Leçon 127 : Exemples de nombres remarquables ; exemples d'anneaux de nombres remarquables. Applications.

Références : Duvernet, Perrin, Gozard, Rombaldi (Ana réelle), Rombaldi (Alg. géom.)

I - Nombres constructibles

1) Nombres rationnels, nombres irrationnels remarquables

2) Nombres décimaux

3) Nombres premiers, nombres de Carmichael

4) Carrés dans les corps finis

II - Corps de nombres algébriques et sous-corps de nombres constructibles

1) Nombres algébriques et transcendants

2) Constructions géométriques à la règle et au compas

III - Anneaux de nombres de la forme $\mathbb{Z}[\omega]$

1) Un exemple d'anneau non factoriel : $\mathbb{Z}[i\sqrt{5}]$

2) L'anneau $\mathbb{Z}[i]$ et le problème des deux carrés

DEV 1 : Théorème de Korselt

DEV 2 : $\mathbb{Z}[i]$ et le problème des deux carrés

Leçon 127 : Exemples de nombres remarquables, exemples d'anneaux de nombres remarquables. Applications.

I - Nombres remarquables

1) Nombres rationnels, nombres irrationnels [Rat] [DUV]

DEF1 : On définit $\mathbb{Q}$ le corps des rationnels comme le corps des fractions de $\mathbb{Z}$.

REM2 : $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. $\mathbb{Q}$ est le plus petit corps de caractéristique nulle à isomorphisme près.

DEF3 : Un nombre irrationnel est un élément de $\mathbb{R} \setminus \mathbb{Q}$.

THM4 : Soit $d \in \mathbb{N}$ qui n'est pas un carré parfait. Alors $\sqrt{d}$ est irrationnel.

EX5 : $\sqrt{2}$ est irrationnel et donc X^2-2 est irréductible sur $\mathbb{Q}$.

THM5 : e est irrationnel
THM6 : π est irrationnel.
} on raisonne par l'absurde et on aboutit à une suite d'entiers strictement positifs qui tend vers 0.

2) Nombres décimaux [Rat] (Ana)

DEF7 : On définit $\mathbb{D} = \left\{ \frac{a}{10^m} \mid a \in \mathbb{Z}, m \in \mathbb{N} \right\}$

PROP8 : $\mathbb{D}$ est un anneau commutatif unitaire mais n'est pas un corps : $\mathbb{D}^\times = \{ r = \pm 2^\alpha 5^\beta \mid (\alpha, \beta) \in \mathbb{Z}^2 \}$.

THM9 : L'ensemble $\mathbb{R}$ est archimédien :
$\forall (a,b) \in \mathbb{R}_+^* \times \mathbb{R}^+, \exists n \in \mathbb{N}^*, na > b$

THM10 : $\forall x \in \mathbb{R}, \exists ! n \in \mathbb{N}, n \leq x < n+1$

DEF11 : L'entier n du THM10 est appelé partie entière de x et notée $\lfloor x \rfloor$.

A tout réel x, on associe les suites $(r_n)_{n\in\mathbb{N}}$ et $(s_n)_{n\in\mathbb{N}}$ définies par : $\forall n \in \mathbb{N}, r_n = \frac{\lfloor 10^n x \rfloor}{10^n}$ et $s_n = r_n + \frac{1}{10^n}$.

THM12 : Les suites (r_n), (s_n) sont des suites adjacentes de nombres décimaux qui convergent vers x avec $r_n \leq x < s_n \ \forall n$.

COR13 : Les ensembles $\mathbb{D}$ et $\mathbb{Q}$ sont denses dans $\mathbb{R}$.

COR14 : $\mathbb{R} \setminus \mathbb{Q}$ est dense dans $\mathbb{R}$.

