

Dato il polinomio generico  $q_0 + \dots + q_{n-1}x^{n-1} + q_nx^n$ , consideriamo le sue  $n-1$  radici complesse (sappiamo, dal Teorema Fondamentale dell'Algebra, che esse esistono)  $x_1, \dots, x_n$ . Si hanno le **FORMULE DI VIÉTE**:

$$\left\{ \begin{array}{l} x_1 + x_2 + \dots + x_n = -\frac{q_{n-1}}{q_n} \\ (x_1x_2 + \dots + x_1x_n) + \dots + x_{n-1}x_n = \frac{q_{n-2}}{q_n} \\ \vdots \\ x_1 \cdot \dots \cdot x_n = (-1)^n \frac{q_0}{q_n} \end{array} \right.$$

Inoltre, dalle **FORMULE DI LAGRANGE** sappiamo che:

$$x^2 + bx + c = 0 \Rightarrow (x_1 - x_2)(x_2 - x_1) = - (x_1 - x_2)^2 = 4c - b^2$$

Def. (Autonomorfismo):

Dato  $K$  un campo,  $\varphi : K \rightarrow K$  è un **AUTOMORFISMO** se  $\varphi$  è un isomorfismo.

Esempi:

1)  $\text{Id}_K$  è un automorfismo di  $K$ .

2) se  $F \subseteq K$  sottocampo, si definiscono gli  $F$ -automorfismi.

Proposizione:

L'insieme degli automorfismi di un campo  $K$  forma un gruppo rispetto alla composizione. Se  $F \subseteq K$  è un sottocampo, gli  $F$ -automorfismi sono un sottogruppo.

Esempi:

1) In  $\mathbb{C}$ , il coniugio è un  $\mathbb{R}$ -automorfismo. Si ha che  $\text{Id}$  e coniugio sono gli unici  $\mathbb{R}$ -autom.

di  $\mathbb{C}$ .

- 2)  $\mathbb{R}$  ha un' unica automorfismo (l' identità  $\text{Id}_{\mathbb{R}}$ )
- 3)  $\mathbb{C}$  ha infiniti automorfismi

Dato il polinomio non costante  $f(x) \in F[x]$ , sappiamo che  $\exists$  estensione di  $F$  in cui  $f$  si fattorizza completamente.

Def. (Campo di Riducibilità Completa):

K estensione di  $F$  è il **CAMPO DI RIDUCIBILITÀ COMPLETA** di  $f(x) \in F[x]$  se:

- 1)  $f(x)$  si fattorizza completamente in  $K[x]$
- 2) se  $b_1, \dots, b_k$  sono le radici di  $f$  in  $K$ , allora  $K = F(b_1, \dots, b_k)$

Proposizione (Unicità del CRC):

Se  $K_1, K_2$  sono CRC di  $f(x) \in F[x]$ , allora  $\exists \varphi : K_1 \rightarrow K_2$  isomorfismo t.c.  $\varphi(a) = a \quad \forall a \in F$

Esempio:

Dato  $\tau : F_1 \rightarrow F_2$  isomorfismo di campi, si ha

$\tau_x : F_1[x] \rightarrow F_2[x]$  isomorfismo di anelli t.c. :

$$f \in F_1[x] \Rightarrow \tau_x(f) = f^\tau$$

Proposizione

Se  $K_1$  è CRC di  $f(x) \in F[x]$  e  $K_2$  è CRC di  $f^\tau(x) \in F_2[x]$ ,  $\exists \varphi : K_1 \rightarrow K_2$  isomorfismo

che estende  $\tau$ , ovvero  $\varphi(a) = \tau(a) \quad \forall a \in F_1$

$$\begin{array}{ccc} F_1 & \xrightarrow{\tau} & F_2 \\ \cap & & \cap \\ K_1 & \xrightarrow{\varphi} & K_2 \end{array}$$

Dim.:

Per induzione su  $n = \deg f$

$n=1 : \checkmark$

$n-1 \rightsquigarrow n :$

sia  $b \in K_1$  radice di  $f$ , consideriamo il suo polinomio minimo su  $F_1$   $g(x)$

$\Rightarrow g(x)$  è irriducibile e dunque  $f : f(x) = g(x)q(x)$

$\Rightarrow f^\tau = g^\tau \cdot q^\tau$  con  $\tau_x : F_1[x] \rightarrow F_2[x]$  isomorfismo

$\Rightarrow g^\tau$  è irriducibile

$\Rightarrow$  sia  $c$  radice di  $g^\tau$  in  $K_2$  ( $\exists$ )

$\Rightarrow g^\tau$  è il polinomio minimo di  $c$  su  $F_2$ .

