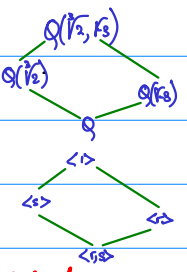
Théorie de Galois



M. Lalín

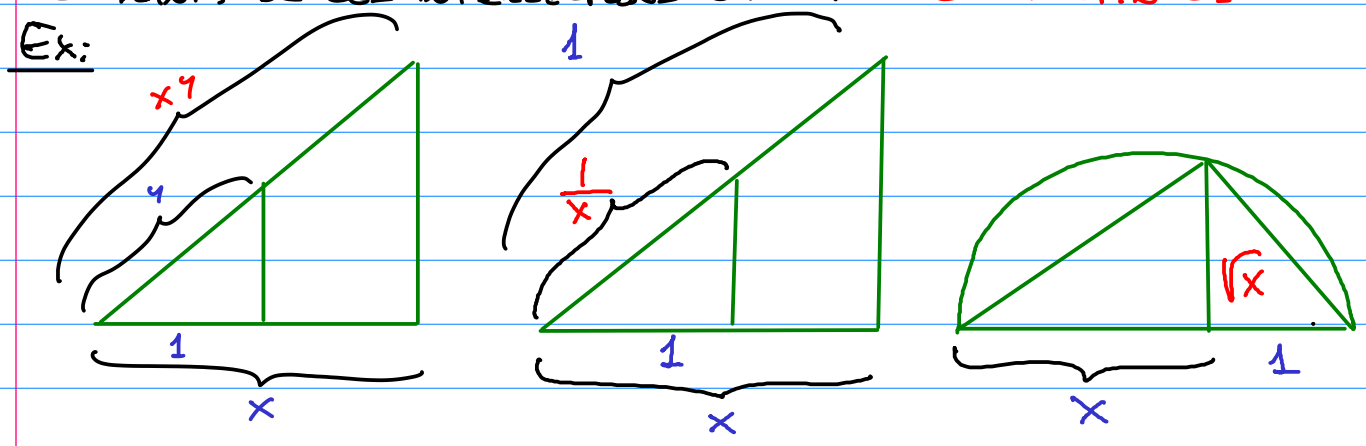
13.3 Constructions à la règle et au compas

On a le plan euclidien $\mathbb{C}$ et les **points constructibles** 0 et 1. À chaque pas on peut :

1. Construire une droite passant par deux points constructibles
2. Dessiner un cercle centré sur un des points constructibles avec un rayon égal à une distance entre deux points constructibles
3. Retrouver l'intersection finie entre deux droites différentes, deux cercles différents, ou une droite et un cercle

Les points de ces intersections sont aussi **constructibles**

Ex:



Un élément $x \in \mathbb{R}$ est **constructible** s'il y a deux points constructibles P, Q du plan tel que x = distance entre P et Q. Les nombres constructibles sont, alors, un sous-corps de $\mathbb{R}$ (et de $\mathbb{C}$). On peut montrer aussi Γ

L'intersection de deux droites est donnée par

$$\begin{cases} a_1 x + b_1 y = c_1 \\ a_2 x + b_2 y = c_2 \end{cases} \in \mathbb{Q}(a_i, b_i, c_i)$$

L'intersection d'une droite et un cercle est donnée par

$$\begin{cases} a_1 x + b_1 y = c_1 \\ (x-a_2)^2 + (y-b_2)^2 = c_2^2 \end{cases} \rightsquigarrow \text{extension quadratique de } \mathbb{Q}(a_i, b_i, c_i)$$

L'intersection de deux cercles est donnée par

$$\begin{cases} (x-a_1)^2 + (y-b_1)^2 = c_1^2 \\ (x-a_2)^2 + (y-b_2)^2 = c_2^2 \end{cases} \rightsquigarrow \begin{cases} (x-a_1)^2 + (y-b_1)^2 = c_1^2 \\ (2a_1 - 2a_2)x + (2b_1 - 2b_2)y = \\ \qquad = c_2^2 - c_1^2 + a_1^2 + b_1^2 - a_2^2 - b_2^2 \end{cases}$$

$\rightsquigarrow$ extensión quadratique de $\mathbb{Q}(a_i, b_i, c_i)$

Par conséquent, on a prouvé que

THÉORIE DE GALOIS

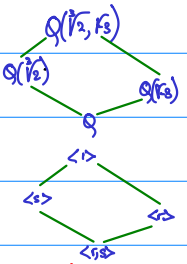
M. LAFIN

PROP: $\alpha \in \mathbb{R}$ EST CONSTRUCTIBLE $\Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}] = 2^k$ $k \geq 0$.

