Extensions de corps

Dans tout ce qui suit, les corps seront supposés *commutatifs*.

Extensions de corps

Soit K un corps.

Définition

Une *extension* de K est un corps L qui contient K comme sous-corps. On note L/K l'extension. Un morphisme d'extensions entre L_1/K et L_2/K est un morphisme $f : L_1 \to L_2$ qui induit l'identité sur K. On parle aussi du *K-morphisme* $f : L_1 \to L_2$.

Exemples

(1) $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{Q}(X)/\mathbb{Q}$.
(2) $\mathbb{Q}\left[\sqrt{2}\right] = \{a + b\sqrt{2}\,;\, a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$. C'est l'image du morphisme $\mathrm{ev}_{\sqrt{2},\mathbb{Q}} : \mathbb{Q}[X] \to \mathbb{C}$ qui envoie P sur $P(\sqrt{2})$, dont le noyau est $\langle X^2 - 2\rangle$: il induit un isomorphisme $\mathbb{Q}[X]/\langle X^2 - 2\rangle \xrightarrow{\sim} \mathbb{Q}\left[\sqrt{2}\right]$. Comme $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$, cela montre que $\mathbb{Q}\left[\sqrt{2}\right]$ est un corps : c'est une extension de $\mathbb{Q}$.

Définition

Les corps $\mathbb{Q}$ et $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ avec p premier sont appelés les *corps premiers*.

Proposition

On a les deux possibilités suivantes :

- $\text{car}(K) = 0$ donc $\mathbb{Q} \subset K$;
- $\text{car}(K) = p$ est premier et $\mathbb{F}_p \subset K$.

Exercice

Montrer que le seul automorphisme d'un corps premier est l'identité.

Remarque

Si L/K est une extension, alors L est naturellement muni d'une structure de K-espace vectoriel (on peut additionner les éléments de L et les multiplier par un élément de K).

Définition

Le *degré* de l'extension L/K est l'entier (fini ou infini) $[L : K] := \dim_K(L)$. Si le degré est fini, on dit que l'extension L/K est *finie*.

Exemple

$[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$, $[\mathbb{Q}(X) : \mathbb{Q}] = \infty$ et $\left[\mathbb{Q}\left[\sqrt{2}\right] : \mathbb{Q}\right] = 2$.

Théorème- Construction fondamentale

Si $P \in K[X]$ est irréductible de degré d, le quotient $K[X]/\langle P(X)\rangle$ est une extension de degré d de K. Une base est fournie par $(1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{d-1})$ (où $\overline{X}$ est l'image de X dans $K[X]/\langle P(X)\rangle$).

Remarques

(1) Calcul des inverses dans $K[X]/\langle P(X)\rangle$. Si $Q \in K[X]$ est tel que $\pi(Q) = a \in K[X]/\langle P(X)\rangle^\times$, on a $Q \notin \langle P\rangle$, donc $\text{pgcd}(P, Q) = 1$: il existe une relation de Bézout $UP + QV = 1$ avec $U, V \in K[X]$. Dans $K[X]/\langle P(X)\rangle$, on a $\overline{Q}\,\overline{V} = 1$: V est un représentant de a^{-1} dans $K[X]$.
(2) On voit sur cet exemple d'où vient la terminologie de « degré » d'une extension.

Exemple

$P = X^2 - 2$ est irréductible dans $\mathbb{Z}[X]$: il l'est dans $\mathbb{Q}[X]$. L'extension correspondante est $\mathbb{Q}[\sqrt{2}] = \{x + y\sqrt{2},\ \ x, y \in \mathbb{Q}\}$; on a $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. Calculons l'inverse de $1 + \sqrt{2}$. On a $X^2 - 2 = (X - 1)(X + 1) - 1$: en projetant dans $\mathbb{Q}[\sqrt{2}]$, il vient $(1 + \sqrt{2})^{-1} = -1 + \sqrt{2}$.

Exercice

Soit $P \in K[X]$. Montrer que les propriétés suivantes sont équivalentes :

(i) P est irréductible ;

(ii) $K[X]/\langle P(X)\rangle$ est un corps ;

(iii) $K[X]/\langle P(X)\rangle$ est un intègre.

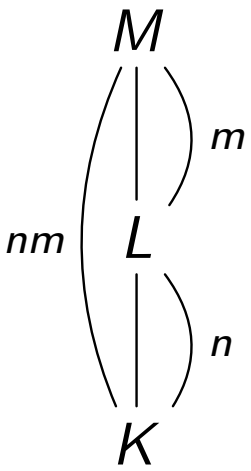
À quelle condition sur P l'anneau $K[X]/\langle P(X)\rangle$ est-il réduit ?

Théorème de la base télescopique

Si L/K et M/L sont des extensions, alors M/K est une extension, et

$$[M : K] = [M : L][L : K].$$

La proposition précédente se résume simplement par le diagramme suivant :



Extensions de corps

Définition

Soit L/K une extension. Une *sous-extension* de L/K est un sous-corps E de L qui contient K.

Exemple

$\mathbb{R}$ et une sous-extension de $\mathbb{C}\,/\,\mathbb{Q}$.

Remarques

(1) D'après le théorème de la base télescopique, si E/K est une sous-extension d'une extension finie L/K, alors $[E : K]|[L : K]$. Cela implique par exemple que si $[L : K]$ est premier, les seules sous-extensions de L/K sont L et K.
(2) Si L/K est une extension et $(E_i)_{i\in I}$ une famille de sous-extensions, alors $\bigcap_{i\in I} E_i$ est une sous-extension de L/K.

Définition

Soient L/K une extension et $S \subset L$. La sous-extension de L/K *engendrée* par S est la plus petite sous-extension de L/K qui contient S. Elle existe et est unique : c'est l'intersection des sous-extensions de L/K qui contiennent S. On la note $K(S)$.
On dit que L est *engendrée* par S sur K si $L = K(S)$. L'extension L/K est dite *de type fini* s'il existe S fini tel que $L = K(S)$.

Remarques

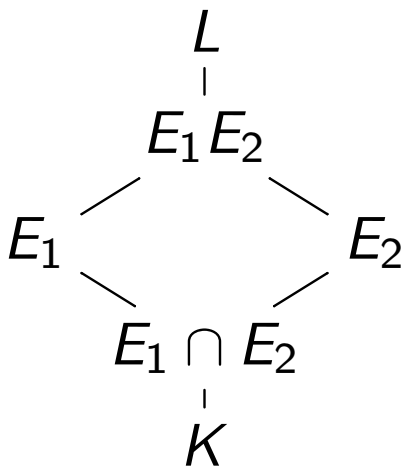
(1) $K(S)$ est constitué des éléments qui peuvent s'écrire sous $R(s_1, \ldots, s_n)$ avec $s_1, \ldots, s_n \in S$ et $R \in K(X_1, \ldots, X_n)$ une fraction rationnelle dont le dénominateur ne s'annule pas en $(s_1, \ldots, s_n)$.
(2) Si L/K est finie, alors c'est une extension de type fini (une K-base de L est génératrice). ⚠La réciproque est fausse : $\mathbb{Q}(X)$ est de type fini sur $\mathbb{Q}$, mais $[\mathbb{Q}(X) : \mathbb{Q}] = \infty$.

