Extensions de Corps - Exemples et Applications

125

Cadre : $\mathbb{K}$ désigne un corps et A un anneau.

I - Corps et Extensions de Corps :

1°) Définitions et Premières propriétés :

Déf : un corps $\mathbb{K}$ est un anneau non nul, tel que tous les éléments non nuls soient inversibles.

Ex : $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, sont des corps. $\mathbb{Z}/p\mathbb{Z}$ corps ac p premier.

Déf : Il existe un uniq morphisme d'anneaux $f : \begin{pmatrix} \mathbb{Z} \to A \\ n \mapsto n1_A \end{pmatrix}$ ...
on appelle Caractéristique de A, l'unique plus petit entier naturel $c \in \mathbb{N}$ / $\mathrm{Ker} f = c\mathbb{Z}$. on note $\mathrm{car} A = c$.

Ex : $\mathrm{car}\,\mathbb{R} = \mathrm{car}\,\mathbb{Z} = \mathrm{car}\,\mathbb{Q} = \mathrm{car}\,\mathbb{Z} = 0$; $\mathrm{car}\,\mathbb{F}_p = p$ avec p premier

Prop : si $\mathrm{car} A = 0$ alors A est un anneau infini.

Cex : $\mathbb{F}_p(X)$ corps infini de caractéristique p.

Déf : on appelle extension de corps de k, tout corps $\mathbb{K}$ / il existe un morphisme de corps $j : (k \to K)$.
on note K/k l'extension de corps ou encore $k \subset K$.

Rmq : si k sous corps de K alors K/k extension de corps.

Ex : $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $K(T)/\mathbb{K}$, Tout corps est l'extension de son corps 1er.

Déf : on appelle degré de l'extension K/k, noté $[K:k]$, la dimension de $\mathbb{K}$ comme k-ev : $[K,k] = \dim_k \mathbb{K}$.

Ex : $[\mathbb{C}:\mathbb{R}] = 2$, $[\mathbb{R},\mathbb{Q}] = +\infty$, $[k(X):k] = +\infty$.

Rmq : $[K:k] = 1 \iff \mathbb{K} = k$.

Rmq : si K/k extension de degré fini "n" alors $\mathbb{K} \simeq k^n$.

Théo : de la base Télescopique : soit $k \subset K \subset L$ extension de corps
1°) Soient $(\alpha_i)_{i\in I}$ une base de K sur k et $(\beta_j)_{j\in J}$ une base de L sur K. Alors $(\alpha_i\beta_j)_{i,j \in I\times J}$ base de L sur K.
2°) L/K est une extension finie $\iff$ K/k, L/K le sont aussi. De plus, $[L:k] = [L:K][K:k]$

Ex : Base de $\mathbb{Q}(\sqrt{2})$: $\{1, \sqrt{2}\}_{\mathbb{Q}}$
Base de $\mathbb{Q}(\sqrt{2})(\sqrt{3})$: $\{1, \sqrt{3}\}_{\mathbb{Q}(\sqrt{2})}$ $\Big\} \Rightarrow$ Base de $\mathbb{Q}(\sqrt{2},\sqrt{3})$: $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$
$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2\times 2 = 4$.

App : si K/k extension de degré p premier alors K/k est une extension monogène et n'admet aucune sous extension.

Déf : on dit que K/k est une extension de type fini ssi il existe une partie finie $\{\alpha_1, \dots, \alpha_n\}$ de K / $K = k(\alpha_1, \dots, \alpha_n)$.

Rmq : si $K = k(\alpha)$, on parle d'extension monogène / simple

Déf après $1/n$

Ex : $\mathbb{Q}(\sqrt[3]{2})$ extension monogène de degré 3.

