TEORIA DI GALOIS: PRELIMINARI

R anello commutativo con unità

Definiamo:

$$S = \{ n1 \mid n \in \mathbb{Z} \} \text{ sottoanello di } R$$

$S \cong \mathbb{Z}_n$ o $S \cong \mathbb{Z}$

In questo caso si dice che R ha caratteristica n e si scrive $\operatorname{char} R = n$

In questo caso si dice che R ha caratteristica 0 e si scrive $\operatorname{char} R = 0$

Proposizione: R dominio d'integrità allora

o $\operatorname{char} R = 0$ o $\operatorname{char} R = p$ con p primo

dim (omessa)

Def Sia E un campo e F sottocampo di E

$S \subseteq E$ sottoinsieme:

- definiamo $F[S]$ il più piccolo sottoanello di E che contiene F e S
- definiamo $F(S)$ il più piccolo sottocampo di E che contiene F e S

Se $S = \{u_1, \dots, u_n\}$ si scrive $F[u_1, \dots, u_n]$ e $F(u_1, \dots, u_n)$

Oss : $S, T \subseteq E$ $\quad (F[T])[S] = F[T \cup S]$

$(F(T))(S) = F(T \cup S)$

Def: F sottocampo di E (in questo caso si può dire che E estensione di F)

E può essere visto come F spazio vettoriale si definisce $[E:F]$ come la dimensione di E come F spazio vettoriale
$[E:F]$ si dice grado di E su F

Teorema $\quad F \subseteq E \subseteq K$ campi

Abbiamo che $[K:F]$ finito $\iff$ $[K:E]$ e $[E:F]$ sono finiti

Inoltre se $[K:F]$ finito allora $[K:F] = [K:E] \cdot [E:F]$

dim (omessa)

Consideriamo $F \subseteq E$ estensione, $u \in E$

$$\varphi : \underbrace{F[x]}_{\text{anello dei polinomi}} \longrightarrow F[u]$$

$$p(x) = a_n x^n + \dots + a_0 \longrightarrow p(u) = a_n u^n + \dots + a_0$$

Osservazioni:

1. φ è suriettivo

2. se $\ker\varphi = \{0\}$ abbiamo che:

   i) $F[x] \cong F[u]$

   ii) $F[u] \subsetneq F(u)$

   ($F[u]$ non è un campo
   e
   $F(u)$ è il campo dei quozienti di $F[u]$)

   iii) $p(u) = a_n u^n + \dots + a_1 u + a_0 \neq 0$
   per ogni $p(x) \in F[x]$
   In questo caso u si dice <u>trascendente</u>

   iv) $[F(u); F] = \infty$

3. se $\ker\varphi \neq \{0\}$ definiamo $q(x) \in F[x]$
   tale che $\ker\varphi = (q(x)) = \{k(x)q(x) \mid k(x) \in F[x]\}$

[
- $(q(x))$ si dice ideale generato da $q(x)$
- $q(x)$ esiste perché $F[x]$ è un P.I.D.
- $q(x) \neq 0$
]

Vale che:

i) $q(x)$ è un polinomio di grado minimo tra quelli non nulli in $\ker \varphi$

(se richiedo che $q(x)$ sia monico $q(x)$ è unico)

ii) $\frac{F[x]}{(q(x))} \cong F[u]$ e $q(x)$ è irriducibile

questo implica: $\ker\varphi$ massimale, $F[u]$ campo e $F[u] = F(u)$

iii) Esiste $p(x) \in F(x)$ tc $p(u) = 0$

in questo caso u si dice <u>algebrico</u>

iv) Se $\ker\varphi = (q(x))$ ottengo

$[F(u) : u] = \deg q(x) < \infty$

con base $\{1, u, u^2, \dots, u^{n-1}\}$

Possiamo riassumere una parte dell'informazione nella seguente proposizione:

<u>Prop</u> $F \subseteq E$ estensione e $u \in F$

u è algebrico su $F \iff [F(u) : F] < \infty$

<u>Def</u> Se u è algebrico $[F(u) : F]$ si dice il <u>grado</u> di u su F

CAMPO DI SPEZZAMENTO DI UN'POLINOMIO

Teorema (Ruffini): Siano F campo e $p(x) \in F(x)$,

Si consideri $a \in F$

$$p(a) = 0 \iff (x-a) \mid p(x)$$

Def. Sia F campo, $p(x) \in F[x]$

$F \subseteq E$ è un campo di spezzamento per $p(x)$ su F se

1) $p(x) = a(x-r_1) \dots (x-r_n)$ in $E[x]$

2) $E = F(r_1, \dots, r_n)$

[E è generato dalle radici di $p(x)$]

Oss: r_i sono algebrici $p(r_i) = 0 \Rightarrow [E:F] < \infty$

Teorema Siano F campo e $p(x) \in F(x)$, $p(x)$ non costante

Allora $p(x)$ ha un campo di spezzamento

Dim: $p(x) = P_1(x) \dots P_k(x)$ fattori irriducibili

($F[x]$ è un UFD, dominio a fattorizzazione unica)

Induzione su $n-k$

$\boxed{n-k=0}$ $\deg(P_i(x)) = 1$ per ogni $i \Rightarrow$

$\Rightarrow F$ è un campo di spezzamento di $p(x)$ su F

passo induttivo posso supporre $n-k>0$ allora esiste i tale che $\deg(p_i(x))>1$

Definisco $K=\dfrac{F[x]}{(p_i(x))}$ campo [$p_i(x)$ è irriducibile]

