02/05/20 **Clase 8**

$$\begin{matrix} K & & \\ |<\infty & \longrightarrow & \mathcal{O}_K \text{ - anillo de enteros} \\ \mathbb{Q} & & \cup \\ & & I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)} \end{matrix}$$

Tema de hoy: teorema de Kummer - Dedekind

Lema Sea R anillo de números. Para primo invertible $\mathfrak{p} \subset R$, $e \geq 1$ se tiene $\#(R/\mathfrak{p}^e) = \#(R/\mathfrak{p})^e$.

Dem Caso base: $e=1$.

$R \supsetneq \mathfrak{p} \supsetneq \mathfrak{p}^2 \supsetneq \mathfrak{p}^3 \supsetneq \cdots \qquad \mathfrak{p}^{n+1} \subsetneq \mathfrak{p}^n$.

$$\frac{R/\mathfrak{p}^e}{\mathfrak{p}^{e-1}/\mathfrak{p}^e} \simeq R/\mathfrak{p}^{e-1} \text{ (iso de grupos abelianos)}$$

Afirmación: $\quad \mathfrak{p}^{e-1}/\mathfrak{p}^e \simeq R/\mathfrak{p}$

$$\#(R/\mathfrak{p}^e) = \#(\mathfrak{p}^{e-1}/\mathfrak{p}^e)\cdot(R/\mathfrak{p}^{e-1}) = \#(R/\mathfrak{p})\cdot\#(R/\mathfrak{p}^{e-1})$$

Escojamos $\alpha \in \mathfrak{p}^{e-1} \setminus \mathfrak{p}^e \implies \mathfrak{p}^e \subsetneq \mathfrak{p}^e + \alpha R \subseteq \mathfrak{p}^{e-1}$

(usando que $\mathfrak{p}$ es invertible). $\qquad \mathfrak{p} \subsetneq (\mathfrak{p}^e + \alpha R)\mathfrak{p}^{-(e-1)} \subseteq R$

$$\implies \mathfrak{p}^e + \alpha R = \mathfrak{p}^{e-1}. \quad (*)$$

$$\varphi: R \longrightarrow \mathfrak{p}^{e-1}/\mathfrak{p}^e \qquad (*) \implies \varphi \text{ es sobre.}$$
$$x \longmapsto \alpha x + \mathfrak{p}^e.$$

$$\ker\varphi = \{x \in R \mid \alpha x \in \mathfrak{p}^e\} = \mathfrak{p}.$$

$R/\mathfrak{p} \simeq \mathfrak{p}^{e-1}/\mathfrak{p}^e \qquad \square$

Nota ¿Qué pasa si $\mathfrak{p}$ no es invertible?

$R = \mathbb{Z}[\sqrt{-3}], \qquad \mathfrak{p} = (2, 1+\sqrt{-3}). \qquad \mathfrak{p}^2 \subsetneq 2R \subsetneq \mathfrak{p}$

$\mathfrak{p}^2 = 2R\cdot\mathfrak{p}. \qquad R/\mathfrak{p} \simeq \mathbb{F}_2. \qquad \#(\mathfrak{p}/\mathfrak{p}^2) = 4 \qquad \triangle$

Dado un anillo de números $R = \mathbb{Z}[\alpha]$, α entero algebraico. ¿cómo factorizar $p\mathbb{Z}[\alpha]$, donde $p \in \mathbb{Z}$ primo racional?

Teorema (Kummer-Dedekind) Sea $f(x) \in \mathbb{Z}[x]$ el pol. mínimo, pongamos $n = \deg f = [\mathbb{Q}(\alpha):\mathbb{Q}]$. Sea $p \in \mathbb{Z}$ primo racional.

Sean $g_i \in \mathbb{Z}[x]$ pol. mónicos t.q.

$$\bar{f}(x) = \bar{g}_1^{e_1} \cdots \bar{g}_s^{e_s} \quad \text{en } \mathbb{F}_p[x]. \quad \text{Entonces:}$$

1) Los primos $\mathfrak{p} \subset \mathbb{Z}[\alpha]$ t.q. $p \in \mathfrak{p}$ son

$\mathfrak{p}_i = (p, g_i(\alpha))$

2) Se tiene $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s} \subseteq p\mathbb{Z}[\alpha]$, y se cumple "="

ssi los $\mathfrak{P}_i$ son invertibles.

