3(y + K) = (0,3) + K = K.$$

   Por consiguiente, concluimos que $O(x + K) = 2 \neq 3 = O(y + K)$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = D_3 \times D_4 \times D_5$ y $H = S_5 \times C_2 \times C_2$.

Solución: Lema Auxiliar. Dados tres grupos finitos A, B, C, y tres elementos $a \in A$, $b \in B$, $c \in C$ se tiene que el orden de (a, b, c) como elemento del grupo producto $A \times B \times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a, b, c)) = m.c.m.\{O(a), O(b), O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b), O(c)\}$, por la definición del grupo producto tenemos que $(a, b, c)^m = (a^m, b^m, c^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$, $b^m = 1_B$ y $c^m = 1_C$, luego $(a, b, c)^m = 1_{A \times B \times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a, b, c)) \mid m$. Por otra parte, si $O((a, b, c)) = t$ como $(a, b, c)^t = 1_{A \times B \times C}$ se tiene que $a^t = 1_A$, $b^t = 1_B$ y $c^t = 1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$, $O(b) \mid t$ y $O(c) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Determinar si G y H son o no son grupos isomorfos.

   Solución: Observamos que $\#G = \#H = 480$, por tanto, no podemos emplear el cardinal para determinar si son isomorfos o no. Por tanto, con la notación del **E156**, si consideramos el elemento $x = ((123), (1234), (12345))$ de G por el Lema Auxiliar $O(x) = 60$. Por otro lado, empleando la descomposición en ciclos disjuntos (**Cor. 1.4.1.**), comprobamos que los posibles órdenes de los elementos de S_5 son $\{1, 2, 3, 4, 5, 6\}$. Por el Lema Auxiliar, los posibles órdenes de los elementos de H son $\{1, 2, 3, 4, 5, 6, 10\}$. Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y G no son isomorfos porque en G hay un elemento de orden 60 y en H no.

2. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.

Solución: Por la Proposición 1.6.2, como $\mathbb{Z}/3\mathbb{Z} = \langle 1 \rangle$ es cíclico f queda completamente determinado por $f(1)$. Además por la Proposición 1.6.2. sabemos que $O(f(1)) \mid 3$ y que para cada $b \in G$ con $O(b) \mid 3$ existe un único homomorfismo $f_b : \mathbb{Z}/3\mathbb{Z} \to G$ tal que $f(1) = b$. Por consiguiente determinar los homomorfismos equivale a determinar los elementos $b \in G$ con $O(b) \in \{1, 3\}$.
Observamos que $O(b) = 1$ si y sólo si $b = 1_G$. Empleando el **E156**, vemos que el posible orden de los elementos de D_3 es $\{1, 2, 3\}$ de los elementos de D_4 es $\{1, 2, 4\}$ y de D_5 es $\{1, 2, 5\}$. Por tanto, por el Lema Auxiliar, deducimos que los elementos de orden 3 de G son $((123), id, id)$ y $((132), id, id)$. Por consiguiente, hay tres homomorfismos de grupos $\mathbb{Z}/3\mathbb{Z}$ en G determinados por $f_1(1) = (id, id, id)$, $f_2(1) = ((123), id, id)$ y $f_3(1) = ((132), id, id)$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si $\text{car}(R) = n > 0$, entonces $\text{car}(R \times R \times R) = n^3$.

   Solución: Falso. Por el **Ejemplo II.4.8**, sabemos que $(R, +, \cdot) = (\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ es un dominio. Como los dominios son anillos unitarios, por el **Teorema.II.3.18**, $\text{car}(\mathbb{Z}/3\mathbb{Z}) = O(1_{\mathbb{Z}/3\mathbb{Z}}) = 3$. Como en el anillo producto $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ las operaciones se definen componete a componete es un anillo unitario con elemento neutro $(1_{\mathbb{Z}/3\mathbb{Z}}, 1_{\mathbb{Z}/3\mathbb{Z}}, 1_{\mathbb{Z}/3\mathbb{Z}})$. Por el **Teorema.II.3.18**, se tiene que $\text{car}(R \times R \times R) = O((1, 1, 1)) = 3 \neq 27 = 3^3$.

2. Si $\text{car}(R) = n > 0$ y R es un cuerpo, entonces $\#R < \infty$.

   Solución: Falso. Por el **Ejemplo II.4.8**, sabemos que $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ es un dominio. Como los dominios son anillos unitarios, por el **Teorema.II.3.18**, $\text{car}(\mathbb{Z}/3\mathbb{Z}) = O(1_{\mathbb{Z}/3\mathbb{Z}}) = 3$. Por **Ejercicio.A.29**, sabemos que $(\mathbb{Z}/3\mathbb{Z}[x], +, \cdot)$ es un dominio. Por el **Ejercicio.A.24**, sabemos que la característica de $\mathbb{Z}/3\mathbb{Z}[x]$ es la misma que la de $\mathbb{Z}/3\mathbb{Z}[x]$, es decir, $\text{car}(\mathbb{Z}/3\mathbb{Z}[x]) = \text{car}(\mathbb{Z}/3\mathbb{Z}) = 3$. Por el **Ejercicio.A.26**, la característica de $\mathbb{Z}/3\mathbb{Z}[x]$ coincide con la característica de su cuerpo de fracciones $F(\mathbb{Z}/3\mathbb{Z}[x]) = \mathbb{Z}/3\mathbb{Z}(x)$. Finalmente, como $\mathbb{Z}/3\mathbb{Z}[x]$ tiene infinitos elementos, concluimos que $R = \mathbb{Z}/3\mathbb{Z}(x)$ es un cuerpo con infinitos elementos y con $\text{car}(R) = 3 > 0$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Recordamos que el anillo $\mathbb{C}[x, y]$ se define como $\mathbb{C}[x]([y])$

1. Probar que $x^2 + y^2 - 4$ es un elemento irreducible de $\mathbb{C}[x, y]$.

   Solución: Sabemos que $\mathbb{C}[x, y] = (\mathbb{C}[x])([y])$ como $\mathbb{C}$ es un cuerpo $\mathbb{C}[x]$ es un D.E. y por los **Teoremas II.5.27** y **II.5.22** $\mathbb{C}[x]$ es un D.F.U. Observamos que podemos escribir $P(x, y) = x^2 + y^2 - 4 = a_2(x)y^2 + a_1(x)y + a_0(x)$ con $a_2(x) = 1$, $a_1(x)$ y $a_0(x) = x^2 - 4 = (x + 2)(x - 2)$ que es un polinomio primitivo de $(\mathbb{C}[x])([y])$. Por el **Ejercicio A.43**, tenemos que $x - 2$ es un elemento irreducible de $\mathbb{C}[x]$. Aplicando el **Criterio de Eisenstein (Ejercicio A.66)** a $P(x, y)$ para $p = x - 2$ deducimos que $x^2 + y^2 - 4$ es un elemento irreducible de $\mathbb{C}[x, y]$.

2. Probar que $\mathbb{C}[x, y]/(x^2 + y^2 - 4)$ es un dominio.

   Solución: En el apartado anterior hemos visto que $\mathbb{C}[x]$ es un D.F.U., por el **Problema A.60**, $\mathbb{C}[x, y]$ es un D.F.U.. Por el apartado anterior sabemos que $P(x, y)$ es irreducible, luego por la **Proposición II.5.10**, $P(x, y)$ es primo. Por la **Proposición II.5.6**, $(P(x, y))$ es un ideal primo. Por el **Proposición II.4.14**, $\mathbb{C}[x, y]/(x^2 + y^2 - 4)$ es un dominio.

3. Si $I = (x^2 + y^2 - 4)$, probar que $(x + iy) + I \in U(\mathbb{C}[x, y]/I)$.

   Solución: Basta observar que, por la definición de la suma y el producto en $\mathbb{C}[x, y]/I$ y como $4 + I = x^2 + y^2 + I$, tenemos que $((x + iy) + I)((1/4)(x - iy) + I) = (1/4)(x^2 + y^2) + I = 1 + I$.

UNIVERSIDAD DE CANTABRIA

EXAMEN FINAL
miércoles 3 de junio de 2020
CONVOCATORIA ORDINARIA

G90 - Estructuras Algebraicas
Curso 2019-2020

INSTRUCCIONES SOBRE EL EXAMEN FINAL

REALIZACIÓN DEL EXAMEN

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

DOCUMENTO PDF DEL EXAMEN

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

ENTREGA DEL EXAMEN

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo si $\#G=\infty$ entonces existe $a\in G$ tal que $O(a)=\infty$.
2. Sea $(G,\cdot)$ un grupo $K\lhd G$ un subgrupo. Si $Z(G)=\{z\in G\,;\, zx=xz \text{ para todo } x\in G\}$, entonces $K\subseteq Z(G)$.
3. Dado $K\subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K\subseteq A_n$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G=C_3\times C_5\times C_{15}$ y $H=C_9\times C_{25}$.

1. Construir, si es posible, un endomorfismo $f:G\to G$ tal que $\mathrm{Ker}f\approx \mathrm{Im}f$.
2. Determinar razonadamente si existe K con $\#K=\#G$ de modo que $K\not\approx H$ y $K\not\approx G$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I\subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un D.F.U. y $a,b,c\in R$ con $a\neq 0$, entonces

   $$d \text{ es un m.c.d. de } b \text{ y } c \text{ si y solo si } ad \text{ es un m.c.d. de } ab \text{ y } ac.$$

2. Existe R es no conmutativo de modo que se satisface la siguiente propiedad:
   para todos $r,s,t\in R$ con $r\neq 0$ si $rs=tr$, entonces $s=t$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Consideramos el dominio $\mathbb{Z}[\sqrt{15}]=\{a+b\sqrt{15}\,;\, a,b\in\mathbb{Z}\}$.

1. Probar que $7+2\sqrt{15}$ es irreducible en $\mathbb{Z}[\sqrt{15}]$.
2. Demuestra que $4+\sqrt{15}$ es una unidad en $\mathbb{Z}[\sqrt{15}]$ y dar 6 divisores diferentes de 1 en $\mathbb{Z}[\sqrt{15}]$.
3. Probar que $\mathbb{Z}[\sqrt{15}]$ y que $\mathbb{Z}[\sqrt{3}]=\{a+b\sqrt{3}\,;\, a,b\in\mathbb{Z}\}$ no son anillos isomorfos.

Esquema de una solución de la versión J del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo si $\#G=\infty$ entonces existe $a\in G$ tal que $O(a)=\infty$.

   Solución: Falsa. Tenemos que $(\mathbb{Q},+)$ es un grupo abeliano, luego $\mathbb{Z}\lhd\mathbb{Q}$. Por el Teorema 1.5.6, $(\mathbb{Q}/\mathbb{Z},+)$ es un grupo. Dado un elemento $a+\mathbb{Z}\in\mathbb{Q}/\mathbb{Z}$, existen $p\in\mathbb{Z}$ y $q\in\mathbb{N}$ tales que $a=p/q$. Observamos que $q(a+\mathbb{Z})=q(p/q+\mathbb{Z})=p+\mathbb{Z}=0+\mathbb{Z}$ y concluimos que $O(a+\mathbb{Z})<\infty$. Dados dos elementos distintos $r,s\in[0,1)\cap\mathbb{Q}$ tenemos que $r-s\notin\mathbb{Z}$, luego $r+\mathbb{Z}\neq s+\mathbb{Z}$. En otras palabras, cada elemento de $[0,1)\cap\mathbb{Q}$ define una clase distinta en $\mathbb{Q}/\mathbb{Z}$. Por la Propiedad de Densidad, $\#([0,1)\cap\mathbb{Q})=\infty$, luego $\#(\mathbb{Q}/\mathbb{Z})=\infty$ (Alternativa ver **E82**).

2. Sea $(G,\cdot)$ un grupo $K\lhd G$ un subgrupo. Si $Z(G)=\{z\in G\,;\,zx=xz \text{ para todo } x\in G\}$, entonces $K\subseteq Z(G)$.

   Solución: Falsa. Con la notación del **E156**, basta considerar $G=D_4$, $K=\langle a\rangle$. Sabemos que $\#K=4$ y que $\#D_4=8$. Por el Teorema de Lagrange, se tiene que $\#(D_4:K)=2$ y, por **E167**, concluimos que $K\lhd D_4$. Comprobamos empleando las propiedades del **E156** que $Z(D_4)=\langle a^2\rangle=\{1,a^2\}$, luego $K\not\subseteq Z(D_4)$.

3. Dado $K\subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K\subseteq A_n$.

   Solución: Verdadera. Tenemos que $\#K=2k+1$ con $k\in\mathbb{Z}$, por el Corolario 1.5.1.a), para todo $\alpha\in K$ tenemos que $O(\alpha)\mid 2k+1$. Por la Proposición 1.3.6.2, $\alpha^{2k+1}=id$. Luego $\alpha^{2k}\alpha=1$ y deducimos que $\alpha=\alpha^{-2k}=(\alpha^{-k})^2$. Por consiguiente, tanto si $\beta=\alpha^{-k}$ es una permutación par como si β es impar, β^2 es par. En consecuencia, $\alpha=\beta^2\in A_n$ y concluimos que $K\subseteq A_n$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G=C_3\times C_5\times C_{15}$ y $H=C_9\times C_{25}$.

Solución: Lema Auxiliar. Dados tres grupos finitos A,B,C, y tres elementos $a\in A$, $b\in B$,$c\in C$ se tiene que el orden de (a,b,c) como elemento del grupo producto $A\times B\times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a,b,c))=m.c.m.\{O(a),O(b),O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m=m.c.m.\{O(a),O(b),O(c)\}$, por la definición del grupo producto tenemos que $(a,b,c)^m=(a^m,b^m,c^m)$. Por la Proposición 1.3.6.2, $a^m=1_A$, $b^m=1_B$ y $c^m=1_C$, luego $(a,b,c)^m=1_{A\times B\times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a,b,c))\mid m$. Por otra parte, si $O((a,b,c))=t$ como $(a,b,c)^t=1_{A\times B\times C}$ se tiene que $a^t=1_A$, $b^t=1_B$ y $c^t=1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a)\mid t$, $O(b)\mid t$ y $O(c)\mid t$, luego $m\mid t$ y concluimos que $t=m$. □

1. Construir, si es posible, un endomorfismo $f:G\to G$ tal que $\mathrm{Ker}f\approx\mathrm{Im}f$.

   Solución: Consideramos $f:G\to G$ dado por $f(a,b,c)=(0,c)$. Comprobamos de forma directa que f es un endomorfismo (proyección), que $\mathrm{Ker}f=C_3\times C_5\times\{0\}$ y que $\mathrm{Im}f=\{0\}\times\{0\}\times C_{15}$. Finalmente, demostramos que $\mathrm{Ker}f\approx\mathrm{Im}f\approx C_{15}$, para probar esto se puede ver que ambos grupos son cíclicos de orden 15 y concluir usando la Proposición 1.6.3.

2. Determinar razonadamente si existe K con $\#K=\#G$ de modo que $K\not\approx H$ y $K\not\approx G$.

   Solución: Observamos que $\#G=\#H=225$. Buscamos K con $\#K=225$ de modo que $K\not\approx H$ y $K\not\approx G$. Consideramos $K:=C_9\times C_5\times C_5$, cumple que $\#K=225$. Por el Teorema 1.3.1, sabemos que el orden de los elementos de C_3 es 1 o 3,el orden de los elementos de C_5 es 1 o 5, el orden de los elementos de C_9 es 1, 3 o 9,el orden de los elementos de C_{15} es 1, 3, 5 o 15, y que el orden de los elementos de C_{25} es 1, 5 o 25. Empleando el Lema Auxiliar vemos que:

   - en K no hay ningún elemento de orden 25 pero sí hay elementos de orden 9.
   - en G no hay ningún elemento de orden 25 ni de orden 9.
   - en $C_1\times C_9\times C_{25}\approx C_9\times C_{25}=H$ hay elementos de orden 9 y de orden 25.

   Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y K no son isomorfos y G y K tampoco son isomorfos.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un D.F.U. y $a,b,c \in R$ con $a \neq 0$, entonces

$$d \text{ es un m.c.d. de } b \text{ y } c \text{ si y solo si } ad \text{ es un m.c.d. de } ab \text{ y } ac.$$

Solución: Cierto. Supongamos que d es un m.c.d. de b y c. Por (MCD.I), $d \mid b$ y $d \mid c$, luego $ad \mid ab$ y $ad \mid ac$, es decir, ad satisface (MCD.I). Como R es un D.F.U., sabemos que existe x un m.c.d de ab y ac. Como $a \mid ab$ y $a \mid ac$, por (MCD.II), $a \mid x$. Dicho de otro modo, existe $r \in R$ tal que $x = ar$. Por (MCD.I), $x \mid ab$ y $x \mid ac$, luego $ar \mid ab$ y $ar \mid ac$. Como $a \neq 0$ y como R es un dominio, por la Ley de Cancelación, **Teorema.II.4.6**, se tiene que $r \mid b$ y que $r \mid c$. Como d es un m.c.d. de b y c, por (MCD.II), $r \mid d$, luego $x = ar \mid ad$ y como x es un m.c.d de ab y ac concluimos que ad también satisface (MCD.II) para ab y ac. En resumen, ad es un un m.c.d de ab y ac.
Recíprocamente, supongamos que ad es un m.c.d. de ab y ac. Por (MCD.I), $ad \mid ab$ y $ad \mid ac$, Como $a \neq 0$ y como R es un dominio, por la Ley de Cancelación, **Teorema.II.4.6**, se tiene que $d \mid b$ y $d \mid c$, es decir, d satisface (MCD.I). Si $s \mid b$ y $s \mid c$, tenemos que $as \mid ab$ y $as \mid ac$. Por (MCD.II), $as \mid ad$ y de nuevo por la Ley de Cancelación $s \mid d$, es decir, d satisface (MCD.II).

2. Existe R es no conmutativo de modo que se satisface la siguiente propiedad:
para todos $r,s,t \in R$ con $r \neq 0$ si $rs = tr$, entonces $s = t$.

Solución: Falso. Veamos que si R satisface esta propiedad, entonces R debe ser conmutativo. Dados $x,y \in R$, si $x = 0$ o $y = 0$, por la **Proposición.II.1.9**, $xy = 0_R = yx$. Supongamos que $x \neq 0$ y que $y \neq 0$. Tomamos $s = yx$, $t = xy$ y $r = x$, como por la propiedad asocitiva se tiene que $rs = x(yx) = (xy)x = tr$, aplicando la propiedad, dado que $r = x \neq 0$, concluimos que $yx = s = t = xy$. En consecuencia, hemos visto que R es conmutativo. En resumen, R no puede satisfacer la propiedad y al mismo tiempo ser no conmutativo.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Consideramos el dominio $\mathbb{Z}[\sqrt{15}] = \{a + b\sqrt{15}\,;\, a,b \in \mathbb{Z}\}$.

1. Probar que $7 + 2\sqrt{15}$ es irreducible en $\mathbb{Z}[\sqrt{15}]$.

Solución: Emplearemos las propiedades de la función $N(a + b\sqrt{15}) = a^2 - b^2 15$ del **E460**. Se tiene que $N(7 + 2\sqrt{15}) = -11$. Como -11 es primo en $\mathbb{Z}$, por la propiedad (IV), $7 + 2\sqrt{15}$ es irreducible en $\mathbb{Z}[\sqrt{15}]$.

2. Demuestra que $4 + \sqrt{15}$ es una unidad en $\mathbb{Z}[\sqrt{15}]$ y dar 6 divisores diferentes de 1 en $\mathbb{Z}[\sqrt{15}]$.

Solución: Con la notación del primer apartado $N(4 + \sqrt{15}) = 16 - 15 = 1$ y, por el **E460**, $u = 4 + \sqrt{15}$ es una unidad en $\mathbb{Z}[\sqrt{15}]$. Observamos que u^n para $n \in \mathbb{N}$ es una unidad porque $N(u^n) = (N(u))^n = 1$. Comprobamos que $u^2 = 31 + 8\sqrt{15}$ y que $u^3 = 244 + 63\sqrt{15}$ y tenemos seis divisores diferentes de 1 en $\mathbb{Z}[\sqrt{15}]$: u, $u^{-1} = 4 - \sqrt{15}$, u^2, $u^{-2} = 31 - 8\sqrt{15}$, u^3 y $u^{-3} = 244 - 63\sqrt{15}$.

3. Probar que $\mathbb{Z}[\sqrt{15}]$ y que $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3}\,;\, a,b \in \mathbb{Z}\}$ no son anillos isomorfos.

Solución: Razonamos por reducción al absurdo y suponemos que existe $\psi : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}[\sqrt{15}]$ un isomorfismo de anillos. Como ψ es un isomorfismo podemos probar que $\psi(1) = 1$. En consecuencia, por (HA.I), $\psi(3) = \psi(1 + 1 + 1) = \psi(1) + \psi(1) + \psi(1) = 3$. Por otro lado, por (HA.II), $\psi(3) = \psi(\sqrt{3}\sqrt{3}) = (\psi(\sqrt{3}))^2$. En resumen, deberían existir $a,b \in \mathbb{Z}$ tales que $(a + b\sqrt{15})^2 = (\psi(\sqrt{3}))^2 = \psi(3) = 3$. Reescribiendo, esta igualdad existirían $a,b \in \mathbb{Z}$ tales que $a^2 + b^2 15 + 2ab\sqrt{15} = 3$. Igualando términos, tenemos dos opciones o $a = 0$ y $b^2 5 = 1$ (imposible) o $b = 0$ y $a^2 = 3$ (imposible) porque $a,b \in \mathbb{Z}$.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.
2. Sea $(G, \cdot)$ un grupo si $a, b \in G$ son tales que $O(a) < \infty$ y $O(b) < \infty$, entonces $O(ab) < \infty$.
3. Sea $(G, \cdot)$ un grupo y H_1, H_2 subgrupos de G tales que $H_1 \lhd H_2$ y que $H_2 \lhd G$ entonces $H_1 \lhd G$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = S_4$ y $H = D_4 \times \mathbb{Z}/3\mathbb{Z}$.

1. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.
2. Determinar si G y H son o no son grupos isomorfos.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio, entonces $\#R \neq 21$.
2. Si R es un dominio, S es un dominio, $f : S \to R$ es un homomorfismo de anillos e I es maximal en R, entonces $f^{-1}(I)$ es maximal en S.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[i] = \{a + bi\,;\, a, b \in \mathbb{Z}\}$, el anillo de los enteros de Gauss, consideramos el ideal $I = (1 + 7i)$ y el anillo cociente $A = \mathbb{Z}[i]/I$.

1. Probar que $i+I = 7+I$ y deducir que para todo elemento $a+bi$ de $\mathbb{Z}[i]$ existe $k \in \mathbb{Z}$ tal que $(a+bi)+I = k+I$.
2. Construye un homomorfismo de anillos $\Psi : \mathbb{Z} \to A$ sobreyectivo.
3. Encuentra un valor de $n \in \mathbb{N}$ tal que $\mathbb{Z}/n\mathbb{Z} \approx A$. ¿Es A un cuerpo?

Esquema de una solución de la versión K del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.

   Solución: Falsa. Escribimos α como el producto de ciclos disjuntos $\alpha = (1\,8)(2\,7)(4\,9\,5\,6)$. Por la Proposición 1.4.1, sabemos las permutaciones disjuntas conmutan y se tiene que
   $$\alpha^3 = (1\,8)^3(2\,7)^3(4\,9\,5\,6)^3 = (1\,8)(2\,7)(4\,6\,5\,9).$$
   Finalmente, observamos que $(4\,6\,5\,9) = (4\,9)(4\,5)(4\,6)$. En consecuencia, α^3 descompone como producto de 5 transposiciones y concluimos que es impar y, por tanto, $\alpha^3 \notin A_9$.

2. Sea $(G, \cdot)$ un grupo si $a, b \in G$ son tales que $O(a) < \infty$ y $O(b) < \infty$, entonces $O(ab) < \infty$.

   Solución: Falsa. Consideremos como grupo G, el grupo lineal $(GL(2,\mathbb{R}), \cdot)$ de las matrices 2×2 invertibles con coeficientes en $\mathbb{R}$ y tomamos
   $$A := \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \qquad B := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
   Observamos que $A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id$, $B^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id$, $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Por tanto, deducimos que $O(A) = 2$ y $O(B) = 2$. Sin embargo, probamos por inducción que para todo $n \in \mathbb{N}$ se tiene que $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ y concluimos que $O(AB) = \infty$. (Alternativa ver **E78**).

3. Sea $(G, \cdot)$ un grupo y H_1, H_2 subgrupos de G tales que $H_1 \lhd H_2$ y que $H_2 \lhd G$ entonces $H_1 \lhd G$.

   Solución: Falsa. Con la notación del **E156**, basta considerar $G = D_4$, $H_1 = \{id, b\} = \langle b\rangle$ y $H_2 = \{id, b, a^2, a^2b\} = \langle a, b\rangle$. Sabemos que $\#H_1 = 2$, $\#H_2 = 4$ y que $\#D_4 = 8$. Por el Teorema de Lagrange, se tiene que $\#(H_2 : H_1) = 2$ y $\#(D_4 : H_2) = 2$. Por el **E167**, concluimos que $H_1 \lhd H_2$ y que $H_2 \lhd D_4$. Finalmente, observamos que $aH_1 = \{a, ab\}$ y que $H_1a = \{a, ba\}$ y, por el **E156**, sabemos $ba = a^3b$ y que $a^3b \neq ab$. Por consiguiente, $aH_1 \neq H_1a$ y concluimos que H_1 no es normal en D_4.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = S_4$ y $H = D_4 \times \mathbb{Z}/3\mathbb{Z}$.

Solución: Lema Auxiliar. Dados dos grupos finitos A, B, y dos elementos $a \in A$, $b \in B$, se tiene que el orden de (a, b) como elemento del grupo producto $A \times B$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a, b)) = m.c.m.\{O(a), O(b)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b)\}$, por la definición del grupo producto tenemos que $(a, b)^m = (a^m, b^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$ y $b^m = 1_B$, luego $(a, b)^m = 1_{A\times B}$ y, de nuevo la Proposición 1.3.6.2, $O((a, b)) \mid m$. Por otra parte, si $O((a, b)) = t$ como $(a, b)^t = 1_{A\times B}$ se tiene que $a^t = 1_A$ y $b^t = 1_B$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$ y $O(b) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.

   Solución: Por la Proposición 1.6.2, como $\mathbb{Z}/3\mathbb{Z} = \langle 1\rangle$ es cíclico f queda completamente determinado por $f(1)$. Además por la Proposición 1.6.2. sabemos que $O(f(1)) \mid 3$ y que para cada $b \in G$ con $O(b) \mid 3$ existe un único homomorfismo $f_b : \mathbb{Z}/3\mathbb{Z} \to G$ tal que $f(1) = b$. Por consiguiente determinar los homomorfismos equivale a determinar los elementos $b \in G$ con $O(b) \in \{1, 3\}$.
   Observamos que $O(b) = 1$ si y sólo si $b = 1_G$. Empleando la descomposición en ciclos disjuntos de los elementos de S_4 (**Cor. 1.4.1.**), vemos que los elementos de orden 3 de S_4 son necesariamente ciclos de longitud 3. Por consiguiente, hay 9 homomorfismos de grupos $\mathbb{Z}/3\mathbb{Z}$ en G determinados por $f_1(1) = id$, $f_2(1) = (123)$, $f_3(1) = (132)$, $f_4(1) = (124)$, $f_5(1) = (142)$, $f_6(1) = (134)$, $f_7(1) = (143)$, $f_8(1) = (234)$ y $f_9(1) = (243)$.

2. Determinar si G y H son o no son grupos isomorfos.

   Solución: Observamos que $\#G = \#H = 24$, por tanto, no podemos emplear el cardinal para determinar si son isomorfos o no. Por tanto, con la notación del **E156**, si consideramos el elemento $x = ((1234), 1)$ de H por el Lema Auxiliar $O(x) = 12$. Por otro lado, empleando la descomposición en ciclos disjuntos (**Cor. 1.4.1.**), comprobamos que los posibles órdenes de los elementos de $G = S_4$ son $\{1, 2, 3, 4\}$. Deducimos ni de orden 49 de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y G no son isomorfos porque en H hay un elemento de orden 12 y en G no.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio, entonces $\#R \neq 21$.

   Solución: Cierto. Razonamos por reducción al absurdo y suponemos que $\#R = 21$. Como R es un dominio, por (D.II) es un anillo unitario. Por el **Teorema II.3.18**, se tiene que $\text{car}(R) = O(1_R)$. Por el **Teorema de Lagrange**, $O(1_R) \mid \#R = 21$, luego $O(1_R)$ es $1, 3, 7$ o 21. Por el **Corolario II.4.9**, tenemos que $\text{car}(R) = p$ con p primo. Por tanto, tenemos dos opciones:
   (A) $\text{car}(R) = O(1_R) = 7$. Por la definición de característica, $7x = 0$ para todo $x \in R$, luego $O(x) \mid 7$ para todo $x \in R$. Por el **Teorema de Cauchy para grupos Abelianos**, como $3 \mid \#R$, existe un elemento $r \in R$ con $O(r) = 3$, contradiciendo que $O(r) \mid 7$.
   (B) $\text{car}(R) = O(1_R) = 3$, razonando como en el caso (A) llegamos a contradicción.

2. Si R es un dominio, S es un dominio, $f : S \to R$ es un homomorfismo de anillos e I es maximal en R, entonces $f^{-1}(I)$ es maximal en S.

   Solución: Falso. Basta considerar $S = \mathbb{Z}$, $R = \mathbb{Q}$ y $f : \mathbb{Z} \to \mathbb{Q}$ la inclusión canónica dada por $f(m) = m$ para todo $m \in \mathbb{Z}$ que es un homomorfismo de anillos. El ideal $I = (0)$ es maximal en $\mathbb{Q}$, porque $I \neq \mathbb{Q}$ (M.I) y si J es otro ideal con $I \subsetneq J$, existe $q \in J$ con $q \neq 0$, luego $1 = q^{-1}q \in J$ y por tanto, $J = \mathbb{Q}$, es decir, se satisface (M.II). Sin embargo, $f^{-1}(I) = (0)$ que no es un ideal maximal de $\mathbb{Z}$ porque, por ejemplo, $(0) \subsetneq (2) \subsetneq \mathbb{Z}$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[i] = \{a + bi\,;\, a, b \in \mathbb{Z}\}$, el anillo de los enteros de Gauss, consideramos el ideal $I = \big(1 + 7i\big)$ y el anillo cociente $A = \mathbb{Z}[i]/I$.

1. Probar que $i+I = 7+I$ y deducir que para todo elemento $a+bi$ de $\mathbb{Z}[i]$ existe $k \in \mathbb{Z}$ tal que $(a+bi)+I = k+I$.

   Solución: Observamos que $i - 7 = i(1 + 7i) \in I$, luego $i + I = 7 + I$. Dado un elemento $a + bi$ de $\mathbb{Z}[i]$ con $a, b \in \mathbb{Z}$, por las propiedades de la suma y el producto en A, se tiene que $(a+bi)+I = (a+I)+(b+I)(7+I) = (a + b7) + I$. En otras palabras, como $a + b7 \in \mathbb{Z}$, queda demostrado el apartado.

2. Construye un homomorfismo de anillos $\Psi : \mathbb{Z} \to A$ sobreyectivo.

   Solución: Basta considerar $\Psi = p \circ f$ donde $f : \mathbb{Z} \to \mathbb{Z}[i]$ es la inyección canónica y $p : \mathbb{Z}[i] \to \mathbb{Z}[i]/I$ es la aplicación de paso al cociente. Como f y p son homomorfismos de anillos, por la **Proposición II.3.3**, Ψ es también un homomorfismo de anillos y está dado por $\Psi(k) = k + I$. Por el apartado anterior, para todo elemento $a + bi$ de $\mathbb{Z}[i]$ existe $k \in \mathbb{Z}$ tal que $(a + bi) + I = k + I$, luego $\Psi(k) = (a + bi) + I$, es decir, Ψ es sobreyectivo.

3. Encuentra un valor de $n \in \mathbb{N}$ tal que $\mathbb{Z}/n\mathbb{Z} \approx A$. ¿Es A un cuerpo?

   Solución: Observamos que dado $k \in \mathbb{Z}$, $k \in \text{Ker}\Psi$ si y solo si $k + I = I$, es decir, si y solo si $k \in I$. Vemos que $k \in I$ si y solo si existen $a, b \in \mathbb{Z}$ con $k = (a + bi)(1 + 7i)$, es decir, si y solo si, existen $a, b \in \mathbb{Z}$, $k = a - 7b$ y $0 = 7a + b$. Deducimos que $k \in \text{Ker}\Psi$ si y solo si existe $a \in \mathbb{Z}$ tal que $k = 50a$, es decir, si y solo si, $k \in 50\mathbb{Z}$, dicho de otro modo, $n = 50$. Como Ψ es sobreyectivo, por **Primer teorema de isomorfía (Teorema II.3.8)**, $\mathbb{Z}/50\mathbb{Z} \approx A$. Por el **Ejemplo II.4.8**, tenemos que $\mathbb{Z}/50\mathbb{Z}$ no es un cuerpo porque 50 no es primo. Deducimos que A tampoco es un cuerpo porque, por ejemplo, la imagen de un divisor de cero no nulo por un isomorfismo es un divisor de cero no nulo. En otras palabras, en A hay divisores de cero no nulos.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo no abeliano y $K \lhd G$ un subgrupo no abeliano entonces G/K es no abeliano.
2. En D_{37} consideramos el subgrupo R de las rotaciones entonces $R \lhd D_{37}$.
3. Sea $(G,\cdot)$ un grupo abeliano y $a,b \in G$ elementos de orden finito, entonces $O(ab)$ es el $m.c.m(O(a),O(b))$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ y $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times D_7$.

1. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.
2. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio y todo ideal de R distinto de R es primo, entonces R es un cuerpo.
2. Si $r,s \in R$ entonces $(r+s)^2 = r^2 + 2rs + s^2$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[x]$, el anillo de los polinomios con coeficientes enteros, consideramos el ideal $I = (10, x-3)$ y el anillo cociente $A = \mathbb{Z}[x]/I$.

1. Probar que $x+I = 3+I$ y deducir que para todo elemento $P(x)$ de $\mathbb{Z}[x]$ existe $k \in \mathbb{Z}$ tal que $P(x)+I = k+I$.
2. Probar que $Q(x) = 6x^3 + 5x^2 + 8x + 12$ es irreducible en $\mathbb{Z}[x]$.
3. Encuentra el inverso de $Q(x) + I$ en A.

Esquema de una solución de la versión L del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo no abeliano y $K \lhd G$ un subgrupo no abeliano entonces G/K es no abeliano.

   Solución: Falsa. Basta considerar $G = S_4$ y $K = A_4$. Observamos que $(123),(234) \in A_4 \subseteq S_4$ y que $(123)(234) = (12)(34) \neq (13)(24) = (234)(123)$ luego G y K no son abelianos. Por el **E116**, $\#A_4 = 12$ y como $\#S_4 = 24$, por el Teorema de Lagrange, se tiene que $\#(S_4 : A_4) = 2$. Por el **E167**, vemos que $A_4 \lhd S_4$. Como $\#(S_4 : A_4) = \#(S_4/A_4) = 2$, por el Corolario 1.5.1.b), el grupo cociente S_4/A_4 es cíclico y, por tanto, es abeliano.

2. En D_{37} consideramos el subgrupo R de las rotaciones entonces $R \lhd D_{37}$.

   Solución: Verdadera. Por el **E156**, sabemos que $\#R = 37$ y que $\#D_{37} = 2 \cdot 37 = 74$. Por el Teorema de Lagrange, $\#(D_{37} : R) = 2$. Por el **E167**, concluimos que $R \lhd D_{37}$.

3. Sea $(G,\cdot)$ un grupo abeliano y $a, b \in G$ elementos de orden finito, entonces $O(ab)$ es el $m.c.m(O(a), O(b))$.

   Solución: Falsa. Basta considerar en el grupo $(\mathbb{Z}/12\mathbb{Z},+)$ los elementos $a = 2$ y $b = 4$, tenemos que $O(a) = 6$ y $O(b) = 3$. Observamos que $m.c.m(O(a), O(b)) = 6$ pero tenemos que $a + b = 6$ y $O(a + b) = O(6) = 2$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ y $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times D_7$.

Solución: Lema Auxiliar. Dados tres grupos finitos A, B, C, y tres elementos $a \in A$, $b \in B$,$c \in C$ se tiene que el orden de (a, b, c) como elemento del grupo producto $A \times B \times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a, b, c)) = m.c.m.\{O(a), O(b), O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b), O(c)\}$, por la definición del grupo producto tenemos que $(a, b, c)^m = (a^m, b^m, c^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$, $b^m = 1_B$ y $c^m = 1_C$, luego $(a, b, c)^m = 1_{A\times B\times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a, b, c)) \mid m$. Por otra parte, si $O((a, b, c)) = t$ como $(a, b, c)^t = 1_{A\times B\times C}$ se tiene que $a^t = 1_A$, $b^t = 1_B$ y $c^t = 1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$, $O(b) \mid t$ y $O(c) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.

   Solución: Consideramos $f : G \to G$ dado por $f(a, b) = (0, b)$. Comprobamos de forma directa que f es un endomorfismo (proyección), que $\mathrm{Ker} f = \mathbb{Z}/14\mathbb{Z} \times \{0\}$ y que $\mathrm{Im} f = \{0\} \times \mathbb{Z}/14\mathbb{Z}$. Demostramos que $\mathrm{Ker} f \approx \mathrm{Im} f \approx \mathbb{Z}/14\mathbb{Z}$, para probar esto se puede ver que ambos grupos son cíclicos de orden 15 y concluir usando la Proposición 1.6.3.

2. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

   Solución: Observamos que $\#G = \#H = 196$. Buscamos K con $\#K = 196$ de modo que $K \not\approx H$ y $K \not\approx G$. Consideramos $K := \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, cumple que $\#K = 196$. Por el Teorema 1.3.1, sabemos que el orden de los elementos de $\mathbb{Z}/2\mathbb{Z}$ es 1 o 2, el orden de los elementos de $\mathbb{Z}/4\mathbb{Z}$ es 1, 2 o 4, el orden de los elementos de $\mathbb{Z}/7\mathbb{Z}$ es 1 o 7, el orden de los elementos de $\mathbb{Z}/14\mathbb{Z}$ es 1, 2, 7 o 14. Por otro lado, por el **E156**, comprobamos que los posibles órdenes de los elementos de D_7 son $\{1, 2, 7\}$. Empleando el Lema Auxiliar vemos que:

   - en K hay elementos de orden 4.
   - en $\mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \approx G$ no hay ningún elemento de orden 4.
   - en H no hay ningún elemento de orden 4.

   Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, G y K no son isomorfos y H y K tampoco son isomorfos.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio y todo ideal de R distinto de R es primo, entonces R es un cuerpo.

   Solución: Cierto. Como R es dominio se satisfacen (F.I) y (F.II) basta comprobar que se satisface (F.III), es decir, que $U(R) = R\backslash\{0_R\}$. Como R es un dominio por (D.III), se tiene que $U(R) \subseteq R\backslash\{0_R\}$. Veamos ahora que se cumple la contención contraria. Dado $x \in R\backslash\{0_R\}$ consideremos el ideal $J_1 = (x)$.
   Si $J_1 \subsetneq R$, consideramos el ideal $J_2 = (x^2)$. Como $x^2 \in J_1$ y $J_1 \subsetneq R$, se tiene que $J_2 \subseteq J_1 \subsetneq R$. Por hipótesis, J_2 es primo. Como $x \cdot x = x^2 \in J_2$, tenemos que $x \in J_2$. Por consiguiente, existe $r \in R$ tal que $x = rx^2$ y por la Ley de Cancelación, **Teorema.II.4.6**, $1_R = rx$. Por tanto, $1_R \in J_1$ y tenemos que $J_1 = R$ contradiciendo nuestra suposición.
   Si $J_1 = R$, entonces $1_R \in (x)$, luego existe $u \in R$ tal que $1_R = ux$, es decir, $x \in U(R)$ y concluimos que R es un cuerpo.

2. Si $r, s \in R$ entonces $(r+s)^2 = r^2 + 2rs + s^2$.

   Solución: Falso. Basta considerar R el anillo de las matrices 2×2 con coeficientes en $\mathbb{R}$, es decir, $(\mathrm{Mat}_{2\times 2}(\mathbb{R}),+,\cdot)$ y tomar $r = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ y $s = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Observamos que

   $$r^2 + 2rs + s^2 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}^2 + 2\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix},$$

   pero $(r+s)^2 = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix}$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[x]$, el anillo de los polinomios con coeficientes enteros, consideramos el ideal $I = (10, x-3)$ y el anillo cociente $A = \mathbb{Z}[x]/I$.

1. Probar que $x+I = 3+I$ y deducir que para todo elemento $P(x)$ de $\mathbb{Z}[x]$ existe $k \in \mathbb{Z}$ tal que $P(x)+I = k+I$.

   Solución: Observamos que $x - 3 \in I$, luego $x + I = 3 + I$. Dado un elemento $P(x) = \sum_{j=0}^{n} a_j x^j$ de $\mathbb{Z}[x]$, por las propiedades de la suma y el producto en A, se tiene que $P(x) + I = (\sum_{j=0}^{n} a_j x^j) + I = \sum_{j=0}^{n} \left((a_j + I)(x+I)^j\right) = \sum_{j=0}^{n} \left((a_j + I)(3+I)^j\right) = P(3) + I$. Como $P(3) \in \mathbb{Z}$, queda demostrado el apartado.

