Sous-groupes distingués

Definition

H est **distingué** dans G, noté $H \triangleleft G$ si $\forall g \in H, \quad gH = Hg$

- $H \triangleleft G \iff H = \text{Ker}\varphi$ avec $G/\text{Ker}\varphi \simeq \text{Im}\varphi$
- Si $H \triangleleft G$, $G/H = \{gH | g \in G\}$ est un groupe et $|G/H| = |G|/|H|$

Definition

- Une **suite exacte** est $1 \to G_1 \xrightarrow{i} G_2 \xrightarrow{s} G_3 \to 1$ avec i injective, s surjective et $\text{Im}i = \text{Ker}s$
- Une **action** d'un groupe G sur E est $\varphi : G \longrightarrow \text{Bij}(E) : g.e := \varphi(g)(e)$
- Une action φ est **fidèle** si φ est injective et **transitive** si φ e
- L'**orbite** de $x \in E$ est $G.x$ (les orbites partitionnent E), son **stabilisateur** est $G_x = \{g \in G \mid g.x = x\}$. On note $E^H := \{x \in E \mid \forall h \in H, h.x = x\}$
- le **type** de $\sigma \in S_n$ est $(n_1, \cdots, n_N)$ avec les n_i les longueurs des orbites non triviaux.

Lemme de Cauchy Soit G fini et $p \in \mathcal{P}$ divisant $\#G$. Alors $\exists x \in G, \ o(x) = p$.

Lemme de Gauss Si $P \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$ alors il l'est dans $\mathbb{Q}[X]$.

Critère d'Eisenstein Soit $P = \sum_{k=0}^{n} a_k X^k$ unitaire. Si $\exists p \in \mathcal{P} : p | a_0, \cdots a_{n-1}$ et $p^2 \not| a_0$ alors P est irréductible dans $\mathbb{Q}[X]$.

Résolubilité de groupes

Definition

- G est **résoluble** si on peut écrire $\{e\} = G_n \triangleleft \cdots \triangleleft G_0 = G$ avec G_{i-1}/G_i commutatif
- Le **sous-groupe dérivé** de G est $DG := \langle \{[a, b] = aba^{-1}b^{-1}\} \rangle$

- $DG \triangleleft G$ et G/DG est commutatif : cela définit la **suite dérivée**.
- Si $0 \to G \to M \to D \to 0$ est une suite exacte, M résoluble $\iff$ G et D le sont.
- G est résoluble $\iff \exists n \in \mathbb{N}^*, \quad D^n G = \{e\}$

Tous les anneaux sont considérés commutatifs dans ce cours.

Idéaux

- $I \triangleleft (A, +)$, A/I est un anneau et l'injection π est un morphisme d'anneaux.
- A/I est un corps $\iff$ I est un **idéal maximal** de A (pour $\subset$)

Théorème Chinois

Si $(I_i)_{i=1}^n$ idéaux avec $\forall i \neq j, I_i + I_j = A$ **alors** $\bigcap I_i = I_1 \cdots I_n$ et $A/(I_1 \cdots I_n) \simeq \Pi(A/I_i)$

Definition

$\text{car}(\mathbb{K}) = p \in \mathcal{P} \cup \{0\}$ où pour $\varphi : n \longmapsto n1_A$, $\text{Ker}\varphi = p\mathbb{Z}$

$\exists! \psi : \mathbb{Z}/\text{car}\mathbb{K}\ \mathbb{Z} \hookrightarrow \mathbb{K}$ et si $p = \text{car}\mathbb{K} < +\infty, \quad \text{Im}\psi \simeq \mathbb{F}_p$ c'est le **sous-corps premier** de $\mathbb{K}$

Extensions de corps

Definition

- Si $\mathbb{K}$ est un corps et une k-algèbre c'est une **extension** de k notée $\mathbb{K}/k$
- Le **degré** de $\mathbb{K}/k$ est $[\mathbb{K} : k] := \dim_k(\mathbb{K})$

