[Tau]
[Rom]
[Per]

127 - Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables

I- Nombres remarquables

1) Nombre e et π [Tau] 43-44

- Fct exp propriétés, nombre d'Euler e
- $t \in \mathbb{R} \mapsto e^{it} \in \mathbb{U}$
- def π

2) Nombres rationnels et irrationnels ♥

- def $\mathbb{Q}$, corps fractions de $\mathbb{Z}$
  ↳ de caractéristique 0
- $\sqrt{2}$, π, e

3) Nombres premiers [Rom] 303 305 284

- def, exemples
- Th fondamental de l'arithmétique
- lien pgcd, ppcm
- infinité
- Fermat
- Dirichlet

DEV 1

II- Anneaux de nombres remarquables

1) Anneaux entiers de Gauss [Per] 56-57

- def, norme
- $\mathbb{Z}$
- Th des 2 carrés
- irréductibles $\mathbb{Z}[i]$

DEV 2

2) Nombres algébriques [Per] 65-66-67

- éléments algébriques et transcendant

- polynome minimal
- extension

3) Corps cyclotomique [Per] 67

- Racine nième
- U_n
- polynômes cyclotomiques + prop.

127: Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables

I- Nombres remarquables

1) Nombres e et π

[Tau] 43 **Définition 1**: On définit la fonction exponentielle complexe par $e^z = \exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!}$ $\forall z \in \mathbb{C}$

Proposition 2:
- $z \in \mathbb{C} \mapsto e^z$ est C^∞
- $\forall z, \zeta \in \mathbb{C}$ $e^{z+\zeta} = e^z e^\zeta$
- $\forall z \in \mathbb{C}$ $|e^z| = e^{Re(z)}$
- $\forall z \in \mathbb{C}$ $e^z \neq 0$
- $|e^z| = 1 \Leftrightarrow z \in i\mathbb{R}$
- $\forall z \in \mathbb{C}$ $(e^z)^{-z} = e^{-z}$

44 **Théorème 3**: L'application $(\mathbb{R}, +) \xrightarrow{\varphi} (\mathbb{U}, \times), t \mapsto e^{it}$ est un homéomorphisme de groupe surjectif.
$\ker \varphi = a\mathbb{Z}$.

Définition 4: Le réel a qui est le plus petit réel positif t tel que $e^{it} = 1$ est noté 2π

2) Nombres rationnels et irrationnels

Définition 5: on définit l'ensemble des nombres rationnels $\mathbb{Q}$ comme l'ensemble des nombres étant des quotients de deux entiers relatifs. Il s'agit du corps des fractions de $\mathbb{Z}$.
Les nombres irrationnels sont $\mathbb{R} \setminus \mathbb{Q}$

Exemples 6: $\sqrt{2}$, π, e sont irrationnels

3) Nombres premiers

Définition 7: On dit que $p \in \mathbb{N}$ est premier s'il est supérieur ou égal à 2 et si ses seuls diviseurs positifs sont 1 et p. [R] 303

Théorème 8: (Euclide) Tout entier relatif $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ a au moins un diviseur premier.

Théorème 9: L'ensemble P des nombres premiers est infini 305

Théorème 10: (Fondamental de l'arithmétique)
Tout entier naturel $n \geq 2$ se décompose de manière unique sous la forme : $n = q_1^{\alpha_1} \dots q_r^{\alpha_r}$
où $q_i \in P$ tels que $2 \leq q_1 < q_2 < \dots < q_r$ et $\alpha_k \in \mathbb{N}^*$

Théorème 11: Soient $n \geq 2$, $m \geq 2$ deux entiers tels que $n = \prod_{k=1}^{r} q_k^{\alpha_k}$ $m = \prod_{k=1}^{r} q_k^{\beta_k}$ leurs décomposition en facteurs premiers : $q_k \in P$ et $\alpha_k, \beta_k \in \mathbb{N}$
On a alors: $n \wedge m = \prod_{k=1}^{r} q_k^{\min(\alpha_k, \beta_k)}$ et $n \vee m = \prod_{k=1}^{r} q_k^{\max(\alpha_k, \beta_k)}$

Théorème 12: (Fermat): Soit p entier naturel premier 254
Pour tout entier relatif a premier avec p on a $a^{p-1} \equiv 1 \ [p]$ et $\forall a \in \mathbb{Z}$ $a^p \equiv a \ [p]$

Théorème 13: (Dirichlet faible) DEV 1
Soit $n \geq 2$, il existe une infinité de nombres premiers congru à 1 modulo n.

