Idéaux d'un corps de nombres.

$$\begin{array}{ccccc} k & \supset & \mathbb{Z}_k & \supset & \overline{\mathbb{Q}} \\ | n & & \cup & & \\ \mathbb{Q} & \supset & \mathbb{Z} & \supset & a\cap\mathbb{Z} = a\mathbb{Z} \qquad a>0 \end{array}$$

Si $\mathfrak{a}$ est un idéal de $\mathbb{Z}_k$, $\mathfrak{a}\neq\{0\}$, alors $\mathfrak{a}\cap\mathbb{Z}\neq\{0\}$

$\exists\, \alpha\in\mathfrak{a}$, $\alpha\neq 0$. $\quad \exists\, m\geq 1, \exists\, a_i\in\mathbb{Z}$

$\alpha^m + a_1\alpha^{m-1} + \dots + a_m = 0 \qquad a_m\neq 0.$

$a_m = -\alpha^m - \dots - a_1\alpha \in \mathfrak{a}\cap\mathbb{Z}.$

Si $\mathfrak{p}$ est un idéal premier de $\mathbb{Z}_k$, alors

$\mathfrak{p}\cap\mathbb{Z} = p\mathbb{Z}$ $\quad$ p nombre premier

$$\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}_k \\ \downarrow & \searrow & \downarrow \\ \mathbb{Z}/p\mathbb{Z} & \hookrightarrow & \mathbb{Z}_k/\mathfrak{p} \end{array}$$

$\mathbb{Z}_k/\mathfrak{p}$ anneau intègre

$\mathbb{Z}_k/\mathfrak{p}$ est fini

$|\mathbb{Z}_k/\mathfrak{p}| = N\mathfrak{p}$

Sous-anneau intègre $\Rightarrow$ intègre $\Rightarrow p$ premier.

$x\in A,\ x\neq 0$

$[x]: A \to A$ bijective.

Tout anneau fini intègre A est un corps.

$\Rightarrow \mathfrak{p}$ idéal maximal.

$\mathbb{Z}_k/\mathfrak{p}$ est le corps résiduel de l'idéal premier $\mathfrak{p}$.

p = caractéristique résiduel.

$$\begin{array}{ccc} \mathbb{Z}_k/\mathfrak{p} & & f = [\mathbb{Z}_k/\mathfrak{p} : \mathbb{F}_p] \\ | & f & \\ \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} & & N(\mathfrak{p}) = p^f \end{array}$$

Rappels. A anneau $\mathfrak{a}, \mathfrak{b}$ idéaux.

$\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}\cap\mathfrak{b} \subset \mathfrak{a} \subset \mathfrak{a}+\mathfrak{b} = \{\alpha+\beta,\ \alpha\in\mathfrak{a}, \beta\in\mathfrak{b}\}$

idéal engendré par $\alpha\beta$, $\alpha\in\mathfrak{a}$, $\beta\in\mathfrak{b}$.

idéal engendré par $\mathfrak{a}\cup\mathfrak{b}$

Exemple. $A=\mathbb{Z}$ $\quad \mathfrak{a}=4\mathbb{Z}$ $\quad \mathfrak{b}=6\mathbb{Z}$

$\mathfrak{a}\mathfrak{b} = 24\mathbb{Z} \subset \mathfrak{a}\cap\mathfrak{b} = 12\mathbb{Z} \subset 4\mathbb{Z} \subset 6\mathbb{Z}$

$\mathfrak{a}+\mathfrak{b} = 2\mathbb{Z}$ $\quad 2 = \text{pgcd}(4,6).$

$2\mathbb{Z}+3\mathbb{Z} = \mathbb{Z}$

- A anneau $\mathfrak{a}$ idéal $\quad \mathfrak{a}=A \iff 1\in\mathfrak{a}$

  $\iff \mathfrak{a}\cap A^\times \neq \phi$ $\qquad A=(1)$

- Si $\mathfrak{a}+\mathfrak{b}=A$, alors $\mathfrak{a}\cap\mathfrak{b}=\mathfrak{a}\mathfrak{b}$.

  et $A/\mathfrak{a}\mathfrak{b} \cong A/\mathfrak{a}\times A/\mathfrak{b}$.

