Teoría de Galois

Soluciones a algunos ejercicios de la Hoja 1

Carolina Vallejo Rodríguez

A lo largo de todo el curso por anillo entenderemos un anillo unitario y conmutativo. Entenderemos que todo homomorfismo de anillos $\varphi\colon R \to S$ satisface $\varphi(1_R) = 1_S$.

Repaso de Teoría de Anillos

1. Sea R un anillo finito. Demuestra que todo elemento no nulo de R es o bien un elemento invertible, o bien un divisor de cero. Decide de manera razonada si la afirmación sigue siendo cierta si R es infinito.

Solución: Podemos escribir $R = \{0, a_0, a_1, \ldots, a_n\}$ donde $a_1 = 1$. Si $a \in R^\times$ no es un divisor de 0, entonces $aa_i = aa_j$ implica que $a(a_i - a_j) = 0$ de donde concluimos que $a_i = a_j$. La aplicación $\varphi_a\colon R^\times \to R^\times$ definida por $\varphi_a(a_i) = aa_i$ es inyectiva entre conjuntos finitos del mismo cardinal, por tanto es sobreyectiva y existe algún a_i de modo que $aa_i = a_0 = 1$. Luego $a \in \mathcal{U}(R)$ es invertible. No es cierta, $\mathbb{Z}$ es un dominio de integridad y $\mathcal{U}(\mathbb{Z}) = \{\pm 1\}$.

2. Sea R un anillo y $a \in R$, escribimos $(a) = \{ar \ : r \in R\} = aR \subseteq R$. Demuestra que:

a) (a) es un ideal de R.

b) $(a) = R$ si, y solo, si $a \in \mathcal{U}(R)$.

c) R es un cuerpo si, y solo si, sus únicos ideales son $\{0\}$ y R.

Solución:

a) Sean $ar, as \in (a)$ se tiene que $ar - as = a(r-s) \in (a)$. Sea $t \in R$, entonces $(ar)t = a(rt) \in (a)$.

b) Si $(a) = R$, entonces $1 = ar$ y $a \in \mathcal{U}(R)$. Recíprocamente, si $a \in \mathcal{U}(R)$, entonces $1 = aa^{-1} \in (a)$. En particular, para cada $r \in R$, se tiene que $r = 1r \in (a)$. Concluimos que $R \subseteq (a)$ y, por tanto, $R = (a)$.

c) Si R es un cuerpo y $\{0\} \neq I \leq R$, cualquier elemento no cero $a \in I$ es una unidad entonces $1 \in I$ e $I = R$. Para probar la dirección inversa tomar cualquier $r \in R^\times$, entonces $r \in (r) \leq R$. Por hipótesis $(r) = R$ de donde concluimos que $r \in \mathcal{U}(R)$. Hemos probado que $\mathcal{U}(R) = R^\times$, es decir, R es un cuerpo.

3. Sea R un dominio de integridad y $a, b \in R$. Prueba que $(a) = (b)$ si, y solo si, existe un $c \in \mathcal{U}(R)$ tal que $a = bc$.

Solución: Podemos suponer que $a, b \neq 0$. Como $a \in (a) = (b)$ entonces existe algún $c \in R$ tal que $a = bc$. De forma similar existe algún $d \in R$ de forma que $b = ad$. Entonces $a = adc$ y restando obtenemos $a(1 - dc) = 0$. Aquí usamos que R es un dominio de integridad, lo que nos garantiza que $1 - dc = 0$, es decir, $dc = 1$ y $c, d \in \mathcal{U}(R)$. Para probar la implicación contraria no necesitamos que R sea un dominio de identidad. Si $a = bc$ con $c \in \mathcal{U}(R)$ tenemos que $a \in (b)$, por tanto $(a) \subseteq (b)$. Por otro lado $b = ac^{-1} \in (a)$ y obtenemos la otra inclusión $(b) \subseteq (a)$.

4. Sean $I \subseteq J$ ideales en un anillo R. Demuestra que:

a) $J/I \subseteq R/I$ es un ideal.

b) (Teorema de Isomorfía) Sea $\varphi\colon R \to S$ un homomorfismo de anillos. Prueba que $\ker(\varphi)$ es un ideal de R, $\varphi(R)$ es un subanillo de S y que $\overline{\varphi}\colon R/\ker(\varphi) \to \varphi(R)$ es un isomorfismo de anillos. En particular

$$R/\ker(\varphi) \cong \varphi(R)\,.$$

c) El anillo cociente $(R/I)/(J/I)$ es isomorfo a R/J. *Sugerencia: usa el teorema de isomorfía.*

d) (Teorema de correspondencia) Existe una correspondencia entre los ideales de R que contienen a I y los ideales del anillo cociente R/I.

Solución: Los apartados **a)** y **b)** son rutina. Definimos $\pi\colon R/I \to R/J$ por $\pi(r+I) = r+J$. La aplicación está bien definida porque $I \subseteq J$ (cercioraos), y $\ker(\pi) = \{r+I \mid r \in J\} = J/I$. Por el Teorema de Isomorfía se tiene que $(R/I)/(J/I) \cong R/J$. El apartado **d)** también es rutina.

5. Sea n un número natural. Prueba que $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ es un cuerpo si, y solo si, n es primo.

Solución: Notamos que si $n = ab$, entonces $(a+n\mathbb{Z})(b+n\mathbb{Z}) = 0$. Esta observación permite demostrar una de las implicaciones. Para la contraria pensar que si n es primo, entonces $(n,k) = 1$ para todo $0 < k < n$ y por Bézout se tiene que $1 = ak + bn$.

6. Dados $I = \{(3x, y) : x, y \in \mathbb{Z}\}$ y $J = \{(a, 0) : a \in \mathbb{Z}\}$, demuestra que I es un ideal maximal y J es un ideal primo no maximal de $\mathbb{Z} \times \mathbb{Z}$.

