$$\varphi : K[a_1, \dots, a_n] \xrightarrow{\sim} K[X_1, \dots, X_n]^{\mathfrak{S}_n} \hookrightarrow K[X_1, \dots, X_n],$$
$$a_i \longmapsto \sigma_i$$

que le corps de décompos. de $\varphi(P) = X^n - \sigma_1 X^{n-1} + \dots + (-1)^n \sigma_n$ est $K(X_1, \dots, X_n) \supseteq K(\sigma_1, \dots, \sigma_n)$ et que son groupe de Galois est $\mathfrak{S}_n$. Or pour $n \geq 5$, le groupe $\mathfrak{S}_n$ n'est pas résoluble (on a $D\mathfrak{S}_n = \mathfrak{A}_n$ et $D\mathfrak{A}_n = \mathfrak{A}_n$). ✓

<u>Cor. 4</u> (Galois, ~1830) : Il existe des polynômes $P \in \mathbb{Q}[X]$ tels que l'équation $P = 0$ n'est pas résoluble par radicaux.

Dém. : Il suffit de trouver $P \in \mathbb{Q}[X]$ tel que le groupe de Galois d'un corps de décomposition $E \supseteq \mathbb{Q}$ est isomorphe à $\mathfrak{S}_5$. On se sert pour cela de la technique de réduction modulo p. Voir ci-dessous (p. 82) pour la fin de la démonstration. ✓

2.10 Réduction modulo p

Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire.

Notations :

$Gal_{\mathbb{Q}}(P)$ = groupe de Galois d'un corps de décompos. E de P sur $\mathbb{Q}$

Pour un nombre premier p :

$Gal_{\mathbb{F}_p}(\bar{P})$ = groupe de Galois d'un corps de décompos. L de l'image $\bar{P}$ de P dans $\mathbb{F}_p[X]$

Rques : On sait que

- $Gal_{\mathbb{Q}}(P)$ peut être "très compliqué" : conjecturalement tout groupe fini apparaît sous cette forme,
- $Gal_{\mathbb{F}_p}(\bar{P})$ est "très simple" : cyclique, engendré par le morphisme de Frobenius.

Idée : Etudier $Gal_{\mathbb{Q}}(P)$ en établissant des liens avec les $Gal_{\mathbb{F}_p}(\bar{P})$ pour des nombres premiers p convenables.

NB : Il n'existe pas de morphisme d'anneaux entre $\mathbb{Q}$ et $\mathbb{F}_p$.

Mais il existe un zigzag de morphismes d'anneaux :

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathbb{Q} \\ \downarrow & & \\ \mathbb{F}_p & & \end{array}$$

(1)

Rque : Si $\bar{P}$ est séparable, P est séparable car $\mathrm{disc}(\bar{P}) \in \mathbb{F}_p$ est la réduction modulo p de $\mathrm{disc}(P) \in \mathbb{Z}$.

Résultat principal

Thm 6 : Soit p premier tel que $\bar{P}$ est séparable.
Alors il existe un couple (φ_0, j), où
- φ_0 est une bijection $\Omega \xrightarrow{\sim} \bar{\Omega}$ de l'ens. des racines de P sur l'ens. des racines de $\bar{P}$,
- j est morph. de groupes injectif
$$j : \mathrm{Gal}_{\mathbb{F}_p}(\bar{P}) \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(P)$$

$$\begin{array}{ccc} \Omega & \xrightarrow{j(g)} & \Omega \\ {\scriptstyle\varphi_0}\downarrow & & \downarrow{\scriptstyle\varphi_0} \\ \bar{\Omega} & \longrightarrow & \bar{\Omega} \\ & g \in \mathrm{Gal}_{\mathbb{F}_p} & \end{array} \qquad \mathrm{Gal}_{\mathbb{Q}} \ni$$

tels que
$$g \circ \varphi_0(\xi) = \varphi_0 \circ j(g)(\xi)$$
pour tous $\xi \in \Omega$ et tous $g \in \mathrm{Gal}_{\mathbb{F}_p}(\bar{P})$.
En outre, φ_0 est canonique à composition avec un élément de $\mathrm{Gal}_{\mathbb{Q}}(P)$ près et j est canonique à composition avec une conjugaison près.

Dém. : voir la fin du paragraphe.