2. Probar que $Q(x) = 6x^3 + 5x^2 + 8x + 12$ es irreducible en $\mathbb{Z}[x]$.

   Solución: El polinomio $Q(x)$ es primitivo en $\mathbb{Z}[x]$ y consideramos su clase módulo 5, es decir, el polinomio $\overline{Q(x)} = x^3 + 3x + 2$ de $(\mathbb{Z}/5\mathbb{Z})[x]$. Comprobamos que $\overline{Q(x)}$ no tiene raíces en $\mathbb{Z}/5\mathbb{Z}$ porque $\overline{Q(0)} = 2$, $\overline{Q(1)} = \overline{Q(2)} = 1$, $\overline{Q(3)} = \overline{Q(4)} = 3$. Por consiguiente, por el **Ejercicio A.44**, como $\mathrm{gr}(\overline{Q(x)}) = 3$ y como $\mathbb{Z}/5\mathbb{Z}$ es un cuerpo (**Ejemplo II.4.8**), tenemos que $\overline{Q(x)}$ es irreducible en $(\mathbb{Z}/5\mathbb{Z})[x]$. Finalmente, por el **Criterio de irreducibilidad módulo** 5 **(Problema A.64)**, concluimos que $Q(x)$ es irreducible en $\mathbb{Z}[x]$.

3. Encuentra el inverso de $Q(x) + I$ en A.

   Solución: Por el primer apartado sabemos que $Q(x) + I = Q(3) + I = 243 + I$. Como $10 \in I$, $243 - 3 = 240 \in I$, luego $Q(x) + I = 3 + I$. Finalmente, observamos que $(3+I)(7+I) = (21+I) = 1 + I$ porque $21 - 1 = 20 \in I$. En consecuencia, $(Q(x)+I)^{-1} = (7+I)$.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo si $x,y,z\in G$ entonces $O(xyz)=O(zyx)$.
2. Dado $K\subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K\subseteq A_n$.
3. Sea $(G,\cdot)$ un grupo $K\lhd G$ un subgrupo y $a\in G$. Si $O(aK)=n\in\mathbb{N}$, entonces $a^n=1_G$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G=D_3\times D_4\times D_5$ y $H=S_5\times C_2\times C_2$.

1. Determinar si G y H son o no son grupos isomorfos.
2. Determinar todos los homomorfismos de grupos de $f:\mathbb{Z}/3\mathbb{Z}\to G$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I\subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un D.I.P., entonces R/I es D.I.P.
2. Si $\mathrm{car}(R)=n>0$, entonces $\mathrm{car}(R\times R\times R)=n^3$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En el anillo de los polinomios con coeficientes racionales, $\mathbb{Q}[x]$, consideramos: $P_1(x)=(3/4)x^7+36x-18$ y $P_2(x)=(4/3)x^3+4x^2-(40/3)x-32$ de $\mathbb{Q}[x]$.

1. Probar que $P_1(x)$ es irreducible en $\mathbb{Q}[x]$ y que $P_2(x)$ no es irreducible en $\mathbb{Q}[x]$.
2. Determinar si $R_1=\mathbb{Q}[x]/(P_1(x))$ y $R_2=\mathbb{Q}[x]/(P_2(x))$ son o no son cuerpos.
3. Encuentra en R_1 el inverso de $((x-2)/200)+(P_1(x))$.

Esquema de una solución de la versión M del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo si $x,y,z\in G$ entonces $O(xyz)=O(zyx)$.

   Solución: Falsa. Basta considerar $G=Q_8$ (ver **E64**) y tomar $x=i$, $y=j$ y $z=k$ tenemos que $xyz=ijk=kk=-1$ luego $O(xyz)=2$ pero $zyx=kji=k(-k)=1$ luego $O(zyx)=1$.

2. Dado $K\subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K\subseteq A_n$.

   Solución: Verdadera. Tenemos que $\#K=2k+1$ con $k\in\mathbb{Z}$, por el Corolario 1.5.1.a), para todo $\alpha\in K$ tenemos que $O(\alpha)\mid 2k+1$. Por la Proposición 1.3.6.2, $\alpha^{2k+1}=id$. Luego $\alpha^{2k}\alpha=1$ y deducimos que $\alpha=\alpha^{-2k}=(\alpha^{-k})^2$. Por consiguiente, tanto si $\beta=\alpha^{-k}$ es una permutación par como si β es impar, β^2 es par. En consecuencia, $\alpha=\beta^2\in A_n$ y concluimos que $K\subseteq A_n$.

3. Sea $(G,\cdot)$ un grupo $K\lhd G$ un subgrupo y $a\in G$. Si $O(aK)=n\in\mathbb{N}$, entonces $a^n=1_G$.

   Solución: Falsa. Basta considerar $(G,\cdot)=(\mathbb{Z},+)$, $K=3\mathbb{Z}$ y $a=2$. Como $(\mathbb{Z},+)$ es abeliano tenemos que $3\mathbb{Z}\lhd\mathbb{Z}$ y $O(2+3\mathbb{Z})=3$ pero $3\cdot 2=6\neq 0$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G=D_3\times D_4\times D_5$ y $H=S_5\times C_2\times C_2$.

Solución: Lema Auxiliar. Dados tres grupos finitos A,B,C, y tres elementos $a\in A$, $b\in B$, $c\in C$ se tiene que el orden de (a,b,c) como elemento del grupo producto $A\times B\times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a,b,c))=m.c.m.\{O(a),O(b),O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m=m.c.m.\{O(a),O(b),O(c)\}$, por la definición del grupo producto tenemos que $(a,b,c)^m=(a^m,b^m,c^m)$. Por la Proposición 1.3.6.2, $a^m=1_A$, $b^m=1_B$ y $c^m=1_C$, luego $(a,b,c)^m=1_{A\times B\times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a,b,c))\mid m$. Por otra parte, si $O((a,b,c))=t$ como $(a,b,c)^t=1_{A\times B\times C}$ se tiene que $a^t=1_A$, $b^t=1_B$ y $c^t=1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a)\mid t$, $O(b)\mid t$ y $O(c)\mid t$, luego $m\mid t$ y concluimos que $t=m$. □

1. Determinar si G y H son o no son grupos isomorfos.

   Solución: Observamos que $\#G=\#H=480$, por tanto, no podemos emplear el cardinal para determinar si son isomorfos o no. Por tanto, con la notación del **E156**, si consideramos el elemento $x=((123),(1234),(12345))$ de G por el Lema Auxiliar $O(x)=60$. Por otro lado, empleando la descomposición en ciclos disjuntos (**Cor. 1.4.1.**), comprobamos que los posibles órdenes de los elementos de S_5 son $\{1,2,3,4,5,6\}$. Por el Lema Auxiliar, los posibles órdenes de los elementos de H son $\{1,2,3,4,5,6,10\}$. Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y G no son isomorfos porque en G hay un elemento de orden 60 y en H no.

2. Determinar todos los homomorfismos de grupos de $f:\mathbb{Z}/3\mathbb{Z}\to G$.

   Solución: Por la Proposición 1.6.2, como $\mathbb{Z}/3\mathbb{Z}=\langle 1\rangle$ es cíclico f queda completamente determinado por $f(1)$. Además por la Proposición 1.6.2. sabemos que $O(f(1))\mid 3$ y que para cada $b\in G$ con $O(b)\mid 3$ existe un único homomorfismo $f_b:\mathbb{Z}/3\mathbb{Z}\to G$ tal que $f(1)=b$. Por consiguiente determinar los homomorfismos equivale a determinar los elementos $b\in G$ con $O(b)\in\{1,3\}$.
   Observamos que $O(b)=1$ si y sólo si $b=1_G$. Empleando el **E156**, vemos que el posible orden de los elementos de D_3 es $\{1,2,3\}$ de los elementos de D_4 es $\{1,2,4\}$ y de D_5 es $\{1,2,5\}$. Por tanto, por el Lema Auxiliar, deducimos que los elementos de orden 3 de G son $((123),id,id)$ y $((132),id,id)$. Por consiguiente, hay tres homomorfismos de grupos $\mathbb{Z}/3\mathbb{Z}$ en G determinados por $f_1(1)=(id,id,id)$, $f_2(1)=((123),id,id)$ y $f_3(1)=((132),id,id)$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un D.I.P., entonces R/I es D.I.P.

   Solución: Falso. Basta considerar $(R,+,\cdot) = (\mathbb{Z},+,\cdot)$ e $I = 6\mathbb{Z}$. El anillo cociente R/I es $(\mathbb{Z}/6\mathbb{Z},+,\cdot)$ que no es un dominio porque 6 no es primo (**Ejemplo II.4.8**). En consecuencia R/I no es un dominio de ideales principales (D.I.P.).

2. Si $\text{car}(R) = n > 0$, entonces $\text{car}(R \times R \times R) = n^3$.

   Solución: Falso. Por el **Ejemplo II.4.8**, sabemos que $(R,+,\cdot) = (\mathbb{Z}/3\mathbb{Z},+,\cdot)$ es un dominio. Como los dominios son anillos unitarios, por el **Teorema.II.3.18**, $\text{car}(\mathbb{Z}/3\mathbb{Z}) = O(1_{\mathbb{Z}/3\mathbb{Z}}) = 3$. Como en el anillo producto $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ las operaciones se definen componete a componete es un anillo unitario con elemento neutro $(1_{\mathbb{Z}/3\mathbb{Z}}, 1_{\mathbb{Z}/3\mathbb{Z}}, 1_{\mathbb{Z}/3\mathbb{Z}})$. Por el **Teorema.II.3.18**, se tiene que $\text{car}(R \times R \times R) = O((1,1,1)) = 3 \neq 27 = 3^3$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En el anillo de los polinomios con coeficientes racionales, $\mathbb{Q}[x]$, consideramos: $P_1(x) = (3/4)x^7 + 36x - 18$ y $P_2(x) = (4/3)x^3 + 4x^2 - (40/3)x - 32$ de $\mathbb{Q}[x]$.

1. Probar que $P_1(x)$ es irreducible en $\mathbb{Q}[x]$ y que $P_2(x)$ no es irreducible en $\mathbb{Q}[x]$.

   Solución: Observamos que podemos escribir $P_1(x) = (3/4)(x^7 + 48x - 24)$ y también que $P_2(x) = (4/3)(x^3 + 3x^2 - 10x - 24)$. Como $Q_1(x) = x^7 + 48x - 24$ es primitivo, por el **Ejercicio A.57**, sabemos que $P_1(x)$ es irreducible en $\mathbb{Q}[x]$ si y solo si $Q_1(x)$ es irreducible en $\mathbb{Z}[x]$. Aplicando el **Criterio de Eisenstein (Problema A.66)** a $Q_1(x)$ para $p = 3$, vemos que $Q_1(x)$ es irreducible en $\mathbb{Z}[x]$. Por el **Teorema de la raíz racional (Ejercicio A.70)**, sabemos que las posibles raíces racionales de $Q_2(x) = x^3 + 3x^2 - 10x - 24$ son divisores de 24. Comprobamos que $-2, 3, -4$ son raíces de $Q_2(x)$ y, en consecuencia, también son raíces de $P_2(x)$. Por el **Ejercicio A. 44**, concluimos que $P_2(x)$ no es irreducible.

2. Determinar si $R_1 = \mathbb{Q}[x]/(P_1(x))$ y $R_2 = \mathbb{Q}[x]/(P_2(x))$ son o no son cuerpos.

   Solución: Por el **Ejercicio A.48** y el apartado 1, R_1 es un cuerpo y R_2 no es un cuerpo.

3. Encuentra en R_1 el inverso de $((x-2)/200) + (P_1(x))$.

   Solución: Mediante el Algoritmo de Euclides calculamos el m.c.d. y los enteros de la identidad de Bezout de $P(x) = (1/200)(x-2)$ y $P_1(x)$, vemos que

   $$\begin{aligned} P_1(x) &= (1)P_1(x) + (0)P(x), \\ P(x) &= (0)P_1(x) + (1)P(x), \\ 150 &= (1)P_1(x) + ((-150)(x^6 + 2x^5 + 4x^4 + 8x^3 + 16x^2 + 32x + 112))P(x). \end{aligned}$$

   En consecuencia, tomando clases módulo $I = (P_1(x))$ en la última igualdad tenemos que

   $$1 + I = (-x^6 - 2x^5 - 4x^4 - 8x^3 - 16x^2 - 32x - 112 + I)(P(x) + I).$$

   En otras palabras, El inverso de $P(x) + I$ en R_1 es $-x^6 - 2x^5 - 4x^4 - 8x^3 - 16x^2 - 32x - 112 + I$.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.
2. Sea $(G, \cdot)$ un grupo $K \lhd G$ un subgrupo y $x, y \in G$. Si $O(x) = O(y) < \infty$, entonces $O(xK) = O(yK)$.
3. Sea $(G, \cdot)$ un grupo si $x, y, z \in G$ entonces $O(xyz) = O(yzx)$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = C_3 \times C_5 \times C_{15}$ y $H = C_9 \times C_{25}$.

1. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.
2. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un D.F.U. y $a, b, c \in R$ con $a \neq 0$, entonces

   $$d \text{ es un m.c.d. de } b \text{ y } c \text{ si y solo si } ad \text{ es un m.c.d. de } ab \text{ y } ac.$$

2. Si R es un D.I.P., entonces cada ideal del anillo cociente R/I es principal.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Recordamos que el anillo $\mathbb{C}[x, y]$ se define como $\mathbb{C}[x]([y])$

1. Probar que $x^2 + y^2 - 4$ es un elemento irreducible de $\mathbb{C}[x, y]$.
2. Probar que $\mathbb{C}[x, y]/(x^2 + y^2 - 4)$ es un dominio.
3. Si $I = (x^2 + y^2 - 4)$, probar que $(x + iy) + I \in U(\mathbb{C}[x, y]/I)$.

Esquema de una solución de la versión N del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.

   Solución: Falsa. Escribimos α como el producto de ciclos disjuntos $\alpha = (1\,8)(2\,7)(4\,9\,5\,6)$. Por la Proposición 1.4.1, sabemos las permutaciones disjuntas conmutan y se tiene que

   $$\alpha^3 = (1\,8)^3(2\,7)^3(4\,9\,5\,6)^3 = (1\,8)(2\,7)(4\,6\,5\,9).$$

   Finalmente, observamos que $(4\,6\,5\,9) = (4\,9)(4\,5)(4\,6)$. En consecuencia, α^3 descompone como producto de 5 transposiciones y concluimos que es impar y, por tanto, $\alpha^3 \notin A_9$.

2. Sea $(G, \cdot)$ un grupo $K \lhd G$ un subgrupo y $x, y \in G$. Si $O(x) = O(y) < \infty$, entonces $O(xK) = O(yK)$.

   Solución: Falsa. Basta considerar como grupo $(G, \cdot)$ el grupo producto $(\mathbb{Z}/6\mathbb{Z}, +) \times (\mathbb{Z}/6\mathbb{Z}, +)$, $K = \langle (2,3) \rangle$, $x = (1,0)$ e $y = (0,1)$. Como G es abeliano se tiene que $K \lhd G$. Observamos que $O(x) = 6$ porque $n(1,0) = (n \,(\text{mód}\, 6), 0)$ para todo $n \in \mathbb{N}$. Como 6 es el menor natural n tal que $n \equiv 0 (\text{mód}\, 6)$, deducimos que $O(x) = 6$. Análogamente vemos que $O(y) = 6$. Mediante un cálculo directo comprobamos que

   $$K = \{(0,0),(2,3),(4,0),(0,3),(2,0),(4,3)\},$$
   $$x + K = \{(1,0),(3,3),(5,0),(1,3),(3,0),(5,3)\}, \qquad y + K = \{(0,1),(2,4),(4,1),(0,4),(2,1),(4,4)\}.$$

   Observamos que $x + K \neq K$, $y + K \neq K$, $2(x + K) = (2,0) + K = K$ y que

   $$2(y + K) = (0,2) + K = \{(0,2),(2,5),(4,2),(0,5),(2,2),(4,5)\}, \qquad 3(y + K) = (0,3) + K = K.$$

   Por consiguiente, concluimos que $O(x + K) = 2 \neq 3 = O(y + K)$.

3. Sea $(G, \cdot)$ un grupo si $x, y, z \in G$ entonces $O(xyz) = O(yzx)$.

   Solución: Verdadera. Observamos que $xyz = x(yzx)x^{-1}$, luego aplicando el **E75.(iii)**, deducimos que $O(yzx) = O(x(yzx)x^{-1}) = O(xyz)$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = C_3 \times C_5 \times C_{15}$ y $H = C_9 \times C_{25}$.

Solución: Lema Auxiliar. Dados tres grupos finitos A, B, C, y tres elementos $a \in A$, $b \in B$,$c \in C$ se tiene que el orden de (a, b, c) como elemento del grupo producto $A \times B \times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a,b,c)) = m.c.m.\{O(a), O(b), O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b), O(c)\}$, por la definición del grupo producto tenemos que $(a,b,c)^m = (a^m, b^m, c^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$, $b^m = 1_B$ y $c^m = 1_C$, luego $(a,b,c)^m = 1_{A\times B\times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a,b,c)) \mid m$. Por otra parte, si $O((a,b,c)) = t$ como $(a,b,c)^t = 1_{A\times B\times C}$ se tiene que $a^t = 1_A$, $b^t = 1_B$ y $c^t = 1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$, $O(b) \mid t$ y $O(c) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\text{Ker} f \approx \text{Im} f$.

   Solución: Consideramos $f : G \to G$ dado por $f(a,b,c) = (0,c)$. Comprobamos de forma directa que f es un endomorfismo (proyección), que $\text{Ker} f = C_3 \times C_5 \times \{0\}$ y que $\text{Im} f = \{0\} \times \{0\} \times C_{15}$. Finalmente, demostramos que $\text{Ker} f \approx \text{Im} f \approx C_{15}$, para probar esto se puede ver que ambos grupos son cíclicos de orden 15 y concluir usando la Proposición 1.6.3.

2. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

   Solución: Observamos que $\#G = \#H = 225$. Buscamos K con $\#K = 225$ de modo que $K \not\approx H$ y $K \not\approx G$. Consideramos $K := C_9 \times C_5 \times C_5$, cumple que $\#K = 225$. Por el Teorema 1.3.1, sabemos que el orden de los elementos de C_3 es 1 o 3,el orden de los elementos de C_5 es 1 o 5, el orden de los elementos de C_9 es 1, 3 o 9,el orden de los elementos de C_{15} es 1, 3, 5 o 15, y que el orden de los elementos de C_{25} es 1, 5 o 25. Empleando el Lema Auxiliar vemos que:

- en K no hay ningún elemento de orden 25 pero sí hay elementos de orden 9.
- en G no hay ningún elemento de orden 25 ni de orden 9.
- en $C_1 \times C_9 \times C_{25} \approx C_9 \times C_{25} = H$ hay elementos de orden 9 y de orden 25.

Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y K no son isomorfos y G y K tampoco son isomorfos.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un D.F.U. y $a, b, c \in R$ con $a \neq 0$, entonces

$$d \text{ es un m.c.d. de } b \text{ y } c \text{ si y solo si } ad \text{ es un m.c.d. de } ab \text{ y } ac.$$

Solución: Cierto. Supongamos que d es un m.c.d. de b y c. Por (MCD.I), $d \mid b$ y $d \mid c$, luego $ad \mid ab$ y $ad \mid ac$, es decir, ad satisface (MCD.I). Como R es un D.F.U., sabemos que existe x un m.c.d de ab y ac. Como $a \mid ab$ y $a \mid ac$, por (MCD.II), $a \mid x$. Dicho de otro modo, existe $r \in R$ tal que $x = ar$. Por (MCD.I), $x \mid ab$ y $x \mid ac$, luego $ar \mid ab$ y $ar \mid ac$. Como $a \neq 0$ y como R es un dominio, por la Ley de Cancelación, **Teorema.II.4.6**, se tiene que $r \mid b$ y que $r \mid c$. Como d es un m.c.d. de b y c, por (MCD.II), $r \mid d$, luego $x = ar \mid ad$ y como x es un m.c.d de ab y ac concluimos que ad también satisface (MCD.II) para ab y ac. En resumen, ad es un un m.c.d de ab y ac.
Recíprocamente, supongamos que ad es un m.c.d. de ab y ac. Por (MCD.I), $ad \mid ab$ y $ad \mid ac$, Como $a \neq 0$ y como R es un dominio, por la Ley de Cancelación, **Teorema.II.4.6**, se tiene que $d \mid b$ y $d \mid c$, es decir, d satisface (MCD.I). Si $s \mid b$ y $s \mid c$, tenemos que $as \mid ab$ y $as \mid ac$. Por (MCD.II), $as \mid ad$ y de nuevo por la Ley de Cancelación $s \mid d$, es decir, d satisface (MCD.II).

2. Si R es un D.I.P., entonces cada ideal del anillo cociente R/I es principal.

Solución: Cierto. Consideramos el homomorfismo de anillos sobreyectivo $p : R \to R/I$ de paso al cociente dado por $p(a) = a + I$. Dado L un ideal de R/I, por la **Proposición II.3.4.(vi)**, sabemos que $p^{-1}(L)$ es un ideal de R. Como R es un D.I.P., existe $x \in R$ tal que $\big(x\big) = p^{-1}(L)$.
Veamos que $L = \big(p(x)\big)$. Como $x \in \big(x\big) = p^{-1}(L)$, se tiene que $p(x) \in L$ luego $\big(p(x)\big) \subseteq L$. Recíprocamente, dado $\ell \in L$ como p es sobreyectiva, existe $y \in R$ tal que $p(y) = \ell$. Por consiguiente, $y \in \big(x\big) = p^{-1}(L)$. Como R es un dominio, $\big(x\big) = \{rx; r \in R\}$, es decir, $y = rx$ para algún $r \in R$. Como p es homomorfismo de anillos, $\ell = p(y) = p(r)p(x)$. Deducimos que $\ell \in \big(p(x)\big)$ y concluimos que $L \subseteq \big(p(x)\big)$. En resumen hemos probado que cada ideal L del anillo cociente R/I está generado por un único elemento, es decir, es principal.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Recordamos que el anillo $\mathbb{C}[x, y]$ se define como $\mathbb{C}[x]([y])$

1. Probar que $x^2 + y^2 - 4$ es un elemento irreducible de $\mathbb{C}[x, y]$.

Solución: Sabemos que $\mathbb{C}[x, y] = (\mathbb{C}[x])([y])$ como $\mathbb{C}$ es un cuerpo $\mathbb{C}[x]$ es un D.E. y por los **Teoremas II.5.27** y **II.5.22** $\mathbb{C}[x]$ es un D.F.U. Observamos que podemos escribir $P(x, y) = x^2 + y^2 - 4 = a_2(x)y^2 + a_1(x)y + a_0(x)$ con $a_2(x) = 1$, $a_1(x)$ y $a_0(x) = x^2 - 4 = (x + 2)(x - 2)$ que es un polinomio primitivo de $(\mathbb{C}[x])([y])$. Por el **Ejercicio A.43**, tenemos que $x - 2$ es un elemento irreducible de $\mathbb{C}[x]$. Aplicando el **Criterio de Eisenstein (Ejercicio A.66)** a $P(x, y)$ para $p = x - 2$ deducimos que $x^2 + y^2 - 4$ es un elemento irreducible de $\mathbb{C}[x, y]$.

2. Probar que $\mathbb{C}[x, y]/(x^2 + y^2 - 4)$ es un dominio.

Solución: En el apartado anterior hemos visto que $\mathbb{C}[x]$ es un D.F.U., por el **Problema A.60**, $\mathbb{C}[x, y]$ es un D.F.U.. Por el apartado anterior sabemos que $P(x, y)$ es irreducible, luego por la **Proposición II.5.10**, $P(x, y)$ es primo. Por la **Proposición II.5.6**, $(P(x, y))$ es un ideal primo. Por el **Proposición II.4.14**, $\mathbb{C}[x, y]/(x^2 + y^2 - 4)$ es un dominio.

3. Si $I = (x^2 + y^2 - 4)$, probar que $(x + iy) + I \in U(\mathbb{C}[x, y]/I)$.

Solución: Basta observar que, por la definición de la suma y el producto en $\mathbb{C}[x, y]/I$ y como $4 + I = x^2 + y^2 + I$, tenemos que $((x + iy) + I)((1/4)(x - iy) + I) = (1/4)(x^2 + y^2) + I = 1 + I$.

UNIVERSIDAD DE CANTABRIA

Examen final
miércoles 3 de junio de 2020
Convocatoria ordinaria

G90 - Estructuras Algebraicas
Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo finito y abeliano, si $d \mid \#G$ entonces existe $a \in G$ tal que $O(a) = d$.
2. En D_{37} consideramos el subgrupo R de las rotaciones entonces $R \lhd D_{37}$.
3. Sea $(G,\cdot)$ un grupo $K \lhd G$ un subgrupo. Si $Z(G) = \{z \in G\,;\, zx = xz \text{ para todo } x \in G\}$, entonces $K \subseteq Z(G)$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = S_4$ y $H = D_4 \times \mathbb{Z}/3\mathbb{Z}$.

1. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.
2. Determinar si G y H son o no son grupos isomorfos.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si $\mathrm{car}(R) = n > 0$ y R es un cuerpo, entonces $\#R < \infty$.
2. Si R es un dominio, entonces $\#R \neq 21$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Consideramos el dominio $\mathbb{Z}[\sqrt{15}] = \{a + b\sqrt{15}\,;\, a,b \in \mathbb{Z}\}$.

1. Probar que $7 + 2\sqrt{15}$ es irreducible en $\mathbb{Z}[\sqrt{15}]$.
2. Demuestra que $4 + \sqrt{15}$ es una unidad en $\mathbb{Z}[\sqrt{15}]$ y dar 6 divisores diferentes de 1 en $\mathbb{Z}[\sqrt{15}]$.
3. Probar que $\mathbb{Z}[\sqrt{15}]$ y que $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3}\,;\, a,b \in \mathbb{Z}\}$ no son anillos isomorfos.

Esquema de una solución de la versión Ñ del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo finito y abeliano, si $d \mid \#G$ entonces existe $a \in G$ tal que $O(a) = d$.

   Solución: Falsa. Basta considerar $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ que es un grupo finito y abeliano. Tenemos que $\#G = 4$, pero $O((0,0)) = 1$ y $O((0,1)) = O((1,0)) = O((1,1)) = 2$, es decir, no existe $a \in G$ con $O(a) = 4$.

2. En D_{37} consideramos el subgrupo R de las rotaciones entonces $R \lhd D_{37}$.

   Solución: Verdadera. Por el **E156**, sabemos que $\#R = 37$ y que $\#D_{37} = 2 \cdot 37 = 74$. Por el Teorema de Lagrange, $\#(D_{37} : R) = 2$. Por el **E167**, concluimos que $R \lhd D_{37}$.

3. Sea $(G,\cdot)$ un grupo $K \lhd G$ un subgrupo. Si $Z(G) = \{z \in G\,;\, zx = xz \text{ para todo } x \in G\}$, entonces $K \subseteq Z(G)$.

   Solución: Falsa. Con la notación del **E156**, basta considerar $G = D_4$, $K = \langle a \rangle$. Sabemos que $\#K = 4$ y que $\#D_4 = 8$. Por el Teorema de Lagrange, se tiene que $\#(D_4 : K) = 2$ y, por **E167**, concluimos que $K \lhd D_4$. Comprobamos empleando las propiedades del **E156** que $Z(D_4) = \langle a^2 \rangle = \{1, a^2\}$, luego $K \not\subseteq Z(D_4)$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = S_4$ y $H = D_4 \times \mathbb{Z}/3\mathbb{Z}$.

Solución: Lema Auxiliar. Dados dos grupos finitos A, B, y dos elementos $a \in A$, $b \in B$, se tiene que el orden de (a,b) como elemento del grupo producto $A \times B$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a,b)) = m.c.m.\{O(a), O(b)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b)\}$, por la definición del grupo producto tenemos que $(a,b)^m = (a^m, b^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$ y $b^m = 1_B$, luego $(a,b)^m = 1_{A\times B}$ y, de nuevo la Proposición 1.3.6.2, $O((a,b)) \mid m$. Por otra parte, si $O((a,b)) = t$ como $(a,b)^t = 1_{A\times B}$ se tiene que $a^t = 1_A$ y $b^t = 1_B$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$ y $O(b) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.

   Solución: Por la Proposición 1.6.2, como $\mathbb{Z}/3\mathbb{Z} = \langle 1 \rangle$ es cíclico f queda completamente determinado por $f(1)$. Además por la Proposición 1.6.2. sabemos que $O(f(1)) \mid 3$ y que para cada $b \in G$ con $O(b) \mid 3$ existe un único homomorfismo $f_b : \mathbb{Z}/3\mathbb{Z} \to G$ tal que $f(1) = b$. Por consiguiente determinar los homomorfismos equivale a determinar los elementos $b \in G$ con $O(b) \in \{1, 3\}$.
   Observamos que $O(b) = 1$ si y sólo si $b = 1_G$. Empleando la descomposición en ciclos disjuntos de los elementos de S_4 (**Cor. 1.4.1.**), vemos que los elementos de orden 3 de S_4 son necesariamente ciclos de longitud 3. Por consiguiente, hay 9 homomorfismos de grupos $\mathbb{Z}/3\mathbb{Z}$ en G determinados por $f_1(1) = id$, $f_2(1) = (123)$, $f_3(1) = (132)$, $f_4(1) = (124)$, $f_5(1) = (142)$, $f_6(1) = (134)$, $f_7(1) = (143)$, $f_8(1) = (234)$ y $f_9(1) = (243)$.

2. Determinar si G y H son o no son grupos isomorfos.

   Solución: Observamos que $\#G = \#H = 24$, por tanto, no podemos emplear el cardinal para determinar si son isomorfos o no. Por tanto, con la notación del **E156**, si consideramos el elemento $x = ((1234), 1)$ de H por el Lema Auxiliar $O(x) = 12$. Por otro lado, empleando la descomposición en ciclos disjuntos (**Cor. 1.4.1.**), comprobamos que los posibles órdenes de los elementos de $G = S_4$ son $\{1, 2, 3, 4\}$. Deducimos ni de orden 49 de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y G no son isomorfos porque en H hay un elemento de orden 12 y en G no.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si $\mathrm{car}(R) = n > 0$ y R es un cuerpo, entonces $\#R < \infty$.

   Solución: Falso. Por el **Ejemplo II.4.8**, sabemos que $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ es un dominio. Como los dominios son anillos unitarios, por el **Teorema.II.3.18**, $\mathrm{car}(\mathbb{Z}/3\mathbb{Z}) = O(1_{\mathbb{Z}/3\mathbb{Z}}) = 3$. Por **Ejercicio.A.29**, sabemos que $(\mathbb{Z}/3\mathbb{Z}[x], +, \cdot)$ es un dominio. Por el **Ejercicio.A.24**, sabemos que la característica de $\mathbb{Z}/3\mathbb{Z}[x]$ es la misma que la de $\mathbb{Z}/3\mathbb{Z}[x]$, es decir, $\mathrm{car}(\mathbb{Z}/3\mathbb{Z}[x]) = \mathrm{car}(\mathbb{Z}/3\mathbb{Z}) = 3$. Por el **Ejercicio.A.26**, la característica de $\mathbb{Z}/3\mathbb{Z}[x]$ coincide con la característica de su cuerpo de fracciones $F(\mathbb{Z}/3\mathbb{Z}[x]) = \mathbb{Z}/3\mathbb{Z}(x)$. Finalmente, como $\mathbb{Z}/3\mathbb{Z}[x]$ tiene infinitos elementos, concluimos que $R = \mathbb{Z}/3\mathbb{Z}(x)$ es un cuerpo con infinitos elementos y con $\mathrm{car}(R) = 3 > 0$.

2. Si R es un dominio, entonces $\#R \neq 21$.

   Solución: Cierto. Razonamos por reducción al absurdo y suponemos que $\#R = 21$. Como R es un dominio, por (D.II) es un anillo unitario. Por el **Teorema II.3.18**, se tiene que $\mathrm{car}(R) = O(1_R)$. Por el **Teorema de Lagrange**, $O(1_R) \mid \#R = 21$, luego $O(1_R)$ es $1, 3, 7$ o 21. Por el **Corolario II.4.9**, tenemos que $\mathrm{car}(R) = p$ con p primo. Por tanto, tenemos dos opciones:
   (A) $\mathrm{car}(R) = O(1_R) = 7$. Por la definición de característica, $7x = 0$ para todo $x \in R$, luego $O(x) \mid 7$ para todo $x \in R$. Por el **Teorema de Cauchy para grupos Abelianos**, como $3 \mid \#R$, existe un elemento $r \in R$ con $O(r) = 3$, contradiciendo que $O(r) \mid 7$.
   (B) $\mathrm{car}(R) = O(1_R) = 3$, razonando como en el caso (A) llegamos a contradicción.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Consideramos el dominio $\mathbb{Z}[\sqrt{15}] = \{a + b\sqrt{15}\,;\, a, b \in \mathbb{Z}\}$.

1. Probar que $7 + 2\sqrt{15}$ es irreducible en $\mathbb{Z}[\sqrt{15}]$.

   Solución: Emplearemos las propiedades de la función $N(a + b\sqrt{15}) = a^2 - b^2 15$ del **E460**. Se tiene que $N(7 + 2\sqrt{15}) = -11$. Como -11 es primo en $\mathbb{Z}$, por la propiedad (IV), $7 + 2\sqrt{15}$ es irreducible en $\mathbb{Z}[\sqrt{15}]$.

2. Demuestra que $4 + \sqrt{15}$ es una unidad en $\mathbb{Z}[\sqrt{15}]$ y dar 6 divisores diferentes de 1 en $\mathbb{Z}[\sqrt{15}]$.

   Solución: Con la notación del primer apartado $N(4 + \sqrt{15}) = 16 - 15 = 1$ y, por el **E460**, $u = 4 + \sqrt{15}$ es una unidad en $\mathbb{Z}[\sqrt{15}]$. Observamos que u^n para $n \in \mathbb{N}$ es una unidad porque $N(u^n) = (N(u))^n = 1$. Comprobamos que $u^2 = 31 + 8\sqrt{15}$ y que $u^3 = 244 + 63\sqrt{15}$ y tenemos seis divisores diferentes de 1 en $\mathbb{Z}[\sqrt{15}]$: u, $u^{-1} = 4 - \sqrt{15}$, u^2, $u^{-2} = 31 - 8\sqrt{15}$, u^3 y $u^{-3} = 244 - 63\sqrt{15}$.

3. Probar que $\mathbb{Z}[\sqrt{15}]$ y que $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3}\,;\, a, b \in \mathbb{Z}\}$ no son anillos isomorfos.

   Solución: Razonamos por reducción al absurdo y suponemos que existe $\psi : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}[\sqrt{15}]$ un isomorfismo de anillos. Como ψ es un isomorfismo podemos probar que $\psi(1) = 1$. En consecuencia, por (HA.I), $\psi(3) = \psi(1 + 1 + 1) = \psi(1) + \psi(1) + \psi(1) = 3$. Por otro lado, por (HA.II), $\psi(3) = \psi(\sqrt{3}\sqrt{3}) = (\psi(\sqrt{3}))^2$. En resumen, deberían existir $a, b \in \mathbb{Z}$ tales que $(a + b\sqrt{15})^2 = (\psi(\sqrt{3}))^2 = \psi(3) = 3$. Reescribiendo, esta igualdad existirían $a, b \in \mathbb{Z}$ tales que $a^2 + b^2 15 + 2ab\sqrt{15} = 3$. Igualando términos, tenemos dos opciones o $a = 0$ y $b^2 5 = 1$ (imposible) o $b = 0$ y $a^2 = 3$ (imposible) porque $a, b \in \mathbb{Z}$.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo si hay un elemento $a \in G$ de orden 18, entonces hay por lo menos 6 elementos de orden 18.
2. Dado $K \subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K \subseteq A_n$.
3. Sea $(G,\cdot)$ un grupo y H_1, H_2 subgrupos de G tales que $H_1 \lhd H_2$ y que $H_2 \lhd G$ entonces $H_1 \lhd G$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ y $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times D_7$.

1. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.
2. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio y todo ideal de R distinto de R es primo, entonces R es un cuerpo.
2. Existe R es no conmutativo de modo que se satisface la siguiente propiedad:
   para todos $r,s,t \in R$ con $r \neq 0$ si $rs = tr$, entonces $s = t$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[i] = \{a+bi\,;\, a,b \in \mathbb{Z}\}$, el anillo de los enteros de Gauss, consideramos el ideal $I = (1+7i)$ y el anillo cociente $A = \mathbb{Z}[i]/I$.

1. Probar que $i+I = 7+I$ y deducir que para todo elemento $a+bi$ de $\mathbb{Z}[i]$ existe $k \in \mathbb{Z}$ tal que $(a+bi)+I = k+I$.
2. Construye un homomorfismo de anillos $\Psi : \mathbb{Z} \to A$ sobreyectivo.
3. Encuentra un valor de $n \in \mathbb{N}$ tal que $\mathbb{Z}/n\mathbb{Z} \approx A$. ¿Es A un cuerpo?

Esquema de una solución de la versión O del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo si hay un elemento $a \in G$ de orden 18, entonces hay por lo menos 6 elementos de orden 18.

   Solución: Verdadera. Por la Proposición 1.3.6, $\#(\langle a\rangle) = O(a) = 18$. Por el Teorema 1.3.1.c), en $\langle a\rangle$ hay $\varphi(18)$ elementos de orden 18. Por el **E13**, $\varphi(18) = 18(1/2)(2/3) = 6$ y, como $\langle a\rangle \subseteq G$, concluimos que hay por lo menos 6 elementos de orden 18 en G.

2. Dado $K \subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K \subseteq A_n$.

   Solución: Verdadera. Tenemos que $\#K = 2k+1$ con $k \in \mathbb{Z}$, por el Corolario 1.5.1.a), para todo $\alpha \in K$ tenemos que $O(\alpha) \mid 2k+1$. Por la Proposición 1.3.6.2, $\alpha^{2k+1} = id$. Luego $\alpha^{2k}\alpha = 1$ y deducimos que $\alpha = \alpha^{-2k} = (\alpha^{-k})^2$. Por consiguiente, tanto si $\beta = \alpha^{-k}$ es una permutación par como si β es impar, β^2 es par. En consecuencia, $\alpha = \beta^2 \in A_n$ y concluimos que $K \subseteq A_n$.

3. Sea $(G,\cdot)$ un grupo y H_1, H_2 subgrupos de G tales que $H_1 \lhd H_2$ y que $H_2 \lhd G$ entonces $H_1 \lhd G$.

   Solución: Falsa. Con la notación del **E156**, basta considerar $G = D_4$, $H_1 = \{id, b\} = \langle b\rangle$ y $H_2 = \{id, b, a^2, a^2b\} = \langle a, b\rangle$. Sabemos que $\#H_1 = 2$, $\#H_2 = 4$ y que $\#D_4 = 8$. Por el Teorema de Lagrange, se tiene que $\#(H_2 : H_1) = 2$ y $\#(D_4 : H_2) = 2$. Por el **E167**, concluimos que $H_1 \lhd H_2$ y que $H_2 \lhd D_4$. Finalmente, observamos que $aH_1 = \{a, ab\}$ y que $H_1a = \{a, ba\}$ y, por el **E156**, sabemos $ba = a^3b$ y que $a^3b \neq ab$. Por consiguiente, $aH_1 \neq H_1a$ y concluimos que H_1 no es normal en D_4.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ y $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times D_7$.

Solución: Lema Auxiliar. Dados tres grupos finitos A, B, C, y tres elementos $a \in A$, $b \in B$,$c \in C$ se tiene que el orden de (a,b,c) como elemento del grupo producto $A \times B \times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a,b,c)) = m.c.m.\{O(a), O(b), O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b), O(c)\}$, por la definición del grupo producto tenemos que $(a,b,c)^m = (a^m, b^m, c^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$, $b^m = 1_B$ y $c^m = 1_C$, luego $(a,b,c)^m = 1_{A\times B\times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a,b,c)) \mid m$. Por otra parte, si $O((a,b,c)) = t$ como $(a,b,c)^t = 1_{A\times B\times C}$ se tiene que $a^t = 1_A$, $b^t = 1_B$ y $c^t = 1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$, $O(b) \mid t$ y $O(c) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.

   Solución: Consideramos $f : G \to G$ dado por $f(a,b) = (0,b)$. Comprobamos de forma directa que f es un endomorfismo (proyección), que $\mathrm{Ker} f = \mathbb{Z}/14\mathbb{Z} \times \{0\}$ y que $\mathrm{Im} f = \{0\} \times \mathbb{Z}/14\mathbb{Z}$. Demostramos que $\mathrm{Ker} f \approx \mathrm{Im} f \approx \mathbb{Z}/14\mathbb{Z}$, para probar esto se puede ver que ambos grupos son cíclicos de orden 15 y concluir usando la Proposición 1.6.3.

2. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

   Solución: Observamos que $\#G = \#H = 196$. Buscamos K con $\#K = 196$ de modo que $K \not\approx H$ y $K \not\approx G$. Consideramos $K := \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, cumple que $\#K = 196$. Por el Teorema 1.3.1, sabemos que el orden de los elementos de $\mathbb{Z}/2\mathbb{Z}$ es 1 o 2, el orden de los elementos de $\mathbb{Z}/4\mathbb{Z}$ es 1, 2 o 4, el orden de los elementos de $\mathbb{Z}/7\mathbb{Z}$ es 1 o 7, el orden de los elementos de $\mathbb{Z}/14\mathbb{Z}$ es 1, 2, 7 o 14. Por otro lado, por el **E156**, comprobamos que los posibles órdenes de los elementos de D_7 son $\{1, 2, 7\}$. Empleando el Lema Auxiliar vemos que:

   - en K hay elementos de orden 4.
   - en $\mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \approx G$ no hay ningún elemento de orden 4.
   - en H no hay ningún elemento de orden 4.

Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, G y K no son isomorfos y H y K tampoco son isomorfos.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio y todo ideal de R distinto de R es primo, entonces R es un cuerpo.

   Solución: Cierto. Como R es dominio se satisfacen (F.I) y (F.II) basta comprobar que se satisface (F.III), es decir, que $U(R) = R\backslash\{0_R\}$. Como R es un dominio por (D.III), se tiene que $U(R) \subseteq R\backslash\{0_R\}$. Veamos ahora que se cumple la contención contraria. Dado $x \in R\backslash\{0_R\}$ consideremos el ideal $J_1 = (x)$.
   Si $J_1 \subsetneq R$, consideramos el ideal $J_2 = (x^2)$. Como $x^2 \in J_1$ y $J_1 \subsetneq R$, se tiene que $J_2 \subseteq J_1 \subsetneq R$. Por hipótesis, J_2 es primo. Como $x \cdot x = x^2 \in J_2$, tenemos que $x \in J_2$. Por consiguiente, existe $r \in R$ tal que $x = rx^2$ y por la Ley de Cancelación, **Teorema.II.4.6**, $1_R = rx$. Por tanto, $1_R \in J_1$ y tenemos que $J_1 = R$ contradiciendo nuestra suposición.
   Si $J_1 = R$, entonces $1_R \in (x)$, luego existe $u \in R$ tal que $1_R = ux$, es decir, $x \in U(R)$ y concluimos que R es un cuerpo.

2. Existe R es no conmutativo de modo que se satisface la siguiente propiedad:
   para todos $r,s,t \in R$ con $r \neq 0$ si $rs = tr$, entonces $s = t$.

   Solución: Falso. Veamos que si R satisface esta propiedad, entonces R debe ser conmutativo. Dados $x,y \in R$, si $x = 0$ o $y = 0$, por la **Proposición.II.1.9**, $xy = 0_R = yx$. Supongamos que $x \neq 0$ y que $y \neq 0$. Tomamos $s = yx$, $t = xy$ y $r = x$, como por la propiedad asocitiva se tiene que $rs = x(yx) = (xy)x = tr$, aplicando la propiedad, dado que $r = x \neq 0$, concluimos que $yx = s = t = xy$. En consecuencia, hemos visto que R es conmutativo. En resumen, R no puede satisfacer la propiedad y al mismo tiempo ser no conmutativo.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[i] = \{a+bi\,;\, a,b \in \mathbb{Z}\}$, el anillo de los enteros de Gauss, consideramos el ideal $I = \big(1+7i\big)$ y el anillo cociente $A = \mathbb{Z}[i]/I$.

1. Probar que $i+I = 7+I$ y deducir que para todo elemento $a+bi$ de $\mathbb{Z}[i]$ existe $k \in \mathbb{Z}$ tal que $(a+bi)+I = k+I$.

   Solución: Observamos que $i - 7 = i(1+7i) \in I$, luego $i + I = 7 + I$. Dado un elemento $a+bi$ de $\mathbb{Z}[i]$ con $a,b \in \mathbb{Z}$, por las propiedades de la suma y el producto en A, se tiene que $(a+bi)+I = (a+I)+(b+I)(7+I) = (a+b7)+I$. En otras palabras, como $a+b7 \in \mathbb{Z}$, queda demostrado el apartado.

2. Construye un homomorfismo de anillos $\Psi : \mathbb{Z} \to A$ sobreyectivo.

   Solución: Basta considerar $\Psi = p \circ f$ donde $f : \mathbb{Z} \to \mathbb{Z}[i]$ es la inyección canónica y $p : \mathbb{Z}[i] \to \mathbb{Z}[i]/I$ es la aplicación de paso al cociente. Como f y p son homomorfismos de anillos, por la **Proposición II.3.3**, Ψ es también un homomorfismo de anillos y está dado por $\Psi(k) = k + I$. Por el apartado anterior, para todo elemento $a+bi$ de $\mathbb{Z}[i]$ existe $k \in \mathbb{Z}$ tal que $(a+bi)+I = k+I$, luego $\Psi(k) = (a+bi)+I$, es decir, Ψ es sobreyectivo.

3. Encuentra un valor de $n \in \mathbb{N}$ tal que $\mathbb{Z}/n\mathbb{Z} \approx A$. ¿Es A un cuerpo?

   Solución: Observamos que dado $k \in \mathbb{Z}$, $k \in \mathrm{Ker}\Psi$ si y solo si $k + I = I$, es decir, si y solo si $k \in I$. Vemos que $k \in I$ si y solo si existen $a,b \in \mathbb{Z}$ con $k = (a+bi)(1+7i)$, es decir, si y solo si, existen $a,b \in \mathbb{Z}$, $k = a - 7b$ y $0 = 7a + b$. Deducimos que $k \in \mathrm{Ker}\Psi$ si y solo si existe $a \in \mathbb{Z}$ tal que $k = 50a$, es decir, si y solo si, $k \in 50\mathbb{Z}$, dicho de otro modo, $n = 50$. Como Ψ es sobreyectivo, por **Primer teorema de isomorfía (Teorema II.3.8)**, $\mathbb{Z}/50\mathbb{Z} \approx A$. Por el **Ejemplo II.4.8**, tenemos que $\mathbb{Z}/50\mathbb{Z}$ no es un cuerpo porque 50 no es primo. Deducimos que A tampoco es un cuerpo porque, por ejemplo, la imagen de un divisor de cero no nulo por un isomorfismo es un divisor de cero no nulo. En otras palabras, en A hay divisores de cero no nulos.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo no abeliano y $K \lhd G$ un subgrupo no abeliano entonces G/K es no abeliano.
2. Sea $(G,\cdot)$ un grupo si $\#G = \infty$ entonces existe $a \in G$ tal que $O(a) = \infty$.
3. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = D_3 \times D_4 \times D_5$ y $H = S_5 \times C_2 \times C_2$.

1. Determinar si G y H son o no son grupos isomorfos.
2. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si $\mathrm{car}(R) = n > 0$, entonces $\mathrm{car}(R \times R \times R) = n^3$.
2. Si R es un dominio, S es un dominio, $f : S \to R$ es un homomorfismo de anillos e I es maximal en R, entonces $f^{-1}(I)$ es maximal en S.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[x]$, el anillo de los polinomios con coeficientes enteros, consideramos el ideal $I = (10, x-3)$ y el anillo cociente $A = \mathbb{Z}[x]/I$.

1. Probar que $x+I = 3+I$ y deducir que para todo elemento $P(x)$ de $\mathbb{Z}[x]$ existe $k \in \mathbb{Z}$ tal que $P(x)+I = k+I$.
2. Probar que $Q(x) = 6x^3 + 5x^2 + 8x + 12$ es irreducible en $\mathbb{Z}[x]$.
3. Encuentra el inverso de $Q(x) + I$ en A.

Esquema de una solución de la versión P del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo no abeliano y $K \lhd G$ un subgrupo no abeliano entonces G/K es no abeliano.

   Solución: Falsa. Basta considerar $G = S_4$ y $K = A_4$. Observamos que $(123), (234) \in A_4 \subseteq S_4$ y que $(123)(234) = (12)(34) \neq (13)(24) = (234)(123)$ luego G y K no son abelianos. Por el **E116**, $\#A_4 = 12$ y como $\#S_4 = 24$, por el Teorema de Lagrange, se tiene que $\#(S_4 : A_4) = 2$. Por el **E167**, vemos que $A_4 \lhd S_4$. Como $\#(S_4 : A_4) = \#(S_4/A_4) = 2$, por el Corolario 1.5.1.b), el grupo cociente S_4/A_4 es cíclico y, por tanto, es abeliano.

2. Sea $(G,\cdot)$ un grupo si $\#G = \infty$ entonces existe $a \in G$ tal que $O(a) = \infty$.

   Solución: Falsa. Tenemos que $(\mathbb{Q},+)$ es un grupo abeliano, luego $\mathbb{Z} \lhd \mathbb{Q}$. Por el Teorema 1.5.6, $(\mathbb{Q}/\mathbb{Z},+)$ es un grupo. Dado un elemento $a+\mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, existen $p \in \mathbb{Z}$ y $q \in \mathbb{N}$ tales que $a = p/q$. Observamos que $q(a+\mathbb{Z}) = q(p/q+\mathbb{Z}) = p+\mathbb{Z} = 0+\mathbb{Z}$ y concluimos que $O(a+\mathbb{Z}) < \infty$. Dados dos elementos distintos $r, s \in [0,1) \cap \mathbb{Q}$ tenemos que $r - s \notin \mathbb{Z}$, luego $r+\mathbb{Z} \neq s+\mathbb{Z}$. En otras palabras, cada elemento de $[0,1) \cap \mathbb{Q}$ define una clase distinta en $\mathbb{Q}/\mathbb{Z}$. Por la Propiedad de Densidad, $\#([0,1) \cap \mathbb{Q}) = \infty$, luego $\#(\mathbb{Q}/\mathbb{Z}) = \infty$ (Alternativa ver **E82**).

3. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.

   Solución: Falsa. Escribimos α como el producto de ciclos disjuntos $\alpha = (1\,8)(2\,7)(4\,9\,5\,6)$. Por la Proposición 1.4.1, sabemos las permutaciones disjuntas conmutan y se tiene que

   $$\alpha^3 = (1\,8)^3(2\,7)^3(4\,9\,5\,6)^3 = (1\,8)(2\,7)(4\,6\,5\,9).$$

   Finalmente, observamos que $(4\,6\,5\,9) = (4\,9)(4\,5)(4\,6)$. En consecuencia, α^3 descompone como producto de 5 transposiciones y concluimos que es impar y, por tanto, $\alpha^3 \notin A_9$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = D_3 \times D_4 \times D_5$ y $H = S_5 \times C_2 \times C_2$.

Solución: Lema Auxiliar. Dados tres grupos finitos A, B, C, y tres elementos $a \in A$, $b \in B$, $c \in C$ se tiene que el orden de (a,b,c) como elemento del grupo producto $A \times B \times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a,b,c)) = m.c.m.\{O(a), O(b), O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b), O(c)\}$, por la definición del grupo producto tenemos que $(a,b,c)^m = (a^m, b^m, c^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$, $b^m = 1_B$ y $c^m = 1_C$, luego $(a,b,c)^m = 1_{A\times B\times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a,b,c)) \mid m$. Por otra parte, si $O((a,b,c)) = t$ como $(a,b,c)^t = 1_{A\times B\times C}$ se tiene que $a^t = 1_A$, $b^t = 1_B$ y $c^t = 1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$, $O(b) \mid t$ y $O(c) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Determinar si G y H son o no son grupos isomorfos.

   Solución: Observamos que $\#G = \#H = 480$, por tanto, no podemos emplear el cardinal para determinar si son isomorfos o no. Por tanto, con la notación del **E156**, si consideramos el elemento $x = ((123), (1234), (12345))$ de G por el Lema Auxiliar $O(x) = 60$. Por otro lado, empleando la descomposición en ciclos disjuntos (**Cor. 1.4.1.**), comprobamos que los posibles órdenes de los elementos de S_5 son $\{1,2,3,4,5,6\}$. Por el Lema Auxiliar, los posibles órdenes de los elementos de H son $\{1,2,3,4,5,6,10\}$. Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y G no son isomorfos porque en G hay un elemento de orden 60 y en H no.

2. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.

Solución: Por la Proposición 1.6.2, como $\mathbb{Z}/3\mathbb{Z} = \langle 1 \rangle$ es cíclico f queda completamente determinado por $f(1)$. Además por la Proposición 1.6.2. sabemos que $O(f(1)) \mid 3$ y que para cada $b \in G$ con $O(b) \mid 3$ existe un único homomorfismo $f_b : \mathbb{Z}/3\mathbb{Z} \to G$ tal que $f(1) = b$. Por consiguiente determinar los homomorfismos equivale a determinar los elementos $b \in G$ con $O(b) \in \{1, 3\}$.
Observamos que $O(b) = 1$ si y sólo si $b = 1_G$. Empleando el **E156**, vemos que el posible orden de los elementos de D_3 es $\{1, 2, 3\}$ de los elementos de D_4 es $\{1, 2, 4\}$ y de D_5 es $\{1, 2, 5\}$. Por tanto, por el Lema Auxiliar, deducimos que los elementos de orden 3 de G son $((123), id, id)$ y $((132), id, id)$. Por consiguiente, hay tres homomorfismos de grupos $\mathbb{Z}/3\mathbb{Z}$ en G determinados por $f_1(1) = (id, id, id)$, $f_2(1) = ((123), id, id)$ y $f_3(1) = ((132), id, id)$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si $\text{car}(R) = n > 0$, entonces $\text{car}(R \times R \times R) = n^3$.

   Solución: Falso. Por el **Ejemplo II.4.8**, sabemos que $(R, +, \cdot) = (\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ es un dominio. Como los dominios son anillos unitarios, por el **Teorema.II.3.18**, $\text{car}(\mathbb{Z}/3\mathbb{Z}) = O(1_{\mathbb{Z}/3\mathbb{Z}}) = 3$. Como en el anillo producto $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ las operaciones se definen componete a componete es un anillo unitario con elemento neutro $(1_{\mathbb{Z}/3\mathbb{Z}}, 1_{\mathbb{Z}/3\mathbb{Z}}, 1_{\mathbb{Z}/3\mathbb{Z}})$. Por el **Teorema.II.3.18**, se tiene que $\text{car}(R \times R \times R) = O((1, 1, 1)) = 3 \neq 27 = 3^3$.

2. Si R es un dominio, S es un dominio, $f : S \to R$ es un homomorfismo de anillos e I es maximal en R, entonces $f^{-1}(I)$ es maximal en S.

   Solución: Falso. Basta considerar $S = \mathbb{Z}$, $R = \mathbb{Q}$ y $f : \mathbb{Z} \to \mathbb{Q}$ la inclusión canónica dada por $f(m) = m$ para todo $m \in \mathbb{Z}$ que es un homomorfismo de anillos. El ideal $I = (0)$ es maximal en $\mathbb{Q}$, porque $I \neq \mathbb{Q}$ (M.I) y si J es otro ideal con $I \subsetneq J$, existe $q \in J$ con $q \neq 0$, luego $1 = q^{-1}q \in J$ y por tanto, $J = \mathbb{Q}$, es decir, se satisface (M.II). Sin embargo, $f^{-1}(I) = (0)$ que no es un ideal maximal de $\mathbb{Z}$ porque, por ejemplo, $(0) \subsetneq (2) \subsetneq \mathbb{Z}$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En $\mathbb{Z}[x]$, el anillo de los polinomios con coeficientes enteros, consideramos el ideal $I = (10, x - 3)$ y el anillo cociente $A = \mathbb{Z}[x]/I$.

1. Probar que $x+I = 3+I$ y deducir que para todo elemento $P(x)$ de $\mathbb{Z}[x]$ existe $k \in \mathbb{Z}$ tal que $P(x)+I = k+I$.

   Solución: Observamos que $x - 3 \in I$, luego $x + I = 3 + I$. Dado un elemento $P(x) = \sum_{j=0}^{n} a_j x^j$ de $\mathbb{Z}[x]$, por las propiedades de la suma y el producto en A, se tiene que $P(x) + I = (\sum_{j=0}^{n} a_j x^j) + I = \sum_{j=0}^{n} \left((a_j + I)(x + I)^j\right) = \sum_{j=0}^{n} \left((a_j + I)(3 + I)^j\right) = P(3) + I$. Como $P(3) \in \mathbb{Z}$, queda demostrado el apartado.

2. Probar que $Q(x) = 6x^3 + 5x^2 + 8x + 12$ es irreducible en $\mathbb{Z}[x]$.

   Solución: El polinomio $Q(x)$ es primitivo en $\mathbb{Z}[x]$ y consideramos su clase módulo 5, es decir, el polinomio $\overline{Q(x)} = x^3 + 3x + 2$ de $(\mathbb{Z}/5\mathbb{Z})[x]$. Comprobamos que $\overline{Q(x)}$ no tiene raíces en $\mathbb{Z}/5\mathbb{Z}$ porque $\overline{Q(0)} = 2$, $\overline{Q(1)} = \overline{Q(2)} = 1$, $\overline{Q(3)} = \overline{Q(4)} = 3$. Por consiguiente, por el **Ejercicio A.44**, como $\text{gr}(\overline{Q(x)}) = 3$ y como $\mathbb{Z}/5\mathbb{Z}$ es un cuerpo (**Ejemplo II.4.8**), tenemos que $\overline{Q(x)}$ es irreducible en $(\mathbb{Z}/5\mathbb{Z})[x]$. Finalmente, por el **Criterio de irreducibilidad módulo** 5 **(Problema A.64)**, concluimos que $Q(x)$ es irreducible en $\mathbb{Z}[x]$.

3. Encuentra el inverso de $Q(x) + I$ en A.

   Solución: Por el primer apartado sabemos que $Q(x) + I = Q(3) + I = 243 + I$. Como $10 \in I$, $243 - 3 = 240 \in I$, luego $Q(x) + I = 3 + I$. Finalmente, observamos que $(3 + I)(7 + I) = (21 + I) = 1 + I$ porque $21 - 1 = 20 \in I$. En consecuencia, $(Q(x) + I)^{-1} = (7 + I)$.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. En D_{37} consideramos el subgrupo R de las rotaciones entonces $R \lhd D_{37}$.
2. Sea $(G,\cdot)$ un grupo $K \lhd G$ un subgrupo y $a \in G$. Si $O(aK) = n \in \mathbb{N}$, entonces $a^n = 1_G$.
3. Sea $(G,\cdot)$ un grupo si $a, b \in G$ son tales que $O(a) < \infty$ y $O(b) < \infty$, entonces $O(ab) < \infty$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = C_3 \times C_5 \times C_{15}$ y $H = C_9 \times C_{25}$.

1. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.
2. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un D.F.U. y $a, b, c \in R$ con $a \neq 0$, entonces

   $$d \text{ es un m.c.d. de } b \text{ y } c \text{ si y solo si } ad \text{ es un m.c.d. de } ab \text{ y } ac.$$

2. Si $r, s \in R$ entonces $(r+s)^2 = r^2 + 2rs + s^2$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En el anillo de los polinomios con coeficientes racionales, $\mathbb{Q}[x]$, consideramos: $P_1(x) = (3/4)x^7 + 36x - 18$ y $P_2(x) = (4/3)x^3 + 4x^2 - (40/3)x - 32$ de $\mathbb{Q}[x]$.

1. Probar que $P_1(x)$ es irreducible en $\mathbb{Q}[x]$ y que $P_2(x)$ no es irreducible en $\mathbb{Q}[x]$.
2. Determinar si $R_1 = \mathbb{Q}[x]/(P_1(x))$ y $R_2 = \mathbb{Q}[x]/(P_2(x))$ son o no son cuerpos.
3. Encuentra en R_1 el inverso de $((x-2)/200) + (P_1(x))$.

Esquema de una solución de la versión Q del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. En D_{37} consideramos el subgrupo R de las rotaciones entonces $R \lhd D_{37}$.

   Solución: Verdadera. Por el **E156**, sabemos que $\#R = 37$ y que $\#D_{37} = 2 \cdot 37 = 74$. Por el Teorema de Lagrange, $\#(D_{37} : R) = 2$. Por el **E167**, concluimos que $R \lhd D_{37}$.

2. Sea $(G, \cdot)$ un grupo $K \lhd G$ un subgrupo y $a \in G$. Si $O(aK) = n \in \mathbb{N}$, entonces $a^n = 1_G$.

   Solución: Falsa. Basta considerar $(G, \cdot) = (\mathbb{Z}, +)$, $K = 3\mathbb{Z}$ y $a = 2$. Como $(\mathbb{Z}, +)$ es abeliano tenemos que $3\mathbb{Z} \lhd \mathbb{Z}$ y $O(2 + 3\mathbb{Z}) = 3$ pero $3 \cdot 2 = 6 \neq 0$.

3. Sea $(G, \cdot)$ un grupo si $a, b \in G$ son tales que $O(a) < \infty$ y $O(b) < \infty$, entonces $O(ab) < \infty$.

   Solución: Falsa. Consideremos como grupo G, el grupo lineal $(GL(2, \mathbb{R}), \cdot)$ de las matrices 2×2 invertibles con coeficientes en $\mathbb{R}$ y tomamos

   $$A := \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \qquad B := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

   Observamos que $A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id$, $B^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id$, $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Por tanto, deducimos que $O(A) = 2$ y $O(B) = 2$. Sin embargo, probamos por inducción que para todo $n \in \mathbb{N}$ se tiene que $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ y concluimos que $O(AB) = \infty$. (Alternativa ver **E78**).

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = C_3 \times C_5 \times C_{15}$ y $H = C_9 \times C_{25}$.

Solución: Lema Auxiliar. Dados tres grupos finitos A, B, C, y tres elementos $a \in A$, $b \in B$,$c \in C$ se tiene que el orden de (a, b, c) como elemento del grupo producto $A \times B \times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a, b, c)) = m.c.m.\{O(a), O(b), O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b), O(c)\}$, por la definición del grupo producto tenemos que $(a, b, c)^m = (a^m, b^m, c^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$, $b^m = 1_B$ y $c^m = 1_C$, luego $(a, b, c)^m = 1_{A \times B \times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a, b, c)) \mid m$. Por otra parte, si $O((a, b, c)) = t$ como $(a, b, c)^t = 1_{A \times B \times C}$ se tiene que $a^t = 1_A$, $b^t = 1_B$ y $c^t = 1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$, $O(b) \mid t$ y $O(c) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

   Solución: Observamos que $\#G = \#H = 225$. Buscamos K con $\#K = 225$ de modo que $K \not\approx H$ y $K \not\approx G$. Consideramos $K := C_9 \times C_5 \times C_5$, cumple que $\#K = 225$. Por el Teorema 1.3.1, sabemos que el orden de los elementos de C_3 es 1 o 3,el orden de los elementos de C_5 es 1 o 5, el orden de los elementos de C_9 es 1, 3 o 9,el orden de los elementos de C_{15} es 1, 3, 5 o 15, y que el orden de los elementos de C_{25} es 1, 5 o 25. Empleando el Lema Auxiliar vemos que:

   - en K no hay ningún elemento de orden 25 pero sí hay elementos de orden 9.
   - en G no hay ningún elemento de orden 25 ni de orden 9.
   - en $C_1 \times C_9 \times C_{25} \approx C_9 \times C_{25} = H$ hay elementos de orden 9 y de orden 25.

   Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y K no son isomorfos y G y K tampoco son isomorfos.

2. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.

   Solución: Consideramos $f : G \to G$ dado por $f(a, b, c) = (0, c)$. Comprobamos de forma directa que f es un endomorfismo (proyección), que $\mathrm{Ker} f = C_3 \times C_5 \times \{0\}$ y que $\mathrm{Im} f = \{0\} \times \{0\} \times C_{15}$. Finalmente, demostramos que $\mathrm{Ker} f \approx \mathrm{Im} f \approx C_{15}$, para probar esto se puede ver que ambos grupos son cíclicos de orden 15 y concluir usando la Proposición 1.6.3.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un D.F.U. y $a,b,c \in R$ con $a \neq 0$, entonces

$$d \text{ es un m.c.d. de } b \text{ y } c \text{ si y solo si } ad \text{ es un m.c.d. de } ab \text{ y } ac.$$

Solución: Cierto. Supongamos que d es un m.c.d. de b y c. Por (MCD.I), $d \mid b$ y $d \mid c$, luego $ad \mid ab$ y $ad \mid ac$, es decir, ad satisface (MCD.I). Como R es un D.F.U., sabemos que existe x un m.c.d de ab y ac. Como $a \mid ab$ y $a \mid ac$, por (MCD.II), $a \mid x$. Dicho de otro modo, existe $r \in R$ tal que $x = ar$. Por (MCD.I), $x \mid ab$ y $x \mid ac$, luego $ar \mid ab$ y $ar \mid ac$. Como $a \neq 0$ y como R es un dominio, por la Ley de Cancelación, **Teorema.II.4.6**, se tiene que $r \mid b$ y que $r \mid c$. Como d es un m.c.d. de b y c, por (MCD.II), $r \mid d$, luego $x = ar \mid ad$ y como x es un m.c.d de ab y ac concluimos que ad también satisface (MCD.II) para ab y ac. En resumen, ad es un un m.c.d de ab y ac.
Recíprocamente, supongamos que ad es un m.c.d. de ab y ac. Por (MCD.I), $ad \mid ab$ y $ad \mid ac$, Como $a \neq 0$ y como R es un dominio, por la Ley de Cancelación, **Teorema.II.4.6**, se tiene que $d \mid b$ y $d \mid c$, es decir, d satisface (MCD.I). Si $s \mid b$ y $s \mid c$, tenemos que $as \mid ab$ y $as \mid ac$. Por (MCD.II), $as \mid ad$ y de nuevo por la Ley de Cancelación $s \mid d$, es decir, d satisface (MCD.II).

2. Si $r,s \in R$ entonces $(r+s)^2 = r^2 + 2rs + s^2$.

Solución: Falso. Basta considerar R el anillo de las matrices 2×2 con coeficientes en $\mathbb{R}$, es decir, $(\mathrm{Mat}_{2\times 2}(\mathbb{R}),+,\cdot)$ y tomar $r = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ y $s = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Observamos que

$$r^2 + 2rs + s^2 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}^2 + 2\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix},$$

pero $(r+s)^2 = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix}$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** En el anillo de los polinomios con coeficientes racionales, $\mathbb{Q}[x]$, consideramos: $P_1(x) = (3/4)x^7 + 36x - 18$ y $P_2(x) = (4/3)x^3 + 4x^2 - (40/3)x - 32$ de $\mathbb{Q}[x]$.

1. Probar que $P_1(x)$ es irreducible en $\mathbb{Q}[x]$ y que $P_2(x)$ no es irreducible en $\mathbb{Q}[x]$.

Solución: Observamos que podemos escribir $P_1(x) = (3/4)(x^7 + 48x - 24)$ y también que $P_2(x) = (4/3)(x^3 + 3x^2 - 10x - 24)$. Como $Q_1(x) = x^7 + 48x - 24$ es primitivo, por el **Ejercicio A.57**, sabemos que $P_1(x)$ es irreducible en $\mathbb{Q}[x]$ si y solo si $Q_1(x)$ es irreducible en $\mathbb{Z}[x]$. Aplicando el **Criterio de Eisenstein (Problema A.66)** a $Q_1(x)$ para $p = 3$, vemos que $Q_1(x)$ es irreducible en $\mathbb{Z}[x]$. Por el **Teorema de la raíz racional (Ejercicio A.70)**, sabemos que las posibles raíces racionales de $Q_2(x) = x^3 + 3x^2 - 10x - 24$ son divisores de 24. Comprobamos que $-2, 3, -4$ son raíces de $Q_2(x)$ y, en consecuencia, también son raíces de $P_2(x)$. Por el **Ejercicio A. 44**, concluimos que $P_2(x)$ no es irreducible.

2. Determinar si $R_1 = \mathbb{Q}[x]/(P_1(x))$ y $R_2 = \mathbb{Q}[x]/(P_2(x))$ son o no son cuerpos.

Solución: Por el **Ejercicio A.48** y el apartado 1, R_1 es un cuerpo y R_2 no es un cuerpo.

3. Encuentra en R_1 el inverso de $((x-2)/200) + (P_1(x))$.

Solución: Mediante el Algoritmo de Euclides calculamos el m.c.d. y los enteros de la identidad de Bezout de $P(x) = (1/200)(x-2)$ y $P_1(x)$, vemos que

$$\begin{aligned} P_1(x) &= (1)P_1(x) + (0)P(x), \\ P(x) &= (0)P_1(x) + (1)P(x), \\ 150 &= (1)P_1(x) + ((-150)(x^6 + 2x^5 + 4x^4 + 8x^3 + 16x^2 + 32x + 112))P(x). \end{aligned}$$

En consecuencia, tomando clases módulo $I = (P_1(x))$ en la última igualdad tenemos que

$$1 + I = (-x^6 - 2x^5 - 4x^4 - 8x^3 - 16x^2 - 32x - 112 + I)(P(x) + I).$$

En otras palabras, El inverso de $P(x) + I$ en R_1 es $-x^6 - 2x^5 - 4x^4 - 8x^3 - 16x^2 - 32x - 112 + I$.

UNIVERSIDAD DE CANTABRIA

Examen final

miércoles 3 de junio de 2020

Convocatoria ordinaria

G90 - Estructuras Algebraicas

Curso 2019-2020

Instrucciones sobre el examen final

Realización del examen

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

Documento PDF del examen

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

Entrega del examen

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo $K \lhd G$ un subgrupo y $x, y \in G$. Si $O(x) = O(y) < \infty$, entonces $O(xK) = O(yK)$.
2. Dado $K \subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K \subseteq A_n$.
3. Sea $(G,\cdot)$ un grupo abeliano y $a, b \in G$ elementos de orden finito, entonces $O(ab)$ es el $m.c.m(O(a), O(b))$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = S_4$ y $H = D_4 \times \mathbb{Z}/3\mathbb{Z}$.

1. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.
2. Determinar si G y H son o no son grupos isomorfos.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un D.I.P., entonces R/I es D.I.P.
2. Si R es un dominio, entonces $\#R \neq 21$.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Recordamos que el anillo $\mathbb{C}[x, y]$ se define como $\mathbb{C}[x]([y])$

1. Probar que $x^2 + y^2 - 4$ es un elemento irreducible de $\mathbb{C}[x, y]$.
2. Probar que $\mathbb{C}[x, y]/(x^2 + y^2 - 4)$ es un dominio.
3. Si $I = (x^2 + y^2 - 4)$, probar que $(x + iy) + I \in U(\mathbb{C}[x, y]/I)$.

Esquema de una solución de la versión R del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Sea $(G,\cdot)$ un grupo $K \lhd G$ un subgrupo y $x, y \in G$. Si $O(x) = O(y) < \infty$, entonces $O(xK) = O(yK)$.

   Solución: Falsa. Basta considerar como grupo $(G,\cdot)$ el grupo producto $(\mathbb{Z}/6\mathbb{Z},+) \times (\mathbb{Z}/6\mathbb{Z},+)$, $K = \langle(2,3)\rangle$, $x = (1,0)$ e $y = (0,1)$. Como G es abeliano se tiene que $K \lhd G$. Observamos que $O(x) = 6$ porque $n(1,0) = (n\,(\mathrm{m\acute{o}d}\,6), 0)$ para todo $n \in \mathbb{N}$. Como 6 es el menor natural n tal que $n \equiv 0(\,\mathrm{m\acute{o}d}\,6)$, deducimos que $O(x) = 6$. Análogamente vemos que $O(y) = 6$. Mediante un cálculo directo comprobamos que

   $$K = \{(0,0),(2,3),(4,0),(0,3),(2,0),(4,3)\},$$
   $$x + K = \{(1,0),(3,3),(5,0),(1,3),(3,0),(5,3)\}, \qquad y + K = \{(0,1),(2,4),(4,1),(0,4),(2,1),(4,4)\}.$$

   Observamos que $x + K \neq K$, $y + K \neq K$, $2(x + K) = (2,0) + K = K$ y que

   $$2(y + K) = (0,2) + K = \{(0,2),(2,5),(4,2),(0,5),(2,2),(4,5)\}, \qquad 3(y + K) = (0,3) + K = K.$$

   Por consiguiente, concluimos que $O(x + K) = 2 \neq 3 = O(y + K)$.

2. Dado $K \subseteq S_n$ un subgrupo con $\#K$ impar. Entonces $K \subseteq A_n$.

   Solución: Verdadera. Tenemos que $\#K = 2k + 1$ con $k \in \mathbb{Z}$, por el Corolario 1.5.1.a), para todo $\alpha \in K$ tenemos que $O(\alpha) \mid 2k + 1$. Por la Proposición 1.3.6.2, $\alpha^{2k+1} = id$. Luego $\alpha^{2k}\alpha = 1$ y deducimos que $\alpha = \alpha^{-2k} = (\alpha^{-k})^2$. Por consiguiente, tanto si $\beta = \alpha^{-k}$ es una permutación par como si β es impar, β^2 es par. En consecuencia, $\alpha = \beta^2 \in A_n$ y concluimos que $K \subseteq A_n$.

3. Sea $(G,\cdot)$ un grupo abeliano y $a, b \in G$ elementos de orden finito, entonces $O(ab)$ es el $m.c.m(O(a), O(b))$.

   Solución: Falsa. Basta considerar en el grupo $(\mathbb{Z}/12\mathbb{Z},+)$ los elementos $a = 2$ y $b = 4$, tenemos que $O(a) = 6$ y $O(b) = 3$. Observamos que $m.c.m(O(a), O(b)) = 6$ pero tenemos que $a + b = 6$ y $O(a + b) = O(6) = 2$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = S_4$ y $H = D_4 \times \mathbb{Z}/3\mathbb{Z}$.

Solución: Lema Auxiliar. Dados dos grupos finitos A, B, y dos elementos $a \in A$, $b \in B$, se tiene que el orden de (a,b) como elemento del grupo producto $A \times B$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a,b)) = m.c.m.\{O(a), O(b)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b)\}$, por la definición del grupo producto tenemos que $(a,b)^m = (a^m, b^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$ y $b^m = 1_B$, luego $(a,b)^m = 1_{A\times B}$ y, de nuevo la Proposición 1.3.6.2, $O((a,b)) \mid m$. Por otra parte, si $O((a,b)) = t$ como $(a,b)^t = 1_{A\times B}$ se tiene que $a^t = 1_A$ y $b^t = 1_B$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$ y $O(b) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Determinar todos los homomorfismos de grupos de $f : \mathbb{Z}/3\mathbb{Z} \to G$.

   Solución: Por la Proposición 1.6.2, como $\mathbb{Z}/3\mathbb{Z} = \langle 1\rangle$ es cíclico f queda completamente determinado por $f(1)$. Además por la Proposición 1.6.2. sabemos que $O(f(1)) \mid 3$ y que para cada $b \in G$ con $O(b) \mid 3$ existe un único homomorfismo $f_b : \mathbb{Z}/3\mathbb{Z} \to G$ tal que $f(1) = b$. Por consiguiente determinar los homomorfismos equivale a determinar los elementos $b \in G$ con $O(b) \in \{1, 3\}$.
   Observamos que $O(b) = 1$ si y sólo si $b = 1_G$. Empleando la descomposición en ciclos disjuntos de los elementos de S_4 (**Cor. 1.4.1.**), vemos que los elementos de orden 3 de S_4 son necesariamente ciclos de longitud 3. Por consiguiente, hay 9 homomorfismos de grupos $\mathbb{Z}/3\mathbb{Z}$ en G determinados por $f_1(1) = id$, $f_2(1) = (123)$, $f_3(1) = (132)$, $f_4(1) = (124)$, $f_5(1) = (142)$, $f_6(1) = (134)$, $f_7(1) = (143)$, $f_8(1) = (234)$ y $f_9(1) = (243)$.

2. Determinar si G y H son o no son grupos isomorfos.

Solución: Observamos que $\#G = \#H = 24$, por tanto, no podemos emplear el cardinal para determinar si son isomorfos o no. Por tanto, con la notación del **E156**, si consideramos el elemento $x = ((1234), 1)$ de H por el Lema Auxiliar $O(x) = 12$. Por otro lado, empleando la descomposición en ciclos disjuntos (**Cor. 1.4.1.**), comprobamos que los posibles órdenes de los elementos de $G = S_4$ son $\{1, 2, 3, 4\}$. Deducimos ni de orden 49 de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, H y G no son isomorfos porque en H hay un elemento de orden 12 y en G no.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un D.I.P., entonces R/I es D.I.P.

   Solución: Falso. Basta considerar $(R, +, \cdot) = (\mathbb{Z}, +, \cdot)$ e $I = 6\mathbb{Z}$. El anillo cociente R/I es $(\mathbb{Z}/6\mathbb{Z}, +, \cdot)$ que no es un dominio porque 6 no es primo (**Ejemplo II.4.8**). En consecuencia R/I no es un dominio de ideales principales (D.I.P.).

2. Si R es un dominio, entonces $\#R \neq 21$.

   Solución: Cierto. Razonamos por reducción al absurdo y suponemos que $\#R = 21$. Como R es un dominio, por (D.II) es un anillo unitario. Por el **Teorema II.3.18**, se tiene que $\text{car}(R) = O(1_R)$. Por el **Teorema de Lagrange**, $O(1_R) \mid \#R = 21$, luego $O(1_R)$ es $1, 3, 7$ o 21. Por el **Corolario II.4.9**, tenemos que $\text{car}(R) = p$ con p primo. Por tanto, tenemos dos opciones:
   (A) $\text{car}(R) = O(1_R) = 7$. Por la definición de característica, $7x = 0$ para todo $x \in R$, luego $O(x) \mid 7$ para todo $x \in R$. Por el **Teorema de Cauchy para grupos Abelianos**, como $3 \mid \#R$, existe un elemento $r \in R$ con $O(r) = 3$, contradiciendo que $O(r) \mid 7$.
   (B) $\text{car}(R) = O(1_R) = 3$, razonando como en el caso (A) llegamos a contradicción.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Recordamos que el anillo $\mathbb{C}[x, y]$ se define como $\mathbb{C}[x]([y])$

1. Probar que $x^2 + y^2 - 4$ es un elemento irreducible de $\mathbb{C}[x, y]$.

   Solución: Sabemos que $\mathbb{C}[x, y] = (\mathbb{C}[x])([y])$ como $\mathbb{C}$ es un cuerpo $\mathbb{C}[x]$ es un D.E. y por los **Teoremas II.5.27** y **II.5.22** $\mathbb{C}[x]$ es un D.F.U. Observamos que podemos escribir $P(x, y) = x^2 + y^2 - 4 = a_2(x)y^2 + a_1(x)y + a_0(x)$ con $a_2(x) = 1$, $a_1(x)$ y $a_0(x) = x^2 - 4 = (x + 2)(x - 2)$ que es un polinomio primitivo de $(\mathbb{C}[x])([y])$. Por el **Ejercicio A.43**, tenemos que $x - 2$ es un elemento irreducible de $\mathbb{C}[x]$. Aplicando el **Criterio de Eisenstein (Ejercicio A.66)** a $P(x, y)$ para $p = x - 2$ deducimos que $x^2 + y^2 - 4$ es un elemento irreducible de $\mathbb{C}[x, y]$.

2. Probar que $\mathbb{C}[x, y]/(x^2 + y^2 - 4)$ es un dominio.

   Solución: En el apartado anterior hemos visto que $\mathbb{C}[x]$ es un D.F.U., por el **Problema A.60**, $\mathbb{C}[x, y]$ es un D.F.U.. Por el apartado anterior sabemos que $P(x, y)$ es irreducible, luego por la **Proposición II.5.10**, $P(x, y)$ es primo. Por la **Proposición II.5.6**, $(P(x, y))$ es un ideal primo. Por el **Proposición II.4.14**, $\mathbb{C}[x, y]/(x^2 + y^2 - 4)$ es un dominio.

3. Si $I = (x^2 + y^2 - 4)$, probar que $(x + iy) + I \in U(\mathbb{C}[x, y]/I)$.

   Solución: Basta observar que, por la definición de la suma y el producto en $\mathbb{C}[x, y]/I$ y como $4 + I = x^2 + y^2 + I$, tenemos que $((x + iy) + I)((1/4)(x - iy) + I) = (1/4)(x^2 + y^2) + I = 1 + I$.

UNIVERSIDAD DE CANTABRIA

EXAMEN FINAL
miércoles 3 de junio de 2020
CONVOCATORIA ORDINARIA

G90 - Estructuras Algebraicas
Curso 2019-2020

INSTRUCCIONES SOBRE EL EXAMEN FINAL

REALIZACIÓN DEL EXAMEN

- Las respuestas a las preguntas del examen deben escribirse con bolígrafo azul o negro en folio blanco.
- Esta terminantemente prohibido emplear lápiz, bolígrafos de otros colores y/o elementos de escritura electrónica.
- Las respuestas a las distintas preguntas del examen deben escribirse en hojas separadas.
- Solamente se pueden emplear los resultados demostrados en clase para responder a las preguntas y estos resultados se deben referenciar de forma adecuada.

DOCUMENTO PDF DEL EXAMEN

- Tras finalizar el examen se deben escanear o fotografiar los folios completos con las respuestas.
- Las imágenes de los folios del examen se deben integrar en un **único archivo .pdf**.
- El archivo PDF se debe renombrar siguiendo el siguiente formato: **APELLIDOSNOMBRE_EXAMENFINAL.pdf**

ENTREGA DEL EXAMEN

- El examen debe enviarse a la dirección de correo electrónico: jimenezjj@unican.es
- El envío debe realizarse desde la cuenta de correo oficial de la Universidad de Cantabria.
- El envío debe realizarse antes de las 12:45 del miércoles 3 de junio.

El incumplimiento de estas instrucciones supondrá automáticamente la calificación de Suspenso "0".

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.
2. Sea $(G, \cdot)$ un grupo si $x, y, z \in G$ entonces $O(xyz) = O(zyx)$.
3. Sea $(G, \cdot)$ un grupo $K \lhd G$ un subgrupo. Si $Z(G) = \{z \in G\,;\, zx = xz \text{ para todo } x \in G\}$, entonces $K \subseteq Z(G)$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ y $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times D_7$.

1. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.
2. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R, +, \cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio y todo ideal de R distinto de R es primo, entonces R es un cuerpo.
2. Si R es un D.I.P., entonces cada ideal del anillo cociente R/I es principal.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Consideramos el dominio $\mathbb{Z}[\sqrt{15}] = \{a + b\sqrt{15}\,;\, a, b \in \mathbb{Z}\}$.

1. Probar que $7 + 2\sqrt{15}$ es irreducible en $\mathbb{Z}[\sqrt{15}]$.
2. Demuestra que $4 + \sqrt{15}$ es una unidad en $\mathbb{Z}[\sqrt{15}]$ y dar 6 divisores diferentes de 1 en $\mathbb{Z}[\sqrt{15}]$.
3. Probar que $\mathbb{Z}[\sqrt{15}]$ y que $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3}\,;\, a, b \in \mathbb{Z}\}$ no son anillos isomorfos.

Esquema de una solución de la versión S del examen.

C1 **[2.4 puntos=0.8+0.8+0.8 puntos]** Determinar razonadamente si las siguientes afirmaciones son verdaderas o falsas. Las afirmaciones son independientes unas de otras.

1. Si $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 9 & 6 & 4 & 2 & 1 & 5 \end{pmatrix}$ entonces $\alpha^3 \in A_9$.

   Solución: Falsa. Escribimos α como el producto de ciclos disjuntos $\alpha = (1\,8)(2\,7)(4\,9\,5\,6)$. Por la Proposición 1.4.1, sabemos las permutaciones disjuntas conmutan y se tiene que

   $$\alpha^3 = (1\,8)^3(2\,7)^3(4\,9\,5\,6)^3 = (1\,8)(2\,7)(4\,6\,5\,9).$$

   Finalmente, observamos que $(4\,6\,5\,9) = (4\,9)(4\,5)(4\,6)$. En consecuencia, α^3 descompone como producto de 5 transposiciones y concluimos que es impar y, por tanto, $\alpha^3 \notin A_9$.

2. Sea $(G, \cdot)$ un grupo si $x, y, z \in G$ entonces $O(xyz) = O(zyx)$.

   Solución: Falsa. Basta considerar $G = Q_8$ (ver **E64**) y tomar $x = i$, $y = j$ y $z = k$ tenemos que $xyz = ijk = kk = -1$ luego $O(xyz) = 2$ pero $zyx = kji = k(-k) = 1$ luego $O(zyx) = 1$.

3. Sea $(G, \cdot)$ un grupo $K \lhd G$ un subgrupo. Si $Z(G) = \{z \in G\,;\, zx = xz \text{ para todo } x \in G\}$, entonces $K \subseteq Z(G)$.

   Solución: Falsa. Con la notación del **E156**, basta considerar $G = D_4$, $K = \langle a \rangle$. Sabemos que $\#K = 4$ y que $\#D_4 = 8$. Por el Teorema de Lagrange, se tiene que $\#(D_4 : K) = 2$ y, por **E167**, concluimos que $K \lhd D_4$. Comprobamos empleando las propiedades del **E156** que $Z(D_4) = \langle a^2 \rangle = \{1, a^2\}$, luego $K \nsubseteq Z(D_4)$.

P1 **[2.6 puntos=1.3+1.3 puntos]** Consideramos los grupos $G = \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ y $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times D_7$.

Solución: Lema Auxiliar. Dados tres grupos finitos A, B, C, y tres elementos $a \in A$, $b \in B$,$c \in C$ se tiene que el orden de (a, b, c) como elemento del grupo producto $A \times B \times C$ es el m.c.m. de los órdenes de cada elemento en su grupo, es decir, $O((a, b, c)) = m.c.m.\{O(a), O(b), O(c)\}$.

*Demostración del Lema Auxiliar (Análoga a la prueba del **E80**).* Si $m = m.c.m.\{O(a), O(b), O(c)\}$, por la definición del grupo producto tenemos que $(a, b, c)^m = (a^m, b^m, c^m)$. Por la Proposición 1.3.6.2, $a^m = 1_A$, $b^m = 1_B$ y $c^m = 1_C$, luego $(a, b, c)^m = 1_{A\times B\times C}$ y, de nuevo la Proposición 1.3.6.2, $O((a, b, c)) \mid m$. Por otra parte, si $O((a, b, c)) = t$ como $(a, b, c)^t = 1_{A\times B\times C}$ se tiene que $a^t = 1_A$, $b^t = 1_B$ y $c^t = 1_C$. En consecuencia, por Proposición 1.3.6.2, $O(a) \mid t$, $O(b) \mid t$ y $O(c) \mid t$, luego $m \mid t$ y concluimos que $t = m$. □

1. Construir, si es posible, un endomorfismo $f : G \to G$ tal que $\mathrm{Ker} f \approx \mathrm{Im} f$.

   Solución: Consideramos $f : G \to G$ dado por $f(a, b) = (0, b)$. Comprobamos de forma directa que f es un endomorfismo (proyección), que $\mathrm{Ker} f = \mathbb{Z}/14\mathbb{Z} \times \{0\}$ y que $\mathrm{Im} f = \{0\} \times \mathbb{Z}/14\mathbb{Z}$. Demostramos que $\mathrm{Ker} f \approx \mathrm{Im} f \approx \mathbb{Z}/14\mathbb{Z}$, para probar esto se puede ver que ambos grupos son cíclicos de orden 15 y concluir usando la Proposición 1.6.3.

2. Determinar razonadamente si existe K con $\#K = \#G$ de modo que $K \not\approx H$ y $K \not\approx G$.

   Solución: Observamos que $\#G = \#H = 196$. Buscamos K con $\#K = 196$ de modo que $K \not\approx H$ y $K \not\approx G$. Consideramos $K := \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, cumple que $\#K = 196$. Por el Teorema 1.3.1, sabemos que el orden de los elementos de $\mathbb{Z}/2\mathbb{Z}$ es 1 o 2, el orden de los elementos de $\mathbb{Z}/4\mathbb{Z}$ es 1, 2 o 4, el orden de los elementos de $\mathbb{Z}/7\mathbb{Z}$ es 1 o 7, el orden de los elementos de $\mathbb{Z}/14\mathbb{Z}$ es 1, 2, 7 o 14. Por otro lado, por el **E156**, comprobamos que los posibles órdenes de los elementos de D_7 son $\{1, 2, 7\}$. Empleando el Lema Auxiliar vemos que:

   - en K hay elementos de orden 4.
   - en $\mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \approx G$ no hay ningún elemento de orden 4.
   - en H no hay ningún elemento de orden 4.

   Deducimos de la Proposición 1.6.2.a) que el orden de un elemento es invariante por isomorfismo. Por consiguiente, G y K no son isomorfos y H y K tampoco son isomorfos.

C2 **[2.6 puntos=1.3+1.3 puntos]** Sea $(R,+,\cdot)$ un anillo e $I \subseteq R$ un ideal. Decidir si los enunciados siguientes son ciertos o falsos. En caso de ser ciertos realizar la demostración y en caso de ser falsos ilustrarlo con un contraejemplo. Los enunciados son independientes.

1. Si R es un dominio y todo ideal de R distinto de R es primo, entonces R es un cuerpo.

   Solución: Cierto. Como R es dominio se satisfacen (F.I) y (F.II) basta comprobar que se satisface (F.III), es decir, que $U(R) = R\backslash\{0_R\}$. Como R es un dominio por (D.III), se tiene que $U(R) \subseteq R\backslash\{0_R\}$. Veamos ahora que se cumple la contención contraria. Dado $x \in R\backslash\{0_R\}$ consideremos el ideal $J_1 = (x)$.
   Si $J_1 \subsetneq R$, consideramos el ideal $J_2 = (x^2)$. Como $x^2 \in J_1$ y $J_1 \subsetneq R$, se tiene que $J_2 \subseteq J_1 \subsetneq R$. Por hipótesis, J_2 es primo. Como $x \cdot x = x^2 \in J_2$, tenemos que $x \in J_2$. Por consiguiente, existe $r \in R$ tal que $x = rx^2$ y por la Ley de Cancelación, **Teorema.II.4.6**, $1_R = rx$. Por tanto, $1_R \in J_1$ y tenemos que $J_1 = R$ contradiciendo nuestra suposición.
   Si $J_1 = R$, entonces $1_R \in (x)$, luego existe $u \in R$ tal que $1_R = ux$, es decir, $x \in U(R)$ y concluimos que R es un cuerpo.

2. Si R es un D.I.P., entonces cada ideal del anillo cociente R/I es principal.

   Solución: Cierto. Consideramos el homomorfismo de anillos sobreyectivo $p : R \to R/I$ de paso al cociente dado por $p(a) = a + I$. Dado L un ideal de R/I, por la **Proposición II.3.4.(vi)**, sabemos que $p^{-1}(L)$ es un ideal de R. Como R es un D.I.P., existe $x \in R$ tal que $\big(x\big) = p^{-1}(L)$.
   Veamos que $L = \big(p(x)\big)$. Como $x \in \big(x\big) = p^{-1}(L)$, se tiene que $p(x) \in L$ luego $\big(p(x)\big) \subseteq L$. Recíprocamente, dado $\ell \in L$ como p es sobreyectiva, existe $y \in R$ tal que $p(y) = \ell$. Por consiguiente, $y \in \big(x\big) = p^{-1}(L)$. Como R es un dominio, $\big(x\big) = \{rx; r \in R\}$, es decir, $y = rx$ para algún $r \in R$. Como p es homomorfismo de anillos, $\ell = p(y) = p(r)p(x)$. Deducimos que $\ell \in \big(p(x)\big)$ y concluimos que $L \subseteq \big(p(x)\big)$. En resumen hemos probado que cada ideal L del anillo cociente R/I está generado por un único elemento, es decir, es principal.

P2 **[2.4 puntos=0.8+0.8+0.8 puntos]** Consideramos el dominio $\mathbb{Z}[\sqrt{15}] = \{a + b\sqrt{15}\,;\, a, b \in \mathbb{Z}\}$.

1. Probar que $7 + 2\sqrt{15}$ es irreducible en $\mathbb{Z}[\sqrt{15}]$.

   Solución: Emplearemos las propiedades de la función $N(a + b\sqrt{15}) = a^2 - b^2 15$ del **E460**. Se tiene que $N(7 + 2\sqrt{15}) = -11$. Como -11 es primo en $\mathbb{Z}$, por la propiedad (IV), $7 + 2\sqrt{15}$ es irreducible en $\mathbb{Z}[\sqrt{15}]$.

2. Demuestra que $4 + \sqrt{15}$ es una unidad en $\mathbb{Z}[\sqrt{15}]$ y dar 6 divisores diferentes de 1 en $\mathbb{Z}[\sqrt{15}]$.

   Solución: Con la notación del primer apartado $N(4 + \sqrt{15}) = 16 - 15 = 1$ y, por el **E460**, $u = 4 + \sqrt{15}$ es una unidad en $\mathbb{Z}[\sqrt{15}]$. Observamos que u^n para $n \in \mathbb{N}$ es una unidad porque $N(u^n) = (N(u))^n = 1$. Comprobamos que $u^2 = 31 + 8\sqrt{15}$ y que $u^3 = 244 + 63\sqrt{15}$ y tenemos seis divisores diferentes de 1 en $\mathbb{Z}[\sqrt{15}]$: u, $u^{-1} = 4 - \sqrt{15}$, u^2, $u^{-2} = 31 - 8\sqrt{15}$, u^3 y $u^{-3} = 244 - 63\sqrt{15}$.

3. Probar que $\mathbb{Z}[\sqrt{15}]$ y que $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3}\,;\, a, b \in \mathbb{Z}\}$ no son anillos isomorfos.

   Solución: Razonamos por reducción al absurdo y suponemos que existe $\psi : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}[\sqrt{15}]$ un isomorfismo de anillos. Como ψ es un isomorfismo podemos probar que $\psi(1) = 1$. En consecuencia, por (HA.I), $\psi(3) = \psi(1 + 1 + 1) = \psi(1) + \psi(1) + \psi(1) = 3$. Por otro lado, por (HA.II), $\psi(3) = \psi(\sqrt{3}\sqrt{3}) = (\psi(\sqrt{3}))^2$. En resumen, deberían existir $a, b \in \mathbb{Z}$ tales que $(a + b\sqrt{15})^2 = (\psi(\sqrt{3}))^2 = \psi(3) = 3$. Reescribiendo, esta igualdad existirían $a, b \in \mathbb{Z}$ tales que $a^2 + b^2 15 + 2ab\sqrt{15} = 3$. Igualando términos, tenemos dos opciones o $a = 0$ y $b^2 5 = 1$ (imposible) o $b = 0$ y $a^2 = 3$ (imposible) porque $a, b \in \mathbb{Z}$.

UNIVERSIDAD DE CANTABRIA

EXAMEN FINAL
Convocatoria ordinaria
miércoles 16 de junio de 2021

G90 - Estructuras Algebraicas

Curso 2020-2021

Nombre y apellidos:

INSTRUCCIONES DE LA PRUEBA

- Las respuestas a las preguntas de la prueba deben escribirse con bolígrafo azul o negro.
- Está prohibido emplear lápiz, bolígrafos de otros colores y típex.
- No se permite el uso de calculadora ni de ningún otro dispositivo electrónico.
- No se permite el uso de apuntes, de libros ni de ningún otro tipo de material bibliográfico.
- No se puede abandonar el aula antes de que haya transcurrido media hora desde el inicio de la prueba.
- Todas las respuestas deben estar justificadas correctamente.

1. [2.4 puntos=2x1.2]

(a) **Define:** Homomorfismo de grupos (0.2p).
Sean G y H dos grupos y $f : G \to H$ un homomorfismo de grupos.
Demostrar que $G/\mathrm{Ker} f \approx \mathrm{Im} f$ (1p).

(b) Sea $(D,+,\cdot)$ un dominio.
Define: Elemento irreducible en D (0.2p), Elemento primo en D (0.2p).
Dado $p \in D$ primo **demostrar** que p es irreducible (0.8p).

2. [3 puntos=6x0.5] Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(a) Sea $n \geq 3$. Si $\sigma \in S_n$ con $O(\sigma)$ impar, entonces $\sigma \in A_n$.
Verdadero. *Prueba de la veracidad:*
Si $\sigma = \mathrm{Id}$, entonces $\sigma \in A_n$ porque A_n es subgrupo de S_n.
Si $\sigma \neq \mathrm{Id}$, entonces $\sigma = \tau_1\tau_2\cdots\tau_s$ con τ_i ciclo de longitud ℓ_i para cada $i \in \{1,2,\ldots,s\}$ y τ_i y τ_j disjuntos si $i \neq j$ (T.I.4.12).
Además sabemos que $O(\sigma) = \text{m.c.m.}(\ell_1,\ell_2,\ldots,\ell_s)$, ver (C.I.4.15).
Como $O(\sigma)$ es impar, tenemos que ℓ_i **es impar para todo** $i \in \{1,2,\ldots,s\}$**.**
Por otro lado todo ciclo de longitud ℓ descompone como producto de $\ell - 1$ transposiciones:

$$(i_1,i_2,\ldots,i_\ell) = (i_1,i_\ell)(i_1,i_{\ell-1})\cdots(i_1,i_3)(i_1,i_2).$$

Por tanto, cada τ_i es par por ser ℓ_i impar y concluimos que σ es par por ser producto de permutaciones pares.

(b) Sean $(G,\cdot)$ un grupo y $g,h \in G$. Si $O(g) < \infty$ y $O(h) < \infty$, entonces $O(gh) < \infty$.
Falso. *Contraejemplo 1:* Se pueden considerar en el grupo de isometrías afines en un espacio euclídeo afín real de dimensión 3 con la composición. Dos simetrías con respecto a planos paralelos no coincidentes g y h tienen orden 2, mientras que su composición gh es una traslación en la dirección ortogonal a los planos que tiene orden infinito (E.I.3.24).
Contraejemplo 2: En el grupo lineal especial $G = \mathrm{SL}(2,\mathbb{R})$ formado por las matrices 2×2 reales con determinante 1 con la operación del producto de matrices. Tomamos

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{y} \qquad h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Comprobamos que $O(g)=4$, $O(h)=3$ porque

$$g^2=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} \qquad g^3=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \qquad g^4=\mathrm{Id}$$

$$h^2=\begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix} \qquad h^3=\mathrm{Id}.$$

Luego $O(g)<\infty$ y $O(h)<\infty$ mientras que $O(gh)$ es infinito porque

$$(gh)=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \qquad \text{por inducción se prueba que} \qquad (gh)^n=\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix} \qquad \forall\, n\in\mathbb{N}.$$

(Cuestionarios V/F Moodle)

(c) Dados tres grupos G,H,K con $\#G=\#H=\#K=74$, tenemos que al menos una de las tres afirmaciones siguientes es cierta:

$$(1)\ G\times G\approx H\times H \qquad (2)\ G\times G\approx K\times K \qquad (3)\ H\times H\approx K\times K.$$

Verdadero. *Prueba de la veracidad:*
Como $74=2\cdot 37$ y $p=37>2$ es primo tenemos que para cada uno de los grupos G,H,K se cumple que (T.I.6.28):

O bien G es isomorfo a D_{37} o bien G es isomorfo a C_{74}
O bien H es isomorfo a D_{37} o bien H es isomorfo a C_{74}
O bien K es isomorfo a D_{37} o bien K es isomorfo a C_{74}

En consecuencia, dos de ellos son isomorfos a o bien D_{37} o bien a C_{74}, luego deben ser isomorfos entre sí porque si $A\approx C$ y $B\approx C$, entonces $A\approx B$.
Supongamos, sin pérdida de generalidad, que $G\approx H$, luego existe $\Phi: G\to H$ un isomorfismo. Comprobamos que $f: G\times G\to H\times H$ dado por $f(g_1,g_2)=(\Phi(g_1),\Phi(g_2))$ es también un isomorfismo.

(d) El anillo $\mathbb{Z}\times\mathbb{Z}$ con la suma y el producto componente a componente y el anillo de los enteros de Gauss $\mathbb{Z}[i]$ con la suma y el producto heredados de $\mathbb{C}$ son anillos isomorfos.
Falso. *Prueba de la falsedad:*
Razonamos por reducción al absurdo y supongamos que existe $\Phi:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}[i]$ un isomorfismo de anillos. Observamos que $(1,0)\cdot(0,1)=(0,0)$ en $\mathbb{Z}\times\mathbb{Z}$, luego

$$0 \overset{\Phi\ hom.grupos}{=} \Phi(0,0)=\Phi\left((1,0)\cdot(0,1)\right) \overset{\text{(HA.II)}}{=} \Phi(1,0)\cdot\Phi(0,1).$$

Como el producto en $\mathbb{Z}[i]$ es el producto heredado de $\mathbb{C}$ y en $\mathbb{C}$ no hay divisores de cero porque es cuerpo, tenemos que $\Phi(1,0)=0$ o $\Phi(0,1)=0$, lo que es imposible porque Φ es biyectiva.

(e) Consideramos el ideal $I=(2x^5+9x^3+12x^2+6)$ de $\mathbb{Q}[x]$, entonces $\mathbb{Q}[x]/I$ es un cuerpo y dados los polinomios $P_1(x)=x^3+6$ y $P_2(x)=\frac{1}{24}(x^2+\frac{9}{2})$ de $\mathbb{Q}[x]$ se tiene que el inverso de $P_1(x)+I$ en $\mathbb{Q}[x]/I$ es $P_2(x)+I$.
Verdadero. *Prueba de la veracidad:*
Consideramos el polinomio $Q(x)=2x^5+9x^3+12x^2+6$ como un máximo común divisor de sus coeficientes es 1 es primitivo.
Por tanto, $Q(x)$ es irreducible en $\mathbb{Q}[x]$ si y solo si es irreducible en $\mathbb{Z}[x]$. (C.II.6.56)
Aplicando el Criterio de Eisenstein para $p=3$, como $p\mid 9$, $p\mid 12$, $p\mid 6$ y $p\nmid 2$ y $p^2\nmid 6$, concluimos que $Q(x)$ es irreducible en $\mathbb{Z}[x]$.
Como $\mathbb{Q}$ es cuerpo y $Q(x)$ es irreducible, tenemos que $\mathbb{Q}[x]/I$ es un cuerpo (T.II.6.44).

Finalmente, observamos que

$$(P_1(x)+I)(P_2(x)+I) = P_1(x)P_2(x)+I = \frac{1}{24}(x^5+\frac{9}{2}x^3+6x^2+27)+I$$
$$= \frac{1}{48}(2x^5+9x^3+12x^2+54)+I = \frac{1}{48}(Q(x)+48)+I = (\frac{Q(x)}{48}+I)+(1+I) \overset{Q(x)\in I}{=} 1+I$$

En consecuencia, el inverso de $P_1(x)+I$ en $\mathbb{Q}[x]/I$ es $P_2(x)+I$.

(f) Si$(R,+,\cdot)$ es un anillo conmutativo y unitario con $\text{car}(R)=21$, entonces $\#R<\infty$.
Falso. *Contraejemplo:* Tenemos que $(\mathbb{Z}/21\mathbb{Z},+,\cdot)$ es un anillo conmutativo y unitario y que $\text{car}(\mathbb{Z}/21\mathbb{Z}) = O(1) = 21$ en $(\mathbb{Z}/21\mathbb{Z},+)$ (T.II.2.16).
Por tanto, $((\mathbb{Z}/21\mathbb{Z})[x],+,\cdot)$ es un anillo conmutativo y unitario con $\text{car}(\mathbb{Z}/21\mathbb{Z}[x]) = \text{car}(\mathbb{Z}/21\mathbb{Z}) = 21$ (II.6.2-II.6.3-II.6.4-II.6.12) y tenemos que $\#(\mathbb{Z}/21\mathbb{Z}[x]) = \infty$.

---

3. [2.3 puntos=0.7+0.6+1] Se considera $\mathbb{Z}$ como subgrupo de $(\mathbb{Q},+)$.

(a) Probar que $\mathbb{Z} \lhd \mathbb{Q}$ (0.2p).
Demostrar que todo elemento de $(\mathbb{Q}/\mathbb{Z},+)$ tiene orden finito.(0.5p)

(b) Dados $m,n \in \mathbb{N}$, con $m \neq n$, probar que la clase de $1/n$ es distinta de la clase de $1/m$. ¿Es el grupo cociente $\mathbb{Q}/\mathbb{Z}$ un grupo finito? (0.6p)

(c) Probar que todos los elementos de orden $n \in \mathbb{N}$ de $\mathbb{Q}/\mathbb{Z}$ pertenecen a $<1/n+\mathbb{Z}>$ (0.5p).
Determinar cuántos homomorfismos de grupos existen de $\mathbb{Z}/21\mathbb{Z}$ en $\mathbb{Q}/\mathbb{Z}$. (0.5p)

Solución (ver E.I.3.29).

(a) Como $(\mathbb{Q},+)$ es un grupo conmutativo, todo subgrupo suyo es normal (Obs.I.5.20). En particular, tenemos que $\mathbb{Z} \lhd \mathbb{Q}$.
Como $\mathbb{Z} \lhd \mathbb{Q}$ podemos considerar el grupo cociente $(\mathbb{Q}/\mathbb{Z},+)$. Un elemento de $\mathbb{Q}/\mathbb{Z}$ es de la forma $q+\mathbb{Z}$ con $q \in \mathbb{Q}$. Dado $r \in \mathbb{N}$ por la definición de la suma en $\mathbb{Q}/\mathbb{Z}$ se tiene que

$$r(q+\mathbb{Z}) = (q+\mathbb{Z})+\cdots(r \text{ veces})\cdots+(q+\mathbb{Z}) = (rq)+\mathbb{Z}.$$

Podemos suponer que $q = a/b$ con $a \in \mathbb{Z}$ y $b \in \mathbb{N}$. Observamos que

$$b(q+\mathbb{Z}) = (bq)+\mathbb{Z} = a+\mathbb{Z} \overset{a\in\mathbb{Z}}{=} 0+\mathbb{Z} = 0_{\mathbb{Q}/\mathbb{Z}}.$$

Por tanto, $\{r \in \mathbb{N} : r(q+\mathbb{Z}) = 0_{\mathbb{Q}/\mathbb{Z}}\} = \{r \in \mathbb{N} : rq \in \mathbb{Z}\} \neq \emptyset$, y podemos deducir que

$$O(q+\mathbb{Z}) = \text{mín}\{r \in \mathbb{N} : rq \in \mathbb{Z}\} < \infty.$$

En consecuencia, todo elemento de $(\mathbb{Q}/\mathbb{Z},+)$ tiene orden finito.

(b) Dados $m,n \in \mathbb{N}$, tenemos que

$$\frac{1}{n}+\mathbb{Z} = \frac{1}{m}+\mathbb{Z} \quad \Leftrightarrow \quad \frac{1}{n}-\frac{1}{m} \in \mathbb{Z} \quad \Leftrightarrow \quad \frac{m-n}{nm} \in \mathbb{Z}.$$

Por consiguiente, la clase de $1/n$ y la clase de $1/m$ coinciden si y solo si existe $k \in \mathbb{Z}$ tal que $m-n = knm$, luego $m = n(1+km)$ y $n = m(1-kn)$, por ello, $n \mid m$ y $m \mid n$ y, como $m,n \in \mathbb{N}$, concluimos que necesariamente $n = m$.
Por tanto, si $m \neq n$, necesariamente $1/n+\mathbb{Z} \neq 1/m+\mathbb{Z}$.
De forma que, para cada numero natural $n \in \mathbb{N}$ tenemos un elemento distinto $1/n+\mathbb{Z}$ de $\mathbb{Q}/\mathbb{Z}$, luego $\#(\mathbb{Q}/\mathbb{Z}) = \infty$.

(c) Dado un elemento $q+\mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ con $q \in \mathbb{Q}$ y $O(q+\mathbb{Z}) = n \in \mathbb{N}$, veamos que

$$q+\mathbb{Z} \in H_n =< 1/n+\mathbb{Z} > .$$

Por lo escrito en el apartado (a):

$$n = O(q+\mathbb{Z}) = \text{mín}\{r \in \mathbb{N} \,:\, r(q+\mathbb{Z}) = 0_{\mathbb{Q}/\mathbb{Z}}\} = \text{mín}\{r \in \mathbb{N} \,:\, rq \in \mathbb{Z}\}$$

Escribimos $q = a/b$ con $a \in \mathbb{Z}$ y $b \in \mathbb{N}$ y a y b primos entre sí. Tenemos que $rq \in \mathbb{Z}$ si y solo si $b \mid ra$, y como son primos entre sí, se cumple que

$$rq \in \mathbb{Z} \qquad \Leftrightarrow \qquad b \mid r.$$

Por tanto, $n = O(q+\mathbb{Z}) = \text{mín}\{r \in \mathbb{N} \,:\, r \in b\mathbb{Z}\} = b$, luego hemos probado que si $O(q+\mathbb{Z}) = n \in \mathbb{N}$ podemos escribir $q = a/n$ con $a \in \mathbb{Z}$ y a y n primos entre sí. De esta forma, se tiene que

$$q+\mathbb{Z} = \frac{a}{n}+\mathbb{Z} = a(\frac{1}{n}+\mathbb{Z}) \in H_n =< 1/n+\mathbb{Z} > .$$

Dicho de otra manera, todos los elementos de orden $n \in \mathbb{N}$ de $\mathbb{Q}/\mathbb{Z}$ pertenecen al subgrupo $H_n =< 1/n+\mathbb{Z} >$.

Observamos que $O(1/n) = n$, $H_n =< 1/n+\mathbb{Z} >$ es un grupo cíclico de orden $\#H_n = O(1/n) = n$ y para cada divisor $d \mid n$ con $d \in \mathbb{N}$ tenemos que H_n tiene un único subgrupo de orden d que es

$$< (n/d)/n+\mathbb{Z} >=< 1/d+\mathbb{Z} >= H_d \qquad \text{(P.I.3.16)}$$

En otras palabras, si $d \mid n$ tenemos que $H_d \subseteq H_n$ y podemos concluir por doble contención que

$$H_n =< 1/n+\mathbb{Z} >= \{q+\mathbb{Z} \in \mathbb{Q}/\mathbb{Z} : O(q+\mathbb{Z}) \mid n\}.$$

Finalmente, como $(\mathbb{Z}/21\mathbb{Z},+)$ es cíclico de orden 21, $\mathbb{Z}/21\mathbb{Z} =< 1 >$, la imagen de todo homomorfismo está determinado de forma única por la imagen de 1 y hay tantos homorfismos distintos como elementos en $q+\mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ cuyo orden $O(q+\mathbb{Z})$ divida a 21 (P.I.6.12). Como todos estos elementos están en H_{21} tenemos $\#H_{21} = 21$ homomorfismos de grupos distintos de $\mathbb{Z}/21\mathbb{Z}$ en $\mathbb{Q}/\mathbb{Z}$.

---

4. **[2.3 puntos=0.7+0.8+0.8]** Consideramos el dominio

$$\mathbb{Z}[\sqrt{21}] = \{a+b\sqrt{21} \,:\, a,b \in \mathbb{Z}\} \subseteq \mathbb{R}$$

(a) Dada la aplicación $N : \mathbb{Z}[\sqrt{21}] \to \mathbb{Z}$ dada por

$$N(a+b\sqrt{21}) = a^2 - b^2 21.$$

Demostrar que satisface las propiedades:
(I) $N(\alpha) = 0$ si y sólo si $\alpha = 0$. (0.2p)
(II) $N(\alpha\beta) = N(\alpha)N(\beta)$. (0.1p)
(III) $u \in U(\mathbb{Z}[\sqrt{21}])$ si y sólo si $N(u) = \pm 1$. (0.2p)
(IV) Si $N(\alpha)$ es primo en $\mathbb{Z}$, entonces α es irreducible en $\mathbb{Z}[\sqrt{21}]$. (0.2p)

(b) ¿Es $-2+\sqrt{21}$ irreducible y $55+12\sqrt{21}$ una unidad en $\mathbb{Z}[\sqrt{21}]$? (0.3p)
¿Es $\mathbb{Z}[\sqrt{21}]/(17)$ un dominio? (0.5p)

(c) Probar que 2 es irreducible en $\mathbb{Z}[\sqrt{21}]$. (0.3p)
Demostrar que $(1+\sqrt{21}, 2)$ no es principal en $\mathbb{Z}[\sqrt{21}]$. (0.3p)
¿Es $\mathbb{Z}[\sqrt{21}]$ un dominio euclídeo? (0.2p)

Solución.

(a) Escribimos $\alpha = a_1 + a_2\sqrt{21}$, $\beta = b_1 + b_2\sqrt{21}$ con $a_1, a_2, b_1, b_2 \in \mathbb{Z}$.
Observamos que $N(a+b\sqrt{21}) = (a+b\sqrt{21})(a-b\sqrt{21}) = a^2 - b^2 21$.

(I) Por la definición de N, si $\alpha = 0$, tenemos que $N(\alpha) = 0^2 - 0^2 \cdot 21 = 0$.
Por otro lado, si $N(\alpha) = 0$ entonces $a_1^2 = a_2^2 \cdot 21$.
Si $a_2 = 0$, entonces $a_1 = 0$ y hemos terminado.
Si $a_2 \neq 0$, entonces $\sqrt{21} = |a_1|/|a_2|$ y basta ver que $\sqrt{21}$ es irracional para concluir que esta situación es imposible.

Prueba de que $\sqrt{21}$ es irracional: Razonamos por reducción al absurdo. Si $\sqrt{21} = r/s$ con $r, s \in \mathbb{N}$ y r y s primos entre sí. Tenemos que $21s^2 = r^2$, luego $s \mid r^2$. Por la Identidad de Bezout, como r y s primos entre sí, existen $x, y \in \mathbb{Z}$ tales que $xr + ys = 1$, por tanto, multiplicando por r, vemos que

$$xr^2 + ysr = r \qquad \overset{s|r^2}{\Rightarrow} \qquad s \mid r.$$

Como r y s son primos entre sí y $s \mid r$ la única opción es $s = 1$, luego $21 = r^2$ con $r \in \mathbb{Z}$ que es absurdo porque 21 no es un cuadrado.
Nota: Como $\sqrt{21}$ es irracional, tenemos que $a_1 + a_2\sqrt{21} = \beta = b_1 + b_2\sqrt{21}$ con $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ si y solo si $a_1 = b_1$ y $a_2 = b_2$.

(II) Si $\alpha\beta = c_1 + c_2\sqrt{21}$ tenemos que

$$\begin{aligned} N(\alpha)N(\beta) &= (a_1 + a_2\sqrt{21})(a_1 - a_2\sqrt{21})(b_1 + b_2\sqrt{21})(b_1 - b_2\sqrt{21}) \\ &= (a_1 + a_2\sqrt{21})(b_1 + b_2\sqrt{21})(a_1 - a_2\sqrt{21})(b_1 - b_2\sqrt{21}) \\ &= (c_1 + c_2\sqrt{21})(c_1 - c_2\sqrt{21}) = N(\alpha\beta) \end{aligned}$$

(III) Si $u \in U(\mathbb{Z}[\sqrt{21}])$, entonces $u \cdot u^{-1} = 1$ luego $N(uu^{-1}) = N(1) = 1$. Por (II), tenemos que $N(u)N(u^{-1}) = 1$, luego $N(u) \in U(\mathbb{Z}) = \{1, -1\}$.
Recíprocamente, si $N(u) = 1$, escribimos $u = v_1 + v_2\sqrt{21}$ y vemos que por la definición de N, $(v_1 + v_2\sqrt{21})(v_1 - v_2\sqrt{21}) = v_1^2 - v_2^2 21 = N(u) = 1$ Luego u es invertible en $\mathbb{Z}[\sqrt{21}]$ y su inverso es $v_1 - v_2\sqrt{21}$.

(IV) Suponemos que $N(\alpha)$ es primo y que $\alpha = \beta\gamma$ con $\beta, \gamma \in \mathbb{Z}[\sqrt{21}]$. Por (II), $N(\alpha) = N(\beta)N(\gamma)$. Como $N(\alpha)$ es primo en $\mathbb{Z}$ que es dominio deducimos que $N(\alpha)$ es irreducible en $\mathbb{Z}$, luego tenemos que o bien $N(\beta) \in U(\mathbb{Z})$ o bien $N(\gamma) \in U(\mathbb{Z})$, es decir, o bien $N(\beta) = \pm 1$ o bien $N(\gamma) = \pm 1$. Por (III), se tiene que o bien $\beta \in U(\mathbb{Z}[\sqrt{21}])$ o bien $\gamma \in U(\mathbb{Z}[\sqrt{21}])$. Por consiguiente, α es irreducible en $\mathbb{Z}[\sqrt{21}]$.

(b) Como $N(-2+\sqrt{21}) = 4 - 21 = -17$ y -17 es primo en $\mathbb{Z}$ tenemos por (a)(IV) que $-2 + \sqrt{21}$ es irreducible en $\mathbb{Z}[\sqrt{21}]$.
Como

$$\begin{aligned} N(55 + 12\sqrt{21}) &= 55^2 - 12^2 \cdot 21 \overset{\text{operando con cuidado}}{=} 5^2(11)^2 - (11+1)^2 \cdot 21 \\ &= 5^2 11^2 - 11^2 21 - 21 - 22 \cdot 21 \overset{\substack{-21=-22+1 \\ 5^2-21=4}}{=} 11^2 4 - 22 \cdot 22 + 1 = 1 \end{aligned}$$

Nota: es posible desarrollar el producto, pero el tiempo de examen es limitado y es más fácil equivocarse.
Por (a)(III), $55 + 12\sqrt{21}$ es una unidad en $\mathbb{Z}[\sqrt{21}]$ (0.3p)

Observamos que $17 = 21 - 4 = (-2 + \sqrt{21})(2 + \sqrt{21})$, con $N(-2 + \sqrt{21}) = -17$ y con $N(2 + \sqrt{21}) = -17$, luego por (a)(III), ni $-2 + \sqrt{21}$ es una unidad ni $2 + \sqrt{21}$ es una unidad en $\mathbb{Z}[\sqrt{21}]$, luego 17 no es irreducible en $\mathbb{Z}[\sqrt{21}]$. Como $\mathbb{Z}[\sqrt{21}]$ es un dominio, tenemos

que todo elemento primo es irreducible (P.II.5.9), por tanto 17 tampoco es un elemento primo y tenemos que (17) no es un ideal primo (P.II.5.9).
En consecuencia, $\mathbb{Z}[\sqrt{21}]/(17)$ no es un dominio (II.4.15).

(c) Razonamos por reducción al absurdo y suponemos que 2 no es irreducible en $\mathbb{Z}[\sqrt{21}]$. Por tanto, existen $\beta,\gamma\in\mathbb{Z}[\sqrt{21}]$, no unidades, tales que $2=\beta\gamma$. Por (a)(II), se tiene que

$$N(\beta)N(\gamma)=N(\beta\gamma)=N(2)=4.$$

y, por (a)(III), como β y γ no son unidades $N(\beta),N(\gamma)\notin\{1,-1\}$. En consecuencia, $N(\beta)=\pm2$ y $N(\gamma)=\pm2$. Para llegar a una contradicción veremos que no hay ningún elemento $N(\beta)=2$ o $N(\beta)=-2$, es decir, basta ver que las ecuaciones

$$(\star)\quad b_1^2-b_2^2\cdot 21=2 \qquad\qquad b_1^2-b_2^2\cdot 21=-2.$$

no tienen soluciones enteras. Si existieran $b_1,b_2\in\mathbb{Z}$, satisfaciendo alguna de las ecuaciones anteriores, tomando clases módulo 2, tendríamos que

$$b_1^2-b_2^2\equiv 0(\text{ mód }2)\qquad\Rightarrow\qquad (b_1-b_2)(b_1+b_2)\equiv 0(\text{ mód }2).$$

luego o $(b_1-b_2)\equiv 0(\text{ mód }2)$ o $(b_1+b_2)\equiv 0(\text{ mód }2)$. En ambos casos, concluimos que b_1 y b_2 son ambos pares o ambos impares. Si ambos fueran pares tendríamos que $b_1=2k_1$ y $b_2=2k_2$, luego

$$(2k_1)^2-(2k_2)^2\cdot 21=\pm2\qquad\Rightarrow\qquad 2k_1^2-2k_2^2\cdot 21=\pm1,$$

lo que es imposible porque la resta de dos números pares no puede ser impar. Si ambos fueran impares tendríamos que $b_1=2k_1+1$ y $b_2=2k_2+1$, luego

$$(2k_1+1)^2-(2k_2+1)^2\cdot 21=\pm2\quad\Rightarrow\quad 4k_1^2+4k_1+1-(4k_2^2+4k_2+1)\cdot 21=\pm2,$$

Operando vemos que $2(k_1^2+k_1-21k_2^2-21k_2-5)=\pm1$, o que es imposible porque ±1 no es par. En conclusión, las ecuaciones $(\star)$ no tienen soluciones enteras y 2 es irreducible en $\mathbb{Z}[\sqrt{21}]$.

Razonamos por reducción al absurdo y suponemos que el ideal $(1+\sqrt{21},2)$ es principal.
En otras palabras, suponemos que existe $\alpha\in\mathbb{Z}[\sqrt{21}]$ tal que $(1+\sqrt{21},2)=(\alpha)$.
Como $1+\sqrt{21}\in(\alpha)$ tenemos que $\beta\alpha=1+\sqrt{21}$ para algún $\beta\in\mathbb{Z}[\sqrt{21}]$.
De la misma forma, $\gamma\alpha=2$ para algún $\gamma\in\mathbb{Z}[\sqrt{21}]$.
Como 2 es irreducible o bien γ es una unidad o bien α es una unidad en $\mathbb{Z}[\sqrt{21}]$.
Si γ fuera una unidad, tendríamos que $1+\sqrt{21}=\beta\alpha=\beta\gamma^{-1}2$. Como $\beta\in\mathbb{Z}[\sqrt{21}]$ y $\gamma\in U(\mathbb{Z}[\sqrt{21}])$, tenemos que $\beta\gamma^{-1}=m_1+m_2\sqrt{21}\in\mathbb{Z}[\sqrt{21}]$. Sin embargo, esto es imposible porque si $2(m_1+m_2\sqrt{21})=1+\sqrt{21}$, entonces $m_1=m_2=1/2\notin\mathbb{Z}$, luego $\beta\gamma^{-1}\notin\mathbb{Z}[\sqrt{21}]$.
Si α fuera una unidad, entonces $1\in(\alpha)$ y $(\alpha)=\mathbb{Z}[\sqrt{21}]$.
Por consiguiente, como $1\in(1)=(\alpha)=(1+\sqrt{21},2)$ existen $\lambda=\ell_1+\ell_2\sqrt{21},\mu=m_1+\sqrt{21}\in\mathbb{Z}[\sqrt{21}]$ tales que

$$1=\lambda(1+\sqrt{21})+\mu 2\quad\overset{\text{operando e igualando}}{\Rightarrow}\quad\begin{cases}\ell_1+21\ell_2+2m_1=1,\\ \ell_1+\ell_2+2m_2=0.\end{cases}.$$

Por la primera ecuación ℓ_1 y ℓ_2 deben tener distinta paridad y por la segunda ecuación deben tener la misma paridad, llegando de esta forma a una contradicción.
En consecuencia, como ambas situaciones son imposibles, el ideal $(1+\sqrt{21},2)$ de $\mathbb{Z}[\sqrt{21}]$ no es principal.

Como en $\mathbb{Z}[\sqrt{21}]$ hay un ideal que no es principal, $\mathbb{Z}[\sqrt{21}]$ no es D.I.P. (P.II.5.25)
Como todo D.E. es D.I.P. (T.II.5.33), tenemos que $\mathbb{Z}[\sqrt{21}]$ no es D.E.