Solución: Usaremos la caracterización de ideales primos y maximales. Definimos $\varphi\colon \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}_3$ según $\varphi(x,y) = x + 3\mathbb{Z}$. Se puede comprobar que φ es un epimorfismo de anillos con $\ker(\varphi) = I$. Por el Teorema de Isomorfía $\mathbb{Z}\times\mathbb{Z}/I \cong \mathbb{Z}_3$ es un cuerpo. Luego I es maximal y, por tanto, primo. Definir $\varphi'\colon \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ según $\varphi'(x,y) = y$. Usando este homomorfismo podéis concluir que J es primo pero no maximal.

7. Dado un dominio de integridad R. Se dice que un elemento $0 \neq a \in R$ es irreducible si $a \notin \mathcal{U}(R)$ y siempre que $a = bc$ se tiene que $b \in \mathcal{U}(R)$ o $c \in \mathcal{U}(R)$. Se dice que $0 \neq a \in R$ es primo si $a \notin \mathcal{U}(R)$ e $I = (a)$ es un ideal primo de R, es decir, siempre que $bc \in I$ se tiene que $b \in I$ o $c \in I$.

a) Demuestra que los elementos primos en R son irreducibles.

b) Prueba que si R es un dominio de ideales principales, entonces el recíproco del apartado anterior también es cierto, es decir, todo elemento irreducible en R es primo.
Sugerencia para el segundo apartado: demuestra que en un DIP todo elemento irreducible genera un ideal maximal (lo vimos en clase).

Solución: **a)** Sea $a \in R$ primo y supongamos que $a = bc$. Como $bc \in (a)$, por definición se tiene que $b \in (a)$ o $c \in (a)$. Supongamos que $b \in (a)$, el razonamiento es completamente análogo en el otro caso. Entonces $b = ad$ con $d \in R$. Sustituyendo $a = bc = adc$, de donde obtenemos que $a(1-dc) = 0$, como estamos en un dominio de integridad $dc = 1$, es decir, $c \in \mathcal{U}(R)$.

8. Demuestra que el conjunto $S = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ con las operaciones suma y producto módulo 10 es un anillo. ¿Cuál es su unidad? ¿Es un cuerpo?
Construye las tablas de suma y producto de S o trabaja en $\mathbb{Z}_{10} = \mathbb{Z}/10\mathbb{Z}$ teniendo en cuenta las propiedades de los ideales y cocientes.

9. Sea $d \in \mathbb{Z}$, $1 \neq d \neq e^2$ con $e \in \mathbb{Z}$, consideramos el subanillo

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Definimos la aplicación $N\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ como $N(a+b\sqrt{d}) = a^2 - db^2$. Demuestra que N cumple:

(i) $N(x) = 0$ si, y solo si, $x = 0$.

(ii) $N(xy) = N(x)N(y)$.

(iii) $x \in \mathcal{U}(\mathbb{Z}[\sqrt{d}])$ si, y solo si, $N(x) = \pm 1$. *Sugerencia: nota que $N(a+b\sqrt{d}) = (a+b\sqrt{d})(a-b\sqrt{d})$.*

10. Halla las unidades de $\mathbb{Z}[i]$ y $\mathbb{Z}[\sqrt{3}i]$. Decide si todo número primo $p \in \mathbb{Z}$ es primo en $\mathbb{Z}[i]$.
Sugerencia: considera primos de la forma $p = a^2 + b^2$ para $a, b \in \mathbb{Z}$.

Solución: Por el ejercicio anterior sabemos que $\mathcal{U}(\mathbb{Z}[i])$ son los elementos $a+bi$ con norma ± 1, es decir, tales que $a^2 + b^2 = \pm 1$. Es directo comprobar que $\mathcal{U}(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. En el caso de $\mathbb{Z}[\sqrt{3}i]$, las unidades son elementos $a + b\sqrt{3}i$ con norma $a^2 + 3b^2 = \pm 1$ y $a, b \in \mathbb{Z}$. En este caso $\mathcal{U}(\mathbb{Z}[\sqrt{3}i]) = \{\pm 1\}$. Notamos que $2 = (1+i)(1-i)$, pero tanto $(1-i)$ como $(1+i)$ no pertenecen al ideal generado por $(2) = 2\mathbb{Z}[i]$. Es decir,

2 no es primo en $\mathbb{Z}[i]$. En general, cualquier primo de la forma $a^2+b^2=(a+bi)(a-bi)$ no es primo en $\mathbb{Z}[i]$. Por un Teorema de Fermat los primos impares en $\mathbb{Z}$ de la forma a^2+b^2 son exactamente los primos congruentes con 1 módulo 4. Una de las implicaciones de este Teorema de Fermat es muy sencilla. ¿Sabes cuál?

El anillo $\mathbb{Z}[i]$ se conoce como el anillo de enteros de Gauss.

11. Prueba que $\mathbb{Z}[\sqrt{3}i]$ no es un dominio de ideales principales. Demuestra que $\mathbb{Z}[\sqrt{3}i]$ tampoco es un dominio de factorización única.
Sugerencia: prueba que 2, $1+\sqrt{3}i$ *y* $1-\sqrt{3}i$ *son elementos irreducibles en* $\mathbb{Z}[\sqrt{3}i]$. *Nota que*

$$(1+\sqrt{3}i)(1-\sqrt{3}i)=4=2\cdot 2\,,$$

en particular en $\mathbb{Z}[\sqrt{3}i]$ *hay elementos irreducibles que no son primos.*

12. ¿Cuántos elementos tiene el anillo $\mathbb{Z}[i]/(2i)$? ¿Se trata de un cuerpo?
Sugerencia: nota que $(2i)=(2)=2\mathbb{Z}[i]$.

13. Sea $R=\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$. Considera el anillo $S=R/2R$.

a) Calcula cuántos elementos tiene S.

b) Encuentra todos los subanillos de S.

c) Encuentra todos los ideales de S.

