Ejercicios de *Introduction to Commutative Algebra*

1 Rings and Ideals

1.1 Elementos nilpotentes en anillos de polinomios, nilradical y radical de Jacobson

Ejercicio 1.1. Let x be a nilpotent element of a ring A. Show that $1 + x$ is a unit of A. Deduce that the sum of a nilpotent element and a unit is a unit.

Solución. Si $x \in A$ es nilpotente y $x^n = 0$, entonces $(-x)^n = 0$, también. Si $y = -x$,

$$(1 - y)\,(1 + y + \cdots + y^{n-1}) = 1 - y^n = 1 \ .$$

En particular, $1 - y = 1 + x$ es una unidad.

□

Ejercicio 1.2. Let A be a ring and let $A[x]$ be the ring of polynomials un an indeterminate x, with coefficients in A. Let $f = a_0 + a_1\,x + \cdots + a_m\,x^m \in A[x]$. Prove that:

(i) f is a unit in $A[x]$, if and only if a_0 is a unit in A and $a_1, \ldots, a_m$ are nilpotent;[1]

(ii) f is nilpotent, if and only if $a_0, a_1, \ldots, a_m$ are nilpotent;

(iii) f is a zero-divisor, if and only if there exists $a \neq 0$ in A such that $a\,f = 0$;[2]

(iv) f is said to be *primitive*, if $\langle a_0, a_1, \ldots, a_m\rangle = \langle 1\rangle$. Prove that, if $f, g \in A[x]$, then $f\,g$ is primitive, if and only if f and g are primitive.

Solución. Sean $f = a_0 + a_1\,x + \cdots + a_m\,x^m$ y $h \in A[x]$ tal que $f = a_0 + h\,x$, es decir, $h = a_1 + a_2\,x + \cdots + a_m\,x^{m-1}$. Supongamos, primero que a_0 es unidad en A y que $a_1, \ldots, a_m$ son nilpotentes. En este caso, h y $h\,x$ son nilpotentes en $A[x]$. Por el Ejercicio 1, f es una unidad.

---

[1]Hint: If $b_0 + b_1\,x + \cdots + b_n\,x^n$ is the inverse of f, prove, by induction on r, that $a_n^{r+1}\,b_{m-r} = 0$. Hence show that a_n is nilpotent, and then use Ex. .

[2]Hint: Choose a polynomial $g = b_0 + b_1\,x + \cdots + b_n\,x^n$ of least degree m such that $f\,g = 0$. Then $a_m\,b_n = 0$, hence $a_m\,g = 0$ (because $a_n\,g$ annihilates f and has degree less than n). Now show by induction that $a_{m-r}\,g = 0$.

Recíprocamente, supongamos que f es una unidad y que $g = b_0 + b_1\,x + \cdots\ b_n\,x^n$ es inverso de f. Supongamos, además, que $m = \mathsf{gr}(f)$ y que $n = \mathsf{gr}(g)$. Sea

$$c_k \;=\; \sum_{i+j=k} a_i\,b_j \tag{1}$$

el coeficiente en grado k del producto $f\,g$. Entonces, $c_0 = 1$ y $c_k = 0$, para todo $k \geq 1$. Dado que $a_i = 0$ y que $b_j = 0$, para $i > m$ y $j > n$, las únicas condiciones no triviales sobre los c_k y, en particular, sobre los coeficientes de f, se obtienen con $k \leq m + n$. Por ejemplo,

$$\begin{aligned}
1 \;&=\; c_0 \;=\; a_0\,b_0\ ,\\
0 \;&=\; c_1 \;=\; a_0\,b_1 + a_1\,b_0\ ,\\
&\;\vdots\\
0 \;&=\; c_{m+n-1} \;=\; a_m\,b_{n-1} + a_{m-1}\,b_n\ ,\\
0 \;&=\; c_{m+n} \;=\; a_m\,b_n\ .
\end{aligned}$$

Supongamos, primero, que $m = 0$. Entonces, $a_0 \in A^\times$ y su inverso es b_0. Pero $a_0\,b_j = 0$ (en A), para $j \geq 1$ implica que $b_j = 0$ y $n = 0$, también. Simétricamente, $n = 0$ implica $m = 0$. Si, en cambio, $m > 0$ (y, por lo tanto, $n > 0$), entonces $0 < 1 \leq m+n-1 < m+n$. En particular, como $b_n \neq 0$ y $a_m\,b_n = 0$, a_m es divisor de cero. Ahora, multiplicando la anteúltima condición por a_m, se deduce

$$0 \;=\; a_m^2\,b_{n-1} + a_m\,a_{m-1}\,b_n \;=\; a_m^2\,b_{n-1}\ .$$

Supongamos, inductivamente, que $n > r_0 \geq 0$ y que

$$a_m^{r+1}\,b_{n-r} \;=\; 0\ , \tag{2}$$

para todo $r \leq r_0$. En particular, $a_m^{r_0+1}\,b_j = 0$, para todo $j \geq n - r_0$. Para que b_j, con $j < n - r_0$, *no* aparezca en la sumatoria (1) que define al coeficiente c_k –cuestión válida, pues $a_i = 0$, si $i > m$–, es suficiente que $k \geq m + n - r_0$ (pues, en ese caso, $i \leq m$ y $j < n - r_0$ implican $i + j < m + n - r_0 \leq k$). Eligiendo $k = m + n - r_0 - 1$, como $k \geq m > 0$, $c_k = 0$ y

$$\begin{aligned}
0 \;=\; a_m^{r_0+1}\,c_k \;&=\; \sum_{\substack{i+j=k\\ j\geq n-r_0}} a_i\,a_m^{r_0+1}\,b_j\\
&=\; a_m^{r_0+2}\,b_{n-(r_0+1)}\ .
\end{aligned}$$

La última igualdad se deduce como consecuencia de lo mencionado luego de (2). Esto demuestra que $a_m^{r+1}\,b_{n-r} = 0$ para todo $r \geq 0$ y, en particular, que $a_m^{n+1}\,b_0 = 0$. Pero b_0 (al igual que a_0) es una unidad en A, con lo cual $a_m^{n+1} = 0$. Finalmente, como a_m es nilpotente (en A), $a_m\,x^m$ lo es en $A[x]$ y, apelando al Ejercicio (1), nuevamente,

$$f \;-\; a_m\,x^m$$

es una unidad (en $A[x]$). Inductivamente en el grado de f, se deduce que $a_0 \in A^\times$ y que $a_1, \ldots, a_m \in \mathfrak{N}(A)$. Esto prueba el ítem (i).

