Álgebra Moderna II

Clase pasada:

Creamos relaciones en R

i.e. $a_1, \dots, a_n \in R$

Pasamos $R \longrightarrow R/(a_1,\dots,a_n) = \overline{R}$

y $\overline{a_1} = \overline{a_2} = \cdots = \overline{a_n} = 0$ en $\overline{R}$.

Hoy: Adjuntaremos elementos a un anillo R.

EJEMPLO:

$\alpha \in \mathbb{C}$

R

$\mathbb{Z}$

$$R' = R[\alpha] = \{ r_0 + r_1\alpha + \cdots + r_n\alpha^n \mid r_k \in R \}$$

$n \geq 0$

El subanillo más pequeño que contiene R & α.

LA ESTRUCTURA DE $R[\alpha]$ DEPENDE DE α

* Si $\alpha \in R$, entonces $R[\alpha] = R$.

* Si α satisface un polinomio mónico sobre R, de grado n.

Ej: $x^2+1 \quad \alpha = i$

entonces

$$R' = \{r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}\}$$

$$= R^n$$

↑ como grupos abelianos.

$(r_0, \ldots, r_n)$

↓

Claro, $\alpha^n + r_{n-1}\alpha^{n-1} + \cdots + r_1\alpha + r_0 = 0 \Rightarrow$

$$\alpha^n = -(r_{n-1}\alpha^{n-1} + \cdots + r_0).$$

Por tanto, potencias más altas que n pueden expresarse en términos de potencias de grado $0, 1, \ldots, n-1$.

EJEMPLO: $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$

($i^2 = -1$)

¡OJO! α podría no satisfacer ningún polinomio mónico con coeficientes en R.

↳ EJEMPLO: $R = \mathbb{Z}$ ó $\mathbb{Q}$ $\alpha = \pi$ ó e

en este caso ↳ α es transcendental sobre R y

$R' = R[\alpha]$ ← polinomios en una variable

$= R[x]$ ←

si α es transcendental sobre R.

si α satisface un polinomio mónico sobre R, digamos $f(x)$,

entonces $R' = R[x]/(f(x))$.

Por lo tanto, si deseamos un anillo R' que contenga a R & α (el cual satisface un polinomio mónico $f(x)$), podemos tomar

$R' = R[x]/(f(x))$

$$R' = R[x]/(f(x)) = \{r_0 + r_1 x + \cdots + r_{n-1} x^{n-1}\}$$

$$= R^n$$

↑ como grupo $(+, 0)$

la mult. depende de $f(x)$.

EJEMPLO:

* $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1) = \mathbb{Z} + \mathbb{Z}x$

$x^2 + 1 = 0$.

$R = \mathbb{Z}/3\mathbb{Z}$

$\{0, 1, 2\}$

$0^2 \equiv 0$

$1^2 \equiv 1 \pmod 3$

$2^2 \equiv 1$

$\Rightarrow x^2 - 2 = f(x)$

no tiene raices en $\mathbb{Z}/3\mathbb{Z}$.

↳ No factoriza sobre $\mathbb{Z}/3\mathbb{Z}$

entonces

$$R' = \mathbb{Z}[x]/(x^2-2) = \mathbb{Z}/3\mathbb{Z} + \mathbb{Z}/3\mathbb{Z}\, x$$

↑ aditivo

9 elementos.

Afirmación: R' es un campo.

Claro, $(a+bx)(a-bx) = a^2 - 2b^2 \neq 0$ en $\mathbb{Z}/3\mathbb{Z}$

si $a, b \neq 0$

Por tanto, $(a+bx)(a-bx)/_{a^2-2b^2} = 1$ en R'.

Más aún, si F es un campo, ¿Cuándo es $F[x]/(f(x)) = F^n$ un campo?

↑ aditivo

Proposición: $F[x]/(f(x))$ es un campo

sii $f(x)$ es irreducible sobre F.

Demostración: ~~$\Rightarrow$) si $R = F[x]/(f(x))$ es un campo, entonces tiene sólo dos ideales. Ver $\mathbb{Z}/2\mathbb{Z}$~~

siguiente página.

R campo $\longleftrightarrow$ los únicos ideales de R son $\{0\}$ & R.