UNIVERSIDAD DE CANTABRIA

EXAMEN FINAL
Convocatoria extraordinaria
lunes 5 de julio de 2021

G90 - Estructuras Algebraicas
Curso 2020-2021

Nombre y apellidos:

INSTRUCCIONES DE LA PRUEBA

- Las respuestas a las preguntas de la prueba deben escribirse con bolígrafo azul o negro.
- Está prohibido emplear lápiz, bolígrafos de otros colores y típex.
- No se permite el uso de calculadora ni de ningún otro dispositivo electrónico.
- No se permite el uso de apuntes, de libros ni de ningún otro tipo de material bibliográfico.
- No se puede abandonar el aula antes de que haya transcurrido media hora desde el inicio de la prueba.
- Todas las respuestas deben estar justificadas correctamente.

1. **[2.8 puntos=2x1.4]** Demostrar los siguientes resultados:

(a) **Define:** Grupo (0.2p), Orden de un elemento de un grupo (0.2p).
Sea $(G,\cdot)$ un grupo finito y $S \subseteq G$ un subgrupo.
Demostrar que: para todo $a \in G$ se tiene que $\#(aS) = \#S = \#(Sa)$. (0.3p)
Demostrar que: $\#G = \#(G:S)\#S$. (0.5 p)
Demostrar que: para todo $a \in G$ se cumple que $O(a) \mid \#G$. (0.2p)

(b) **Define:** Dominio (0.3p), Cuerpo (0.3p).
Demostrar que: todo dominio finito es un cuerpo (0.8p).

2. **[2.4 puntos=6x0.4]** Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(a) Dado $(G,+)$ un grupo abeliano, H es un subgrupo de G con $H \neq G$ y $g \in G$. Si $O(g+H) = n \in \mathbb{N}$, entonces $n \cdot g = 0_G$.
Falso. Basta considerar $G = \mathbb{Z}$ y $H = 2\mathbb{Z}$, entonces $O(1+2\mathbb{Z}) = 2$ pero $2 \cdot 1 = 2 \neq 0$.

(b) Dado $(G,\cdot)$ un grupo, $g,h \in G$ dos elementos tales que $gh = hg$. Si $O(g) < \infty$, $O(h) < \infty$, entonces $O(gh) \mid \text{m.c.m.}(O(g),O(h))$.
Verdadero. Como g y h conmutan, es decir, $gh = hg$, podemos probar por inducción que

$$(gh)^k = g^k h^k \qquad \forall k \in \mathbb{N}.$$

Como $O(g) < \infty$, $O(h) < \infty$, escribimos $n = O(g)$ y $\ell = O(h)$, y $m = \text{m.c.m.}(n,\ell)$, luego $m = m_1 n$ y $m = m_2 \ell$ con $n,m,\ell,m_1,m_2 \in \mathbb{N}$. En consecuencia, tenemos que

$$(gh)^m = g^m h^m = g^{m_1 n} h^{m_2 \ell} = (g^n)^{m_1} (h^\ell)^{m_2} \overset{\substack{O(g)=n \\ O(h)=\ell}}{=} (1_G)^{m_1} (1_G)^{m_2} = 1_G.$$

En consecuencia, concluimos que $O(gh) \mid \text{m.c.m.}(O(g),O(h))$ (I.3.13)

(c) Sea D un dominio y $a \in D$. Entonces el subgrupo aditivo generado por a y el ideal generado por a coinciden, es decir, y $< a >= (a)$.
Falso. Basta considerar en $D = \mathbb{Z}[x]$, que es un dominio porque $\mathbb{Z}$ es dominio (II.6.23), el polinomio $a = P(x) = 2$. Tenemos que

$$< 2 >= \{2k : k \in \mathbb{Z}\} = \{Q(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x] \ : a_0 \in 2\mathbb{Z} \text{ y } a_j = 0 \text{ si } j \in \mathbb{N}\}.$$

$$(2) = \{2R(x) : R(x) \in \mathbb{Z}[x]\} = \{Q(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x] \ : a_j \in 2\mathbb{Z} \ \forall j \in \mathbb{N}_0\}.$$

En otras palabras, $< 2 >$ es el conjunto de todos los polinomios de grado 0 cuyo único coeficiente no nulo es par y (2) es el conjunto de todos los polinomios, de cualquier grado, de tal forma que todos sus coeficientes son pares, luego $< 2 > \subsetneq (2)$.

(d) $(2\mathbb{Z}, +)$ y $(5\mathbb{Z}, +)$ son grupos isomorfos, pero $(2\mathbb{Z}, +, \cdot)$ y $(5\mathbb{Z}, +, \cdot)$ no son anillos isomorfos.
Verdadero. La aplicación $f : 2\mathbb{Z} \to 5\mathbb{Z}$ dada por $f(2m) = 5m$ para cada $m \in \mathbb{Z}$ es un isomorfismo de grupos porque:
-f es **homomorfismo**: $f(2m + 2\ell) = f(2(m + \ell)) = 5(m + \ell) = 5m + 5\ell = f(2m) + f(2\ell)$ para todos $m, \ell \in \mathbb{Z}$.
-f es **inyectiva**: si $f(2m) = f(2\ell)$, entonces $5m = 5\ell$ y, por la Ley de Cancelación en $\mathbb{Z}$, concluimos que $m = \ell$.
-f es **sobreyectiva**: Dado $k \in 5\mathbb{Z}$ tenemos que $k = 5m$ para algún $m \in \mathbb{Z}$, luego basta observar que $f(2m) = 5m = k$.
Sin embargo, $(2\mathbb{Z}, +, \cdot)$ y $(5\mathbb{Z}, +, \cdot)$ no son anillos isomorfos porque, razonando por reducción al absurdo, si existiera $\Phi : 2\mathbb{Z} \to 5\mathbb{Z}$ un isomorfismo de anillos tendríamos que:

$$\Phi(4) = \Phi(2 + 2) = \Phi(2) + \Phi(2) \qquad \text{y} \qquad \Phi(4) = \Phi(2 \cdot 2) = \Phi(2)\Phi(2).$$

Por lo tanto, tenemos que $2 \cdot \Phi(2) = \Phi(2)\Phi(2)$, operando vemos que $\Phi(2)[2 - \Phi(2)] = 0$, luego como $5\mathbb{Z}$, no hay divisores de cero no nulos porque $5\mathbb{Z} \subseteq \mathbb{Z}$, vemos que $\Phi(2) = 0$ o $\Phi(2) = 2$. El primer caso es imposible porque como Φ es homomorfismo de anillos $\Phi(0) = 0$ y Φ no sería inyectiva, luego Φ no sería isomorfismo. El segundo caso es imposible porque $2 \notin 5\mathbb{Z}$. En conclusión, $(2\mathbb{Z}, +, \cdot)$ y $(5\mathbb{Z}, +, \cdot)$ no son anillos isomorfos

(e) $\mathbb{Q}[x]$ es isomorfo al cuerpo fracciones de $\mathbb{Z}[x]$.
Falso. $\mathbb{Q}[x]$ no es un cuerpo porque el polinomio $P(x) = x$ no tiene inverso para el producto, luego no puede ser isomorfo a ningún cuerpo. (II.4.22)

(f) Dado D un D.F.U. y $J \subseteq D$ un ideal primo en D, entonces J es maximal.
Falso. Basta considerar $D = \mathbb{Z}[x]$, que es un D.F.U. porque $\mathbb{Z}$ es D.F.U. (II.6.57) y el ideal $J = (x)$. En $\mathbb{Z}[x]$ el ideal $J = (x)$ es primo porque en un D.F.U. los elementos irreducibles son primos y porque $P(x) = x$ es irreducible porque tiene grado 1 y es primitivo (II.6.50). Sin embargo, J no es maximal porque $J \subsetneq (x, 2) \subsetneq \mathbb{Z}[x]$, la primera inclusión estricta es cierta porque $2 \notin J = (x)$ y la segunda es cierta porque $1 \notin (x, 2)$.

3. **[2.4 puntos=0.4+0.6+0.5+0.9]** Dado $(G,\cdot)$ un grupo, $a \in G$ definimos la aplicación **multiplicación a la izquierda por** a por

$$\begin{array}{rccc} T_a: & G & \to & G \\ & b & \to & ab \end{array}$$

Se pide:

(a) Probar que T_a es una permutación de G, es decir, $T_a \in S(G)$.

(b) Probar que $\mathcal{T} = \{T_a \ : \ a \in G\}$ es un subgrupo de $(S(G),\circ)$.

(c) Probar que $f : G \to \mathcal{T}$ dada por $f(a) = T_a$ es un isomorfismo de grupos.

(d) Encontrar un subgrupo de S_n isomorfo a $(U(\mathbb{Z}[i]),\cdot)$ con $n = \#U(\mathbb{Z}[i])$. (0.2p)
Encontrar un subgrupo de S_m isomorfo a $(U(\mathbb{Z}\times\mathbb{Z}),\cdot)$ con $m = \#U(\mathbb{Z}\times\mathbb{Z})$. (0.2p)
Encontrar un subgrupo de S_k isomorfo a $(U(\mathbb{Z}/10\mathbb{Z}),\cdot)$ con $k = \#U(\mathbb{Z}/10\mathbb{Z})$. (0.2p)
Con la información obtenida determinar si las siguientes afirmaciones son ciertas o no:

(1) $U(\mathbb{Z}[i]) \approx U(\mathbb{Z}\times\mathbb{Z})$ (2) $U(\mathbb{Z}[i]) \approx U(\mathbb{Z}/10\mathbb{Z})$ (3) $U(\mathbb{Z}\times\mathbb{Z}) \approx U(\mathbb{Z}/10\mathbb{Z})$. (0.3p)

(a) Probar que T_a es una permutación de G, es decir, $T_a \in S(G)$.
Solución. Por definición una permutación s de G, es una aplicación $s : G \to G$ biyectiva, luego basta probar que T_a es biyectiva:
-T_a es **inyectiva**: si $T_a(b) = T_a(c)$, entonces $ab = ac$ y, como G es un grupo, existe $a^{-1} \in G$, luego multiplicando por a^{-1} a ambos lados, concluimos que $b = c$.
-T_a es **sobreyectiva**: Dado $g \in G$ tenemos que $T_a(a^{-1}g) = a(a^{-1}g) = g$.
En consecuencia, $T_a \in S(G)$.

(b) Probar que $\mathcal{T} = \{T_a \ : \ a \in G\}$ es un subgrupo de $(S(G),\circ)$.
Solución. Vamos a probar que $\mathcal{T}$ es un subgrupo de $(S(G),\circ)$ empleando la Observación I.2.5. Vemos que:
(I) $1_{S(G)} = \mathrm{Id} \in \mathcal{T}$ porque para todo $b \in G$ se tiene que $T_{1_G}(b) = 1_G b = b = \mathrm{Id}(b)$, luego $\mathrm{Id} = T_{1_G} \in \mathcal{T}$.
(II) Dados $T_{a_1}, T_{a_2} \in \mathcal{T}$, vemos que para todo $b \in G$ se tiene que

$$T_{a_1} \circ T_{a_2}(b) = T_{a_1}(T_{a_2}b) = T_{a_1}(a_2 b) = a_1(a_2 b) = (a_1 a_2)b = T_{a_1 a_2}(b),$$

luego $T_{a_1} \circ T_{a_2} = T_{a_1 a_2} \in \mathcal{T}$.
(III) Dado $T_a \in \mathcal{T}$, veamos que $(T_a)^{-1} = T_{a^{-1}}$. Para todo $b \in G$ se tiene que

$$T_a \circ T_{a^{-1}}(b) \overset{(b.II)}{=} T_{aa^{-1}}(b) = T_{1_G}(b) \overset{(b.I)}{=} \mathrm{Id}(b),$$

$$T_{a^{-1}} \circ T_a(b) \overset{(b.II)}{=} T_{a^{-1}a}(b) = T_{1_G}(b) \overset{(b.I)}{=} \mathrm{Id}(b),$$

luego $T_a \circ T_{a^{-1}} = \mathrm{Id}$ y $T_{a^{-1}} \circ T_a = \mathrm{Id}$, por la unicidad del elemento opuesto $(T_a)^{-1} = T_{a^{-1}}$. Como $(T_a)^{-1} = T_{a^{-1}}$, concluimos que $(T_a)^{-1} \in \mathcal{T}$.
En consecuencia, $\mathcal{T} = \{T_a \ : \ a \in G\}$ es un subgrupo de $(S(G),\circ)$.

(c) Probar que $f : G \to \mathcal{T}$ dada por $f(a) = T_a$ es un isomorfismo de grupos.
Solución. Veamos que f es un homomorfismo de grupos biyectivo:
-f es **homomorfismo**: $f(a_1 a_2) = T_{a_1 a_2} \overset{(b.II)}{=} T_{a_1} \circ T_{a_2} = f(a_1) \circ f(a_2)$ para todos $a_1, a_2 \in G$.
-f es **inyectiva**: si $f(a_1) = \mathrm{Id}$, entonces $T_a = \mathrm{Id}$, luego $T_a(1_G) = \mathrm{Id}(1_G)$, luego $a1_G = 1_G$, y en consecuencia $a = 1_G$. Por tanto, $\mathrm{Ker} f = \{1_G\}$ y f es inyectiva.
-f es **sobreyectiva**: dado $T_a \in \mathcal{T}$ basta observar que $f(a) = T_a$.

(d) Encontrar un subgrupo de S_n isomorfo a $(U(\mathbb{Z}[i]),\cdot)$ con $n = \#U(\mathbb{Z}[i])$. (0.2p)
Encontrar un subgrupo de S_m isomorfo a $(U(\mathbb{Z}\times\mathbb{Z}),\cdot)$ con $m = \#U(\mathbb{Z}\times\mathbb{Z})$. (0.2p)
Encontrar un subgrupo de S_k isomorfo a $(U(\mathbb{Z}/10\mathbb{Z}),\cdot)$ con $k = \#U(\mathbb{Z}/10\mathbb{Z})$. (0.2p)
Con la información obtenida determinar si las siguientes afirmaciones son ciertas o no:

(1) $U(\mathbb{Z}[i]) \approx U(\mathbb{Z}\times\mathbb{Z})$ (2) $U(\mathbb{Z}[i]) \approx U(\mathbb{Z}/10\mathbb{Z})$ (3) $U(\mathbb{Z}\times\mathbb{Z}) \approx U(\mathbb{Z}/10\mathbb{Z})$. (0.3p)

Solución. Calculamos $U(\mathbb{Z}[i])$ empleando la aplicación $N(a+bi) = a^2+b^2$. Sabemos que $u \in U(Z[i])$ si y solo si $N(u) = 1$. Luego $u = a+bi \in U(Z[i])$ si y solo si $N(a+bi) = a^2+b^2 = 1$, las únicas soluciones enteras de esta ecuación son $a = \pm 1$ y $b = 0$, $a = 0$ y $b = \pm 1$. En consecuencia, $U(\mathbb{Z}[i]) = \{1, i, -1, -i\}$, luego $n = 4$ y empleando los apartados anteriores vemos que:

$T_1 : U(\mathbb{Z}[i])$	$\to U(\mathbb{Z}[i])$	$T_i :$	$U(\mathbb{Z}[i]) \to U(\mathbb{Z}[i])$	$T_{-1} :$	$U(\mathbb{Z}[i]) \to U(\mathbb{Z}[i])$	$T_{-i} :$	$U(\mathbb{Z}[i]) \to U(\mathbb{Z}[i])$
1	$\to 1$		$1 \to i$		$1 \to -1$		$1 \to -i$
i	$\to i$		$i \to -1$		$i \to -i$		$i \to 1$
-1	$\to -1$		$-1 \to -i$		$-1 \to 1$		$-1 \to i$
$-i$	$\to -i$		$-i \to 1$		$-i \to i$		$-i \to -1$

demos establecer el siguiente isomorfismo de $\mathcal{T} = \{T_1, T_i, T_{-1}, T_{-i}\}$ en un subgrupo de S_4 de forma natural:

$$T_1 \to \mathrm{Id} \qquad T_i \to (1,2,3,4) \qquad T_{-1} \to (1,3)(2,4) \qquad T_i \to (1,4,3,2).$$

Como $U(\mathbb{Z}[i]) \approx \mathcal{T}$ por (c) y como $\mathcal{T} \approx < (1,2,3,4) >$ concluimos que $U(\mathbb{Z}[i]) \approx < (1,2,3,4) >$.

Calculamos $U(\mathbb{Z}\times\mathbb{Z})$ empleando el Ejercicio II.1.30 sabemos que $U(\mathbb{Z}\times\mathbb{Z}) = U(\mathbb{Z})\times U(\mathbb{Z})$. Como $U(\mathbb{Z}) = \{1,-1\}$, concluimos que $U(\mathbb{Z}\times\mathbb{Z}) = \{(1,1),(1,-1),(-1,1),(-1,-1)\}$, luego $m = 4$ y empleando los apartados anteriores vemos que:

$T_{(1,1)} : U(\mathbb{Z}\times\mathbb{Z})$	$\to U(\mathbb{Z}\times\mathbb{Z})$	$T_{(1,-1)} :$	$U(\mathbb{Z}\times\mathbb{Z}) \to$	$U(\mathbb{Z}\times\mathbb{Z})$	$T_{(-1,1)} :$	$U(\mathbb{Z}\times\mathbb{Z}) \to$	$U(\mathbb{Z}\times\mathbb{Z})$	$T_{(-1,-1)} :$	$U(\mathbb{Z}\times\mathbb{Z}) \to$	$U(\mathbb{Z}\times\mathbb{Z})$
$(1,1)$	$\to (1,1)$		$(1,1) \to$	$(1,-1)$		$(1,1) \to$	$(-1,1)$		$(1,1) \to$	$(-1,-1)$
$(1,-1)$	$\to (1,-1)$		$(1,-1) \to$	$(1,1)$		$(1,-1) \to$	$(-1,-1)$		$(1,-1) \to$	$(-1,1)$
$(-1,1)$	$\to (-1,1)$		$(-1,1) \to$	$(-1,-1)$		$(-1,1) \to$	$(1,1)$		$(-1,1) \to$	$(1,-1)$
$(-1,-1)$	$\to (-1,-1)$		$(-1,-1) \to$	$(-1,1)$		$(-1,-1) \to$	$(1,-1)$		$(-1,-1) \to$	$(1,1)$

Luego podemos establecer el siguiente isomorfismo de $\mathcal{T} = \{T_{(1,1)}, T_{(1,-1)}, T_{(-1,1)}, T_{(-1,-1)}\}$ en un subgrupo de S_4 de forma natural:

$$T_{(1,1)} \to \mathrm{Id} \qquad T_{(1,-1)} \to (1,2)(3,4) \qquad T_{(-1,1)} \to (1,3)(2,4) \qquad T_{(-1,-1)} \to (1,4)(2,3).$$

Como $U(\mathbb{Z}\times\mathbb{Z}) \approx \mathcal{T}$ por (c) y como $\mathcal{T} \approx \{\mathrm{Id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} = V_4$ concluimos que $U(\mathbb{Z}\times\mathbb{Z}) \approx V_4$.

Calculamos $U(\mathbb{Z}/10\mathbb{Z})$ empleando el Ejercicio I.1.7 sabemos que $U(\mathbb{Z}/10\mathbb{Z}) = \{a \in \mathbb{Z}/10\mathbb{Z} \ : \ \text{m.c.d.}(a,10) = 1\}$. Por tanto, $U(\mathbb{Z}/10\mathbb{Z}) = \{1,3,7,9\}$, $k = 4$ y empleando los apartados anteriores vemos que:

$T_1 : U(\mathbb{Z}/10\mathbb{Z})$	$\to U(\mathbb{Z}/10\mathbb{Z})$	$T_3 :$	$U(\mathbb{Z}/10\mathbb{Z}) \to U(\mathbb{Z}/10\mathbb{Z})$	$T_7 :$	$U(\mathbb{Z}/10\mathbb{Z}) \to U(\mathbb{Z}/10\mathbb{Z})$	$T_9 :$	$U(\mathbb{Z}/10\mathbb{Z}) \to U(\mathbb{Z}/10\mathbb{Z})$
1	$\to 1$		$1 \to 3$		$1 \to 7$		$1 \to 9$
3	$\to 3$		$3 \to 9$		$3 \to 1$		$3 \to 7$
7	$\to 7$		$7 \to 1$		$7 \to 9$		$7 \to 3$
9	$\to 9$		$9 \to 7$		$9 \to 3$		$9 \to 1$

Luego podemos establecer el siguiente isomorfismo de $\mathcal{T} = \{T_1, T_3, T_7, T_9\}$ en un subgrupo de S_4 de forma natural:

$$T_1 \to \mathrm{Id} \qquad T_3 \to (1,2,4,3) \qquad T_7 \to (1,3,4,2) \qquad T_i \to (1,4)(2,3).$$

Como $U(\mathbb{Z}/10\mathbb{Z}) \approx \mathcal{T}$ por (c) y como $\mathcal{T} \approx < (1,2,4,3) > \approx < (1,2,3,4) >$ deducimos que $U(\mathbb{Z}/10\mathbb{Z}) \approx < (1,2,3,4) >$.

Finalmente, concluimos que (1) y (3) son falsas porque $U(\mathbb{Z}[i])$ y $U(\mathbb{Z}/10\mathbb{Z})$ son cíclicos y $U(\mathbb{Z}\times\mathbb{Z})$ no es cíclico (I.6.37) y que (2) es cierta porque todos los grupos cíclicos del mimo orden son isomorfos (I.6.19), luego $U(\mathbb{Z}[i]) \approx U(\mathbb{Z}/10\mathbb{Z}) \approx <(1,2,3,4)> \approx C_4 \approx \mathbb{Z}/4\mathbb{Z}$

---

4. **[2.4 puntos=4x0.6]** En $\mathbb{Z}/3\mathbb{Z}[x]$, consideramos los polinomios

$$P_1(x) = x^4+2x^3+2x+2, \qquad P_2(x) = x^4+x^3+x^2+x+1, \qquad P_3(x) = x^3+x+2.$$

(a) Determinar, razonadamente, la lista completa de polinomios irreducibles de grado menor o igual que 2 de $\mathbb{Z}/3\mathbb{Z}[x]$.
Solución.

Comentario general: Como $\mathbb{Z}/3\mathbb{Z}$ es un cuerpo porque 3 es primo, tenemos que $\mathbb{Z}/3\mathbb{Z}[x]$ es un Dominio Euclideo y podemos aplicar los resultados de la Sección II.6.4.

Por la definición de irreducible, el polinomio nulo $P_0(x) = 0$ no es irreducible y los polinomios de grado 0 que son $P_1(x) = 1$ y $P_2(x) = 2$ no son irreducibles porque son unidades. (II.6.36)
Como $\mathbb{Z}/3\mathbb{Z}$ es un cuerpo, todos los polinomios de grado 1 son irreducibles en $\mathbb{Z}/3\mathbb{Z}[x]$ (II.6.38). Hay 6 polinomios de grado 1: x, $x+1$, $x+2$, $2x$, $2x+1$, $2x+2$.
Como $\mathbb{Z}/3\mathbb{Z}$ es un cuerpo, un polinomio de grado 2 es irreducible en $\mathbb{Z}/3\mathbb{Z}[x]$ si y solo si no tiene raíces en $\mathbb{Z}/3\mathbb{Z}$. Hay 18 polinomios de grado 2 en $\mathbb{Z}/3\mathbb{Z}[x]$, aquellos cuyo término independiente es nulo tienen a 0 como raíz, luego son reducibles. En consecuencia, basta estudiar 12 polinomios y podemos reducir el estudio a polinomios mónicos, puesto que todo polinomio es asociado a un polinomio mónico y la condición de ser irreducible es estable para asociados. De esta forma:

$$x^2+1 \sim 2x^2+2 \qquad x^2+x+1 \sim 2x^2+2x+2 \qquad x^2+2x+1 \sim 2x^2+x+2$$
$$x^2+2 \sim 2x^2+1 \qquad x^2+x+2 \sim 2x^2+2x+1 \qquad x^2+2x+2 \sim 2x^2+x+1$$

Estudiamos si los 6 polinomios mónicos de $\mathbb{Z}/3\mathbb{Z}$ con término independiente no nulo, tienen o no raíces:

Raíz / Polinomio	x^2+1	x^2+2	x^2+x+1	x^2+x+2	x^2+2x+1	x^2+2x+2
$x=1$	2	0	0	1	1	2
$x=2$	2	0	1	2	0	1

En consecuencia hay 12 polinomios irreducibles de grado menor o igual que 2 y la **lista completa** es:

x	$x+1$	$x+2$	x^2+1	x^2+x+2	x^2+2x+2
$2x$	$2x+2$	$2x+1$	$2x^2+2$	$2x^2+2x+1$	$2x^2+x+1$

(b) ¿Es $R_1 = \mathbb{Z}/3\mathbb{Z}[x]/(P_1(x))$ un dominio? ¿Es $R_2 = \mathbb{Z}/3\mathbb{Z}[x]/(P_2(x))$ un cuerpo?
Solución. Como $\mathbb{Z}/3\mathbb{Z}[x]$ es un D.E, tenemos que $P_1(x)$ (o $P_2(x)$) es irreducible si y solo si no descompone como polinomios de grado menor que $\mathrm{gr}(P_1)(=\mathrm{gr}(P_2)) = 4$.
Tanto para $P_1(x)$ como para $P_2(x)$, tenemos tres posibilidades:
(1) o bien tienen una raíz en $\mathbb{Z}/3\mathbb{Z}$, en cuyo caso descompone como un polinomio de grado 1 y un polinomio de grado 3.
(2) o bien no tienen raíces en $\mathbb{Z}/3\mathbb{Z}$ y descompone como el producto de dos polinomios de grado 2 **irreducibles**.
(3) o bien son irreducibles.

Estudiamos si tienen raíces:

Raíz / Polinomio	$P_1(x)=x^4+2x^3+2x+2$	$P_2(x)=x^4+x^3+x^2+x+1$
$x=1$	1	2
$x=2$	2	1

Ninguno de los dos tiene raíces, luego o bien descompone como el producto de dos polinomios de grado 2 **irreducibles** o bien son irreducibles.
Como la descomposición en irreducibles es única, salvo producto por asociados, en $\mathbb{Z}/3\mathbb{Z}[x]$ porque es D.F.U. por ser D.E. y como $P_1(x)$ y $P_2(x)$ son mónicos, si alguno fuera reducible uno de los factores debería ser uno de los polinomios mónicos irreducibles de grado 2 que hemos listado en el apartado (a): x^2+1, x^2+x+2 o x^2+2x+2. Observamos que:

$$(x^2+1)(x^2+2x+2)=x^4+x^2+2x^3+2x+2x^2+2=x^4+2x^3+2x+2=P_1(x)$$

luego $P_1(x)$ no es irreducible. Mientras que $P_2(x)$ como su término independiente es 1 sus únicos factores posibles son x^2+x+2 o x^2+2x+2 y observamos que

$$(x^2+x+2)(x^2+2x+2)=x^4+x^3+2x^2+2x^3+2x^2+x+2x^2+2x+1=x^4+1,$$
$$(x^2+x+2)(x^2+x+2)=x^4+x^3+2x^2+x^3+x^2+2x+2x^2+2x+1=x^4+2x^3+2x^2+x+1,$$
$$(x^2+2x+2)(x^2+2x+2)=x^4+2x^3+2x^2+2x^3+x^2+x+2x^2+x+1=x^4+x^3+2x^2+2x+1,$$

en ningún caso obtenemos $P_2(x)$, luego $P_2(x)$ es irreducible.

Por un lado, como $P_1(x)$ no es irreducible, tenemos que $P_1(x)$ no es primo (II.5.9), luego el ideal $(P_1(x))$ no es primo (II.5.9)y $R_1=\mathbb{Z}/3\mathbb{Z}[x]/(P_1(x))$ no es un dominio (II.4.15).

Por otro lado, como $P_2(x)$ es irreducible, $R_2=\mathbb{Z}/3\mathbb{Z}[x]/(P_2(x))$ un cuerpo (II.6.44).

(c) Determinar, si existe, el inverso para el producto de $x^2+1+(P_2(x))$ en R_2.
Solución. Como R_2 es cuerpo, el inverso de $x^2+1+(P_2(x))$ y para encontrarlo aplicamos el algoritmo de Euclides extendido con $A(x)=P_2(x)=x^4+x^3+x^2+x+1$ y $B(x)=x^2+1$:

$$(r_0=r_0s_0+r_1t_0)\quad x^4+x^3+x^2+x+1=(x^4+x^3+x^2+x+1)\cdot(1)+(x^2+1)\cdot(0),$$
$$(r_1=r_0s_1+r_1t_1)\quad x^2+1=(x^4+x^3+x^2+x+1)\cdot(0)+(x^2+1)\cdot(1),$$
$$(r_2=r_0s_2+r_1t_2)\quad 1=(x^4+x^3+x^2+x+1)\cdot(1)+(x^2+1)\cdot(2x^2+2x),$$
$$(r_3=r_0s_3+r_1t_3)\quad 0=(x^4+x^3+x^2+x+1)\cdot(2x^2+2)+(x^2+1)\cdot(x^4+x^3+x^2+x+1).$$

Luego tenemos que m.c.d. $(x^4+x^3+x^2+x+1,x^2+1)=1$ (el último resto no nulo)y la identidad de Bezout:

$$1=(x^4+x^3+x^2+x+1)\cdot(1)+(x^2+1)\cdot(2x^2+2x).$$

Tomando clases módulo $I_2=(P_2(x))$ vemos que $1+I_2=(x^2+1+I_2)(2x^2+2x+I_2)$, luego el inverso de de x^2+1+I_2 en R_2 es $2x^2+2x+I_2$.

(d) Consideramos el ideal $I=(P_1(x),P_3(x))$ de $\mathbb{Z}/3\mathbb{Z}[x]$. Determinar si I es principal o no y, en caso de ser principal encontrar un polinomio $P(x)\in\mathbb{Z}/3\mathbb{Z}[x]$ tal que $I=(P(x))$. (0.4p)
Probar que $I/(P_1(x))\approx(P_3(x))/(x^5+2x^3+2x^2+x+2)$. (0.2p)
Solución. Como $\mathbb{Z}/3\mathbb{Z}[x]$ es D.E., es D.I.P., luego I es principal. Sabemos que $P_1(x)$ descompone como producto de irreducibles como $P_1(x)=(x^2+1)(x^2+2x+2)$ que son irreducibles por el apartado (a).
Por otro lado, vemos que $P_3(2)=(2)^3+(2)+2=0$, luego $x=2$ es raíz, realizando la división de $P_3(x)$ entre $(x+1)$ vemos que $P_3(x)=(x+1)(x^2+2x+2)$ que son irreducibles por el apartado (a).

En consecuencia, un m.c.d. $(P_1(x), P_3(x))$ es $D(x) = x^2+2x+2$ y que un m.c.m. $(P_1(x), P_3(x))$ es $M(x) = (x+1)(x^2+2x+2)(x^2+1) = x^5+2x^3+2x^2+x+2$. Por las propiedades de los D.I.P (II.5.28):

$$I = (P_1(x), P_3(x)) = (P_1(x)) + (P_3(x)) = (D(x)) \qquad (P_1(x)) \cap (P_3(x)) = (M(x)).$$

Luego el polinomio buscado es $P(x) = D(x)$ y por el Segundo Teorema de Isomorfía:

$$(P_1(x)) + (P_3(x))/(P_1(x)) \approx (P_3(x))/(x^5+2x^3+2x^2+x+2).$$

UNIVERSIDAD DE CANTABRIA

EXAMEN FINAL
Convocatoria ordinaria
miércoles 8 de junio de 2022

G90 - Estructuras Algebraicas

Curso 2021-2022

Nombre y apellidos:

INSTRUCCIONES DE LA PRUEBA

- Las respuestas a las preguntas de la prueba deben escribirse con bolígrafo azul o negro.
- Está prohibido emplear lápiz, bolígrafos de otros colores y típex.
- No se permite el uso de calculadora ni de ningún otro dispositivo electrónico.
- No se permite el uso ni de apuntes, ni de libros, ni de ningún otro tipo de material bibliográfico.
- No se puede abandonar el aula antes de que haya transcurrido una hora desde el inicio de la prueba.
- El abandono del aula supone la finalización del examen por parte del estudiante.
- Todas las respuestas deben estar justificadas correctamente.

1. **[3.75 puntos=3x1.25]** Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(a) Si G y H son dos grupos cíclicos, entonces el grupo producto $G \times H$ es cíclico.
Falso. Basta tomar $G = H = \mathbb{Z}/2\mathbb{Z}$. Tenemos que $(\mathbb{Z}/2\mathbb{Z}, +)$ es cíclico porque $\mathbb{Z}/2\mathbb{Z} =< 1 >$. Sin embargo, tenemos que

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0),(1,0),(0,1),(1,1)\}$$

y que $< (0,0) >= \{(0,0)\}$, $< (1,0) >= \{(0,0),(1,0)\}$, $< (0,1) >= \{(0,0),(0,1)\}$ y que $< (1,1) >= \{(0,0),(1,1)\}$. Por tanto, no existe $a \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ tal que $< a >= \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b) Toda permutación distinta de la identidad o es un ciclo o descompone como producto de ciclos disjuntos.
Cierto. Como $\sigma \neq \mathrm{Id}$, existe $a \in \{1,2,\ldots,n\}$ tal que $\sigma(a) \neq a$. Establecemos la siguiente notación:

$$a_0 := a, \quad a_1 := \sigma(a_0), \quad a_2 := \sigma(a_1) = \sigma^2(a_0), \quad \ldots \quad a_m := \sigma(a_{m-1}) = \sigma^m(a_0), \quad \ldots$$

Como el conjunto $\{1,2,\ldots,n\}$ es finito, existen $m, \ell \in \mathbb{Z}$ con $0 \leq \ell < m$ tal que $a_m = a_\ell$. En otras palabras, se tiene que $\sigma^m(a_0) = \sigma^\ell(a_0)$ y aplicando σ^{-1} a ambos ℓ veces vemos que $\sigma^{m-\ell}(a_0) = a_0$.
Por tanto $\{s \in \mathbb{N} : \sigma^s(a_0) = a_0\} \neq \emptyset$ y, por el Principio de Buena Ordenación, podemos considerar $r = \min\{s \in \mathbb{N} : \sigma^s(a_0) = a_0\}$. Como r es el mínimo, tenemos que $a_m \neq a_\ell$ si $0 \leq \ell < m \leq r-1$: en caso contrario, razonando como antes, tendríamos que $\sigma^{m-\ell}(a_0) = a_0$ lo que es imposible porque $m - \ell \leq m < r$. En consecuencia, podemos considerar el siguiente ciclo de longitud r:

$$a = a_0 \to a_1, \qquad a_1 \to a_2, \qquad \ldots\ldots, \qquad a_{r-2} \to a_{r-1}, \qquad a_{r-1} \to a_r = a,$$

es decir, $(a_0, a_1, \ldots, a_{r-1})$.
Tenemos dos opciones:
Si $\sigma(x) = x$ para todo $x \in \{1,2,\ldots,n\} \backslash \{a_0, a_1, \ldots, a_{r-1}\}$, entonces $\sigma = (a_0, a_1, \ldots, a_{r-1})$ y hemos terminado.
Si existe $b \in \{1,2,\ldots,n\} \backslash \{a_0, a_1, \ldots, a_{r-1}\}$ tal que $\sigma(b) \neq b$. Repetimos el procedimiento y tomando $b_0 = b$ construimos el ciclo $(b_0, b_1, \ldots, b_{s-1})$. Veamos que este ciclo es disjunto con el anterior. Razonamos por reducción al absurdo si $a_m = b_\ell$ tendríamos que $\sigma^m(a_0) = \sigma^\ell(b_0)$, entonces $\sigma^{m-\ell}(a_0) = b_0$ luego se tendría que $b_0 \in \{a_0, a_1, \ldots, a_{r-1}\}$, lo que es imposible.

Como $\{1,2,\ldots,n\}$ es finito iterando el procedimiento y en un número finito de pasos descomponemos σ como

$$\sigma = (a_0, a_1, \ldots, a_{r-1})(b_0, b_1, \ldots, b_{s-1}) \cdots (y_0, y_1, \ldots, y_{t-1}),$$

donde los ciclos son disjuntos.

(c) Si G es un subgrupo de orden 730 y H es un subgrupo normal de G propio y no trivial tal que G/H es un grupo de orden par no abeliano, entonces G/H es un grupo diédrico.

Cierto. En primer lugar, observamos que 730 descompone en factores primos como $730 = 2 \cdot 5 \cdot 73$. Por el Teorema de Lagrange, tenemos que $\#(H) \cdot \#(G/H) = 730$. Como H es propio y no trivial y como $\#(G/H)$ es par, tenemos que $\#H \in \{5, 73, 365\}$ y $\#(G/H) \in \{2, 10, 146\}$. Por el Teorema de Clasificación de los Grupos de Orden Primo, si $\#(G/H)$, tendríamos que $G/H \approx C_2$ es cíclico, luego sería abeliano en contradicción con la hipótesis. En consecuencia, o bien $\#(G/H) = 10 = 2 \cdot 5$ o bien $\#(G/H) = 146 = 2 \cdot 73$, luego por el Teorema de Clasificación de los Grupos de Orden $2p$ con p primo y $p \geq 2$, tenemos que o bien $G/H \approx C_{2p}$ o bien $G/H \approx D_p$. Finalmente, usando de nuevo que G/H no es abeliano, concluimos que o bien $G/H \approx D_5$ o bien $G/H \approx D_{73}$.

---

2. **[3.25 puntos=1.5+1.75]** Sea $(G, \cdot)$ un grupo y $H \subseteq G$ un subgrupo de G de orden $k \in \mathbb{N}$.

(a) Probar que para todo $x \in G$ se cumple que $xHx^{-1} = \{xhx^{-1} \ : \ h \in H\}$ es un subgrupo de G. ¿Cuál es el orden de xHx^{-1}?
Solución. Vamos a aplicar el Test de Caracterización de subgrupos. En primer lugar, observamos que xHx^{-1} es no vacío porque $1_G \in H$ y $1_G = x1_Gx^{-1} \in xHx^{-1}$. Tomamos $a, b \in xHx^{-1}$ y veamos que $ab^{-1} \in xHx^{-1}$. Como $a \in xHx^{-1}$ existe $h_1 \in H$ tal que $a = xh_1x^{-1}$ y, análogamente, existe $h_2 \in H$ tal que $b = xh_2x^{-1}$. En consecuencia, se tiene que

$$ab^{-1} = (xh_1x^{-1})(xh_2x^{-1})^{-1} = (xh_1x^{-1})((x^{-1})^{-1}h_2^{-1}x^{-1}) = (xh_1x^{-1})(xh_2^{-1}x^{-1}) = xh_1h_2^{-1}x^{-1}.$$

Como H es subgrupo y como $h_1, h_2 \in H$ tenemos que $h_1h_2^{-1} \in H$, luego $ab^{-1} \in xHx^{-1}$.
Por otro lado, vemos que $\#(xHx^{-1}) = \#H = k$, para ello basta comprobar que la aplicación

$$\begin{array}{rccc} \Phi: & H & \to & xHx^{-1} \\ & h & \to & xhx^{-1} \end{array}$$

es biyectiva. Por la definición de xHx^{-1} es sobreyctiva, porque dado $a \in xHx^{-1}$ existe $h_1 \in H$ tal que $a = xh_1x^{-1}$, luego $\Phi(h_1) = a$. Veamos que es inyectiva, suponemos ahora que $\Phi(h_1) = \Phi(h_2)$, es decir, que $xh_1x^{-1} = xh_2x^{-1}$, luego multiplicando por x a la derecha y por x^{-1} a la izquierda concluimos que $h_1 = h_2$. En resumen, Φ es biyectiva y $\#(xHx^{-1}) = \#H = k$.

(b) Demostrar que si H es el único subgrupo de orden k de G, entonces $H \lhd G$. Dar un ejemplo de un grupo no abeliano de forma que todos sus subgrupos sean normales, justificando en cada caso por qué el correspondiente subgrupo es normal.
Solución. Por el apartado (a), para todo $x \in G$ sabemos que H y xHx^{-1} son subgrupos de G de orden k. Como sólo hay un subgrupo de orden k necesariamente para todo $x \in G$ se tiene que $H = xHx^{-1}$. En particular, esto quiere decir que para todo $x \in G$ y todo $h \in H$ se tiene que $xhx^{-1} \in H$, luego $H \lhd G$.
Podemos tomar como grupo con las propiedades requeridas el grupo de los cuaterniones $Q_8 = \{\pm 1, \ \pm i, \ \pm j, \ \pm k\}$.
Recordamos la relación fundamental $i^2 = j^2 = k^2 = ijk = -1$.
Q_8 no es abeliano porque $ij = k$ y $ji = -k$.
Vamos a dar la lista de subgrupos:

Estudiamos primero los subgrupos generados por un elemento:

$$<\{1\}>=\{1\} \qquad <\{-1\}>=\{1,-1\} \qquad <\{i\}>=\{1,\ -1,\ i,\ -i\}$$

$$<\{j\}>=\{1,\ -1,\ j,\ -j\} \qquad <\{k\}>=\{1,\ -1,\ k,\ -k\}$$

Con esta información también vemos que, para grupos generados por dos elementos $<\{a,b\}>$ tenemos que si $a=\pm 1$ entonces $<\{a,b\}>=<\{b\}>$ y si $b=\pm 1$ entonces $<\{a,b\}>=<\{a\}>$, luego ya los hemos listado. Luego sólo debemos estudiar $<\{i,j\}>$, $<\{j,k\}>$ y $<\{i,k\}>$. Como $ij=k$, $ik=-j$ y $jk=i$, concluimos que $Q_8=<\{i,j\}>=<\{j,k\}>=<\{i,k\}>$ Por tanto, los subgrupos de Q_8 son

$$=<\{1\}>=\{1\} \qquad <\{-1\}>=\{1,-1\} \qquad <\{i\}>=\{1,\ -1,\ i,\ -i\}$$

$$<\{j\}>=\{1,\ -1,\ j,\ -j\} \qquad <\{k\}>=\{1,\ -1,\ k,\ -k\} \qquad Q_8$$

Los subgrupos trivales $\{1\}$ y Q_8 son siempre normales.
Los subgrupos $<\{i\}>$, $<\{j\}>$ y $<\{k\}>$ son normales porque tienen índice 2, es decir, $\#(Q_8:H)=2$.
Finalmente, el subgrupo $<\{-1\}>=\{1,-1\}$ es normal porque es el único subgrupo de orden 2.