Théorème de la base télescopique

Si $\mathbb{L}/\mathbb{K}$ et $\mathbb{K}/k$ sont de bases respectives (μ_j) et (λ_i)
alors $(\lambda_i\mu_j)$ est une base de $\mathbb{L}/k$ et $[\mathbb{L} : k] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : k]$

Definition

Si A et B sont des $\mathbb{K}$- algèbres, $\mathrm{Hom}_{\mathbb{K}}(A, B)$: morphismes de $\mathbb{K}$-algèbres de A dans B

On a la bijection $\left\{ \begin{array}{ccc} \mathrm{Hom}_k(\mathbb{K}[X], B) & \longrightarrow & B \\ \varphi & \longmapsto & \varphi(X) \end{array} \right.$

Definition

- Le **corps de rupture** de $P \in k[X]$ irréductible sur k est $k[X]/(P)$
- Le **corps de décomposition** de $P \in k[X]$ est $k[x_1, \cdots x_n]$ avec $\{x_i\} = Z_{\overline{k}}(P)$

- $[k[X]/(P) : k] = \deg P$ et l'image de X (notée x) dans $k[X]/(P)$ est racine de P
- $\mathbb{K} := k[X]/(P) \simeq k[x]$ et $\mathrm{Hom}_k(\mathbb{K}, \mathbb{L}) \simeq Z_{\mathbb{L}}(P)$

Soit P irréductible dans $k[X]$ de degré d et de corps de décomposition $\mathbb{L}$: $[\mathbb{L} : k] \leq d!$ avec égalité ssi P est à racines simples.

Algébricité

Definition

- $x \in \mathbb{K}$ est **algébrique** sur k si $\exists P \in k[X] - \{0\}$ avec $P(x) = 0$, sinon x est **transcendant**. Les algébriques forment un sous-corps de $\mathbb{K}$.
- $\mathbb{K}/k$ est une **extension algébrique** si les éléments de $\mathbb{K}$ sont algébriques sur k.
- Le **polynôme minimal** de $x \in \mathbb{K}$ algébrique sur k est l'unique polynôme de $k[X]$ tel que $\{P \in k[X] \mid P(x) = 0\} = \pi_{x,k}\ k[X]$
- Les k-**conjugués** dans $\mathbb{L}$ de x algébrique sur k sont $\mathrm{Conj}_{k,\mathbb{L}}(x) := Z_{\mathbb{L}}(\pi_{x,k})$

- $\deg_k[x] := [k[x] : k] = \deg \pi_{x,k}$
- x algébrique sur $k \iff [k[x] : k] < +\infty \iff k[x]$ est un corps.
- Si $x_1 \cdots x_n$ sont algébriques, $[k[x_1, \cdots, x_n] : k] \leq \Pi \deg_k(x_i)$
- $[\mathbb{K} : k] < +\infty \iff \mathbb{K}/k$ est algébrique et engendrée par un nombre fini d'éléments.
- On a la bijection $\left\{ \begin{array}{ccc} \mathrm{Hom}_k(k[x], \mathbb{L}) & \longrightarrow & \mathrm{Conj}_{k,\mathbb{L}}(x) \\ \sigma & \longmapsto & \sigma(x) \end{array} \right.$ pour x algébrique sur k.

Clôture algébrique

Definition

- $\mathbb{K}$ est **algébriquement clos** si tout $P \in \mathbb{K}[X]$ non constant est scindé sur $\mathbb{K}$.
- $\mathbb{K}$ est une **clôture algébrique** du sous-corps k si $\mathbb{K}/k$ est algébrique et que tout $P \in k[x]$ est scindé sur $\mathbb{K}$.

Théorème de Steiniz

Tout corps k admet une clôture algébrique $\overline{k}$ unique à morphisme de k-algèbres près.

