Grupos y Anillos. Examen Temas 1-3. 21 de abril de 2020. Soluciones

(1) (a) **Demostrar que $1+i$ y 3 son irreducibles en $\mathbb{Z}[i]$ y que $\mathbb{Z}[i]/(3+3i)$ es el producto directo de dos cuerpos finitos. ¿Qué cardinal tiene cada uno de los dos cuerpos?**

(b) **Factorizar 5 en $\mathbb{Z}[i]$ y demostrar que $\mathbb{Z}[i]/(5)$ es el producto directo de dos cuerpos finitos. ¿Qué cardinal tiene cada uno de los dos cuerpos?**

(c) **Demostrar que $1+i$ y 7 son irreducibles en $\mathbb{Z}[i]$ y que $\mathbb{Z}[i]/(7+7i)$ es el producto directo de dos cuerpos finitos. ¿Qué cardinal tiene cada uno de los dos cuerpos?**

(d) **Factorizar 13 en $\mathbb{Z}[i]$ y demostrar que $\mathbb{Z}[i]/(13)$ es el producto directo de dos cuerpos finitos. ¿Qué cardinal tiene cada uno de los dos cuerpos?**

(e) **Demostrar que $1+2i$ y 7 son irreducibles en $\mathbb{Z}[i]$ y que $\mathbb{Z}[i]/(7+14i)$ es el producto directo de dos cuerpos finitos. ¿Qué cardinal tiene cada uno de los dos cuerpos?**

(f) **Factorizar 21 en $\mathbb{Z}[i]$ y demostrar que $\mathbb{Z}[i]/(21)$ es el producto directo de dos cuerpos finitos. ¿Qué cardinal tiene cada uno de los dos cuerpos?**

En todos estos ejercicios va bien utilizar la norma que en este caso toma la forma $N(a+bi) = a^2+b^2$. Sabemos que un elemento de $\mathbb{Z}[i]$ es unidad si y solo si su norma es 1 y usando esto es fácil ver que si p es un número primo, entonces un elemento a de $\mathbb{Z}[i]$ cuya norma es p es irreducible en $\mathbb{Z}[i]$ y en tal caso $p = a\overline{a}$ es la factorización de p. Sin embargo si p no es la norma de ningún elemento, o sea no es suma de dos cuadrados entonces p es irreducible en $\mathbb{Z}[i]$. Por ejemplo $N(1+i) = 2$, $N(2+i) = N(1+2i) = 5$, con lo que $1+i$ y $1+2i$ son irreducibles y $2 = (1+i)(1-i)$ y $5 = (1+2i)(1-2i)$ son factorizaciones en producto de irreducibles y sin embargo 3 y 7 no son suma de dos cuadrados y por tanto son irreducibles en $\mathbb{Z}[i]$. Con esto queda hecha la primera parte.

Para aplicar la segunda parte hay que aplicar el Teorema Chino de los Restos. En todos los casos se pide probar que $\mathbb{Z}[i]/(ab)$ es producto de dos cuerpos y en todos los casos a y b o son los irreducibles que aparecen en la primera parte o ab es la factorización que se pide. Hay que tener cuidado de demostrar que $(a)+(b) = \mathbb{Z}[i]$ para poder aplicar el Teorema Chino de los Restos pero en todos los casos es verdad pues a y b son irreducibles no asociados lo que es fácil de ver. Por tanto $\mathbb{Z}[i]/(ab) \cong \mathbb{Z}[i]/(a) \times \mathbb{Z}[i]/(b)$ y los dos factores son cuerpos.

Para ver el cardinal de $\mathbb{Z}[i]/(a)$ hay dos opciones. Si a es un número natural entonces todo elemento de $\mathbb{Z}[i]/(a)$ es de la forma $x+yi$ con $0 \leq x, y < a$ y dos elementos de este tipo no están en la misma clase módulo a. Por tanto $|\mathbb{Z}[i]/(a)| = a^2$. Sin embargo si a no está en $\mathbb{Z}$ pero a es irreducible entonces $p = N(a) = a\overline{a}$ resulta ser primo. Si resulta que a y $\overline{a}$ no son asociados entonces $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(a) \times \mathbb{Z}[i]/(\overline{a})$ con lo que $p^2 = |\mathbb{Z}[i]/(a)| \cdot |\mathbb{Z}[i]/(\overline{a})$. Eso implica que $|Z[i]/(a)| = p$. Con esto se pueden hacer todos los casos menos el caso en que $a = 1+i$ pues en este caso a y $\overline{a}$ sí que son asociados. Pero en este caso se tiene que $1+i$ está en la misma clase que 0 y por tanto i está en la misma clase que 1. Luego $|\mathbb{Z}[i]/(1+i)| = 2$.