SI $\alpha \in \mathbb{C}$ ON DIT QUE α EST CONSTRUCTIBLE SSI $Re(\alpha)$ ET $Im(\alpha)$ SONT CONSTRUCTIBLES. ON A

THÉO: $\alpha \in \mathbb{C}$ CONSTRUCTIBLE SSI $\mathbb{Q}(\alpha) \subseteq k$ TEL QUE

$\mathbb{Q} = k_0 \subset k_1 \subset \dots \subset k_n \subset k_{n+1} \subset \dots \subset k_m = k$ où $[k_{n+1} : k_n] = 2$

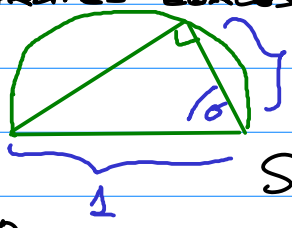


THÉO: LES PROBLÈMES DE L'ANTIQUITÉ NE SONT PAS RÉSOLUBLES.

① QUADRATURE DU CERCLE. IL EST IMPOSSIBLE DE CONSTRUIRE UN CARRÉ DONT L'AIRE ÉGALE CELLE D'UN DISQUE DONNÉ PARCE QUE $[\mathbb{Q}(\pi):\mathbb{Q}] = \infty \neq 2^k$ (π EST TRANSCENDANT)

② DUPLICATION DU CUBE. IL EST IMPOSSIBLE DE CONSTRUIRE UN CUBE DE VOLUME DOUBLE PARCE QUE $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3 \neq 2^k$

③ TRISECTION DE L'ANGLE. IL EST IMPOSSIBLE DE SECTIONNER EN TROIS PARTIES ÉGALES N'IMPORTE QUEL ANGLE



ON PEUT CONSTRUIRE UN ANGLE θ SSI ON PEUT CONSTRUIRE $\cos\theta$

SI ON PREND $\theta = \frac{\pi}{3}$, $\cos\theta = \frac{1}{2}$ ON PEUT LE CONSTRUIRE. PEUT-ON CONSTRUIRE $\theta/3$? ON A EN GÉNÉRAL.

$$\cos\theta = 4\cos^3(\theta/3) - 3\cos(\theta/3)$$

SI $\cos\theta = \frac{1}{2}$ ON A $4x^3 - 3x - \frac{1}{2} = 0 \Rightarrow 8x^3 - 6x - 1 = 0$

SI $y = 2x$, $P(y) = y^3 - 3y - 1 = 0$ IRRÉDUCTIBLE PAR LEMME DE LA RACINE, $P(1) = -1$, $P(-1) = 1$ ET $\deg = 3$. SINON, $z = y - 1$, $z^3 + 3z^2 - 3 = 0$, IRRÉDUCTIBLE PAR EISENSTEIN, $p = 3$