Rque : Supposons que $\bar{P} \in \mathbb{F}_p[X]$ est séparable et se factorise en un produit de polynômes irréductibles de degrés $d_1, \dots, d_r$.
On sait que $\mathrm{Gal}_{\mathbb{F}_p}(\bar{P})$ agit transitivement sur les racines de chaque facteur irréductible de $\bar{P}$ et que $\mathrm{Gal}_{\mathbb{F}_p}(\bar{P})$ est engendré par le morph. de Frobenius Fr.
Donc la permutation des racines de $\bar{P}$ induite par Fr se décompose → p. 82 → p. 75 → p. 76

en un produit de cycles à supports disjoints de longueurs $d_1, d_2, \dots, d_r$. Le théorème montre que $Gal_{\mathbb{Q}}(P)$ contient un élément $j(F_r)$ dont la permutation associée se décompose de la même façon en cycles à supports disjoints de longueurs $d_1, \dots, d_r$!

Exemple : Considérons $P = X^5 - X - 1$. Rappelons que pour p premier et $q = p^d$, on a (Cor. 1.3.5)

$$X^q - X = \prod_{d' | d} (\text{polynômes irréd. de } \mathbb{F}_p[X] \text{ de degré } d')$$

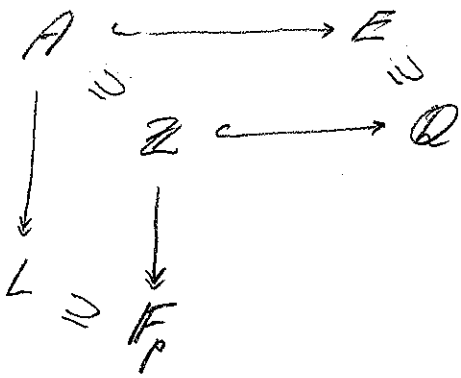
Donc $PGCD(P, X^q - X)$ calculé dans $\mathbb{F}_p[X]$ est le produit des facteurs irréd. de P de tous les degrés d' divisant d.

$p = 2$: $\bar{P} = X^5 + X + 1$ est séparable et sans facteurs de degré 1.
On a $PGCD(X^5 + X + 1, X^4 - X) = X^2 + X + 1$, irréductible.
Donc $\bar{P} = Q_1 Q_2$ où Q_1 est irréd. de degré 2 et Q_2 irréd. de degré 3. Ainsi $Gal_{\mathbb{Q}}(P)$ contient un élément σ produit d'une transpos. et d'un 3-cycle (à supports disjoints). Le cube σ^3 est une transposition.

$p = 3$: $\bar{P} = X^5 - X - 1$ est séparable et sans facteur de degré 1. On a $PGCD(\bar{P}, X^9 - X) = 1$. Donc $\bar{P}$ n'a pas de facteurs irréd. de degré 2. Donc $\bar{P}$ est irréd. Ainsi $Gal_{\mathbb{Q}}(P)$ contient un 5-cycle (et P lui-même est irréd.).

Conclusion : $Gal_{\mathbb{Q}}(P) \simeq \mathfrak{S}_5$ et $P = 0$ n'est pas rés. par radicaux.

On va construire un anneau A et un "zigzag d'extensions"



L'anneau A n'est pas unique. On travaille avec la version la moins sophistiquée (plus sophistiquée : A = anneau des entiers algébriques du corps E, cf. le cours de Marc Hindry).

Fixons un nombre premier p. Soient $\xi_1, \dots, \xi_n$ les racines de P dans E. On a

$$E = \mathbb{Q}[\xi_1, \dots, \xi_n]$$

Def. : $A := \mathbb{Z}[\xi_1, \dots, \xi_n] \subset E$

Rque : En tant que $\mathbb{Q}$-espace vectoriel, E est donc engendré par A.

Prop 1 : A est un $\mathbb{Z}$-module libre de rang $[E:\mathbb{Q}]$.

Dém. : Pour chaque racine ξ_i, la puissance ξ_i^n est combin. $\mathbb{Z}$-lin. des puissances ξ_i^k, $0 \leq k < n$, car P est unitaire de degré n à coeff. dans $\mathbb{Z}$. Donc les

$$\xi_1^{e_1} \cdots \xi_n^{e_n}, \quad 0 \leq e_i \leq n-1, \ 1 \leq i \leq n,$$

engendrent le $\mathbb{Z}$-module A. Donc A est de type fini. En outre, A est sans torsion (car E est sans torsion). Donc A est libre de type fini. Son rang est égal à la dimension de $\mathbb{Q} \otimes_{\mathbb{Z}} A$ sur $\mathbb{Q}$ (comme pour tout $\mathbb{Z}$-module de type fini) et $\mathbb{Q} \otimes_{\mathbb{Z}} A \xrightarrow{\sim} E$. ✓

Rque: Comme A est libre sur $\mathbb{Z}$, on a $pA \neq A$. Donc $A/pA \neq 0$.