Théorème de prolongement des morphismes

v1 Soit $\mathbb{K}/k$, Ω/k avec $\mathbb{K}$ algébrique, Ω algébriquement clos **alors** $\mathbb{K}$ se plonge dans Ω

v2 Soit B/A avec A, B des k-algèbres et Ω algébriquement clos vérifiant Ω/A algébrique.

alors tout $\sigma : A \longrightarrow \Omega$ se prolonge en $\sigma' : B \longrightarrow \Omega$:

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & \Omega \\ & \overset{\sigma'}{\nearrow} & \\ B & & \end{array}$$

Corps finis

Definition

Pour $p \in \mathcal{P}$, on note $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. On note $\mathbb{F}_q := Z_\Omega(X^q - X)$ pour $q = p^n$ (voir plus bas)

- Soit k un corps fini. On a $q := \#k = (\mathrm{car}k)^n =: p^n$ et $k = Z_\Omega(X^q - X)$ avec $\Omega = \overline{\mathbb{F}_p}$.
- Le **morphisme de Frobenius** $F : x \longmapsto x^p \ \in \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$
- $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n|m$
- Soit $\mathbb{K}$ un corps. Si $\mathbb{L} \subset (\mathbb{K}^*, \times)$ est fini, il est cyclique.
- $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$ est cyclique d'ordre m engendré par $F_q := x \longmapsto x^q = F^n$

$P \in \mathbb{F}_p[X]$ irréductible de degré d a comme corps de rupture $\mathbb{K} = \mathbb{F}_{p^d}$ car $[\mathbb{K} : \mathbb{F}_p] = d$

$P \in \mathbb{F}_p[X]$ est irréductible sur $\mathbb{F}_p[X]$ ssi il n'a pas de racine dans $\mathbb{F}_{p^r}$ pour $r \leq \frac{\deg P}{2}$.

Tout $\mathbb{F}_q \subset \overline{\mathbb{F}_p}$ extension de $\mathbb{F}_p$ est noyau d'un F^d et $[\mathbb{F}_p[x] : \mathbb{F}_p] = \min\{d \geq 1 |\ F^d(x) = x\}$

$N := o(x, \overline{\mathbb{F}_p}^\times) \wedge p = 1$ et $[\mathbb{F}_p[x] : \mathbb{F}] = o(p, \mathbb{Z}/N\mathbb{Z}^\times)$; $\pi_{x,\mathbb{F}_p} = \prod_{n=0}^{d-1}(X - F^n(x))$

Corps parfaits

Definition

- k est **parfait** si $\mathrm{car}k = 0$ ou si $F \in \mathrm{Aut}_{\mathbb{F}_p}(k)$ (tout $x \in k$ a une $\sqrt[p]{x} \in k$, $p = \mathrm{car}k$)
- $P \in k[X]$ est **séparable** $\iff$ ses racines dans $\overline{k}$ sont simples $\iff P \wedge P' = 1$

- si k est parfait et $\mathbb{K}/k$ est finie alors $\mathbb{K}$ est parfait.
- k est parfait $\iff$ les irréductibles de $k[X]$ sont séparables.
- si k est parfait et $\mathbb{K}/k$ finie alors $\#\mathrm{Hom}_k(\mathbb{K}, \Omega) = [\mathbb{K} : k]$ avec $\Omega = \overline{k}$

Théorème de l'élément primitif

Soit k parfait et $\mathbb{K}/k$ une extension finie **alors** $\mathbb{K}/k$ est **monogène** ($\mathbb{K} = k[x]$)

Extensions galoisiennes

On fixe k parfait avec $k \subset E \subset \mathbb{K}$.

Definition

- $\mathbb{K}/k$ est **galoisienne** si elle est algébrique et que $\forall x \in \mathbb{K},\ \mathrm{Conj}_{k,\Omega}(x) \subset \mathbb{K}$
- dans ce cas on note son **groupe de Galois** $\mathrm{Gal}(\mathbb{K}/k) := \mathrm{Aut}_k(\mathbb{K})$