---

3. **[3 puntos=1.5+1.5]** Sea $(G,\cdot)$ un grupo cíclico finito y $d\in\mathbb{N}$.

(a) ¿Cuántos elementos de orden d hay en G? Dado $n\in\mathbb{N}$, $n>2$, determinar si el grupo $(U(\mathbb{Z}/(n^2-1)\mathbb{Z}),\cdot)$ es cíclico o no.
Solución. Recordamos los siguientes resultados probados sobre grupos cíclicos:
(A) Si H es un grupo cíclico de orden k tiene $\varphi(k)$ generadores, es decir, $\varphi(k)$ elementos de orden k, donde $\varphi(k)$ es la Función de Euler.
(B) Si $G=<a>$ es un grupo cíclico de orden n entonces para todo divisor d de n existe un único subgrupo de orden d que se puede expresar como

$$G_d=<a^{n/d}>=\{b\in G\ :\ O(b)\mid d\}.$$

Por tanto, tenemos dos opciones:
(1) si $d\nmid \#(G)$, entonces $\#(G)$ no tiene elementos de orden d porque $O(a)\mid \#(G)$ para todo $a\in G$.
(2) si $d\mid \#(G)$, entonces, por (B), todos los elementos de orden d de G pertenecen a G_d, luego basta contar los elementos de orden d del subgrupo G_d. Como G_d es cíclico y de orden d, por (A), tiene $\varphi(d)$ elementos de orden d.

En particular, observamos que un grupo cíclico o bien no tiene elementos de orden 2 o bien sólo tiene un elemento de orden 2, porque $(\varphi(2)=1)$.
Vemos que $(U(\mathbb{Z}/(n^2-1)\mathbb{Z}),\cdot)$ no es cíclico porque tiene 2 elementos de orden 2.
Observamos que

$$n^2-1\equiv 0 \,\text{mód}\, (n^2-1) \qquad \Rightarrow \qquad n^2\equiv 1 \,\text{mód}\, (n^2-1)$$

luego, como $n\not\equiv 1 \,\text{mód}\, (n^2-1)$, se cumple que $O(n)=2$, es decir, n tiene orden 2 en $(U(\mathbb{Z}/(n^2-1)\mathbb{Z}),\cdot)$.
Por otro lado, $(-1)^2=1$ en $(U(\mathbb{Z}/(n^2-1)\mathbb{Z}),\cdot)$ y, como $n^2-2\equiv -1 \,\text{mód}\, (n^2-1)$, tenemos que $(n^2-2)^2=1$ en $(U(\mathbb{Z}/(n^2-1)\mathbb{Z}),\cdot)$.
Como $n^2-2\not\equiv 1 \,\text{mód}\, (n^2-1)$ para todo $n\in\mathbb{N}$, se cumple que $O(n^2-2)=2$. También se puede comprobar directamente que

$$(n^2-2)^2\equiv n^4-4n^2+4 \overset{n^2\equiv 1 \,\text{mód}\, (n^2-1)}{\equiv} 1-4+-4\equiv 1 \,\text{mód}\, (n^2-1).$$

Por tanto, tenemos que $O(n)=2$ y $O(n^2-2)=2$ en $(U(\mathbb{Z}/(n^2-1)\mathbb{Z}),\cdot)$, además $n^2-2 \not\equiv n \bmod (n^2-1)$ porque $n>2$.
Obsérvese que en el caso $n=2$, $(U(\mathbb{Z}/3\mathbb{Z}),\cdot)$ es isomorfo a $(\mathbb{Z}/2\mathbb{Z},+)$ y sí es cíclico.

En resumen, tenemos dos elementos distintos de orden 2, luego $(U(\mathbb{Z}/(n^2-1)\mathbb{Z}),\cdot)$ no es cíclico.

(b) Para $n=10$, calcular $2^{11^{18}}$ en $(U(\mathbb{Z}/99\mathbb{Z}),\cdot)$.
Solución. Recordamos que $U(\mathbb{Z}/k\mathbb{Z})=\{a\in\mathbb{Z}/k\mathbb{Z} \,:\, \text{m.c.d.}\,(a,k)=1\}$, luego tiene $\varphi(k)=\#(U(\mathbb{Z}/k\mathbb{Z}))$ elementos, donde $\varphi(k)$ es la Función de Euler. Por tanto, para todo $a\in U(\mathbb{Z}/k\mathbb{Z})$ tenemos que $O(a)\mid\varphi(k)$, por lo tanto, $a^{\varphi(k)}=1$ en $U(\mathbb{Z}/k\mathbb{Z})$.

(Equivalentemente se puede usar el Teorema de Euler nos dice que si $\text{m.c.d.}\,(a,k)=1$, entonces $a^{\varphi(k)}\equiv 1 \mod k$)

Por tanto, para calcular $2^{11^{18}}$ en $(U(\mathbb{Z}/99\mathbb{Z}),\cdot)$, basta dividir el exponente 11^{18} entre $\varphi(99)$ porque de esa forma podemos sustituir 11^{18} por el resto de la división, es decir, cambiar el exponente por $11^{18} \mod \varphi(99)$. Usando las propiedades de la función de Euler, tenemos que

$$\varphi(99)=\varphi(9)\varphi(11)=(3^2-3)(11-1)=60.$$

Luego tenemos que calcular $11^{18} \mod 60$, para ello como $\text{m.c.d.}\,(11,60)=1$, es decir, 11 está en $U(\mathbb{Z}/60\mathbb{Z})$ podemos repetir la misma estrategia y calcular $18 \mod \varphi(60)$. En este caso, se tiene que

$$\varphi(60)=\varphi(4)\varphi(3)\varphi(5)=(4-2)(3-1)(5-1)=16.$$

En consecuencia, se tiene que $18\equiv 2 \mod 16$, luego $11^{18}\equiv 11^2\equiv 121\equiv 1 \mod 60$ y tenemos que $2^{11^{18}}\equiv 2 \mod 99$. En conclusión, $2^{11^{18}}$ es 2 en $(U(\mathbb{Z}/99\mathbb{Z}),\cdot)$.

---

4. **[3.75 puntos=3x1.25]** Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(a) Sea $(R,+,\cdot)$ un anillo conmutativo y unitario. Todo ideal maximal es primo y además I es un ideal primo si y sólo si R/I es un dominio.

Ciertas ambas.

- Sea I un ideal maximal, como satisface (M.I) satisface (P.I). Veamos que se satisface (P.II). Dados $a,b\in R$ con $ab\in I$. Si $a\notin I$, entonces I está estrictamente contenido en el ideal $(I\cup(a))$, donde $(a)=\{ra \,:\, r\in R\}$ y, como I es maximal, por (M.II) tenemos que $R=(I\cup(a))$. El ideal $(I\cup(a))$ coincide con el ideal $I+(a)$, luego $R=I+(a)$. Como R es unitario $1_R\in R=I+(a)$, luego existen $x\in I$ y $r\in R$ tales que $1_R=x+ra$. Multiplicando por b a ambos lados y, empleando la propiedad conmutativa, vemos que $b=b1_R=b(x+ra)=bx+rab$. Como $x\in I$, $bx\in I$ y como $ab\in I$, $rab\in I$ de forma que $b=bx+rab\in I$. Análogamente, si $b\notin I$ vemos que $a\in I$. En conclusión, I verifica (P.II).

- Como $(R,+,\cdot)$ es un un anillo conmutativo y unitario $(R/I,+,\cdot)$ es también un anillo conmutativo y unitario para todo ideal I de R. En otras palabras, sólo hace falta ver que ocurre con la propiedad (D.III).
$\Rightarrow$ Supongamos que R/I es un dominio. Por (D.III), $0_{R/I}=0_R+I$ es divisor del cero, es decir, existe $a+I\in R/I$ con $a+I\neq 0_{R/I}$ tal que $(a+I)(0_R+I)=0_R+I$. Como $a+I\neq 0_R+I$, tenemos que $a\notin I$ y, por tanto, $I\neq R$ y se satisface (P.I).
Dados $a,b\in R$ con $ab\in I$, observamos que $(a+I)(b+I)=(ab)+I=I=0_{R/I}$. Por (D.III),

o $a+I=0_{R/I}=I$ o $b+I=0_{R/I}=I$, es decir, o $a\in I$ o $b\in I$. Por consiguiente, I verifica (P.II).
$\Leftarrow$ Supongamos que I es un ideal primo. Por (P.I), existe $a\in R$ con $a\notin I$, luego $a+I\neq 0_{R/I}$ y se cumple que $(a+I)(0_R+I)=0_{R/I}$, es decir, $0_{R/I}$ es divisor del cero.
Veamos ahora que es el único divisor del cero. Dados $a,b\in R$ con $(a+I)(b+I)=0_{R/I}$. Tenemos que $(ab)+I=(a+I)(b+I)=0_{R/I}=I$, luego $ab\in I$. Por (P.II), o $a\in I$ o $b\in I$, es decir, o $a+I=I$ o $b+I=I$, por lo cual se satisface (D.III).

(b) Sea $f:R\to S$ un homomorfismo de anillos. Entoces se tiene que:
- si $a\in R$ es idempotente, $f(a)$ es idempotente en S.
Cierto.
Como a es un elemento idempotente, se tiene que $a^2=a$. Por ser f homomormismo de anillos, $f(a^2)=f(a\cdot_R a)=f(a)\cdot_S f(a)=f(a)^2$. Por otra parte, $f(a^2)=f(a)$ y por tanto $f(a)$ es idempotente.

- Si $a\in R$ es nilpotente, $f(a)$ es nilpotente en S.
Cierto.
Como a es un elemento nilpotente, existe $n\in\mathbb{N}$ tal que $a^n=0_R$ y se tiene que por ser f homomormismo de anillos, $f(a^n)=f(a\cdot_R a\cdot_R a\cdots a)=f(a)\cdot_S f(a)\cdot_S f(a)\cdots f(a)=f(a)^n$. Por otra parte, $f(a^n)=f(0_R)=0_S$ donde esta última igualdad es cierta en cualquier homomorfismo de anillos y por tanto $f(a)$ es nilpotente.

- Si R,S son anillos unitarios y $a\in R$ es unidad, $f(a)$ es unidad en S.
Falso.
Basta tomar $R=S=\mathbb{Z}$ y $f:\mathbb{Z}\to\mathbb{Z}$ el homomorfismo de anillos definido por $f(a)=0$ para todo $a\in\mathbb{Z}$. Claramente $\mathbb{Z}$ es un anillo unitario y f es homomorfismo de anillos pues $f(x+y)=0=0+0=f(x)+f(y)$ y $f(x\cdot y)=0=0\cdot 0=f(x)\cdot f(y)$ pero $f(1)=0\notin U(\mathbb{Z})$.

(c) Sea (D,δ) un dominio euclideo y sea $p(x)\in D[x]$ de grado 2 ó 3. $p(x)$ es irreducible en $D[x]$ si y sólo si $p(x)$ no tiene raíces en D.

Falso.

$R=(\mathbb{Z},\delta)$ es un dominio euclideo con la aplicación valor absoluto $\delta(m)=|m|$ (no es necesario probarlo). $p(x)=3x^2-6$ no es irreducible en $\mathbb{Z}[x]$ pues $p(x)=3*(x^2-3)$ pero no tiene raíces. Para grado 3 el polinomio $q(x)=3x^3-6=3(x^3-2)$ tampoco es irreducible y no tiene raíces. Sin embargo, si es cierto que si es irreducible no puede tener raíces.

---

5. **[3.25 puntos=1.25+1+1]** Sea $p\in\mathbb{Z}$ un número primo y

$$\mathbb{Q}_{(p)}=\{m/n\in\mathbb{Q}:mcd(m,n)=1,\ p\nmid n\}.$$

(a) Probar que $\mathbb{Q}_{(p)}$ es un subanillo de $\mathbb{Q}$ y que $\mathbb{Q}$ no posee subanillos propios que contengan a $\mathbb{Q}_{(p)}$. ¿Es $\mathbb{Q}_{(p)}$ ideal?

En primer lugar $\mathbb{Q}_{(p)}\neq\emptyset$ pues $\frac{1}{q}\in\mathbb{Q}_{(p)}$ con $q\neq p$ otro número primo (podria tomarse tambien $1=1/1\in\mathbb{Q}_{(p)}$ pues $p\nmid 1$). Seguidamente, dados $m_1/n_1,m_2/n_2\in\mathbb{Q}_{(p)}$, se tiene que

$$\frac{m_1}{n_1}-\frac{m_1}{n_1}=\frac{m_1n_2-m_2n_1}{n_1n_2}\qquad\text{y}\qquad\frac{m_1}{n_1}\frac{m_1}{n_1}=\frac{m_1m_2}{n_1n_2}$$

están en $\mathbb{Q}_{(p)}$ ya que $p \nmid n_1 n_2$, pues p es un primo de $\mathbb{Z}$ que no divide ni a n_1 ni a n_2. Por tanto $\mathbb{Q}_{(p)}$ es subanillo.

Por otro lado, $\mathbb{Q}_{(p)}$ no es ideal pues $1/q \in \mathbb{Q}_{(p)}$ con $q \neq p$ otro primo, $1/p \in \mathbb{Q}$ y

$$\frac{1}{q}\frac{1}{p} = \frac{1}{pq} \notin \mathbb{Q}_{(p)}.$$

Veamos que $\mathbb{Q}$ no posee subanillos propios que contengan a $\mathbb{Q}_{(p)}$. Sea A un subanillo de $\mathbb{Q}$ tal que $\mathbb{Q}_{(p)} \subsetneq A$. Entonces existe $x = a/b \in A$ con $mcd(a,b) = 1$ tal que $x \notin \mathbb{Q}_{(p)}$, es decir $p \mid b$. Sea $b = p^k c$ para algun $k \in \mathbb{N}$ y c no divisible por p. Entonces $x = p^{-k}(a/c)$ y $a/c \in \mathbb{Q}_{(p)}$. Además, como $mcd(a,b) = 1$, se tiene que $p \nmid a$ y a/c tiene inverso en $\mathbb{Q}_{(p)}$ que es precisamente c/a. Luego, $p^{-k} = x(c/a) \in A$ (pues $x \in A$ y $c/a \in \mathbb{Q}_{(p)} \subsetneq A$ y A es subanillo). Como $p^{-1} = p^{k-1}p^{-k}$ y $p^{k-1} \in \mathbb{Z}$, se tiene que $p^{-1} \in A$. Dado que cualquier elemento $y \in \mathbb{Q}$ se puede escribir de la forma $y = p^r(m/n)$ con $r \in \mathbb{Z}$ y $m/n \in \mathbb{Q}_{(p)}$, se tiene que $y \in A$, pues si $r \geq 0$, $y \in \mathbb{Q}_{(p)}$ y si $r < 0$, $p^r = (p^{-1})^{-r} \in A$ ya que $-r > 0$. Por tanto $A = \mathbb{Q}$.

(b) Sea $\mathfrak{m} = \{m/n \in \mathbb{Q}_{(p)} : p \mid m\}$. Demostrar que $\mathfrak{m}$ es un ideal formado por las no unidades de $\mathbb{Q}_{(p)}$.

En primer lugar, $p/1 \in \mathfrak{m}$ y $\mathfrak{m} \neq \emptyset$.Si $m_1/n_1, m_2/n_2 \in \mathfrak{m}$, es decir, si $p \mid m_1$ y $p \mid m_2$, entonces $p \mid m_1n_2 - m_2n_1$ y $\mathfrak{m}$ es un subgrupo del grupo aditivo de $\mathbb{Q}_{(p)}$. Y si $m_1/n_1 \in \mathbb{Q}_{(p)}$ y $m_2/n_2 \in \mathfrak{m}$, entonces $p \mid m_1m_2$, es decir $(m_1/n_1)(m_2/n_2) \in \mathfrak{m}$. Se tiene entonces que $\mathfrak{m}$ es un ideal de $\mathbb{Q}_{(p)}$. Por otra parte, $\mathfrak{m}$ es el conjunto de las no unidades de $\mathbb{Q}_{(p)}$, ya que si $m/n \notin \mathfrak{m}$, entonces $p \nmid m$ y m/n es unidad en $\mathbb{Q}_{(p)}$.

(c) Encontrar un isomorfismo de anillos entre $\mathbb{Z}/p\mathbb{Z}$ y $\mathbb{Q}_{(p)}/\mathfrak{m}$.

Sea la aplicación $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Q}_{(p)}/\mathfrak{m}$ dada por $f(r) = \frac{r}{1} + \mathfrak{m}$. En primer lugar hay que ver está bien definida, es decir si $r_1, r_2 \in \mathbb{Z}/p\mathbb{Z}$ tal que $r_1 = r_2$ entonces $f(r_1) = f(r_2)$. Pero como $r_1 = r_2$, existe $k \in \mathbb{Z}$ tal que $r_2 = r_1 + kp$. Por tanto $f(r_2) = f(r_1 + kp) = \frac{r_1+kp}{1} + \mathfrak{m} = \frac{r_1}{1} + \frac{kp}{1} + \mathfrak{m} = \frac{r_1}{1} + \mathfrak{m}$ pues $kp/1 \in \mathfrak{m}$ y se tiene que ambos tienen la misma imagen por f. Comprobamos que f es entonces homomorfismo de anillos, $f(x+y) = \frac{x+y}{1} + \mathfrak{m} = \frac{x}{1} + \frac{y}{1} + \mathfrak{m} = f(x) + f(y)$ y de la misma forma para el producto.

Veamos que es inyectivo; si $x, y \in \mathbb{Z}/p\mathbb{Z}$ tal que $f(x) = f(y)$ entonces $\frac{x}{1} + \mathfrak{m} = \frac{y}{1} + \mathfrak{m}$, equivalentemente $\frac{x}{1} - \frac{y}{1} \in \mathfrak{m}$ y por tanto $x - y$ es un múltiplo de p, luego $x = y$ en $\mathbb{Z}/p\mathbb{Z}$.

Veamos que es sobreyectivo; Sea $m/n + \mathfrak{m} \in \mathbb{Q}_{(p)}/\mathfrak{m}$. Hay que buscar un elemento $r \in \mathbb{Z}/p\mathbb{Z}$ tal que $f(r) = \frac{r}{1} + \mathfrak{m} = m/n \in \mathfrak{m}$, es decir tal que $(m/n) - r \in \mathfrak{m}$. Es equivalente a que $p \mid m - nr$. Como $p \nmid n$ (pues $m/n \in \mathbb{Q}_{(p)}$), n tiene inverso en $\mathbb{Z}/p\mathbb{Z}$. Sea $t = n^{-1} \in \mathbb{Z}/p\mathbb{Z}$ (y $p \nmid t$) y llamamos $r = mt$. Se tiene que $f(r) = mt/1 + \mathfrak{m} = m/n + \mathfrak{m}$.

---

6. [3 puntos=1.5+1.5] Sea $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$

(a) En el anillo $\mathbb{Z}[\sqrt{7}] \subset \mathbb{R}$, demuestra que $a = (8 + 3\sqrt{7})$ es una unidad. Claramente $a > 1$, calcula además otras 3 unidades, a_1, a_2 y a_3 tales que $a_1 < -1 < a_2 < 0 < a_3 < 1$. ¿cuántas unidades más serias capaz de dar?

Se tiene que $(8+3\sqrt{7}) \cdot (8-3\sqrt{7}) = 8^2 - 3 \cdot 2 \cdot 7 = 64 - 63 = 1$ y por tanto a es unidad.Otra forma de verlo es calcular el inverso de a en $\mathbb{R}$, racionalizando, y comprobar que se encuentra

en $\mathbb{Z}[\sqrt{7}]$;

$$\frac{1}{a} = \frac{1}{8+3\sqrt{7}} = \frac{8-3\sqrt{7}}{(8+3\sqrt{7})(8-3\sqrt{7})} = 8-3\sqrt{7}.$$

Aunque el enunciado ya nos dice que $a > 1$ no es díficil comprobarlo porque $3\sqrt{7} > 0$, por tanto, $a > 8 > 1$. Usando las propiedades de los números reales como $a \in (0,\infty)$, entonces $0 < 1/a = a^{-1} < 1$ y podemos tomar $a_3 = a^{-1}$ que es una unidad. De la misma forma $-a < -1$ y es unidad pues $(-a)\cdot(-a^{-1}) = 1$ y tomamos $a_1 = -a$. Por último, para a_2 basta considerar $-a^{-1}$.

En este anillo hay infinitas unidades: tenemos que $\pm a^k \in \mathbb{Z}[\sqrt{7}$ por ser anillo. Comprobar que son unidades es trivial pues $a^k \cdot a^{-k} = 1$ y son distintas dos a dos porque $a^k < a^{k+1}$ con $k \in \mathbb{N}$ porque $a > 1$. De hecho, se puede demostrar que son las únicas, es decir, todas las unidades son de la forma $\pm a^k$ con $k \in \mathbb{Z}$, pero este resultado no es trivial y no pregunta eso el enunciado.

(b) El anillo $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ es euclideo con la aplicación $\delta(a+bi) = a^2+b^2$. Determinar todos los máximos común divisores de $1+7i$ y $4-6i$.

En primer lugar si d es un maximo común divisor de $1+7i$ y $4-6i$ si y sólo si $d\cdot u$ es un maximo común divisor de $1+7i$ y $4-6i$, con $u \in \mathbb{Z}[i]^\star$. Las unidades de $\mathbb{Z}[i]$ son $\{\pm 1, \pm i\}$. Para calcular el máximo común divisor únicamente hay que aplicar el Algoritmo de Euclides. En primer lugar, como $\delta(1+7i) = 50, \delta(4-6i) = 52$ hay que encontrar $q, r \in \mathbb{Z}[i]$ tal que $4-6i = q_1\cdot(1+7i) + r_1$ con $r = 0$ o $\delta(r) < 50$. Para ello basta con dividir en los números complejos

$$\frac{4-6i}{1+7i} = \frac{-19}{25} + \frac{-17}{25}i$$

y tomar $q = a+bi \in Z[i]$ tal que $|a-(-\frac{19}{25})| \leq \frac{1}{2}$, $|b-(-\frac{19}{25})| \leq \frac{1}{2}$. Es decir, tomar $q = -1-i$, de esta forma $r_1 = -2+2i$ y $\delta(r_1) = 8 < 50$. Seguidamente

$$\frac{1+7i}{-2+2i} = \frac{3}{2} - 2i$$

y por tanto $q_2 = (1-2i)$ (podria tomarse tambien $q_2 = 2-2i$ y $r_2 = -1+i$. Ahora se tiene que $-2+2i = 2(-1+i)+0$ y por tanto un máximo común divisor de $1+7i$ y $4-6i$ es $-1+i$. Luego todos son $\{-1+i, 1-i, -1-i, 1+i\}$.

Otra forma de realizar este ejercicio es apoyarse en la aplicación $N(a+bi) = a^2+b^2$ que dota al anillo $\mathbb{Z}[i]$ de estructura de dominio euclideo. Esta aplicación es multiplicativa, es decir, $\forall x, y \in \mathbb{Z}[i]$ se tiene que $N(xy) = N(X)N(y)$. Este hecho implica que si $x \mid y$ en $\mathbb{Z}[i]$ entonces $N(x) \mid N(y)$ en $\mathbb{Z}$. Como $N(4-6i) = 52, N(1+7i) = 50$, si d es un maximo común divisor de ambos se tiene que $N(d) \mid 2 = mcd(50,52)$ Como los elementos que cumplen $N(u) = 1$ son unidades ($u = \pm 1, \pm i$), estos siempre dividen a d. Por tanto, para buscar el máximo común divisor$d$ habrá que comprobar si los elementos x con $N(x) = 2$ dividen a ambos. Se tiene que $N(x) = 2$ si y solo si $x = \pm 1 \pm i$ y es fácil comprobar que estos cuatro diviven tanto a $4-6i$ como a $1+7i$. Además, estos cuatro elementos son asociados, es decir, se diferencian en producto por una unidad. Son precisamente los máximos común divisores de $1+7i$ y $4-6i$.

UNIVERSIDAD DE CANTABRIA

EXAMEN FINAL
Convocatoria extraordinaria
lunes 27 de junio de 2022

G90 - Estructuras Algebraicas

Curso 2021-2022

Nombre y apellidos:

INSTRUCCIONES DE LA PRUEBA

- Las respuestas a las preguntas de la prueba deben escribirse con bolígrafo azul o negro.
- Está prohibido emplear lápiz, bolígrafos de otros colores y típex.
- No se permite el uso de calculadora ni de ningún otro dispositivo electrónico.
- No se permite el uso ni de apuntes, ni de libros, ni de ningún otro tipo de material bibliográfico.
- **Antes de comenzar el examen, los dispositivos electrónicos y los materiales bibliográfico deben situarse, fuera del alcance del estudiante, en el espacio del aula reservado con esta finalidad.**
- No se puede abandonar el aula antes de que haya transcurrido una hora desde el inicio de la prueba.
- El abandono del aula y/o el incumplimiento de estas normas supone la finalización del examen por parte del estudiante.
- Todas las respuestas deben estar justificadas correctamente.

PARTE I.

1. **[2.25 puntos=3x0.75]** Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(a) Dado $(G,\cdot)$ un grupo y $a \in G$ un elemento tal que $O(a) = d$, entonces para todo $k \in \mathbb{N}$ se tiene que

$$O(a^k) = \frac{O(a)}{\text{m.c.d.}\,(d,k)}.$$

Cierto. Dado $k \in \mathbb{N}$, como $a^k \in < a >$ y $\# < a >= d < \infty$, $O(a^k) = m < \infty$. Denotamos por $f := \text{m.c.d.}\,(d,k) \in \mathbb{N}$ y, por las propiedades del m.c.d. en $\mathbb{Z}$, $d = fd_1$ y $k = fk_1$ con $\text{m.c.d.}\,(d_1,k_1) = 1$. Veamos que $m = O(a^k) = d_1$. Observamos que

$$(a^k)^{d_1} = a^{kd_1} = a^{fk_1d_1} = a^{dk_1} = (a^d)^{k_1} = 1_G.$$

En consecuencia, por las propiedades del orden, se tiene que $m \mid d_1$.
Veamos ahora que $d_1 \mid m$. Como $(a^k)^m = 1_G$, se tiene que $a^{km} = 1_G$ y, por las propiedades del orden, $O(a) \mid km$. En otras palabras, $d \mid km$ o, equivalentemente, $fd_1 \mid fk_1m$. Por las propiedades de divisibilidad en $\mathbb{Z}$, $d_1 \mid k_1m$ y como $\text{m.c.d.}\,(d_1,k_1) = 1$, concluimos que $d_1 \mid m$, por las propiedades del m.c.d. en $\mathbb{Z}$. En resumen, $O(a^k) \mid d_1$ y $d_1 \mid O(a^k)$ y ambos son naturales, se cumple que $O(a^k) = d_1$, es decir,

$$O(a^k) = d_1 = \frac{d}{f} = \frac{d}{\text{m.c.d.}\,(d,k)} = \frac{O(a)}{\text{m.c.d.}\,(O(a),k)}.$$

(b) Dado $(G,\cdot)$ un grupo y N un subgrupo de G tal que N es abeliano, es decir, para todos $a,b \in N$ se tiene que $a \cdot b = b \cdot a$, entonces N es normal en G.
Falso. Basta considerar $G = D_3$, numeramos los vértices del triángulo y denotamos de la forma habitual a los giros $a = (1,2,3)$, $a^2 = (1,3,2)$ y a las simetrías $b_1 = (2,3)$, $b_2 = (1,3)$, $b_3 = (1,2)$. Tomamos $N =< b_1 >= \{\text{id}, b_1\}$ tenemos que N es abeliano. Sin embargo, N no es normal en G porque $aN = \{a, b_3\}$ es distinto de $Na = \{a, b_2\}$.

(c) Para todo $n \in \mathbb{N}$, con $n \geq 3$, se tiene que $S_n =< \{(1,2),(1,2,\ldots,n)\} >$.
Cierto. Observamos que:

$$(1,2,\ldots,n)^{-1} = (n,n-1,\ldots,2,1) \in < \{(1,2),(1,2,\ldots,n)\} > .$$

Luego

$$(1,2,\ldots,n)(1,2)(1,2,\ldots,n)^{-1} = (1,2,\ldots,n)(1,2)(n,n-1,\ldots,2,1) \in < \{(1,2),(1,2,\ldots,n)\} > .$$

Realizando el cálculo vemos que $(1,2,\ldots,n)(1,2)(n,n-1,\ldots,2,1) = (2,3)$, luego

$$(2,3) \in < \{(1,2),(1,2,\ldots,n)\} > .$$

Análogamente para todo $i \in \{1,2,\ldots,n-2\}$ vemos que

$$(i+1,i+2) = (1,2,\ldots,n)^i(1,2)(1,2,\ldots,n)^{-i} \in < \{(1,2),(1,2,\ldots,n)\} >$$

$$(1,n) = (1,2,\ldots,n)^{n-1}(1,2)(1,2,\ldots,n)^{-(n-1)} \in < \{(1,2),(1,2,\ldots,n)\} >$$

En consecuencia, todas las transposiciones de términos consecutivos, es decir, de la forma $(i,i+1)$ con $i \in \{1,\ldots,n-1\}$ y la transposición $(1,n)$ están en $< \{(1,2),(1,2,\ldots,n)\} >$.
Veamos ahora que cualquier transposición se puede poner como producto de transposiciones de este tipo. Dados $i,j \in \{1,\ldots,n\}$ con $i < j$, tenemos que

$$(i,j) = (j-1,j)\cdots(i+1,i+2)(i,i+1)(i+1,i+2)\cdots(j-1,j).$$

Por tanto, todas para toda transposición τ, tenemos que $\tau \in < \{(1,2),(1,2,\ldots,n)\} >$. Finalmente, como toda permutación $\sigma \in S_n$ descompone como producto de transposiciones tenemos que $S_n =< \{(1,2),(1,2,\ldots,n)\} >$.

---

2. [1.5 puntos] Probar que $(\mathbb{Q},+)$ no posee ningún subgrupo propio de índice finito. ¿Ocurre lo mismo en $(\mathbb{Q}\backslash\{0\},\cdot)$?

Solución. Suponemos que H es un subgrupo de $(\mathbb{Q},+)$ con índice finito, $\#(\mathbb{Q}:H) < \infty$. Como $(\mathbb{Q},+)$ es abeliano, tenemos que todo subgrupo es normal, luego $H \lhd \mathbb{Q}$ y podemos considerar el grupo cociente $(\mathbb{Q}/H,+)$ que sabemos que tiene orden $\#(\mathbb{Q}/H) = (\mathbb{Q}:H) = n \in \mathbb{N}$. Por consiguiente, para todo $q \in \mathbb{Q}$ se tiene que $O(q+H)|n$, luego

$$n(q+H) = 0_{\mathbb{Q}/H} = 0+H.$$

Por tanto, vemos que $nq+H = H$, es decir, $nq \in H$ para todo $q \in \mathbb{Q}$. Usando esta propiedad, vemos que dado $x \in \mathbb{Q}$ podemos tomar $q = x/n$ y deducir que

$$x = n\frac{x}{n} = nq \in H.$$

En conclusión, $\mathbb{Q} = H$ y H no es un subgrupo propio.

Por otro lado, en $(\mathbb{Q}\backslash\{0\},\cdot)$ sí existen subgrupos propios de índice finito. Basta tomar $H = \mathbb{Q}_{>0}$ que es subgrupo porque $1 \in H$ porque $1 > 0$, si $a,b \in H$, entonces $a,b > 0$, luego $ab > 0$ y se concluye que $ab \in H$ y, finalmente, si $a > 0$, entonces $a^{-1} = 1/a > 0$, luego $a^{-1} \in H$.
Observamos que $\#(\mathbb{Q}:H) = 2$ porque dado $q \in \mathbb{Q}\backslash\{0\}$ tenemos dos opciones: si $q > 0$, entonces $q \in H$, luego $qH = H$, si $q < 0$, entonces $q \notin H$, pero $-q \in H$ luego $qH = (-1)H$. En otras palabras, sólo hay dos clases módulo H, H y $(-1)H$.

---

3. **[1.25 puntos]** Describe los elementos y los subgrupos del grupo $(\mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z}),\cdot)$ y clasifícalo.

Solución. En primer lugar, calculamos las matrices 2×2 con coeficientes en $\mathbb{Z}/2\mathbb{Z}$ invertibles. Para ello podemos proceder de muchas formas. Por ejemplo podemos calcular las posibles bases de $(\mathbb{Z}/2\mathbb{Z})^2$ y ponerlas en filas. De esta forma obtenemos 6 matrices en $\mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z})$:

$$A_1=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad A_2=\begin{pmatrix}1&0\\1&1\end{pmatrix},\quad A_3=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad A_4=\begin{pmatrix}0&1\\1&1\end{pmatrix},\quad A_5=\begin{pmatrix}1&1\\1&0\end{pmatrix},\quad A_6=\begin{pmatrix}1&1\\0&1\end{pmatrix}.$$

Podríamos estudiar el orden de los elementos uno a uno y las distintas posibilidades para los subgrupos. Otra opción es establecer directamente la clasificación de $(\mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z}),\cdot)$. Como $\#\mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z})=6$, que es de la forma $2p$, tenemos dos posibilidades o $\mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z})\simeq C_6$ o $\mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z})\simeq D_3$ observamos que

$$A_2A_3=\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}0&1\\1&1\end{pmatrix}=A_4$$
$$A_3A_2=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&0\\1&1\end{pmatrix}=\begin{pmatrix}1&1\\1&0\end{pmatrix}=A_5$$

En consecuencia, $\mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z})$ no es abeliano, luego es isomorfo a D_3.
Usando esta clasificación, de forma inmediata, se obtiene que sus elemento tienen órdenes:

$$O(A_1)=1,\quad O(A_2)=O(A_3)=O(A_6)=2,\quad O(A_4)=O(A_5)=3.$$

En otras palabras, A_1 es la identidad, A_2, A_3 y A_6 son las simetrías y A_4 y A_5 son las rotaciones. Los subgrupos son:

$$\{A_1\},\quad \{A_1,A_2\},\quad \{A_1,A_3\},\quad \{A_1,A_6\}$$
$$\{A_1,A_4,A_5\},\quad \{A_1,A_2,A_3,A_4,A_5,A_6\}.$$

UNIVERSIDAD DE CANTABRIA

EXAMEN FINAL
Convocatoria extraordinaria
lunes 27 de junio de 2022

G90 - Estructuras Algebraicas
Curso 2021-2022

Nombre y apellidos:

INSTRUCCIONES DE LA PRUEBA

- Las respuestas a las preguntas de la prueba deben escribirse con bolígrafo azul o negro.
- Está prohibido emplear lápiz, bolígrafos de otros colores y típex.
- No se permite el uso de calculadora ni de ningún otro dispositivo electrónico.
- No se permite el uso ni de apuntes, ni de libros, ni de ningún otro tipo de material bibliográfico.
- **Antes de comenzar el examen, los dispositivos electrónicos y los materiales bibliográfico deben situarse, fuera del alcance del estudiante, en el espacio del aula reservado con esta finalidad.**
- No se puede abandonar el aula antes de que haya transcurrido una hora desde el inicio de la prueba.
- El abandono del aula y/o el incumplimiento de estas normas supone la finalización del examen por parte del estudiante.
- Todas las respuestas deben estar justificadas correctamente.

PARTE II.

4. **[2.25 puntos=3x0.75]** Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(a) Sea $(R,+,\cdot)$ un anillo entonces para todos $a,b\in R$ se tiene que $(a+b)^2=a^2+2ab+b^2$.
Falso. Basta tomar, en el anillo $R=\mathrm{Mat}_{2\times 2}(\mathbb{Z})$, las matrices:

$$a=\begin{pmatrix}1&1\\0&1\end{pmatrix} \qquad \text{y} \qquad b=\begin{pmatrix}1&0\\0&2\end{pmatrix}$$

Tenemos que

$$(a+b)^2=\begin{pmatrix}2&1\\0&3\end{pmatrix}^2=\begin{pmatrix}4&5\\0&9\end{pmatrix}.$$

$$a^2+2ab+b^2=\begin{pmatrix}1&2\\0&1\end{pmatrix}+2\begin{pmatrix}1&2\\0&2\end{pmatrix}+\begin{pmatrix}1&0\\0&4\end{pmatrix}=\begin{pmatrix}4&6\\0&9\end{pmatrix}.$$

Por tanto, la igualdad no se cumple.

(b) Sea $(R,+,\cdot)$ un anillo unitario e I un ideal de R tal que $I\cap U(R)\neq\emptyset$, entonces $I=R$.
Cierto. Como $I\cap U(R)\neq\emptyset$, entonces existe $u\in I\cap U(R)$. Como u es unidad tenemos que existe u^{-1} y $1_R=u^{-1}u$. Veamos que $R\subseteq I$ (la otra contención siempre es cierta). Dado $r\in R$ tenemos que

$$r=r\,1_R=\overbrace{r\,u^{-1}}^{\in R}\overbrace{u}^{\in I}\in I$$

porque I es un ideal. En conclusión, se cumple que $I=R$.

(c) Sea $(D,+,\cdot)$ un dominio, entonces todo elemento primo es un elemento irreducible.
Cierto. Supongamos que a es primo y que existen $b,c\in D$ tales que $a=bc$, entonces $a1_D=bc$, es decir, $a\mid bc$. Como a es primo $a\mid b$ o $a\mid c$. Supongamos que $a\mid b$, luego $ar=b$ para algún $r\in D$. Podemos escribir $a=rac$ y como $a\neq 0_D$, por la Ley de Cancelación, $rc=1_D$, esto es, $c\in U(D)$. Análogamente si $a\mid c$, vemos que $b\in U(D)$ y concluimos que a es irreducible.

5. [1.5 puntos] Probar que un anillo conmutativo y unitario $(R,+,\cdot)$ es un cuerpo si y solo si sus únicos ideales son (0) y R (y son distintos). ¿Cuántos ideales tiene $\mathbb{Z}/2022\mathbb{Z}$?¿y cuántos ideales tiene $\mathbb{Z}/n\mathbb{Z}$ (con $n \in \mathbb{N}$)?

Solución. Como R es conmutativo y unitario sólo hay que probar que:

$$U(R) = R\backslash\{0\} \qquad \Leftrightarrow \qquad \text{los únicos ideales de } R \text{ son } (0) \text{ y } R \text{ (y son distintos).}$$

$\Rightarrow$ Como $U(R) = R\backslash\{0\}$, entonces $1_R \neq 0_R$, luego R es no es el anillo trivial y tenemos que (0) y R son distintos.
Dado I un ideal de R distinto de (0), veamos que $I = R$. Como $I \neq (0)$, existe $u \in I \cap (R\backslash\{0\}) = I \cap U(R)$, luego como en el apartado 4.(b), probamos que $I = R$. En conclusión, los únicos ideales de R son (0) y R (y son distintos)
$\Leftarrow$ Como (0) y R son distintos, R es no es el anillo trivial, luego $1_R \neq 0_R$, y tenemos que $U(R) \subseteq R\backslash\{0\}$. Veamos que se tiene la otra contención. Dado $a \in R\backslash\{0\}$, tenemos que $I = (a)$ es un ideal de R distinto de (0). Por tanto, se cumple que $I = R$ y vemos que $1_R \in R = I = (a)$, luego existe $c \in R$ tal que $1_R = c \cdot a$, en consecuencia, $a \in U(R)$ y hemos probado que $U(R) = R\backslash\{0\}$.