Solución: Es fácil comprobar que $S=\{a_0+b_0\sqrt{2}+2R\mid a_0,b_0\in\{0,1\}\}=\{0+2R,1+2R,\sqrt{2}+2R,1+\sqrt{2}+2R\}$. Por tanto, $|S|=4$. El conjunto $\{0,1\}$ siempre forma un subanillo. Supongamos que T es un subanillo, si $\sqrt{2}\in T$ entonces $1+\sqrt{2}\in T$. Si $1+\sqrt{2}\in T$, entonces $1+\sqrt{2}-1=\sqrt{2}\in T$. Por tanto, los únicos subanillos son el trivial y el total. (Al final hemos abusado de notación denotando los elementos del cociente S por un representante de la clase.)

14. Demuestra que si $\varphi\colon R\to S$ es un homomorfismo de anillos y $a\in\mathcal{U}(R)$, entonces $\varphi(a)\in\mathcal{U}(S)$. ¿Es cierto el recíproco? Concluye que si φ es biyectivo entonces $\mathcal{U}(R)=\mathcal{U}(S)$.

Solución: Si $1=ab$ con $b\in R$, entonces $1=\varphi(1)=\varphi(ab)=\varphi(a)\varphi(b)$, luego $\varphi(a)\in\mathcal{U}(S)$. Si φ es biyectivo, entonces $\varphi^{-1}\colon S\to R$ es un homomorfismo y por tanto manda unidades a unidades, luego $\mathcal{U}(R)=\mathcal{U}(S)$.

El recíproco no es cierto. De hecho, si φ no es biyectivo, más allá de $\varphi(\mathcal{U}(R))\subseteq\mathcal{U}(S)$ (que hemos probado en el párrafo anterior), cualquier cosa puede ocurrir. Por ejemplo, si $\iota\colon\mathbb{Z}\to\mathbb{Q}$ es la inclusión (homomorfismo inyectivo), notamos que $2\in\mathcal{U}(\mathbb{Q})$ pero $2\notin\mathcal{U}(\mathbb{Z})$. Si consideramos la proyección canónica $\pi\colon\mathbb{Z}\to\mathbb{Z}_2$ (homomorfismo sobreyectivo), la imagen de todo elemento impar de $\mathbb{Z}$ es una unidad en $\mathbb{Z}_2$, pero $\mathcal{U}(\mathbb{Z})=\{\pm 1\}$.

15. 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. Concluye que si φ es un isomorfismo de anillos a es irreducible, si y solo si, $\varphi(a)$ es irreducible. ¿Qué ocurre si solo asumes que φ es sobreyectivo en la primera parte del ejercicio?

Solución: Si $\varphi(a)=st$ con $s,t\in S$. Como φ es sobreyectivo, sean $b,c\in R$ tales que $\varphi(b)=s$ y $\varphi(c)=t$. Entonces $\varphi(bc)=st=\varphi(a)$ y como $\ker(\varphi)=\{0\}$, obtenemos que $a=bc$. Como a es irreducible, o bien b o bien c es una unidad de R. Por el ejercicio anterior, o bien r o bien s es una unidad de S. Es decir, $\varphi(a)$ es irreducible.

En la primera versión puse que si a es irreducible y φ es sobreyectivo, entonces $\varphi(a)$ era irreducible; pero esto es falso. Consideremos

$$\varphi=e_1\colon\mathbb{Q}[x]\to\mathbb{Q},$$

es un epimorfismo de anillos con $\ker(\varphi)=(x-1)$ (la descripción del núcleo no es necesaria para realizar el ejercicio, pero siempre está bien recordarlo). El elemento $x\in\mathbb{Q}[x]$ es irreducible, pero su imagen $\varphi(x)=1$ no es elemento irreducible.

16. Demuestra que:

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

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

Solución: Para el primer apartado, notamos que $\varphi(1) = 1$, entonces $\varphi(p) = \varphi(1+\cdots+1) = \varphi(1)+\cdots+\varphi(1) = p\varphi(1) = 0$ no es invertible, mientras que p es una unidad de $\mathbb{Q}$. Para el segundo apartado, analicemos la imagen de $\sqrt{2}$ por φ. Si $\varphi(\sqrt{2}) = a \in \mathbb{Q}$, entonces $2 = \varphi(2) = \varphi(\sqrt{2}^2) = \varphi(2)^2 = a^2$ (hemos usado que $\varphi(1) = 1$ y $\varphi(a+b) = \varphi(a) + \varphi(b)$ para la primera igualdad, como en el caso anterior). Entonces $a \in \mathbb{Q}$ es una raíz de 2, imposible pues $\sqrt{2}$ no es racional.
La idea que subyace a este ejercicio es que si φ es un homomorfismo de anillos, y tenemos una ecuación en R, entonces las imágenes por φ de soluciones de la ecuación en R son soluciones de la ecuación en S que resulta al aplicar φ a los coeficientes. Confrontar con el ejercicio 42 al final de esta hoja de problemas.

Anillos de polinomios

17. Prueba que $I = (2, x) \subseteq \mathbb{Z}[x]$ no es un ideal principal. En particular, $\mathbb{Z}[x]$ no es un dominio de ideales principales.

18. Demuestra que si R es un dominio de integridad y $f(x), g(x) \in R[x]$ son polinomios no nulos entonces el grado del producto es la suma de los grados. ¿Qué ocurre si R no es un dominio de integridad? Concluye que el anillo de polinomios $R[x]$ es un dominio de integridad si, y solo, si R es un dominio de integridad.

Solución: Basta notar que el coeficiente del término de mayor grado de fg es el producto de los coeficientes directores de f y g, que no es cero por ser R un dominio de integridad. En $\mathbb{Z}_4[x]$ el producto de $f(x) = 2x+1$ por sí mismo es $f(x)f(x) = (2x+1)^2 = 1$ que tiene grado 0.

19. Sea R un dominio de integridad. Demuestra que los únicos elementos invertibles de $R[x]$ son los elementos de R que son invertibles. ¿Sucede lo mismo si R no es un dominio de integridad?

