ESTRUCTURAS ALGEBRAICAS. Problemas. 14 de Diciembre.

Ejercicio 1. Hoja 6. Sea $\varphi\colon R \to S$ un homomorfismo de anillos biyectivo. Prueba que si $a \in R$ es irreducible, entonces $\varphi(a) \in S$ es irreducible. ¿Qué ocurre si solo asumes que φ es sobreyectivo? *Sugerencia: considera el epimorfismo evaluación $ev_1\colon \mathbb{Q}[x] \to \mathbb{Q}$ para responder a la segunda pregunta.*

Solución:

Decimos que un elemento $a \in R$, no nulo ni unidad, es irreducible si no admite una expresión de la forma $a = a_1a_2$ con $a_1, a_2 \in R$ no unidades. En general, para cualquier homomorfismo de anillos $\varphi\colon R \to S$, si $u \in R$ es una unidad, $\varphi(u)$ es una unidad en S, puesto que

$$1_R = uu^{-1} \implies 1_S = \varphi(1_R) = \varphi(uu^{-1}) = \varphi(u)\varphi(u)^{-1}\,.$$

Supongamos que $\varphi(a)$ no es irreducible, entonces existen $s_1, s_2 \in S$ no unidades tales que $\varphi(a) = s_1s_2$. Como φ es sobreyectivo, existen $a_1, a_2 \in R$ tales que $s_i = \varphi(a_i)$, para $i = 1, 2$. Por el argumento anterior, a_1, a_2 no son unidades en R. Tenemos que

$$\varphi(a) = \varphi(a_1)\varphi(a_2) = \varphi(a_1a_2)\,.$$

Como φ es inyectiva, concluimos que $a = a_1a_2$, con a_1, a_2 no unidades en R. Es decir, a no es irreducible, dando lugar a una contradicción.

Si φ solo es sobreyectiva, el resultado no es cierto en general. Consideramos el homomorfismo de evaluación $ev_1\colon \mathbb{Q}[x] \to \mathbb{Q}$. Es claro que el polinomio $X + 1$ es un elemento irreducible de $\mathbb{Q}[x]$. Sin embargo, $ev_1(X + 1) = 2$ no es irreducible en $\mathbb{Q}$, por ser una unidad.

Ejercicio 2. Hoja 6. Demuestra que en el anillo $\mathbb{Z}[\sqrt{-5}]$ los elementos 2, 3, $1 \pm \sqrt{-5}$ son irreducibles pero no son primos.

Solución:

Recordamos que en $\mathbb{Z}[\sqrt{-5}]$ podemos definir una aplicación norma $N\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ dada por:

$$N(a + b\sqrt{-5}) = a^2 + 5b^2\,.$$

Se puede comprobar que:

- Para todo $x, y \in \mathbb{Z}[\sqrt{-5}]$, $N(xy) = N(x)N(y)$.
- $x \in \mathbb{Z}[\sqrt{-5}]$ es una unidad si y solo si $N(x) = 1$.
- Si $x|y$, entonces $N(x)|N(y)$.

Observamos que $N(2) = 4$, $N(3) = 9$, y $N(1 \pm \sqrt{-5}) = 6$. Si los elementos 2, 3, $1 \pm \sqrt{-5}$ no fueran irreducibles, existirían elementos $x, y \in \mathbb{Z}[\sqrt{-5}]$ tales que $N(x) = 2$ y $N(y) = 3$. Pero esto no es posible, pues

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 < 5 \implies N(a + b\sqrt{-5}) = a^2\,,$$

y 2 y 3 no son cuadrados en $\mathbb{Z}$. Por tanto, los elementos 2, 3, $1 \pm \sqrt{-5}$ son irreducibles.

Sin embargo, estos elementos no son primos puesto que:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})\,,$$

pero 2 y 3 no dividen a $1 \pm \sqrt{-5}$, y $1 \pm \sqrt{-5}$ no divide a 2 ni a 3.