Para ver cuántos ideales distintos tiene $\mathbb{Z}/2022\mathbb{Z}$ o $\mathbb{Z}/n\mathbb{Z}$ observamos que el homomorfismo de paso al cociente:

$$\begin{array}{rccc} p_n: & \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & k & \to & k+n\mathbb{Z} \end{array}$$

tiene por núcleo $\ker(p_n) = n\mathbb{Z}$ y establece una biyección entre los ideales de $\mathbb{Z}$ que contienen al $\ker(p_n) = n\mathbb{Z}$ y los ideales de $\mathbb{Z}/n\mathbb{Z}$(probar). Por tanto, para estudiar los ideales de $\mathbb{Z}/n\mathbb{Z}$, basta estudiar los ideales de $\mathbb{Z}$ que contienen al $\ker(p_n) = n\mathbb{Z}$. Sabemos que los ideales de $\mathbb{Z}$ son de la forma $k\mathbb{Z}$ con $k \in \mathbb{N}$. Luego tenemos que buscar los $k \in \mathbb{N}$ tales que $n\mathbb{Z} \subseteq k\mathbb{Z}$, es decir, tales que $n \in k\mathbb{Z}$.
Por tanto, $\mathbb{Z}/n\mathbb{Z}$ tiene

$$\#\{k \in \mathbb{N} : k \mid n\}$$

ideales, es decir, tiene tantos ideales como divisores naturales distintos tiene n.
Por ejemplo, como $2022 = 2 \cdot 3 \cdot 337$, tenemos que los divisores de 2022 son:

$$1, \quad 2, \quad 3, \quad 337, \quad 6, \quad 674, \quad 1011, \quad 2022.$$

Por consiguiente, $\mathbb{Z}/2022\mathbb{Z}$ tiene 8 ideales distintos:

$$\mathbb{Z}/2022\mathbb{Z}, \quad 2\mathbb{Z}/2022\mathbb{Z}, \quad 3\mathbb{Z}/2022\mathbb{Z}, \quad 337\mathbb{Z}/2022\mathbb{Z},$$
$$6\mathbb{Z}/2022\mathbb{Z}, \quad 674\mathbb{Z}/2022\mathbb{Z}, \quad 1011\mathbb{Z}/2022\mathbb{Z}, \quad 2022\mathbb{Z}/2022\mathbb{Z} = (0).$$

---

6. [1.25 puntos] En $(\mathbb{Z}/3\mathbb{Z})[x]$ consideramos el polinomio $P(x) = x^3 + x^2 + x + 2$ y el anillo cociente $A = (\mathbb{Z}/3\mathbb{Z})[x]/(P(x))$ Determinar un sistema completo de representantes de A. ¿Es A un dominio? ¿Es A un cuerpo? ¿cuántos elementos tiene A?

Solución. En primer lugar, observamos que $P(x) = x^3 + x^2 + x + 2$ no tiene raíces en $(\mathbb{Z}/3\mathbb{Z})$ porque

$$P(0) = 2 \qquad P(1) = 2 \qquad P(2) = 1$$

Como $P(x)$ es un polinomio de grado 3 y $(\mathbb{Z}/3\mathbb{Z})$ es un cuerpo y no tiene raíces, podemos deducir que $P(x)$ es irreducible en $(\mathbb{Z}/3\mathbb{Z})[x]$. Por tanto, por el Corolario II.6.45, tenemos que A es un cuerpo con $3^3 = 27$ elementos.
Para calcular un sistema completo de representantes, basta calcular todos los restos de dividir un polinomio de $(\mathbb{Z}/3\mathbb{Z})[x]$ entre $P(x) = x^3 + x^2 + x + 2$, porque dado cualquier polinomio $A(x)$ de $(\mathbb{Z}/3\mathbb{Z})[x]$ tenemos que $A(x) + (P(x)) = R(x) + (P(x))$ donde $R(x)$ es el resto de dividir $A(x)$ entre $P(x)$. Además restos distintos originan clases distintas porque su diferencia no está en $I = (P(x))$, dado que los polinomios de I no nulos tienen grado por lo menos 3.

En conclusión, un sistema completo de representantes es:

$$0+I \quad x+I \quad 2x+I \quad x^2+I \quad 2x^2+I \quad (x^2+x)+I \quad (x^2+2x)+I$$
$$1+I \quad (x+1)+I \quad (2x+1)+I \quad (x^2+1)+I \quad (2x^2+1)+I \quad (x^2+x+1)+I \quad (x^2+2x+1)+I$$
$$2+I \quad (x+2)+I \quad (2x+2)+I \quad (x^2+2)+I \quad (2x^2+2)+I \quad (x^2+x+2)+I \quad (x^2+2x+2)+I$$
$$(2x^2+x)+I \quad (2x^2+x+1)+I \quad (2x^2+x+2)+I \quad (2x^2+2x)+I \quad (2x^2+2x+1)+I \quad (2x^2+2x+2)+I$$

UNIVERSIDAD DE CANTABRIA

PRIMERA PRUEBA

miércoles 15 de marzo de 2023

G90 - Estructuras Algebraicas

Curso 2022-2023

Nombre y apellidos:

INSTRUCCIONES DE LA PRUEBA

- Las respuestas a las preguntas de la prueba deben escribirse con bolígrafo azul o negro.
- Está prohibido emplear lápiz, bolígrafos de otros colores y típex.
- No se permite el uso de calculadora ni de ningún otro dispositivo electrónico.
- No se permite el uso ni de apuntes, ni de libros, ni de ningún otro tipo de material bibliográfico.
- Antes de comenzar el examen, los dispositivos electrónicos y los materiales bibliográficos deben situarse, fuera del alcance del estudiante, en el espacio del aula reservado con esta finalidad.
- No se puede abandonar el aula antes de que haya transcurrido una hora desde el inicio de la prueba.
- El abandono del aula y/o el incumplimiento de estas normas supone la finalización del examen por parte del estudiante.
- Todas las respuestas deben estar justificadas correctamente.

1. **[1 punto]** Define los siguientes conceptos:

(a) **[0,5 puntos]** Mínimo común múltiplo de dos enteros.

Sean $a,b \in \mathbb{Z}$. Decimos que un elemento $m \in \mathbb{Z}$ es **un mínimo común múltiplo de** a **y** b si
(MCM.I) se tiene que $a \mid m$ y $b \mid m$. (*Múltiplo común*)
(MCM.II) para todo $n \in \mathbb{Z}$ tal que $a \mid n$ y $b \mid n$ se cumple que $m \mid n$.
(*Mínimo para la relación de divisibilidad*)

(b) **[0,5 puntos]** Orden de un elemento de un grupo.

Sea $(G,\cdot)$ un grupo y $a \in G$. Se llama **orden de** a al entero positivo más pequeño m tal que $a^m = 1_G$, si no existe dicho entero decimos que el **orden de** a **es infinito**. En ambos caso lo denotamos por $O(a)$, es decir,

- Si $\{m \in \mathbb{N}_{\geq 1} : a^m = 1_G\} = \emptyset$, entonces $O(a) = \infty$.
- Si $\{m \in \mathbb{N}_{\geq 1} : a^m = 1_G\} \neq \emptyset$, entonces $O(a) = \min\{m \in \mathbb{N}_{\geq 1} : a^m = 1_G\}$.

2. **[3 puntos - p.121 - A.1.8]** Sabemos que $(\mathbb{N},+)$ es un monoide conmutativo donde se cumple la ley de cancelación, es decir, para todos $a,b,c \in \mathbb{N}$ si $a+c = a+b$, entonces $c = b$. En el producto cartesiano $\mathbb{N} \times \mathbb{N}$ definimos la siguiente relación:

$$(n,m)\ R\ (n',m') \qquad \Leftrightarrow \qquad n+m' = n'+m.$$

Se pide:

(a) **[1 punto]** Probar que R es una relación de equivalencia.

Solución. Tenemos que probar que R es reflexiva, simétrica y transitiva.

Dado $(n,m) \in \mathbb{N} \times \mathbb{N}$ se tiene que $n+m = n+m$ porque la igualdad es reflexiva, luego $(n,m)R(n,m)$, es decir, R es **reflexiva**.

Dados $(n,m),(n',m') \in R$ tales que $(n,m)\ R\ (n',m')$ se tiene que $n+m' = n'+m$, dado que la igualdad es simétrica $n'+m = n+m'$. Por tanto, deducimos que $(n',m')\ R\ (n,m)$, es decir, R es **simétrica**.

Dados $(n,m),(n',m'),(n'',m'') \in R$ tales que $(n,m)\,R\,(n',m')$ y $(n',m')\,R\,(n'',m'')$, se tiene que $n+m'=n'+m$ y $n'+m''=n''+m'$. Sumando ambas ecuaciones se cumple que

$$(n+m')+(n'+m'')=(n'+m)+(n''+m').$$

Aplicando las propiedad asociativa y conmutativa del monoide $(\mathbb{N},+)$, varas veces a ambos lados de la igualdad, vemos que

$$(n'+m')+(n+m'')=(n'+m')+(n''+m).$$

Aplicando la ley de cancelación para $a=n'+m'$, $b=n+m''$ y $c=n''+m$, deducimos que se cumple la igualdad $n+m''=n''+m$. Por tanto, R es **transitiva** y en conclusión, R es una **relación de equivalencia.**

En el conjunto cociente $A=\mathbb{N}\times\mathbb{N}/R$ definimos, para todos $n,m,\ell,k\in\mathbb{N}$, la correspondencia $\boxplus$:

$$[(n,m)]_R \boxplus [(\ell,k)]_R = [(n+\ell,m+k)]_R.$$

(b) [1 punto] Probar que $\boxplus$ es una operación interna en A.

Solución. Tenemos que probar que $\boxplus$ es aplicación y es interna.

Dados $n,m,\ell,k\in\mathbb{N}$, como la suma es interna en el monoide $(\mathbb{N},+)$, tenemos que $n+\ell\in\mathbb{N}$ y que $m+k\in\mathbb{N}$. Por tanto, se tiene que $(n+\ell,m+k)\in\mathbb{N}\times\mathbb{N}$, luego

$$[(n,m)]_R \boxplus [(\ell,k)]_R = [(n+\ell,m+k)]_R \in \mathbb{N}\times\mathbb{N}/R.$$

En otras palabras, $\boxplus$ es **interna** en A.

Como la correspondencia $\boxplus$ está definida sobre un cociente, para comprobar que es aplicación tenemos que comprobar que su imagen no depende de los representantes elegidos, es decir, que $\boxplus$ está bien definida. Tomamos $[(n,m)]_R,[(n',m')]_R,[(\ell,k)]_R[(\ell',k')]_R \in A$ tales que

$$[(n,m)]_R=[(n',m')]_R, \qquad [(\ell,k)]_R=[(\ell',k')]_R.$$

En otras palabras, se tiene que

$$n+m'=n'+m, \qquad \ell+k'=\ell'+k.$$

Sumando ambas igualdades se tiene que

$$(n+m')+(\ell+k')=(n'+m)+(\ell'+k).$$

Aplicando las propiedad asociativa y conmutativa del monoide $(\mathbb{N},+)$, varas veces a ambos lados de la igualdad, vemos que

$$(n+\ell)+(m'+k')=(n'+\ell')+(m+k).$$

Por tanto, se tiene que $[(n+\ell,m+k)]_R=[(n'+\ell',m'+k')]_R$, es decir, se cumple que

$$[(n,m)]_R \boxplus [(\ell,k)]_R = [(n',m')]_R \boxplus [(\ell',k')]_R,$$

luego $\boxplus$ es **aplicación.**

(c) [1 punto] Probar que $(A,\boxplus)$ es un grupo abeliano.

Solución. Observamos que $A\neq\emptyset$ porque $\mathbb{N}\neq\emptyset$. Tenemos que probar que la operación $\boxplus$ cumple las propiedades asociativa, conmutavia, la existencia de neutro y la existencia de opuesto.
Dados $[(n,m)]_R,[(\ell,k)]_R,[(p,q)]_R\in A$ se tiene que

$$[(n,m)]_R \boxplus ([(\ell,k)]_R \boxplus [(p,q)]_R) = [(n,m)]_R \boxplus [(\ell+p,k+q)]_R = [(n+(\ell+p),m+(k+q)]_R$$
$$\overset{\text{Asociativa }(\mathbb{N},+)}{=} [(n+\ell)+p,(m+k)+q]_R = [(n+\ell,m+k)]_R \boxplus [(p,q)]_R = ([(n,m)]_R \boxplus [(\ell,k)]_R) \boxplus [(p,q)]_R.$$

Por consiguiente, $\boxplus$ cumple la **propiedad asociativa.**

Dados $[(n,m)]_R,[(\ell,k)]_R\in A$ se tiene que

$$[(n,m)]_R \boxplus [(\ell,k)]_R = [(n+\ell,m+k)]_R \overset{\text{Conmutativa }(\mathbb{N},+)}{=} [(\ell+n,k+m)]_R = [(\ell,k)]_R \boxplus [(n,m)]_R.$$

Por ende, $\boxplus$ cumple la **propiedad conmutativa.**

Veamos que $[(0,0)]_R$ es el **neutro** de $(A,\boxplus)$. Como hemos probado la propiedad conmutativa antes, sólo tenemos que probar que es el neutro por la derecha. Dado $[(n,m)]_R \in A$ se tiene que

$$[(n,m)]_R \boxplus [(0,0)]_R = [(n+0,m+0)]_R \overset{\text{Neutro } (\mathbb{N},+)}{=} [(n,m)]_R.$$

Dado $[(n,m)]_R \in A$ vemos que $[(m,n)]_R$, que también es un elemento de A, es su **opuesto**. De nuevo, vomo hemos probado la propiedad conmutativa antes, sólo tenemos que probar que es el opuesto por la derecha.

$$[(n,m)]_R \boxplus [(m,n)]_R = [(n+m,m+n)]_R.$$

Como tenemos que $n+m = n+m$ se cumple que $(n+m)+0 = 0+(m+n)$ por las propiedades asociativa y conmutativa del monoide $(\mathbb{N},+)$, luego $[(n+m,m+n)]_R = [(0,0)]_R$. En consecuencia, se cumple que $[(n,m)]_R \boxplus [(m,n)]_R = [(0,0)]_R$, lo que prueba la existencia de opuesto. En conclusión, $(A,\boxplus)$ es un grupo abeliano.

---

3. **[4 puntos]** Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(a) **[2 puntos(I.3.6)]** Todo subgrupo de un grupo cíclico es cíclico.

Cierta Dado un grupo cíclico $(G,\bullet)$ y H un subgrupo de G, existe $a \in G$ tal que $G =< a >$. Distinguimos dos casos:

(a) Si $H = \{1_G\}$, tenemos que $H =< 1_G >$ y, por tanto, es cíclico.

(b) Si $H \neq \{1_G\}$, existe $x \in H$, $x \neq 1_G$. Como $G =< a >$, existe $m \in \mathbb{Z}$ con $m \neq 0$ tal que $x = a^m$. Como H es subgrupo, $x^{-1} = a^{-m} \in H$. En resumen, podemos suponer que existe $k \in \mathbb{N}_{\geq 1}$ tal que $a^k \in H$.

Consideramos $A := \{k \in \mathbb{N}_{\geq 1} : a^k \in H\}$, como $A \neq \emptyset$ y $A \subseteq \mathbb{N}_{\geq 1}$, por el Principio de Buena Ordenación existe $d = \text{mín}(A)$. Veamos que $H =< a^d >$.

- $\supseteq$ Como H es subgrupo, $< a^d > \subseteq H$ porque $a^d \in H$.
- $\subseteq$ Dado $y \in H$, como $G =< a >$, existe $n \in \mathbb{Z}$ tal que $y = a^n$. realizando la división Euclidea de n entre d existe $q, r \in \mathbb{Z}$ con $n = dq + r$ y $0 \leq r < d$. Por tanto, se tiene que $a^n = a^{qd+r} = (a^d)^q a^r$. Como $a^d, a^n \in H$, deducimos que $a^r = a^n (a^d)^{-q} \in H$ porque H es un subgrupo. Como $0 \leq r < d$ y como $d = \text{mín}(A)$, concluimos que $r = 0$, luego $a^n = (a^d)^q \in < a^d >$.

En definitiva, $H =< a^d >$, luego H es cíclico.

(b) **[2 puntos (Test I.3.- Pregunta 8)]** Sean $(G,\cdot)$ un grupo y $x \in G$ tal que $O(x) = 2023$. Entonces el grupo G contiene al menos 1503 elementos de orden 2023.

Cierta. Consideramos el subgrupo $H =< x >$. Tenemos que H es un grupo cíclico y por las propiedades del orden $\#(H) = \#(< x >) = O(x) = 2023$. Por tanto, H es un grupo cíclico finito y, por las propiedades de estos grupos, sabemos que tiene $\varphi(\#(H))$ generadores, es decir, $\varphi(2023)$ elementos de orden 2023. Por tanto, podemos garantizar que en G hay al menos $\varphi(2023)$ elementos de orden 2023.

Para calcular $\varphi(2023)$, descomponemos 2023 en factores primos y vemos que $2023 = 7 \cdot (17)^2$. Aplicando las propiedades de la función φ de Euler vemos que

$$\varphi(2023) = \varphi(7)\varphi(17^2) = (7-1)(17^2-17) = 6 \cdot 272 = 1632.$$

Por tanto, podemos garantizar que en G hay al menos 1632 elementos de orden 2023, luego seguro que hay 1503 elementos de orden 2023.

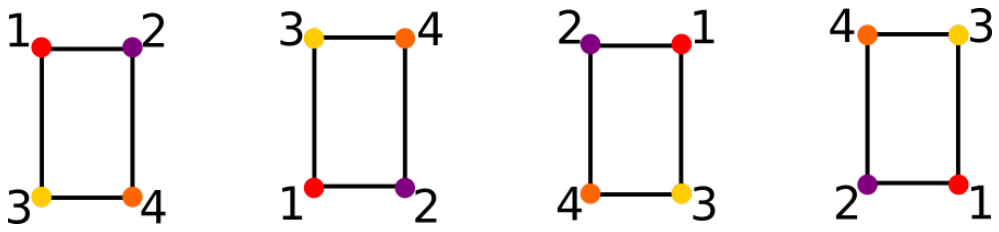
---

4. **[2 puntos - Ejercicios 21 y 44]** La Organización Mundial de los Colchones (OMC) recomienda cambiar de posición el colchón cada 3 meses. Pedro y Manuel, que siguen a pies juntillas las recomendaciones de la OMC, aprovechan el cambio de estación para modificar la posición del colchón. Sin embargo, nunca recuerdan en qué posición estaba el colchón la estación anterior. Por tanto, no saben en qué posición les toca poner el colchón esta vez y terminan siempre riñendo.

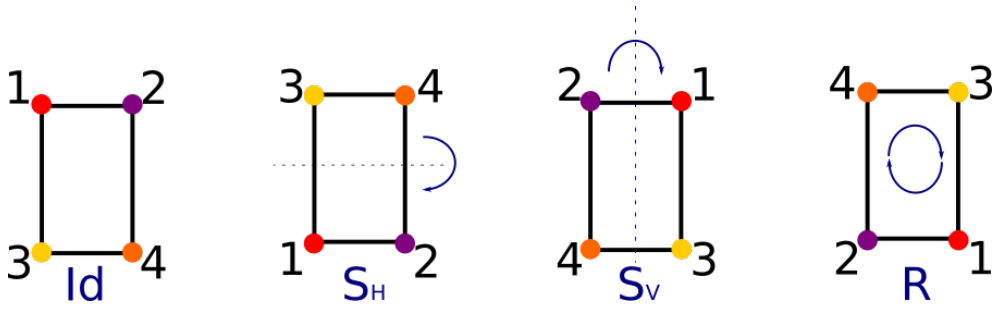
Manuel lleva un tiempo pensando que quizás exista una regla de oro: un movimiento del colchón que realizado de la misma forma cada estación les permita recorrer todas las posiciones de colchón al cabo de un tiempo. De esta forma no tendrían que recordar en qué posición estaba el colchón la estación anterior y se acabarían las discusiones. Pedro, que está estudiando el Grado en Matemáticas, observa que pueden eliminar los elementos superficiales y simplificar el problema: como su cama es 150×200 y no van a dormir sobre el canto del colchón, en realidad pueden suponer que el colchón es un rectángulo y que hay cuatro posiciones posibles.

Ayuda a Manuel y a Pedro. Describe el grupo de movimientos del colchón: ¿Cuál es su tabla?¿Es abeliano?¿Cuál es el orden de sus elementos?¿Cuáles son sus subgrupos?¿Cuál es su centro?¿Existe una regla de oro que realizada de la misma forma cada estación les permita recorrer todas las posiciones?

Solución. Tal y como se indica en el enunciado, tenemos que estudiar el grupo de isometrías del plano que dejan invariante un rectángulo que no es un cuadrado. Si numeramos las esquinas del rectángulo que representa al colchón tenemos que las cuatro posibles posiciones son:



Partiendo de la posición inicial: si no hacemos nada (la identidad), permanecemos en la posición inicial; si hacemos la simetría con respecto al eje horizontal, podemos llegar a la segunda posición; si hacemos la simetría con respecto al eje vertical llegamos a la tercera posición; y rotando 180^o, situamos el rectángulo en la cuarta posición.



Cualquier otro movimiento, por extraño que sea, nos tiene que conducir a una de las cuatro posibles posiciones del colchón y, por ende, será equivalente a alguno de los cuatro movimientos descritos. Por consiguiente, podemos concluir que el grupo de movimientos del colchón está formado por cuatro movimientos: La Identidad (Id), la Simetría horizontal (S_H), la simetría vertical (S_V) y la rotación de 180^o (R).

Operando construimos la tabla de este grupo:

	Id	S_H	S_V	R
Id	Id	S_H	S_V	R
S_H	S_H	Id	R	S_V
S_V	S_V	R	Id	S_H
R	R	S_V	S_H	Id

Se trata de un **grupo abeliano** porque su tabla es simétrica. Además todo elemento es su propio inverso, es decir, tenemos que

$$Id \circ Id = Id, \qquad S_H \circ S_H = Id, \qquad S_V \circ S_V = Id, \qquad R \circ R = Id.$$

En consecuencia, el **orden de los elementos** del grupo es $O(\mathrm{Id}) = 1$ y $O(S_H) = O(S_V) = O(R) = 2$. Dado T un subgrupo de nuestro grupo, tenemos que $Id \in T$. Consideramos las siguientes posibilidades:

(a) Si T no contiene más elementos, entonces $T = \{Id\} =< Id >$ que es un subgrupo.

(b) Si T contiene otro elemento, entonces tenemos que T contiene al subgrupo generado por ese elemento, es decir, $< S_H > \subseteq T$, $< S_V > \subseteq T$, o $< R > \subseteq T$. Si se da la igualdad en algún caso podemos concluir que T tiene dos elementos y que es de alguna de las tres formas siguientes:

$$(b.1)\ T =< S_H >= \{Id, S_H\}, \qquad (b.2)\ T =< S_V >= \{Id, S_V\}, \qquad (b.3)\ T =< R >= \{Id, R\}.$$

(c) Si T, además de la identidad, tiene otros dos elementos, como

$$S_H \circ S_V = R, \qquad S_H \circ R = S_V, \qquad S_V \circ R = S_H,$$

y, como T es subgrupo, podemos concluir que T tiene que tener al elemento que falta del grupo. En otras palabras, T no puede tener exactamente 3 elementos, es decir, en este caso $T = S$.

En resumen, el grupo G de movimientos del colchón tiene **cinco subgrupos**:

$$\{Id\} \qquad < S_H > \qquad < S_V > \qquad < R > \qquad G.$$

Como G es abeliano su **centro** es todo el grupo, es decir, $Z(G) = G$.

Finalmente, para saber si existe una regla de oro, un movimiento del colchón que realizado de la misma forma cada estación les permita recorrer todas las posiciones de colchón al cabo de un tiempo, tenemos que determinar si el grupo G es cíclico o no. Podemos ver que G **no es cíclico** de muchas formas:

Argumento 1: G no es cíclico porque $\#G = 4$ y G no tiene elementos de orden 4.

Argumento 2: G no es cíclico porque tiene dos elementos distintos de orden 2.

Argumento 3: G no es cíclico porque tiene dos subgrupos distintos de orden 2.

En conclusión, como G no es cíclico podemos afirmar que **no existe una regla de oro que realizada de la misma forma cada estación les permita recorrer todas las posiciones**.

UNIVERSIDAD DE CANTABRIA

SEGUNDA PRUEBA

miércoles 3 de mayo de 2023

G90 - Estructuras Algebraicas

Curso 2022-2023

Nombre y apellidos:

INSTRUCCIONES DE LA PRUEBA

- Las respuestas a las preguntas de la prueba deben escribirse con bolígrafo azul o negro.
- Está prohibido emplear lápiz, bolígrafos de otros colores y típex.
- No se permite el uso de calculadora ni de ningún otro dispositivo electrónico.
- No se permite el uso ni de apuntes, ni de libros, ni de ningún otro tipo de material bibliográfico.
- Antes de comenzar el examen, los dispositivos electrónicos y los materiales bibliográficos deben situarse, fuera del alcance del estudiante, en el espacio del aula reservado con esta finalidad.
- No se puede abandonar el aula antes de que haya transcurrido una hora desde el inicio de la prueba.
- El abandono del aula y/o el incumplimiento de estas normas supone la finalización del examen por parte del estudiante.
- Todas las respuestas deben estar justificadas correctamente.

1. **[2 puntos]** Define los siguientes conceptos:

(a) **[0,5 puntos]** Índice de una permutación.

Sea $\sigma \in S_n$ una permutación. Definimos el índice de σ como:

$$i(\sigma) = \begin{cases} 1 & \text{si } \sigma \text{ es par } (\sigma \text{ descompone en un número par de transposiciones}) \\ -1 & \text{si } \sigma \text{ es impar } (\sigma \text{ descompone en un número impar de transposiciones}) \end{cases}$$

(b) **[0,5 puntos]** Índice de un subgrupo.

Sea $(G,\bullet)$ un grupo y sea $S \subseteq G$ un subgrupo. Se define el **índice de S en G** como el cardinal del conjunto $\mathfrak{D}$ de clases a la derecha módulo S (o de $\mathfrak{I}$ porque coinciden) y se representa por $\#(G:S)$.

(c) **[0,5 puntos]** Divisor del cero.

Sea $(R,+,\cdot)$ un anillo conmutativo y $a \in R$ decimos que a **es un divisor del cero** cuando existe $c \in R$ tal que $c \neq 0_R$ tal que $a \cdot c = 0_R$.

(d) **[0,5 puntos]** Unidad de un anillo.

Sea $(R,+,\cdot)$ un anillo unitario y $a \in R$, decimos que a **es una unidad de** R si a tiene inverso para el producto, es decir, si existe $b \in R$ tal que $a \cdot b = b \cdot a = 1_R$.

2. [2 puntos] Demostrar el siguiente resultado:

Sea $\sigma \in S_n$ una permutación y $\sigma_1, \sigma_2, \ldots, \sigma_s \in S_n$ ciclos disjuntos de longitudes respectivas $\ell_1, \ell_2, \ldots, \ell_s \in \mathbb{N}_{\geq 1}$ tales que $\sigma = \sigma_1 \sigma_2 \cdots \sigma_s$. Entonces se cumple que

$$O(\sigma) = \text{m.c.m.}\,(\ell_1, \ell_2, \ldots, \ell_s) \quad \text{en} \quad (S_n, \circ).$$

Demostración (I.4.15). Escribimos $m := \text{m.c.m.}\,(\ell_1, \ell_2, \ldots, \ell_s)$. En primer lugar, veamos que $O(\sigma) \mid m$. Como los ciclos disjuntos conmutan, se cumple que

$$\sigma^m = (\sigma_1 \sigma_2 \cdots \sigma_s)^m = (\sigma_1 \sigma_2 \cdots \sigma_s) \cdots (\text{m veces}) \cdots (\sigma_1 \sigma_2 \cdots \sigma_s) = \sigma_1^m \sigma_2^m \cdots \sigma_s^m.$$

Como $\ell_i \mid m$ para todo $i \in \{1, 2, \ldots, s\}$, se tiene que existe $k_i \in \mathbb{N}_{\geq 1}$ tal que $\ell_i k_i = m$ y como $\sigma_i^{\ell_i} = \text{Id}$, deducimos que $\sigma_i^m = \text{Id}$ y que $\sigma^m = \text{Id}$. Por consiguiente, como $\#S_n < \infty$, tenemos que $O(\sigma)$ es finito y podemos aplicar las propiedades del orden para deducir que $O(\sigma) \mid m$.

Veamos que $m \mid O(\sigma)$. Sea $t := O(\sigma)$, luego $\sigma^t = \text{Id}$. Como los ciclos disjuntos conmutan, se cumple que

$$\text{Id} = \sigma^t = (\sigma_1 \sigma_2 \cdots \sigma_s)^t = \sigma_1^t \sigma_2^t \cdots \sigma_s^t.$$

Para cada $k \in \{1, 2, \ldots, n\}$ que σ_1 **deja fijo** se tiene que $\sigma_1(k) = k$ y que $\sigma_1^t(k) = k$.
Para cada $k \in \{1, 2, \ldots, n\}$ que σ_1 **no deja fijo**, como los ciclos son disjuntos, tenemos que $\sigma_i(k) = k$ para todo $i \in \{2, 3, \ldots, s\}$. En consecuencia, $k = \text{Id}(k) = \sigma^t(k) = \sigma_1^t(k)$.
En resumen, para todo $k \in \{1, 2, \ldots, n\}$ se tiene que $\sigma_1^t(k) = k$, es decir, $\sigma_1^t = \text{Id}$ y $\text{Id} = \sigma_2^t \cdots \sigma_r^t$.
Por las propiedades del orden, concluimos que $O(\sigma_1) \mid t$ o, escrito de otro modo, $\ell_1 \mid t$.
Realizando el mismo procedimiento con los ciclos restantes vemos que $\ell_i \mid t$ para todo $i \in \{1, 2, \ldots, s\}$. Por la definición del mínimo común múltiplo, podemos asegurar que $m \mid t$, es decir, $m \mid O(\sigma)$. Finalmente, como $O(\sigma) \mid m$ y como $m \mid O(\sigma)$, concluimos que $O(\sigma) = m$.

---

3. [4 puntos] Sea $(G, \cdot)$ un grupo. Recordamos que el centro de G está definido por

$$Z(G) = \{x \in G \ : \ \text{para todo } g \in G \text{ se tiene que } x \cdot g = g \cdot x \ \}.$$

(a) [1 punto] Probar que $Z(G)$ es un subgrupo normal de G.

Solución. (I.2.20+I.5.38) Probaremos que $Z(G)$ es un subgrupo de G en primer lugar.

Como $1_G \in Z(G)$, tenemos que $Z(G) \neq \emptyset$. Dados $x, y \in Z(G)$ y $g \in G$ tenemos que

$$xy^{-1}g = x(g^{-1}y)^{-1} \overset{y \in Z(G)}{=} x(yg^{-1})^{-1} = xgy^{-1} \overset{x \in Z(G)}{=} gxy^{-1}.$$

Por tanto, $x \cdot y^{-1} \in Z(G)$ y tenemos que $Z(G)$ es subgrupo de G.

Veamos ahora que $Z(G)$ es normal en G.

Tomamos $x \in Z(G)$ y $g \in G$ se tiene que

$$g^{-1}xg \overset{x \in Z(G)}{=} g^{-1}gx = 1_G x = x \in Z(G).$$

Por consiguiente, $Z(G)$ es normal en G.

(b) [1 punto] Suponemos el grupo cociente $G/Z(G)$ es cíclico. Probar que G es abeliano.

Solución. (Ejercicio 98) Si $G/Z(G)$ es cíclico, entonces existe $x \in G$ tal que $G/Z(G) = < xZ(G) >$. Dados $a, b \in G$ tenemos que $aZ(G), bZ(G) \in G/Z(G) = < xZ(G) >$, luego existen $j, k \in \mathbb{Z}$ tal que $aZ(G) = (xZ(G))^j$ y $bZ(G) = (xZ(G))^k$. Operando tenemos que

$$aZ(G) = x^j Z(G) \qquad bZ(G) = x^k Z(G),$$

y, por la definición de las clases laterales, $x^{-j}a = z_1 \in Z(G)$ y $x^{-k}b = z_2 \in Z(G)$, es decir, $a = z_1x^j$ y $b = z_2x^k$ con $z_1, z_2 \in Z(G)$. Por lo tanto, se tiene que

$$ab = z_1x^jz_2x^k \overset{z_1,z_2\in Z(G)}{=} x^{j+k}z_2z_1 \overset{\text{conmutativo}}{=\!=} x^{k+j}z_2z_1 \overset{z_1,z_2\in Z(G)}{=} z_2x^kz_1x^j = ba.$$

Por consiguiente, hemos probado que dados $a, b \in G$ se tiene que $ab = ba$, luego G es abeliano.

(c) [1 punto] Calcular $Z(D_{102})$.

Solución. Por los resultados probados sabemos que podemos representar D_{102} como

$$D_{102} = \{r^is^j \ : \ i \in \{0,1,2,3,\ldots,101\} \ j \in \{0,1\}\}.$$

donde $r^is^j = r^is^j$ si y sólo si $i = \ell$ y $j = k$. Además se cumple la relación $sr^k = r^{102-k}s$ para todo $k \in \{1,2,3,\ldots,102\}$ y tenemos que $O(s) = 2$ y que $O(r) = 102$.

En primer lugar, veamos que $\{r^0, r^{102}\} \subseteq Z(D_{102})$. Como $r^0 = \mathrm{Id}$ es el elemento neutro de D_{102} conmuta con todos los elementos de de D_{102}, luego $\mathrm{Id} \in Z(D_{102})$. Por otro lado, dada una rotación r^i con $i \in \{0,1,2,3,\ldots,101\}$ tenemos que

$$r^ir^{51} = r^{i+51} \overset{\text{conmutativo}}{=\!=} r^{51+i} = r^{51}r^i,$$

luego r^{51} conmuta con todas las rotaciones. Dada una simetría r^i con $i \in \{0,1,2,3,\ldots,101\}$ tenemos que

$$(r^is)r^{51} = r^ir^{102-51}s = r^{i+51}s \overset{\text{conmutativo}}{=\!=} r^{51+i}s = r^{51}(r^is),$$

luego r^{51} conmuta con todas las simetrías y concluimos que $r^{51} \in Z(D_{102})$.

En segundo lugar, veamos que $\{r^0, r^{102}\} = Z(D_{102})$, es decir, que el resto de elementos de D_{102} no están en el centro. Dada una rotación r^i con $i \in \{0,1,2,3,\ldots,101\}$ y con $i \notin \{0,51\}$ veamos que no conmuta con s. Tenemos que

$$sr^i = r^{102-i}s \neq r^is,$$

porque $i \neq 102 - i$ y $i, 102 - i \in \{1,\ldots,101\}$. Por otra parte, dada una simetría r^is con $i \in \{0,1,2,3,\ldots,101\}$ veamos que no conmuta con r. Tenemos que

$$(r^is)r = r^i(sr) = r^i(r^{101}s) \neq r^i(r^1s) = r^{i+1}s = r(r^is).$$

porque $r^{101} \neq r$. Por ende, los únicos elementos de D_{102} que conmutan con todos los elementos son Id y r^{51}, luego $Z(D_{102}) = \{\mathrm{Id}, r^{51}\}$.

(d) [1 punto] Probar que no puede existir un homomorfismo de grupos $f : D_{102} \to C$ tal que $\mathrm{Ker}(f) = \{\mathrm{Id}, r^{51}\}$ y donde C es un grupo cíclico.

Solución.(Ejercicio 98) Si existiera un homomorfismo de grupos $f : D_{102} \to C$ con C un grupo cíclico tal que $\mathrm{Ker}(f) = \{\mathrm{Id}, r^{51}\}$, por el Primer Teorema de Isomorfía tendríamos que

$$D_{102}/\mathrm{Ker}(f) \approx \mathrm{Im}(f).$$

Como C es cíclico y como $\mathrm{Im}(f)$ es un subgrupo de C, tenemos que $\mathrm{Im}(f) = C'$ es cíclico. Por otro lado, por el apartado **(c)** se tiene que $\mathrm{Ker}(f) = \{\mathrm{Id}, r^{51}\} = Z(D_{102})$, luego tendríamos que

$$D_{102}/Z(D_{102}) \approx C',$$

es decir, tendríamos que $D_{102}/Z(D_{102})$ es cíclico. Por el apartado **(b)**, esto significaría que D_{102} es abeliano lo que hemos probado en el apartado **(c)** que es falso. En consecuencia, no puede existir un homomorfismo con esas características.

4. **[2 puntos]** Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(a) **[1 punto]** $(\mathbb{Z},+,+)$ es un anillo conmutativo y unitario.*

Falso. (Ejercicio 131) $(\mathbb{Z},+,+)$ no es un anillo porque no se cumple la propiedad distributiva:

$$1+(1+1)=3\neq 4=(1+1)+(1+1).$$

(b) **[1 punto]** Sea $(R,+,\cdot)$ un anillo conmutativo y unitario e I y J_1,J_2 tres ideales tales que $I+J_1=R$ e $I+J_2=R$, entonces $I+(J_1\cap J_2)=R$.

Cierto. (Ejercicio II.2.26) Vemos en primer lugar que $1_R\in I+(J_1\cap J_2)$. Como $I+J_1=R$ e $I+J_2=R$, tenemos que $1_R\in I+J_1=R$ e $1_R\in I+J_2=R$, es decir, existen $x_1,x_2\in I$, $y_1\in J_1$ e $y_2\in J_2$ tales que

$$1_R=x_1+y_1 \qquad 1_R=x_2+y_2.$$

Multiplicando ambas expresiones

$$1_R=1_R\cdot 1_R=(x_1+y_1)(x_2+y_2)=x_1x_2+x_1y_2+y_1x_2+y_1y_2.$$

Como $x_1,x_2\in I$ e I es ideal se tiene que x_1x_2, x_1y_2, $y_1x_2\in I$, luego $x_1x_2+x_1y_2+y_1x_2\in I$. Por otro lado, como $y_1\in J_1$ se tiene que $y_1y_2\in J_1$ y como $y_2\in J_2$ se tiene que $y_1y_2\in J_2$, luego $y_1y_2\in J_1\cap J_2$. En resumen, se cumple que

$$1_R=\overbrace{x_1x_2+x_1y_2+y_1x_2}^{\in I}+\overbrace{y_1y_2}^{\in J_1\cap J_2},$$

es decir, $1_R\in I+(J_1\cap J_2)$. Ahora dado cualquier $r\in R$, como $1_R\in I+(J_1\cap J_2)$, por ser $I+(J_1\cap J_2)$ ideal, se tiene que $r=r1_R\in I+(J_1\cap J_2)$ y, en consecuencia, $I+(J_1\cap J_2)=R$.

*La primera operación es la suma habitual en $\mathbb{Z}$ y la segunda también, no es una errata. Se pueden emplear que las propiedades conocidas de la suma habitual en $\mathbb{Z}$ para responder a las preguntas, no es necesario demostrarlas.

UNIVERSIDAD DE CANTABRIA

EXAMEN FINAL
CONVOCATORIA ORDINARIA
miércoles 7 de junio de 2023

G90 - Estructuras Algebraicas

Curso 2022-2023

Nombre y apellidos:

INSTRUCCIONES DE LA PRUEBA

- Las respuestas a las preguntas de la prueba deben escribirse con bolígrafo azul o negro.
- Está prohibido emplear lápiz, bolígrafos de otros colores y típex.
- No se permite el uso de calculadora ni de ningún otro dispositivo electrónico.
- No se permite el uso ni de apuntes, ni de libros, ni de ningún otro tipo de material bibliográfico.
- Antes de comenzar el examen, los dispositivos electrónicos y los materiales bibliográficos deben situarse, fuera del alcance del estudiante, en el espacio del aula reservado con esta finalidad.
- No se puede abandonar el aula antes de que haya transcurrido una hora desde el inicio de la prueba.
- El abandono del aula y/o el incumplimiento de estas normas supone la finalización del examen por parte del estudiante.
- Todas las respuestas deben estar justificadas correctamente.

1. **[1 puntos]** Define los siguientes conceptos:

(a) **[0,2 puntos]** Relación de congruencia a la derecha en $(G,\cdot)$ módulo S.

(b) **[0,2 puntos]** Elemento irreducible de un dominio.

(c) **[0,4 puntos]** Dominio euclídeo.

(d) **[0,2 puntos]** Polinomio primitivo.

2. **[1+1=2 puntos]** Demuestra DOS de los siguientes TRES resultados:

(a) Sean $(G,\bullet)$ y $(H,\bullet)$ dos grupos, $f: G \to H$ un homomorfismo de grupos y $N \lhd G$ con $N \subseteq \mathrm{Ker}(f)$. Entonces:

(i) Existe un único homomorfismo $\overline{f}: G/N \to H$ tal que para todo $a \in G$ se tiene que $\overline{f}(aN) = f(a)$.

(ii) Si $N = \mathrm{Ker}(f)$, entonces $\overline{f}$ es inyectivo.

(b) Sea $(R,+,\cdot)$ un anillo, $n \in \mathbb{N}_{\geq 1}$ e $I_1, I_2, \ldots I_n \subseteq R$ ideales tales que se cumple que

$$(\star) \text{ para todo } j \in \{1,2,\ldots,n\} \qquad I_j + \bigcap_{k\in\{1,2,\ldots,n\},k\neq j} I_k = R,$$

entonces se tiene que

$$R/(I_1 \cap I_2 \cap \cdots \cap I_n) \qquad \approx \qquad R/I_1 \times R/I_2 \times \cdots \times R/I_n.$$

(c) Todo dominio de integridad finito es cuerpo.

Si se realizan las tres demostraciones sólo se evaluarán los apartados (a) y (b).

UNIVERSIDAD DE CANTABRIA

EXAMEN FINAL
CONVOCATORIA ORDINARIA
miércoles 7 de junio de 2023

G90 - Estructuras Algebraicas

Curso 2022-2023

Nombre y apellidos:

INSTRUCCIONES DE LA PRUEBA

- Las respuestas a las preguntas de la prueba deben escribirse con bolígrafo azul o negro.
- Está prohibido emplear lápiz, bolígrafos de otros colores y típex.
- No se permite el uso de calculadora ni de ningún otro dispositivo electrónico.
- No se permite el uso ni de apuntes, ni de libros, ni de ningún otro tipo de material bibliográfico.
- Antes de comenzar el examen, los dispositivos electrónicos y los materiales bibliográficos deben situarse, fuera del alcance del estudiante, en el espacio del aula reservado con esta finalidad.
- No se puede abandonar el aula antes de que haya transcurrido una hora desde el inicio de la prueba.
- El abandono del aula y/o el incumplimiento de estas normas supone la finalización del examen por parte del estudiante.
- Todas las respuestas deben estar justificadas correctamente.