(2) (2 puntos) **Sea A el conjunto de los polinomios con coeficientes racionales cuyo termino independiente es un número entero.**

(a) **Demostrar que A es un subanillo de $\mathbb{Q}[X]$.**

(b) **Demostrar que si p es un número primo entonces el ideal generado por p y X en A es principal y el ideal generado por esos elementos en $\mathbb{Q}[X]$ también es principal.**

Si $P = \sum_{i\geq 0} p_i X^i$ y $Q = \sum_{i\geq 0} q_i X^i$ entonces los términos principales de $P - Q$ y PQ son $p_0 + q_0$ y $p_0 q_0$ y ambos son enteros por serlo p_0 y q_0. Como todos los demás son racionales (pues $\mathbb{Q}[X]$ es un anillo) y 0 obviamente pertenece a A esto demuestra que A es subanillo de $\mathbb{Q}[X]$.

Sabemos que $\mathbb{Q}[X]$ es un DIP, por tanto todo ideal de $\mathbb{Q}[X]$ es principal y en particular lo será el generado por p y X en ese anillo. Por otro lado $X = \frac{X}{p}p$, con lo que X está en el ideal principal generado por p en A y por tanto el ideal generado por p y X en A está generado por p, con lo que es principal.

(3) (3 puntos) **Sea D un dominio y sea K el cuerpo de fracciones de D. Sea P un ideal primo de D. Si I es un ideal de D entonces denotamos**

$$I_P = \left\{ \frac{a}{b} : a \in I, b \in D \setminus P \right\}.$$

Demostrar:

(a) **D_P es un subanillo de K.**

(b) **Un elemento x de D_P es unidad de D_P si y sólo si $x \notin P_P$.**

(c) **Si I es un ideal de D entonces I_P es un ideal de D_P.**

(d) **Si I es un ideal de D entonces $I_P = D_P$ si y sólo si $I \not\subseteq P$.**

(e) **Todo ideal propio de D_P es de la forma I_P para algún ideal I de D contenido en P.**

(f) **Si I y J son dos ideales primos de D contenidos en P entonces $I \subseteq J$ si y solo si $I_P \subseteq J_P$.**

(a) $0 = \frac{0}{1}$ y $1 \notin P$. Por tanto $0 \in D_P$. Si $x, y \in D_P$ entonces $x = \frac{a}{r}$ e $y = \frac{b}{s}$ con $a, b \in D$ y $r, s \in D \setminus P$. Entonces $rs \in D \setminus P$, por ser P ideal primo de D y por tanto

$$x - y = \frac{a}{r} - \frac{b}{s} = \frac{as - br}{rs}, \frac{a}{r}\, xy = \frac{b}{s} = \frac{ab}{rs} \in D_P.$$

(b) Sea $x \in D_P \setminus P_P$. Entonces $x = \frac{a}{r}$ con $a \in D$ y $r \in D \setminus P$. Además $a \notin P$ pues $x \notin P_P$. Luego $x^{-1} = \frac{b}{a} \in D_P$ y por tanto $x \in D_P^*$.

Recíprocamente, supongamos que $x \in P_P$. Entonces $x = \frac{a}{r}$ con $a \in P$ y $r \in D \setminus P$. Vamos a ver que eso implica que x no es invertible en D_P. En caso contrario tendríamos

que $x\frac{b}{s} = 1$ con $b \in D$ y $s \in D \setminus P$. Entonces $rs = ab \in P$ en contra de que $r, s \notin P$ y P es ideal primo.

(c) De nuevo (i) $0 = \frac{0}{1}$ y $1 \notin P$. Por tanto $0 \in I_P$. Si $x, y \in I_P$ y $z \in D_P$ entonces $x = \frac{a}{r}$, $y = \frac{b}{s}$ y $z = \frac{c}{t}$ con $a, b \in I$, $c \in D$ y $r, s, t \in D \setminus P$. Entonces $rs, tr \in D \setminus P$, por ser P ideal primo de D y por tanto

$$x + y\frac{a}{r} + \frac{b}{s} = \frac{as + br}{rs}, zx = \frac{c}{t}\,\frac{a}{r} = \frac{ac}{tr} \in D_P.$$

(d) Si $I \not\subseteq P$ entonces existe $x \in I \setminus P$ y por tanto $x \in I_P$ y $\frac{1}{x} \in D_P$. Luego $1 = I_P$, con lo que $D_P = I_P$. Sin embargo si $I \subseteq P$ entonces $I_P \in P_P$ y por el apartado (ii) se tiene que $1 \notin I_P$, con lo que $I_P \neq D_P$.