2°) Extensions algébriques - Transcendantes :

Déf : soit K/k une extension de corps. soit $a \in K\setminus k$.
on dit que "a" élément algébrique de K ssi $\exists P \in k[X] / P(a) = 0$
on dit que "a" élément transcendant de K ssi $\nexists P \in k[X] / P(a) = 0$

Déf : on appelle polynome minimal de "a" sur k, l'unique polynome unitaire, irréductible de $k[X]$ qui s'annule en "a", noté $\mu_{a,k}$

Ex : • $\sqrt{2}, i, \sqrt[3]{2}$ algébrique sur $\mathbb{Q}$ de polynome minimal X^2-2, X^2+1, X^3-2.
• e, π transcendant sur $\mathbb{Q}$ (ADMIS)

Prop : "a" algébrique sur $k \iff k(a) \simeq k[a] \iff [k(a):k] = \deg \mu_{a,k} < +\infty$
Dans ce cas, $(1, a, a^2, \dots, a^{\deg \mu_{a,k} - 1})$ k-base de $k(a)$.

Rmq : si $\deg \mu_{a,k} = 1$ alors $a \in k$.

Ex : soit $a = 2^{1/n} \in \mathbb{R}\setminus\mathbb{Q}$, de polynôme minimal : $X^n - 2$.

Déf : on dit que K/k est une extension algébrique ssi tous les éléments de K sont algébriques.
on parle d'extension transcendante, dans le cas contraire.

Ex : l'ensemble des éléments algébrique sur k est une extension algébrique de k.

Prop : une extension de degré fini est algébrique.

Cex : l'ensemble des éléments algébrique sur $\mathbb{Q}$ est infini

Déf : on dit que $P \in K[X]\setminus K$ est séparable ssi P est scindé à racines simples dans l'une des extensions de corps de K.

Déf : soit L/K une extension algébrique.
on dit que L est une extension séparable de K ssi tous les éléments de K, ont leurs polynomes minimales séparables.

Ex : $X^2+1 \in \mathbb{Q}[X]$ séparable ; $X^2+T \in \mathbb{F}_2[X]$ inséparable.

Théo : de l'élément primitif → corps de décomp AVANT
soit L/K une extension de degré fini et séparable. Alors L/K est une extension monogène ie $\exists x \in L \,/\, L = K(x)$.
on dit que x est l'élément primitif de K/k.

App : $\mathbb{Q}(i,\sqrt{2}) = \mathbb{Q}(i+\sqrt{2})$, $\mathbb{Q}(i,j,\sqrt{2}) = \mathbb{Q}(i+j+\sqrt{2})$

II - Adjonction de Racines :

1°) Corps de Rupture :

Déf : soit k un corps. soit $P \in k[X]$ un polynome irréductible.
une extension K/k est appelé corps de rupture de P sur k ssi $\exists \alpha \in K \,/\, P(\alpha) = 0$ et $K = k(\alpha)$.

Théo : Existence et Unicité :
soit k un corps. soit $P \in k[X]$ irréductible. Alors il existe toujours un corps de rupture et il est unique à isomorphisme près.

Ex : $\mathbb{C} = \mathbb{R}[X]/(X^2+1) \simeq \mathbb{R}(i)$; $\mathbb{F}_2(j) = \mathbb{F}_2[X]/(X^2+X+1) \simeq \mathbb{F}_2(j^2)$

Rmq : si $\deg P = 1$ avec $P \in k[X]$ alors k corps de rupture de P.

App : soit $P \in k[X] \,/\, \deg P = n$.
[P irréductible dans $k[X]$ $\Leftrightarrow$ P n'a pas de racines dans les extensions $K/k \,/\, [K:k] \leq n/2$]

2°) Corps de Décomposition :

a) Définitions Propriétés :

Déf : soit K/k extension de corps. soit $P \in k[X] \,/\, \deg P = n$.
on appelle corps de décomposition de P sur k, l'extension de corps minimal de k dans laquelle P est un produit de facteur de degré 1. on le note $L = \mathcal{D}_k(P)$.

Théo : Existence et Unicité :
$\forall P \in k[X]$, il existe toujours un corps de décomposition de P sur k, unique à isomorphisme près.