Si f es nilpotente (en $A[x]$), entonces $1 + f$ es una unidad en el anillo de polinomios y los coeficientes $a_0, a_1, \ldots, a_m$ son nilpotentes, por el ítem anterior, demostrando (ii).

En cuanto a (iii), si $a\,f = 0$, f es divisor de cero. Recíprocamente, si f es divisor de 0, existe $g \in A[x]$ no nulo, tal que $f\,g = 0$. Más aun, podemos asumir que $g = b_0 + b_1\,x + \cdots b_n\,x^n$ con n mínimo (en particular, $b_n \neq 0$ y $n = \mathsf{gr}(g)$). Dado que $a_m\,b_n = 0$ y que $(a_m\,g)\,f = 0$, por minimalidad de n, $a_m\,g = 0$. Si $h_r \in A[x]$ es el polinomio que se obtiene truncando f en grado r (h_r es de grado r o menor, o cero),

$$0 = f\,g = h_{m-1}\,g + a_m\,g\,x\ ,$$

de lo que se deduce que $h_{m-1}\,g = 0$. Esto implica que $a_{m-1}\,b_n = 0$ y que $a_{m-1}\,g = 0$, por la minimalidad de n. Inductivamente, $a_r\,g = 0$, para cada $r \geq 0$, y $a_r\,b_n = 0$. Esto implica que $f\,b_n = 0$.

Finalmente, para probar (iv), sean $f = a_0 + a_1\,x + \cdots + a_m\,x^m$ y $g = b_0 + b_1\,x + \cdots + b_n\,x^n$ y sea c_k el coeficiente en grado k del producto $f\,g$, dado por (1). Si $f\,g$ es primitivo y $\sum_k c_k\,\gamma_k = 1$, entonces $\sum_i a_i \Big(\sum_j b_j\,\gamma_{i+j} \Big) = 1$, lo que implica que f es primitivo. Si, en ca,bio, el producto $f\,g$ n es primitivo y el conjunto $\{c_k\}_k$ está contenido en algún ideal maximal $\mathfrak{m} \subset A$, entonces $f\,g = 0$ en $(A/\mathfrak{m})[x]$. Pero $A/\mathfrak{m}$ es cuerpo y, en particular, el anillo de polinomios $(A/\mathfrak{m})[x]$ es un dominio íntegro, con lo cual, o bien $f = 0$, o bien $g = 0$, allí; es decir, o bien f no es primitivo (y sus coeficientes están contenidos en $\mathfrak{m}$), o bien g no lo es.

□

Ejercicio 1.3. Generalize the results of Exercise 1.2 to a polynomial ring $A[x_1, \ldots, x_r]$ in several indeterminates.

Solución. □

Ejercicio 1.4. In the ring $A[x]$, the Jacobson radical is equal to the nilradical.

Solución. En un anillo conmutativo A, un elemento $x \in A$ pertenece al radical de Jacobson $\mathfrak{R}(A)$, si y sólo si $1 - y\,x \in A^\times$, cualquiera sea $y \in A$. También, x pertenece al nilradical $\mathfrak{N}(A)$, si y sólo si es nilpotente. Pasando al anillo de polinomios, si $f \in \mathfrak{R}(A[x])$, entonces $1 + f$ es una unidad y, como en la demostración del Ejercicio 1.2 (ii), los coeficientes de f son nilpotentes, lo que implica que f es nilpotente.

□

Ejercicio 1.5. Let A be a ring and let $A[\![x]\!]$ be the ring of formal power series $f = \sum_{n\geq 0} a_n\,x^n$ with coefficients in A. Show that:

(i) f is a unit in $A[\![x]\!]$, if and only if a_0 is a unit in A;

(ii) if f is nilpotent, then a_n is nilpotent for all $n \geq 0$. Is the converse true? (See Exercise **??**)

(iii) f belongs to the Jacobson radical of $A[\![x]\!]$, if and only if a_0 belongs to the Jacobson radical of A;

(iv) the contraction of a maximal ideal $\mathfrak{m}$ of $A[\![x]\!]$ is a maximal ideal of A, and $\mathfrak{m}$ is generated by $\mathfrak{m}^c$ and x;

(v) every prime ideal of A is the contraction of a prime ideal of $A[\![x]\!]$.

Solución. Si $f, g \in A[\![x]\!]$ con coeficientes a_i y b_j, respectivamente, el coeficiente en grado k del producto $f\,g$ está dado por $c_k = \sum_{i+j=k} a_i\, b_j$. En particular, si f es una unidad, $a_0\, b_0 = 1$ (en A), para cierto $b_0 \in A$. Recíprocamente, si $a_0\, b_0 = 1$ en A, entonces es posible definir, inductivamente, coeficientes b_j de manera que $g = \sum_{j\geq 0} b_j\, x^j$ sea el inverso de f:

$$b_k \;=\; \big(-\sum_{\substack{i+j=k\\ i\neq 0}} a_i\, b_j\big)\, b_0 \;. \tag{3}$$

Si f es nilpotente, existe $k \geq 0$ tal que $f^k = 0$. Para este valor de k, $a_0^k = 0$, es decir, a_0 es nilpotente en A. En particular, a_0 es nilpotente en $A[\![x]\!]$ y $f - a_0$ es nilpotente. Si $g = \sum_{i\geq 1} a_i\, x^{i-1}$, $f - a_0 = g\, x$ y existe $l \geq 0$ tal que $g^l\, x^l = 0$. Dado que una serie es igual a 0, si y sólo si sus coeficientes son todos nulos (en A), se deduce que $g^l = 0$, es decir, que g es nilpotente. Inductivamente, a_n es nilpotente para todo $n \geq 0$.

