1 Recasages

- **121 :** Nombres premiers. Applications.
- **122 :** Anneaux principaux. Exemples et applications.
- **127 :** Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications.
- **144 :** Racines d'un polynôme. Fonctions symétriques élémentaires. Applications.
- **191 :** Exemples d'utilisation de techniques d'algèbres en géométrie.

2 Résultats préliminaires

Théorème :

L'ensemble des nombres complexes constructibles est un sous corps de $\mathbb{C}$ stable par racine carrée.

Preuve :

Par constructions élémentaires à la règle et au compas, savoir construire une somme, un produit, etc...

Théorème de Wantzel :

Soit $z \in \mathbb{C}$, z est constructible si et seulement si il existe $p \geq 1$ et une suite de sous-corps $(L_j)_{1\leq j\leq p}$ de $\mathbb{C}$ tels que :

- $L_1 = \mathbb{Q}$
- $\forall 1 \leq j \leq p-1, L_j \subset L_{j+1}$ et $[L_{j+1} : L_j] = 2$
- $z \in L_p$

Preuve :

- Si z est constructible, on note M un point ayant z pour affixe. M s'obtient à l'aide d'un nombre fini de constructions de points $M_1, \dots, M_p$ avec $M_i(x_i, y_i)$. On obtient alors une tour d'extension :

$$K_0 \subset K_1 \subset \cdots \subset K_p \quad \text{avec} \quad K_{i+1} = K_i(x_i, y_i)$$

  Pour montrer que $[K_{i+1} : K_i] \leq 2$, on considère les différents cas possibles selon si M_i est l'intersection de deux droites, deux cercles ou d'une droite et d'un cercle. On conclut alors en considérant uniquement une suite de sous corps (L_i) strictement croissante pour l'inclusion.

- Réciproquement, on montre par récurrence qu'en considérant cette tour d'extension quadratique, on a que tous les sous-corps L_i sont inclus dans l'ensemble des nombres constructibles. L'hérédité repose sur le théorème précédent.

Corollaire :

Tout nombre constructible est algébrique et son degré est une puissance de 2.

Preuve :

Résultat immédiat d'après le théorème précédent car :

$$[L_p : \mathbb{Q}] = 2^p = [L_p : \mathbb{Q}(z)][\mathbb{Q}(z) : \mathbb{Q}]$$

Lemme :

$\forall q \in \mathbb{N}, 2^q + 1$ est premier $\implies$ q est une puissance de 2.

Preuve :

Supposons que q ne soit pas une puissance de 2 et donc que $q = (2a+1)2^b$ avec $a, b \in \mathbb{N}$.
On a :

$$2^q + 1 = (2^{2^b})^{2q+1} - (-1)^{2q+1} = (2^{2^b} + 1)\sum_{i=0}^{2q}(-1)^i(2^{2^b})^{2a-i}$$

Donc $2^q + 1$ est divisible par $2^{2^b} + 1$ donc n'est pas premier, donc q est une puissance de 2.

Lemme :

Si $m \wedge n = 1$, $e^{i\frac{2\pi}{mn}}$ est constructible si et seulement si $e^{i\frac{2\pi}{m}}$ et $e^{i\frac{2\pi}{n}}$ sont constructibles

Preuve :

- On a $e^{i\frac{2\pi}{n}} = \left(e^{i\frac{2\pi}{mn}}\right)^m$ donc est construtible. De même pour $e^{i\frac{2\pi}{m}}$.
- On a :

$$m \wedge n = 1 \implies \exists \lambda, \mu \in \mathbb{Z}, \lambda n + \mu m = 1 \implies \frac{\lambda}{m} + \frac{\mu}{n} = \frac{1}{mn}$$

D'où :

$$e^{i\frac{2\pi}{mn}} = e^{i2\pi(\frac{\lambda}{m}+\frac{\mu}{n})}$$

Donc est construtible.

3 Développement

Théorème :

Si p est un nombre premier supérieur ou égal à 3, le polygone à p^α côtés est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat.