Prop : soit $\mathcal{D}_k(P)$ corps de décomposition de $P \in k[X]\setminus k$.
si $n = \deg P > 0$ et $\alpha_1, \dots, \alpha_n$ racines distinctes ou confondues de P dans $\mathcal{D}_k(P)$ alors $\mathcal{D}_k(P) = k(\alpha_1, \dots, \alpha_n)$

Ex : $k = \mathbb{Q}$, $P = X^3-2$, $\mathcal{D}_k(P) = \mathbb{Q}(\sqrt[3]{2}, j) \neq \mathbb{Q}(\sqrt[3]{2})$ corps de rupture
$k = \mathbb{Q}$, $P = X^2-2$, $\mathcal{D}_k(P) = \mathbb{Q}(\sqrt{2})$ corps de rupture et corps de décomposition

Rmq : k corps de décomposition sur k, $\forall P \in k[X] \,/\, \deg P = 1$.

b) Applications aux corps Finis :

Théo : soit p un nombre premier. soit $n \in \mathbb{N}^*$. on pose $p^n = q$.
1°) il existe un corps fini à p^n éléments. Il est noté $\mathbb{F}_{p^n}$.
c'est le corps de décomposition sur $\mathbb{F}_p$ de $X^{p^n} - X$.
2°) ce corps fini à p^n élément est unique à isomorphisme près.

Théo : soient p premier, $n \in \mathbb{N}^*$, Notons $q = p^n$. Alors
$\mathbb{F}_q \simeq \mathbb{F}_p[X]/(\pi)$ où $\pi \in \mathbb{F}_p[X]$ irréductible quelconque / $\deg \pi = n$

Cor : • il existe des polynomes irréductibles de tout degré dans $\mathbb{F}_p[X]$
• si π est un polynome irréductible de degré n sur $\mathbb{F}_p$ alors $\pi(X)$ divise $X^{p^n} - X$ dans $\mathbb{F}_p[X]$, donc est scindé sur $\mathbb{F}_{p^n}$, donc son corps de rupture $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(\pi)$ est aussi son corps de décomposition.

App : Dénombrement des polynomes irréductibles unitaires sur $\mathbb{F}_q$

3°) Clôture Algébrique :

Déf : on dit que K est algébriquement clos s'il vérifie l'une quelconque des équivalences suivantes :

1°) Tout polynome de degré ≥ 1 de $K[X]$ admet au moins une racine ds K

2°) Tout polynome de degré ≥ 1 de $K[X]$ est scindé sur K.

3°) Tout polynome irreductible de $K[X]$ est degré 1.

4°) ⓢ L/K extension algébrique ⓢ $L=K$.

Ex : $\mathbb{Q}, \mathbb{R}$ ne sont pas algébriquement clos car X^2+1 n'a pas de racine dans $\mathbb{Q}, \mathbb{R}$.

App : D'Alembert - Gauss : $\mathbb{C}$ est algébriquement clos.

Prop : Tout corps algébriquement clos est infini.

Ex : un corps fini n'est jamais algébriquement clos

Théo : Pour tout corps k, il existe au moins une extension algébriquement close de k.

Prop : un corps algébriquement clos n'admet aucune extension algébriq.

App : Les polynomes irreductibles de $\mathbb{C}[X]$ sont des polynomes de degré 1. Les polynomes irreductibles de $\mathbb{C}[X]$ sont des polynomes de degré 1 et 2.

Déf : soit L/K extension de corps.
on appelle Cloture algébrique de K, toute extension L de K telle que
i) L est algébriquement clos
ii) L est algébrique sur K.
on note $\overline{K}=L$ la cloture algébrique.

Théo : Tout corps admet une unique cloture algébrique (à isomorphisme près).

Ex : $\mathbb{C}$ cloture algébrique de $\mathbb{R}$ mais pas de $\mathbb{Q}$

App : cloture algébriq de $\mathbb{F}_{p^n}$ coïncide avec celle de $\mathbb{F}_p$: $\bigcup_{i\in\mathbb{N}} \mathbb{F}_{p^{i!}}$

III - Construction à la règle et compas :

Déf : soit P_0 une partie de $\mathbb{R}^2$ avec $\mathrm{card}(P_0) \geq 2$. on considère :
a) les droites (AB) avec $(A,B) \in P_0^2$, $A \neq B$
b) les cercles $C(A, \|AB\|)$ avec $(A,B) \in P_0^2$, $A \neq B$
on dit qu'un point M du plan $\mathbb{R}^2$ est constructible en une étape à partir de P_0 par la règle et le compas ⓢ M est le point d'intersect° de deux droites distinctes de type a) ou de deux cercles distincts de type b) ou d'une droite de type a) et d'un cercle de type b), construit à la règle et au compas.