Ejercicio 3. Hoja 6. Prueba que $\mathbb{Z}[\sqrt{-3}]$ no es un dominio de factorización única mostrando dos factorizaciones distintas de 4. ¿Es $\mathbb{Z}[\sqrt{-3}]$ un dominio de ideales principales?

Solución:

Afirmamos que $4 = 2 \cdot 2 = (1 - \sqrt{3}i)(1 + \sqrt{3}i)$ son dos descomposiciones en factores irreducibles distintas. Veamos que $\omega = 2, 1 \pm \sqrt{3}i$ es irreducible en $\mathbb{Z}[\sqrt{-3}]$. Si existieran elementos $z = a + bi, z' = a' + b'i \in \mathbb{Z}[\sqrt{-3}]$ tales que $\omega = zz'$, tendríamos que

$$|\omega|^2 = |z|^2|z'|^2 \Rightarrow 4 = (a^2 + 3b^2)(a'^2 + 3b'^2).$$

Tenemos tres posibles soluciones:

- $a^2 + 3b^2 = 1$ y $a'^2 + 3b'^2 = 4$, de manera que $z = \pm 1$ y $z' = \pm\omega$.
- $a^2 + 3b^2 = 2$ y $a'^2 + 3b'^2 = 2$, que no admite soluciones enteras.
- $a^2 + 3b^2 = 4$ y $a'^2 + 3b'^2 = 2$, de manera que $z = \pm\omega$ y $z' = \pm 1$.

Por tanto, cada ω es un elemento irreducible, no asociados entre ellos. Entonces tenemos dos descomposiciones distintas y concluimos que $\mathbb{Z}[\sqrt{-3}]$ no es un anillo factorial.

Todo dominio de ideales principales es un dominio de factorización única. Por tanto, como $\mathbb{Z}[\sqrt{-3}]$ no es un DFU, tampoco puede ser un DIP.

Ejercicio 4. Hoja 6. Sea $\varphi\colon A \to B$ un homomorfismo de anillos. Prueba que si A es un cuerpo entonces φ es necesariamente inyectivo.

Solución:

Si A es un cuerpo, los únicos ideales de A son (0) y A. Si ϕ es un homomorfismo de anillos, entonces $\ker(\phi)$ es un ideal de A. Si $\ker(\phi) = (0)$, entonces ϕ es un homomorfismo inyectivo. Si $\ker(\phi) = A$, entonces tendríamos $\phi(1_A) = 0_B$, por lo que, ϕ no sería un homomorfismo de anillos.

Ejercicio 5. Hoja 6. Demuestra que:

(a) No existe ningún homomorfismo de anillos (cuerpos) $\varphi\colon \mathbb{Q} \to \mathbb{F}_p$ para ningún primo $p \in \mathbb{Z}$.

(b) No existe ningún homomorfismo de anillos (cuerpos) $\varphi\colon \mathbb{R} \to \mathbb{Q}$.

Solución:

(a) Supongamos que $\varphi\colon \mathbb{Q} \to \mathbb{F}_p$ es un homomorfismo de anillos. Entonces $\varphi(1) = [1]_p$. Por tanto, se tiene que

$$[1]_p = \varphi(1) = \varphi\left(p \cdot \frac{1}{p}\right) = p\varphi\left(\frac{1}{p}\right) = [0]_p\,.$$

Esto es una contradicción.

(b) Supongamos que $\varphi\colon \mathbb{R} \to \mathbb{Q}$ es un homomorfismo de cuerpos, entonces necesariamente es inyectivo. Pero esto implicaría que $|\mathbb{R}| \leq |\mathbb{Q}|$, algo que no es posible, pues $\mathbb{Q}$ es numerable, pero $\mathbb{R}$ no lo es.

Ejercicio 6. Hoja 6. Prueba que el grupo de automorfismos del cuerpo $\mathbb{Q}$ es trivial.

