Cadre : $\mathbb{K}$, $\mathbb{L}$, $\mathbb{M}$ sont des corps, tous les corps étudiés sont supposés commutatifs. Sauf indication contraire, p désigne un nombre premier. Sauf indication contraire, $n \in \mathbb{N}$

I - Notion d'extension

1 - Degré d'une extension

Déf 1 : On note que $\mathbb{L}$ est une extension (de corps) de $\mathbb{K}$ ou $\mathbb{K}$ est un sous-corps de $\mathbb{L}$. On note $\mathbb{K} \subset \mathbb{L}$

Ex 2 : $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$, $\mathbb{F}_2 \subset \mathbb{F}_4$

Prop 3 : Si $\mathbb{K} \subset \mathbb{L}$ alors $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel

Déf 4 : Si $\mathbb{K} \subset \mathbb{L}$ est une extension et que $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie, alors on appelle degré de $\mathbb{L}$ sur $\mathbb{K}$ le nombre $[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}}(\mathbb{L})$, et on dit alors que l'extension est finie. $[\mathbb{L} : \mathbb{K}]$

Prop 5 : Si $\mathbb{K}$ et $\mathbb{L}$ sont tous deux finis, alors $|\mathbb{L}| = |\mathbb{K}|^{[\mathbb{L} : \mathbb{K}]}$

Thm 6 : (Théorème de la base téléscopique)

Soient $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ des corps, soit $(e_i)_{i \in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j \in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors $(e_i f_j)_{(i,j) \in I \times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.

Si les extensions $\mathbb{K} \subset \mathbb{L}$ et $\mathbb{L} \subset \mathbb{M}$ sont finies, alors $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$

Ex 7 : $[\mathbb{C} : \mathbb{R}] = 2$

Ex : $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ donc $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] \times [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4$

2 - Extensions algébriques

Déf 8 : Soit $\mathbb{K} \subset \mathbb{L}$ un corps, A une partie de $\mathbb{L}$. On dit que A engendre $\mathbb{L}$ sur $\mathbb{K}$ si $\mathbb{L}$ est le plus petit sous-corps contenant $\mathbb{K}$ et A. On note $\mathbb{L} = \mathbb{K}(A)$

Ex 9 : $\mathbb{C} = \mathbb{R}(i)$

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, (a,b) \in \mathbb{Q}^2\}$

Déf 10 : (Eléments algébriques, transcendants)

Soit $\mathbb{K} \subset \mathbb{L}$ une extension, soit $x \in \mathbb{L}$, on dit que :

(i) x est algébrique sur $\mathbb{K}$ si $\exists P \in \mathbb{K}[X], P \neq 0 \quad P(x) = 0$

(ii) x est transcendant sur $\mathbb{K}$ si x n'est pas algébrique

Rq 11 : On peut interpréter cette définition en utilisant le morphisme d'évaluation en x : $\mathrm{ev}_x : \mathbb{K}[X] \to \mathbb{L}$, $P \mapsto P(x)$. Si x est transcendant sur $\mathbb{K}$ alors ev_x est injectif.

Déf 12 : (Polynôme minimal)

Soit $\mathbb{K} \subset \mathbb{L}$ une extension et soit $x \in \mathbb{L}$ un élément algébrique sur $\mathbb{K}$. Alors $\ker(\mathrm{ev}_x)$ est un idéal non nul de $\mathbb{K}[X]$, engendré par un unique polynôme unitaire de degré minimal, noté μ_x. On l'appelle le polynôme minimal de x sur $\mathbb{K}$. On a bien entendu $\mu_x \neq 0$

Ex 13 : (i) i est bien sûr algébrique sur $\mathbb{R}$ (pour $X^2 + 1$)

(ii) $\sqrt{2}$ est algébrique sur $\mathbb{Q}$, son polynôme minimal est $X^2 - 2$