Déf : un point M de $\mathbb{R}^2$ est dit constructible à partir de P_0, s'il existe une suite finie de points $M_1, \dots, M_n = M$ tels que $\forall 1 \leq i \leq n$, le point M_i est construit en une étape à partir de l'ensemble de points $P_0 \cup \{M_1, \dots, M_{i-1}\}$

Prop : soit $x \in \mathbb{R}$. [le point $(x,0)$ constructible $\Leftrightarrow$ $(0,x)$ constructible
on dit dans ce cas que x est un nombre constructible.

Prop : Tout élément de $\mathbb{Q}$ est constructible.

Prop : $M(x,y)$ constructible $\Leftrightarrow$ x, y sont constructibles.

Théo : Wantzel : soit $t \in \mathbb{R}$.
[t est constructible $\Leftrightarrow$ $\exists$ une suite finie $(K_0, K_1, \dots, K_p)$ de sous corps de $\mathbb{R}$ / $t \in L^p$, $\forall i \in [\![0, p-1]\!]$, L_{i+1}/L_i extension quadratique, $L_0 = \mathbb{Q}$]

Cor : ⓢ $x \in \mathbb{R}$ est constructible alors $\exists \ell \in \mathbb{N}$ / $[\mathbb{Q}(x):\mathbb{Q}] = 2^\ell$

App : L'Impossibilité de la duplication du cube.

Prop : le point $(\cos\theta, \sin\theta)$ constructible $\Leftrightarrow$ $\cos\theta$ constructible
$\Leftrightarrow$ $\sin\theta$ constructible.
on dit alors que θ est un angle constructible.

Déf : soit $n \in \mathbb{N}^*$. on dit que le polygone régulier à n côtés est constructible ⓢ l'angle $\frac{2\pi}{n}$ est constructible.

Déf : les nombres de Fermat, sont les nombres de la forme
$\forall n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$.

Théo : Gauss - Wantzel :
soit $p \geq 3$ nombre premier. soit $\alpha \in \mathbb{N}^*$.
le polygone régulier à p^α cotés est constructible $\Leftrightarrow$ $\alpha = 1$ et p est un nombre premier de Fermat.

Référence : Gozard. Théorie de Galois
Francinou - Gianella - exercices de mathematique
PERRIN -
Mercier

Premier développement : Théorème de l'élément primitif

1er février 2016

Théorème 1 *Toute extension finie de caractéristique nulle admet un élément primitif.*

Démonstration

Soit $K \subset L$ une extension finie de caractéristique nulle.
Dans un premier temps on suppose qu'il existe $x, y \in L$ tels que : $L = K[x, y]$.
On note P_x et P_y les polynômes minimaux de x et y, de degrés respectifs m et n.
On considère M un corps de décomposition de P_x et P_y, et on note $x_2, \ldots, x_m$ les conjugués de x et $y_2, \ldots, y_n$ les conjugués de y dans M.

On sait que K est de caractéristique nulle, donc séparable.
Donc les racines de P_y sont deux à deux distinctes.
On pose alors $E := \{\frac{x - x_i}{y - y_j} \ ; \ 1 \leqslant i \leqslant m, \ 2 \leqslant j \leqslant n\}$.
E est fini, de cardinal inférieur ou égal à $(m-1)(n-1)$, et comme K est de caractéristique nulle il contient une infinité d'éléments.
On peut donc prendre un t dans K^* tel qu'il ne soit pas dans E, et on pose : $z := x + ty$.

On pose $K' := K[z]$, et $F(X) := P_x(z - tX)$. On va montrer que $K' = L$.

D'abord, on remarque que $P_y \in K[X] \subset K'[X]$, et que F est la composée de deux polynômes de $K'[X]$.
P_y et F sont donc dans $K'[X]$, donc leur pgcd l'est également.