Elegir $\{a_n\}_{n\geq 0} \subset A$ tal que $a_n^{k(n)} = 0$ para una función creciente $k : \mathbb{N} \to \mathbb{N}$.

Si $f \in \mathfrak{R}(A[\![x]\!])$, cualquiera sea $a \in A \subset A[\![x]\!]$, vale que $1 - a\, f$ es una unidad en el anillo de series de potencias. El coeficiente principal de $1 - a\, f$ es igual a $1 - a\, a_0$ y debe ser, por (i), una unidad en A. Como $a \in A$ es arbitrario, se deduce que $a_0 \in \mathfrak{R}(A)$. Recíprocamente, si a_0 pertenece al radical de Jacobson de A y $g = \sum_{j\geq 0} b_j\, x \in A[\![x]\!]$,

$$1 - g\, f \;=\; (1 - b_0\, a_0) + h\, x \;,$$

para cierta $h \in A[\![x]\!]$. Dado que $1 - b_0\, a_0 \in A^\times$, se deduce que $1 - g\, f \in A[\![x]\!]^\times$. Así, $f \in \mathfrak{R}(A[\![x]\!])$.

Sea $\mathfrak{m} \subset A[\![x]\!]$ un ideal maximal y sea $\mathfrak{m}^c = \{a \in A \,:\, a \in \mathfrak{m}\} = \mathfrak{m} \cap A$ el ideal de A que se obtiene por contracción de $\mathfrak{m}$ vía la inclusión. Si $b \notin \mathfrak{m}^c$, entonce $b \notin \mathfrak{m}$ y $\langle b\rangle + \mathfrak{m} = A[\![x]\!]$. Es decir, para $b \in A$ que no pertenece a la contracción $\mathfrak{m}^c$, existe $f, h \in A[\![x]\!]$, $h \in \mathfrak{m}$, tales que

$$1 \;=\; f\, b + h \;.$$

Si $f = \sum_{k\geq 0} f_k\, x^k$ y $h = \sum_{k\geq 0} h_k\, x^k$, entonces, en particular,

$$1 \;=\; f_0\, b + h_0 \;,$$

en A. Si $x \in \mathfrak{m}$, entonces $h - h_0 = \tilde{h}\, x \in \mathfrak{m}$, para cierta $\tilde{h} \in A[\![x]\!]$, de lo que se deduce que $h_0 \in \mathfrak{m}^c$ y, dado que b fue elegido de manera arbitraria en el complemento de $\mathfrak{m}^c$, concluimos que este ideal es maximal en A. En definitiva, todo lo que hay que verificar es que $x \in \mathfrak{m}$, cualquiera sea el ideal maximal $\mathfrak{m} \subset A[\![x]\!]$. Esta afirmación es consecuencia de (i): si $x \notin \mathfrak{m}$, entonces

$$1 = f\,x + h\ ,$$

para ciertas $f, h \in A[\![x]\!]$, $h \in \mathfrak{m}$. Pero, entonces, $h_0 = 1$ y h es una unidad, contradiciendo el hecho de que $\mathfrak{m}$ es un ideal propio de $A[\![x]\!]$.

De esto último, se deduce que, si $\mathfrak{m} \subset A[\![x]\!]$ es maximal y $h \in \mathfrak{m}$, entonces, como $x \in \mathfrak{m}$, $h_0 \in \mathfrak{m}^c$. En conclusión,

$$\mathfrak{m} = \mathfrak{m}^c + \langle x \rangle\ .$$

□

1.2 Otro caso en que $\mathfrak{N} = \mathfrak{R}$

Ejercicio 1.6. A ring A is such that every ideal not contained in the nilradical contains a nonzero idempotent (that is, an elemento e such that $e^2 = e \neq 0$). Prove that the nilradical and the Jacobson radical of A are equal.

Solución. Si $x \in \mathfrak{R}(A) \smallsetminus \mathfrak{N}(A)$, entonces el ideal $\langle x \rangle$ no está contenido en el nilradical y existe, por hipótesis, $e = a\,x \in \langle x \rangle$ idempotente no nulo. Como x pertenece al radical de Jacobson, $u = 1 - a\,x = 1 - e$ es una unidad en A. La igualdad $u^2 = u$ fuerza que $u = 1$ y $e = 0$, lo que es absurdo, pues e es no nulo.

□

1.3 Un caso de altura cero

Ejercicio 1.7. Let A be a ring in which every element x satisfies $x^n = x$ for some $n > 1$ (depending on x). Show that every prime ideal in A is maximal.

Solución. Si $\mathfrak{p} \subset A$ es un primo y $x \notin \mathfrak{p}$ y $n > 1$ es tal que $x^n = x$, entonces $x\,(x^{n-1} - 1) = 0 \in \mathfrak{p}$ implica $x^{n-1} - 1 \in \mathfrak{p}$. En particular, para todo $x \notin \mathfrak{p}$, $x^m \in 1 + \mathfrak{p}$, para cierto $m \geq 1$ ($m = n - 1$ tal que $x^{m+1} = x$). Entonces, $1 \in \langle x \rangle + frakp$ y $\mathfrak{p}$ es maximal.

□

1.4 Existencia de primos minimales

Ejercicio 1.8. Let A be a ring different from 0. Show that the set of prime ideals of A has minimal elements with respect to inclusion.

