Teorema (di Steinitz):

Dato un campo F, $\exists K$ estensione di F algebricamente chiusa. Se K' é estensione algebricamente chiusa di F, allora $\exists \varphi : K \longrightarrow K'$ isomorfismo t.c. $\varphi = id_F$

Lemma:

Se E é estensione algebrica di F infinito, allora $|E| = |F|$

Dim.:

$\forall b \in E$ consideriamo f_b polinomio minimo di b su F. Si ha $|F[x]| = |F|$, quindi l'insieme delle radici in E dei polinomi in $F[x]$ ha la stessa cardinalitá di F.

q.e.d.

N.B.

Se F é finito e E é algebrica, allora E é finito o numerabile.

Teorema (di Cantor):

Se X é un insieme, $\exists Y$ t.c. $|X| < |Y|$

Dim.:

$Y = \mathcal{P}(X) \Rightarrow \nexists f : X \longrightarrow \mathcal{P}(X)$ suriettiva, infatti:
$C = \{x \in X \mid x \notin f(x)\}$. Se f fosse suriettiva, sarebbe $C = f(c)$ per un certo c. Se $c \in f(c)$ allora $c \in C$,

quindi $c \notin C$ ↯ Se $c \notin f(c)$ allora $c \in C$, quindi $c \in f(c)$ ↯ $\Rightarrow C = \emptyset$

q.e.d.

Siano F campo, Ω insieme t.c. $|\Omega| > |F|, |\mathbb{N}|$. Sia inoltre $\mathcal{F}$ l'insieme di tutte le strutture di campo algebriche su F contenute in Ω e di cui F sia un sottocampo. Allora $\mathcal{F}$ é parzialmente ordinato dalla relazione "essere sottocampo". Se $\mathcal{C}$ é una catena in $\mathcal{F}$, allora si ha $\bigcup \mathcal{C} \in \mathcal{F}$. Se $a, b \in \bigcup \mathcal{C}$, $\exists E \in \mathcal{C}$ t.c. $a, b \in E \Rightarrow ab, a+b$ si definiscono usando E. Gli assiomi del campo si verificano normalmente. Inoltre ogni catena in $\mathcal{F}$ ha un maggiorante (Lemma di Zorn): sia K massimale in $\mathcal{F}$, allora K é algebrico su F e K é algebricamente chiuso. (Supponiamo che K non sia algebricamente chiuso $\Rightarrow \exists L$ estensione algebrica propria di $K \Rightarrow |L| = |K|$ oppure $|L| = |\mathbb{N}|$ $\Rightarrow |L \setminus K| < |\Omega| \Rightarrow$ trovo un sottoinsieme $X \subseteq \Omega$ t.c. $|X| = |L \setminus K| \wedge X \cap K = \emptyset \Rightarrow$ trasferisco le operazioni in L su $K' = K \cup X$ e trovo $K' \supsetneq K$, $K' \subseteq \Omega$ contro la massimalitá di K).

Lemma:

Una chiusura algebrica di F é CRC dell'insieme dei polinomi.

Proposizione:

Una chiusura algebrica di $\mathbb{C}[X]$ é isomorfa a $\mathbb{C}$

Equazione cubica:

Sappiamo che se $f \in F[x]$ e K é il suo CRC, si ha $Gal(f/F) = Gal(K/F) \wedge f = (x-b_1) \cdot \ldots \cdot (x-b_n)$ con b_i radici di f, $\deg f = n$. Possiamo identificare $Gal(f/F)$ con un sottogruppo di S_n. Definiamo ora $\delta := \prod_{i<j} (b_i - b_j)$. Il discriminante di f é:

$$\Delta := \delta^2 \in Fix_K(Gal(f/K))$$

Se $\tau \in Gal(f/K)$ si ha che $\tau(\delta) = \delta \Leftrightarrow \tau$ é pari

$\Rightarrow \tau \in F \Leftrightarrow Gal(f/F) \subseteq A_n$

$n = 2$:

$f(x) = x^2 + px + q$ con radici distinte b_1, b_2

$\Rightarrow \widetilde{S_1} = b_1 + b_2 = -p, \ \widetilde{S_2} = b_1 b_2 = q$

$\Rightarrow \delta = b_1 - b_2 \Rightarrow \Delta = (b_1 - b_2)^2 = (b_1 + b_2)^2 - 4 b_1 b_2$