DEF15 : A tout réel x, on associe les suites $(r_n)_{n\in\mathbb{N}}$ et $(a_n)_{n\in\mathbb{N}}$ définie par $\begin{cases} a_0 = \lfloor x \rfloor \\ \forall n \in \mathbb{N}^*, a_n = \lfloor 10^n x \rfloor - 10 \lfloor 10^{n-1} x \rfloor \end{cases}$

On a $a_n = 10^n (r_n - r_{n-1})$ et $a_n \in [\![0;9]\!]$

THM16 : $\forall n \in \mathbb{N}, \sum_{k=0}^{n} \frac{a_k}{10^k} = r_n$ donc :
$\forall x \in \mathbb{R}, x = \sum_{k=0}^{+\infty} \frac{a_k}{10^k}$.

LEMME17 : $\forall x \in \mathbb{R}$, $(a_n)_{n\in\mathbb{N}}$ ne peut être stationnaire à 9.

DEF18 : On appelle développement décimal illimité propre (DDIP) de $x \in \mathbb{R}$ toute égalité $x = \sum_{k=0}^{+\infty} \frac{a_k}{10^k}$ où $(a_n)_{n\in\mathbb{N}} \in \mathcal{D}'$ où $\mathcal{D}' = \{$suite d'entiers entre 0 et 9, $a_0 \in \mathbb{N}$, (a_n) non stationnaire à 9$\}$

THM19 : Le DDIP d'un réel est unique.

COR20 : $\mathbb{R}$ est non dénombrable.

THM21 : $x \in \mathbb{R}_+^*$ est décimal si et seulement si son DDIP est fini

DEF22 : On dit que le DDIP de $x \in \mathbb{R}$ est périodique lorsqu'il existe $p \geq 0$ et $q \geq 1$ tels que $x = a_0, a_1 \dots a_p b_1 \dots b_q b_1 \dots b_q$

THM23 : $x \in \mathbb{R}^+$ est rationnel si et seulement si son DDIP est périodique.

3) Nombres premiers et nombres de Carmichael [Rom] (Alg.)

DEF24 : On dit que $p \in \mathbb{N}$ est premier lorsque $p \geq 2$ et lorsque ses seuls diviseurs positifs sont 1 et p.

EX25 : Les nombres de Fermat sont les entiers de la forme $2^{2^n}+1$. Ils sont premiers pour $n \in [\![0;4]\!]$ et pas pour $n \in [\![5;32]\!]$.

THM26 (Euclide) Tout entier relatif $n \in \mathbb{Z} \setminus \{-1;0;1\}$ a au moins un diviseur premier

THM27 : Tout entier $n \geq 2$ non premier a au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$

THM28 : L'ensemble des nombres premiers est infini

THM 29 : Tout entier naturel $n \geq 2$ se décompose de manière unique sous la forme $n = q_1^{\alpha_1} \cdots q_r^{\alpha_r}$ où $2 \leq q_1 < \cdots < q_r$ sont des nombres premiers et $\alpha_k \in \mathbb{N}^*$.

THM 30 : (Fermat) Pour p premier et $a \in \mathbb{N}$, On a $a^{p-1} \equiv 1 \mod p$.

DEF 31 : On appelle nombre de Carmichael tout entier $n \geq 3$ non premier tel que $a^{n-1} \equiv 1 \mod n$ pour tout a premier avec n.

DEV 1

LEMME 32 : Un nombre de Carmichael est impair.

LEMME 33 : Un nombre de Carmichael est sans facteur carré.

THM 34 : (Korselt) Soit $n \geq 3$ un entier. LASSE :

1) $\exists r \geq 3$, $\exists 3 \leq p_1 < \cdots < p_r$ tel que $n = \prod_{j=1}^{r} p_j$ et pour tout $j \in [1;r]$, $p_j - 1 \mid n-1$.
2) n n'est pas premier et : $\forall x \in \mathbb{Z}/n\mathbb{Z}$, $x^n = x$
3) n est un nombre de Carmichael.