Preuve :

- Supposons que $e^{\frac{2i\pi}{p^\alpha}}$ est constructible, on a donc que $\cos\frac{2i\pi}{p^\alpha}$ est constructible.
  - D'après le théorème de Wantzel, on a $[\mathbb{Q}(\cos\frac{2i\pi}{p^\alpha}) : \mathbb{Q}] = 2^m$.
  - En notant $q = p^\alpha$ et $\omega = e^{\frac{2i\pi}{q}}$ racine unité de $X^q - 1$, on a : $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(q) = p^{\alpha-1}(p-1)$.
  - Par ailleurs, $\omega^2 - 2\omega\cos\frac{2i\pi}{p^\alpha} + 1 = 0$ d'où ω est algébrique et de degré 2 sur $\mathbb{Q}(\cos\frac{2i\pi}{p^\alpha})$. D'où $[\mathbb{Q}(\omega) : \mathbb{Q}(\cos\frac{2i\pi}{p^\alpha})] = 2$.

  D'où $2^{m+1} = p^{\alpha-1}(p-1) \implies \alpha = 1$ et $p = 1 + 2^{m+1}$.
  p est bien un nombre premier de Fermat d'après le premier lemme préliminaire.
- Soit $p = 2^N + 1$ un nombre premier de Fermat. On veut montrer que le polygone a p côtés est constructible. On cherche donc à appliquer la réciproque du théorème de Wantzel.
  - Soit $K = \mathbb{Q}(\omega)$, $\phi_p(X) = X^{p-1} + \cdots + X + 1$ est le polynôme minimal de ω. On a donc $[K : \mathbb{Q}] = p - 1 = 2^N$ et $\mathcal{B} = (1, \omega, \ldots, \omega^{p-2})$ est une base de K sur $\mathbb{Q}$.
  - Soit $G = \mathrm{Gal}_{\mathbb{Q}}(K/\mathbb{Q}) = \mathrm{Aut}(K)$. $(G, \circ)$ est un groupe, on détermine les éléments de G.

    Soit $g \in G$, g est entièrement déterminé par $g(\omega)$ car g est $\mathbb{Q}$-linéaire.
    De plus, on a :

$$\phi_p(\omega) = \omega^{p-1} + \cdots + \omega + 1 = 0 \implies g(\omega)^{p-1} + \cdots + g(\omega) + 1 = 0$$

    Les valeurs de $g(\omega)$ sont les racines de ϕ_p qui sont les $\omega, \ldots, \omega^{p-1}$, on définit alors $g_k(\omega) = \omega^k$.
    On a donc $G = \{\underbrace{g_1}_{=1_K}, g_2, \ldots, g_{p-1}\}$ d'ordre $p-1$.
  - Soit $(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{1}, \ldots, \overline{p-1}\}$. On définit $\psi : \begin{cases} G & \to & (\mathbb{Z}/p\mathbb{Z})^\times \\ g_k & \mapsto & \overline{k} \end{cases}$ qui est un isomorphisme de groupes.
    Or $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique donc G aussi d'où $G =< g >$.
    On a donc que $\mathcal{B} = (g^k(\omega))_{0\le k\le p-2}$ est une base de K sur $\mathbb{Q}$ d'ordre 2^N.
  - On définit $G_i =< g^{2^i} >$.
    g est d'ordre 2^N donc g^{2^i} est d'orde 2^{N-i} c'est-à-dire que G_i est un groupe d'ordre 2^{N-i}. D'où :

$$G = G_0 \supset G_1 \supset \cdots \supset G_N = \{1_K\}$$

    On pose $K_i = \{z \in K, g^{2^i}(z) = z\}$ un sous-corps de K.
    On a $K_i \subset K_{i+1}$ car $g^{2^{i+1}} = \left(g^{2^i}\right)^2$ d'où :

$$K_0 \subset \cdots \subset K_N = K$$

  - Montrons que $K_0 = \mathbb{Q}$, on a déjà $\mathbb{Q} \subset K_0 = \{z \in K, g(z) = z\}$.

    Soit $z \in K_0$, on a dans la base $\mathcal{B}$:

$$z = \lambda_0\omega + \cdots + \lambda_{p-3}g^{p-3}(\omega) + \lambda_{p-2}g^{p-2}(\omega)$$

    D'où :

$$g(z) = z = \lambda_0 g(\omega) + \cdots + \lambda_{p-3}g^{p-2}(\omega) + \lambda_{p-2}\omega$$

    Et donc :

$$z = \lambda_0(\omega + \cdots + g^{p-2}(\omega)) = \lambda_0(\omega + \cdots + \omega^{p-1}) = -\lambda_0 \in \mathbb{Q}$$

  - Montrons que les inclusions entre les sous-corps sont strictes. Il suffit de trouver un $z \in K_{i+1}$ et $z \notin K_i$. C'est-à-dire tel que :

$$g^{2^{i+1}}(z) = z \quad \text{mais} \quad g^{2^i}(z) \neq z$$

Posons :

$$z = \omega + g^{2^{i+1}}(\omega) + g^{2^{i+2}}(\omega) + \cdots + g^{2^i(2^{N-i-1}-1)}(\omega)$$

On a bien $g^{2^{i+1}}(z) = z$ mais $g^{2^i}(z) \neq z$ par unicité de l'écriture de z dans $\mathcal{B}$.