DONC $[\mathbb{Q}(\cos(\theta/3)) : \mathbb{Q}] = 3 \neq 2^k$ #

13.4 CORPS DE DÉCOMPOSITION ET CLÔTURE ALGÉBRIQUE

DÉF: SOIT F UN CORPS ET K/F UNE EXTENSION. SOIT $f(x) \in F[x]$

ON DIT QUE K EST UN CORPS DE DÉCOMPOSITION DE $f(x)$ SI $f(x)$ SE DÉCOMPOSE EN FACTEURS LINÉAIRES DANS K

$$f(x) = c(x - a_1)\dots(x - a_n), \quad a_i \in K$$

ET $f(x)$ NE SE DÉCOMPOSE COMPLÈTEMENT EN AUCUNE SUBEXTENSION DE K. ALORS $K = F(a_1, \dots, a_n)$

THÉO: SOIT F UN CORPS, $f(x) \in F[x]$, IL Y A UN CORPS DE DÉCOMPOSITION

DÉM: D'ABORD ON PROUVE L'EXISTENCE D'UNE EXTENSION E OÙ f SE DÉCOMPOSE

THÉORIE DE GALOIS

M. LALÍN

Soit $n = \deg f$. Si $n=1$, $k=F$. Si $n>1$, si f se décompose sur F, $k=F$. Sinon, $\exists\, p(x)$ facteur de $f(x)$, $\deg p(x) \geq 2$. Par un théorème précédent il y a une extension E_1 de F où $p(x)$ a une racine. Alors $f(x) = (x-\alpha)\, g(x)$ sur $E_1[x]$ avec $\deg g = n-1$.

On continue par induction et on trouve une extension E qui contient toutes les racines de $f(x)$. Soit k l'intersection de tous les sous-corps E qui contient F et les racines de $f(x)$. Alors k est un corps de décomposition de $f(x)$ #

Déf Si k/F algébrique et k corps de décomposition d'une collection de polynômes de $F[x]$, on dit que k est NORMAL.

Ex $x^2-2 \in \mathbb{Q}[x]$, $k = \mathbb{Q}(\sqrt{2})$

$(x^2-2)(x^2-3) \in \mathbb{Q}[x]$, $k = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$x^3-2 \in \mathbb{Q}[x]$, $k = \mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$ $\quad \zeta_3 = \frac{-1+\sqrt{3}i}{2}$

$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i) : \mathbb{Q}] = 6$ mais $\mathbb{Q}(\sqrt[3]{2})$ n'est pas normal !

$x^4+4 = (x^2+2x+2)(x^2-2x+2) \in \mathbb{Q}[x]$ racines $\pm 1 \pm i \Rightarrow k = \mathbb{Q}(i)$

Prop Le corps de décomposition d'un polynôme de $\deg n$ sur F a $\deg \leq n!$ sur F

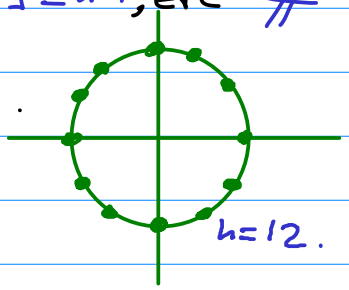
Dém On ajoute une racine $[F(\alpha_1) : F] \leq n$ et $f(x) = (x-\alpha_1) f_1(x)$ sur $F_1 = F(\alpha_1)$ avec $\deg f_1 = n-1$. On continue $[F_1(\alpha_2) : F_1] \leq n-1$, etc #

Ex x^n-1 sur $\mathbb{Q}$. Les nombres complexes sont

$re^{i\theta} = r(\cos\theta + i \sin\theta)$ avec $r>0$, $0 \leq \theta < 2\pi$

Les solutions de $x^n=1$ sont

$e^{2\pi i k/n} = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}$ $\quad k = 0, 1, \ldots, n-1$



$\mathbb{C}$ a un sous-corps qui est le corps de décomposition de x^n-1

Si $\zeta_n = e^{2\pi i/n}$, on trouve que toutes les racines sont de la forme ζ_n^k, $k = 0, 1, \ldots, n$. ζ_n est un générateur du groupe des n-RACINES DE L'UNITÉ. $\zeta_1 = 1$, $\zeta_2 = -1$, $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$, $\zeta_4 = i$, etc

Déf: $\mathbb{Q}(\zeta_n)$ s'appelle LE CORPS CYCLOTOMIQUE

Si $n=p$ premier, $(x^p-1) = (x-1)(x^p + \cdots + 1)$

$x^p + \cdots + 1$ est irréductible, $x = y+1$, Alors

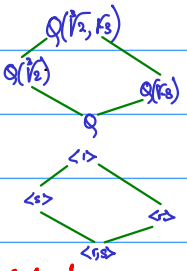
$$x^p + \cdots + 1 = \frac{x^p-1}{x-1} = \frac{(y+1)^p - 1}{y} = y^{p-1} + p\, y^{p-2} + \binom{p}{p-2} y^{p-3} + \cdots + \binom{p}{2} y + p$$

irréductible par Eisenstein.