Définition - compositum

Soient L/K une extension et E_1, E_2 deux sous-extensions. Leur *compositum* est la sous extension engendrée par $E_1 \cup E_2$. C'est la plus petite sous-extension de L/K qui contient E_1 et E_2 : on la note E_1E_2.

Remarques

(1) Si $E_1 = K(S_1)$ et $E_2 = K(S_2)$, alors $E_1E_2 = K(S_1 \cup S_2)$.
(2) ⚠ En général, $E_1 \cup E_2$ n'est pas une sous-extension de L/K.



Extensions algébriques

Soient L/K une extension et $\alpha \in L$. On dispose du morphisme d'évaluation en α

$$\begin{aligned} \mathrm{ev}_{\alpha,K} : K[X] &\to L \\ P &\mapsto P(\alpha). \end{aligned}$$

On note $K[\alpha]$ son image.

Définition

(1) On dit que α est *transcendant* sur K si le morphisme $\mathrm{ev}_{\alpha,K}$ est injectif, et *algébrique* sur K dans le cas contraire.
(2) Si α est algébrique sur K, on appelle *polynôme mininal* de α sur K l'unique générateur unitaire de $\mathrm{Ker}(\mathrm{ev}_{\alpha,K})$. On le note $P_{\alpha,K}$. Le *degré* de α sur K est le degré de $P_{\alpha,K}$, on le note $\deg_K(\alpha)$.

Remarque

⚠Les notions qui précèdent dépendent très fortement du corps de base. Par exemple, si X est une indéterminée, alors $X \in \mathbb{Q}(X)$ est transcendant sur $\mathbb{Q}$, mais algébrique sur $\mathbb{Q}(X)$. L'élément $i \in \mathbb{C}$ est algébrique sur $\mathbb{R}$ et sur $\mathbb{C}$, mais $P_{i,\mathbb{R}}(X) = X^2 + 1$ et $P_{i,\mathbb{C}}(X) = X - i$.

Exemples

(1) Si $L = K(X)$ et P est un polynôme non constant, alors P est transcendant sur K. Les nombres π et e sont transcendants sur $\mathbb{Q}$ (mais c'est un peu difficile à prouver).
(2) Si $\alpha \in K$, alors α est algébrique sur K, et $P_{\alpha,K}(X) = X - \alpha$.
(3) Les nombres $\sqrt{2}$, $\sqrt{2} + \sqrt{3}$ sont algébriques sur $\mathbb{Q}$, de polynômes minimaux sur $\mathbb{Q}$ respectifs $X^2 - 2$ et $X^4 - 10X^2 + 1$.

Proposition

Soient L/K une extension et $\alpha \in L$ algébrique sur K. Alors $P_{\alpha,K}$ est irréductible dans $K[X]$, et l'anneau $K[X]/\langle P_{\alpha,K}\rangle \simeq K[\alpha]$ est un corps. En particulier, on a $K(\alpha) = K[\alpha]$ et $[K(\alpha) : K] = \deg_K(\alpha)$.

Remarque

Si L/K est une extension, $P \in K[X]$ un polynôme unitaire irréductible dans $K[X]$ et $\alpha \in L$ une racine de P, alors $P_{\alpha,K} = P$.

Exemple

Si $n \in \mathbb{N}_{>0}$, le polynôme $X^n - 2$ est irréductible dans $\mathbb{Z}[X]$ (Eisenstein), donc dans $\mathbb{Q}[X]$. Comme il admet $e^{\frac{2ik\pi}{n}}\sqrt[n]{2}$ comme racine, c'est le polynôme minimal de $e^{\frac{2ik\pi}{n}}\sqrt[n]{2}$ pour tout $k \in \{0, \ldots, n-1\}$.

Proposition

Soient L/K une extension, E/K une sous-extension et $\alpha \in L$ algébrique sur K. Alors α est algébrique sur E et $P_{\alpha,E} \mid P_{\alpha,K}$ dans $E[X]$.

Exemple

Les nombres $\sqrt{2}$, $\sqrt{2}+\sqrt{3}$ sont algébriques sur $\mathbb{Q}$, donc *a fortiori* sur $E = \mathbb{Q}[\sqrt{2}]$. Les polynômes minimaux sur E sont $X - \sqrt{2}$ et $X^2 - 2\sqrt{2}X - 1$ respectivement.

Proposition - critère d'algébricité

Soient L/K une extension et $\alpha \in L$. Les conditions suivantes sont équivalentes :

(i) α est algébrique sur K ;

(ii) $K[\alpha]$ est un corps ;

(iii) $K(\alpha)$ est un K-espace vectoriel de dimension finie ;

(iv) il existe une sous-extension finie E de L/K telle que $\alpha \in E$.

Corollaire

Soient L/K une extension et $\alpha, \beta \in L^\times$ algébriques sur K, alors $\alpha - \beta$ et $\alpha\beta^{-1}$ sont algébriques sur K. En particulier, l'ensemble des éléments de L qui sont algébriques sur K est une sous-extension de L/K.

Définition - corps des nombres algébriques

On pose $$\overline{\mathbb{Q}} = \{z \in \mathbb{C}\,;\, z \text{ est algébrique sur } \mathbb{Q}\}.$$

D'après le corollaire, c'est un sous-corps de $\mathbb{C}$: on l'appelle le *corps des nombres algébriques*.

Proposition

Le corps $\overline{\mathbb{Q}}$ est dénombrable.

Corollaire

On a $\text{Card}(\mathbb{C} \setminus \overline{\mathbb{Q}}) = \text{Card}(\mathbb{C})$.

Remarque historique

Théorème de Liouville

Soit $\alpha \in \overline{\mathbb{Q}} \cap \mathbb{R}$ de degré $d > 1$ sur $\mathbb{Q}$. Il existe une constante $c(\alpha) \in \mathbb{R}_{>0}$ telle que pour tout $(p, q) \in \mathbb{Z} \times \mathbb{N}_{>0}$, on ait $\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}$.

Corollaire - premières constructions de nombres transcendants

$\sum_{n=0}^{\infty} \frac{1}{2^{n!}}$ est transcendant sur $\mathbb{Q}$.

Extensions finies, extensions algébriques

Définition

Une extension L/K est dite *algébrique* si tous les éléments de L sont algébriques sur K.