Prop 14 : On a l'isomorphisme $\frac{\mathbb{K}[X]}{\langle \mu_x \rangle} \xrightarrow{\sim} \mathbb{K}[x] = \mathbb{K}(x)$. Ainsi x est algébrique

Rq 15 : Si x est algébrique, on a μ_x irréductible dans $\mathbb{K}[X]$, et on a $\deg(\mu_x) = [\mathbb{K}(x) : \mathbb{K}]$

Prop 16 : Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps et $x \in \mathbb{L}$. Alors x est algébrique sur $\mathbb{K}$ si $[\mathbb{K}(x) : \mathbb{K}] < +\infty$. Dans ce cas, une $\mathbb{K}$-base de $\mathbb{K}(x)$ est $\{1, x, \dots, x^{\deg(\mu_x)-1}\}$.

Ex 17 : $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(X^2 - 2) = 2$, une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2})$ est $\{1, \sqrt{2}\}$, $\mu_{\sqrt{2}} = X^2 - 2$

Déf 18 : Une extension $\mathbb{K} \subset \mathbb{L}$ est dite algébrique si $\forall x \in \mathbb{L}$, x est algébrique sur $\mathbb{K}$

Ex 19 : $\mathbb{R} \subset \mathbb{C}$ est une extension algébrique

Thm 20 : Si $\mathbb{K} \subset \mathbb{L}$ est une extension, alors $\mathbb{K}' = \{x \in \mathbb{L}, x \text{ est algébrique sur } \mathbb{K}\}$ est un sous-corps de $\mathbb{L}$, $\mathbb{K} \subset \mathbb{K}'$ est une extension algébrique

Ex 21 : $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ est une extension algébrique

II - Théorie des racines

1 - Corps de rupture, corps de décomposition

Déf 22 : (Corps de rupture)

Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ irréductible. Une extension $\mathbb{K} \subset \mathbb{L}$ est un corps de rupture de P sur $\mathbb{K}$ si $\exists x \in \mathbb{L}$, $P(x) = 0$ et $\mathbb{L} = \mathbb{K}(x)$

Ex 23 : $\mathbb{C}$ est le corps de rupture de $X^2 + 1 \in \mathbb{R}[X]$

Thm 24 : Soit $P \in \mathbb{K}[X]$, irréductible. Il existe un corps de rupture de P sur $\mathbb{K}$, unique à isomorphisme près

Déf 25 : (Corps de décomposition)
Soit $P \in \mathbb{K}[X]$ un polynôme de degré n. On appelle corps de décomposition de P sur $\mathbb{K}$ une extension $\mathbb{K} \subset \mathbb{L}$ telle que
(i) Dans $\mathbb{L}[X]$, P est scindé : $P = a\prod_{i=1}^{n}(X - x_i)$, $a \neq 0$, i.e. P a n racines dans $\mathbb{L}$
(ii) $\mathbb{L}$ est le plus petit corps vérifiant la propriété (i) : $\mathbb{L} = \mathbb{K}(x_1, \dots, x_n)$

Th 26 : Soit $P \in \mathbb{K}[X]$. Il existe un corps de décomposition de P sur $\mathbb{K}$ unique à isomorphisme près. On le note $D_{\mathbb{K}}(P)$. On a $[D_{\mathbb{K}}(P) : \mathbb{K}] \leq (\deg P)!$.
Ex 27 : (a) $D_{\mathbb{Q}}(X^2 - 2) = \mathbb{Q}(\sqrt{2})$
(b) $D_{\mathbb{Q}}(X^3 - 2) = \mathbb{Q}(\sqrt[3]{2}, j)$