$\|$

$F[x]/(f(x))$

$\longleftrightarrow$ $\exists$ solo dos ideales en $F[x]$ que contienen a (f) ($(f) \subsetneq R$)

$\longleftrightarrow$ $(f(x))$ es un ideal maximal.

EJER: $\longleftrightarrow$ $f(x)$ es irreducible.

Para probar un campo de órden p^2 necesitamos encontrar un polinomio de grado 2, irreducible sobre $\mathbb{Z}/p\mathbb{Z}$.

EJEMPLO: $p=2$ $f(x)=x^2+x+1$ irreducible (no tiene raices en $\mathbb{Z}/2\mathbb{Z}=\{0,1\}$.)

$p>2$

$f(x)=x^2-c$ es irreducible si c no tiene raíz cuadrada en $\mathbb{Z}/p\mathbb{Z}$

$1^2 \equiv 1$

$2^4 \equiv 4 \pmod 5 \Rightarrow x^2 - 2$ es irreducible sobre $\mathbb{Z}/5\mathbb{Z}$

$3^2 \equiv 4$

$4^2 \equiv 1$

$3^2 \equiv 2 \pmod 7 \Rightarrow x^2 - 2$ factoriza en $\mathbb{Z}/7\mathbb{Z}$.

Argumento:

$$\left(\mathbb{Z}/p\mathbb{Z}\right)^* \xrightarrow{h} \left(\mathbb{Z}/p\mathbb{Z}\right)^*$$

$$a \longmapsto a^2$$

homomorfismo de grupos.

Afirmamos h NO es suprayectiva.

(Por tanto $\exists\, c \in \mathbb{Z}/p\mathbb{Z}$ sin raíz cuadrada)

h es suprayectiva $\Leftrightarrow$ h es injectiva

& h no es injectiva pues

$h(-1) = h(1)$ & $1 \neq -1$

pues $p > 2$.

Por lo tanto, para todo # primo p existe un polinomio cuadrático irreducible sobre $\mathbb{Z}/p\mathbb{Z}$.

↳ Para todo p primo $\exists$ un campo de órden p^2.

//

EJER: Describe el anillo $\mathbb{R}[\alpha]$ donde $\alpha^2 = -1$. ¿Es este un anillo conocido?

EJER: Sea $a \in R$ y $R' = R[x]/(ax-1)$ el anillo que se obtiene al adjuntar a R el inverso mult. de a.

Demostrar que $R \xrightarrow{f} R'$ tiene núcleo el conjunto $b \in R$ tal que $a^n b = 0$ para algún $n > 0$

EJEMPLO: $p(x) = x^2 + x + 1$ IRREDUCIBLE SOBRE $\mathbb{Z}/2\mathbb{Z}$

(no tiene raíces en $\mathbb{Z}/2\mathbb{Z}$)

$R = \mathbb{Z}/2\mathbb{Z}[x] / (p(x))$ campo

$= \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}\, x = \{ a + bx \mid b, a \in \mathbb{Z}/2\mathbb{Z},\ x^2 = -(x+1) \}$

↑ aditivo

multiplicación:

$0 = (0,0)$

$e = (1,0)$

$b = (0,1)$

$c = (1,1) = e + b$

	0	e	b	c
0	0	0	0	0
e	0	e	b	c
b	0	b	b+e	e
c	0	c	e	b

$b^2 = x^2 = -(x+1) = -(b+e)$

$b \cdot c = b(e+b) = b - (b+e)$

$c^2 = (e+b) = e + b^2$

$= e - (b+e)$

$= -b$

Campo de 4 elementos

$\{0, e, b, c\}$

NO EJEMPLO:

$x^2+1 = f(x)$ ← No es irreducible sobre $\mathbb{Z}/2\mathbb{Z}$

$x^2+1 = (x+1)^2$ reducible sobre $\mathbb{Z}/2\mathbb{Z}$

Por tanto,

$$R = \mathbb{Z}/2\mathbb{Z}[x]/(f(x)) = \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}\,x$$

↑ aditivo

multiplicación:

$x^2 = -1 = b^2$

$= -e$

$b \cdot c = b(e+b)$

$= b + b^2$

$= b - e$

$c^2 = (e+b)^2 = e + b^2$

$= e - e = 0$

	0	e	b	c
0	0	0	0	0
e	0	e	b	c
b	0	b	-e	b-e
c	0	c	b-e	0

↑ este cero dice R no es campo!