Solución:
Sea $\varphi \in \mathrm{Aut}(\mathbb{Q})$. Necesariamente, se tiene $\varphi(1) = 1$. Para cada $n \in \mathbb{N}$, es claro que

$$n = 1 + \cdots + 1 = \varphi(1) + \cdots + \varphi(1) = \varphi(1 + \cdots + 1) = \varphi(n).$$

Como φ preserva los inversos, para cada $n \in \mathbb{N}$, se tiene:

$$\varphi(-n) = -n$$

Para cada $n \in \mathbb{Z}$, tenemos

$$\varphi\left(\frac{1}{n}\right) = \frac{1}{n}\,.$$

Finalmente observamos que todo elemento de $\mathbb{Q}$ se escribe como $\frac{r}{s}$ para ciertos $r, s \in \mathbb{Z}$. Por tanto, se tiene que:

$$\varphi\left(\frac{r}{s}\right) = \varphi\left(r \cdot \frac{1}{s}\right) = \varphi(r)\varphi\left(\frac{1}{s}\right) = r \cdot \frac{1}{s} = \frac{r}{s}\,.$$

Así, concluimos que $\varphi = \mathrm{id}_{\mathbb{Q}}$.

Ejercicio 7. Hoja 6. Prueba que el grupo de automorfismos del cuerpo $\mathbb{R}$ es trivial. (*Sugerencia: usa el ejercicio anterior junto con el hecho de que, por ser un cuadrado, todo elemento estrictamente positivo ha de tener imagen estrictamente positiva, lo cual, a su vez, implica que cualquier automorfismo debe preservar el orden*).

Solución:

Sea $\varphi \in \mathrm{Aut}\mathbb{R}$. Para cada $x \in \mathbb{R}_{>0}$, existe $y \in \mathbb{R}$ tal que $x = y^2$. Por lo que, tenemos

$$\varphi(x) = \varphi(y)^2 > 0\,,$$

es decir, la imagen de un elemento estrictamente positivo es también estrictamente positiva. Para cada $a, b \in \mathbb{R}$ tales que $a < b$, tenemos que $b - a > 0$. Por lo que,

$$\varphi(b) - \varphi(a) = \varphi(b - a) > 0.$$

Esto es, $\varphi(a) < \varphi(b)$ y φ preserva el orden. Repitiendo el argumento del ejercicio 6, afirmamos que $\varphi(r) = r$ para todo $r \in \mathbb{Q}$. Para cada $x \in \mathbb{R}$, existen elementos racionales $r, s \in \mathbb{Q}$ tales que $r < \varphi(x) < s$, con $|s - r|$ arbitrariamente pequeño. Por tanto, $\varphi(x) = x$ y concluimos que $\varphi = \mathrm{id}_{\mathbb{R}}$.

Ejercicio 8. Hoja 6. Prueba que el grupo de los automorfismos del cuerpo $\mathbb{Q}[i]$ es isomorfo a C_2.

Solución:
Sea $\varphi \in \mathrm{Aut}(\mathbb{Q}[i])$. Repitiendo el argumento del ejercicio 6, se tiene que $\varphi|_{\mathbb{Q}} = \mathrm{id}|_{\mathbb{Q}}$. Por tanto, falta por determinar $\varphi(i)$. Observamos que

$$\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1\,.$$

Veamos que $(a + bi)^2 = -1$ si y solo si $a = 0$ y $b = \pm 1$. Se tiene que $(a + bi)^2 = (a^2 - b^2) + 2abi$, por lo que, $(a + bi)^2 = -1$ si y solo si $ab = 0$ y $a^2 - b^2 = -1$. Si $a = 0$, entonces $b = \pm 1$. Si $b = 0$, entonces $a^2 = -1$ no tiene solución en $\mathbb{Q}$. Por tanto, $\varphi(i) = \pm i$. Si $\varphi(i) = i$, entonces $\varphi = \mathrm{id}$. Mientras que si $\varphi(i) = -i$, se trata del homomorfismo de conjugación. Es claro que $\varphi^2 = \mathrm{id}$. Por tanto, $\mathrm{Aut}(\mathbb{Q}[i]) \simeq \mathsf{C}_2$.