Solución. Existen ideales maximales. Los ideales maximales son primos. Si $\mathcal{C}$ es una cadena de ideales primos ordenada por inclusión ($\mathfrak{p} < \mathfrak{p}'$, si $\mathfrak{p} \supset \mathfrak{p}'$), entonces $\mathfrak{q} = \bigcap \mathcal{C}$ es un ideal primo: si $x\,y \in \mathfrak{q}$, entonces, para cada $\mathfrak{p} \in \mathcal{C}$, o bien $x \in \mathfrak{p}$, o bien $y \in \mathfrak{p}$. Si ni x, ni y pertenecieran a, $\mathfrak{q}$, existirían primos $\mathfrak{p}$ y $\mathfrak{p}'$ pertenecientes a la cadena tales que $x \notin \mathfrak{p}$ e $y \notin \mathfrak{p}'$. Sin pérdida de generalidad, $\mathfrak{p} < \mathfrak{p}'$, de lo que se deduciría que ni x, ni y pertenecen a $\mathfrak{p}'$.

□

1.5 Ideales radicales

Ejercicio 1.9. Let $\mathfrak{a} \neq 1$ be an ideal in a ring A. Show that $\mathfrak{a} = \mathsf{rad}(\mathfrak{a})$, if and only if $\mathfrak{a}$ is an intersection of prime ideals.

Solución. Si S es una familia de ideales primos que contienen a $\mathfrak{a}$, entonces $\bigcap S \supset \mathsf{rad}(\mathfrak{a})$, pues el radical de un ideal conincide con la intersección de los ideales primos que lo contienen. La afirmación del ejercicio es consecuencia de la inclusión $\mathsf{rad}(\mathfrak{a}) \supset \mathfrak{a}$.

□

1.6 El caso de un único ideal primo

Ejercicio 1.10. Let A be a ring, $\mathfrak{N}$ its nilradical. Show that the following are equivalent:

(i) A has exactly one prime ideal;

(ii) every element of A is either a unit or nilpotent;

(iii) $A/\mathfrak{N}$ is a field.

Solución. Asumiendo (iii), $\mathfrak{N}$ es un ideal maximal. En particular, todo ideal primo es igual a $\mathfrak{N}$, lo que implica (i).

Asumiendo (ii), para todo $x \notin \mathfrak{N}$, $x \in A^\times$, lo que implica (iii).

Asumiendo (i), $\mathfrak{N}$ es el único ideal primo y, en particular, el único ideal maximal. En consecuencia, si $x \in A$ no es una unidad, entonces $x \in \mathfrak{N}$, es decir, (ii).

□

1.7 Anillos de Boole

Ejercicio 1.11.

Solución. □

1.8 Idempotentes en anillos locales

Ejercicio 1.12.

Solución. □

1.9 Construction of an algebraic closure of a field (d'après E. Artin)

Ejercicio 1.13. Let K be a field and let Σ be the set of all irreducible monic polynomials f in one indeterminate with coefficients in K. Let A be the polynomial ring over K generated by the indeterminates x_f, one for each $f \in \Sigma$. Let $\mathfrak{a}$ be the ideal of A generated by the polynomials $f(x_f)$ for all $f \in \Sigma$. Show that $\mathfrak{a} \neq \langle 1 \rangle$.

Let $\mathfrak{m}$ be a maximal ideal of A containing $\mathfrak{a}$, and let $K_1 = A/\mathfrak{m}$. Then K_1 is an extension field of K in which each $f \in \Sigma$ has a root. Repeat the construction with K_1 in place of K, obtaining a field K_2, and so on. Let $L = \bigcup_{n \geq 1} K_n$. Then L is a field in which each $f \in \Sigma$ splits completely into linear factors. Let $\overline{K}$ be the set of all elements of L which are algebraic over K. Then $\overline{K}$ is an algebraic closure of K.

Solución. Si $\mathfrak{a} = \langle 1 \rangle$, existirían $f_1, \ldots, f_r \in \Sigma$ y $h_1, \ldots, h_r \in A$ tales que

$$1 = h_1 f_1(x_{f_1}) + \cdots + h_r f_r(x_{f_r}) . \tag{4}$$

Esta igualdad es válida, en particular, en el subanillo $B \subset A$ compuesto por todos aquellos polinomios con coeficientes en K que involucran, únicamente, las variables x_{f_i} y las x_f que aparecen en los h_i; el anillo B es una anillo de polinomios en una cantidad finita de indeterminadas. Por otro lado, existe una extensión finita E/K que contiene, para cada f_i, una raíz α_i. Por propiedad universal del anillo de polinomios B, existe un único morfismo de K-álgebras $\mu : B \to E$ que verifica

$$\mu(x_f) = \begin{cases} \alpha_i & \text{si } f = f_i \ , \\ 0 & \text{en otro caso.} \end{cases}$$

(Es suficiente pedir que $\mu(x_{f_i}) = \alpha_i$, aunque se pierda la unicidad de μ). Aplicando μ a la identidad (4), se deduce que $1 = 0$ en E. Pero esto es absurdo, pues E es un cuerpo.

El cuerpo L es algebraicamente cerrado, pues todo polinomio $f \in L[x]$ tiene coeficientes pertenecientes a algún subcuerpo K_n y, por lo tanto, f posee alguna raíz en $K_{n+1} \subset L$.

□

1.10 Los divisores de cero

Ejercicio 1.14. In a ring A, let Σ be the set of all ideals in which every element is a zerodivisor. Show that the set Σ has maximal elements and that every maximal element of Σ is a prime ideal. Hence the set of zerodivisors in A is a union of prime ideals.

Solución. Sea $D \subset A$ el conjunto de todos los divisores de cero en A y sea $\mathcal{M}$ el conjunto de los elementos maximales de la familia Σ. En primer lugar, asumiendo que Σ posee elementos maximales, si $x \in D$, el ideal $\langle x \rangle$ pertenece a Σ y está contenido en algún $I \in \mathcal{M}$. Entonces, $D \subset \bigcup \mathcal{M}$ y, como los ideales pertenecientes a Σ están incluidos, por definición, en D, $\bigcup \mathcal{M} \subset D$. Es decir, D es la unión de los elementos maximales de Σ. Más aun, si dichos elementos son ideales primos, entonces D es unión de ideales primos. Esto prueba la última afirmación.