Consideriamo  $\tau_c : F_1[x] \rightarrow K_2$  l.c.  $\tau_c(x) = c$

$\Rightarrow \text{Ker } \tau_c = (g(x)) \Rightarrow \exists \tilde{\tau}_c : F_1[x] \rightarrow K_2$

$$\downarrow \qquad \nearrow \tilde{\tau}_c \text{ iniettivo}$$

$$F_1[x]/(g)$$

$\Rightarrow$  tuttavia sappiamo che  $F_1[x]/(g) = F_1(b)$ , quindi consideriamo  $F_1(b) \rightarrow F_2(c)$  isomorfismo

$\Rightarrow f(x) = (x-b)f_1(x)$  in  $F_1(b)$  con  $\deg f_1 = n-1$

$\Rightarrow K_1$  è CRC di  $f_1$  su  $F_1$ ,  $K_2$  è CRC di  $f_1^{\tau_1}$  su  $F_2$

q.e.d.

esempi:

1)  $x^3 - 1$  in  $\mathbb{Q}[x]$ :

$\Rightarrow$  le radici in  $\mathbb{C}$  sono  $1, \omega, \omega^2 = \bar{\omega}$  con  $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$

$\Rightarrow$  si ha  $\omega^2 + \omega + 1 = 0$

$\Rightarrow$  un CRC è  $\mathbb{Q}(\omega)$  ( $\neq \mathbb{Q}(i, \sqrt{3})$ )

2)  $x^3 - 2$  in  $\mathbb{Q}[x]$ :

$\Rightarrow$  le radici in  $\mathbb{C}$  sono  $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$  con  $\omega$  come sopra

$\Rightarrow$  il CRC è  $\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$

$\Rightarrow$  notiamo che:

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$$

$= 2 \cdot 3 = 6$

3)  $x^4 - x$  in  $\mathbb{F}_2[x]$  ( $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ,  $p$  primo)

$$\Rightarrow f(x) = x(x^3 - 1) = x(x-1)(x^2+x+1)$$

$\Rightarrow$  basta trovare una radice  $b$  di  $x^2+x+1$

$\Rightarrow$  il CRC è  $\mathbb{F}_2(b)$

Classificazione dei campi finiti:

Un campo ha caratteristica 0 oppure  $p$  primita. Se  $F$  campo ha caratteristica 0, allora  $\mathbb{Z} \leq F$  e quindi  $\mathbb{Q} \leq F$ . Un campo finito ha caratteristica  $p > 0$  ( $p$  primita) e quindi contiene  $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ , dunque è uno spazio vettoriale su  $\mathbb{F}_p$  di dim =  $n$ . Si ha quindi:

$$|F| = p^n$$

Lema (*Sogno della matricola*):

Se  $R$  è un anello commutativo di caratteristica  $p$  (con  $p$  primo), allora  $(a+b)^p = a^p + b^p \quad \forall a, b \in R$

Dim.:

$$(a+b)^p = \sum_{k=0}^p \binom{p}{k} a^{p-k} b^k = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p$$
$$\Rightarrow \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k = 0 \text{ dato che } p \mid \binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{k}$$

q.e.d.

Teorema (*Classificazione dei campi finiti*):

Se  $F$  è un campo finito t.c.  $|F| = q = p^n$ ,  $p$  primo, allora  $F$  è il CRC di  $x^q - x \in \mathbb{F}_p[x]$ . In particolare 2 campi con  $q$  elementi sono isomorfi.

Dim.:

Sia  $K$  un CRC di  $x^q - x$  su  $\mathbb{F}_p$ . Sia  $K_0 = \{b \in K \mid b^q = b\}$ .

$K_0$  è un sottocampo di  $K$ , quindi  $K = K_0$ :

$$1) b, c \in K_0 \Rightarrow (b-c)^q = b^q - c^q = b - c, (bc)^q = b^q c^q = bc$$

$$2) \text{ se } b \neq 0, (b^{-1})^q = (b^q)^{-1} = b^{-1}$$

$\Rightarrow$  calcoliamo  $|K_0|$ :

$$f(x) = x^q - x \Rightarrow f'(x) = qx^{q-1} - 1 = -1$$

$\Rightarrow \text{MCD}\{f(x), f'(x)\} = 1 \Rightarrow f$  non ha radici multiple

$$\Rightarrow |K_0| = q$$

In  $F$  ci sono  $q-1$  elementi non nulli, quindi

$$|F \setminus \{0\}| = q-1 \Rightarrow a^{q-1} = 1 \quad \forall a \in F \setminus \{0\} \quad (F \setminus \{0\} \text{ è un}$$

gruppo !!!)  $\Rightarrow a^q = a \quad \forall a \in F$ , quindi  $F$  contiene solo radici di  $x^q - x$  che quindi si fattorizza completamente

q.e.d.

