Lemme 2 : Un polynôme irréductible $P \in K[X]$ est séparable ssi $P' \neq 0$. En particulier, si $\mathrm{car}\, K = 0$, tout polynôme irréductible est séparable.

Dém. : "$\Rightarrow$" P sépar. $\Rightarrow$ $\mathrm{PGCD}(P, P') = 1 \Rightarrow P' \neq 0$.

"$\Leftarrow$" $P' \neq 0$ et $\deg P' < \deg P \underset{P \text{ irréd.}}{\Longrightarrow} \mathrm{PGCD}(P, P') = 1$. ✓

Rque : Soit p un nombre premier. Alors

p divise $\binom{p}{i}$ pour $1 \leq i \leq p-1$,

car dans $\mathbb{Z}/p\mathbb{Z}[X]$, on a

$$0 = \frac{d}{dX}\left[(X+1)^p - X^p\right] = \sum_{i=1}^{p-1} \binom{p}{i} i X^{i-1}.$$

Donc si A est un anneau com. t.q. $p \cdot 1_A = 0$, alors

$$(a+b)^p = a^p + b^p, \quad \forall a, b \in A.$$

Déf : Supposons $\mathrm{car}\, K = p > 0$. Le <u>morphisme de Frobenius</u> de K est l'homomorphisme de corps

$$F_r : K \longrightarrow K, \quad x \longmapsto x^p.$$

Rques : 1) F_r est bien sûr injectif. Si K est fini, il est donc un automorphisme.

2) Si $K = \mathbb{F}_p(T)$, alors l'image de F_r est formée des fractions $P(T^p)/Q(T^p)$, $P, Q \in \mathbb{F}_p[T]$, $Q \neq 0$. Donc, par exemple, T n'est pas dans l'image de F_r. Cela implique que $P = X^p - T \in K[X]$ est irréd. et non séparable, comme le montre le lemme suivant.

Lemme 3: Supposons K de caract. $p>0$. Si $a \notin Fr(K)$, alors $P = X^p - a$ est irréd. et non séparable.

Dém.: Soit Q un facteur irréd. unitaire de P et x une racine de P dans une extension L de K. On a

$$P = X^p - a = X^p - x^p = (X-x)^p$$

et donc $Q = (X-x)^i$ pour un $1 \leq i \leq p$. Comme $x \notin K$, on a $i \geq 2$, donc Q n'est pas séparable, donc $Q' = 0$, donc $i = p$ et $Q = P$ est irréductible et non séparable. ✓

Déf: Le corps K est *parfait* si tout polynôme irréductible de $K[X]$ est séparable.

Prop. 4: a) Si $\mathrm{car} K = 0$, K est parfait.

b) Si $\mathrm{car} K = p > 0$, alors K est parfait ssi Fr est surjectif.
En particulier, les corps finis sont parfaits.

Dém.: a) par le Lemme 2.

b) "$\Rightarrow$" par le Lemme 3.

"$\Leftarrow$" Supposons $P \in K[X]$ irréductible et non séparable.
Alors $P' = 0$ par le Lemme 2. Mais alors on a

$$P(X) = a_0 + a_p X^p + a_{2p} X^{2p} + \dots + a_{rp} X^{rp}$$
$$= (b_0 + b_1 X + \dots + b_r X^r)^p$$

pour des $a_{ip} \in K$ et des $b_i \in K$ t.q. $b_i^p = a_{ip}$, $1 \leq i \leq r$.
C'est une contradiction car P est irréductible ✓

1.3 Corps finis

Rques : Soit K un corps fini.

L'homomorphisme $\mathbb{Z} \xrightarrow{\varphi} K$, $n \longmapsto n 1_K$

a pour image un quotient fini et intègre de $\mathbb{Z}$.

Donc son noyau est $p\mathbb{Z}$ pour un nombre premier p.

p est la caractéristique de K ; l'image de φ est le sous-corps premier de K. Il est can. isom. à $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. K devient une $\mathbb{F}_p$-algèbre finie et en particulier un espace vect. de dim. finie sur $\mathbb{F}_p$.

Donc $|K| = |\mathbb{F}_p^n| = p^n$ pour un entier $n \geq 1$.

