On a alors que $\exists\, b_i, c_i \in K[S]\setminus\{0\}, i=0,1,\dots,n$, t.q. $a_i = \frac{b_i}{c_i}$. On obtient donc que pour

$$P_1(X) := \sum_{i=0}^{n} \left(b_i \cdot \prod_{j\neq i} c_j\right) X^i \in K[S][X]\setminus\{0\},$$

$P_1(x) = 0$.

Comme S est alg. indép., $K[X_s \mid s \in S] \hookrightarrow K[S]$ est injectif. ($X_s \mapsto s$) De plus, si $S \cup \{x\}$ alg. indép., alors

$$\begin{array}{ccccc} K[X, X_s \mid s \in S] & \hookrightarrow & K[S][X] & \hookrightarrow & L, \\ X_s & \mapsto & s & \longmapsto & s \\ X & \mapsto & X & \longmapsto & x \end{array}$$

ce qui contredit l'existence de $P_1 \in K[S][X]\setminus\{0\}$ t.q. $P_1(x) = 0$.

$(\Leftarrow)$ Comme S alg. indép., le K-morphisme $K[X_s \mid s \in S] \longrightarrow K(S)$ est injectif. ($X_s \mapsto s$) Si x est transcendant dans $L/K(S)$, on a que le $K(S)$-morphisme

$$\begin{array}{ccc} K(S)[X] & \longrightarrow & L \\ X & \mapsto & x \end{array}$$

est injectif.

Donc le K-morph.

$$\begin{array}{ccc} K[X, X_s \mid s \in S] & \longrightarrow & L \\ X_s & \mapsto & s \\ X & \mapsto & x \end{array}$$

est injectif, d'où $S \cup \{x\}$ est alg. indép. dans L/K. ∎

<u>Exemples</u> : (1) $\{\pi, \pi - 1\}$ n'est pas algéb. indép. dans $\mathbb{R}/\mathbb{Q}$.

(2) On ne sait pas si $\{\pi, e\}$ est alg. indép. dans $\mathbb{R}/\mathbb{Q}$, et donc on ne sait pas si $\mathbb{Q}(\pi, e)/\mathbb{Q}$ est purement transcendante.

(3) $\{\sqrt{2}, \pi\}$ n'est pas alg. indép. dans $\mathbb{R}/\mathbb{Q}$

$\mathbb{Q}(\sqrt{2}, \pi)$ n'est pas transcendante pure

(4) $K(X_1, \ldots, X_n)/K$ est transcendante pure

(5) $\mathbb{R}(X, \sqrt{1-X^2})/\mathbb{R}$ est transcendante pure car

$$\mathbb{R}(X, \sqrt{1-X^2}) \cong \mathbb{R}\left(\frac{\sqrt{1+X^2}}{\sqrt{1-X^2}}\right) \quad \text{(paramétrisation du cercle)}$$

$$\mathbb{R}\left(\frac{\sqrt{1+X^2}}{\sqrt{1-X^2}}\right) \overset{!!}{=} T$$

(6) $\mathbb{Q}(X, \sqrt{X^3-X})/\mathbb{Q}$ n'est pas transcendante pure, même si tot. transcendante $\longrightarrow$ (corps de fonctions elliptiques)

(7) Dans la tour $\mathbb{R}(X,Y)/\mathbb{R}(X+Y)/\mathbb{R}$, l'ext. $\mathbb{R}(X,Y)/\mathbb{R}(X+Y)$ est transcendante pure.

<u>Déf. 2.3</u> Une <u>base de transcendance pour L/K</u> est un sous-ensemble maximal algébriquement indépendant dans L/K.

<u>Lemme 2.4</u> Un ensemble alg. indép. $S \subseteq L$ est une base de transcendance de L/K ssi $L/K(S)$ est algébrique

<u>Preuve</u> : Voir le lemme précédent. ∎

~~d'où $\exists a_0,\dots,a_n, b_0,\dots,b_n \in K[S]$ t.q. $\frac{a_0}{b_0} + \frac{a_1}{b_1}\alpha + \dots + \frac{a_n}{b_n}\alpha^n = 0$~~

~~donc $A_0 + A_1\alpha + \dots + A_n\alpha^n = 0$ avec $A_i = a_i \prod_{i \neq j} b_j \in K[S]$.~~