En particular, se tiene que $\mathcal{U}(K[x]) = K^\times$, donde K es un cuerpo.
Sugerencia: para contestar la pregunta considera $\mathbb{Z}_4[x]$.

Solución: El ejemplo del ejercicio anterior contesta la segunda pregunta del actual. De hecho, $\mathcal{U}(\mathbb{Z}_4[x]) = \{2q+1 \mid q \in \mathbb{Z}_4[x]\}$. Para probar la primera parte, se puede usar un argumento de grados.

20. (Homomorfismo evaluación) Sea R un anillo y $a \in R$, prueba que la aplicación $e_a\colon R[x] \to R$ definida por $p \mapsto p(a)$ es un homomorfismo de anillos sobreyectivo. Si $R = K$ es un cuerpo, concluye que $\ker(e_a)$ es un ideal maximal de $K[x]$ y da un generador de $\ker(e_a)$.

21. Fijado un entero $n \in \mathbb{Z}$ con $n \geq 2$, demuestra que el anillo cociente $\mathbb{Z}[x]/n\mathbb{Z}[x]$ es isomorfo a $\mathbb{Z}_n[x]$. Concluye que el ideal $n\mathbb{Z}[x]$ es primo si, y solo si, n es un número primo.

Solución: Definimos $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}_n[x]$ como $\varphi(a_0 + \cdots + a_n x^n) = \overline{a_0} + \cdots + \overline{a_n}x^n$, donde $\overline{a}$ denota la clase módulo n de $a \in Z$ (es decir, φ es la reducción de coeficientes módulo n). Hay que comprobar que φ es un homomorfismo de anillos sobreyectivo. Esto es rutina, y en el ejercicio 34 **a)** se generaliza este hecho. Notamos que $\ker(\varphi) = n\mathbb{Z}[x] = (n)$. La primera parte del ejercicio es ahora consecuencia del Teorema de Isomorfía. Como $\mathbb{Z}_n[x]$ es un dominio de integridad si, y solo si, $\mathbb{Z}_n$ es dominio de integridad; por el Teorema de caracterización de ideales primos y maximales, concluimos que $n\mathbb{Z}[x]$ es primo si, y solo si, n es primo. Usando de nuevo esa caracterización podemos concluir que $n\mathbb{Z}[x]$ nunca es maximal. ¿Puedes encontrar un ideal propio I de $\mathbb{Z}[x]$ que contenga estrictamente a $n\mathbb{Z}[x]$ cuando $n\mathbb{Z}[x] \neq \mathbb{Z}[x]$?

22. ** Demuestra que en $\mathbb{Z}[x]$ el ideal $(5, x+2)$ es maximal y que el anillo cociente $\mathbb{Z}[x]/(5, x+2)$ es isomorfo al cuerpo $\mathbb{Z}_5$.
Sugerencia: prueba que $\mathbb{Z}[x]/(5, x+2) \cong \mathbb{Z}_5[x]/(x+2)$ y que $(x+2) = \ker(e_{-2})$.

Solución: Tenemos que $I = (5) \subseteq J = (x+2, 5) \subseteq \mathbb{Z}[x]$. Entonces $\mathbb{Z}[x]/(x+2, 5) \cong (\mathbb{Z}[x]/5\mathbb{Z}[x])/((x+2, 5)/(5)) \cong \mathbb{Z}_5[x]/(x+2)\mathbb{Z}_5[x] = \mathbb{Z}_5[x]/(x+2)$, en la última igualdad hemos abusado ligeramente de

notación. Hay que comprobar que el isomorfismo $\mathbb{Z}[x]/5\mathbb{Z}[x] \cong \mathbb{Z}_5[x]$ lleva $(x+2,5)/(5) = J/I = J/5\mathbb{Z}[x]$ en $(x+2)\mathbb{Z}_5[x]$. Una vez tenemos $\mathbb{Z}[x]/(x+2,5) = \mathbb{Z}_5[x]/(x+2)$ se trata de ver que $(x+2) = \ker(e_{-2})$ donde $e_{-2}\colon \mathbb{Z}_5[x] \to \mathbb{Z}_5$. Como $\mathbb{Z}_5[x]/\ker(e_{-2}) \cong \mathbb{Z}_5$ es un cuerpo, tenemos que $\mathbb{Z}[x]/(x+2,5)$ es un cuerpo y, por tanto, $(x+2,5)$ es un ideal maximal de $\mathbb{Z}[x]$. En el camino, hemos probado la existencia del isomorfismo deseado.

23. Considera el anillo cociente $R = \mathbb{Z}_3[x]/(x^2+x+1)$.

a) Describe los ideales de R. ¿Se trata de un cuerpo?

b) ¿Cuántos elementos tiene R?

c) Calcula $\overline{x+1}^{-1}$ en R.

Solución: Sea $f \in \mathbb{Z}_3[x]$, denotamos for $\overline{f} = f + I$, donde $I = (x^2+x+1)$. Es decir, $\overline{f} \in \mathbb{Z}_3[x]/I$ y todos los elementos de este anillo son de esta forma. Por el algoritmo de la división, si $g \in \mathbb{Z}_3[x]$ se tiene que $g = fd + r$ donde $\delta(r) < \delta(f) = 2$. Además, $\overline{g} = g + I = r + I = \overline{r}$. Es decir $R = \{\overline{ax+b} \mid a, b \in \mathbb{Z}_3\}$. Es decir, $\mathbb{Z}_3[x]/I$ tiene 9 elementos. Observamos que $(x+2)^2 = x^2+x+1 \in I$, así que $\overline{x+2}$ es un divisor de cero, y el anillo cociente no es un cuerpo. También podríamos haber notado que si $p(x) = x^2+x+1$, entonces $p(1) = 0 = p'(1)$, así que 1 es raíz de p con multiplicidad 2. Es decir, $p(x) = (x+2)^2$. Como $\mathbb{Z}_3[x]$ es un dominio de ideales principales, por el teorema de correspondencia de ideales, los ideales de R son todos principales. Sabemos que $\overline{f} \in R$ es una unidad si, y solo si, $\mathrm{mcd}(f,p) = 1$. Como podemos suponer que el gado de f es menor o igual a 1, $\overline{f}$ genera un ideal no trivial si, y solo si, $f(x) = x+2$. (Notamos que $(\overline{x+1}) = R$ porque $\overline{x+1}$ es una unidad en R). Los ideales de R son $\{0\}$, $(\overline{x+2}) = \{0, \overline{x+2}, \overline{x^2+1}\}$ y R. Para acabar $\overline{x}\overline{x+1} = 2$ luego $\overline{x+1}^{-1} = \overline{2x}$.