2 - Clôture algébrique et fermeture algébrique

Déf 28 : (Corps algébriquement clos)
$\mathbb{K}$ est dit algébriquement clos si tout polynôme $P \in \mathbb{K}[X]$ admet ses racines dans $\mathbb{K}$.
Ex 29 : $\mathbb{C}$ est algébriquement clos
C-Ex 30 : $\mathbb{Q}$, $\mathbb{R}$ ne sont pas algébriquement clos, $X^2 + 1 = (X - i)(X + i)$, $i \notin \mathbb{Q}, \mathbb{R}$.
Déf 31 : (Clôture algébrique)
Une extension $\mathbb{K} \subset \mathbb{L}$ est une clôture algébrique si $\mathbb{L}$ vérifie
(i) $\mathbb{L}$ est algébriquement clos
(ii) $\mathbb{L}$ est algébrique sur $\mathbb{K}$
Ex 32 : $\mathbb{C}$ est clôture algébrique de $\mathbb{R}$, i ($\mathbb{C} = \mathbb{R}(i)$)

Déf 33 : (Extension algébriquement fermée)
Une extension $\mathbb{K} \subset \mathbb{L}$ est dite algébriquement fermée si tout $x \in \mathbb{L}$ algébrique sur $\mathbb{K}$ est dans $\mathbb{K}$.
Prop 34 : Soit $\mathbb{K} \subset \mathbb{L}$ une extension. $\mathbb{K}' = \{x \in \mathbb{L} \mid x \text{ algébrique sur } \mathbb{K}\}$ est algébriquement fermé dans $\mathbb{L}$. $\mathbb{K}'$ est appelée fermeture algébrique de $\mathbb{K}$ dans $\mathbb{L}$.
Th 35 : (Théorème de Steinitz, Admis)
Tout corps possède une clôture algébrique $\mathbb{L}$. Si $\mathbb{L}'$ est une autre clôture algébrique alors $\exists \varphi : \mathbb{L} \xrightarrow{\sim} \mathbb{L}'$ un isomorphisme de corps tel que $\varphi|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}}$.

Rq 36 : Si on veut on se donne un polynôme admettant une racine on peut toujours se placer dans une clôture algébrique du coup on parlera

III - Application

1 - Corps finis

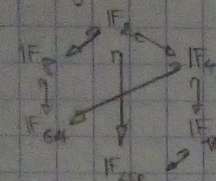
Déf 37 : (Caractéristique)
On définit la caractéristique d'un anneau A, notée $\mathrm{Car}(A)$ comme étant le plus grand entier d tel que $\ker(\varphi) = d\mathbb{Z}$, où $\varphi : \mathbb{Z} \to A$, $n \mapsto n \cdot 1_A$.
Prop 38 : Si A est intègre alors $\mathrm{Car}(A)$ est 0 ou un nombre premier.
Cor 39 : Ainsi $\mathrm{Car}(\mathbb{K})$ est infini ou est un nombre premier.
Déf 40 : Soit p un nombre premier. On définit le corps à p éléments, noté $\mathbb{F}_p$, par $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$, vu comme anneau $\mathbb{F}_p$ est donc de caractéristique p, nombre premier.
Th 41 : Soit $n \in \mathbb{N}$, soit $q = p^n$. Il existe un unique corps de cardinal q unique à isomorphisme près, noté $\mathbb{F}_q$. On peut l'obtenir comme corps de décomposition de $X^q - X \in \mathbb{F}_p[X]$.

Prop 42 : Soit $P \in \mathbb{F}_p[X]$ irréductible, de degré n. On a alors
$$\frac{\mathbb{F}_p[X]}{\langle P \rangle} \simeq \mathbb{F}_{p^n}$$
$\mathbb{F}_{p^n}$ est un $\mathbb{F}_p$-espace vectoriel de dimension $n = \deg(P)$. Si on note $\pi : \mathbb{F}_p[X] \to \frac{\mathbb{F}_p[X]}{\langle P \rangle}$, alors $\{1, \overline{0}^{\Gamma}, \dots, \overline{0}^{\Gamma^{n-1}}\}$ est une $\mathbb{F}_p$-base de $\mathbb{F}_{p^n}$, $\overline{Q} \mapsto Q$
Ex 43 : $\mathbb{F}_4 = \frac{\mathbb{F}_2[X]}{\langle X^2 + X + 1 \rangle}$, $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$ où $\alpha = \overline{X}^{\Gamma}$, $\alpha^2 + \alpha + 1 = 0$, i.e. $\alpha^2 = \alpha + 1$
Prop 44 : $\mathbb{F}_{p^n} = \{\text{Racines de } X^{p^n} - X\}$

Prop 45 : $\mathbb{F}_{p^{n_1}} \subset \mathbb{F}_{p^{n_2}}$ est une extension de corps si, et seulement si $n_1 \mid n_2$.