~~Conclusion : S est maximal.~~

Thm. 2.5 Soit L/K une ext. Elle contient une base de transcendance. Toute base de transcendance de L/K a même cardinal. Ce dernier est dit le degré de transcendance de L/K, et sera noté par $\deg.\mathrm{tr.}(L/K)$

Preuve : Existence : Soit $E \subseteq L$ un ensemble ~~générateur~~ alg. indépendant dans L/K. Soit $S \subseteq L$ un ensemble générateur de L/K t.q. $E \subseteq S$. Soit $\mathcal{B} := \{U \subseteq L$ - alg. ind. / K t.q. $E \subseteq U \subseteq S\}$. C'est un ensemble $\neq \emptyset$ partiellement ordonné $(\subseteq)$. Si $(T_\alpha)_\alpha$ est une chaîne dans $\mathcal{B}$, alors $\bigcup_\alpha T_\alpha \in \mathcal{B}$ ~~est~~ est une majorante de la chaîne.

Pour voir que $\bigcup_\alpha T_\alpha$ est alg. ind. : sinon $\exists a_1,\dots,a_n \in \bigcup_\alpha T_\alpha$ et $P(X_1,\dots,X_n) \in K[X_1,\dots,X_n]$ t.q. $P(a_1,\dots,a_n) = 0$. Comme $(T_\alpha)_\alpha$ est une chaîne, $\exists \alpha_0$ t.q. $a_1,\dots,a_n \in T_{\alpha_0}$, ce qui contredit l'hypothèse $T_{\alpha_0} \in \mathcal{B}$.

Par le lemme de Zorn, $\mathcal{B}$ a un élt. maximal B, et $B \subseteq S$.

- Si $\exists t \in S \setminus B$ t.q. t est transcendante sur $L/K(B)$, alors par le lemme 2.3 $B \cup \{t\} \subseteq S$ est alg. indépendante. Cela contredit la maximalité de B.

Donc $\forall t \in S \setminus B$, t est alg. dans $L/K(B)$, d'où $\underset{\substack{\| \\ L}}{K(B)(S \setminus B)}/K(B)$ est algébrique, et on peut conclure par le lemme 2.4.

Rmq. L'existence montre aussi que tout ensemble générateur de l'extension L/K contient une base de transcendance.

Cardinalité: Soient $B_1, B_2 \subseteq L$ deux bases de transc. de L/K. [16

Supposons que $\mathrm{Card}(B_1) \leq \mathrm{Card}(B_2)$.

- Ier cas: ~~Card~~ $\{B_2\}$ est infini. Pour $\alpha \in B_1$, $\exists B_\alpha \subseteq B_2$ fini,

α est algébrique sur $K(B_\alpha)$. On a donc $\bigcup_{\alpha \in B_1} B_\alpha \subseteq B_2$ avec B_α

Soit $B' := \bigcup_{\alpha \in B_1} B_\alpha$. Soit $\beta \in B_2 \setminus B'$. Alors β est algébrique dans

$L/K(B_1)$ et $K(B_1)/K(B')$ est algébrique. On a donc que

β est algébrique dans $L/K(B')$, absurde car alors $B' \cup \{\beta\} \subseteq B_2$

n'est pas alg. indépendante. Donc $B_2 = B'$, d'où B_1 - infini et

$\mathrm{Card}(B_1) = \mathrm{Card}(B_2)$.

IIème cas: B_2 est fini, donc B_1 est fini. Soit $B_1 = \{\beta_1, .., \beta_m\}$ et

$B_2 = \{\alpha_1, .., \alpha_n\}$, avec $m \leq n$. On raisonne par récurrence sur m.

Si $m = 0$, alors L/K - alg., d'où $B_2 = \emptyset$ et $n = 0$. Si $m > 0$,

$\exists P \in K[X, Y_1, .., Y_n]$ ~~irréductible~~ t.q. $P(\beta_1, \alpha_1, ..., \alpha_n) = 0$ avec

β_1 qui apparaît, et au moins un des α_i qui apparaît, car β_1 n'est pas

alg. sur K. Supposons que c'est α_1, d'où α_1 - alg. dans $L/K(\beta_1, \alpha_2, .., \alpha_n)$. Soit $B' := \{\beta_1, \alpha_2, .., \alpha_n\}$.