Lemme. $\mathbb{Z}_k \supset \mathfrak{a}, \mathfrak{b}$ idéaux non nuls
si $\mathfrak{a}\mathfrak{b} = \mathfrak{a}$, alors $\mathfrak{b} = (1)$.

Dém. comme $\mathbb{Z}$-module,
$\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$.
$\alpha_i \in \mathfrak{a} = \mathfrak{a}\mathfrak{b} \Rightarrow \alpha_i = \sum_{j=1}^{n} \beta_{ij}\alpha_j$.
$\beta_{ij} \in \mathfrak{b}$.
$B = (\beta_{ij})_{\substack{1\le i\le n \\ 1\le j\le n}}$
$\det(B - I_n) = 0 \Rightarrow 1 \in \mathfrak{b}$.

Théorème. Tout idéal non nul $\mathfrak{a}$ de $\mathbb{Z}_k$ s'écrit, de manière unique à l'ordre près,
$\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$
$\mathfrak{p}_i$ idéaux premiers
α_i entiers ≥ 1
$r \ge 0$.
$\mathfrak{a} \subseteq \mathfrak{p}_i^{\alpha_i} \subset \mathfrak{p}_i^{\alpha_i - 1} \subset \cdots \subset \mathfrak{p}_i \subset \mathbb{Z}_k$
$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ = ensemble des idéaux premiers de $\mathbb{Z}_k$ contenant $\mathfrak{a}$.

$\mathfrak{a}$ idéal non nul de $\mathbb{Z}_k$
$\mathfrak{p}$ premier contenant $\mathfrak{a}$.
α le plus grand entier ≥ 1 tel que $\mathfrak{a} \subseteq \mathfrak{p}^\alpha$. $\alpha = v_{\mathfrak{p}}(\mathfrak{a})$.

$\bigcap_{m \ge 1} \mathfrak{p}^m = (0)$

$\mathfrak{a} = \prod_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$

Lemme $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$

$N(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$

$N(\mathfrak{a}) = \prod_{\mathfrak{p} \supset \mathfrak{a}} N(\mathfrak{p})^{v_{\mathfrak{p}}(\mathfrak{a})}$

Lemme. Si $\mathfrak{a}$ est un idéal de $\mathbb{Z}_k$
$\mathfrak{a} \neq 0$ et $\mathfrak{p}$ un idéal premier de $\mathbb{Z}_k$
$\mathfrak{p} \neq 0$. Alors $\mathfrak{a}/\mathfrak{p}\mathfrak{a}$
est un espace vectoriel sur $\mathbb{Z}_k/\mathfrak{p}$
de dimension 1.

$\mathfrak{a}$ sous-$\mathbb{Z}_k$-module de $\mathbb{Z}_k$
$\cup$
$\mathfrak{p}\mathfrak{a}$
$M = \mathfrak{a}/\mathfrak{p}\mathfrak{a}$ est un $\mathbb{Z}_k$-module.
$\mathbb{Z}_k/\mathfrak{p}$ corps résiduel.
$\mathbb{Z}_k \times M \to M$
$(\mathbb{Z}_k/\mathfrak{p}) \times M$?

$\alpha \in \mathfrak{p}$ $\quad (\alpha, x)$

$\mathbb{Z}_k \times M \longrightarrow M$

$\downarrow \qquad \downarrow \qquad \nearrow$

$\mathfrak{p}(\alpha) x \quad (\mathbb{Z}_k/\mathfrak{p}) \times M$

$\| \quad (0,0)$

$M = a/\mathfrak{p}a$.

$a \in a$.

$\alpha \cdot (a) \bmod \mathfrak{p}a$

$\|$

x

$\alpha a \in \mathfrak{p}a$.