Calculons ce pgcd. Dans $M[X]$, F se décompose ainsi :

$$\begin{aligned} F(X) &= ((z - tX) - x)\prod_{i=2}^{m}((z - tX) - x_i) \\ &= (x + ty - tX - x)\prod_{i=2}^{m}(x + ty - tX - x_i) \\ &= t(y - X)\prod_{i=2}^{m}(x - x_i + t(y - X)) \end{aligned}$$

et P_y ainsi :

$$P_y(X) = (X - y)\prod_{j=2}^{n}(X - y_j)$$

Donc $X - y$ divise F et P_y.

Par ailleurs, par choix de t, on a :

$$\begin{aligned} &\forall\, 2 \leqslant i \leqslant m,\ \forall\, 2 \leqslant j \leqslant n, \quad x - x_i + t(y - y_j) \neq 0 \\ &\implies \forall\, 2 \leqslant j \leqslant n, \quad F(y_j) \neq 0 \end{aligned}$$

Donc y est l'unique racine commune de F et P_y dans $M[X]$.
Donc $X - y = \gcd(F, P_y)$.
Donc $y \in K'$.

De même, $x \in K'$.
Donc $K' = L$, ie L admet z comme élément primitif.

On a ainsi démontré le cas où L est engendré par deux éléments.
Montrons par récurrence que : $\forall n \geqslant 2$, $L := K(x_1, \ldots, x_n)$ est monogène.

- Pour $n = 2$, cette proposition est vraie d'après ce qui précède.

- Soit $n \geqslant 2$, tel que la proposition soit vraie au rang n.
  On pose : $L := K(x_1, \ldots, x_{n+1}) = K(x_1, \ldots, x_n)(x_{n+1})$.
  D'après l'hypothèse de récurrence, il existe $y \in L$ tel que $K(x_1, \ldots, x_n) = K(y)$.
  On a donc : $L = K(y)(x_{n+1}) = K(y, x_{n+1})$.
  D'après ce qui précède, il existe donc $z \in L$ tel que $K(y, x_{n+1}) = K(z)$.
  L est monogène, la propriété est donc vérifiée au rang n+1.

On a ainsi démontré le théorème.

Application : En appliquant la méthode utilisée dans la démonstration, on peut trouver $\alpha \in \mathbb{C}$ tel que $\mathbb{Q}(\alpha) = \mathbb{Q}(i, j, \sqrt{2})$:

Commençons par trouver z tel que $\mathbb{Q}(z) = \mathbb{Q}(i, \sqrt{2})$.
Le polynôme minimal de i est $P(X) = X^2 + 1$ de racines i et $-i$, et le polynôme minimal de $\sqrt{2}$ est $Q(X) = X^2 - 2$, de racines $\sqrt{2}$ et $-\sqrt{2}$.
Il faut donc trouver $t \in \mathbb{Q}^*$ tel que $i + t\sqrt{2} \neq -i - t\sqrt{2}$.
$t = 1$ convient. En posant $z = i + \sqrt{2}$, on a donc : $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(z)$.

Passons à α.
Le polynôme minimal de j est $R(X) = X^2 + X + 1$, de racines j et j^2, et le polynôme minimal de z est $(X^2 - 1)^2 + 8$ (admis), de racines z, $-z$, $\overline{z}$ et $-\overline{z}$.
Il faut donc trouver $t' \in \mathbb{Q}^*$ tel que $i + \sqrt{2} + t'j \neq \pm i \pm \sqrt{2} + t'j$, les signes devant i et $\sqrt{2}$ n'étant pas simultanément positifs.
Ici encore, $t' = 1$ convient. D'où finalement : $\mathbb{Q}(i, j, \sqrt{2}) = \mathbb{Q}(i + j + \sqrt{2})$.

Polygones réguliers constructibles [1]

Leçons : 102, 121, 125, 182, 183

[MerCdG], théorème 318

Théorème (*Gauss-Wantzel*)

Soit p un nombre premier impair, $\omega \exists \mathbb{N}^*$.
Alors l'angle $\frac{2\omega}{p^{\omega}}$ est constructible $\exists$ $\omega = 1$ et p est un nombre premier de Fermat (c'est-à-dire que p est un nombre premier qui s'écrit sous la forme $1 + 2^{2^{\omega}}$, où $\omega \in \mathbb{N}$).

