Resumen MAT214 (Anillos)

Convención: Todos los anillos serán abelianos (salvo quizás los anillos de matrices).

Un anillo abeliano k es un **cuerpo** si $k \neq \{0\}$ y si $(k \setminus \{0\}, \cdot)$ es un grupo (abeliano). En particular, $k^\times = k \setminus \{0\}$.

§Morfismos

Un **morfismo** de anillos es una aplicación $\varphi : A \to B$ preservando suma y multiplicación y tal que $\varphi(1_A) = 1_B$. Si φ es biyectivo diremos que es un **isomorfismo**.

Si $\varphi : A \hookrightarrow B$ es inyectivo, decimos que A es un **subanillo** de B.

Una A-**álgebra** es un anillo B con un morfismo (estructural) $\varphi : A \to B$. Notación típica: si $a \in A$ y $b \in B$ escribimos $a \cdot b := \varphi(a)b$.

Ejemplo: El anillo de polinomios $A[X_1, \dots, X_n]$ es un A-álgebra.

§Dominios

Sea $A \neq \{0\}$. Diremos que A es un **dominio** si para todos $a, b \in A$ se tiene que

$$ab = 0 \Rightarrow a = 0 \text{ ó } b = 0.$$

En tal caso, se define su **cuerpo de fracciones** K_A (o $\mathrm{Fr}(A)$) como el cociente de $A \times A \setminus \{0\}$ por la relación de equivalencia $(a, b) \sim (c, d) \Leftrightarrow ad = bc$, y denotamos $[(a, b)] := \frac{a}{b}$.

Ejemplo: Si $A = \mathbb{Z}$, entonces $K_A = \mathbb{Q}$.

§Ideales

Un subconjunto $I \subseteq A$ es un **ideal** si $(I, +)$ es un subgrupo de $(A, +)$ y si para todos $a \in A$ y $b \in I$ se tiene que $ab \in I$. En tal caso, el cociente A/I es un anillo.

Propiedad universal: Sea $\varphi : A \to B$ morfismo tal que $I \subseteq \ker(\varphi)$, entonces existe un único morfismo $\hat{\varphi} : A/I \to B$ tal que

$$\begin{tikzcd} A \arrow[rr, "\varphi"] \arrow[dr, "p"'] & & B \\ & A/I \arrow[ur, "\exists!\, \hat{\varphi}"'] & \end{tikzcd}$$

es un diagrama conmutativo (es decir, $\varphi = \hat{\varphi} \circ p$).

Observación: Si $J \subseteq B$ es un ideal y $\varphi : A \to B$ es un morfismo, entonces $\varphi^{-1}(J) \subseteq A$ es un ideal. En particular, $\ker(\varphi) \subseteq A$ es un ideal.

Propiedades/Ejemplos:

1. $I_n = n\mathbb{Z} \subseteq \mathbb{Z}$ es un ideal.
2. A es un cuerpo $\Leftrightarrow$ $\{0\}$ y A son los únicos ideales.
3. Si $\{I_j\}_{j \in J}$ es una familia arbitraria de ideales en A, entonces $\cap_{j \in J} I_j$ es un ideal. En particular, si $S \subseteq A$ es un subconjunto denotamos por

   $$\langle S \rangle = \bigcap_{\substack{S \subseteq I, \\ I \text{ ideal}}} I$$

   al **ideal generado por** S.
4. Si $\varphi : A \to B$ es un morfismo, entonces $A/\ker(\varphi) \cong \mathrm{Im}(\varphi)$.

§Ideales primos

Un subconjunto $S \subseteq A$ es **multiplicativo** si $1 \in S$ y si $a, b \in S$ implica que $ab \in S$.

Un ideal $\mathfrak{p} \subseteq A$ es **primo** si el conjunto $A \setminus \mathfrak{p}$ es multiplicativo. Es decir,

$$\mathfrak{p} \text{ ideal primo} \Leftrightarrow \begin{cases} 1 \notin \mathfrak{p} \ (\Leftrightarrow \mathfrak{p} \neq A), \text{ y} \\ ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \text{ ó } b \in \mathfrak{p} \end{cases}$$

Proposición: Sea $\varphi : A \to B$ un morfismo y $\mathfrak{q} \subseteq B$ un ideal. Entonces:

1. $\mathfrak{q}$ ideal primo $\Rightarrow \varphi^{-1}(\mathfrak{q})$ ideal primo.
2. Si φ es sobreyectivo: $\mathfrak{q}$ ideal primo $\Leftrightarrow \varphi^{-1}(\mathfrak{q})$ ideal primo.

Corolario: $\mathfrak{p} \subseteq A$ ideal primo $\Leftrightarrow A/\mathfrak{p}$ es un dominio.

§Ideales maximales

Un ideal $\mathfrak{m} \subseteq A$ es **maximal** si $1 \notin \mathfrak{m}$ ($\Leftrightarrow \mathfrak{m} \neq A$) y si para todo $I \subseteq A$ ideal tal que $\mathfrak{m} \subsetneq I$ se tiene que $I = A$.