Exemple

Les extensions $\overline{\mathbb{Q}}/\mathbb{Q}$ et $\mathbb{Q}(X)[\sqrt{2}]/\mathbb{Q}(X)$ sont algébriques, mais $\mathbb{R}/\mathbb{Q}$ et $\mathbb{Q}(X)/\mathbb{Q}$ ne le sont pas.

Proposition

Les intersection et les composés d'extensions algébriques sont algébriques. Une sous-extension engendrée par des éléments algébriques est algébrique.

Proposition

Une extension L/K est finie si et seulement si elle est algébrique et de type fini.

Remarques

(1) On a montré qu'une extension L/K est finie si et seulement si elle est de la forme $L = K(\alpha_1, \ldots, \alpha_n)$ avec $\alpha_1, \ldots, \alpha_n \in L$ algébriques sur K.
(2) Si K est de caractéristique nulle et L/K est finie, on peut montrer qu'il existe $\alpha \in L$ tel que $L = K(\alpha)$ (théorème de l'élément primitif).
(3) ⚠ Une extension algébrique n'est pas nécessairement finie. Par exemple, $\overline{\mathbb{Q}}/\mathbb{Q}$ est algébrique par définition, mais elle n'est pas de degré fini (car $n = \left[\mathbb{Q}\left(\sqrt[n]{2}\right) : \mathbb{Q}\right] \leq [\overline{\mathbb{Q}} : \mathbb{Q}]$ pour tout $n \in \mathbb{N}_{>0}$).

Exercice

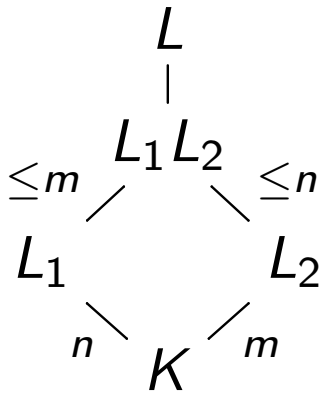
Montrer que toute extension algébrique est réunion de ses sous-extensions finies.

Corollaire

Soient M/L et L/K deux extensions. Alors M/K est algébrique si et seulement si M/L et L/K sont algébriques.

Proposition

Soient L/K une extension et L_1/K, L_2/K deux sous-extensions finies. Alors L_1L_2/K est finie et $[L_1L_2 : K] \leq [L_1 : K][L_2 : K]$.



Remarque

⚠ L'inégalité précédente peut être stricte. C'est trivialement le cas lorsque $L_1 = L_2 \neq K$. Autre exemple (plus instructif) : $K = \mathbb{Q}$, $L_1 = \mathbb{Q}\left(\sqrt[3]{2}\right)$ et $L_2 = \mathbb{Q}\left(j\sqrt[3]{2}\right)$.

Corollaire

Soient L/K une extension et L_1, L_2 deux sous-extensions finies tq $\text{pgcd}([L_1 : K], [L_2 : K]) = 1$, alors $[L_1 L_2 : K] = [L_1 : K][L_2 : K]$.

Exercices

(1) Calculer les degrés de $\mathbb{Q}(\sqrt{2}, \sqrt[2]{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ sur $\mathbb{Q}$.
(2) Montrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ et $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$.
(3) Soient L/K une extension et L_1, L_2 deux sous-extensions algébriques. Montrer que $L_1 L_2/K$ est algébrique.

Corps de rupture, corps de décomposition

Définition

Soient L/K une extension de corps et $P \in K[X]$.
(1) On dit que L est un *corps de rupture* si L est engendré sur K par une racine de P.
(2) On dit que P est *scindé* sur L si ses facteurs irréductibles dans $L[X]$ sont tous degré 1.
(3) On dit que L est un *corps de décomposition* de P sur K si P est scindé dans $L[X]$ et L est engendré sur K par les racines de P.

Exemples

(1) $\mathbb{C}$ est corps de rupture (et de décomposition) de X^2+1 sur $\mathbb{R}$.
(2) Le corps $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de X^3-2 sur $\mathbb{Q}$, mais pas un corps de décomposition : il ne contient pas $j\sqrt[3]{2}$. Le corps $\mathbb{Q}(j,\sqrt[3]{2})$ est un corps de décomposition.

Proposition

Si $P \in K[X]$ est irréductible, le corps $K[X]/\langle P(X)\rangle$ est un corps de rupture de P sur K, et tout corps de rupture de P sur K est isomorphe à $K[X]/\langle P(X)\rangle$.

Corollaire

Tout $P \in K[X]$ admet un corps de décomposition.

Exemple

$P(X) = X^3 - 2 \in \mathbb{Q}[X]$ est irréductible sur $\mathbb{Q}$. Un corps de rupture de P est $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{C}$. Un corps de décomposition est $\mathbb{Q}(j, \sqrt[3]{2})$.

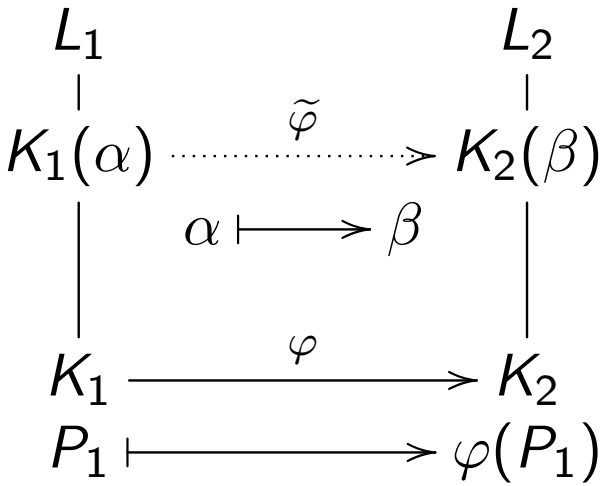
Exercice

Si $P \in K[X]$ est de degré d et L est un corps de décomposition de P sur K, on a $[L : K] \leq d!$

Théorème - Prolongement des isomorphismes

Soient L_1/K_1 et L_2/K_2 des extensions, $\varphi\colon K_1 \xrightarrow{\sim} K_2$ un isomorphisme, et $P \in K_1[X]$ un polynôme irréductible. Notons $\varphi(P) \in K_2[X]$ le polynôme irréductible obtenu en appliquant φ aux coefficients de P. Soient $\alpha \in L_1$ (resp. $\beta \in L_2$) une racine de P (resp. de $\varphi(P)$). Il existe un unique isomorphisme $\widetilde{\varphi}\colon K_1(\alpha) \xrightarrow{\sim} K_2(\beta)$ qui prolonge φ et tel que $\widetilde{\varphi}(\alpha) = \beta$.

On peut résumer la proposition précédente par le diagramme suivant :



Définition

Soient L/K une extension et $\alpha, \beta \in L$ algébriques sur K. On dit que α et β sont *conjugués* sur K s'ils ont même polynôme minimal sur K.