(e) Sea J un ideal de D_P y sea $I = J \cap D$. Por el Tercer Teorema de Isomorfía I es un ideal de D. Vamos a ver que $J = I_P$. Si $x \in I_P$ entonces $x = a/b$ con $a \in I$ y $b \in D \setminus P$. Entonces $a = bx \in I \subseteq J$ y $\frac{1}{b} \in D_P$ con lo que $x = \frac{1}{b}a \in J$. Recíprocamente, si $x \in J$ entonces $x = \frac{a}{b}$ con $a \in D$ y $b \in D \setminus P$. Entonces $a = xb \in J \cap D = I$ y por tanto $x \in I_P$.

(f) Sean I y J ideales primos de D contenidos en P. Claramente si $I \subseteq J$ entonces $I_P \subseteq J_P$. Supongamos que $I \not\subseteq J$. Entonces existe $x \in I \setminus J$. Luego $x \in I_P$ y vamos a ver que $x \notin J_P$. En caso contrario, $x = \frac{a}{r}$ con $a \in J$ y $r \in D \setminus P$. Entonces $a = rx \in J$ y como $x \notin J$ y J es ideal primo necesariamente $r \in J \subseteq P$ lo que contradice que $r \notin P$.

(4) (2 puntos) **Decidir si los siguientes polinomios son irreducibles y los que no lo sean escribirlos como producto de irreducibles en $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$.**

$$f = 13X^4 + 4X^3 - X + 9, \quad g = 3X^6 - 21X^5 + 21X^2 - 84.$$

$$f = 3X^4 - 2X^2 - X - 9, \quad g = 3X^6 + 9X^5 + 36X^2 + 108X + 54.$$

$$f = 3X^6 - 21X^5 + 21X^2 - 84, \quad g = 3X^4 - 8X^2 - X - 9.$$

$$f = 26X^4 + 8X^3 - 4X + 12, \quad g = X^6 + 3X^5 - 10X^4 + 15X - 3.$$

$$f = 7X^6 + 21X^5 - 63X^4 + 105X - 210, \quad g = 3X^4 - 4X^3 - X - 9.$$

$$f = 26X^4 + 8X^3 - 4X + 12, \quad g = X^4 + 10X^3 + 20X^2 + 7X + 11.$$

Los polinomios $13X^4+4X^3-X+9$, $3X^4-2X^2-X-9$, $3X^4-8X^2-X-9$, $3X^4-4X^3-X-9$ y $X^4+10X^3+20X^2+7X+11$ son primitivos y sus reducciones módulo 2 son iguales a X^4+X+1. Este último no tiene raíces en $\mathbb{Z}_2$ y no es producto de dos polinomios de grado 2 pues el único polinomio irreducible de grado 2 en $\mathbb{Z}_2[X]$ es $X^2 + X + 1$ cuyo cuadrado es $X^4 + X^2 + 1$. Por tanto todos ellos son irreducibles.

$3X^6 - 21X^5 + 21X^2 - 84 = 3f$ con $f = (X^6 - 7X^5 + 7X^2 - 28)$. Aplicando el Criterio de Eisenstein con $p = 7$ deducimos que f es irreducible en $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$. Por tanto el polinomio original es irreducible en $\mathbb{Q}[X]$ y no lo es en $\mathbb{Z}[X]$ pero la factorización dada al principio es su factorización en producto de irreducibles.

$26X^4 + 8X^3 - 4X + 12 = 2f$ con $f = 13X^4 + 4X^3 - 2X + 6$. Aplicando el Criterio de Eisenstein con $p = 2$ deducimos que f is irreducible en $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$. Por tanto el polinomio

original es irreducible en $\mathbb{Q}[X]$ y no lo es en $\mathbb{Z}[X]$ pero la factorización dada al principio es su factorización en producto de irreducibles.

$7X^6+21X^5-63X^4+105X-210 = 7f$ con $f = X^6+3X^5-9X^4+15X-30$. Aplicando el Criterio de Eisenstein con $p = 3$ deducimos que f is irreducible en $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$. Por tanto el polinomio original es irreducible en $\mathbb{Q}[X]$ y no lo es en $\mathbb{Z}[X]$ pero la factorización dada al principio es su factorización en producto de irreducibles.