Además, si $\mathbb{Z}[\alpha]/\mathfrak{P}_i \simeq \mathbb{F}_{p^{f_i}}$, entonces $\sum_i e_i f_i = n$.

Dem. $\mathbb{Z}[\alpha] \xleftarrow{\simeq} \mathbb{Z}[x]/(f)$. (*)

$g(\alpha) \longleftarrow g \text{ mód } f$

$\{\text{primos } \mathfrak{P} \subset \mathbb{Z}[\alpha] \mid p \in \mathfrak{P}\} \longleftrightarrow \{\text{primos } \mathfrak{P} \subset \mathbb{Z}[\alpha]/(p)\}$.

Reduciendo (*) mód p,

$$\mathbb{Z}[\alpha]/(p) \underset{\text{(*) mód } p}{\simeq} \mathbb{Z}[x]/(p,f) \simeq \mathbb{F}_p[x]/(\bar{f})$$

$$g(\alpha) \text{ mód } p \longleftarrow \bar{g} \text{ mód } \bar{f}$$

$\{\text{primos } \mathfrak{P} \subset \mathbb{Z}[\alpha]/(p)\} \longleftrightarrow \{\text{primos } \mathfrak{P} \subset \mathbb{F}_p[x]/(\bar{f})\}$

$\updownarrow$

$\{(\bar{g}) \subset \mathbb{F}_p[x] \mid \bar{g} \mid \bar{f}\}$

factores irreducibles.

Ejercicio: haciendo explícitas todas las identificaciones, se obtiene 1)

2) Consideremos $\prod_i (p, g_i(\alpha))^{e_i} \overset{?}{\subseteq} p\mathbb{Z}[\alpha]$.

p divide a todo generador de $\prod_i (p, g_i(\alpha))^{e_i}$,

posiblemente salvo $g_1(\alpha)^{e_1} \cdots g_s(\alpha)^{e_s}$.

$$g_1(\alpha)^{e_1} \cdots g_s(\alpha)^{e_s} \equiv f(\alpha) = 0 \quad (\text{mód } p)$$

•) Si $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s} = p\mathbb{Z}[\alpha] \Longrightarrow p\mathbb{Z}[\alpha]$ invertible

$\Longrightarrow$ los $\mathfrak{P}_i$ son invertibles.

•) Asumamos que los $\mathfrak{P}_i$ son invertibles.

$\mathbb{Z}[\alpha]/\mathfrak{P}_i \simeq \mathbb{F}_{p^{f_i}} \longleftrightarrow \deg g_i = f_i$.

$$\left(\sum_i e_i f_i = \sum_i e_i \cdot \deg g_i = n \longleftarrow \boxed{\bar{f} = \prod_i \bar{g}_i^{e_i}}\right.$$

Nos gustaría ver que $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s} \overset{?}{=} p\mathbb{Z}[\alpha]$.

$$[\mathbb{Z}[\alpha] : p\mathbb{Z}[\alpha]] = \#\left(\frac{\mathbb{Z} \oplus \alpha \oplus \cdots \oplus \alpha^{n-1}\mathbb{Z}}{(p)}\right) = p^n$$

$[\mathbb{Z}[\alpha] : \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}] = ?!$

$\mathfrak{p}_i + \mathfrak{p}_j = R \Rightarrow \mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j} = R.$

t.c.d.r.: $\mathbb{Z}[\alpha] / \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s} \simeq \dfrac{\mathbb{Z}[\alpha]}{\mathfrak{p}_1^{e_1}} \times \cdots \times \dfrac{\mathbb{Z}[\alpha]}{\mathfrak{p}_s^{e_s}}.$

$\#(\mathbb{Z}[\alpha] / \mathfrak{p}_i^{e_i}) \underset{\text{Lema}}{=} \#(\mathbb{Z}[\alpha] / \mathfrak{p}_i)^{e_i} = p^{f_i e_i}.$

$[\mathbb{Z}[\alpha] : \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}] = p^{\sum_i e_i f_i} = p^n.$ $\square$

Ejemplo $R = \mathbb{Z}[\sqrt{-3}]$. $f = x^2 + 3$.