Corollaire

D'après la théorème de prolongement des isomorphismes, $\alpha, \beta \in L$ sont conjugués sur K si et seulement s'il existe un K-isomorphisme $\sigma : K(\alpha) \to K(\beta)$ tel que $\sigma(\alpha) = \beta$.

Corollaire

Si $P \in K[X]$, deux corps de décomposition de P sur K sont isomorphes comme extensions de K.

Corps algébriquement clos, clôture algébrique

Définition

Soit K un corps. Les propriétés suivantes sont équivalentes :

(i) Tout polynôme non constant à coefficients dans K est scindé ;

(ii) tout polynôme non constant à coefficients dans K admet une racine dans K ;

(iii) K n'a pas d'extension algébrique non triviale.

Si elles sont vérifiées, on dit que K est *algébriquement clos*.

Théorème - d'Alembert-Gauss

Le corps $\mathbb{C}$ est algébriquement clos.

Corollaire

Les polynômes irréductibles dans $\mathbb{R}[X]$ sont :

- les polynômes de degré 1 ;
- les trinômes du second degré à discriminant strictement négatif.

Définition

Soit K un corps. Une *clôture algébrique* de K est une extension $\overline{K}/K$ algébrique telle que $\overline{K}$ est algébriquement clos.

Proposition

Si C/K une extension avec C algébriquement clos, alors

$$\overline{K} = \{z \in C\,;\, z \text{ est algébrique sur } K\}$$

est une clôture algébrique de K.

Exemple

$\mathbb{C}$ étant algébriquement clos, $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$.

Théorème - Steiniz

Tout corps K admet une clôture algébrique. Si $\overline{K}$ est une clôture algébrique et C/K une extension avec C algébriquement clos, il existe un K-morphisme $\overline{K} \to C$. Les clôtures algébriques de K sont donc deux à deux isomorphes.

Construction de base. Soit $(P_\lambda)_{\lambda\in\Lambda}$ la famille des polynômes irréductibles unitaires de $K[X]$. Posons $A = K[X_\lambda]_{\lambda\in\Lambda}$, et I l'idéal de A engendré par les éléments $P_\lambda(X_\lambda) \in A$. Supposons $I = A$: il existe une égalité de la forme $\sum_{i=1}^{n} Q_i P_{\lambda_i}(X_{\lambda_i}) = 1$ où $\lambda_1, \dots \lambda_n \in \Lambda$ et $Q_1, \dots, Q_n \in A$. Soit L/K tq chaque P_{λ_i} a une racine α_i dans L et $\varphi\colon A \to L$ le morphisme d'anneaux K-linéaire défini par

$$\varphi(X_\lambda) = \begin{cases} \alpha_i & \text{si } \lambda = \lambda_i \text{ pour } i \in \{1, \dots, n\} \\ 0 & \text{sinon} \end{cases}$$

En appliquant φ à l'égalité, il vient $0 = 1$: contradiction.

L'idéal I est donc *strict* : soit $\mathfrak{m}$ un idéal maximal de A tel que $I \subset \mathfrak{m}$ (Krull) et posons $\widetilde{K} = A/\mathfrak{m}$. C'est un corps, extension algébrique de K (engendré sur K par les classes des X_λ), et $P_\lambda(\overline{X}_\lambda) = 0$ dans le quotient $\widetilde{K} = A/\mathfrak{m}$. Si $P \in K[X]$ est non constant, il existe $\lambda \in \Lambda$ tel que $P_\lambda \mid P$, donc P a racine dans $\widetilde{K}$.

Corollaire

Soient L/K une extension algébrique et $\overline{K}$ une clôture algébrique de K. Alors il existe un K-morphisme $L \to \overline{K}$.

Exemples fondamentaux

Extensions cyclotomiques

Soit $n \in \mathbb{N}_{>0}$. Posons

$$\mu_n = \{z \in \mathbb{C}\,;\, z^n = 1\}.$$

C'est un sous-groupe cyclique de $\mathbb{C}^\times$. Notons μ_n^* le sous-ensemble de μ_n constitué des éléments d'ordre n, *i.e.* des générateurs du groupe μ_n (ses éléments sont les *racines primitives n-ièmes de l'unité*). On a

$$\mu_n = \bigsqcup_{d|n} \mu_d^*$$

(c'est la partition de μ_n suivant l'ordre des éléments). Fixons $\zeta \in \mu_n^*$. On pose

$$\Phi_n(X) = \prod_{\xi \in \mu_n^*} (X - \xi) = \prod_{\substack{1 \leq k < n \\ \mathrm{pgcd}(k,n)=1}} (X - \zeta^k)$$

C'est un polynôme de degré $\varphi(n)$, unitaire, séparable et à coefficients dans $\mathbb{C}$.

Exemples

On a

$$\Phi_1(X) = X - 1$$
$$\Phi_2(X) = X + 1$$
$$\Phi_3(X) = X^2 + X + 1$$
$$\Phi_4(X) = X^2 + 1$$
$$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$$
$$\Phi_6(X) = X^2 - X + 1$$
$$\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$
$$\Phi_8(X) = X^4 + 1$$
$$\Phi_9(X) = X^6 + X^3 + 1$$

Remarque

Contrairement aux apparences, les coefficients des polynômes cyclotomiques ne sont pas tous dans $\{-1, 0, 1\}$: on a

$$\Phi_{105}(X) = X^{48}+X^{47}+X^{46}-X^{43}-X^{42}-2X^{41}-X^{40}-X^{39}+X^{36}$$
$$+X^{35}+X^{34}+X^{33}+X^{32}+X^{31}-X^{28}-X^{26}-X^{24}-X^{22}-X^{20}+X^{17}$$
$$+X^{16}+X^{15}+X^{14}+X^{13}+X^{12}-X^{9}-X^{8}-2X^{7}-X^{6}-X^{5}+X^{2}+X+1$$

Proposition

Si $n \in \mathbb{N}_{>0}$, on a $X^n - 1 = \prod_{d|n} \Phi_d(X)$, $n = \sum_{d|n} \varphi(d)$ et $\Phi_n \in \mathbb{Z}[X]$.

Exemple

Si p est premier et $r \in \mathbb{N}_{>0}$, on a $\Phi_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1}$: on a en particulier

$$\Phi_p(X) = 1 + X + \cdots + X^{p-1}$$

et $\Phi_{p^r}(X) = \Phi_p\left(X^{p^{r-1}}\right)$.

On a vu que Φ_p est irréductible dans $\mathbb{Q}[X]$. C'est un fait général :

Proposition

Si $n \in \mathbb{N}_{>0}$, le polynôme Φ_n est irréductible sur $\mathbb{Q}$. En particulier, c'est le polynôme minimal de ζ sur $\mathbb{Q}$.

