Ayudantia 24

Profesor: Cristóbal Rivas
Ayudantes: Benjamin Martinez, Javier Pavez

Viernes 25 de Noviembre 2022

Ejercicios para la ayudantía

Lema 24.1. Sea A un D.I. Dado $a \in A$, denotamos por $(a) := \{ab \mid b \in A\}$ al ideal generado por $a \in A$. Sean $a, b \in A$

a) Muestre que un ideal I de A contiene a (a) si y solo si $a \in I$.

Demostración. Notemos por definición de ideal principal que $(a) \subset I$ si y solo si $ak \in I$ para todo $k \in A$. Dado que I es un ideal y $1 \in A$, lo anterior ocurre si y solo si $a \in I$.

Concluimos lo pedido. □

b) Muestre que $(a) \subseteq (b)$ si y solo si b divide a a.

Demostración. Demostraremos por equivalencias.

Notemos que por definición del ideal generado por a, $(a) \subset (b)$ si y solo si $ka \in (b)$ para todo $k \in A$. Dado que (b) es un ideal y $1 \in A$, $ka \in (b)$ para todo $k \in A$ si y solo si $a \in (b)$. Luego, por definición del ideal generado por (b), $a \in (b)$ si y solo si $a = bq$ para algún $q \in A$. Pero lo último es equivalente a decir que b divide a a.

Dada todas las equivalencias anteriores, concluimos que $(a) \subset (b)$ si y solo si b divide a a. □

c) Muestre que $(a) = (b)$ si y solo si b y a son asociados.

Demostración. Primero escribiremos el hecho $(a) = (b)$ como algo equivalente y más sencillo de manejar, llegaremos a eso a través de equivalencias directas. Luego, demostraremos cada implicancia por separado.

Por hipótesis $(a) = (b)$. Eso sucede si y solo si $(a) \subset (b)$ y $(b) \subset (a)$. Por el ejercicio anterior, lo anterior ocurre si y solo si a divide a b y b divide a a. Esto es equivalente a decir que $a = bq_1$ y $b = aq_2$, para algunos q_1, $q_2 \in A$.

De lo anterior obtenemos que $(a) = (b)$ si y solo si $a = bq_1$ y $b = aq_2$, para algunos q_1, $q_2 \in A$. Por lo que solo debemos demostrar que $a = bq_1$ y $b = aq_2$, para algunos q_1, $q_2 \in A$ si y solo si a y b son asociados. Lo demostraremos viendo cada implicancia por separado.

($\Longrightarrow$) Juntando ambas igualdades tenemos que $b = aq_2 = (bq_1)q_2 = b(q_1q_2)$. Dado que estamos en un D.I. podemos usar la ley de cancelación y obtener que $q_1q_2 = 1$. Por lo que q_1, $q_2 \in A^*$ y obtenemos que a y b son asociados.

($\Longleftarrow$) Si a y b son asociados, tendremos que $a = bu$ con $u \in A^*$. Denotanto $u = q_2$ conseguimos una de dos igualdades por demostrar. Como $u \in A^*$, podemos multiplicar por su inverso multiplicativo, obtenemos que $au^{-1} = b$. Denotanto $u^{-1} = q_1$ conseguimos dos de las igualdades que queríamos mostrar.

Dados los dos caminos, concluimos que $a = bq_1$ y $b = aq_2$, para algunos q_1, $q_2 \in A$ si y solo si a y b son asociados. Y por lo tanto $(a) = (b)$ si y solo si a y b son asociados. □

Ejercicio 24.1. Sea A un D.I.P. y sean $a, b \in A$

a) Muestre que $(a) + (b) := \{k_1a + k_2b \,|\, k_1, k_2 \in A\}$ es un ideal de A. Muestre además que $(a) + (b)$ coincide con (a, b), el ideal generado por a y b.

Demostración. La demostración de que $(a) + (b)$ es un ideal, es un caso particular del Ejercicio 17.1. b) de la ayudantía 17.

La igualdad de los ideales la veremos por doble contención.