$\Rightarrow [\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$ (EN GÉNÉRAL $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$, FONCTION D'EULER)

EX $x^p - 2$ $K = \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ $[\mathbb{Q}(\sqrt[p]{2}):\mathbb{Q}] = p$ } LES DEUX DIVISENT
$[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$ } $[K:\mathbb{Q}]$ $\gcd(p, p-1) = 1$

DONC $p(p-1) = [\mathbb{Q}(\sqrt[p]{2}, \zeta_p):\mathbb{Q}]$



THÉO SOIT $\varphi : F \xrightarrow{\sim} F_1$ ISOMORPHISME DE CORPS. SOIT $f(x) \in F[x]$ $f_1(x) \in F_1[x]$, $\varphi(f(x)) = f_1(x)$

SOIT E, E_1 LES CORPS DE DÉCOMPOSITION DE $f(x)$ SUR F ET DE $f_1(x)$ SUR F_1. ALORS, IL Y A $\sigma : E \xrightarrow{\sim} E_1$ ISOMORPHISME TEL QUE $\sigma|_F = \varphi$

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E_1 \\ | & & | \\ F & \xrightarrow{\varphi} & F_1 \end{array}$$

DÉM SOIT $\deg f(x) = n$. ON FAIT INDUCTION SUR n. ON A $\varphi : F \xrightarrow{\sim} F_1$, ON PEUT L'ÉTENDRE À $\varphi : F[x] \xrightarrow{\sim} F_1[x]$. LES FACTEURS DE $f(x)$ SONT EN CORRESPONDANCE AVEC LES FACTEURS DE $f_1(x)$. SI $f(x)$ SE DÉCOMPOSE EN FACTEURS LINÉAIRES SUR F, LE MÊME EST VRAI POUR $f_1(x)$ SUR F_1. DANS CE CAS, ON PREND $E = F$, $E_1 = F_1$, $\sigma = \varphi$.

SUPPOSONS QUE LE THÉORÈME EST VRAI POUR TOUT f AVEC $\deg f < n$.

ALORS, SOIT f AVEC $\deg f = n$ ET SOIT $p(x) \mid f(x)$ IRRÉDUCTIBLE, $p_1(x) = \varphi(p(x))$. SOIT $\alpha \in E$ UNE RACINE DE $p(x)$, $\beta \in E$ UNE RACINE DE $p_1(x)$. ON A $G = F(\alpha)$, $G_1 = F_1(\beta)$ SOIT $\phi : G \to G_1$ UNE EXTENSION DE φ. ON A

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\phi} & F_1(\beta) \\ | & & | \\ F & \xrightarrow{\varphi} & F_1 \end{array}$$

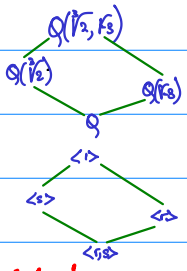
ON A $f(x) = (x-\alpha)\,g(x)$, $f_1(x) = (x-\beta)\,g_1(x)$.

$\deg g(x) = \deg g_1(x) = n-1$ ON A E, E_1 LES CORPS DE DÉCOMPOSITION DE $g(x)$, $g_1(x)$ SUR $G(x)$, $G_1(x)$. ALORS, PAR INDUCTION, $\sigma : E \xrightarrow{\sim} E_1$ TEL QUE $\sigma|_G = \phi$ ET $\phi|_F = \varphi$. ALORS $\sigma|_F = \varphi$ #

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E_1 \\ | & & | \\ G & \xrightarrow{\phi} & G_1 \\ | & & | \\ F & \xrightarrow{\varphi} & F_1 \end{array}$$

COROL: DEUX CORPS DE DÉCOMPOSITION DE $f(x) \in F[x]$ SUR F SONT ISOMORPHES

DÉF: UNE CLÔTURE ALGÉBRIQUE $\overline{F}$ D'UN CORPS F EST UNE EXTENSION ALGÉBRIQUE TELLE QUE $\forall f(x) \in F[x]$, $f(x)$ SE DÉCOMPOSE EN FACTEURS LINÉAIRES SUR $\overline{F}$



Déf: Un corps k est dit **algébriquement clos** si tout polynôme de $k[x]$ a une racine sur k

Obs Si k a toutes les racines des polynômes de $k[x]$, alors $k=E$. Aussi: $k=E \Rightarrow k$ algébriquement clos.