Esempi:

1)  $x^8 - x$  in  $\mathbb{F}_2[x]$ :

$$x^8 - x = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

$\Rightarrow x^2 + x + 1$  è irriducibile in  $\mathbb{F}_2[x]$ , calcoliamo:

$$\begin{array}{r|l} x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 & x^2 + x + 1 \\ \hline x^6 + x^5 + x^4 & x^4 + x \\ & \hline x^3 + x^2 + x + 1 & \\ x^3 + x^2 + x & \\ \hline 1 & \end{array} \quad \times$$

$\Rightarrow x^3 + x + 1$  è irriducibile in  $\mathbb{F}_2[x]$ , calcoliamo:

$$\begin{array}{r|l} x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 & x^3 + x + 1 \\ \hline x^6 + x^4 + x^3 & x^3 + x^2 + 1 \\ \hline x^5 & + x^2 + x + 1 \\ x^5 + x^3 + x^2 & \\ \hline x^3 & + x + 1 \\ x^3 + x + 1 & \\ \hline 0 & \end{array} \quad \checkmark$$

Teorema:

Se  $G$  è sottogruppo finito di  $F \setminus \{0\}$  con  $F$  campo, allora  $G$  è ciclico. In particolare tutti i sottogruppi di un campo finito sono ciclici.

### Lemma:

Dato  $G$  gruppo abeliano, se  $a, b \in G$  hanno ordine finito, allora  $\exists c \in G$  t.c.  $\sigma(c) = \text{mcm}\{\sigma(a), \sigma(b)\}$

### Dim. (Lemma):

Siano  $m = \sigma(a)$ ,  $n = \sigma(b)$ , se  $\text{MCD}\{m, n\} = 1$  allora  $\langle a \rangle \cap \langle b \rangle = \{1\}$ . Per il Teorema Cinese del Resto,  $\sigma(ab) = mn = \text{mcm}\{m, n\}$ . In generale, sia  $q = \text{mcm}\{m, n\} \Rightarrow q = p_1^{v_1} \cdots p_k^{v_k}$  con  $p_i$  primi  
 $\Rightarrow$  sia  $m'$  il prodotto dei  $p_i^{v_i}$  che dividono  $m$  e  
 sia  $m' = \frac{q}{m}$   
 $\Rightarrow \text{MCD}\{m', n\} = 1$ ,  $\text{mcm}\{m', n\} = m'n = q$   
 $\Rightarrow \sigma(a^{\frac{m}{m'}}) = m'$ ,  $\sigma(b^{\frac{n}{m'}}) = m'$

q.e.d.

### Dim. (Teorema):

Sia  $a \in G$  di ordine massimo  $m$  e sia  $X$  l'insieme di elementi di  $G$  il cui ordine divide  $m$ . Allora certamente si ha  $\langle a \rangle \subseteq X$ . Ogni elemento di  $X$  è radice di  $x^m - 1$ , quindi  $|X| \leq m = |\langle a \rangle|$   
 $\Rightarrow X = \langle a \rangle$ . Se fosse  $\langle a \rangle \neq G$  ci sarebbe  $b \in G$  il cui ordine  $n$  non divide  $m$ . In tal caso si avrebbe:  $\text{mcm}\{m, n\} > m \nmid$

q.e.d.

Nel caso  $F = \mathbb{C}$ , abbiamo i gruppi delle radici  $n$ -esime di 1, un generatore è  $\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ . In generale, in ogni campo  $F$  le radici  $n$ -esime di 1 formano un gruppo ciclico. Calcoliamone la cardinalità:

$$f(x) = x^n - 1 \Rightarrow f'(x) = nx^{n-1}$$

Se la caratteristica è 0 oppure  $p \nmid n$ ,  $x^{n-1}$  non ha radici multiple. Se la caratteristica è  $p \mid n$ ,  $x^{n-1}$  ha radici multiple

---