La familia Σ es no vacía: $0 \in \Sigma$. Si $\mathcal{C}$ es una cadena de elementos de la familia ordenada por inclusión, entonces $\bigcup \mathcal{C}$ es un ideal y todos sus elementos son divisores de cero. En conclusión, Σ posee elementos maximales.

Sea $I \in \Sigma$ un elemento maximal y sean $x, y \in A$ tales que $x\,y \in I$. Esto implica que $x\,y$ es divisor de cero y existe $a \in A$ no nulo, tal que $x\,y\,a = 0$. Si $y\,a = 0$, y es divisor de cero, si no, x es divisor de cero. En el primer caso, $\langle y \rangle + I \in \Sigma$, con lo cual, por maximalidad de I, $y \in I$. En el segundo caso, $x \in I$. En definitiva, I es primo.

□

1.11 The prime spectrum of a ring

Ejercicio 1.15. Let A be a ring and let X be the set of all prime ideals of A. For each subset E of A, let $\mathcal{V}(E)$ denote the set of all prime ideals of A which contain E. Prove that

(i) if $\mathfrak{a}$ is the ideal generated by E, then $\mathcal{V}(E) = \mathcal{V}(\mathfrak{a}) = \mathcal{V}(\mathsf{rad}\,\mathfrak{a})$;

(ii) $\mathcal{V}(0) = X$, $\mathcal{V}(1) = \varnothing$;

(iii) if $\{E_i\}_i$ is any family of subsets of A, then

$$\mathcal{V}(\bigcup_i E_i) = \bigcap_i \mathcal{V}(E_i) \ ;$$

(iv) $\mathcal{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathcal{V}(\mathfrak{a}\,\mathfrak{b}) = \mathcal{V}(\mathfrak{a}) \cup \mathcal{V}(\mathfrak{b})$.

These results show that the sets $\mathcal{V}(E)$ satisfy the axioms for closed sets in a topological space. The resulting topology is called the *Zariski topology*. The topological space X is called *the prime spectrum of* A, and is written $\mathsf{Spec}(A)$.

Solución. □

Ejercicio 1.16. Draw pictures of $\mathsf{Spec}(\mathbb{Z})$, $\mathsf{Spec}(\mathbb{R})$, $\mathsf{Spec}(\mathbb{C}[x])$, $\mathsf{Spec}(\mathbb{R}[x])$, $\mathsf{Spec}(\mathbb{Z}[x])$.

Solución. □

Ejercicio 1.17. For each $f \in A$, let X_f denote the complemento of $\mathcal{V}(f)$ in $X = \mathsf{Spec}(A)$. The sets X_f are open. Show that they form a basis of open sets for the Zariski topology, and that:

(i) $X_f \cap X_g = X_{f\,g}$;

(ii) $X_f = \varnothing$, if and only if f is nilpotent;

(iii) $X_f = X$, if and only if f is a unit;

(iv) $X_f = X_g$, if and only if $\mathsf{rad}(\langle f \rangle) = \mathsf{rad}(\langle g \rangle)$;

(v) X is (quasi-) compact (that is, every open covering of X has a finite subcovering);[3]

(vi) more generally, each X_f is (quasi-) compact;

[3]Hint: To prove (v), remark that it is enough to consider a convering of X by basic open sets X_{f_i} ($i \in I$). Show that the f_i generate the unit ideal and hence that there is an equation of the form

$$1 = \sum_j g_j\, f_j$$

($g_i \in A$), where J is some *finite* subset of I. Then the X_{f_j} ($j \in J$) cover X.

(vii) an open subset of X is (quasi-) compact, if and only if it is a finite union of sets X_f.

The sets X_f are called *basic open sets* of $X = \mathsf{Spec}(A)$.

Solución. Todo abierto es de la forma $\mathsf{Spec}(A) \smallsetminus \mathcal{V}(\mathfrak{a})$ para algún ideal $\mathfrak{a} \subset A$. Dados, entonces $\mathfrak{a}$ y $x \in \mathsf{Spec}(A) \smallsetminus \mathcal{V}(A)$, existe $f \in \mathfrak{a}$ tal que $f \notin \mathfrak{p}_x$. Dado que

$$X_f \;=\; \big\{ y \in \mathsf{Spec}(A) \;:\; f \notin \mathfrak{p}_y \big\}\;, \tag{5}$$

se concluye que $x \in X_f \subset \mathsf{Spec}(A) \smallsetminus \mathcal{V}(\mathfrak{a})$. En definitiva, los conjuntos X_f constituyen una base de abiertos para la topología de Zariski.

Para probar que $\mathsf{Spec}(A)$ es compacto, será suficiente demostrar que todo cubrimiento por abiertos principales, es decir, de la forma X_f, admite un subcubrimiento finito, puesto que todo abierto es unión de abiertos básicos. Supongamos, entonces, que $\{f_i\}_i$ es una familia de elementos de A tal que

$$\mathsf{Spec}(A) \;=\; \bigcup_i X_{f_i}\;.$$

El ideal $\mathfrak{a} = \langle f_i \,:\, i \rangle$ no está contenido en ningún ideal primo, ya que, si $\mathfrak{p} \supset \mathfrak{a}$, entonces $f_i \in \mathfrak{p}$ para todo i, lo que equivale a que el punto correspondiente a $\mathfrak{p}$ no pertenezca a ninguno de los X_{f_i}. Expresado de otra manera, $\mathfrak{a} = 1$, es decir que existen un subconjunto finito de índices j y elementos correspondientes $g_j \in A$ tales que

$$1 \;=\; \sum_j g_j\, f_j\;.$$

Así, si $x \in \mathsf{Spec}(A)$, $1 \notin \mathfrak{p}_x$ y existe j tal que $f_j \notin \mathfrak{p}_x$, lo que quiere decir que $x \in X_{f_j}$.

Los abiertos X_f también son compactos, pues la localización $A \to A_f$ induce un homeomorfismo $X_f = \mathsf{Spec}(A_f)$.