Ejercicio 9. Hoja 6. Deduce del ejercicio anterior que el grupo de los automorfismos continuos del cuerpo $\mathbb{C}$ es isomorfo a C_2.

Solución:

Sea $\varphi \in \mathrm{Aut}(\mathbb{C})$. Repitiendo el argumento del ejercicio 8, tenemos que $\varphi|_{\mathbb{Q}[i]} = \mathrm{id}_{\mathbb{Q}[i]}$. Ahora, podemos interpretar $\mathbb{C} = \mathbb{R} + \mathbb{R}i = \mathbb{R}[i]$. Se puede probar que $\mathbb{Q}[i]$ es denso en $\mathbb{C}$. Dado que dos funciones continuas son iguales si coinciden en un subconjunto denso, entonces φ coincide sobre $\mathbb{Q}[i]$ con $\mathrm{id}_{\mathbb{Q}[i]}$ o con el homomorfismo de conjugación. Por tanto, existen dos únicos automorfismos continuos de $\mathbb{C}$, determinados por $\varphi(i) = i$ y $\varphi(i) = -i$. Como veíamos en el ejercicio 8, este grupo es isomorfo a C_2.

Ejercicio 10. Hoja 6. ¿Cuántos elementos tiene el anillo $\mathbb{F}_3[x]/(x^2 + x + 1)$? ¿Se trata de un cuerpo?

Solución:
Usando la relación $x^2 = -x - 1$, tenemos que

$$\mathbb{F}_3[X]/(x^2 + x + 1) = \{ax + b \colon a, b \in \mathbb{F}_3\}.$$

Por tanto, este anillo tiene $3^2 = 9$ elementos.

Comprobamos que $p(x) = x^2 + x + 1$ no es irreducible puesto que $p(1) = 0$. De hecho, se tiene $p(x) = (x - 1)^2$ en $\mathbb{F}_3[X]$. Como $p(x)$ no es irreducible, el ideal $(x^2 + x + 1)$ no es maximal en $\mathbb{F}_3[X]$. Por tanto, el anillo cociente $\mathbb{F}_3[x]/(x^2 + x + 1)$ no es un cuerpo.

Ejercicio 11. Hoja 6. Factoriza los siguientes polinomios en su correspondiente anillo:

(a) $X^5 + 2X + 2 \in \mathbb{Q}[X]$;

(b) $X^4 - 1$ en $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{F}_2[X]$ y $\mathbb{F}_3[X]$;

(c) $X^4 + X^3 - X^2 \in \mathbb{F}_2[X]$.

Solución:

(a) Observamos que 2 divide a $a_0 = a_1 = 2$ y $a_2 = a_3 = a_4 = 0$, no divide a $a_5 = 1$ y 2^2 no divide a $a_0 = 2$. Por tanto, el criterio de Einsestein nos dice que el polinomio es irreducible sobre $\mathbb{Q}[X]$.

(b) En $K[X]$, tenemos que $X^4 - 1 = (X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X^2 + 1)$, siendo $X - 1$ y $X + 1$ factores irreducibles.

- En $\mathbb{R}[X]$, el factor X^2+1 es irreducible. Si no lo fuera, tendríamos que $X^2+1 = (aX+b)(cX+d)$, con $a, b, c, d \in \mathbb{R}$, es decir, $ac = 1,\ ad + bc = 0,\ bd = 1$, lo que implicaría $c^2 + d^2 = 0$. De donde se seguiría que $X^2+1 = (aX+b)\cdot 0$, una contradicción. Por tanto, la descomposición en factores irreducibles sería $X^4 - 1 = (X - 1)(X + 1)(X^2 + 1)$.