$\dim_{\mathbb{Z}_k/\mathfrak{p}} (a/\mathfrak{p}a) \geq 1$

$\mathfrak{p}a \neq a \qquad \mathfrak{p} \neq \mathbb{Z}_k$.

$a = \mathbb{Z}_k \quad \mathfrak{p}a = \mathfrak{p}$. $\dim_{\mathbb{Z}_k/\mathfrak{p}} a/\mathfrak{p}a = 1$.

$\mathbb{Z}_k \supsetneq \mathfrak{p} \supsetneq \mathfrak{p}^2 \supsetneq \cdots \supsetneq \mathfrak{p}^m \supsetneq \mathfrak{p}^{m+1} \supsetneq \cdots$

$\mathfrak{p}^m / \mathfrak{p}^{m+1}$ est un $\mathbb{Z}_k/\mathfrak{p}$

espace vectoriel de dimension ≥ 1

$0 \neq \alpha \in \mathfrak{p}^m \qquad \alpha \mathbb{Z}_k \subset \mathfrak{p}^m$.

$(N(\mathfrak{p}))^m = N(\mathfrak{p}^m)$ divise $N_{k/\mathbb{Q}}(\alpha)$.

$a \subset b$

$\Rightarrow N b \mid N a$.

$\mathbb{Z}_k \longrightarrow \mathbb{Z}_k/b$.

$\mathbb{Z}_k/a$ $\quad$ surj.

$\Rightarrow \{ m \geq 1, \ \alpha \in \mathfrak{p}^m \}$ fini.

Idéal entier de k = idéal de $\mathbb{Z}_k$.

Idéaux fractionnaires $\subset k$

(idéal fractionnaire contenu dans $\mathbb{Z}_k$ est un idéal entier).

Déf. Idéal fractionnaire $\mathfrak{I}$ de k, = sous $\mathbb{Z}_k$-module de k tel qu'il existe un élément $\alpha \in \mathbb{Z}_k$, $\alpha \neq 0$, $\alpha \mathfrak{I} \subset \mathbb{Z}_k$.

Exemple. $k = \mathbb{Q}$. idéal fractionnaire $\Leftrightarrow u\mathbb{Z}$, $u \in \mathbb{Q}$. $(u > 0)$

Exemple $\quad [k : \mathbb{Q}] = n$. $\quad \mathfrak{p}$ idéal (entier) premier $\neq 0$.

$\mathfrak{p}' = \{ x \in k \ ; \ x\mathfrak{p} \subset \mathbb{Z}_k \}$

$\exists \alpha \in \mathbb{Z}_k \setminus \{0\}$, $\alpha \mathfrak{p}' \subset \mathbb{Z}_k$, premier $\in \mathfrak{p}$

Proposition. $\mathfrak{p}'$ est un idéal fractionnaire de k et $\mathfrak{p}\mathfrak{p}' = \mathbb{Z}_k$.

$\mathfrak{I}, \mathfrak{J}$ deux idéaux fractionnaires, $\mathfrak{I}\mathfrak{J}$ le sous-$\mathbb{Z}_k$-module de k engendré par les xy, $x \in \mathfrak{I}, y \in \mathfrak{J}$. $\alpha \mathfrak{I} \subset \mathbb{Z}_k$ $\quad \beta \mathfrak{J} \subset \mathbb{Z}_k$.

$\mathfrak{I}\mathfrak{J}$ est un idéal fractionnaire.

Décomposition d'un idéal fractionnaire en produit d'idéaux premiers.

Notation. $\mathfrak{p}^{-1} = \{x \in k,\ x\mathfrak{p} \subset \mathbb{Z}_k\}$

Tout idéal fractionnaire $\mathfrak{J}$ de k $\mathfrak{J} \neq 0$ s'écrit de manière unique

$$\mathfrak{J} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{J})}, \quad v_{\mathfrak{p}}(\mathfrak{J}) \in \mathbb{Z}$$

$\mathfrak{p}$: idéaux premiers $\neq 0$ de $\mathbb{Z}_k$

$\mathfrak{p}^0 = (1)$

$\{\mathfrak{p};\ v_{\mathfrak{p}}(\mathfrak{J}) \neq 0\}$ est fini.

$$N(\mathfrak{J}) := \prod_{\mathfrak{p}} N(\mathfrak{p})^{v_{\mathfrak{p}}(\mathfrak{J})}$$

Retour aux idéaux entiers.