Soient p un nombre premier et $n \geq 1$ un entier.

Prop. 1 : a) Il existe un corps fini $\mathbb{F}_q$ à $q = p^n$ éléments, unique (rappel) à isom. (non unique pour $n \geq 2$!) près.

b) $\mathbb{F}_q$ est un corps de décomposition de $X^q - X \in \mathbb{F}_p[X]$.

c) Le groupe $\mathbb{F}_q^\times$ est cyclique.

Thm 2 : Le groupe $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ est cyclique d'ordre n et engendré par $\mathrm{Fr} : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $x \longmapsto x^p$.

Dém. : On a $\mathrm{Fr} \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ et Fr est d'ordre n car

$x^{p^n} = x$, $\forall x \in \mathbb{F}_q$, et

$x^{p^m} \neq x$ si $1 \leq m < n$ et x engendre $\mathbb{F}_q^\times$.

Or on a $|\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = n$ d'après la prop. 1.1.2 :

$\mathbb{F}_q$ est un corps de décomp. sur $\mathbb{F}_p$ du polynôme $X^q - X$, qui est à racines simples dans $\mathbb{F}_q$. Donc $|Gal(\mathbb{F}_q/\mathbb{F}_p)| = n$ ✓

$$\begin{array}{ccc} \mathbb{F}_q & \xrightarrow{\tilde{\sigma}} & \mathbb{F}_q \\ \uparrow & & \uparrow \\ \mathbb{F}_p & \xrightarrow[\sigma = \mathrm{Id}]{} & \mathbb{F}_p \end{array}$$

Rque : Dém. directe du fait que $Gal(\mathbb{F}_q/\mathbb{F}_p)$ est d'ordre n :
Soient x un générateur de $\mathbb{F}_q^\times$ et P son polynôme minimal. Alors x engendre le corps $\mathbb{F}_q$. Donc $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(P)$ et P est de degré n. Comme P a un facteur $X-x$ en commun avec $X^q - X$ et est irréductible dans $\mathbb{F}_p[X]$, P divise $X^q - X$. Donc P est scindé à racines simples dans $\mathbb{F}_q$. Par le lemme 1.1.1, on a la bijection

$$Gal(\mathbb{F}_q/\mathbb{F}_p) \xrightarrow{\sim} \{\text{racines de } P \text{ dans } \mathbb{F}_q\}, \quad \sigma \longmapsto \sigma(x).$$

Thm 3 : Soit d un diviseur de n. Alors

$$K_d = \{x \in \mathbb{F}_q \mid Fr^d(x) = x\}$$

est un ss-corps à p^d éléments de $\mathbb{F}_q$ et c'est le seul. Tout ss-corps de $\mathbb{F}_q$ est obtenu ainsi.

Dém. : Comme $Fr^d : \mathbb{F}_q \to \mathbb{F}_q$ est un automorphisme, K_d est un ss-corps. Il est formé des racines de $P = X^{p^d} - X$, i.e. de 0 et des racines (p^d-1)-ièmes de 1. Or d divise n donc $p^d - 1$ divise $p^n - 1$ et $\mathbb{F}_q^\times$ contient (p^d-1) racines (p^d-1)-ièmes de 1. Donc $|K_d| = p^d$ (et $K_d \simeq \mathbb{F}_{p^d}$). Réciproquement, soit $L \subseteq \mathbb{F}_q$ un sous-corps. On a $|L| = p^m$ pour un $m \geq 1$. Comme $\mathbb{F}_q$ est un L-espace vectoriel, on a $q = p^n = (p^m)^r$ pour un r, et m divise n. On a $L \subseteq K_m$ car

$x^{p^m} = x$ pour tout $x \in L \tilde{=} \mathbb{F}_{p^m}$. Donc $L = K_n$ car les deux ont même nombre d'éléments. ✓