Rq 46 : Soit q le modèle de $\mathbb{F}_q$, on peut écrire $\mathbb{F}_{q^n}$, q étant une puissance de p ($q = p^{\alpha}$)

Ex 48 : On a les injections suivantes



$4 = 2^2$ $\quad 64 = 2^6$

$8 = 2^3$ $\quad 256 = 2^8$

$16 = 2^4$

$\hookrightarrow$ = Injection

Def 49 : (Fonction de Möbius) On définit la fonction de Möbius μ sur $\mathbb{N}$ par
(i) $\mu(1) = 1$ (ii) $\mu(p_1 \cdots p_r) = (-1)^r$ si $p_1, \dots, p_r$ sont premiers distincts
(iii) $\mu(n) = 0$ si n a un facteur premier de multiplicité au moins 2

Th 49 : (Comptage des polynômes irréductibles unitaires de $\mathbb{F}_q[X]$)
Soit $q = p^n$, $A(n,q) = \{$ Polynômes de $\mathbb{F}_q[X]$, irréductibles, unitaires de degré n $\}$
Soit $I(n,q) = \# A(n,q)$. On a alors :
(i) $X^{q^n} - X = \prod_{d \mid n} \prod_{P \in A(d,q)} P$
(ii) Si μ est la fonction de Möbius, alors $I(n,q) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$
(iii) On a l'équivalent $I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$

DVPT 1

2 - Corps cyclotomiques

Def 50 : (Racine n-ième primitive)
On définit les racines n-ièmes primitives de l'unité par l'ensemble
$\mu_n^\times = \{ e^{\frac{2ik\pi}{n}},\ k \wedge n = 1 \}$

Rq 51 : On a $\# \mu_n^\times = \varphi(n)$ (indicatrice d'Euler). $\mu_n^\times \simeq \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$

Ex 52 : $\mu_1^\times = \{1\}$, $\mu_2^\times = \{-1\}$, $\mu_3^\times = \{j, j^2\}$, $\mu_4^\times = \{i, -i\}$

Def 53 : (Polynôme cyclotomique)
On définit le n-ième polynôme cyclotomique par $\Phi_n(X) = \prod_{\zeta \in \mu_n^\times} (X - \zeta)$

Prop 54 : On a $\Phi_n \in \mathbb{Q}[X]$ et même $\Phi_n \in \mathbb{Z}[X]$

Prop 55 : $X^n - 1 = \prod_{d \mid n} \Phi_d$, et on retrouve la formule $n = \sum_{d \mid n} \varphi(d)$

Ex 56 : $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$

Th 57 : Φ_n est irréductible sur $\mathbb{Q}$

Cor 58 : Φ_n est le polynôme minimal de $\zeta \in \mu_n^\times$ sur $\mathbb{Q}$

Def 59 : (Corps cyclotomique)
On définit le corps cyclotomique par $\mathbb{Q}(\zeta) = \frac{\mathbb{Q}[X]}{\langle \Phi_n \rangle}$

Prop 60 : Une $\mathbb{Q}$-base de $\mathbb{Q}(\zeta)$ est $\{1, \zeta, \dots, \zeta^{\varphi(n)-1}\}$ et on a :
$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. C'est une extension de degré $\varphi(n)$

Th 61 : (Stabilité par tout automorphisme de corps cyclotomique)
Soit ζ une racine primitive n-ième de l'unité
$\{ x \in \mathbb{Q}(\zeta),\ \forall \sigma \in \mathrm{Aut}_{\mathrm{corps}}(\mathbb{Q}(\zeta)),\ \sigma(x) = x \} = \mathbb{Q}$