4) Carrés dans un corps fini [PER] [DUV]

Si p est premier, on pose $q = p^n$ $(n \geq 1)$. On suppose connue l'existence et l'unicité de $\mathbb{F}_q$.

DEF 35 : On pose $\mathbb{F}_q^2 = \{x^2 / x \in \mathbb{F}_q\}$ et $(\mathbb{F}_q^*)^2 = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

PROP 36 : • Pour $p = 2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$

• Pour $p > 2$, $\# \mathbb{F}_q^2 = \frac{q+1}{2}$ et $\#(\mathbb{F}_q^*)^2 = \frac{q-1}{2}$

PROP 37 : On suppose $p > 2$. $x \in (\mathbb{F}_q^*)^2 \Leftrightarrow x^{\frac{q-1}{2}} = 1$

COR 38 : Soit p premier, $p > 2$. On pose $q = p^n$, $n \in \mathbb{N}^*$

-1 est un carré dans $\mathbb{F}_q \Leftrightarrow q \equiv 1 \mod 4$

REM 39 : On utilise ce résultat dans la preuve du théorème des deux carrés.

II - Corps des nombres algébriques et sous-corps des nombres constructibles

1) Corps des nombres algébriques

DEF 40 : Soit L/K une extension et $\alpha \in L$. Soit $\varphi : K[T] \to L$, $P \mapsto P(\alpha)$

• Si φ est injectif, on dit que α est transcendant sur K.

• Sinon, on dit que α est algébrique sur K. $I = \ker(\varphi)$ est principal engendré par π_α unitaire qu'on appelle polynôme minimal de α sur K.

THM 41 : Soit L/K une extension et $\alpha \in L$. LASSE :

1) α est algébrique sur K
2) $K[\alpha] = K(\alpha)$
3) $\dim_K K[\alpha] < \infty$

THM 42 : Soit L/K une extension. On pose $M = \{x \in L / x \text{ algébrique sur } K\}$. Alors M est un sous-corps de L.

EX 43 : Les nombres $\sqrt{2}$; i ; $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$.

DEF 44 : L/K est dite algébrique lorsque tout $\alpha \in L$ est algébrique sur K.

PROP 45 : Soit $A = \{\alpha \in \mathbb{C} \mid \alpha \text{ algébrique sur } \mathbb{Q}\}$. A est un corps algébrique mais $A/\mathbb{Q}$ n'est pas finie.

THM 46 : (Liouville) Soit $\alpha \in \mathbb{R}$ nombre algébrique de degré $d \geq 2$. Soit $k \in \mathbb{N}$ tel que $P = k\pi_\alpha \in \mathbb{Z}[X]$. On pose $C' = \max_{x \in [\alpha-1;\alpha+1]} |P'(x)|$ et $C = \min(C', \frac{1}{C'})$. Alors pour tout $\frac{p}{q} \in \mathbb{Q}$ avec $q > 0$, $|\alpha - \frac{p}{q}| \geq \frac{C}{q^d}$.

DEF 47 : On dit que $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ est un nombre de Liouville lorsque pour tout n assez grand, il existe $\frac{p}{q} \in \mathbb{Q}$ $(q \geq 2)$ tel que $|\alpha - \frac{p}{q}| < \frac{1}{q^n}$.

THM 48 : Tout nombre de Liouville est transcendant

APPLI 49 : Le nombre $\alpha = \sum_{k=0}^{+\infty} \frac{1}{10^{k!}}$ est transcendant

THM 50 : (Hermite-Lindemann ADMIS) Soit a un nombre algébrique non nul, alors e^a est transcendant

COR 51 : e et π sont transcendants.

α) Constructions géométriques à la règle et au compas

Soit P un plan affine euclidien orienté. $R=(O,\vec{i},\vec{j})$ un repère orthonormé direct.

DEF 52: Soit $X\subset P$, $\#X\geq 2$. On dit que $M\in P$ est constructible en un pas à partir de X lorsque M est intersection soit de deux droites, soit de deux cercles, soit d'une droite et d'un cercle.