24. Sea $p \in \mathbb{Q}[x]$ dado por $p(x) = (x^2+1)(x^4+2x+2)$. Escribimos $R = \mathbb{Q}[x]/(p)$ y $\bar{f} = f + (p)$.

a) Describe los ideales en R. ¿Es R un cuerpo?

b) Decide justificadamente si $\overline{x}$ y $\overline{x+1}$ son divisores de cero en R.

c) Decide si $\overline{x}$ y $\overline{x+1}$ son elementos invertibles en R y, en caso afirmativo, encuentra sus inversos.
Sugerencia: el teorema del máximo común divisor y el algoritmo de la división son relevantes.

Solución: (a) Para describir los ideales de R, notad que por el Teorema de Correspondencia de ideales, y por ser $\mathbb{Q}[x]$ un dominio de ideales principales, en particular, R es un dominio de ideales principales. Los elementos de R se pueden describir todos como clases $\overline{f}$ de polinomios $f \in \mathbb{Q}[x]$ de grado menor o igual que 5 por el algoritmo de la división. Además, sabemos que $\overline{f} \in \mathcal{U}(R)$, si y solo si, $\mathrm{mcd}(f,p) = 1$. Es decir, que los elementos $\overline{f} \in R$ que generan ideales no triviales se corresponden con polinomios de grado menor o igual que 5, tales que $\mathrm{mcd}(f,p) > 1$. Como los factores x^2+1 y x^4+2x+2 de la descomposicin de p son irreducibles (por no tener raíces y por Einsestein, respectivamente). Si $\mathrm{mcd}(f,p) > 1$ con $\delta(f) \leq 5$ entonces $\mathrm{mcd}(f,p) = x^2+1$ o $\mathrm{mcd}(f,p) = x^4+2x+2$. En el primer caso $(\overline{f}) = (\overline{x^2+1})$ y en el segundo $(\overline{f}) = (\overline{x^4+2x+2})$. Con esto hemos probado que los ideales de R son:

$$\{0\}, (\overline{x^2+1}), (\overline{x^4+2x+2}), R\,.$$

(b) y (c) $\overline{x}$ y $\overline{x+1}$ son unidades de R porque $\mathrm{mcd}(x, p(x)) = 1 = \mathrm{mcd}(x+1, p(x))$. En particular no son divisores de 0. Por la identidad de Bézout, sabemos que existen $g, h \in \mathbb{Q}[x]$ tales que $1 = xg(x) + p(x)h(x)$. Entonces $1 = \overline{xg}(x)$, es decir, $\overline{g}$ es el inverso de $\overline{x}$ en R. Usando el algoritmo de la división:

$$p(x) = x^6 + x^4 + 2x^3 + 2x^2 + 2x + 2 = (x^5 + x^3 + 2x^2 + 2x + 2)x + 2\,.$$

Por tanto $1 = -\frac{1}{2}(x^5 + x^3 + 2x^2 + 2x + 2)x + \frac{1}{2}p(x)$. Tomando clases módulo p obtenemos $\overline{x}^{-1} = \overline{x^5 + x^3 + 2x^2 + 2x + 2} \in R$. El inverso de $\overline{x+1}$ se halla de forma similar.

25. Halla un generador de $I = (x^3+1, x^2+1)$ en $\mathbb{Z}_2[x]$.

Solución: Sabemos que $\mathbb{Z}_2[x]$ es un DIP. Para calcular un generador de I tenemos que escoger un $0 \neq f \in I$ con grado menor posible. La manera de calcular un elemento de estas características es usar el Teorema del máximo común divisor. Notamos que $x^3+1 = (x+1)(x^2+x+1)$ y $x^2+1 = (x+1)^2$, además $-1 = 1 \in \mathbb{Z}_2$ no es una raíz de x^2+x+1, por lo que $\mathrm{mcd}(x^3+1, x^2+1) = x+1$. Por un lado $I \subseteq (x+1)$. Por otro lado, por el Teorema del máximo común divisor sabemos existen $g, h \in \mathbb{Z}_3[x]$ de modo que $x+1 = (x^3+1)g(x) + (x^2+1)h(x)$, luego $(x+1) \subseteq I$. Entonces $I = (x+1)$. ¿Puedes encontrar $g, h \in \mathbb{Z}_3[x]$ tales que $x+1 = (x^3+1)g(x) + (x^2+1)h(x)$?

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

27. 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 $\mathbb{Z}_p[x]$.

28. Si $f \in \mathbb{Z}[x]$ y $r/s \in \mathbb{Q}$ es una raíz de f con $(r,s) = 1$, entonces s divide al coeficiente director de f y r divide al término independiente de f. En particular, las raíces racionales de polinomios enteros mónicos son números enteros.

Criterios de irreducibilidad

29. Considera un cuerpo K. Demuestra los siguientes enunciados:

a) (Teorema de Ruffini) Sean $p \in K[x]$ y $a \in K$. Entonces $p(a) = 0$ si, y solo si, $p(x) = (x-a)q(x)$ con $q \in K[x]$.

b) Todo polinomio de grado uno en $K[x]$ es irreducible.

c) Todo polinomio de grado dos o tres en $K[x]$ es irreducible si, y solo si, no tiene raíces en K.