DVPT 2

3 - Constructibilité à la règle et au compas

Def 62 : (Extension quadratique)
Soit $\mathbb{K} \subset \mathbb{L}$ une extension, avec $\mathrm{Car}(\mathbb{K}) \neq 2$. On dit que $\mathbb{L}$ est une extension quadratique de $\mathbb{K}$ si $\exists x \in \mathbb{L} \setminus \mathbb{K} : x^2 \in \mathbb{K}$ et $\mathbb{L} = \mathbb{K}(x)$

Ex 63 : (i) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ est une extension quadratique
(ii) $\mathbb{R} \subset \mathbb{C}$ est une autre extension quadratique

C-Ex 64 : $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ n'est pas une extension quadratique

Def 65 : (Nombre constructible à la règle et au compas)
Un point $M \in \mathbb{R}^2$ est (constructible à la règle et au compas) à partir de $A \subset \mathbb{R}^2$ si $\exists M_0, \dots, M_n \in \mathbb{R}^2 : M = M_n$ et $\forall i \in [\![0, n]\!]$, M_i est l'intersection de deux éléments parmi une droite passant par deux points de $A \cup \{M_0, \dots, M_{i-1}\}$ ou un cercle centré en un point de $A \cup \{M_0, \dots, M_{i-1}\}$ et de rayon la distance entre deux points de cet ensemble. $x \in \mathbb{R}$ est constructible si $(x, 0)$ l'est.

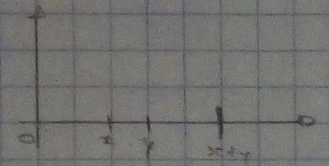
Ex 66 : Les $(0,n)$, $(n,0)$, $(x,0)$ $(x \in \mathbb{Q})$ sont constructibles à la règle et au compas. Si $x \geq 0$ est constructible, alors $\sqrt{x}$ l'est aussi (cf. Annexe)
Si x, y sont constructibles alors $x + y$ et xy l'est aussi.

Th 67 : Soit $x \in \mathbb{R}$ constructible. Alors $[\mathbb{Q}(x) : \mathbb{Q}]$ est une puissance de 2
$\mathbb{Q} \subset \dots \subset \mathbb{Q}(x)$ est une suite d'extensions quadratiques

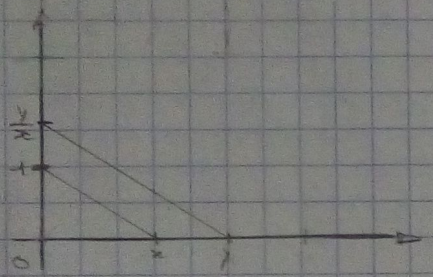
Appli 68 : (Deux problèmes anciens)
(i) La duplication du cube est impossible : $\sqrt[3]{2}$ est non constructible
(ii) La trisection de l'angle est impossible, $\cos\left(\frac{\pi}{9}\right)$ est non constructible

Prop 69 : (Construction de polygones réguliers)
Le pentagone est constructible à la règle et au compas, mais pas l'heptagone ou le nonagone

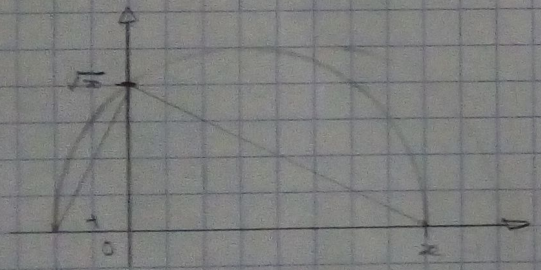
Annexe : Constructibilité à la règle et au compas



Constructibilité d'une somme / différence



Constructibilité d'une multiplication / division



Constructibilité d'une racine carrée

Rq : le cercle est constructible