Cor. 4 (correspondance de Galois) : On a des bijections inverses l'une de l'autre

$$\{\text{ss-groupes de } \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{\text{extensions intermédiaires } \mathbb{F}_p \subseteq L \subseteq \mathbb{F}_q\}$$

$$H \longmapsto \mathbb{F}_q^H = \{x \in \mathbb{F}_q \mid \sigma(x) = x,\ \forall \sigma \in H\}$$

$$\mathrm{Gal}(\mathbb{F}_q/L) \longleftarrow L$$

Dém. : Φ est bijective par le Thm 3. Soit d un diviseur de n. Soient $H = \langle F_p^d \rangle$ et $L = \mathbb{F}_q^H \cong \mathbb{F}_{p^d}$. On a $H \subseteq \mathrm{Gal}(\mathbb{F}_q/L)$ et

$$n/d = [\mathbb{F}_q : L] \underset{\text{P1.1.2}}{\geqslant} |\mathrm{Gal}(\mathbb{F}_q/L)| \geqslant |H| = n/d.$$

Donc $\Psi\Phi(H) = H$. ✓

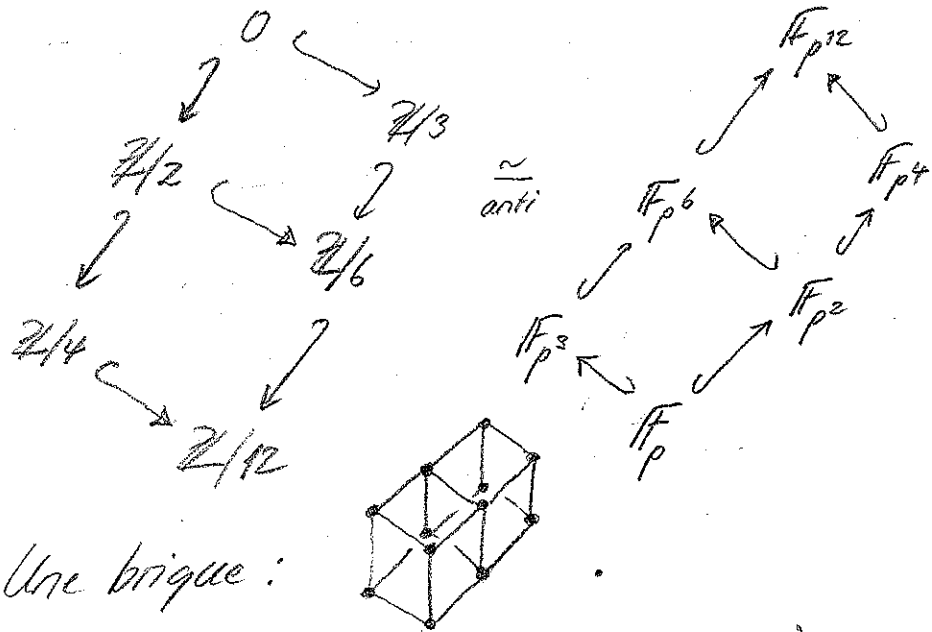
Rque : Ces bijections renversent les inclusions :

$$H_1 \subseteq H_2 \iff \mathbb{F}_q^{H_1} \supseteq \mathbb{F}_q^{H_2}.$$

On a donc un isomorphisme d'ensembles ordonnés :

$$(\text{ss-gr. de } \mathbb{Z}/n\mathbb{Z},\ \subseteq)^{op} \simeq (\text{ss-ext. } \mathbb{F}_p \subseteq L \subseteq \mathbb{F}_q).$$

Pic. pour $n = 12$:



Dessin pour $\mathbb{F}_{p^{60}}$? Une brique : .

Cas général : un produit de chaînes (= ens. totalement ordonnés).

Cor. 5 : Soit $\mathbb{F}_q = \mathcal{O}_0 \cup \mathcal{O}_1 \cup \dots \cup \mathcal{O}_N$ la décomposition en orbites sous l'action de $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Alors chaque $P_{\mathcal{O}_i} = \prod_{x \in \mathcal{O}_i} (X - x)$ est à coeff. dans $\mathbb{F}_p$ et irréd..

En outre, on a $X^q - X = \prod_{i=1}^{N} P_{\mathcal{O}_i}$.