Prop: Soit F un corps. Alors $\overline{F}$ est algébriquement clos

Dém Soit $f(x) \in \overline{F}[x]$, α racine de $f(x)$. Alors $\overline{F}(\alpha)/\overline{F}$ est algébrique, et $\overline{F}/F$ est algébrique. Par conséquent $\overline{F}(\alpha)/F$ est algébrique. Donc α est algébrique sur $F \Rightarrow \alpha \in \overline{F} \Rightarrow$ $\overline{F}$ algébriquement clos. #

Prop: Soit F un corps. Alors $\exists\, k/F$ algébriquement clos.

Dém: Soit $f(x) \in F[x]$ un polynôme unitaire non-constant

Soit x_f une indéterminée (il y a une indéterminée pour chaque polynôme $f(x)$ avec ces conditions). Considérons l'anneau $F[\dots x_f \dots]$ et l'idéal $I = (f(x_f))$. Si I n'est pas propre, alors $1 \in I \Rightarrow$

$$\exists\, g_1, \dots, g_n \in F[\dots x_f \dots],\quad g_1 f_1(x_{f_1}) + g_2 f_2(x_{f_2}) + \dots + g_n f_n(x_{f_n}) = 1$$

Soit $x_{f_i} = x_i$ $i = 1, \dots, n$ et $x_{n+1}, \dots, x_e$ les autres indéterminées dans les g_i's. On a

$$g_1(x_1, \dots, x_e) f_1(x_1) + \dots + g_n(x_1, \dots, x_e) f_n(x_n) = 1$$

Soit F' une extension finie de F telle que $\alpha_i \in F'$ avec $f_i(\alpha_i) = 0$, $i = 1, \dots, n$. On remplace x_i avec α_i, $i = 1, \dots, n$ et x_j avec 0, $j = n+1, \dots, e$. On obtient $0 = 1$ en F'! Contradiction. Alors $I \subsetneq F[\dots x_f \dots]$ Soit M idéal maximal $I \subseteq M$. Soit

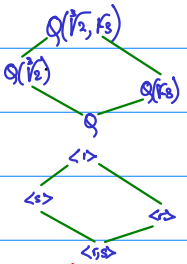
$$K_1 = F[\dots x_f \dots]/M \supseteq F$$

Chaque $f \in F[x]$ a une racine sur K_1, l'image de x_f dans la projection, parce que $f(x_f) \in I \subseteq M$. Étant donné F, on a trouvé K_1/F tel que tout polynôme nonconstant de $F[x]$ a une racine sur K_1

On répète le processus et on trouve

$$F = k_0 \subseteq k_1 \subseteq k_2 \subseteq \dots \quad \text{Soit } k = \bigcup_{j \geq 0} k_j$$

On a $F \subseteq k$. Soit $h(x) \in k[x]$ Alors $\exists\, j$ tel que $h(x) \in k_j[x]$ Alors $h(x)$ a une racine sur $k_{j+1} \subseteq k \Rightarrow k$ algébriquement clos #



PROP: Soit k algébriquement clos, $F \subseteq k$. L'ensemble $\overline{F}$ d'éléments de k qui sont algébriques sur F est une clôture algébrique de F.

DÉM: $\overline{F}/F$ est algébrique. Soit $f(x) \in F[x]$. Alors $f(x)$ se factorise linéairement sur k. Disons, $f(x) = \prod (x - \alpha_i)$, $\alpha_i \in k$, α_i algébrique sur $F \Rightarrow \alpha_i \in \overline{F} \Rightarrow f(x)$ se factorise linéairement sur $\overline{F}$ et $\overline{F}$ est une clôture algébrique de F #

DÉF: Soit k/F et L/F extensions de corps. Un morphisme (de corps) $i : k \longrightarrow L$ est dit un F-plongement si i est injectif et $i|_F$ est l'identité.