Recordemos que $(a, b) = \cap_{I \text{ ideal de } A \text{ tal que } a,b \in I} I$. Como $(a) + (b)$ es un ideal de A tal que a, $b \in (a) + (b)$, esto ya que $a = 1 \cdot a + 0 \cdot b$, $b = 0 \cdot a + 1 \cdot b \in (a) + (b)$, automáticamente tenemos que $(a, b) \subset (a) + (b)$.

Además, como (a, b) es un ideal que contiene a a y a b, necesariamente contendrá a $k_1a + k_2b$ para todo k_1, $k_2 \in A$. De lo anterior deducimos que $(a) + (b) \subset (a, b)$.

Concluimos que $(a, b) = (a) + (b)$. □

b) Muestre que $d = MCD(a, b) \Leftrightarrow (d) = (a) + (b)$.

Demostración. Como estamos en un DIP, tendremos que $(a)+(b) = (f)$ para algún $f \in A$.

Mostraremos lo pedido con una secuencia de equivalencias.

Por definición d es un máximo común divisor si y solo si d divide a a, d divide a b, y si existe un $c \in A$ tal que c divida a a y b se tendrá que d divide a c.

Gracias al Lema 24.1., lo anterior es equivalente a decir que $(a) \subset (d)$, $(b) \subset (d)$, y si existe $c \in A$ tal que $(a) \subset (c)$ y $(b) \subset (c)$ se tendrá que $(d) \subset (c)$.

Dado que todo ideal que contenga a (a) y (b) contendrá a $(a, b) = (a) + (b)$ y que (a), $(b) \subset (a) + (b) = (f)$. Lo anterior es equivalente a decir que $(a) + (b) \subset (d)$ y $(d) \subset (a) + (b)$.

Concluimos que d es un máximo común divisor si y solo si $(d) = (a) + (b)$. □

c) Muestre que $m = MCM(a, b) \Leftrightarrow (m) = (a) \cap (b)$

Demostración. Como estamos en un DIP, tendremos que $(a)\cap(b) = (f)$ para algún $f \in A$.

Mostraremos lo pedido con una secuencia de equivalencias.

Recordemos que m es un mínimo común múltiplo si y solo si a divide a m, b divide a m, y si existe $c \in A$ tal que a divide a c y b divide a c entonces m divide a c.

Gracias al Lema 24.1., lo anterior es equivalente a decir que $(m) \subset (a)$, $(m) \subset (b)$, y si existe $c \in A$ tal que $(c) \subset (a)$ y $(c) \subset (b)$ entonces $(c) \subset (m)$.

Dado que $(a) \cap (b) \subset (a)$, (b), y todo ideal que está contenido en (a) y (b) está contenido en $(a)\cap(b) = (f)$. Lo anterior es equivalente a decir que $(m) \subset (a)\cap(b)$ y $(a)\cap(b) \subset (m)$.

Concluimos que m es un mínimo común múltiplo si y solo si $(m) = (a) \cap (b)$. □

Ejercicio 24.2. Sean $F \subset L \subset K$ extensiones de cuerpos, pruebe que si K/L y L/F son algebraicos, entonces K/F es algebraico.

Demostración. Queremos probar que todo elemento de K es algebraico sobre F.

Sea $\alpha \in K$. Mostraremos que α pertenece a un cuerpo T, tal que T/F es una extensión finita y por lo tanto algebraica.

Dado que K/L es algebraico, tendremos que existe un polinomio $q(x) = \sum_{i=0}^{n} \beta_i x^i$ con coeficientes en L tal que $q(\alpha) = 0$.

Ahora bien, como $\beta_i \in L$ para todo i y L/F es una extensión algebraica, tendremos que para todo i existen polinomios $p_i(x)$ con coeficientes en F tal que $p_i(\beta_i) = 0$. Podemos escoger estos polinomios tales que sean los polinomios minimales en F.

Nuestra hipótesis es que $T = F(\beta_0, ..., \beta_n, \alpha)$, por lo que demostraremos que tiene dimensión finita.

Notemos que por definición de nuestros cuerpos, $F \subset F(\beta_0) \subset F(\beta_0, \beta_1) \subset \cdots \subset F(\beta_0, ..., \beta_n) \subset T$.