□

Ejercicio 1.18. For psychological reasons it is sometimes convenient to denote a prime ideal of A by a letter such as x or y when thinking of it as a point of $X = \mathsf{Spec}(A)$. When thiinking of x as a prime ideal of A, we denote it by $\mathfrak{p}_x$ (logically, of course, it is the same thing). Show that:

(i) the set $\{x\}$ is closed (we say that x is a “closed point”) in $\mathsf{Spec}(A)$, if and only if $\mathfrak{p}_x$ is maximal;

(ii) $\overline{\{x\}} = \mathcal{V}(\mathfrak{p}_x)$;

(iii) $y \in \overline{\{x\}}$, if and only if $\mathfrak{p}_x \subset \mathfrak{p}_y$;

(iv) X is a T_0-space (this means that, if x and y are distinct points of X, then either there is a neighbourhood of x which does not contain y, or else there is a neighbourhood of y which does not contain x).

Solución. □

Ejercicio 1.19. A topological space X is said to be *irreducible*, if $X \neq \varnothing$ and if every pair of nonempty open sets in X intersect, or equivalently if every nonempty open set is dense in X. Show that $\mathsf{Spec}(A)$ is irreducible, if and only if the nilradical of A is a prime ideal.

Solución. □

Ejercicio 1.20. Let X be a topological space.

(i) If Y is an irreducible (Exercise 1.19) subspace of X, then the closure $\overline{Y}$ of Y in X is irreducible.

(ii) Every irreducible subspace of X is contained in a maximal irreducible subspace.

(iii) The maximal irreducible subspaces of X are closed and cover X. They are called the *irreducible components of* X. What are the irreducible components of a Hausdorff space?

(iv) If A is a ring and $X = \mathsf{Spec}A$, then the irreducible components of X are the closed sets $\mathcal{V}(\mathfrak{p})$, where $\mathfrak{p}$ is a minimal prime ideal of A (Exercise 1.8).

Solución. Sea A un anillo y sea $X = \mathsf{Spec}(A)$ su espectro. Por los Ejercicios 1.18 (ii) y 1.20 (i), si $\mathfrak{p} \subset A$ es primo, el conjunto $\mathcal{V}(\mathfrak{p})$ es irreducible (los espacios con un único punto son irreducibles). Para probar que las componentes irreducibles (cerrados irreducibles maximales de X) están en correspondencia con los primos minimales de A, será suficiente probar que, si $\mathfrak{b} \subset A$ es un ideal radical tal que $\mathcal{V}(\mathfrak{b})$ es irreducible, entonces $\mathfrak{b}$ es primo.

Sean $f, g \in A$ tales que $f\,g \in \mathfrak{b}$, pero ni f ni g pertenecen a $\mathfrak{b}$. Por el Ejercicio 1.17 (i), $X_{f\,g} = X_f \cap X_g$ y, si $\mathfrak{p} \supset \mathfrak{b}$ es un ideal primo, entonces $f\,g \in \mathfrak{p}$, es decir, $\mathfrak{p} \notin X_{f\,g}$. Ahora, dado que $f \notin \mathfrak{b}$ y que $\mathfrak{b}$ es radical, existe $\mathfrak{p} \in \mathcal{V}(\mathfrak{b})$ tal que $f \notin \mathfrak{p}$; análogamente, existe $\mathfrak{q} \in \mathcal{V}(\mathfrak{b})$ tal que $g \notin \mathfrak{q}$. Esto implica que $X_f \cap \mathcal{V}(\mathfrak{b})$ y $X_g \cap \mathcal{V}(\mathfrak{b})$ son abiertos no vacíos de $\mathcal{V}(\mathfrak{b})$, pero

$$\big(X_f \cap \mathcal{V}(\mathfrak{b})\big) \cap \big(X_g \cap \mathcal{V}(\mathfrak{b})\big) = X_{f\,g} \cap \mathcal{V}(\mathfrak{b}) = \varnothing \,.$$

En particular, $\mathcal{V}(\mathfrak{b})$ no puede ser irreducible, si $\mathfrak{b}$ no es primo.

□

1.12 El Teorema de Stone

1.13 El espectro maximal

1.14 Variedades afines

2 Modules

Ejercicio 2.1.

Solución. $\square$

Ejercicio 2.2. Let A be a ring, $\mathfrak{a}$ an ideal and M an A-module. Show that $(A/\mathfrak{a}) \otimes_A M$ is isomorphic to $M/\mathfrak{a}\,M$.[4]

Solución. Si bien M podría no ser playo, tensorizar con M preserva la inyectividad, en este caso. Por exactitud del producto tensorial, la sucesión

$$\mathfrak{a} \otimes_A M \longrightarrow A \otimes_A M \longrightarrow (A/\mathfrak{a}) \otimes_A M \longrightarrow 0 \tag{6}$$

es exacta. Resta ver que el núcleo del primer morfismo de la izquierda es cero. Ahora bien,

$$\mathfrak{a} \otimes_A M \;\simeq\; A \otimes_A \mathfrak{a}\,M \;\simeq\; \mathfrak{a}\,M \ , \tag{7}$$

con lo cual, la exactitud de

$$0 \longrightarrow \mathfrak{a}\,M \longrightarrow M$$

implica la exactitud de

$$0 \longrightarrow A \otimes_A \mathfrak{a}\,M \longrightarrow A \otimes_A M \quad ,$$

pues A es playo y, así,

$$0 \longrightarrow \mathfrak{a} \otimes_A M \longrightarrow M$$

es exacta.

Otra manera de probar la inyectividad de $\mathfrak{a} \otimes_A M \to M$ es la siguiente: si $\sum a \otimes x$ es tal que $\sum a\,x = 0$ en M, entonces

$$\sum a \otimes x \;=\; \sum 1 \otimes \cdots \qquad !$$

¡Ah! Entonces, en la ecuación (7), el morfismo natural $\mathfrak{a} \otimes_A M \to M$ dado por $a \otimes x \mapsto a\,x$ no es un isomorfismo, en general. Por ejemplo, si $A = \mathbb{Z}$, $\mathfrak{a} = 2\,\mathbb{Z}$ y $M = \mathbb{Z}/2\mathbb{Z}$, entonces

$$2\,\mathbb{Z} \otimes_{\mathbb{Z}} (Z/2\,\mathbb{Z}) \;\not\simeq\; (2\,\mathbb{Z})\,(\mathbb{Z}/2\mathbb{Z}) \ ,$$

pues el lado izquierdo no es el módulo trivial, mientras que el de la derecha sí lo es.