Démonstration :

- On pose $q = p^{\omega}$ et $\omega = \exp\left(\frac{2i\omega}{q}\right)$.

  On suppose que l'angle $\frac{2\omega}{q}$ est constructible, id est, que $\cos\left(\frac{2\omega}{q}\right)$ est un nombre constructible.

  Alors, par le théorème de Wantzel [2], on obtient : $\left[\mathbb{Q}\left(\cos\frac{2\omega}{q}\right) : \mathbb{Q}\right] = 2^m$, où $m \exists \mathbb{N}$.

  Aussi, le polynôme cyclotomique $\prod_q$ étant le polynôme minimal de ω, on a :

  $$[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg \prod_q = \omega(q) = p^{\omega-1}(p-1).$$

  Comme $\omega^2 - 2\omega \cos\frac{2\omega}{q} + 1 = 0$, on a $\cos\frac{2\omega}{q} \exists \mathbb{Q}(\omega)$ et même $\left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\frac{2\omega}{q}\right)\right] = 2$.
  Par multiplicativité du degré, on obtient $2^{m+1} = p^{\omega-1}(p-1)$.
  Comme p est impair, il vient $\omega = 1$, puis $p = 1 + 2^{m+1}$; montrons que $m+1$ est une puissance de 2.
  On écrit alors $m + 1 = \omega 2^{\omega}$, avec $\omega \exists \mathbb{N}$ et $\omega \exists \mathbb{N}^{\exists}$ impair ; on a alors $p = 1 + \left(2^{2^{\omega}}\right)^{\omega}$.
  Or, ω étant impair, on a dans $\mathbb{Z}[X]$: $1 + X \mid 1 + X^{\omega}$ et donc $1 + 2^{2^{\omega}} \mid p$ et donc, comme p est premier, on en déduit $\omega = 1$.
  Donc p est un nombre premier de Fermat.

- On note $n = 2^{\omega}$, de sorte que $p = 1 + 2^n$, et $\xi = \exp\left(\frac{2i\omega}{p}\right)$.
  On a : $[\mathbb{Q}(\xi) : \mathbb{Q}] = \deg \prod_p = \omega(p) = p - 1$.

---

1. On peut ajouter quelques résultats autour de ce développement pour détailler son utilité.

Lemme

- Les angles de la forme $\frac{2\omega}{2^{\omega}}$ sont constructibles, où $\omega \exists \mathbb{N}^{\exists}$.
- Soient $m, n \exists \mathbb{N}^*$, avec $m \wedge n = 1$,
  Alors l'angle $\frac{2\omega}{mn}$ est constructible $\exists$ $\frac{2\omega}{m}$ et $\frac{2\omega}{n}$ le sont.

En conséquence, les polygones réguliers constructibles sont ceux qui possèdent $2^{\omega} \prod_{p \exists \mathcal{F}} p^{\omega_p}$ côtés, où $\mathcal{F}$ est l'ensemble des nombres premiers de Fermat, et où les ω_p sont des entiers naturels.

En effet :
- C'est immédiat, puisque par récurrence, il suffit de savoir tracer des bissectrices à la règle et au compas.
- $\exists$ Il est facile de construire le multiple d'un nombre constructible (en reportant avec le compas le bon nombre de fois la corde formée par l'angle sur le cercle unité).

  $\exists$ Par Bézout, $\exists \omega, \mu \exists \mathbb{Z}, \omega m + \mu n = 1$; dès lors $\frac{2\omega}{mn} = \omega\frac{2\omega}{m} + \mu\frac{2\omega}{n}$.
  Et on construit sans peine la somme de deux angles constructibles en traçant des représentants de ces angles avec un côté adjacent.

2. Le théorème de Pierre-Laurent Wantzel, énoncé en 1837, donne une condition nécessaire et suffisante pour qu'un nombre soit constructible à la règle et au compas : il faut et il suffit que ce nombre appartienne à une extension de $\mathbb{Q}$ qui soit le terme d'une suite d'extensions quadratiques.