Así, podemos ocupar el Lema 2.90. de los apuntes del curso. Esto quiere decir que $[T : F] = [T : F(\beta_0)] \cdot [F(\beta_0) : F] = [T : F(\beta_0, \beta_1)] \cdot [F(\beta_0, \beta_1) : F(\beta_0)] \cdot [F(\beta_0) : F] = \cdots = [T : F(\beta_0, ..., \beta_n)] \cdot [F(\beta_0, ..., \beta_n) : F(\beta_0, ..., \beta_{n-1})] \cdots [F(\beta_0, \beta_1) : F(\beta_0)] \cdot [F(\beta_0) : F]$.

0° Por lo que para ver la finitud de $[T : F]$, solo nos debemos preocupar de que $[T : F(\beta_0, ..., \beta_n)]$, $[F(\beta_0, ..., \beta_{i+1}) : F(\beta_0, ..., \beta_i)]$ para todo i y $[F(\beta_0) : F]$ sean finitos.

1° Como β_0 es algebraico sobre F, tendremos que $[F(\beta_0) : F] = deg(p_0(x)) < \infty$.

2° Dado que $F \subset F(\beta_0, ..., \beta_i)$, tendremos que $p_{i+1}(x) \in F(\beta_0, ..., \beta_i)[x]$, y como $p_{i+1}(\beta_{i+1}) = 0$, entonces necesariamente existe el polinomio minimal en $F(\beta_0, ..., \beta_i)$ de β_{i+1}, el cuál necesariamente divide a $p_{i+1}(x)$. Es decir, $[F(\beta_0, ..., \beta_{i+1}) : F(\beta_0, ..., \beta_i)] \leq deg(p_{i+1}) < \infty$.

3° Por último, como $q(x) = \sum_{i=0}^{n} \beta_i x^i$, tendremos que $q(x) \in F(\beta_0, ..., \beta_n)[x]$. Como $q(\alpha) = 0$, entonces necesariamente existe el polinomio minimal en $F(\beta_0, ..., \beta_n)$ de α, el cual necesariamente divide a $q(x)$. Es decir, $[T : F(\beta_0, ..., \beta_n)] \leq deg(q(x)) < \infty$.

Así por 0°, 1°, 2° y 3° podemos concluir que $[T : F]$ es finito. El Lema 2.90. (a) nos dice entonces que todo elemento de T es algebraico sobre F. Como $\alpha \in T$, concluimos que α es algebraico sobre F.

Dado que α era un elemento cualquiera de K, concluimos que K/F es una extensión algebraica.

□

Ejercicios para la casita

Ejercicio 24.3. Sea A un D.I. Sean a, $b \in A$. Demuestre que a y b son asociados si y solo si a divide a b y b divide a a.

Ejercicio 24.3. Muestre que $\mathbb{Q}[\sqrt{2}]$ no es subcuerpo de $\mathbb{Q}[\sqrt[3]{2}]$.
Hint: Use el Lema 2.90. (b) de los apuntes del curso.

Ejercicio 24.4. consideremos el cuerpo de p elementos $\mathbb{Z}/p\mathbb{Z}$ con p primo. Sea $n \in \mathbb{N}$.

a) Demuestre que $\alpha^{p^n} = \alpha \ \forall \ \alpha \in \mathbb{Z}/p\mathbb{Z}$.

   Hint: Recuerde que el grupo multiplicativo de $\mathbb{Z}/p\mathbb{Z}$ es $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

b) Supongamos que existe K, un cuerpo que contiene a $\mathbb{Z}/p\mathbb{Z}$ y a todas las raíces del polinomio $p(x) = x^{p^n} - x \in K[x]$. Demuestre que el conjunto $L := \{\alpha \in K \mid p(\alpha) = 0\}$ es un subcuerpo de K que contiene a $\mathbb{Z}/p\mathbb{Z}$.
   Hint: Use el Lema del mechón.

c) Deduzca que L tiene finitos elementos y que por ende $[L : \mathbb{Z}/p\mathbb{Z}] < \infty$.

d) Supongamos $[L : \mathbb{Z}/p\mathbb{Z}] = l$. Muestre que L tiene p^l elementos con $l \leq n$.
Hint: Usar el hecho de que L es un $\mathbb{Z}/p\mathbb{Z}$-espacio vectorial.