Si B' n'est pas alg.

$K(B', \alpha_1)/K(B')$ est algébrique. t.q. $Q(\beta_1, \alpha_2, .., \alpha_n) = 0$

indépendant sur K, alors $\exists Q \in K[X, Y_2, .., Y_n]$ d'où

où β_1 apparaît, donc β_1 est algébrique dans $L/K(\alpha_2, .., \alpha_n)$,

α_1 est algébrique dans $L/K(\alpha_2, .., \alpha_n)$, absurde. Donc B' est alg. ind.

dans L/K. Alors $\{\alpha_2, .., \alpha_n\}$, $\{\beta_2, .., \beta_m\}$ sont des bases de tr. de $L/K(\beta_1)$

d'où $n - 1 = m - 1$ (par l'hypothèse de récurrence), et $n = m$.

Rmq. deg. tr. $(L/K) = 0 \iff L/K$ - algébrique.

Rmq. Soit $L = K(\alpha)/K$ avec α transcendante. Soit M/K. Alors il y a une bijection

$\{K\text{-morphismes } L = K(\alpha) \to M\} \xleftrightarrow{\text{bij}} \{\text{élts. transcendants dans } M/K\}$

$(\varphi : \alpha \mapsto \beta) \mapsto \beta$

<u>Rmq.</u> Pour L/K, on peut toujours prendre une sous-extension maximale E t.q. E/K est purement transcendante et L/E algébr

<u>Exemples:</u> (1) $L = K(X)/K$, $B_1 = \{X\}$, $B_2 = \{X^2\}$

$E_1 = K(X)$,

$E_2 = K(X^2)$

(2) ~~tr~~ deg. tr. $(K(X_i \mid i \in I)/K) = \mathrm{Card}(I)$

(3) $1 \leq$ deg. tr. $(\mathbb{Q}(\pi, e)/\mathbb{Q}) \leq 2$

(4) deg. tr. $(\mathbb{R}(X, \sqrt{1-X^2})/\mathbb{R}) = 1$

(5) deg. tr. $(\mathbb{Q}(X, \sqrt{X^3 - X})/\mathbb{Q}) = 1$

(6) deg. tr. $(\mathbb{C}/\mathbb{Q}) = \infty$

$\overline{\mathbb{Q}}$

$\mathbb{R}/\mathbb{Q}$

$\longrightarrow$ car $\overline{\mathbb{Q}}(X_n \mid n \in \mathbb{N})$, $\mathbb{Q}(X_n \mid n \in \mathbb{N})$ sont dénob

<u>Corollaire 2.6.</u> Soit $M/L/K$ une tour de corps. Alors

$$\text{deg. tr.}(M/K) = \text{deg. tr.}(M/L) + \text{deg. tr.}(L/K).$$

<u>Preuve :</u> Soit B_1, resp. B_2 une base de transc. de M/L, resp. L/K.
On a que $B_1 \cap B_2 = \emptyset$, car $B_1 \cap L = \emptyset$ et $B_2 \subseteq L$. L'ensemble $B_1 \cup B_2$ est alg. indépendant dans M/K. Sinon, $\exists \{\alpha_1, .., \alpha_n\} \subseteq B_1$, $\{\beta_1, .., \beta_m\} \subseteq B_2$, $\subseteq M$, $\subseteq L$ et $P \in K[X_1, .., X_n, Y_1, .., Y_m]$ t.q. $P(\alpha_1, .., \alpha_n, \beta_1, .., \beta_m) = 0$. Comme $\{\alpha_1, .., \alpha_n\}$ est alg. indépendant dans M/L, on a que $X_1, .., X_n$ n'apparaissent pas, donc $P = Q \in K[Y_1, .., Y_m]$ et $P(\beta_1, .., \beta_m) = 0$, ce qui contredit l'ind. alg. de B_2 dans L/K.
De plus, $M/K(B_1 \cup B_2)$ est alg. car : $L/K(B_2)$ et $M/L(B_1)$ le sont, d'où $M/L(B_1 \cup B_2)$ est algébrique. De plus, $L(B_1 \cup B_2)/K(B_1 \cup B_2)$ est alg. car les élts de L, $B_1 \cup B_2$ le sont dans $M/K(B_1 \cup B_2)$. ▨

Rappel (Critère d'Eisenstein): Soit $P(X)=\sum_{i=0}^{m} a_i X^i \in \mathbb{Z}[X]$. Alors s'il $\exists p$ premier t.q. (1) $p \mid a_0, a_1, \ldots, a_{m-1}$
(2) $p \nmid a_m$; $p \nmid a_0^2$,

le polynôme $P(X)$ est irréductible dans $\mathbb{Q}[X]$.

