

Algebra Abstracta II

Nicholas Mc-Donnell

1er semestre 2018

Programa

Profesor: Ricardo Menares

Email: `slmenares@mat.uc.cl`

1. Teoría de Cuerpos
2. Teoría de Galois

Evaluaciones

I1: 19 de Abril

I2: 16 de Mayo

I3: 18 de Junio

Examen: 3 de Julio (Módulos 1 y 2)

T1:

T2:

Exposiciones:

$$NP = 0,8 \cdot \left(\frac{I1 + I2 + I3}{3} \right) + 0,2 \cdot T$$

$$NF = 0,75 \cdot NP + 0,25 \cdot E$$

Eximición: $NP \geq 5,0$

Bibliografía

Algebra, Artin

Índice general

I Cuerpos

1. Anillos

2. Cuerpos

2.1. Morfismos

3. Anillos Euclidianos

Parte I

Cuerpos

Capítulo 1

Anillos

Definición 1.0.1 (Anillo). $(A, +, \cdot)$ es un anillo si:

1. $(A, +)$ es un grupo abeliano
2. \cdot es conmutativa, asociativa y 1 es identidad
3. Propiedad distributiva: $\forall a, b, c \in A : (a + b) \cdot c = a \cdot c + b \cdot c$

Ejemplo: 1.0.1.

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$$

$$\mathbb{Z}/m\mathbb{Z}, m \in \mathbb{Z}$$

$(\mathbb{N}, +, \cdot)$ no es anillo

Observación 1.0.1. $A = \{0\}$ es anillo trivial ($0 \equiv 1$)

Definición 1.0.2 (Divisor de cero). $a \in A$ es divisor de cero si

1. $a \neq 0$
2. $\exists b \in A : b \neq 0 \wedge a \cdot b = 0$

Ejemplo: 1.0.2. En $\mathbb{Z}/4\mathbb{Z}$, $\bar{2} \neq \bar{0}$ y $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$

Definición 1.0.3 (Unidad). $u \in A$ unidad si $\exists v \in A : u \cdot v = 1$

$$A^* = \{\text{unidades de } A\}$$

(A^*, \cdot) es grupo abeliano

Ejemplo: 1.0.3.

- $\mathbb{Z}^* = \{-1, 1\}$
- $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

$$\blacksquare \mathbb{Z}[i]^* = \{-1, 1, -i, i\}$$

Ejercicio: 1.0.4. $m \in \mathbb{Z}, m \neq 0$

$$(\mathbb{Z}/m\mathbb{Z})^* = \{\bar{b} : (b, m) = 1\}$$

Capítulo 2

Cuerpos

Definición 2.0.1 (Cuerpo). Un cuerpo es un anillo tal que $A^\star = A \setminus \{0\}$.

Ejemplo: 2.0.1. \mathbb{R}, \mathbb{Q} son cuerpos

$\mathbb{Z}, \mathbb{Z}[i]$ no son cuerpos

$\mathbb{Q}[i]$ es cuerpo

Definición 2.0.2. Sea A anillo, $p(x) = a_0 + a_1x + \dots + a_nx^n \in A[x]$ es un polinomio con coeficientes en A

Proposición 2.0.2. $A[x] = \{\text{polinomios con coeficientes en } A\}$ es un anillo con las operaciones usuales.

Observación 2.0.1. Si $A \neq \{0\}$, entonces $A[x]$ no es cuerpo.

En efecto, $x \neq 0$ y no tiene inverso pues si tuviera $p(x) = \sum_{i=0}^n a_i x^i$ tal que

$$x \cdot (p(x)) = 1$$

$$x(a_0 + a_1x + \dots + a_nx^n) = 1$$

$$0 + a_0x + a_1x^2 + \dots + a_nx^{n+1} = 1$$

Al ser igualdad de polinomios $0 = 1, \forall i : a_i = 0 \rightarrow \leftarrow$

Ejercicio: 2.0.3. 1. Si A no tiene divisores de cero $(A[x])^\star = A^\star$

2. Encontrar un anillo A tal que $(A[x])^\star \neq A^\star$

2.1. Morfismos

A, B anillos $f : A \rightarrow B$ se dice morfismo de anillos si:

1. $f(0_A) = 0_B, f(1_A) = f(1_B)$

2. $\forall a, b \in A$

Capítulo 3

Anillos Euclidianos

Sea A un anillo. Una función Euclidea $f : A \setminus \{0\} \rightarrow \mathbb{Z}$ es tal que $\forall a, b \in A \setminus \{0\}$, se cumple $f(ab) \geq f(a)$.

A se dice Euclideo si la función f además satisface:

$$\forall a, b \in A : b \neq 0$$

$$\exists q, r \in A : q = bq + r$$

Donde, o bien $r = 0$, o bien $f(r) < f(b)$
(Algoritmo de la división)

Ejemplo: 3.0.1.

1. $A = \mathbb{Z}; f(x) = |x|$
2. $A = F[x]$, F cuerpo
 $f(p(x)) = \text{grado de } p(x)$
(Asumiendo $p(x) \neq 0$)

Observación 3.0.1. Todo anillo Euclideo es un DIP

Demostración. Dada $I \subset A$, con A Euclideo, elegimos $a \in I$ tal que $f(a)$ cumple $f(a) = \min \text{Im}(f)$

Dado $b \in I$, escribimos $b = a \cdot q + r$

Notar que $r = b - a \cdot q \in I$ y si $r \neq 0$, se tiene $f(b) < f(a)$

→←

□