De esto se puede observar, en primer lugar, que el isomorfismo (7) es equivalente a la inyectividad de $\mathfrak{a} \otimes_A M \to M$. En segundo lugar, si M es playo, entonces el isomorfismo (7) es válido. Si A es un dominio de Dedekind y M es un ideal de A, entonces (7) se cumple.

En el contraejemplo a la afirmación, la sucesión exacta corta

[4]Hint: Tensor the exact sequence

$$0 \longrightarrow \mathfrak{a} \longrightarrow A \longrightarrow A/\mathfrak{a} \longrightarrow 0$$

with M.

$$0 \longrightarrow 2\,\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

da lugar a la sucesión exacta

$$2\,\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \xrightarrow{0} \mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \longrightarrow (\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \longrightarrow 0 \quad .$$

Dado que, en este caso, $\mathfrak{a}\,M = 0$, se deduce que el isomorfismo $(A/\mathfrak{a}) \otimes_A M \simeq M/\mathfrak{a}\,M$ es válido, aunque (7) no lo sea.

En el caso general, la sucesión (6) es exacta. Dado que la imagen del primer morfismo es el submódulo $\mathfrak{a}\,M$ (identificando M con $A \otimes_A M$) y dado que el segundo morfismo es sobreyectivo, se deduce que

$$(A/\mathfrak{a}) \otimes_A M \;\simeq\; M/\mathfrak{a}\,M \ .$$

$\square$

3 Rings and Modules of Fractions

4 Notas varias

4.1 Lema de Nakayama

¿Es cierto que $\mathfrak{a} \subset \mathfrak{R}$, si y sólo si los elementos de $1 + \mathfrak{a}$ son unidades?

4.2 Sucesiones exactas

Sea A un anillo (conmutativo con 1) y sean M, M' y M'' tres A-módulos y sean $f : M' \to M$ y $g : M \to M''$ morfismos. Si la sucesión *de A-módulos*

$$0 \longrightarrow \mathsf{Hom}_A(M'', N) \xrightarrow{g^*} \mathsf{Hom}_A(M, N) \xrightarrow{f^*} \mathsf{Hom}_A(M', N)$$

es exacta para todo A-módulo N, entonces la sucesión

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

es exacta.

Observación 4.1. Esta es la versión contravariante. La versión covariante se deduce del isomorfismo $\mathsf{Hom}_A(A, N) \simeq N$.

Para demostrar la afirmación, consideramos, en primer lugar, el módulo $N = \mathsf{coker}(g)$ y el diagrama conmutativo:

$$\begin{tikzcd} M \arrow[r, "g"] \arrow[dr] & M'' \arrow[d] \\ & \mathsf{coker}(g) \end{tikzcd},$$

donde la flecha vertical es el cociente por el submódulo $\mathsf{img}(g)$ y la flecha diagonal es la composición de g con el mismo. Notamos que g es sobre, si *y sólo si* el cociente es el morfismo nulo. En particular, la inyectividad de g^* y el hecho de que la composición de g con el cociente es cero implican que g debe ser sobre.

Por otro lado, $g \circ f = f^*(g) = f^* \circ g^*(\mathsf{id}_{M''})$. Tomando $N = M''$ en la sucesión exacta, se deduce que $g \circ f = 0$ y, por lo tanto, que $\mathsf{img}(f) \subset \mathsf{ker}(g)$.

Finalmente, tomamos $N = \mathsf{coker}(f)$ y consideramos el diagrama

$$\begin{tikzcd} M \arrow[r] \arrow[d, "g"'] & \mathsf{coker}(f) \\ M'' \arrow[ur, dashed] & \end{tikzcd},$$

donde la flecha horizontal es el cociente. Dado que f^* aplicada al morfismo cociente da cero, el mismo debe, por exactitud, pertenecer a la imagen de g^*, es decir, debe existir una flecha diagonal que haga conmutar el diagrama anterior. De la existencia de tal morfismo y de que el núcleo del cociente es $\mathsf{img}(f)$, se deduce que $\mathsf{ker}(g) \subset \mathsf{img}(f)$.

4.3 Exactitud de funtores adjuntos

El bifuntor Hom posee las siguientes propiedades:

Proposición 4.2. *Sea A un anillo conmutativo con unidad y sean $f : M' \to M$ y $g : M \to M''$ morfismos de A-módulos. Entonces,*

(i) la sucesión

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

es exacta, si y sólo si, para todo A-módulo N, la sucesión

$$0 \longrightarrow \mathsf{Hom}_A(M'', N) \xrightarrow{g^*} \mathsf{Hom}_A(M, N) \xrightarrow{f^*} \mathsf{Hom}_A(M', N)$$

lo es;

(ii) la sucesión

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$$

es exacta, si y sólo si, para todo A-módulo P, la sucesión

$$0 \longrightarrow \mathsf{Hom}_A(P, M') \xrightarrow{f_*} \mathsf{Hom}_A(P, M) \xrightarrow{g_*} \mathsf{Hom}_A(P, M'')$$

lo es.