- Si $\mathbb{K}/k$ est galoisienne, $\mathrm{Gal}(\mathbb{K}/k) := \mathrm{Aut}_k(\mathbb{K}) = \mathrm{Hom}_k(\mathbb{K}, \Omega)$ est d'ordre $[\mathbb{K} : k]$ si finie.
- Si $\mathbb{K}/k$ est galoisienne, $\mathbb{K}/E$ est galoisienne. (pas necéssairement E/k)
- $\mathbb{K}/k$ est galoisienne $\iff$ l'injection canonique $\mathrm{Aut}_k(\mathbb{K}) \hookrightarrow \mathrm{Hom}_k(\mathbb{K}, \Omega)$ est bijective.
- Si $\mathbb{K}/k$ est galoisienne, $\forall x \in \mathbb{K},\ \mathrm{Conj}_{k,\Omega}(x) = G.x := \{\sigma(x) \mid \sigma \in \mathrm{Gal}(\mathbb{K}/k)\}$
- Si $\mathbb{K}/k$ est galoisienne, $\mathrm{Gal}(\mathbb{K}/E)$ est un sous-groupe de $\mathrm{Gal}(\mathbb{K}/k)$.
- Si $\mathbb{K}/k$ et E/k sont galoisiennes, $\varphi : \left\{ \begin{array}{ccc} \mathrm{Gal}(\mathbb{K}/k) & \twoheadrightarrow & \mathrm{Gal}(E/k) \\ \sigma & \mapsto & \sigma|_E \end{array} \right.$ est surjective.

  On a alors une **suite exacte de Galois** $0 \to \mathrm{Gal}(\mathbb{K}/E) \to \mathrm{Gal}(\mathbb{K}/k) \xrightarrow{\varphi} \mathrm{Gal}(E/k) \to 0$
  Avec $\mathrm{Ker}\varphi = \mathrm{Gal}(\mathbb{K}/E)$ et $\mathrm{Gal}(E/k) \simeq \mathrm{Gal}(\mathbb{K}/k)\ /\ \mathrm{Gal}(\mathbb{K}/E)$
- $\mathbb{K}/k$ algébrique est galoisienne $\iff \forall x \in \mathbb{K}, \mathrm{Aut}_k(\mathbb{K}).x = \mathrm{Conj}_{k,\Omega}(x)$ (action transitive)
- $\mathbb{K}/k$ finie est galoisienne $\iff \exists P \in k[X] : \mathbb{K} = k[Z_\Omega(P)]$ (corps de décomposition)
- Si $\mathbb{K}/k$ est galoisienne finie, $\mathbb{K}^G := \{x \in \mathbb{K} \mid \forall \sigma \in G, \sigma(x) = x\} = k$

Lemme d'Artin

Supposons $\mathbb{K}$ parfait, soit $G \subset \mathrm{Aut}_k(\mathbb{K})$ un sous-groupe fini,
alors $\mathbb{K}^G$ est parfait, $\mathbb{K}/\mathbb{K}^G$ est galoisienne et $G = \mathrm{Gal}(\mathbb{K}/\mathbb{K}^G)$.

Correspondance de Galois

Soit $\mathbb{K}/k$ galoisienne finie avec $k \subset \mathbb{K} \subset \Omega$ parfaits et $G := \mathrm{Gal}(\mathbb{K}/k)$.
Soient $\mathcal{F} := \{\mathbb{L} \text{ corps} \mid k \subset \mathbb{L} \subset \mathbb{K}\}$ et $\mathcal{G} := \{\text{sous groupes de } G\}$. On a alors :