$\underline{p=2}$ $f \equiv (x+1)^2 \pmod 2$ $g = x+1$, $e = 2$.

$\mathfrak{p}^2 \subsetneq 2R$, donde $\mathfrak{p} = (2, 1+\sqrt{-3})$.

no hay igualdad. ($\mathfrak{p}$ no es invertible).

$\underline{p=3}$ $f \equiv x^2 \pmod 3$ $g = x$, $e = 2$.

$(\sqrt{-3})^2 = 3R.$

$\underline{p=5}$ f es irreducible mód 5 $\Rightarrow$ $\mathfrak{p} = (5)$ es primo.

$\underline{p=7}$ $f = \underbrace{(x+2)}_{g_1}\underbrace{(x-2)}_{g_2}.$ $(\pm 2)^2 \equiv -3 \ (7).$

$\mathfrak{p} \cdot \bar{\mathfrak{p}} = 7R$, donde $\mathfrak{p} = (7, 2+\sqrt{-3})$

$\bar{\mathfrak{p}} = (7, 2-\sqrt{-3}).$

etc....

§ **Ejemplo: campos cuadráticos $\mathbb{Q}(\sqrt{d})$.** [d libre de cuadrados]

$K = \mathbb{Q}(\sqrt{d})$, $d \equiv 2,3 \ (4) \Rightarrow \mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. $f = x^2 - d$.

factorización de $x^2 - d$ mód p $\longleftrightarrow$ $\left(\frac{d}{p}\right)$

Proposición Si $d \equiv 2,3 \ (4)$, $K = \mathbb{Q}(\sqrt{d})$.

Para p primo impar.

- Si $p \mid d \Rightarrow p\mathcal{O}_K = \mathfrak{p}^2$, donde $\mathfrak{p} = (p, \sqrt{d})$.

  "p se ramifica en K"

- Si $\left(\frac{d}{p}\right) = +1 \Rightarrow d \equiv a^2 \pmod p$ para $a \in \mathbb{Z}$

  $p\mathcal{O}_K = \mathfrak{p} \cdot \bar{\mathfrak{p}}$, $\mathfrak{p} = (p, a+\sqrt{d})$, $\bar{\mathfrak{p}} = (p, a-\sqrt{d})$

  "p se escinde en K"

$\cdot)$ Si $\left(\frac{d}{p}\right) = -1 \Rightarrow \mathfrak{p} = p\mathcal{O}_K$ es primo.
"p es inerte".

Si $d \equiv 1\ (4) \Rightarrow \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ $\quad f = x^2 - x - \frac{d-1}{4}$

la factorización de $p\mathcal{O}_K$ para p impar depende de la misma manera de $\left(\frac{d}{p}\right)$

Sin embargo, la factorización de $2\mathcal{O}_K$ depende de d mód 8.

Prop

$d \equiv 1\ (8) \Rightarrow 2\mathcal{O}_K = \mathfrak{p}\cdot\bar{\mathfrak{p}}$,
$\mathfrak{p} = \left(2, \frac{1+\sqrt{d}}{2}\right)$, $\bar{\mathfrak{p}} = \left(2, \frac{1-\sqrt{d}}{2}\right)$

$d \equiv 5\ (8) \Rightarrow 2\mathcal{O}_K = \mathfrak{p}$ es primo.

Prop. Si $d \equiv 2, 3\ (4)$, entonces $2\mathcal{O}_K = \mathfrak{p}^2$, donde

$x^2 - d \equiv (x+1)^2$ mód 2. ó x^2

$$\mathfrak{p} = \begin{cases} (2, \sqrt{d}), & \text{si } d \equiv 2\ (4) \\ (2, 1+\sqrt{d}), & \text{si } d \equiv 3\ (4) \end{cases}$$

§ **Ejemplo: campos ciclotómicos** $\mathbb{Q}(\zeta_p)$, p primo.

$K = \mathbb{Q}(\zeta_p) \Rightarrow \mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

$$f = \Phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Cómo factorizar Φ_p mód q?