Corollaire 2.7 $\overline{\mathbb{Q}}/\mathbb{Q}$ n'est pas finie

$\overline{\mathbb{Q}}^{\mathbb{R}} := \overline{\mathbb{Q}} \cap \mathbb{R}$ n'est pas une ext. finie ~~de~~ $\mathbb{Q}$.

Preuve: Pour $m \in \mathbb{N}_{>0}$, $P_m(X) = p + pX + \ldots + pX^{m-1} + X^m \in \mathbb{Z}[X]$ avec p premier, $P_m(X)$ est irréductible, d'où $[\mathbb{Q}[X]/(P_m(X)) : \mathbb{Q}] = m$. De plus, si $\alpha_m \in \mathbb{C}$ est t.q. $P_m(\alpha)=0$, on a que $\mathbb{Q}[X]/(P_m(X)) \cong \mathbb{Q}(\alpha_m)$, ($\mathbb{Q}$-isomorph.)
d'où $\mathbb{Q}(\alpha_m) \subseteq \overline{\mathbb{Q}}$ et $[\mathbb{Q}(\alpha_m) : \mathbb{Q}] = m$.

– Si m-impair, on peut supposer $\alpha_m \in \mathbb{R}$.

Rmq. $\overline{\mathbb{Q}} = \bigcup_{P(X)\in\mathbb{Q}[X]} \{\alpha \in \mathbb{C} \mid P(\alpha)=0\}$ est une union dénombrable d'ensembles finis, donc $\overline{\mathbb{Q}}$ – dénombrable.

Prop. 2.8 deg. tr. $(\mathbb{C}/\mathbb{Q})$ = deg. tr. $(\mathbb{C}/\overline{\mathbb{Q}}) = \infty$ non-dénombrable.

Preuve: La première égalité est dû à l'additivité de deg. tr (corollaire 2.6). S'il existe I-dénombrable t.q. $\{\alpha_i \mid i \in I\}$ est une base de tr. de $\mathbb{C}/\overline{\mathbb{Q}}$, alors $[\overline{\mathbb{Q}}(\alpha_i \mid i\in I) : \overline{\mathbb{Q}}] = \mathrm{Card}(\mathbb{N})$, d'où $\overline{\mathbb{Q}}(\alpha_i \mid i \in I)$ est dénombrable, et $\mathbb{C}/\overline{\mathbb{Q}}(\alpha_i \mid i\in I)$ est algébrique. Mais comme
$\mathbb{C} = \bigcup_{P(X)\in\overline{\mathbb{Q}}(\alpha_i \mid i\in I)[X]} \{\alpha \in \mathbb{C} \mid P(\alpha)=0\}$ est une union dénombrable d'ensembles finis
donc on aurait que $\mathbb{C}$ est dénombrable, absurde.

Rmq. De manière similaire, deg. tr. $(\overline{\mathbb{Q}}^{\mathbb{R}}/\mathbb{Q}) = \infty$ non dénombrable.

Exemple : Soit $\mathcal{B}$ une base de transcendance de $\mathbb{C}/\mathbb{Q}$.
Soit $\varphi : \mathcal{B} \to \mathcal{B}$ une ~~morph~~ application quelconque ~~ou~~ injective.
Cela induit un $\overline{\mathbb{Q}}$-morphisme

$$\overline{\mathbb{Q}}(\mathcal{B}) \xrightarrow{\bar{\varphi}} \overline{\mathbb{Q}}(\mathcal{B}),$$ qui peut

toujours se prolonger (non uniquement) à

$$\mathbb{C} \xrightarrow{\varphi_0} \mathbb{C}.$$

Si φ n'est pas surjective, φ_0 sera un morphisme de corps non surjectif.

Références :

- Fields and Galois Theory, J. S. Milne
- Polys en français de : – J.-F. Dat
  – O. Debarre
  – A. Mézard
- Algebra, S. Lang