Considero $r=x+(p_i(x))\in K$

osserviamo: $p_i(r)=0$ in K

[$p_i(x)=a_h x^h+\dots+a_0$ calcoliamo in K

$p_i(r)=a_h(x+(p_i(x)))^h+\dots+a_1(x+p_i(x))+a_0$

$=a_h(x^h+(p_i(x)))+\dots+a_1(x+p_i(x))+a_0$

$=a_h x^h+\dots+a_1 x+a_0+(p_i(x))=(p_i(x))=0$]

Siccome $p_i(x)=(x-r)q(x)$ in $K[x]$ [per Teor Ruffini]

Allora $p(x)=q_1(x)\dots q_\ell(x)$ con $q_i(x)$ irriducibile in $K[x]$ e $\ell>k$ (almeno p_i si spezza in due)

Quindi $\ell>k \Rightarrow n-\ell<n-k$

Uso l'ipotesi induttiva e ottengo $E\supseteq K$ campo di spezzamento di $p(x)$ su K

cioè:

$$E = K(k_1 = k, k_2, \dots, k_m)$$

$$P(x) = a(x-k_1)\cdots(x-k_m)$$

E è anche campo di spezzamento suF?

Sappiamo che $K = F(k)$ da cui

$$E = F(k)(k_1 = k, k_2, \dots, k_m) = F(k, k_2, \dots, k_m)$$

$$F(S)(T) = F(S \cup T)$$

quindi E è campo di spezzamento anche suF

Esempi: [per i primi due esempi si pensa a $\mathbb{Q} \subseteq \mathbb{R}$]

1) Consideriamo $p(x) = x^2 - 2 \in \mathbb{Q}[x]$

$\mathbb{Q}[\sqrt{2}]$ è un campo di spezzamento di $p(x)$,

$[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$ e $\{1, \sqrt{2}\}$ è una base di $\mathbb{Q}[\sqrt{2}]$ su $\mathbb{Q}$

2) Consideriamo $q(x) = (x^2 + x - 1)(x^2 - 3) \in \mathbb{Q}[x]$

$\mathbb{Q}\left(\frac{-1+\sqrt{5}}{2}, \frac{-1-\sqrt{5}}{2}, -\sqrt{3}, +\sqrt{3}\right)$ è campo di spezz. di $q(x)$

$$\mathbb{Q}\left(\frac{-1+\sqrt{5}}{2}, \frac{-1-\sqrt{5}}{2}, -\sqrt{3}, +\sqrt{3}\right) = \mathbb{Q}(\sqrt{5}, \sqrt{3})$$

Calcoliamo:

$$[\mathbb{Q}(\sqrt{5}, \sqrt{3}) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt{5}, \sqrt{3}) : \mathbb{Q}(\sqrt{5})]}_{=2} \underbrace{[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]}_{=2} = 4$$

x^3+x+1 in $\mathbb{Z}_2[x]$

Se x^3+x+1 fosse riducibile siccome x^3+x+1 ha grado tre ha un fattore lineare e quindi uno zero ma $0^3+0+1=1$ e $1^3+1+1=1$

Quindi x^3+x+1 è irriducibile

Otteniamo $K = \dfrac{\mathbb{Z}_2[x]}{(x^3+x+1)}$ campo

Definiamo $\alpha = x + (x^3+x+1)$

Denotiamo $K[y]$ l'anello dei polinomi per evitare confusioni con la x precedente

In $K[y]$ abbiamo che:

$$y^3+y+1 = (y-\alpha)(y^2+ay+b)$$

Calcoliamo a, b:

- $-b\alpha = 1 \implies b = \alpha^2+1$

[Problema: trovare un metodo per calcolare b]

- $(y^3+y+1) = (y-\alpha)(y^2+ay+(\alpha^2+1))$

$\implies -\alpha y^2 + ay^2 = 0y^2 \implies a = \alpha$

↗ considero i monomi di grado 2

Otteniamo quindi:

$$y^3+y+1 = (y-x)\underbrace{(y^2+xy+(x^2+1))}_{\text{"def } p(x)}$$

$p(x)$ è irriducibile?

Base di $K = \frac{\mathbb{Z}_2[x]}{(x^3+x+1)}$ su $\mathbb{Z}_2$: $\{\bar{1}, \bar{x}, \bar{x}^2\}$

Possiamo rappresentare K nel seguente modo:

$$K = \{0, 1, x, x^2, x+1, x^2+x, x^2+1, x^2+x+1\}$$

Siccome $p(x)$ ha grado 2, allora $p(x)$ è irriducibile se e solo se $p(x)$ ha radice in K

Si possono fare alcune prove:

$$p(0) = x^2+1 \neq 0$$

coeff. in $\mathbb{Z}_2$

$$p(1) = x^2+x+2 = x^2+x \neq 0$$

$$p(x) = x^2+x^2+x^2+1 = x^2+1 \neq 0$$

$$p(x^2) = x^4+x^3+x^2+1 = x^4+x^2+x = x(\underbrace{x^3+x+1}_{=0})=0$$

$p(x)$ ha una radice $\Rightarrow$ si può scomporre in due fattori lineari in K $\Rightarrow$ K è il campo di spezzamento di x^3+x+1