Primero, si $q = p \Rightarrow \Phi_p = \frac{x^p - 1}{x-1} \equiv \frac{(x-1)^p}{x-1} = (x-1)^{p-1}$ (mód p)

Ahora si $q \neq p$, $\bar{\Phi}_p[x]$ es separable en $\mathbb{F}_q[x]$

($\Leftrightarrow \bar{\Phi}_p[x]$ no tiene factores $\bar{g}_i^{e_i}$ con $e_i > 1$ en $\mathbb{F}_q[x]$)

$f = x^p - 1 \Rightarrow f = (x-1)\cdot\Phi_p(x)$

$\text{mcd}(f, f') = 1$ en $\mathbb{F}_q[x]$. $\Rightarrow \bar{f}$ separable

$-(x^p - 1) + \frac{x}{p}\cdot(px^{p-1}) = 1$ $\quad \Rightarrow \bar{\Phi}_p$ separable

Ejemplo: $\Phi_7(x)$ mód q.

$q=2$: cúbico × cúbico.

$q=3$: irred.

$q=5$: irred.

$q=7$: $(x-1)^6$.

$q=11$: cúbico × cúbico.

$q=13$: cuadr × cuadr × cuadr.

$q=17, 19$: irred.

$q=23$: cúbico × cúbico.

$q=29$: 6 factores lineales.

Lema Sea f el orden de q módulo p

($\Leftrightarrow$ orden de q en $\mathbb{F}_p^\times \Leftrightarrow$ mínimo f t.q. $q^f \equiv 1\ (p)$).

Entonces, los factores irreducibles de $\overline{\Phi}_p$ en $\mathbb{F}_q[x]$ todos tienen grado f.

$$\overline{\Phi}_p = g_1 \cdots g_s, \qquad \deg g_i = f.$$
$$s = (p-1)/f.$$

Dem Consideremos $E = \mathbb{F}_{q^f}$. $E^\times$ es cíclico de orden $q^f - 1$.

$p \mid (q^f - 1) \Rightarrow E^\times$ contiene las raíces p-ésimas.

$\Rightarrow x^p - 1$ (y luego $\overline{\Phi}_p$) se factoriza en factores lineales en $E[x]$.

Tenemos $E = \mathbb{F}_q(\alpha)$ donde $\alpha \neq 1$, $\alpha^p - 1$.
$\alpha \in E$.

$$\begin{array}{c} E \\ | \\ F \\ n\ | \\ \mathbb{F}_q \end{array} \Bigg) f$$

Si $\mathbb{F}_q(\alpha) = F \Rightarrow \alpha \in F^\times$.

$\Rightarrow p \mid (q^n - 1) \Longrightarrow n = f$
por la elección de f.

$\forall\ \alpha \in E$ t.q. $\alpha^p - 1 = 0$, $\alpha \neq 1$ $\deg_{\mathbb{F}_q} \alpha = f$.

$\Rightarrow \deg f^{\alpha}_{\mathbb{F}_q} = f$ $\square$

Aplicando Kummer-Dedekind,

Proposición $p \neq 2$, $K = \mathbb{Q}(\zeta_p)$.

•) $p\mathcal{O}_K = \mathfrak{p}^{p-1}$, $\mathfrak{p} = (p, 1 - \zeta_p)$

•) Si $q \neq p$, entonces

$q\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_s$, donde $\mathfrak{p}_i$ son diferentes primos, $s = (p-1)/f$, donde f es el orden de q mód p.

Ejemplo $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{-3}) & = & \mathbb{Q}(\zeta_3) \\ \cup & & \cup \\ \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] & = & \mathbb{Z}[\zeta_3] \end{array}$$

•) p impar se escinde en $\mathbb{Q}(\sqrt{-3}) \Leftrightarrow \left(\frac{-3}{p}\right) = +1$

•) p se escinde en $\mathbb{Q}(\zeta_3) \Leftrightarrow p \equiv 1 \pmod 3$.

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} +1, & p \equiv 1\ (3) \\ -1, & p \equiv 2\ (3) \end{cases}$$

Caso particular de reciprocidad cuadrática!