$k \supset \mathbb{Z}_k \supset a \cdot \neq 0$.

$\mathbb{Q} \supset \mathbb{Z}$

$p \in \mathbb{Z}_{>0}$ premier $\quad p\mathbb{Z}_k$ idéal entier de k

$p\mathbb{Z}_k = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. $\quad \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ premiers

$e_1, \ldots, e_r$ entiers > 0.

$$p\mathbb{Z}_k = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

$$N(p\mathbb{Z}_k) = N_{k/\mathbb{Q}}(p) = p^n$$

k | n | $\mathbb{Q}$

$$N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r} = p^{e_1 f_1 + \cdots + e_r f_r}.$$

$\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ sont les idéaux premiers de $\mathbb{Z}_k$ qui contiennent p. $\quad N(\mathfrak{p}_i) = p^{f_i}$

$n = e_1 f_1 + \cdots + e_r f_r$.

k donné.

$\{p$ premier, un des e_i est $\geq 2\}$ fini

= diviseurs premiers du discriminant D_k.

Déf. p est ramifié dans l'extension si un des e_i est ≥ 2. ($\Leftrightarrow p \mid D_k$).

p est totalement ramifié si $r = 1, e_1 = n$ ($f_1 = 1$)

$p\mathbb{Z}_k = \mathfrak{p}^n$

p est totalement décomposé si $r = n$

$p\mathbb{Z}_k = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ $\quad \mathfrak{p}_i$ 2 à 2 distincts ($f_i = 1$)

p est inerte dans $k/\mathbb{Q}$ si $r=1$, $e_1=1$, $f_1=n$

$p\mathbb{Z}_k = \mathfrak{p}$ idéal premier de $\mathbb{Z}_k$.

Exemple. $k=\mathbb{Q}(\sqrt{d})$ $d\in\mathbb{Z}$ sans facteur carré.

Δ discriminant $= \begin{cases} d & d\equiv 2 \text{ ou } 3 \bmod 4 \\ 4d & d\equiv 1 \bmod 4 \end{cases}$

p premier impair

$p|\Delta \iff p|d$.

$n=2=e_1f_1+\dots+e_rf_r$.

$r=2$ $e_1=f_1=e_2=f_2=1$ tot. déc.

$r=1$ $e_1=2$ $f_1=1$ ram.

$r=1$ $e_1=1$ $f_1=2$ inerte

p ramifié $\iff p|d$.

p décomposé (totalement) $\iff \left(\frac{d}{p}\right)=1$

p inerte $\iff \left(\frac{d}{p}\right)=-1$.

$N(\mathfrak{p})=p$

$p\mathbb{Z}_k=\mathfrak{p}^2$

$p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2$

$N(\mathfrak{p}_1)=N(\mathfrak{p}_2)=p$

$p\mathbb{Z}_k=\mathfrak{p}$

$N(\mathfrak{p})=p^2$.

$f=2$

$\mathbb{Z}_k/\mathfrak{p}\simeq\mathbb{F}_{p^2}$.

$\mathbb{Z}/p\mathbb{Z}$

Classes d'idéaux.

k / $\mathbb{Q}$: Relation d'équivalence sur l'ensemble des idéaux fractionnaires $\neq 0$

$\mathfrak{I}\sim\mathfrak{J} \iff \exists \alpha\in k^\times,\ \mathfrak{I}=(\alpha)\mathfrak{J}$.

Théorème : L'ensemble des classes d'équiv. est fini. Nombre $h_1(k)$ = nombre de classes de k.

$\mathbb{Z}_k$ principal $\iff h_1(k)=1$.

Théorème de Hermite.

$\forall C>0$ $\{$ k corps de nombres de discriminant $\leq C\}$ fini.