30. Enumera todos los polinomios mónicos irreducibles de grado 1, 2, 3 y 4 de $\mathbb{Z}_2[x]$ y $\mathbb{Z}_3[x]$.

Solución: Hay que usar el ejercicio anterior, sabemos que todo polinomio de grado 1 es irreducible y que los de grado 2 y 3 son irreducibles, si y solo si, no tienen raíces. Finalmente, los polinomios de grado 4 son irreducibles si no tienen raíces y no pueden descomponerse como producto de dos polinomios de grado 2.

31. ¿Cuántos elementos tiene el anillo $\mathbb{Z}_3[x]/(x^2+1)$? ¿Se trata de un cuerpo?
Sugerencia: construye un homomorfismo $\mathbb{Z}_3[x] \to \mathbb{Z}_3[\xi]$ con núcleo (x^2+1), donde $\xi^2 = -1$.

32. Sea R un anillo y sea $a \in R$. Si $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$, definimos $f(x+a) = a_0 + a_1(x+a) + \cdots + a_n(x+a)^n \in R[x]$.

a) Demuestra que $f(x)$ es irreducible si, y solo si, $q(x) = f(x+a)$ es irreducibles.

b) Usa este resultado para probar que los polinomios $\Phi_p(x) = x^{p-1} + \cdots x + 1$ son irreducibles para todo p primo.
Sugerencia: prueba que $\Phi_p(x)(x-1) = x^p - 1$ y, a continuación, demuestra que $\Phi_p(x+1)$ es irreducible usando el criterio de Einsestein.

El polinomio Φ_p es el p-ésimo polinomio ciclotómico.

33. Sea $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ en $K[x]$ con $a_0 \cdot a_n \neq 0$. Prueba que f es irreducible si, y solo si, $\tilde{f}(x) = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$ es irreducible.

34. Decimos que un polinomio $f(x) \in \mathbb{Z}[x]$ es primitivo si el máximo común divisor de sus coeficientes es 1.

a) Prueba que un homomorfismo de anillos $\varphi\colon R \to S$ se extiende de manera natural a un homomorfismo de anillos $R[x] \to S[x]$. En particular, si p es un primo, la reducción de coeficientes módulo p define

un homomorfismo de anillos $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$.

b) Demuestra que en $\mathbb{Z}[x]$ el producto de dos polinomios primitivos es primitivo.
Sugerencia: usa el apartado anterior.

c) (Lema de Gauss) Sea $f(x) \in \mathbb{Z}[x]$ un polinomio de grado $n \geq 2$. Prueba que si $f(x)$ es reducible como polinomio en $\mathbb{Q}[x]$, entonces es reducible como polinomio en $\mathbb{Z}[x]$.

d) Sea $f(x) \in \mathbb{Z}[x]$ mónico y se $p \in \mathbb{Z}$ un primo. Consideramos $\bar{f}(x) \in \mathbb{Z}_p[x]$ la imagen de f via el homomorfismo de anillos $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Demuestra que si $\bar{f}(x)$ es irreducible en $\mathbb{Z}_p[x]$, entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.

e) Aplica el criterio anterior para deducir que $x^3 + x + 1$ es irreducible en $\mathbb{Q}[x]$.

Solución:

a) Sea $\varphi\colon R \to S$ un homomorfismo de anillos, se define de forma natural una aplicación que denotamos también por φ abusando de notación $\varphi\colon R[x] \to S[x]$, donde $\varphi(a_0 + \cdots + a_n x^n) = \varphi(a_0) + \cdots + \varphi(a_n)x^n$. Simplemente, estamos aplicando φ a los coeficientes de los polinomios en $R[x]$. Es rutinario comprobar que $\varphi\colon R[x] \to S[x]$ es un homomorfismo de anillos.

b) Sean $f, g \in \mathbb{Z}[x]$ primitivos. Por reducción al absurdo, supongamos que $fg \in \mathbb{Z}[x]$ no es primitivo. Entonces existe algún primo p que divide cada uno de los coeficientes de fg. Sea $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ el homomorfismo reducción módulo p de coeficientes, tenemos que

$$\varphi(f)\varphi(g) = \varphi(fg) = 0\,.$$

Como $\mathbb{Z}_p[x]$ es un dominio de integridad, $\varphi(f) = 0$ o $\varphi(g) = 0$. En cualquiera de los casos, obtenemos una contradicción con la hipótesis inicial de que f y g son primitivos.

c) Para probar este apartado, si $f \in \mathbb{Z}[x]$, vamos a denotar $c(f)$ al máximo común divisor de los coeficientes de f. Entonces f es pirmitivo, si y solo si, $c(f) = 1$. Además, cualquier $f \in \mathbb{Z}[x]$ se escribe como $f = c(f)\tilde{f}$, donde $f \in \mathbb{Z}[x]$ es primitivo. Por reducción al absurdo, supongamos que $f = gh$ con $g, h \in \mathbb{Q}[x]$ de grado menor que f. Entonces $c(f)\tilde{f} = a/b\tilde{g}c/d\tilde{h}$, donde $\tilde{g}, \tilde{h} \in Z[x]$ son primitivos. Para convenceros de esto, podéis escribir $g(x) = a_0/b_0 + \cdots + a_n/b_n x^n = 1/b(a_0 b_1 \cdots b_n + \cdots a_n b_0 \cdots b_{n-1}x^n)$ donde $b = b_0 \cdots b_n$ y luego tomar como $a = c(bg)$. Entonces $c(f) = ac/bd \in \mathbb{Z}$, de donde se sigue que podemos descomponer f como producto de $ac/bd\tilde{g} \in \mathbb{Z}[x]$ y $\tilde{h} \in \mathbb{Z}[x]$, ambos de grado menor que f; lo que contradice la hipótesis inicial.

d) Consideramos $x^3 + x + 1 \in \mathbb{Z}_2[x]$, que es irreducible porque no tiene raíces en $\mathbb{Z}_2$. Por el segundo apartado de este ejercicio $x^3 + x + 1$ es irreducible en $\mathbb{Z}[x]$, y por el Lema de Gauss es irreducible en $\mathbb{Q}[x]$.