3. **[2 puntos]** Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(a) **[0.5 puntos]** Dados dos grupos G y H, tenemos que todo subgrupo S del grupo producto $G \times H$ es el producto de un subgrupo A de G y un subgrupo B de H, es decir, $S = A \times B$.

Falso. Basta considerar $G = H = \mathbb{Z}/2\mathbb{Z}$ y $S = <(1,1)> = \{(0,0),(1,1)\}$ tenemos que los subgrupos de G (y de H) son $\{0\}$ y $\mathbb{Z}/2\mathbb{Z}$, pero $S \neq \{0\} \times \{0\}$, $S \neq \{0\} \times \mathbb{Z}/2\mathbb{Z}$, $S \neq \mathbb{Z}/2\mathbb{Z} \times \{0\}$ y $S \neq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b) **[0.5 puntos]** Dado G un grupo y $H \subsetneq G$ un subgrupo, entonces G no es isomorfo a H.

Falso. Basta considerar $G = \mathbb{Z}$ y $H = 2\mathbb{Z}$ que es un subgrupo propio. La aplicación $f : \mathbb{Z} \to 2\mathbb{Z}$ dada por $f(m) = 2m$ es un homomorfismo de grupos porque

$$f(m+n) = 2(m+n) = 2m + 2n = f(n) + f(m).$$

Además, f es inyectiva porque si $f(m) = 0$, entonces $2m = 0$, luego $m = 0$. También es sobreyectiva porque dado $x \in 2\mathbb{Z}$ tenemos que existe $k \in \mathbb{Z}$ tal que $x = 2k$, luego $f(k) = x$. Por tanto, se tiene que $(\mathbb{Z}, +)$ y $(2\mathbb{Z}, +)$ son grupos isomorfos.

(c) **[0.5 puntos]** Consideramos el polinomio $P(x) = x^{51} + x^{26} \in \mathbb{Z}/84\mathbb{Z}[x]$, se tiene que $P(5) = 66$ en $\mathbb{Z}/84\mathbb{Z}$.

Cierto. Recordamos que por el Teorema de Euler dice que dado $a \in \mathbb{Z}/n\mathbb{Z}$ tal que m.c.d. $(a,n) = 1$ se tiene que $a^{\varphi(n)} = 1$ en $\mathbb{Z}/n\mathbb{Z}$. Como m.c.d. $(5,84) = 1$ podemos usar este teorema para calcular las potencias de 5. Para ello calculamos $\varphi(84)$ como $84 = 3 \cdot 4 \cdot 7$ tenemos que $\varphi(84) = \varphi(3)\varphi(4)\varphi(7) = (3-1)(4-2)(7-1) = 24$. Por el Teorema de Euler tenemos que

$$P(5) = 5^{51} + 5^{26} = 5^{2 \cdot 24 + 3} + 5^{24+2} = 5^3 + 5^2 = 125 + 25 = 150.$$

Por tanto, se cumple que $P(5) = 66$ en $\mathbb{Z}/84\mathbb{Z}$.

(d) [0.5 puntos] Si R es un anillo conmutativo y unitario finito, entonces $\text{car}(R) > 0$.

Cierto. Como R es finito, tenemos que $(R,+)$ es un grupo finito. Por tanto, todo elemento de $(R,+)$ tiene orden finito, en particular $O(1_R) < \infty$. Como R es unitario, sabemos que $O(1_R) = \infty$ si y solo si $\text{car}(R) = 0$, como $O(1_R) < \infty$ concluimos que $\text{car}(R) > 0$.

---

4. [1 punto] Determinar razonadamente el menor valor de n para el cual existe $\sigma \in S_n$ tal que $O(\sigma) = 2023$ y el menor valor de m para el cual existe $\tau \in A_m$ tal que $O(\tau) = 76$.

Solución. En primer lugar, observamos que $2023 = 7 \cdot 17^2$ y que $76 = 2^2 \cdot 19$. Como el orden de toda permutación es el mínimo común multiplo del orden de los ciclos en los que descompone, para que $O(\sigma) = 2023$ y para que $O(\tau) = 76$ con $\sigma = \sigma_1\sigma_2\cdots\sigma_r$ y con $\tau = \tau_1\tau_2\cdots\tau_s$ debemos tener que

$$2023 = \text{m.c.m.}\,(O(\sigma_1), O(\sigma_2), \ldots, O(\sigma_r)) \quad \text{y} \quad 76 = \text{m.c.m.}\,(O(\tau_1), O(\tau_2), \ldots, O(\tau_s)).$$

En el caso de σ, podríamos conseguir una permutación de orden 2023 considerando un ciclo de orden 2023, luego podemos garantizar que $n \leq 2023$. Observamos que las permutaciones del tipo $(-7-)(-289-)$ también tiene orden $2023 = \text{m.c.m.}\,(7, 289)$. Como necesitamos que $(-7-)$ y $(-289-)$ sean ciclos disjuntos, sabemos que podemos encontrar permutaciones de este tipo necesitamos $7 + 289 = 296$ elementos. Veamos que este es el menor valor n posible para encontrar una permutación de orden 2023. Los divisores de 2023 son 1, 7, 17, 119, 289 y 2023, cualquier combinación de 1, 7, 17, 119, nos da como mínimo común múltiplo 119, luego para que 2023 sea el mínimo común múltiplo necesariamente uno de los ciclos tiene que tener longitud 289 o 2023. El segundo caso no nos interesa porque necesitaríamos que $n \geq 2023$. En el primero, si uno de los ciclos tiene longitud 289, la longitud de alguno de los otros ciclos debe ser 7 o 119 o 2023 para que el mínimo común múltiplo sea 2023. Por consiguiente, la forma de lograrlo permutando la menor cantidad de elementos posibles es con una permutación del tipo $(-7-)(-289-)$, es decir, $n = 296$.

Como τ tiene una descomposición en factores primos similar, razonando de manera análoga vemos que tomando $m = 2^2 + 19 = 23$ podemos garantizar que S_{23} contiene una permutación de tipo $(-4-)(-19-)$ luego que tiene orden 76 y para valores más pequeños de 23 ninguna combinación de los tipos nos da una permutación de orden 76. Sin embargo, no hemos acabado ya que las permutaciones del tipo $(-4-)(-19-)$ son impares por ser el producto de una permutación impar $(-4-)$ y una permutación par $(-19-)$, por ende, no pertenece al subgrupo A_{23}. Para lograr una permutación que tenga orden 76 y sea par necesitamos componer con otra transposición disjunta, esto no altera el orden dado que $76 = \text{m.c.m.}\,(4, 19) = \text{m.c.m.}\,(4, 19, 2)$. El tipo de la permutación es $(-2-)(-4-)(-19-)$, luego necesitamos $m = 2 + 4 + 19 = 25$ elementos para encontrar un elemento de este tipo.

---

5. [1 punto] Sean $(G,\cdot)$ un grupo finito, $k \in \mathbb{N}_{\geq 1}$ y H un subgrupo de G tal que $\#(G) = k \cdot \#(H)$. Probar que para todo $g \in G$ se tiene que $g^{k!} \in H$.

Solución. Como G es un grupo finito y $\#(G) = k \cdot \#(H)$, por el Teorema de Lagrange $\#(G : H) = k$, luego existen k clases laterales a la izquierda (o a la derecha) módulo H. Dado $g \in G$, consideramos las clases laterales de las potencias de g:

$$g^0H, \quad g^1H, \quad g^2H, \quad \ldots \quad g^{k-1}H, \quad g^kH.$$

Como son $k+1$ clases laterales, dos de ellas deben ser iguales, es decir, existen $i, j \in \{0, 1, \ldots, k\}$ con $i < j$ tal que $g^iH = g^jH$, luego $g^{-i}g^j \in H$, es decir, $g^{j-i} \in H$. Por ende, para todo $g \in G$ existe $\ell \in \{1, \ldots, k\}$ tal que $g^\ell \in H$. Concluimos observando que $k! = \ell \cdot \prod_{i=1, i\neq\ell}^{k} i$ y podemos escribir

$$g^{k!} = g^{\ell \cdot \prod_{i=1,i\neq\ell}^{k} i} = \left(g^\ell\right)^{\prod_{i=1,i\neq\ell}^{k} i} \in H,$$

que se cumple porque $g^\ell \in H$ y H es subgrupo.

6. **[3 puntos]** En el anillo producto $\mathbb{Z}\times\mathbb{Z}$ consideramos el subconjunto:

$$I_1 = \{(3k,3m) \ : \ k,m\in\mathbb{Z}\}.$$

(a) **[1 punto]** Probar que I_1 es un ideal de $\mathbb{Z}\times\mathbb{Z}$. Hallar un sistema completo de representante del anillo cociente $A_1 = \mathbb{Z}\times\mathbb{Z}/I_1$.

Solución. Para probar que I_1 es un ideal podríamos emplear el test de caracterización de ideales, pero alternativamente podemos escribir I_1 como el ideal generado por un elemento. En concreto, tenemos que

$$I_1 = \{(3k,3m) \ : \ k,m\in\mathbb{Z}\} = \{(k,m)\cdot(3,3) \ : \ (k,m)\in\mathbb{Z}\times\mathbb{Z}\} = \Big((3,3)\Big).$$

Por tanto, I_1 es un ideal. Para hallar un sistema completo de representante podríamos estudiar bajo que condiciones se cumple que $(a,b)+I_1 = (c,d)+I_1$. En este caso, también podemos considerar la aplicación

$$\begin{array}{rccc} F: & \mathbb{Z}\times\mathbb{Z} & \to & \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z} \\ & (a,b) & \to & F(a,b) = (a+3\mathbb{Z}, b+3\mathbb{Z}) \end{array}$$

Tenemos que F es un homomorfismo de anillos porque en cada componente es un homomorfismo de anillos, la aplicación de paso al cociente. Dado un elemento $x\in\mathbb{Z}/3\mathbb{Z}$ sabemos que es de la forma $x = (c+3\mathbb{Z}, d+3\mathbb{Z})$ con $c,d\in\{0,1,2\}$, luego $F(c,d) = x$, es decir, F es sobreyectivo. Por último, observamos que $(a,b)\in\ker(F)$ si y sólo si $(a+3\mathbb{Z}, b+3\mathbb{Z}) = (0+3\mathbb{Z}, 0+3\mathbb{Z})$, es decir, $a\in 3\mathbb{Z}$ y $b\in 3\mathbb{Z}$. Por ende, se tiene que

$$\mathrm{Ker}(F) = \{(a,b) \ : \ a,b\in 3\mathbb{Z}\} = \{(3k,3m) \ : \ k,m\in\mathbb{Z}\} = I_1.$$

Por el Primer Teorema de Isomorfía, tenemos que $\mathbb{Z}\times\mathbb{Z}/I_1 \approx \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, luego para hallar un sistema completo de representante del anillo cociente $A_1 = \mathbb{Z}\times\mathbb{Z}/I_1$ basta con calcular la contraimagen por F de cada uno de los nueve elementos de $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$. En conclusión, se tiene que un sistema completo de representantes de A_1 es

$$\{(0,0)+I_1,\ (1,0)+I_1,\ (2,0)+I_1,\ (0,1)+I_1,\ (1,1)+I_1,\ (2,1)+I_1,\ (0,2)+I_1,\ (1,2)+I_1,\ (2,2)+I_1\}.$$

(b) **[1 punto]** En anillo de los enteros de Gauss $\mathbb{Z}[i]$ y en el anillo de los polinomios con coeficientes en $\mathbb{Z}/3\mathbb{Z}$ consideramos los anillos cocientes $A_2 = \mathbb{Z}[i]/(3)$ y $A_3 = \mathbb{Z}/3\mathbb{Z}[x]/(x^2+2)$. Estudiar si los anillos A_2 y A_3 son dominios y/o cuerpos.

Solución. Como $\mathbb{Z}[i]$ es un Dominio Euclideo, para saber si $A_2 = \mathbb{Z}[i]/(3)$ es cuerpo basta saber si (3) es maximal. Como todo Dominio Euclideo es Dominio de Ideales Principales y en un D.I.P. son equivalentes (a) es maximal si y solo si a es irreducible, basta saber si $a=3$ es irreducible en $\mathbb{Z}[i]$ o no. Consideramos la aplicación $N:\mathbb{Z}[i]\to\mathbb{N}$ tal que $N(a+bi) = a^2+b^2$. Recordamos que $u\in\mathbb{Z}[i]$ es unidad si y solo si $N(u)=1$. Suponemos que $3=\alpha\beta$ con $\alpha,\beta\in\mathbb{Z}[i]$ y vemos que necesariamente alguno de los dos es una unidad. Aplicando N tenemos que $N(\alpha)N(\beta) = N(3) = 9$, luego tenemos dos posibilidades $N(\alpha)=1$ y $N(\beta)=9$ (Análogo $N(\alpha)=9$ y $N(\beta)=1$) o $N(\alpha)=N(\beta)=3$. En primer caso tenemos la situación deseada. Veamos que el segundo caso es imposible. Si $\alpha = a+bi$, tendríamos que $3 = N(\alpha) = a^2+b^2$, pero la ecuación $3=a^2+b^2$ no tiene soluciones $a,b\in\mathbb{Z}$. Si existiera solución tendríamos que $0\le a^2\le 3$ y $0\le b^2\le 3$, luego $a,b\in[-\sqrt{3},\sqrt{3}]\cap\mathbb{Z} = \{-1,0,1\}$ comprobando casos vemos que es imposible. En consecuencia, el segundo caso es no se puede dar y tenemos que 3 es irreducible en $\mathbb{Z}[i]$. En conclusión, $A_2 = \mathbb{Z}[i]/(3)$ es cuerpo y como todo cuerpo es dominio, tenemos que A_2 es dominio.
De un modo análogo, como $\mathbb{Z}/3\mathbb{Z}$ es cuerpo $\mathbb{Z}/3\mathbb{Z}[x]$ es Dominio Euclideo, luego A_3 es cuerpo si y solo si x^2+2 es irreducible en $\mathbb{Z}/3\mathbb{Z}[x]$. En este caso, observamos que $x^2+2 = (x+1)(x+2)$ como $U(\mathbb{Z}/3\mathbb{Z}[x]) = U(\mathbb{Z}/3\mathbb{Z}) = (\mathbb{Z}/3\mathbb{Z})\backslash\{0\}$, deducimos que x^2+2 no es irreducible, luego A_3 no es cuerpo. Tampoco es dominio porque recordamos que en un D.I.P. todo ideal primo es maximal, luego (x^2+2) no es primo y tenemos que A_3 no es dominio.

(c) [1 puntos] Justificar razonadamente si los anillos A_1, A_2, A_3 son isomorfos o no.

Solución. Observamos que A_1 no es cuerpo porque $(1,0)+I_1 \cdot (0,1)+I_1 = (0,0)+I_1$, es decir, A_1 tiene divisores del cero no nulos, luego no es dominio ni es cuerpo. Como A_2 es cuerpo y A_1,A_3 no lo son, deducimos que A_2 no es isomorfo a ninguno de ellos.

Por tanto, basta estudiar si A_1 y A_3 son isomorfos o no. Como $x^2+2 = (x+1)(x+2)$ si llamamos $J_1 = (x+1)$ y $J_2 = (x+2)$ a los ideales generados por los respectivos elementos. Observamos que

$$1 = 2(x+1) \; + \; x+2 \in J_1 + J_2.$$

Por tanto, se tiene que $J_1 + J_2 = \mathbb{Z}/3\mathbb{Z}[x]$ y, por el Teorema Chino del Resto, tenemos que

$$\mathbb{Z}/3\mathbb{Z}[x]/J_1 \times \mathbb{Z}/3\mathbb{Z}[x]/J_2 \approx \mathbb{Z}/3\mathbb{Z}[x]/J_1J_2.$$

Observamos que $J_1J_2 = \Big(x+1\Big)\Big(x+2\Big) = \Big(x^2+2\Big)$. En otras palabras, hemos probado que

$$\mathbb{Z}/3\mathbb{Z}[x]/J_1 \times \mathbb{Z}/3\mathbb{Z}[x]/J_2 \approx A_3.$$

Consideramos las aplicaciones de evaluación

$$\begin{array}{rccc} e_2: & \mathbb{Z}/3\mathbb{Z}[x] & \to & \mathbb{Z}/3\mathbb{Z} \\ & P(x) & \to & P(2) \end{array} \qquad\qquad \begin{array}{rccc} e_1: & \mathbb{Z}/3\mathbb{Z}[x] & \to & \mathbb{Z}/3\mathbb{Z} \\ & P(x) & \to & P(1) \end{array}$$

Resulta que son homomorfismos de anillos sobreyectivos y que $\mathrm{Ker}(e_2) = \Big(x+1\Big) = J_1$ y que $\mathrm{Ker}(e_1) = \Big(x+2\Big) = J_2$. Por el Primer Teorema de Isomorfía, se tiene que $\mathbb{Z}/3\mathbb{Z}[x]/J_1 \approx \mathbb{Z}/3\mathbb{Z}$ y también que $\mathbb{Z}/3\mathbb{Z}[x]/J_2 \approx \mathbb{Z}/3\mathbb{Z}$ y deducimos que

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \approx \mathbb{Z}/3\mathbb{Z}[x]/J_1 \times \mathbb{Z}/3\mathbb{Z}[x]/J_2 \approx A_3.$$

Por lo probado en el apartado (a), concluimos que $A_1 \approx A_3$.

UNIVERSIDAD DE CANTABRIA

EXAMEN FINAL
CONVOCATORIA EXTRAORDINARIA
jueves 29 de junio de 2023

G90 - Estructuras Algebraicas

Curso 2022-2023

Nombre y apellidos:

INSTRUCCIONES DE LA PRUEBA

- Las respuestas a las preguntas de la prueba deben escribirse con bolígrafo azul o negro.
- Está prohibido emplear lápiz, bolígrafos de otros colores y típex.
- No se permite el uso de calculadora ni de ningún otro dispositivo electrónico.
- No se permite el uso ni de apuntes, ni de libros, ni de ningún otro tipo de material bibliográfico.
- Antes de comenzar el examen, los dispositivos electrónicos y los materiales bibliográficos deben situarse, fuera del alcance del estudiante, en el espacio del aula reservado con esta finalidad.
- No se puede abandonar el aula antes de que haya transcurrido una hora desde el inicio de la prueba.
- El abandono del aula y/o el incumplimiento de estas normas supone la finalización del examen por parte del estudiante.
- Todas las respuestas deben estar justificadas correctamente.

1. **[1.5 puntos]** Define los siguientes conceptos:

(a) **[0.3 puntos]** Grupo.

(b) **[0.2 puntos]** Subgrupo normal.

(c) **[0.2 puntos]** Producto de ideales.

(d) **[0.2 puntos]** Ideal maximal.

(e) **[0.2 puntos]** Elemento primo de un dominio.

(f) **[0.4 puntos]** Dominio de factorización única.

2. **[1+1=2 puntos]** Demuestra DOS de los siguientes TRES resultados:

(a) Sea $(G,\bullet)$ un grupo cíclico finito, es decir, $\#G = n \in \mathbb{N}_{\geq 1}$ y existe $a \in G$ tal que $G =< a >$. Se cumple que:

(I) para cualquier $d \in \mathbb{N}$ divisor de n, G posee sólo un subgrupo de orden d: $G_d :=< a^{n/d} >$.
(II) para cualquier $d \in \mathbb{N}$ divisor de n, se cumple la igualdad $G_d = \{b \in G : O(b) \mid d\}$.

(b) Sean $(G,\bullet)$ un grupo, $N \lhd G$ y sea G/N el conjunto de clases de equivalencia módulo N en G. Definimos la operación:

$$\begin{array}{rccc} \boxdot: & G/N \times G/N & \to & G/N \\ & (aN, bN) & \to & (ab)N \end{array}$$

Entonces $(G/N, \boxdot)$ es un grupo.

(c) Todo dominio euclídeo es dominio de ideales principales.

Si se realizan las tres demostraciones, sólo se evaluarán los apartados (a) y (b).

UNIVERSIDAD DE CANTABRIA

EXAMEN FINAL
CONVOCATORIA EXTRAORDINARIA
jueves 29 de junio de 2023

G90 - Estructuras Algebraicas
Curso 2022-2023

Nombre y apellidos:

INSTRUCCIONES DE LA PRUEBA

- Las respuestas a las preguntas de la prueba deben escribirse con bolígrafo azul o negro.
- Está prohibido emplear lápiz, bolígrafos de otros colores y típex.
- No se permite el uso de calculadora ni de ningún otro dispositivo electrónico.
- No se permite el uso ni de apuntes, ni de libros, ni de ningún otro tipo de material bibliográfico.
- Antes de comenzar el examen, los dispositivos electrónicos y los materiales bibliográficos deben situarse, fuera del alcance del estudiante, en el espacio del aula reservado con esta finalidad.
- No se puede abandonar el aula antes de que haya transcurrido una hora desde el inicio de la prueba.
- El abandono del aula y/o el incumplimiento de estas normas supone la finalización del examen por parte del estudiante.
- Todas las respuestas deben estar justificadas correctamente.

3. [2 puntos] Sea $(G,*)$ el grupo producto $(\mathbb{Z}/4\mathbb{Z},+)\times(U(\mathbb{Z}/4\mathbb{Z}),\cdot)$ con las operaciones componente a componente. Consideramos los subgrupos $H=<(2,3)>$ y $K=<(2,1)>$.

(a) [1 punto] Probar que $H\approx K$. ¿Se cumple que $G/K\approx G/H$?

Solución. En primer lugar observamos que el elemento neutro de $(G,*)$ es $1_G=(0,1)$. Tenemos que

$$(2,3)*(2,3)=(2+2,3\cdot 3)=(0,1) \qquad \text{y} \qquad (2,1)*(2,1)=(2+2,1\cdot 1)=(0,1),$$

luego se tiene que $O((2,3))=O((2,1))=1$. Por tanto, $H=<(2,3)>$ y $K=<(2,1)>$ son cíclicos de orden 2 y, por la unicidad de los grupos cíclicos, son isomorfos $H\approx K$.

Veamos que $G/K\not\approx G/H$. Observamos que $\#(G)=4\cdot 2=8$, luego $\#(G/K)=\#(G/H)=8/2=4$. Para probar que son isomorfos basta ver que uno es cíclico y el otro no. Calculamos las clases laterales de G/H:

$$(0,1)*H=\{(0,1),(2,3)\}, \qquad (1,1)*H=\{(1,1),(3,3)\},$$
$$(2,1)*H=\{(2,1),(0,3)\}, \qquad (3,1)*H=\{(3,1),(1,3)\}.$$

Observamos que $(1,1)*H\cdot(1,1)*H=(2,1)*H$ y que $(1,1)*H\cdot(2,1)*H=(3,1)*H$, luego $O((1,1)*H)=4$. Por tanto, tenemos que $G/H=<(1,1)*H>$ es cíclico. Por otra parte, calculamos las clases laterales de G/K:

$$(0,1)*K=\{(0,1),(2,1)\}, \qquad (1,1)*K=\{(1,1),(3,1)\},$$
$$(0,3)*K=\{(0,3),(2,3)\}, \qquad (3,3)*K=\{(3,3),(1,3)\}.$$

En este caso se tiene que

$$(0,1)*K\cdot(0,1)*K=(0,1)*K, \qquad (1,1)*K\cdot(1,1)*K=(2,1)*K=(0,1)*K,$$
$$(0,3)*K\cdot(0,3)*K=(0,1)*K, \qquad (3,3)*K\cdot(3,3)*K=(2,1)*K=(0,1)*K.$$

En conclusión se tiene que G/K no tiene elementos de orden 4, luego no es cíclico. En resumen, se cumple que $G/K\not\approx G/H$.

(b) [1 punto] Justifica razonadamente, si es posible encontrar cuatro grupos con $\#(G)$ elementos que no sean isomorfos entre sí y que no sean isomorfos a G.

Solución. En primer lugar observamos que G es isomorfo a $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ considerando el isomorfismo

$$\begin{array}{rcl} G=(\mathbb{Z}/4\mathbb{Z},+)\times(U(\mathbb{Z}/4\mathbb{Z}),\cdot) & \to & \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} \\ (a,1) & \mapsto & (a,0) \\ (a,3) & \mapsto & (a,1) \end{array}$$

Por tanto, $(\mathbb{Z}/8\mathbb{Z},+)$ es un grupo con $\#(G)=8$ elementos que no es isomorfo a G porque es cíclico y G no lo es. Por otro lado, $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ es otro grupo con 8 elementos que no es isomorfo ni a G ni a $(\mathbb{Z}/8\mathbb{Z},+)$ porque no tiene elementos de orden 4.
Por otra parte, D_4 es otro grupo con 8 elementos que no es isomorfo ni a G ni a $(\mathbb{Z}/8\mathbb{Z},+)$ ni a $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ porque no es abeliano. Finalmente, Q_8 es un grupo con 8 elementos que no es isomorfo ni a G ni a $(\mathbb{Z}/8\mathbb{Z},+)$ ni a $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ porque no es abeliano. Tenemos que Q_8 y D_4 no son abelianos porque $D_4=<r,s>$ tiene dos elementos de orden 4: r y r^3, mientras que Q_8 tiene 6: $i,-i,j,-j,k,-k$.
En conclusión, sí es posible encontrar cuatro grupos con 8 elementos que no sean isomorfos entre sí y que no sean isomorfos a G: $(\mathbb{Z}/8\mathbb{Z},+)$, $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$, D_4 y Q_8.

---

4. [1 punto] Determinar razonadamente todos los homomorfismos de grupos que existen entre los grupos $(\mathbb{Z}/2023\mathbb{Z},+)$ y $(\mathbb{Z}/629\mathbb{Z},+)$ y todos los homomorfismos de anillos entre $(\mathbb{Z}/2023\mathbb{Z},+,\cdot)$ y $(\mathbb{Z}/629\mathbb{Z},+,\cdot)$.
Solución. Comenzamos determinando los homomorfismos de grupos entre $(\mathbb{Z}/2023\mathbb{Z},+)$ y $(\mathbb{Z}/629\mathbb{Z},+)$. Como $(\mathbb{Z}/2023\mathbb{Z},+)$ es cíclico todo homomorfismo de grupos está determinando por la imagen de un generador, en este caso, basta estudiar las posibles imágenes de $1_{\mathbb{Z}/2023\mathbb{Z}}$. Como $f(1_{\mathbb{Z}/2023\mathbb{Z}})\in\mathbb{Z}/629\mathbb{Z}$ tenemos que $O(f(1_{\mathbb{Z}/2023\mathbb{Z}}))\mid 629$. Por otro lado, se cumple que $O(f(1_{\mathbb{Z}/2023\mathbb{Z}}))\mid O(1_{\mathbb{Z}/2023\mathbb{Z}})=2023$, luego $O(f(1_{\mathbb{Z}/2023\mathbb{Z}}))\mid \text{m.c.d.}\,(2023,629)$. Empleando el Algoritmo de Euclides calculamos m.c.d. $(2023,629)$:

$$\begin{array}{rcccc} 2023 & = & 2023\cdot(1) & + & 629\cdot(0). \\ 629 & = & 2023\cdot(0) & + & 629\cdot(1). \\ 136 & = & 2023\cdot(1) & + & 629\cdot(-3). \\ 85 & = & 2023\cdot(-4) & + & 629\cdot(13). \\ 51 & = & 2023\cdot(5) & + & 629\cdot(-16). \\ 34 & = & 2023\cdot(-9) & + & 629\cdot(29). \\ 17 & = & 2023\cdot(14) & + & 629\cdot(-45). \\ 0 & = & \cdots & + & \cdots. \end{array}$$

En consecuencia, se tiene que m.c.d. $(2023,629)=17$, luego $O(f(1_{\mathbb{Z}/2023\mathbb{Z}}))\mid 17$. Podemos afirmar que $O(f(1_{\mathbb{Z}/2023\mathbb{Z}}))$ sebe estar en el único subgrupo de orden 17 de $(\mathbb{Z}/629\mathbb{Z},+)$ que es

$$<\frac{629}{17}1_{\mathbb{Z}/629\mathbb{Z}}>=<37>=\{0,37,74,111,148,185,222,259,296,333,370,407,444,481,518,555,592\}.$$

Por tanto, los 17 posibles homomorfismos de grupos entre $(\mathbb{Z}/2023\mathbb{Z},+)$ y $(\mathbb{Z}/629\mathbb{Z},+)$ son:

$$f_0(x)=0,\quad f_{37}(x)=37x,\quad f_{74}(x)=74x,\quad f_{111}(x)=111x,\quad f_{148}(x)=148x,\quad f_{185}(x)=185x,$$

$$f_{222}(x)=222x,\ f_{259}(x)=259x,\ f_{296}(x)=296x,\ f_{333}(x)=333x,\ f_{370}(x)=370x,\ f_{407}(x)=407x,$$

$$f_{444}(x)=444x,\quad f_{481}(x)=481x,\quad f_{518}(x)=518x,\quad f_{555}(x)=555x,\quad f_{592}(x)=592x.$$

Veamos ahora los posibles homomorfismos de anillos entre $\mathbb{Z}/2023\mathbb{Z}$ y $\mathbb{Z}/629\mathbb{Z}$. Como todo homomorfismo de anillos es homomorfismo de grupos entre los grupos aditivos, tenemos que estudiar cuáles de los homomorfismos anteriores son además homomorfismos de anillos. Observamos que $f(1)=f(1\cdot 1)=f(1)\cdot f(1)$, luego $f(1)$ debe ser idempotente. En consecuencia, buscamos los elementos idempotentes de $\mathbb{Z}/629\mathbb{Z}$ que estén en $<37>$. Se puede proceder de varias formas, una de ellas sería comprobar caso a caso qué elementos de $<37>$ son idempotentes. Como el tiempo

es limitado, debemos tratar de reducir el problema a un problema más sencillo. Como $629 = 17 \cdot 37$ y 17 y 37 son primos, por el Teorema chino del resto tenemos el siguiente isomorfismo de anillos:

$$\begin{array}{rcl} \Psi : \mathbb{Z}/629\mathbb{Z} & \to & \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/37\mathbb{Z} \\ a + 629\mathbb{Z} & \mapsto & (a + 17\mathbb{Z}, a + 37\mathbb{Z}) \end{array}$$

Observamos que $a + 629\mathbb{Z}^2 = a + 629\mathbb{Z}$ si y solo si $(a^2 + 17\mathbb{Z}, a^2 + 37\mathbb{Z}) = (a + 17\mathbb{Z}, a + 37\mathbb{Z})$, es decir, si y solo si $a + 17\mathbb{Z}$ y $a + 37\mathbb{Z}$ son idempotentes. Como $\mathbb{Z}/17\mathbb{Z}$, $\mathbb{Z}/37\mathbb{Z}$ son cuerpos, si $a^2 = a$, entonces $a(a-1) = 0$ y como todo cuerpo no tiene divisores de cero no nulos, tenemos que $a = 0$ o $a = 1$. Por tanto, los elementos idempotentes de $\mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/37\mathbb{Z}$ son $(0,0)$, $(0,1)$, $(1,0)$ y $(1,1)$. Para concluir basta calcular su pontra imagen por Ψ, es decir, tenemos que resolver 4 sistemas de congruencias:

$$\begin{cases} x \equiv 0 & \text{mód } 17 \\ x \equiv 0 & \text{mód } 37 \end{cases} \qquad \begin{cases} x \equiv 1 & \text{mód } 17 \\ x \equiv 0 & \text{mód } 37 \end{cases} \qquad \begin{cases} x \equiv 0 & \text{mód } 17 \\ x \equiv 1 & \text{mód } 37 \end{cases} \qquad \begin{cases} x \equiv 1 & \text{mód } 17 \\ x \equiv 1 & \text{mód } 37 \end{cases}$$

Para ello, calculamos la Identidad de Bézout entre 17 y 37.

$$\begin{array}{rcccl} 37 & = & 37 \cdot (1) & + & 17 \cdot (0). \\ 17 & = & 37 \cdot (0) & + & 17 \cdot (1). \\ 3 & = & 37 \cdot (1) & + & 17 \cdot (-2). \\ 2 & = & 37 \cdot (-5) & + & 17 \cdot (11). \\ 1 & = & 37 \cdot (6) & + & 17 \cdot (-13). \\ 0 & = & \cdots & + & \cdots. \end{array}$$

Luego 6 es el inverso de 37 en $\mathbb{Z}/17\mathbb{Z}$ y $-13 = 24$ es el inverso de 17 en $\mathbb{Z}/37\mathbb{Z}$. Tenemos que las soluciones de los respectivos sistemas de congruencias son:

$$x \equiv 0 \quad \text{mód } 629 \qquad\qquad x \equiv 1 \cdot 37 \cdot 6 + 0 \cdot 17 \cdot 24 \equiv 222 \quad \text{mód } 629$$

$$x \equiv 0 \cdot 37 \cdot 6 + 1 \cdot 17 \cdot 24 \equiv 408 \quad \text{mód } 62 \qquad\qquad x \equiv 1 \cdot 37 \cdot 6 + 1 \cdot 17 \cdot 24 \equiv 1 \quad \text{mód } 629$$

Por tanto, los dos únicos posibles homomorfismos de anillos son $f_0(x) = 0$ y $f_{222}(x) = 222x$. Comprobamos de forma directa que ambos son homomorfismos de anillos entre $(\mathbb{Z}/2023\mathbb{Z}, +, \cdot)$ y $(\mathbb{Z}/629\mathbb{Z}, +, \cdot)$.

---

5. **[2 puntos]** En el anillo de polinomios $\mathbb{Z}/5\mathbb{Z}[x]$, consideramos los polinomios

$$P_1(x) = x^3 + x^2 + 2x + 2, \qquad P_2(x) = x^3 + 4x^2 + 2x + 3.$$

Denotamos por $I = (P_1(x),\ P_2(x))$ al ideal generado por estos dos polinomios.

(a) **[1 punto]** Encontrar $P(x) \in \mathbb{Z}/5\mathbb{Z}[x]$ tal que $I = (P(x))$, ¿es el anillo cociente $A = \mathbb{Z}/5\mathbb{Z}[x]/I$ un cuerpo?

Solución. Observamos que

$$I = (P_1(x),\ P_2(x)) = \{Q_1(x)P_1(x) + Q_2(x)P_2(x)\ :\ Q_1(x), Q_2(x) \in \mathbb{Z}/5\mathbb{Z}[x]\} = (P_1(x)) + (P_2(x)).$$

Por tanto, como $\mathbb{Z}/5\mathbb{Z}[x]$ es un dominio euclídeo porque $\mathbb{Z}/5\mathbb{Z}$ es cuerpo podemos emplear el algoritmo de euclides para encontrar el máximo comun divisor de $P_1(x)$ y $P_2(x)$:

$$\begin{array}{rcccl} x^3 + x^2 + 2x + 2 & = & x^3 + x^2 + 2x + 2 \cdot (1) & + & x^3 + 4x^2 + 2x + 3 \cdot (0). \\ x^3 + 4x^2 + 2x + 3 & = & x^3 + x^2 + 2x + 2 \cdot (0) & + & x^3 + 4x^2 + 2x + 3 \cdot (1). \\ 2x^2 + 4 & = & x^3 + x^2 + 2x + 2 \cdot (1) & + & x^3 + 4x^2 + 2x + 3 \cdot (4). \\ 0 & = & \cdots & + & \cdots. \end{array}$$

Por tanto un máximo común divisor de $P_1(x)$ y $P_2(x)$ es $2x^2 + 4$ multiplicando por 3 para hacerlo mónico tomamos $P(x) = x^2 + 2$. Por la Identidad de Bézout, se tiene que $I = (P_1(x)) + (P_2(x)) = (P(x))$ porque $\mathbb{Z}/5\mathbb{Z}[x]$ es un dominio de ideales principales.

Por otro lado, para saber si $A = \mathbb{Z}/5\mathbb{Z}[x]/I$ es un cuerpo, como $\mathbb{Z}/5\mathbb{Z}[x]$ es dominio de ideales principales, basta saber si $P(x)$ es irreducible en $\mathbb{Z}/5\mathbb{Z}[x]$. Un polinomio de grado 2 en $\mathbb{Z}/5\mathbb{Z}[x]$ es irreducible si y sólo si no tiene raíces. Observamos que

$$P(0) = 2, \qquad P(1) = 3, \qquad P(2) = 1, \qquad P(3) = 1, \qquad P(4) = 3.$$

Por consiguiente, $P(x)$ es irreducible en $\mathbb{Z}/5\mathbb{Z}[x]$ y se cumple que $A = \mathbb{Z}/5\mathbb{Z}[x]/I$ es un cuerpo.

(b) [1 punto] Consideramos $\alpha = x^3 + 4x + 4 + I \in A$. Escribir α de la forma $\alpha = ax + b + I$ con $a, b \in \mathbb{Z}/5\mathbb{Z}$ y encontrar α^{-1} en A.

Solución. Para calcular el representante buscado tenemos que que calcular el resto de dividir $x^3 + 4x + 4$ entre $P(x) = x^2 + 2$. En este caso, se tiene que

$$x^3 + 4x + 4 = x \cdot P(x) + 2x + 4,$$

luego $a = 1$, $b = 4$ y $\alpha = 2x + 4 + I$. Para concluir y calcular su inverso calculamos la identidad de Bézout de $P(x)$ y $2x + 4$:

$$\begin{array}{rcl} x^2+2 & = & x^2 + 2\cdot(1) + 2x + 4\cdot(0). \\ 2x+4 & = & x^2 + 2\cdot(0) + 2x + 4\cdot(1). \\ 1 & = & x^2 + 2\cdot(1) + (2x+4)\cdot(2x+1). \\ 0 & = & \cdots + \cdots. \end{array}$$

Tomando clases concluimos que $\alpha = 2x + 4 + I$ y $\alpha^{-1} = 2x + 1 + I$ en A.

---

6. [1.5 puntos] Justificar, realizando la demostración o ilustrándolo con un contraejemplo, si las afirmaciones siguientes, consideradas de forma independiente, son ciertas o falsas.

(a) [0.5 puntos] Sea G un grupo finito. Entonces para cada $d \in \mathbb{N}$ con $d \mid \#(G)$, con $d \neq \#(G)$ siempre hay un elemento $x \in G$ de orden d.

Falso. Basta considerar el grupo producto $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Tenemos que $\#(G) = 8$ y que $4 \mid 8$, pero dado un elemento de $x = (a, b, c) \in G$ tenemos que $x + x = (0, 0, 0)$, luego $O(x) \mid 2$. En otras palabras, G no tiene elementos de orden 4 porque todos los elementos tienen orden 1 o 2.

(b) [0.5 puntos] El grupo $\mathbb{Z} \times \mathbb{Z}/ < (4,2) >$ es cíclico.

Falso. Para probar que $\mathbb{Z} \times \mathbb{Z}/ < (4,2) >$ no es cíclico basta ver que no es isomorfo ni a $(\mathbb{Z}, +)$ ni a $(\mathbb{Z}/n\mathbb{Z}, +)$ con $n \in \mathbb{N}_{\geq 1}$. Observamos que

$$< (4,2) >= \{(4k, 2k) \ : \ k \in \mathbb{Z}\}.$$

Consideramos el elemento $\alpha = (1,0) + < (4,2) > \in \mathbb{Z} \times \mathbb{Z}/ < (4,2) >$ y calculamos su orden. Resulta que

$$m\alpha = (m,0) + < (4,2) > \neq (0,0) + < (4,2) >$$

para todo $m \in \mathbb{N}_{\geq 1}$ porque $(m,0) \notin < (4,2) > = \{(4k, 2k) \ : \ k \in \mathbb{Z}\}$ si $m \in \mathbb{N}_{\geq 1}$. En consecuencia, tenemos que $O(\alpha) = \infty$ en $\mathbb{Z} \times \mathbb{Z}/ < (4,2) >$, luego si fuera cíclico debería ser isomorfo a $(\mathbb{Z}, +)$ porque es el único grupo cíclico con elementos de orden infinito. Sin embargo, si consideramos el elemento $\beta = (2,1) + < (4,2) > \in \mathbb{Z} \times \mathbb{Z}/ < (4,2) >$, tenemos que

$$\beta + \beta = (4,2) + < (4,2) > = (0,0) + < (4,2) > .$$

En otras palabras, se tiene que $O(\beta) = 2$, luego $\mathbb{Z} \times \mathbb{Z}/ < (4,2) >$ tampoco es isomorfo a $(\mathbb{Z}, +)$ porque $(\mathbb{Z}, +)$ no tiene elementos de orden 2.

(d) [0.5 puntos] Existe un dominio con 77 elementos.

Falso. Razonamos por reducción al absurdo, supongamos que D es un dominio de integridad con $\#(D) = 77$. Como D es un dominio, por (D.II) es un anillo unitario, luego se tiene que $car(D) =$

$O(1_D)$ donde $O(1_D)$ es el orden de 1_D en $(D,+)$. Por el Teorema de Lagrange $O(1_D)|\#(D) = 1$, luego $O(1_D)$ es $1,7,11$ o 77.
Como la característica de un dominio es o 0 o un número primo, tenemos que $car(D) = p$ con p primo. Por tanto, tenemos dos opciones:
(A) Si $car(D) = O(1_D) = 7$, entonces, por la definición de característica, $7x = 0$ para todo $x \in D$, luego $O(x) \mid 7$ para todo $x \in D$. Por el Teorema de Cauchy para grupos Abelianos, como $11 \mid \#(D)$, existe un elemento $d \in D$ con $O(d) = 11$, contradiciendo que $O(d) \mid 7$.
(B) si $car(D) = O(1_D) = 11$, razonando como en el caso (A) llegamos a contradicción.
En conclusión, no existe un dominio con 77 elementos.