Lemme

Soient A un anneau factoriel, $K = \mathrm{Frac}(A)$ et $P, Q \in K[X]$ unitaires tels que $PQ \in A[X]$. Alors $P, Q \in A[X]$.

Corps finis

Dans tout ce qui suit, K désigne un corps fini.

Proposition

(1) $p := \mathrm{car}(K)$ est un nombre premier ;
(2) on a $\#K = p^d$ avec $d \in \mathbb{N}_{>0}$.

Théorème de Wedderburn

Tout corps fini est commutatif.

Lemme - morphisme de Frobenius

Soient A un anneau commutatif de caractéristique p et $a, b \in A$.
On a

$$(a+b)^p = a^p + b^p.$$

Existence et unicité des corps finis

Définition

Soient F un corps et $P \in F[X]$. On dit que P est *séparable* si ses racines (prises dans une clôture algébrique de F) sont simples.

Lemme - critère de séparabilité

Si F est un corps, un polynôme $P \in F[X]$ est séparable si et seulement si $\text{pgcd}(P, P') = 1$ (où P' désigne le polynôme dérivé).

Remarque

⚠Si $\text{car}(F) = p > 0$, il faut prendre garde au phénomème suivant. Le polynôme dérivé de X^p est $pX^{p-1} = 0$: des polynômes non constants peuvent avoir une dérivée nulle. Plus précisément, les polynômes de dérivée nulle sont ceux de la forme $Q(X^p)$ avec $Q \in F[X]$ (exercice).

Exercices

(1) Soit $P \in F[X]$ un polynôme irréductible. Montrer que P est séparable si et seulement si $P' \neq 0$. En déduire que tout polynôme irréductible est séparable lorsque $\text{car}(F) = 0$.
(2) Soient p un nombre premier, X et T deux indéterminées, et $F = \mathbb{F}_p(T)$. Montrer que le polynôme $P(X) = X^p - T$ est irréductible dans $F[X]$, mais pas séparable.

Théorème

Soient p un nombre premier, $d \in \mathbb{N}_{>0}$ et $q = p^d$.
(1) Il existe un corps à q éléments.
(2) Tout corps à q éléments est un corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$, en particulier, deux corps à q éléments sont isomorphes.

Dans la pratique, on fixe une clôture algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$, et on pose

$$\mathbb{F}_q = \{\alpha \in \overline{\mathbb{F}}_p \,;\, \alpha^q = \alpha\}$$

Corollaire

(1) $\mathbb{F}_q$ est l'unique sous-corps de cardinal q dans $\overline{\mathbb{F}}_p$;
(2) $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n} \Leftrightarrow d \mid n$;
(3) $\mathbb{F}_{p^d} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^{\mathrm{pgcd}(d,n)}}$;
(4) $\overline{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.

Remarques

(1) ⚠On n'a pas $\mathbb{F}_{p^n} \simeq \mathbb{Z}/p^n\mathbb{Z}$ dès que $n > 1$ (l'anneau $\mathbb{Z}/p^n\mathbb{Z}$ n'est pas réduit si $n > 1$). De même, on a $\mathbb{F}_{p^n} \simeq \mathbb{F}_p^n$ en tant que $\mathbb{F}_p$-espace vectoriel, mais pas en tant qu'anneau si $n > 1$ (l'anneau produit $\mathbb{F}_p^n$ n'est pas intègre si $n > 1$).
(2) On a $\mathbb{F}_4 \not\subset \mathbb{F}_8$ (en fait on a $\mathbb{F}_4 \cap \mathbb{F}_8 = \mathbb{F}_2$).

Exercice

Montrer que $\sum_{\alpha \in \mathbb{F}_q} \alpha = 0$. Plus généralement, calculer la somme $\sum_{\alpha \in \mathbb{F}_q} \alpha^k$ pour tout $k \in \mathbb{N}_{>0}$.

Structure du groupe multiplicatif

Lemme

Soit G un groupe abélien (noté multiplicativement).
(1) Si $x \in G$ est d'ordre n et $y \in G$ d'ordre m avec $\text{pgcd}(n, m) = 1$, alors xy est d'ordre nm.
(2) Supposons G fini, et soit d le ppcm des ordres des éléments de G (l'*exposant* de G). Alors G contient un élément d'ordre d.

Proposition

Si F est un corps et G un sous-groupe fini de $F^\times$, alors G est cyclique.

Corollaire

Le groupe $K^\times$ est cyclique.

Corollaire - théorème de l'élément primitif pour un corps fini

Si $\text{car}(K) = p$, il existe $\alpha \in K$ tel que $K = \mathbb{F}_p(\alpha)$.

Dans la pratique, si p est premier et $d \in \mathbb{N}_{>0}$, pour construire et manipuler le corps $\mathbb{F}_{p^d}$, on le présente sous la forme

$$\mathbb{F}_p[X]/(P)$$

avec $P \in \mathbb{F}_p[X]$ irréductible de degré d. On sait que c'est toujours possible, et que le résultat ne dépend pas *à isomorphisme près* du choix de P. Dans le quotient $\mathbb{F}_p[X]/(P)$, on dispose de la base canonique $(1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{d-1})$: on peut représenter les éléments dans cette base. Il est alors très facile de les additionner, un peu plus délicat de les multiplier (il faut multiplier des représentants et prendre le reste par la division euclidienne par P).

Exemples

(1) $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/\langle X^2 + X + 1\rangle$;
(2) $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/\langle X^3 + X + 1\rangle \simeq \mathbb{F}_2[X]/\langle X^3 + X^2 + 1\rangle$.