- $f : \begin{cases} \mathcal{F} & \longrightarrow & \mathcal{G} \\ \mathbb{L} & \longmapsto & \mathrm{Gal}(\mathbb{K}/\mathbb{L}) \end{cases}$ est bijective ; strictement décroissante. $f^{-1} : \begin{cases} \mathcal{G} & \longrightarrow & \mathcal{F} \\ H & \longmapsto & \mathbb{K}^H \end{cases}$
- pour $H \in \mathcal{G}$, $\mathbb{K}/\mathbb{K}^H$ est galoisienne avec $\mathrm{Gal}(\mathbb{K}/\mathbb{K}^H) = H$
- La restriction à $\mathbb{K}^H$ $r_H : \begin{cases} G & \longrightarrow & \mathrm{Hom}_k(\mathbb{K}^H, \Omega) \\ \sigma & \longmapsto & \sigma|_{\mathbb{K}^H} \end{cases}$ est surjective avec $r_H^{-1}(\{I\}) = H$
- pour $H \in \mathcal{G}$, $\mathbb{K}^H/k$ est galoisienne $\iff$ $H \triangleleft G$ et alors $G/H \simeq \mathrm{Gal}(\mathbb{K}^H/k)$
- Si $\mathbb{L}/k$ est galoisienne, on a la suite exacte $1 \to \mathrm{Gal}(\mathbb{K}/\mathbb{L}) \to \mathrm{Gal}(\mathbb{K}/k) \to \mathrm{Gal}(\mathbb{L}/k) \to 1$

Correspondance de Galois des corps finis

$q = p^n$. $\mathbb{F}_{q^n}/\mathbb{F}_q$ est galoisienne finie, $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle F_q \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.
Soit $\mathcal{F} := \{\mathbb{F}_q \subset \mathbb{L} \subset \mathbb{F}_{q^n}\}$ et $\mathcal{G} := \{G' \subset \mathbb{Z}/n\mathbb{Z}\} = \{r\mathbb{Z}/n\mathbb{Z} \mid r|n\} = \langle F_q^r \rangle \simeq \{\mathbb{Z}/\frac{n}{r}\mathbb{Z}\}$
Dans ce cas $f^{-1} : r\mathbb{Z}/n\mathbb{Z} \longmapsto (\mathbb{F}_{q^n})^{\mathbb{F}_{q^r}} = \{x \in \mathbb{F}^{q^n} \mid x^{q^r} = x\} = \mathbb{F}_{q^r}$
Finalement $\mathbb{Z}/n\mathbb{Z} \;/\; r\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/r\mathbb{Z} \simeq \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ qui contient un r-cycle.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & r\mathbb{Z}/r\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/r\mathbb{Z} & \longrightarrow & 0 \\ I & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^r}) & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q) & \longrightarrow & I \end{array}$$

Polynômes et théorie de Galois

Soit $P \in k[X]$ avec k parfait, on peut se ramener au cas où les racines $x_1 \cdots x_n$ sont simples.

Definition

- Le **groupe de Galois** de P sur k est $\mathrm{Gal}(P, k) := \mathrm{Gal}(k[x_1, \cdots x_n]/k)$.
- Le **discriminant** de P est $\mathrm{discr}P := (-1)^{n(n-1)/2} \prod_{x \neq y \in Z(P)} (x - y) \in k^*$

- P est irréductible sur $k[X] \implies \mathrm{Gal}(P, k)$ agit transitivement (une seule orbite)
- Si $\mathrm{car}k \neq 2$, $\exists d \in k^* : d^2 = \mathrm{discr}P \iff \mathrm{Gal}(P, k) \subset A_n$

$P \in k[X]$ irréductible de degré n. Alors $n \mid \#\mathrm{Gal}(P, k) \mid n!$

Si $P \in \mathbb{Z}[X]$ est de degré 3, il est irréductible sur $\mathbb{Q}[X]$ ssi il n'a pas de racine dans $\mathbb{Q}$

Soit $P \in \mathbb{F}_p[X]$ irréductible de degré n et de racines $x_1, \cdots x_n$. On a $P = \pi_{\mathbb{F}_p, x_1}$.
Soit $\mathbb{K} := \mathbb{F}_p[x_1, \cdots x_n] = \mathbb{F}_q \subset \overline{\mathbb{F}_p}$ avec $q = p^r$.
On a $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_p) \simeq \mathbb{Z}/r\mathbb{Z}$ engendré par F, soit $\varphi : \mathrm{Gal}(\mathbb{K}/\mathbb{F}_p) \hookrightarrow S_n$: Imφ contient un n-cycle.