EX Soit $k = \overline{\mathbb{Q}(t_1, t_2, \dots)}$ et soit $L = \overline{\mathbb{Q}(t_1, t_2, \dots)}(t_0)$ extensions de $\overline{\mathbb{Q}}$. Soit $\varphi : k \longrightarrow L$ l'inclusion naturelle, et soit $\psi : L \longrightarrow k$ $\psi|_{\overline{\mathbb{Q}}} = \text{identité}$ et $\psi(t_i) = t_{i+1}$, $i = 0, 1, \dots$ Donc φ, ψ sont des $\overline{\mathbb{Q}}$-plongements mais $k \not\subseteq L$ car $k = \overline{k}$ mais $L \neq \overline{L}$ ($\forall t_0 \notin L$)

LEMME: Soit k/F et L/F extensions telles que k/F est algébrique et $L = \overline{L}$. Alors, il existe un F-plongement $\sigma : k \longrightarrow L$

DÉM: Soit $S = \{(M, \varphi) \mid M$ corps, $F \subseteq M \subseteq k$, $\varphi : M \longrightarrow L$ F-plongement$\}$

On construit un ordre

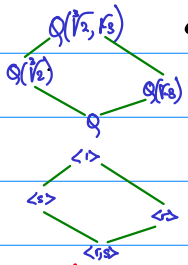
$(M, \varphi) \leq (M', \varphi')$ si $M \subseteq M'$ et $\varphi'|_M = \varphi$

$S \neq \emptyset$ parce que $(F, id) \in S$.

On va prouver que toute chaîne ordonnée a un majorant

Soit $\{(M_j, \varphi_j)\}$ une chaîne, et soit $M = \bigcup M_j$ et $\varphi : M \longrightarrow L$ donné par $\varphi(\alpha) = \varphi_j(\alpha)$ si $\alpha \in M_j$

φ est bien défini à cause de l'ordre et (M, φ) est un majorant pour $\{(M_j, \varphi_j)\}$ Par le lemme de Zorn, S a un élément maximal (M, σ) Il faut voir que $M = k$. Si non, soit $\alpha \in k \setminus M$. Par hypothèse α est algébrique sur F et donc sur M. Comme L algébriquement clos, $\sigma(m_{\alpha,M}(x))$ a une racine $\beta \in L$. On a que $\sigma : M \xrightarrow{\sim} \sigma(M)$ et que $\sigma(m_{\alpha,M}(x))$ est irréductible sur



$\sigma(M)$

On peut donc étendre $\tilde{\sigma} : M(\alpha) \longrightarrow \sigma(M)(\beta) \subseteq L$ tel que $\tilde{\sigma}|_M = \sigma$

Mais cela donne $(M, \sigma) \subsetneq (M(\alpha), \tilde{\sigma})$ contradiction. Donc $M = K$ et on a construit le F-plongement $\sigma : K \longrightarrow L$ #

Théo. Soit F corps. Si K et L sont deux clôtures algébriques de F, alors, il existe φ F-isomorphisme $\varphi : K \longrightarrow L$

Dém: Par le lemme, il y a $\varphi : K \longrightarrow L$, φ F-plongement. Alors L est une extension de $\varphi(K)$. Comme K est algébriquement clos, $\varphi(K)$ est algébriquement clos. Et comme L/F est algébrique, $L/\varphi(K)$ est algébrique et $L = \varphi(K)$. Donc $\varphi : K \longrightarrow L$ est un F-isomorphisme #

Théo! (Théorème Fondamental de l'Algèbre)

$\mathbb{C}$ est algébriquement clos. (À prouver plus tard.)

Coro: $\mathbb{C}$ contient la clôture algébrique de tous ses sous-corps, par exemple, $\overline{\mathbb{Q}} \subseteq \mathbb{C}$.