Extensions quadratiques

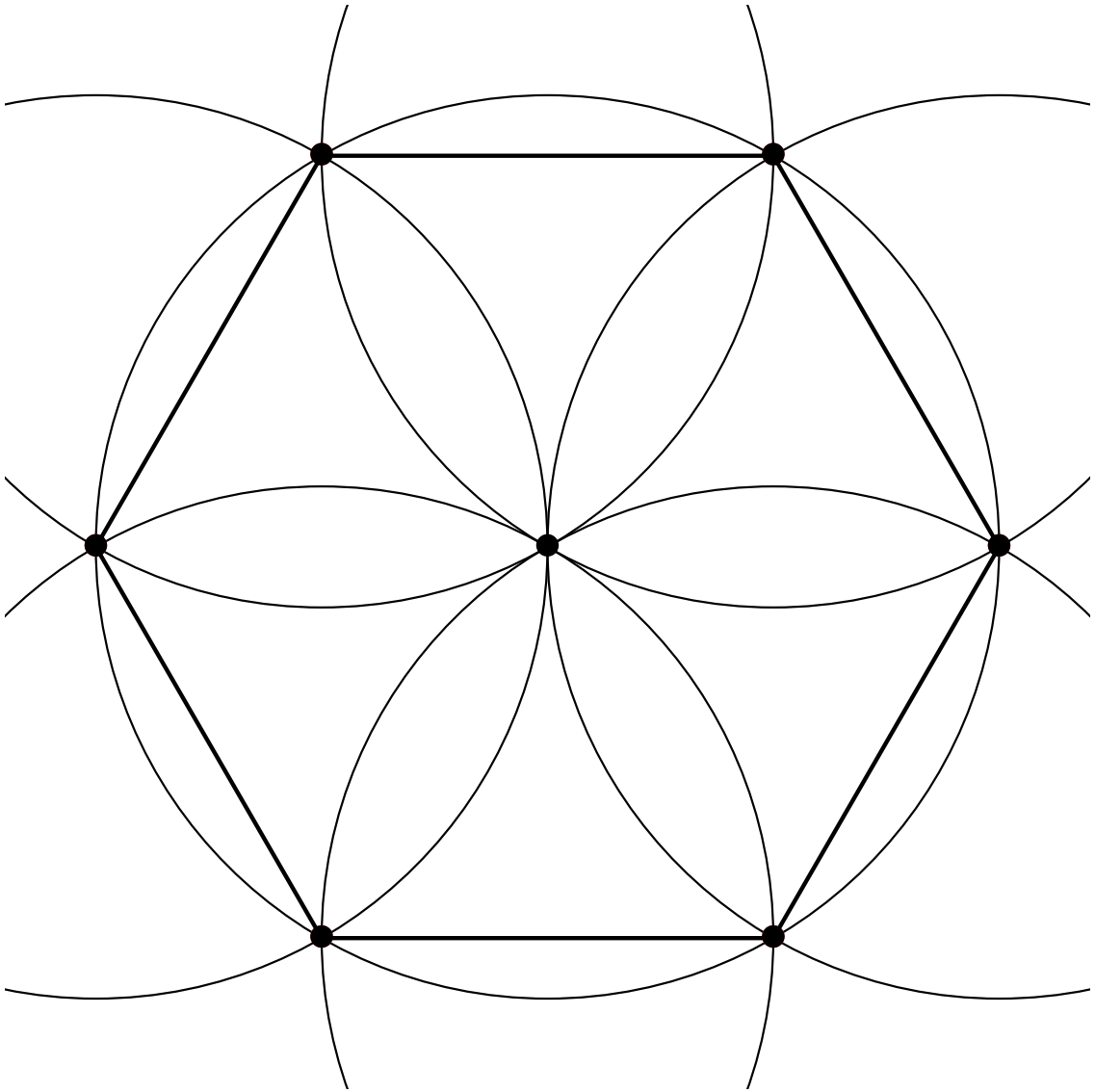
Soit K un corps.

Définition

Une extension de K est dite *quadratique* si elle est de degré 2.

Proposition

Si $\mathrm{car}(K) \neq 2$ et L/K est quadratique, il existe $\alpha \in L \setminus K$ tq $L = K(\alpha)$ et $\alpha^2 \in K$ (*i.e.* L s'obtient à partir de K par adjonction d'une racine carrée). Si $L = K(\beta)$ avec $\beta^2 \in K$, il existe $c \in K^\times$ tel que $\beta = c\alpha$.

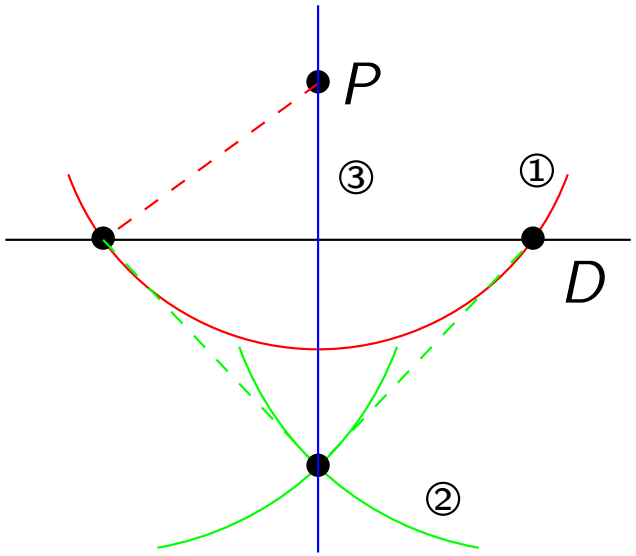


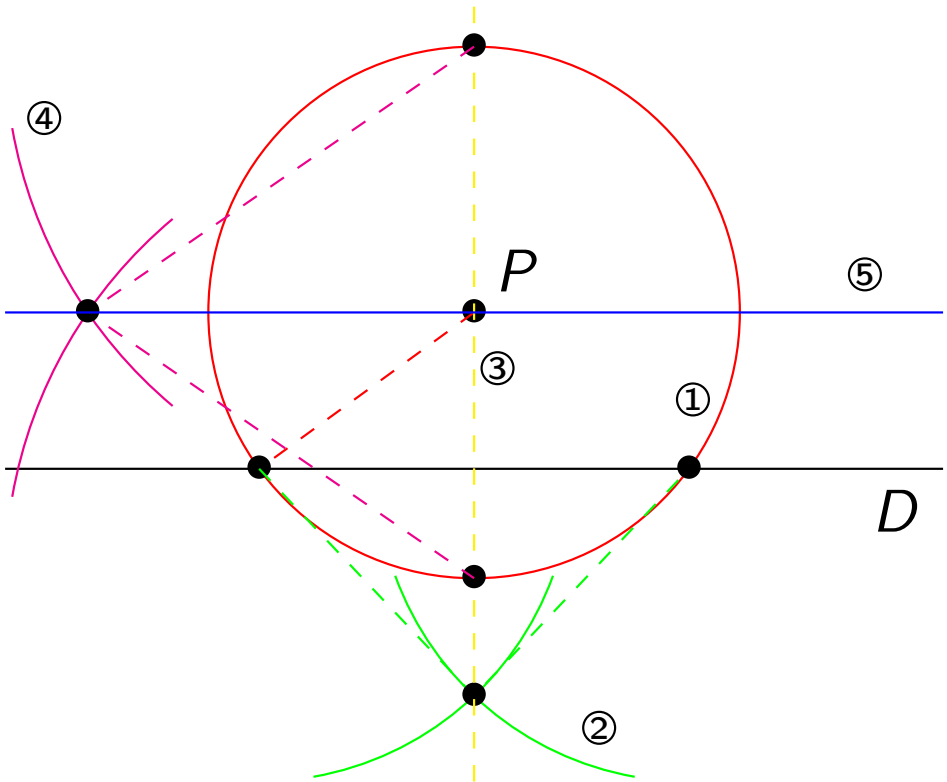
Application aux constructions à la règle et au compas

Soit $\mathscr{P}$ le plan affine euclidien. Étant donnés une droite Δ et deux points $P_0, P_1 \in \Delta$ distincts, quels sont les points $P \in \mathscr{P}$ qu'on peut construire avec une règle non graduée et un compas ? Il s'agit des points $P \in \mathscr{P}$ tels qu'il existe une suite $P_0, P_1, \ldots, P_{n-1}, P_n = P$ telle que pour tout $i \in \{2, \ldots, r\}$, le point P_i s'obtient à partir de $\mathcal{E}_i = \{P_0, P_1, \ldots, P_{i-1}\}$ en effectuant deux des opérations suivantes

(1) tracer une droite passant par deux points de $\mathcal{E}_i$;
(2) tracer un cercle centré en un point de $\mathcal{E}_i$ et passant par un point de $\mathcal{E}_i$;

et en prenant l'intersection des figures ainsi obtenues.
Si D est une droite et P un point (qui peut appartenir à D), on sait construire la perpendiculaire à D qui passe par P, et donc la projection de P sur D. En itérant cette opération, on sait construire la parallèle à D passant par P.