- En $\mathbb{C}[X]$, tenemos que $X^2 + 1 = (X + i)(X - i)$, siendo cada factor irreducible. Por tanto, tendríamos la descomposición en factores irreducibles $X^4 - 1 = (X - 1)(X + 1)(X + i)(X - i)$.

- En $\mathbb{F}_2[X]$, tenemos que $X^2 - \bar{1} = X^2 + \bar{1} = (X + \bar{1})^2$. Por tanto, tendríamos la descomposición en factores irreducibles $X^4 - \bar{1} = (X + \bar{1})^4$.

- En $\mathbb{F}_3[X]$, el polinomio $X^2 + \bar{1}$ es irreducible, puesto que

$$\bar{0}^2 + \bar{1} = \bar{1} \neq \bar{0}, \quad \bar{1}^2 + \bar{1} = \bar{2} \neq \bar{0}, \quad \bar{2}^2 + \bar{1} = \bar{2} \neq \bar{0}.$$

Por tanto, la descomposición en factores irreducibles sería $X^4 - 1 = (X - \bar{1})(X + \bar{1})(X^2 + \bar{1})$.

(c) En $\mathbb{F}_2[X]$, tenemos la descomposición en factores irreducibles $X^4 + X^3 - X^2 = X^2(X^2 + X - \bar{1})$. Sabemos que X es irreducible y $X^2 + X - \bar{1}$ también, porque no tiene ninguna raíz, ya que

$$\bar{0}^2 + \bar{0} - \bar{1} = \bar{1} \neq \bar{0} \quad \text{y} \quad \bar{1}^2 + \bar{1} - \bar{1} = \bar{1} \neq \bar{0}.$$

Ejercicio 12. Hoja 6. Halla un generador de $I = (x^3 + 1, x^2 + 1)$ en $\mathbb{F}_2[x]$.

Solución:

Observamos que

$$x^3 + 1 = (x + 1)(x^2 + x + 1) \quad \text{y} \quad x^2 + 1 = (x + 1)^2 .$$

Por tanto, $\text{mcd}\{x^3 + 1, x^2 + 1\} = x + 1$. De hecho, tenemos que

$$x + 1 = (x^3 + 1) + x(x^2 + 1) .$$

Por tanto, $I = (x + 1)$ en $\mathbb{F}_2[x]$.

Ejercicio 13. Hoja 6. Sea K un cuerpo. Demuestra que si $f \in K[x]$ es un polinomio no nulo de grado n entonces f tiene, a lo sumo, n raíces.
Sugerencia: usa inducción sobre el grado y el algoritmo de división en $K[x]$.

Solución:

Sea $f \in K[x]$ no nulo. Procedemos por inducción sobre $n = \deg(f)$. Si $n = 0$, entonces $f(x) = c$ es constante y $f(k) \neq 0$ para todo $k \in K$, esto es, f tiene cero raíces. Supongamos que el resultado es cierto hasta $n - 1$. Supongamos que f tuviera $n + 1$ raíces distintas $r_1, \ldots, r_{n+1}$. Por el algoritmo de la división, podemos escribir

$$f(x) = (x - r_{n+1})q(x) ,$$

para algún $q \in K[x]$ tal que $\deg(q) \leq n - 1$. Observamos que $(r_i - r_{n+1}) \neq 0$ para todo $i = 1, \ldots, n$. Por tanto, como $r_1, \ldots, r_n$ son raíces de f y K es un dominio de integridad, necesariamente se tiene $q(r_i)$ para todo $i = 1, \ldots, n$. Pero esto da lugar a una contradicción, pues q tiene a lo sumo $n - 1$ raíces distintas.

Ejercicio 14. Hoja 6. Demuestra que si K es un cuerpo infinito y $f, g \in K[x]$ son tales que $f(a) = g(a)$ para todo $a \in K$, entonces $f = g$. ¿Qué ocurre si K es finito?
Sugerencia: para la segunda parte, considera $f(x) = x^p - x$ en $\mathbb{F}_p[x]$.