Dém. : On a $Fr(P_{\mathcal{O}_i}) = P_{\mathcal{O}_i}$. Donc $P_{\mathcal{O}_i}$ est à coeff. dans $\mathbb{F}_p$.
Soit Q un facteur irréd. de $P_{\mathcal{O}_i}$. Comme l'ens. des racines de Q est stable par $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, on a $\deg Q = \deg P_{\mathcal{O}_i}$. Finalement, on a

$$X^q - X = \prod_{x \in \mathbb{F}_q} (X - x) = \prod_{i=1}^{N} \prod_{x \in \mathcal{O}_i} (X - x). \quad \checkmark$$

1.4 Groupe de Galois de $K(X)$ et théorème de Lüroth

Soit K un corps.

But : Comprendre $\mathrm{Gal}(K(X)/K)$ et la nature des extensions intermédiaires $K \subset L \subset K(X)$.

Lemme 1 : Soit $u \in K(X) \setminus K$. Soient $P, Q \in K[X]$ t.q.

$$u = P/Q, \quad \mathrm{PGCD}(P,Q) = 1.$$

a) u est transcendant sur K.

b) L'extension $K(u) \subseteq K(X)$ est algébrique de degré

$$\delta(u) = \max(\deg(P), \deg(Q)).$$

c) Le polynôme minimal de X sur $K(u)$ est le normalisé de $P(T) - Q(T)\cdot u \in K(u)[T]$.

Dém. : a), b), c) : $R(T) := P(T) - Q(T)\cdot u$. On a $R(X) = 0$. Donc X est algébrique sur $K(u)$ de degré $\leq \deg_T R(T) = \max(\deg P, \deg Q)$. $K(X) \supseteq K(u)$ est une extension algébrique et u doit être transcendant sur K (sinon X serait algébrique sur K). Donc on peut considérer

$$R(T) = P(T) - u\,Q(T)$$

comme élément de $(K[T])[u]$, où u est une indéterminée. $R(T)$ y est irréductible car de degré 1 en u et à coeff. premiers entre eux. Donc il est irréd. dans $(K(u))[T]$ et dans $K(u)[T]$ (car non constant en T). ✓

Thm 2 : On a un isomorphisme

$$\mathrm{PGL}_2(K) \xrightarrow{\sim} \mathrm{Gal}(K(X)/K), \quad \overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} \mapsto \left(X \mapsto \frac{aX+b}{cX+d}\right)$$

Dém.: Soit $\varphi: K(X) \to K(X)$ un K-automorphisme. Il est déterminé par $u = \varphi(X)$. Comme φ est surjectif, on a $K(u) = K(X)$. Donc $\delta(u) = [K(X) : K(u)] = 1$.

Ainsi, on a $u = \dfrac{aX+b}{cX+d}$

pour des $a, b, c, d \in K$ t.q. $(c,d) \neq (0,0)$ et (a,b) n'est pas proportionnel à (c,d). Donc $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Gl_2(K)$. On a donc montré que l'application

$$Gl_2(K) \longrightarrow Gal(K(X)/K), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \left(X \longmapsto \frac{aX+b}{cX+d}\right)$$

est surjective. On vérifie que c'est un homomorphisme de noyau $K^* \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. ✓

Thm 3 (Lüroth[1]): Les extensions intermédiaires $K \subsetneq L \subsetneq K(X)$ sont de la forme $L = K(u)$, $u \in K(X)$.

Exemple: $L = \{ f(X) \in K(X) \mid f(X) = f(1/X) \}$ est un corps intermédiaire. On a $L = K(X + 1/X)$!

Rappel: Soit A un anneau factoriel (p.ex. $A = K[X]$). Un polynôme

$$P(T) = a_0 T^n + a_1 T^{n-1} + \dots + a_1 T + a_0 \in A[T] \setminus \{0\}$$

est primitif si les a_i sont premiers entre eux dans leur ensemble. Le produit de deux polynômes primitifs est primitif. On en déduit: si $P \in A[T] \setminus \{0\}$ est primitif et $Q \in \mathrm{Frac}(A)[T]$, alors

$$PQ \in A[T] \Longrightarrow Q \in A[T].$$

---

1) Jakob Lüroth, 1844 - 1910. Le thm est paru dans Math. Ann. en 1874.