35. Discute la irreducibilidad del polinomio $x^5 + 11x^2 + 15$ en $\mathbb{Q}[x]$.
Sugerencia: usa reducción de coeficientes módulo $p = 2$ y prueba que el polinomio resultante es irreducible en $\mathbb{Z}_2[x]$.

36. ** Prueba que el polinomio $x^4 + 1$ es irreducible en $\mathbb{Q}[x]$ pero reducible en $\mathbb{Z}_p[x]$ para todo primo p.
Sugerencia: deja los casos en que p es impar para más adelante.

Solución: Hay distintas formas de probar que x^4+1 es irreducible en $\mathbb{Q}[x]$. Una de ellas es calcular las raíces cuartas de -1 (que son las raíces octavas de la unidad que no son raíces cuartas) y usar que para cualquier cuerpo K, el anillo de polinomios $K[x]$ es un DFU. Como $x^4 + 1$ no tiene raíces en $\mathbb{Q}$ (ni en $\mathbb{R}$), si fuera reducible, tendría que ser producto de dos polinomios irreducibles en $\mathbb{Q}[x]$ de grado 2. De forma concreta, las raíces de $x^4 + 1$ son $\{\pm\frac{1}{\sqrt{2}} \pm \frac{1}{\sqrt{2}}i\}$, entonces, la descomposición como producto de irreducibles en $\mathbb{R}[x]$ es $(x^2 - 2/\sqrt{2}x + 1)(x^2 + 2/\sqrt{2}x + 1)$, y los factores no son polinomios racionales. Por ser $\mathbb{R}[x]$ un DFU, el polinomio $x^4 + 1$ no puede tener una descomposición distinta como producto de polinomios (racionales) de grado 2. Por tanto, $x^4 + 1$ es irreducible en $\mathbb{Q}[x]$.

Creo que otra manera de probar la irreducibilidad en $\mathbb{Q}[x]$ de este polinomio es probar que si $f(x) = x^4 + 1$, entonces $h(x) = f(x+2) = x^4 + 8x^3 + 48x^2 + 32x + 16$ es irreducible. Usando el criterio de reducción

módulo p con $p = 3$ se puede comprobar que $\overline{h}(x) = x^4 + 2x^3 + 2x + 1 \in \mathbb{F}_3[x]$ es irreducible ya que los únicos polinomios irreducibles de grado 2 en $\mathbb{F}_3[x]$ son $x^2 + 1, x^2 + x + 2, x^2 + 2x + 2$ (y ningún producto de dos de ellos resulta $\overline{h}$).

$x^4 + 1 = (x + 1)^4 \in \mathbb{F}_2[x]$. Analizar los casos en qué $p > 2$ requiere más conocimientos. Por ahora, basta con saber que existen polinomios enteros mónicos cuya reducción módulo p para todo p es reducible, pero que son irreducibles en $\mathbb{Q}[x]$.

37. Decide razonadamente si los siguientes polinomios son reducibles en $\mathbb{Q}[x]$:

$$f_1(x) = x^4 + 3x + 6, \quad f_2(x) = x^3 + 11^{11}x + 13^{13}, \quad f_3(x) = x^5 - 9x^2 + 1.$$

Solución. El polinomio f_1 es irreducible por el Criterio de Einsestein con $p = 3$.

Si reducimos el polinomio f_2 módulo 11 (que parece lo obvio a tenor del pequeño teorema de Fermat) se tiene que $f_2 \in \mathbb{F}_{11}[x]$ tiene a 9 como raíz. Si seguimos probando, con $p = 7$ obtendremos $f_2 = x^3 + 2x - 1 \in \mathbb{F}_7[x]$ que ahora sí no tiene raíces en $\mathbb{F}_7$. Otra forma es comprobar que f_2 no tiene raíces racionales usando que estas deberan ser enteras y divisoras de 13^{13}. Se puede descartar que un número positivo sería raíz y también que $d = -1$ y -13^{13} lo sean. Tomando una candidata a raíz $d = -13^j$ con $1 \leq j \leq 12$, evaluando f_2 y operando se llega a

$$11^1 1 = 13^{13-j} - 13^{2j}\,.$$

A la derecha de la igualdad encontramos un número divisible por 13, lo que contradice el teorema fundamental de la aritmética.

El polinomio f_3 no tiene raíces racionales porque ± 1 no son raíces (estamos usando el ejercicio 28). Por tanto, si se descompone como producto de polinomios de grado menor, necesariamente $f_3 = gh$ con $\delta(g) = 3$, $\delta(h) = 2$ y g y h irreducibles en $\mathbb{Q}[x]$. Por el Lema de Gauss además podemos suponer que $g, h \in \mathbb{Z}[x]$. Como el producto de los coeficientes directores de g y h es 1 podemos suponer que g y h son mónicos. Como el producto de sus términos independientes es 1, podemos concluir que ambos tienen el mismo término independiente. De la igualdad $x^5 - 9x^2 + 1 = (a_0 + a_1x + a_2x^2 + x^3)(a_0 + b_1x + x^2) = g(x)h(x)$ con $a_0^2 = 1$ y usando que los polinomios g y h no tienen raíces racionales, se puede obtener una contradicción. Es decir, f_3 es irreducible.

38. Demuestra que para cada $n \geq 1$ hay infinitos polinomios en $\mathbb{Q}[x]$ irreducibles de grado n.
Sugerencia: aplica el criterio de Einsestein.

39. Demuestra que todo polinomio irreducible en $\mathbb{R}[x]$ tiene grado 1 o 2. Factoriza $x^4 - 1$ como producto de polinomios mónicos irreducibles en $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_2[x]$ y $\mathbb{Z}_3[x]$.
Sugerencia: para la primera parte debes asumir el Teorema Fundamental del Álgebra, que probaremos a final de curso. Este dice que todo polinomio no constante en $\mathbb{C}[x]$ tiene una raíz en $\mathbb{C}$.