Solución:

Sea K un cuerpo infinito. Sean $f, g \in K[X]$ tales que $f(a) = g(a)$ para todo $a \in K$. Definimos el polinomio $p = f - g$. Entonces $p(a) = 0$ para todo $a \in K$. Si p es no nulo, por el ejercicio 13, solo puede tener un número finito de raíces. Por tanto, la única posibilidad es que $p = 0$ y $f = g$.

Si K es finito, podemos considerar el polinomio $f(x) = x^p - x$ en $\mathbb{F}_p[x]$. Veremos en el ejercicio 15 que $x^{p-1} - 1$ se anula en todos los elementos de $\mathbb{F}_p^*$. Por tanto, $f(a) = 0$ para todo $a \in \mathbb{F}_p$. Pero $f \neq 0$.

Ejercicio 15. Hoja 6. Sea p un número primo.

(a) Demuestra que todos los elementos del grupo multiplicativo $\mathbb{F}_p^*$ son raíces del polinomio $X^{p-1}-1$.

(b) Deduce que el polinomio $X^{p-1}-1 \in \mathbb{F}_p[X]$ factoriza como producto de $p-1$ polinomios mónicos de grado uno.

Solución:

(a) Recordamos que $|\mathbb{F}_p^*| = \varphi(p) = p-1$. Por tanto, el orden de cada elemento de $\mathbb{F}_p^*$ es un divisor de $p-1$. Sea $\bar{k} \in \mathbb{F}_p^*$ un elemento cualquiera con orden n. Tenemos que

$$\bar{k}^{p-1} = \bar{k}^{n\cdot m} = (\bar{k}^n)^m = \bar{1}^m = \bar{1}.$$

Por tanto, cada elemento de $\mathbb{F}_p^*$ es raíz del polinomio $X^{p-1}-1 \in \mathbb{F}_p^*[X]$.

(b) Como cada elemento $\bar{k} \in \mathbb{F}_p^*$ es raíz del polinomio $X^{p-1}-1 \in \mathbb{F}_p^*[X]$, cada factor $X-\bar{k}$ lo divide. Por tanto, podemos expresar

$$X^{p-1}-1 = \prod_{\bar{k}\in\mathbb{F}_p^*} (X-\bar{k}).$$

Ejercicio 16. Hoja 6. Sea K un cuerpo finito de característica p.

(a) Demuestra que $(x+y)^p = x^p + y^p$ para todo $x, y \in K$.

(b) Concluye que la aplicación $\phi\colon K \to K$ definida como $\phi(x) = x^p$ es un automorfismo de K. El automorfismo ϕ se denomina *automorfismo de Frobenius* de K.

Solución:

(a) La fórmula del binomio nos dice que

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}.$$

Para todo $0 < k < p$, tenemos que

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = p \cdot \frac{(p-1)!}{k!(p-k)!} \qquad \text{con } \frac{(p-1)!}{k!(p-k)!} \in \mathbb{Z},$$

puesto que, como p es primo y $k, p-k < p$, ningún elemento del denominador divide a p. Por tanto, tenemos que

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} \equiv x^p + y^p \mod p.$$

(b) Comprobamos que la aplicación $f\colon K \to K$, $x \mapsto x^p$ es un automorfismo de K:

- Para todo $x, y \in K$, se tiene que
$$f(x+y) = (x+y)^p \underset{(a)}{=} x^p + y^p = f(x) + f(y), \quad f(xy) = (xy)^p = x^p y^p = f(x)f(y).$$
- Es claro que $f(1) = 1^p = 1$.
- Por ser un homomomorfismo entre cuerpos, f es inyectivo.
- Como f es una aplicación inyectiva entre conjuntos finitos del mismo cardinal, necesariamente f es sobreyectiva.