$3X^6+9X^5+36X^2+108X+54 = 3f$ con $f = X^6+3X^5+12X^2+36X+18$. Se comprueba de forma rutinaria que f no tiene ninguna raíz. Vamos a ver que tampoco tiene un divisor de grado 2 en $\mathbb{Z}[X]$. Supongamos que $f = (X^2+a_1X+a_0)(X^4+b_3X^3+b_2X^2+b_1X+b_0)$. Entonces $18 = a_0b_0$. Vamos a demostrar que $2 \mid b_0$. En caso contrario $2 \mid a_0$ y mirando el coeficiente de grado X tenemos que $a_1 \equiv a_1b_0+b_1a_0 = 36 \equiv 0 \bmod 2$, luego $2 \mid a_1$. Mirando ahora el coeficiente de grado X^2 tenemos que $b_0 \equiv b_0+a_1b_1+a_0b_2 = 12 \equiv 0 \bmod 2$, en contra de la hipótesis. Por tanto $2 \mid f$ y eso implica que $2 \nmid a_0$. Mirando el coeficiente de X tenemos que $b_1 \equiv a_1b_0+b_1a_0 = 36 \equiv 0 \bmod 2$, con lo que $2 \mid b_1$; mirando el coeficiente de X^2 tenemos que $b_2 \equiv b_0+a_1b_1+a_0b_2 = 12 \equiv 0 \bmod 2$, luego de nuevo $2 \mid d$ y mirando los coeficientes de X^4 y X^5 tenemos respectivamente que $a_1+b_3 \equiv b_2+a_0b_3+a_1 = 0 \bmod 2$ y $a_1+b_3 = 3 \not\equiv 0 \bmod 2$, lo que nos da una contradicción. Por tanto, si f no es irreducible entonces es producto de dos polinomios de grado 3, o sea $f = (X^3+a_2X^2+a_1X+a_0)(X^3+b_2X^2+b_1X+b_0)$. Mirando el término independiente podemos suponer que $2 \mid a_0$ y $2 \nmid b_0$. Mirando el término de grado 1 tenemos $a_1 \equiv a_1b_0+a_0b_1 = 36 \equiv 0 \bmod 2$, después mirando el término de grado 2 tenemos $a_2 \equiv a_0b_2+a_1b_1+a_2b_0 = 12 \equiv 0 \bmod 2$ y finalmente mirando el término de grado 3 tenemos que $1 \equiv b_0 \equiv a_0+a_1b_2+a_2b_1+b_0 = 0 \bmod 2$, que nos proporciona la contradicción. Por tanto f es irreducible en $\mathbb{Z}[X]$ y como es primitivo también es irreducible en $\mathbb{Q}[X]$. La factorización en $\mathbb{Z}[X]$ es la dada originalmente y el polinomio original es irreducible en $\mathbb{Q}[X]$.

$f = X^6+3X^5-10X^4+15X-3$ es primitivo y es fácil ver que no tiene ninguna raíz. Además $f_2 = X^6+X^5+X+1 = (X+1)^2(X^4+X^3+X^2+X+1)$. Esta última es la factorización de f_2 en $\mathbb{Z}_2[X]$ pues el último polinomio no tiene raíces y no es el cuadrado del único polinomio de grado 2. Por tanto si f es reducible en $\mathbb{Z}[X]$ entonces es divisible por un polinomio de grado 2. Pongamos $f = (X^2+a_1X+a_0)(X^4+b_3X^3+b_2X^2+b_1X+b_0)$. Entonces $a_0b_0 = -3$ con lo que o bien (a) $a_0 = \pm 3$ y $b_0 = \mp 1$ o bien (b) $a_0 = \pm 1$ y $b_0 = \mp 3$. Además $a_1b_0+a_0b_1 = 15$ con lo que en el caso (a) se verifica que $3 \mid a_1$ y en el caso (b) se tiene que $3 \mid b_1$. Ahora mirando el coeficiente de X^2 tenemos que $0 = b_0+a_1b_1+a_0b_2$. En el caso (a) tenemos $0 \equiv \pm 1 \bmod 3$, lo que nos lleva a una contradicción. Por tanto se verifica el caso (b), o sea $a_0 = \pm 1$ y $b_0 = \pm 3$ y $3 \mid b_1$ lo que implica que $3 \mid b_2$. Pero mirando ahora el coeficiente de X^3 tenemos que $0 = b_1+a_1b_2+a_0b_3$ lo que va a implicar que $3 \mid c$. Finalmente el coeficiente de X^4 es $-10 = b_2+a_1b_3+a_0b_0 \equiv 0 \bmod 3$, una contradicción. Concluímos pues que f es irreducible en $\mathbb{Z}[X]$ y como es primitivo también lo es en $\mathbb{Q}[X]$.