Proposición: A cuerpo $\Leftrightarrow \langle 0 \rangle$ ideal maximal.

Corolario: $\mathfrak{m} \subseteq A$ ideal maximal $\Leftrightarrow A/\mathfrak{m}$ es un cuerpo.

Teorema: Todo ideal $I \subsetneq A$ está contenido en un ideal maximal.

§Ideales radicales

El **radical** de un ideal $I \subseteq A$ es el ideal dado por

$$\sqrt{I} = \{a \in A \mid \exists n \in \mathbb{N}^{\geq 1} \text{ tal que } a^n \in I\}.$$

En particular, $I \subseteq \sqrt{I}$ para todo ideal $I \subseteq A$.

El **nilradical** de un anillo A es $\mathrm{Nil}(A) = \sqrt{\langle 0 \rangle} = \{a \in A \mid \exists n \in \mathbb{N}^{\geq 1} \text{ tal que } a^n = 0\}$.

Diremos que $I \subseteq A$ es un **ideal radical** si se verifica la igualdad $I = \sqrt{I}$. Además, diremos que A es un **anillo reducido** si $\mathrm{Nil}(A) = \langle 0 \rangle$ ($\Leftrightarrow \langle 0 \rangle$ es un ideal radical).

Proposición: $I \subseteq A$ ideal radical $\Leftrightarrow A/I$ es un anillo reducido.

Ejemplo: Sea $I \subseteq A$ un ideal, entonces

$$I \text{ maximal} \Rightarrow I \text{ primo} \Rightarrow I \text{ radical}.$$

§Anillos noetherianos

Un anillo A es **noetheriano** si satisface ACC (*ascending chain condition*): Para toda cadena ascendente de ideales en A

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$$

existe $n \in \mathbb{N}$ tal que $I_m = I_{m+1}$ para todo $m \geq n$.

Ejemplos:

1. Todo cuerpo es un anillo noetheriano.
2. $\mathbb{Z}$ es un anillo noetheriano.
3. Si A es un anillo noetheriano y $I \subseteq A$ es un ideal, entonces A/I es noetheriano.

Teorema de la base de Hilbert: Si A es noetheriano, entonces $A[X]$ es noetheriano.

Corolario: Sea k un cuerpo, entonces $k[X_1, \ldots, X_n]$ es noetheriano. En particular, todo ideal $I \subseteq k[X_1, \ldots, X_n]$ es generado por finitos elementos, i.e., $I = \langle f_1, \ldots, f_r \rangle$ para ciertos polinomios f_i.

§Motivación geométrica (Hilbert)

Sea $n \in \mathbb{N}^{\geq 1}$ y $S \subseteq \mathbb{C}[X_1, \ldots, X_n]$ un subconjunto.

Observación: El teorema de la base de Hilbert implica que $I = \langle S \rangle = \langle f_1, \ldots, f_r \rangle$ es finitamente generado.

Los conjuntos de la forma

$$V(S) = \{(a_1, \ldots, a_n) \in \mathbb{C}^n \mid f(a_1, \ldots, a_n) = 0 \text{ para todo } f \in S\}$$

son llamados **conjuntos algebraicos**.

Propiedades/Ejemplos:

1. $V(1) = \emptyset$ y $V(\emptyset) = V(0) = \mathbb{C}^n$.
2. $\bigcap_{i \in I} V(S_i) = V\left(\bigcup_{i \in I} S_i\right)$.
3. $V(S_1) \cup V(S_2) = V(S_1 S_2)$.
4. Sea $(a_1, \ldots, a_n) \in \mathbb{C}^n$ y sea $\langle X_1 - a_1, \ldots, X_n - a_n \rangle \subseteq \mathbb{C}[X_1, \ldots, X_n]$ el ideal maximal asociado. Entonces, $V(\langle X_1 - a_1, \ldots, X_n - a_n \rangle) = \{(a_1, \ldots, a_n)\}$ (punto).

Teorema (Hilbert): Si $\mathfrak{m} \subseteq \mathbb{C}[X_1, \ldots, X_n]$ es un ideal maximal, entonces $\mathfrak{m} = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ para cierto $(a_1, \ldots, a_n) \in \mathbb{C}^n$.

Corolario: Si $S = \{f_i\}_{i \in I}$ es una familia de polinomios en $\mathbb{C}[X_1, \ldots, X_n]$ sin ceros comunes, entonces $\langle S \rangle = \mathbb{C}[X_1, \ldots, X_n]$.

Teorema de los ceros de Hilbert (Hilbert Nullstellensatz): Sea $g \in \mathbb{C}[X_1, \ldots, X_n]$ y sea $I \subseteq \mathbb{C}[X_1, \ldots, X_n]$ un ideal. Si $g(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n) \in V(I)$ (i.e., si $V(I) \subseteq V(g)$), entonces $g \in \sqrt{I}$.