Solución: solamente nos faltó discutir la factorización the $f(x) = x^4 - 1$ como polinomio en $\mathbb{Z}_3[x]$. Vemos que $f(1) = 0 = f(2)$. Como $f'(x) = 4x = x \in \mathbb{Z}_3[x]$, las dos raíces $1, 2$ de f son simples. Por Ruffini, $x^4 - 1 = (x - 1)(x - 2)g(x)$, donde $g \in \mathbb{Z}_3[x]$ tiene grado 2 y no tiene raíces en $\mathbb{Z}_3$, es decir, g es irreducible en $\mathbb{Z}_3[x]$. ¿Cómo es un polinomio irreducible de grado 2 en $\mathbb{Z}_3[x]$? Es un polinomio sin raíces en $\mathbb{Z}_3$. Es fácil comprobar que $g(x) = x^2 + 1$, luego $x^4 - 1 = (x + 1)(x + 2)(x^2 + 1)$ (usando que $1 \equiv -2$ y $2 \equiv -1$ en $\mathbb{Z}_3$).

Cuerpos

Cuando p es un número primo, el anillo $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ tiene estructura de cuerpo. Cuando pensamos en $\mathbb{Z}_p$ como cuerpo, es común usar la notación $\mathbb{F}_p$.

Un cuerpo K tiene característica 0 si su cuerpo primo $F \cong \mathbb{Q}$. Un cuerpo K tiene característica p, si su cuerpo primo $F \cong \mathbb{F}_p$. Por el ejercicio 14 (por ejemplo), sabemos que $\mathbb{Q}$ no es isomorfo a ningún $\mathbb{F}_p$, y del mismo modo si p y q son primos distintos $\mathbb{F}_p$ no es isomorfo a $\mathbb{F}_q$. Más en general, tenemos el siguiente resultado que nos dice que no se pueden construir homomorfismos de anillos entre cuerpos con distinta característica.

40. Sea K un cuerpo de característica p. Demuestra que no existe ningún homomorfismo de cuerpos $\varphi\colon K \to \mathbb{Q}$ para ningún primo $p \in \mathbb{Z}$. En general, si K y E con cuerpos con distinta característica, prueba que entonces no existe ningún homomorfismo de cuerpos $\varphi\colon K \to E$.
Sugerencia: compara con el ejercicio 16.
Solución: como la característica de K es p, sabemos que $1 + \cdots + 1 = 0$ (donde estamos sumando p veces 1). Ahora bien $0 = \varphi(0) = \varphi(1 + \cdots + 1) = 1 + \cdots + 1 = p \in \mathbb{Q}$, una contradicción. De hecho, variaciones del mismo argumento muestran que tampoco podemos construir homomorfismos de cuerpos entre cuerpos con distinta característica.

41. (Frobenius) Sea K un cuerpo de característica p, probar que

$$(a+b)^p = a^p + b^p\,,$$

para todo $a, b \in K$. En particular, la aplicación Frob$\colon K \to K$ dada por $a \mapsto a^p$ es un homomorfismo de anillos inyectivo. Además, Frob fija el cuerpo primo de K.

Solución. Ya probamos que $(a+b)^p = a^p + b^p$ para todo $a, b \in K$ siendo K un cuerpo de carcterística p. De esto se concluye directamente que Frob$\colon K \to K$ dada por $a \mapsto a^p$ es un homomorfismo de anillos (cuerpos) inyectivo. Para la inyectividad, notar que $a^p = 0$ si, y solo si, $a = 0$ (pues estamos en un cuerpo).

La parte delicada es probar que si F es el cuerpo primo de K, entonces Frob$(a) = a$ para todo $a \in F$. Como K tiene característica p, sabemos que $F \cong \mathbb{F}_p$. De hecho, si 1_K es el neutro para el producto de K, entonces $F = \{0_F, 1_F, \ldots, (p-1)1_F\}$. Como Frob$(F) \subseteq K$ es un cuerpo, tenemos que $F \subseteq$ Frob(F). Ahora la restricción de Frob a F es un isomorfismo de cuerpos Frob$|_F\colon F \to$ Frob(F). Como $|F| = |$Frob$(F)|$ se sigue que Frob$|_F \in$ Aut(F). Como $F \cong \mathbb{F}_p$ y ya vimos que Aut$(\mathbb{F}_p) = \{id\}$, se tiene que Frob$|_F = id$, que es exactamente lo que queríamos probar.

42. Si $n > 0$ no es un cuadrado. Demuestra que:

a) $\mathbb{F}_3[\xi] = \{a + b\xi \mid a, b \in \mathbb{F}_3,\ \xi^2 = -1\}$ es un cuerpo.
Este cuerpo ya ha aparecido en esta hoja de problemas. Compara con el ejercicio 31.

b) $\mathbb{Q}[\sqrt{n}] := \{a + b\sqrt{n} : a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{R}$.

c) $\mathbb{Q}[\sqrt{-n}] := \{a + b\sqrt{-n} : a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{C}$.

d) No existe ningún homomorfismo de anillos (cuerpos) $\varphi\colon \mathbb{Q}[i] \to \mathbb{Q}[\sqrt{2}]$.

e) Existen infinitos homomorfismos de anillos $\varphi\colon \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$.

Solución: **d)** Notar que $i^2 = -1$, pero ningún elemento $\alpha \in \mathbb{Q}[\sqrt{2}]$ satisface $\alpha^2 = -1$. Por tanto, no podemos dar una imagen de i mediante un homomorfismo de anillos. *(Notad que en particular $\mathbb{Q}[i]$ y $\mathbb{Q}[\sqrt{2}]$ no pueden ser isomorfos como cuerpos, pues ni siquiera se puede construir un homomorfismo entre ellos.)*

e) En este caso, si mandamos $x \mapsto \alpha$ donde α varía en $\mathbb{Q}[\sqrt{2}]$ y fijamos elemento a elemento $\mathbb{Q}$ obtenemos infinitos homomorfismos de $\mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$. (Compara con el ejercicio 20.)