Sean T y U funtores adjuntos, es decir, que verifican

$$\mathsf{Hom}_A(T(M), N) \simeq \mathsf{Hom}_A(M, U(N))$$

naturalmente. Entonces, dada una sucesión exacta corta

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0 \quad ,$$

para todo N, la siguiente es una sucesión exacta corta:

$$0 \longrightarrow \mathsf{Hom}_A(M'', U(N)) \xrightarrow{g^*} \mathsf{Hom}_A(M, U(N)) \xrightarrow{f^*} \mathsf{Hom}_A(M', U(N)) \quad .$$

Pero esta sucesión es *equivalente* a

$$0 \longrightarrow \mathsf{Hom}_A(T(M''), N) \xrightarrow{T(g)^*} \mathsf{Hom}_A(T(M), N) \xrightarrow{T(f)^*} \mathsf{Hom}_A(T(M'), N) \quad .$$

Como la exactitud de esta sucesión es válida para todo A-módulo N, la sucesión

$$T(M') \xrightarrow{T(f)} T(M) \xrightarrow{T(g)} T(M'') \longrightarrow 0$$

es exacta. Análogamente, se demuestra que, si la sucesión

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$$

es exacta, entonces la siguiente es una sucesión exacta corta, también:

$$0 \longrightarrow U(M') \xrightarrow{U(f)} U(M) \xrightarrow{U(g)} U(M'') \quad .$$

4.4 Primos minimales

Proposición 4.3. *Los ideales primos minimales están contenidos en el conjunto de divisores de cero.*

Sea A un anillo conmutativo con unidad y sea D el *conjunto*[5] de divisores de cero de A. El radical de un subconjunto $E \subset A$ es el conjunto $\mathsf{rad}(E)$ compuesto por todos los elementos del anillo que, elevados a alguna potencia, pertenecen a E. Vale que

$$D \,=\, \mathsf{rad}(D) \,=\, \bigcup_{x\neq 0} \mathsf{rad}(\mathsf{Ann}(x)) \ .$$

Lema 4.4. *Existen primos minimales.*

Lema 4.5. *El conjunto D de divisores de cero es unión de ideales primos.*

Demostración. Si Σ denota el conjunto de ideales contenidos en D, entonces Σ posee elementos maximales. Todo elemento maximal de Σ es un ideal primo. Veamos esta última afirmación. Si $\mathfrak{a} \in \Sigma$ es un elemento maximal e $y \in A \smallsetminus \mathfrak{a}$, entonces $\langle y\rangle + \mathfrak{a}$ es un ideal que contiene estrictamente a $\mathfrak{a}$ y, por lo tanto, no pertenece a Σ. En particular, $\langle y\rangle + \mathfrak{a} \not\subset D$, es decir, existen $t \in A$ y $b \in \mathfrak{a}$ tales que

$$yt + b \,\notin\, D \ .$$

Si $x \in A \smallsetminus \mathfrak{a}$, análogamente, existen $s \in A$ y $a \in \mathfrak{a}$ tales que $xs + a \notin D$. Por lo tanto, si $xy \in \mathfrak{a}$, pero $x, y \notin \mathfrak{a}$,

$$(xs + a)\,(yt + b) \,\in\, (xy)\,st + \mathfrak{a} \,\subset\, \mathfrak{a} \,\subset\, D \ .$$

Pero esto es absurdo, pues el conjunto $A \smallsetminus D$ de los elementos que no son divisores de cero es multiplicativamente cerrado.

Como D es unión de ideales, debe ser unión de los ideales maximales que contiene. En particular, por lo anterior, es unión de ideales primos. □

Observación 4.6. Un subconjunto $S \subset A$ es multiplicativamente cerrado, si $s, t \in S$ implica $st \in S$. En particular, S es multiplicativamente cerrado, si y sólo si su complemento cumple que $xy \in A \smallsetminus S$ implica $x \in A \smallsetminus S$, o bien $y \in A \smallsetminus S$.

Observación 4.7. Supondremos, en lo que queda, que los conjuntos multiplicativamente cerrados verifican $1 \in S$ y $0 \notin S$.[6]

Lema 4.8. *Si $S \subset A$ es un subconjunto multiplicativamente cerrado y maximal (con respecto a $0 \notin S$ y a $1 \in S$), entonces $A \smallsetminus S$ es un ideal primo minimal.*

[5] $2 + 3 = 5$ en $\mathbb{Z}/6\mathbb{Z}$. Si bien $xy = x'y' = 0$ implica $(x + x')\,yy' = 0$, aunque $y, y' \neq 0$, no se deduce que $yy' \neq 0$; justamente, y e y' también son divisores de cero. Con lo cual, no se puede concluir que $x + x'$ sea divisor de cero, si x y x' lo son.

[6] Excluimos los anillos en donde $0 = 1$.

Demostración. Veamos que $A \setminus S$ es ideal. Si $y \in A \setminus S$, entonces

$$T = \left\{ sy^r \,:\, s \in S,\, r \geq 0 \right\}$$

es un conjunto multiplicativamente cerrado que contiene a S y a 1. Por maximalidad de S, se deduce que $0 \in T$, es decir, existen $s \in S$ y $r \geq 0$ tales que

$$sy^r = 0 \;;$$

como $0 \notin S$, $r \geq 1$. Sea $x \in A$ un elemento arbitrario; queremos ver que $xy \in A \setminus S$. Si $xy \in S$, entonces

$$0 = xsy^r = (s\,(xy))\,y^{r-1} \;,$$

con $s\,(xy) \in S$, por ser multiplicativamente cerrado. Pero entonces es posible tomar un valor más pequeño para la potencia r. Como $r = 0$ es imposible, se llega a una contradicción de suponer que xy podría no pertenecer a $A \setminus S$. Así, $A \setminus S$ es cerrado por multiplicar por elementos arbitrarios de A. Veamos que es cerrado por sumas: sean $y, y_1 \notin S$. Argumentando de manera análoga, existen $s, s_1 \in S$ y $r, r_1 \geq 1$ tales que

$$sy^r = s_1 y_1^{r_1} = 0 \;.$$

Pero, entonces, por la fórmula del binomio,

$$ss_1\,(y + y_1)^{r+r_1-1} = 0 \;,$$

con $r + r_1 - 1 \geq 1$. Como $0 \notin S$ y S es multiplicativamente cerrado, $y + y_1 \notin S$.

Que $A \setminus S$ es un ideal primo, se deduce de la Observación 4.6. La minimalidad de $A \setminus S$ es inmediata de la maximalidad de S. $\square$