PROP 53: On peut construire les milieux des segments, les perpendiculaires et les parallèles passant par un point

PROP 54: Soit $x\in\mathbb{R}$. $(x,0)$ est constructible $\Leftrightarrow$ $(0,x)$ l'est. Lorsque c'est le cas, on dit que x est constructible.

PROP 55: Tout élément de $\mathbb{Q}$ est constructible

PROP 56: $M=(x,y)$ est constructible $\Leftrightarrow$ x,y le sont.

THM 57. L'ensemble $\mathbb{E}$ des nombres réels constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.

THM 58: (Wantzel) Soit $t\in\mathbb{R}$. t est constructible si et seulement si il existe une suite finie $(L_0,\dots,L_p)$ de sous-corps de $\mathbb{R}$ vérifiant

- $L_0=\mathbb{Q}$
- $\forall i\in[\![0,p-1]\!]$, $[L_{i+1}:L_i]=2$
- $t\in L_p$.

COR 59: Soit $x\in\mathbb{R}$. Si x est constructible, il existe $e\in\mathbb{N}$ tel que $[\mathbb{Q}(x):\mathbb{Q}]=2^e$.

COR 60: Tout nombre constructible est algébrique

APPLI 61: On peut répondre à quelques problèmes de géométrie historiquement célèbres:

- L'impossibilité de la quadrature du cercle
- L'impossibilité de la duplication du cube.

III - Anneaux de nombres algébriques de la forme $\mathbb{Z}[\omega]$

Dans toute cette partie, N désignera la norme : $N: z\in\mathbb{Z}[\omega]\mapsto z\bar{z}\in\mathbb{N}$ vérifie: N est multiplicative ; $N(zz')=N(z)N(z')$. $N(z)>0$ $\forall z\neq 0$.

1) $\mathbb{Z}[i\sqrt{5}]$: un exemple d'anneau intègre non factoriel

PROP 62: Soit $a\in\mathbb{Z}[i\sqrt{5}]$. $N(a)=1\Leftrightarrow a\in\{-1;1\}$. On en déduit que $\mathbb{Z}[i\sqrt{5}]^\times=\{-1;1\}$.

PROP 63: Les éléments $2,3,1+i\sqrt{5},1-i\sqrt{5}$ sont irréductibles dans $\mathbb{Z}[i\sqrt{5}]$ et $1+i\sqrt{5}$ n'est associé ni à 2 ni à 3.

COR 64: $6=2\times 3=(1+i\sqrt{5})(1-i\sqrt{5})$ donc $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

PROP 65: 2 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$ non premier.

2) $\mathbb{Z}[i]$ et le théorème des deux carrés

DEF 66: $\mathbb{Z}[i]=\{a+ib \mid (a,b)\in\mathbb{Z}^2\}$

PROP 67: $\mathbb{Z}[i]^\times=\{-1;1;-i;i\}$

PROP 68: $\mathbb{Z}[i]$ est euclidien de stathme N

Application au théorème des deux carrés

On étudie $\Sigma=\{n\in\mathbb{N} \mid n=a^2+b^2,\ a,b\in\mathbb{N}\}$.

EX 69: $0;1,2,3,4,5\in\Sigma$ mais $3,6\notin\Sigma$

PROP 70: Σ est stable par multiplication

DEV 2

LEMME 71: $p\in\Sigma\Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i]$

THM 72: Soit $p\in\mathbb{N}$ un nombre premier. On a : $p\in\Sigma\Leftrightarrow p=2$ ou $p\equiv 1 \mod 4$.

THM 73: Soit $n\in\mathbb{N}^*$, $n\neq 1$. On décompose n en facteurs premiers, $n=\prod p^{v_p(n)}$

$n\in\Sigma\Leftrightarrow v_p(n)$ est pair pour $p\equiv 3 \mod 4$.