Théorème de la réduction modulo p

Soit $P \in \mathbb{Z}[X]$ unitaire, séparable. Soit $p \in \mathcal{P}, \overline{P} \in \mathbb{F}_p[X]$ $(\deg \overline{P} = \deg P = n)$
Soit $\varphi : \mathrm{Gal}(P, \mathbb{Q}) \hookrightarrow S_n$ et $\overline{\varphi} : \mathrm{Gal}(\overline{P}, \mathbb{F}_p) \hookrightarrow S_n$. Si $\overline{P}$ est séparable, **alors** :

- $\exists G'$ sous-groupe de $\mathrm{Gal}(P, \mathbb{Q})$ avec $G' \simeq \mathrm{Gal}(\overline{P}, \mathbb{F}_p)$
- $\forall \sigma \in \mathrm{Im}\overline{\varphi},\ \exists \tau \in \mathrm{Im}\varphi$ de même type.
- Si $\overline{P} = P_1 \cdots P_k$ irréductibles alors G contient un élément $c_1 \cdots c_k$ des $\deg P_i$-cycles.
- Si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, il existe un cycle de longueur n dans $\mathrm{Im}\varphi$

Cyclotomie sur k parfait

Soit $n \in \mathbb{N}^*$ avec si $\mathrm{car}k = p > 0, n \wedge p = 1$.

Definition

- $\mu_n(\Omega) := Z_\Omega(X^n - 1) \simeq \mathbb{Z}/n\mathbb{N}$ généré par ζ_n toute **racine primitive** n-ième de 1.
- Le **caractère cyclotomique** $\chi : \mathrm{Gal}(k[\zeta_n]/k) \longrightarrow \mathbb{Z}/n\mathbb{Z}^*$ tel que $g(\zeta) = \zeta^{\chi(g)}$ est un morphisme injectif

- $k[\zeta_n]/k$ est galoisienne c'est la n-ième **extension cyclotomique de** k.
- $G_n := \mathrm{Gal}(k[\zeta_n]/k) = \mathrm{Gal}(X^n - 1, k)$ est commutatif.

Cyclotomie sur $\mathbb{Q}$

Lemme de Gauss

- Soient $P, Q \in \mathbb{Z}[X]$ avec Q unitaire. Si $Q|P$ dans $\mathbb{Q}[X]$ alors aussi dans $\mathbb{Z}[X]$.
- Si $P \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$ alors il l'est dans $\mathbb{Q}[X]$.
- Soit $P \in \mathbb{Z}[X]$ unitaire. Ses facteurs irréductibles dans $\mathbb{Q}[X]$ sont dans $\mathbb{Z}[X]$.

Soit $\zeta_n := e^{\frac{2i\pi}{n}}$

Definition

$$n\text{-ième } \textbf{polynôme cyclotomique} := \phi_n = \prod_{m \in \mathbb{Z}/n\mathbb{N}^*} \left(X - \exp\left(\frac{2im\pi}{n}\right)\right) = \pi_{\zeta_n, \mathbb{Q}} \in \mathbb{Z}[X]$$

- $X^n - 1 = \prod_{d|n} \phi_d$, $\quad \chi$ est surjective donc $\mathrm{Gal}(\mathbb{Q}[e^{\frac{2i\pi}{n}}]/\mathbb{Q}) \simeq \mathbb{Z}/n\mathbb{Z}^*$
- $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \deg \phi_n = \varphi(n) = \#\mathbb{Z}/n\mathbb{Z}^* = \#\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}))$

Constructibilité

- [Wantzel] $z \in \mathbb{C}$ **constructible** $\Leftrightarrow \exists \mathbb{Q} = \mathbb{L}_0 \subset \cdots \subset \mathbb{L}_n \ni z$ avec $[\mathbb{L}_{i+1}/\mathbb{L}i] = 2$
- Soit $z \in \mathbb{C}$ et $\mathbb{K} := \langle \mathrm{Conj}_{\mathbb{Q},\mathbb{C}}(z) \rangle$. z est constructible $\Leftrightarrow [\mathbb{K} : \mathbb{Q}] = 2^n$
- [Gauss-Wantzel] Le polygone régulier à n côtés est constructible $\Leftrightarrow n = 2^N p_1 \cdots p_m$ avec $p_i = 2^{2^{a_i}} - 1 \in \mathcal{P}$

Cyclisme de k parfait

Si car$k = p > 0$, on suppose que $p \wedge n = 1$. On suppose que $\mu_n(\Omega) \subset k$.