P
③
①
D
②

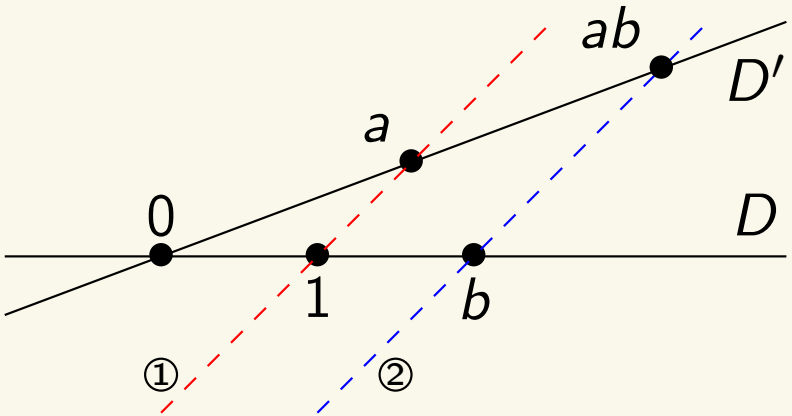

④
P
⑤
③
①
D
②

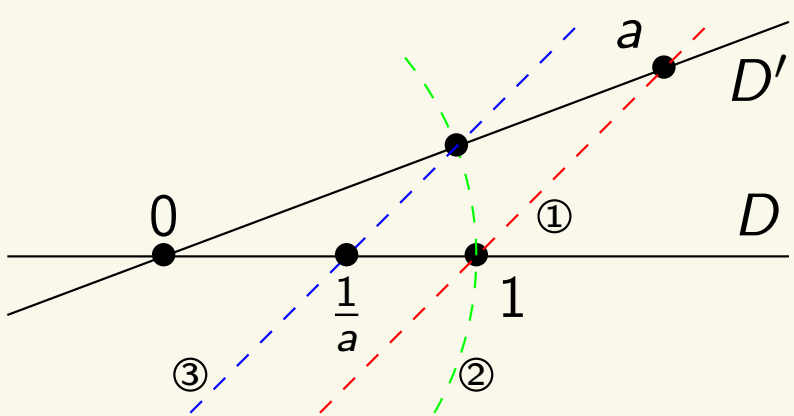
On peut construire la perpendiculaire Δ' à Δ passant par P_0. Cela donne un repère : si $P \in \mathscr{P}$, on peut construire ses projections sur Δ et Δ'. Cela permet de décrire les points constructibles par leurs coordonnées (la longueur P_0P_1 étant l'unité). Il s'agit de déterminer quels sont les nombres réels qui sont coordonnées de points constructibles. On appelle ces réels les *nombres constructibles*.

Proposition

L'ensemble des nombres constructibles est un sous-corps de $\mathbb{R}$.

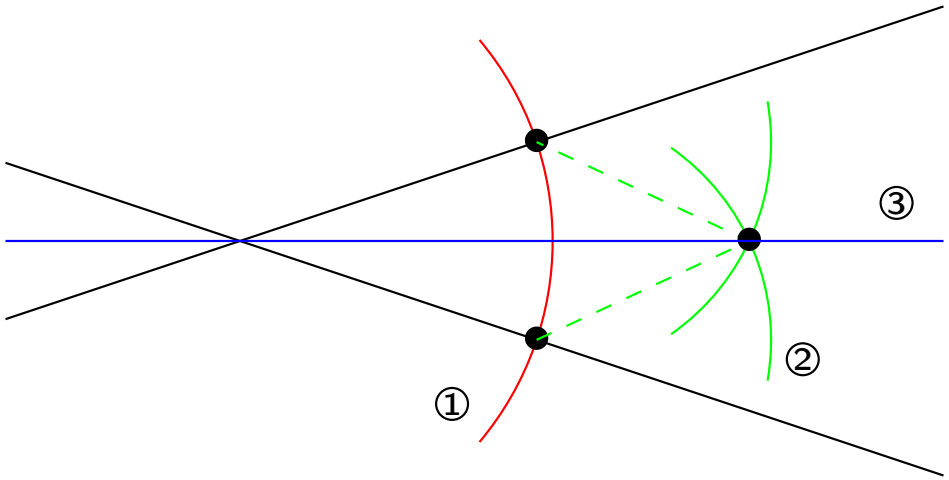
Démonstration





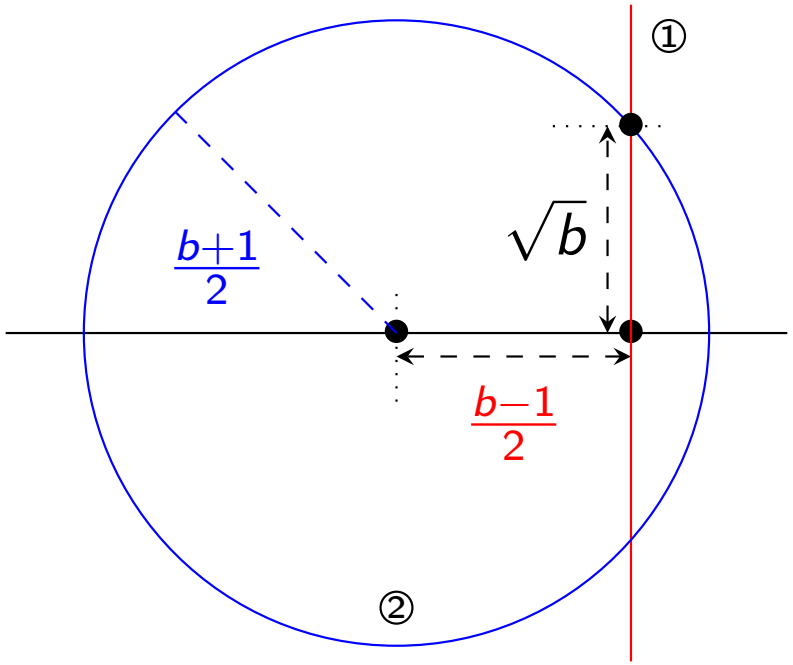
Extensions de corps

Rappelons qu'étant données deux droites de $\mathscr{P}$, leur bissectrice est constructible à la règle et au compas :



Proposition

Un élément $x \in \mathbb{R}$ est constructible si et seulement s'il existe un suite d'extensions $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_r$ telle que $x \in K_r$ et $[K_i : K_{i-1}] = 2$ pour tout $i \in \{1, \ldots, r\}$. En particulier, il est nécessaire (mais pas suffisant en général) que $[\mathbb{Q}(x) : \mathbb{Q}]$ soit une puissance de 2.