– Montrons que $K_{N-1} = \mathbb{Q}(\cos\frac{2\pi}{p})$.
$K_{N-1} = \{z \in K, f(z) = z\}$ avec $f = g^{2^{N-1}}$.
Posons $f(\omega) = \omega^\lambda$.
On a $f^2 = 1_K$ d'où $\omega = f^2(\omega) = \omega^{\lambda^2}$.
On a donc :

$$\omega^{\lambda^2-1} = 1 \implies p|\lambda^2 - 1 \implies \overline{\lambda^2} - \overline{1} = \overline{0} \text{ dans } \mathbb{Z}/p\mathbb{Z}$$

On a donc nécessairement $\overline{\lambda} = -\overline{1}$ et donc $f(\omega) = \omega^{-1}$.

On a donc :

$$f\left(\cos\frac{2\pi}{p}\right) = f\left(\frac{\omega+\omega^{-1}}{2}\right) = \frac{f(\omega)+f(\omega)^{-1}}{2} = \frac{\omega^{-1}+\omega}{2} = \cos\frac{2\pi}{p}$$

On a donc $\cos\frac{2\pi}{p} \in K_{N-1}$ et $\mathbb{Q}(\cos\frac{2\pi}{2}) \subset K_{N-1} \subsetneq K_N = K$.
On a donc :

$$\left[K : \mathbb{Q}\left(\cos\frac{2\pi}{p}\right)\right] = 2 \implies [K : K_{N-1}] = 2 \implies K_{N-1} = \mathbb{Q}\left(\cos\frac{2\pi}{p}\right)$$

– On a :

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_{N-1} \subsetneq K_N = \mathbb{Q}(\omega)$$

On a :

$$2^N = p - 1 = [K : K_0] = [K : K_{N-1}] \dots [K_1 : K_0]$$

Il y a N facteurs distincts car les corps sont distincts donc chaque facteur est égal à 2, d'où $[K_{i+1} : K_i] = 2$.

Donc, d'après le théorème de Wantzel, $\cos\frac{2\pi}{p}$ est constructible, donc $e^{\frac{2i\pi}{p}}$ aussi. Donc le polygone à p côtés aussi.

4 Compléments

- $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^k)$ pour $k \wedge n = 1$.
On a qu'il existe $\lambda, \mu \in \mathbb{Z}$ tels que $\lambda k + \mu n = 1$ d'où $\omega = \omega^{\lambda k+\mu n} = (\omega^k)^\lambda$.
D'où le résultat.

- ψ est bien un isomorphisme car $\psi(g_k) = \overline{1} \implies g_k = id_k$ d'où l'injectivité et $|G| = |(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$ car l'extension est galoisienne (car normale séparable). d4où la bijectivité de ψ.
On a également $g_k \circ g_{k'}(\omega) = g_k(\omega^{k'}) = \omega^{kk'}$ d'où le morphisme.

- Savoir démontrer que ϕ_p est irréductible sur $\mathbb{Q}[X]$ (c.f. développement critère d'Eisenstein).

- Plus généralement, le polygône régulier à n côtés est constructible si et seuelement si il existe $\alpha \in \mathbb{N}$ et $p_1, \dots, p_r$ nombres premiers de Fermat et distincts tels que $n = 2^\alpha p_1 \dots p_r$.
Ceci vient immédiatement car le produit de 2 nombres construtibles est constructible et est bien de cette forme là par unicité de la décomposition en facteurs premiers et d'après le théorème précédent.

- Construction du pentagone :
On a $\omega = e^{i\frac{2\pi}{5}}$ qui est solution de $x^4 + x^3 + x^2 + x + 1 = 0$. On pose $y = x + \frac{1}{x} = 2\cos\left(\frac{2\pi}{5}\right)$ qui est solution de $y^2 + y - 1 = 0$. On en déduit donc la valeur souhaitée (constructible).

5 Références

- Théorie des corps, *Carrega*
- Théorie de Galois, *Gozard*