Definition

- Une **extension cyclique** est $\mathbb{K}/k$ monogène avec $\mathbb{K} = k[\alpha]$ où $\alpha^n \in k^*$
- $\kappa : \begin{cases} \mathrm{Gal}(_K/k) & \longrightarrow & \mu_n(k) \\ g & \longmapsto & g(\alpha)\alpha^{-1} \end{cases}$ est un morphisme de groupes injectif.

- Si $\mathbb{K}/k$ est cyclique alors $\mathbb{K}$ est le corps de rupture et de décomposition de $X^n - \alpha^n$
- Si $\mathbb{K}/k$ est cyclique alors $\mathrm{Gal}(\mathbb{K}/k) \simeq \mathbb{Z}/d\mathbb{Z}$ cyclique avec $d|n$
- $X^n - \alpha^n$ irréductible dans $k[X] \Leftrightarrow \mathrm{Gal}(\mathbb{K}/k) \simeq \mathbb{Z}/n\mathbb{Z} \simeq \mu_n(k)$

Théorème de Kumman

Si $\mathbb{K}/k$ est galoisienne de degré n et $k \supset \mu_n(\Omega)$ et que $\mathrm{Gal}(\mathbb{K}/k)$ est cyclique **alors** $\exists a \in k$ tel que $\mathbb{K}$ soit le corps de décomposition de $X^n - a$

Résolution d'équations

On suppose que car$k = 0$ et plus d'hypothèse sur la contenance de $\mu_n(\Omega)$.

Definition

- $\mathbb{K}/k$ est **radicale** si $\exists k = \mathbb{K}_0 \subset \cdots \subset \mathbb{K}_n$ avec $\mathbb{K}_{i+1} = \mathbb{K}_i[x_i],\ x_i^{n_i} \in \mathbb{K}_i$
- $\mathbb{K}/k$ est **résoluble** si $\exists \mathbb{L} \supset \mathbb{K}$ avec $\mathbb{L}/k$ radicale.
- $P \in k[X]$ est **résoluble** sur k si pour $\mathbb{K} := k[Z_\Omega(P]]$, $\mathbb{K}/k$ est résoluble.

Si $\mathbb{K}/k$ est résoluble alors tout $x \in \mathbb{K}$ s'écrit comme sommes, produits, fractions et radicaux d'éléments de k.

Théorème de Galois

Si $\mathbb{K}/k$ galoisienne est résoluble **alors** $\mathrm{Gal}(\mathbb{K}/k)$ est résoluble

Solutions d'équations polynomiales

Soit $\mathbb{L} := \mathbb{C}(X_1, \cdots X_n)$. S_n agit dessus par permutation des indéterminées.
Soit $\mathbb{K} := \mathbb{L}^{S_n}$, on a par le lemme d'Artin que $\mathbb{L}/\mathbb{K}$ est galoisienne de groupe S_n.

Par le théorème d'Abel-Galois, $\mathbb{L}/\mathbb{K}$ n'est pas résoluble si $n \geq 5$ car S_n ne l'est pas.

Soit $P(X) = \prod_{i=1}^{n}(X - X_i) = X^n + \sum_{i=1}^{n}(-1)^i \sigma_i X^{n-i} \in (\mathbb{C}(X_1 \cdots X_n))[X]$
Les σ_i sont des expressions symétriques en X_i, donc des éléments invariants par l'action de S_n donc dans $\mathbb{K}$. Comme $\mathbb{L}/\mathbb{K}$ n'est pas résoluble si $n \geq 5$, en général les $X_i \in \mathbb{L}$ ne peuvent pas s'écrire en fonction des $\sigma_i \in \mathbb{K}$.