Prop. 2: Soit m un idéal maximal de A contenant pA. Alors A/m est un corps de décomposition de $\bar{P}$ sur $\mathbb{F}_p$.

Exemple: Pour $P = X^4 - 1$, on a $A = \mathbb{Z}[i]$. Pour $p = 5$, on a $p = (1+2i)(1-2i)$ dans $\mathbb{Z}[i]$ et pA est contenu dans les idéaux maximaux $m_1 = (1+2i)$ et $m_2 = (1-2i)$. (Alors $A/m_j \simeq \mathbb{F}_5$ est bien un corps de déc. de X^4-1 sur $\mathbb{F}_5$.)

Dém.: La composée $\mathbb{F}_p \longrightarrow A/pA \longrightarrow A/m$ est un morphisme de corps, le polynôme $\bar{P}$ se scinde dans A/m (car P se scinde dans A) et A/m est engendré sur $\mathbb{F}_p$ par les racines de $\bar{P}$ (car elles sont les images des racines ξ_i de P dans A, qui engendrent A sur $\mathbb{Z}$). ✓

Prop 3: Soit $K \supseteq \mathbb{F}_p$ une extension finie. On a équivalence entre

$\Updownarrow$ i) K est un corps de décomposition de $\bar{P}$;

ii) Il existe un morph. d'anneaux surjectif $\pi : A \longrightarrow K$.

Dém.: i) $\Rightarrow$ ii) Soit m un idéal max. de A contenant pA. Par la prop. 2, l'extension $A/m \supseteq \mathbb{F}_p$ est un corps de décomposition. Or a un isomorphisme d'extensions $A/m \xrightarrow{\sim} K$. D'où le morph.

$$A \longrightarrow A/m \xrightarrow{\sim} K.$$

ii) $\Rightarrow$ i) $\ker \pi =: m$ est un idéal max. contenant pA. Donc A/m est un corps de décompos. et $K \simeq A/m$ également. ✓

Thm 4 ("Lemme de Dedekind"): Soit G un monoïde (= ensemble muni d'une loi binaire associative avec élément neutre). Soit K un corps. Alors l'ensemble $\mathrm{Hom}_{\mathrm{Mon}}(G, K)$ des morphismes de monoïdes $G \longrightarrow (K, \cdot)$ est une partie libre du K-espace vectoriel $\mathrm{Hom}_{\mathrm{Ens}}(G, K)$ de toutes les applications $G \longrightarrow K$.

Dém.: Supposons que $\mathrm{Hom}_{\mathrm{Mon}}(G, K)$ n'est pas une partie libre. Soit $\{\chi_1, \dots, \chi_n\}$ une partie liée minimale et

$$(1) \qquad a_1 \chi_1 + a_2 \chi_2 + \dots + a_n \chi_n = 0$$

une relation non triviale, où $a_1, \dots, a_n \in K$. On a $n \geq 2$ (car tout morph. de monoïdes $\chi : G \longrightarrow K$ est non nul) et tous les a_i sont non nuls (par minimalité de n). Comme $\chi_1 \neq \chi_2$, il existe $z \in G$ tel que $\chi_1(z) \neq \chi_2(z)$. Pour tout $x \in G$, on a

$$a_1 \chi_1(zx) + a_2 \chi_2(zx) + \dots + a_n \chi_n(zx) = 0.$$

Comme $\chi_i(zx) = \chi_i(x)\,\chi_i(z)$, il s'ensuit que

$$(2) \qquad a_1 \chi_1(z) \chi_1 + a_2 \chi_2(z) \chi_2 + \dots + a_n \chi_n(z) \chi_n = 0.$$

L'équation $\chi_1(z) \cdot (1) - (2)$ devient

$$0 \cdot \chi_1 + a_2 (\chi_1(z) - \chi_2(z)) \chi_2 + \dots + a_n (\chi_1(z) - \chi_n(z)) = 0$$

Comme $a_2 \cdot (\chi_1(z) - \chi_2(z)) \neq 0$, cela contredit la minimalité de la partie $\{\chi_1, \dots, \chi_n\}$. ✓

Cas particulier ("Indépendance des caractères"): Si G est un groupe et $\chi_1, \dots, \chi_n$ des caractères distincts deux à deux $G \to K^*$, alors $\chi_1, \dots, \chi_n$ sont lin. indép. dans l'espace des appl. $G \to K$.

Richard Dedekind, 1831 (Braunschweig) – 1916 (Braunschweig)