①
$\frac{b+1}{2}$
$\sqrt{b}$
$\frac{b-1}{2}$
②

Corollaire

Les problèmes suivants ne peuvent pas se résoudre à la règle et au compas :

(1) La quadrature du cercle (*i.e.* étant donné un cercle, construire un carré de même aire), ceci parce que π est transcendant.

(2) Doubler le volume d'un cube (*i.e.* étant donné un cube, construire un cuble de volume double -c'est dans l'espace et pas le plan-), ceci parce que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

(3) La trisection de l'angle (sauf pour des angles particuliers bien sûr). En effet, en vertu de la formule $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$, cela revient à construire une racine du polynôme $4X^3 - 3X - \alpha$ pour $\alpha \in \mathbb{R}$ constructible, mais cela définit des éléments de degré 3 sur $\mathbb{Q}(\alpha)$ en général.

Corollaire

Soit p un nombre premier impair. Pour que le polygône régulier à p côtés soit constructible, il faut que $p = 2^{2^r} + 1$ avec $r \in \mathbb{N}_{>0}$.

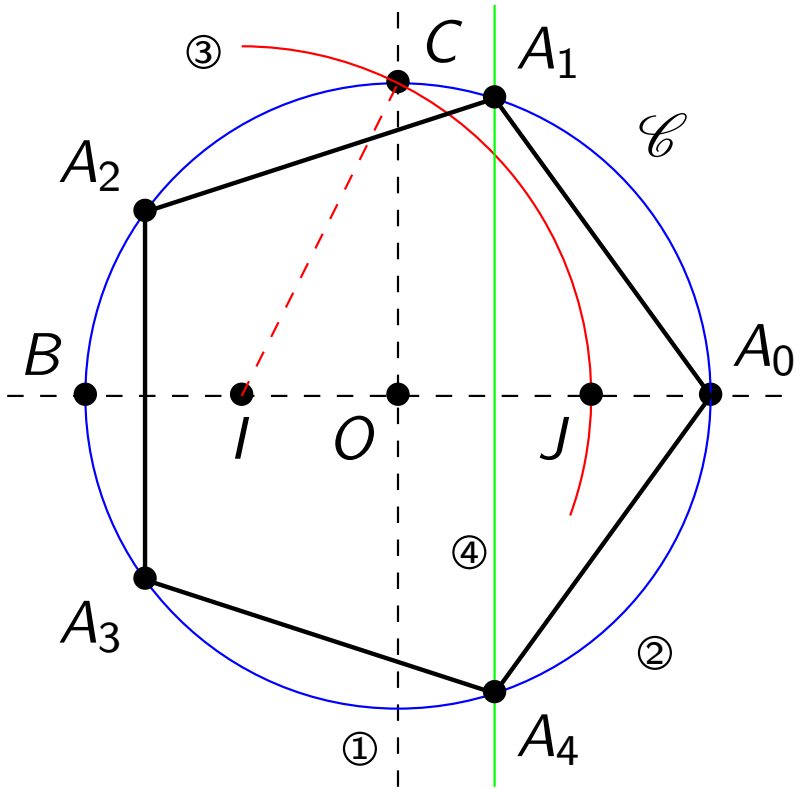
Remarque

On a montré que la condition est *nécessaire* : en fait elle est aussi suffisante. Pour $r = 0, 1, 2, 3$, on obtient les nombres premiers $3, 5, 17$ et 257 respectivement, qui correspondent à des polygônes constructibles. Pour 17, cela a été prouvé par Carl Friedrich Gauss en 1796 (à 19 ans).

Construction du pentagone (polygone à 5 côtés) d'après Ptolémée.

Posons $\zeta = e^{\frac{2i\pi}{5}}$. Il s'agit de construire $\zeta = \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right)$, *i.e.* le réel $\gamma := \cos\left(\frac{2\pi}{5}\right) = \frac{\zeta+\zeta^{-1}}{2}$. Comme $\zeta \neq 1$ et $(\zeta-1)(\zeta^4+\zeta^3+\zeta^2+\zeta+1) = \zeta^5 - 1 = 0$, on a $\zeta^4+\zeta^3+\zeta^2+\zeta+1 = 0$, d'où $\zeta^2+\zeta+1+\zeta^{-1}+\zeta^{-2} = 0$. On a $\gamma^2 = \frac{\zeta^2+2+\zeta^{-2}}{4}$, donc $4\gamma^2+2\gamma-1 = 0$, et γ est racine du polynôme $4X^2+2X-1$: on a $\gamma = \frac{\sqrt{5}-1}{4}$.

Soient O et A_0 deux points deux points distincts de $\mathscr{P}$. Construisons le pentagone régulier de centre O qui admet A_0 comme sommet. On prend (OA_0) comme axe des abscisses et longueur OA_0 comme unité. Il s'agit de construire A_1, A_2, A_3 et A_4 d'affixes respectives ζ, ζ^2, ζ^3 et ζ^4.



$$IC = \frac{\sqrt{5}}{2}$$
$$OJ = \frac{\sqrt{5}-1}{2} = 2\gamma$$

Remarques

(1) Tout point du plan constructible à la règle et au compas peut être construit en utilisant le compas seul (théorème de Mohr-Mascheroni).
(2) Tout point du plan constructible à la règle et au compas peut être construit à la règle seule à condition que soit donné un cercle et son centre (théorème de Poncelet-Steiner).

Exercice

Un polygone régulier à n côtés peut être construit à la règle et au compas si et seulement si n se décompose sous la forme $n = 2^k p_1 \cdots p_r$ où $k \in \mathbb{N}$ et $p_1, \ldots, p_r$ sont des nombres premiers de Fermat distincts.

Remarque : construction de l'heptadécagone

$$\cos\left(\frac{2\pi}{17}\right) = \frac{\sqrt{17}-1+\sqrt{2(17-\sqrt{17})}+\sqrt{2(\sqrt{17}+3)\left(2\sqrt{17}-\sqrt{2(17-\sqrt{17})}\right)}}{16}$$