II- Anneaux de nombres remarquables

1) Anneau des entiers de Gauss

[P] 56 **Définition 14**: On définit l'anneau des entiers de Gauss: $\mathbb{Z}[i] := \{a+ib \in \mathbb{C},\ a,b \in \mathbb{Z}\}$

on lui attribue la norme $N: \mathbb{Z}[i] \to \mathbb{N}$

$z=a+ib \mapsto z\bar{z}=a^2+b^2$

Définition 15: on note Σ l'ensemble:

$$\Sigma = \{n \in \mathbb{N} \text{ tq } \exists (a,b) \in \mathbb{N}^2 \text{ tel que } n=a^2+b^2\}$$

57 **Théorème 16**: Soit p un nombre premier. on a:

$$p \in \Sigma \iff p=2 \text{ ou } p \equiv 1\ [4]$$ DEV2

Théorème 17: Les irréductibles de $\mathbb{Z}[i]$ sont, aux éléments inversibles près:

1) les entiers premiers $p \in \mathbb{N}$ avec $p \equiv 3\ [4]$
2) les entiers de Gauss $a+ib$ dont la norme a^2+b^2 est un nombre premier

2) Nombres algébriques

[Per] 65 **Définition 18**: on dit que L est une extension de corps de K noté K/L lorsque $K \subset L$

66 **Définition 19**: Soit $K \subset L$ une extension et $\alpha \in L$.

Soit $\varphi: K[X] \to L$ le morphisme d'évaluation en α.

1) si φ injectif, on dit que α est transcendant sur K

2) Sinon on dit que α est algébrique sur K. Ainsi il existe $P \in K[X]$ non nul tel que $P(\alpha)=0$.

On a $\ker(\varphi)=(P)$ et on peut supposer P unitaire.

on dit que P est le polynôme minimal de α sur K

Exemples 20: • e (admis) et π sont transcendants sur $\mathbb{Q}$.

• $\sqrt{2}$, i, $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$

Proposition 21: Si α est transcendant, $K[\alpha] \simeq K[X]$ et $K(\alpha) \simeq K(X)$

Théorème 22: Soit $K \subset L$ une extension et $\alpha \in L$.

On a les équivalences:

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

Si P est le polynôme minimal de α, P est irréductible et on a $[K(\alpha):K] = \deg(P)$. on l'appelle degré de α

Exemple 23: $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$

67 **Définition 24**: Soit $K \subset L$ une extension. On dit qu'elle est: 1) finie si $[L:K] < +\infty$

2) algébrique si $\forall \alpha \in L$, α est algébrique sur K

Proposition 25: Toute extension finie est algébrique

Théorème 26: Soit $K \subset L$ une extension. L'ensemble des éléments de L algébriques sur K forment un sous corps

3) Corps cyclotomique

On pose m un entier supérieur ou égal à 1

67 **Définition 27:** On définit $\mu_m = \{z \in \mathbb{C}^* \mid z^m = 1\}$ l'ensemble des racines m-ièmes de l'unité.
C'est un groupe cyclique pour la multiplication dont l'ensemble des générateurs noté μ_m^* est formé des racines primitives m-ièmes de l'unité.

Proposition 28: • $\mu_m^* = \{e^{\frac{2ik\pi}{m}} \mid k \in [\![1, m]\!] \text{ et } k \wedge m = 1\}$
• $|\mu_m^*| = \varphi(m)$ avec φ l'indicatrice d'Euler

Définition 29: On appelle m ième polynôme cyclotomique le polynôme :

$$\Phi_m(X) = \prod_{\zeta \in \mu_m^*} (X - \zeta)$$

Proposition 30: • $X^m - 1 = \prod_{d \mid m} \Phi_d(X)$
• $\Phi_m(X) \in \mathbb{Z}[X]$
• Φ_m est irréductible sur $\mathbb{Q}$

NOMBRES

Premiers nb remarquables rencontrés

① π et e
- → défini la fct exp
- → le nb d'Euler
- ↳ permet de définir π

② Nb rationnels et irrationnels

$\mathbb{Q}$ = corps fractions de $\mathbb{Z}$

$\sqrt{2}$, π, e, ...

③ Nombres premiers
- → bcp de prop
- → Th fond de l'arithmétique
  - ↳ décomposition des nb
- → infinité
- → Fermat
- → Th Dirichlet faible DEV 1

lien

racines de l'unité

$\mathbb{U}_n$
- → polynômes cyclotomiques

$\Phi_n = \prod_{\zeta \in \mathbb{U}_n^*} (X - \zeta)$

irréd sur $\mathbb{Q}$

127 : nombres remarquables et anneaux remarquables

ANNEAU

Entiers de Gauss

$\mathbb{Z}[i]$

$X^2 + 1$ irréductible sur $\mathbb{R}$

Th des 2 carrés

DEV 2

nb algébrique

$\alpha \in L$ racine d'un polynome de $K[X]$ ou L extension de K

↓

extension algébrique