$= p^2 - 4q$

$\Rightarrow$ le radici sono:

$$b_1 = \frac{-p+\delta}{2}, \ b_2 = \frac{-p-\delta}{2}$$

$\Rightarrow \delta \in F \Leftrightarrow Gal(f/F) \subseteq A_2 = \{()\}$

$\Rightarrow$ se $\delta \notin F$, $Gal(f/F) = S_2$

Determinanti di Vandermonde:

Le matrici di Vandermonde sono della forma:

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ v_1 & v_2 & \dots & v_n \\ v_1^2 & v_2^2 & \dots & v_n^2 \\ \vdots & & & \\ v_1^n & v_2^n & \dots & v_n^n \end{pmatrix} \Rightarrow \det(\cdot) = \prod_{1 \leq i < j \leq n} (v_j - v_i)$$

$\underline{n = 3}$:

$f(x) = (x - b_1)(x - b_2)(x - b_3)$ con b_i distinte

$\Rightarrow Gal(f/F) \subseteq S_3$

$$\Rightarrow \delta = -\det \begin{pmatrix} 1 & 1 & 1 \\ b_1 & b_2 & b_3 \\ b_1^2 & b_2^2 & b_3^2 \end{pmatrix}, \quad \Delta = \det \left[\begin{pmatrix} 1 & 1 & 1 \\ b_1 & b_2 & b_3 \\ b_1^2 & b_2^2 & b_3^2 \end{pmatrix} \cdot \begin{pmatrix} 1 & b_1 & b_1^2 \\ 1 & b_2 & b_2^2 \\ 1 & b_3 & b_3^2 \end{pmatrix} \right]$$

$$= \det \begin{pmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2q^2 \end{pmatrix} = -4p^3 - 27q^2$$

$\Rightarrow \tilde{S}_1 = b_1 + b_2 + b_3, \ \tilde{S}_2 = b_1 b_2 + b_1 b_3 + b_2 b_3, \ \tilde{S}_3 = b_1 b_2 b_3$

$\Rightarrow f(x) = x^3 - \tilde{S}_1 x^2 + \tilde{S}_2 x - \tilde{S}_3 = x^3 + px + q$

$\Rightarrow \tilde{S}_1 = 0, \ \tilde{S}_2 = p, \ \tilde{S}_3 = -q$

Si ha quindi:

$$\begin{cases} b_1^2 + b_2^2 + b_3^2 = \tilde{S}_1^2 - 2\tilde{S}_2 = -2p \\ b_1^3 + b_2^3 + b_3^3 = -3q \\ b_1^4 + b_2^4 + b_3^4 = 2p^2 \end{cases}$$

Si distinguono 3 casi:

1) $b_1, b_2, b_3 \in F \Rightarrow Gal(f/F) = \{()\}$

2) $b_1 \in F, \ b_2, b_3 \notin F \Rightarrow f(x) = (x - b_1)\underbrace{(x - b_2)(x - b_3)}_{\text{irriducibile in } F}$

$\Rightarrow Gal(f/F) = \langle (23) \rangle$

3) $b_1, b_2, b_3 \notin F \Rightarrow f$ irriducibile in F.

3.1) $\delta \in F \Rightarrow Gal(f/F) \subseteq A_3 \Rightarrow Gal(f/F) = A_3$

3.2) $\delta \notin F \Rightarrow Gal(f/F) \nsubseteq A_3 \Rightarrow \underbrace{F \subsetneq F(b_1)}_{\text{grado } 3},$

$\underbrace{F \subsetneq F(\delta)}_{\text{grado } 2}$ $(\delta \notin F,\ \delta^2 \in F)$

$\Rightarrow [K:F] \mid 3 \wedge [K:F] \mid 2 \Rightarrow [K:F] \geqslant 6$

$\Rightarrow 6 \leqslant [K:F] \leqslant 6 = |S_3| \Rightarrow [K:F] = 6$

$\Rightarrow |Gal(f/F)| = 6 \Rightarrow Gal(f/F) = S_3$

Quindi:

$x^3 + 3px + 2q = 0$

$p^3 + q^2 < 0 \Rightarrow -q \pm \sqrt{p^3+q^2}$ sono complessi coniugati

$\Rightarrow -q + \sqrt{p^3+q^2} = u^3,\ -q - \sqrt{p^3+q^2} = v^3$

$\Rightarrow uv = -p^3$