On note $G = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta))$; et si $g \exists G$, alors g fixe $\mathbb{Q}$ et est entièrement déterminé par $g(\zeta)$.
g étant un morphisme d'anneaux, on a : $0 = g(0) = g\ \Pi_p(\zeta) = \Pi_p(g(\zeta))$.
Donc $g(\zeta)$ est nécessairement une racine de Π_p, donc $g(\zeta) \exists\ \zeta, \zeta^2, \ldots, \zeta^{p-1}$.
Il faudrait alors montrer qu'on définit bien ainsi des automorphismes du corps $\mathbb{Q}(\zeta)$; et alors

$$G = g_k : \zeta \exists \zeta^k k \exists [\![1, p-1]\!] \exists \mathbb{Z}/p\mathbb{Z}^{\times} \underset{3}{\exists} \mathbb{Z}/(p-1)\mathbb{Z}.$$

Désormais, g désignera un générateur de G.
Pour $i \exists [\![0, n]\!]$, on note $K_i = \mathrm{Ker}\ g^{2^i} - \mathrm{Id}$; c'est un sous-corps de $\mathbb{Q}(\zeta)$.
De plus, $\exists i \exists [\![0, n-1]\!], g^{2^{i+1}} = g^{2^i\,2}$ implique $K_i \exists K_{i+1}$.
Comme g génère G, $g^i(\zeta)_{0 \leqslant i \leqslant p-2}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\zeta)$.
Soit $z \exists K_0$, $\exists \omega_0, \ldots, \omega_{p-2} \exists \mathbb{Q}$, $z = \sum_{i=0}^{p-2} \omega_i g^i(\zeta)$; mais $z = g(z) = \omega_{p-2}\zeta + \sum_{i=1}^{p-2} \omega_{i-1} g^i(\zeta)$.
Tous les scalaires ω_i sont donc égaux et $z = \omega_0 \sum_{i=0}^{p-2} g^i(\zeta) = \omega_0 \sum_{j=1}^{p-1} \zeta^j = -\omega_0 \exists \mathbb{Q}$. Donc $K_0 = \mathbb{Q}$.

Pour montrer que $\exists i \exists [\![0, n-1]\!], K_i \not\exists K_{i+1}$, il faudrait considérer l'élément $z = \sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}h}(\zeta)$.[4]
On en déduit alors qu'on a la suite d'extensions :

$$\mathbb{Q} = K_0 \underset{\neq}{\exists} K_1 \underset{\neq}{\exists} \ldots \underset{\neq}{\exists} K_n = \mathbb{Q}(\zeta).$$

Mais $2^n = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \prod_{i=0}^{n-1} \underbrace{[K_{i+1} : K_i]}_{\geqslant 2}$.
Ainsi, $\exists i \exists [\![0, n-1]\!], [K_{i+1} : K_i] = 2$.
Par le théorème de Wantzel, tous les éléments de $\mathbb{Q}(\zeta)$ sont donc constructibles ; mais $\cos \frac{2\omega}{p} = \frac{\zeta + \zeta^{-1}}{2}$ en fait partie. ■

Références

[MerCdG][5] D.-J. MERCIER – *Cours de géométrie, préparation au CAPES et à l'agrégation*, Publibook, 2008.

3. Pour la cyclicité de $\mathbb{F}_p^{\times}$, on renvoie à la page ??.

4. Okay, je le fais, mais c'est vraiment parce que c'est vous. On a : $g^{2^i}(z) = \sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}h+2^i}(\zeta) \not\exists z$ car les vecteurs de base intervenant dans la décomposition ne sont pas les mêmes (on a décalé les coordonnées de 2^i, alors qu'entre deux coordonnées non-nulles, il y a $2^{i+1} - 1$ zéros). Et aussi : $g^{2^{i+1}}(z) = \sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}(h+1)}(\zeta) = \sum_{h=1}^{2^{n-i-1}-1} g^{2^{i+1}h}(\zeta) + \underbrace{g^{2^{i+1}2^{n-i-1}}(\zeta)}_{=\zeta} = z$.

5. On trouvera également dans cette référence une façon de construire le pentagone régulier à la règle et au compas.