Réseaux algébriques

I) Quelques résultats de théorie des nombres :

1) Définitions

Notations : • $d \geq 2$ un entier

• $P \in \mathbb{Q}[X]$ irréductible de deg d.

• $K = \mathbb{Q}[X]/P(X)$, $R = \{\alpha \in K \mid \exists P_\alpha \in \mathbb{Z}[X]$ irred et unitaire t.q. $P_\alpha(\alpha) = 0\}$

Lemme : K est un corps et un $\mathbb{Q}$-ev de dim d. On dit que K est un corps de nombre de degré d.
R est un anneau.

Preuve : • K corps $\rightsquigarrow$ P irred / $\mathbb{Q}$-ev dim d $\rightsquigarrow$ base $(1, X, \dots, X^{d-1})$ (détails p. d'après)

• R anneau $\rightsquigarrow$ admis

Exemple principal : $P = X^d + 1$ pour d une puissance de 2. (pdg cyclo)
Dans ce cas, $K = \mathbb{Q}[X]/P(X)$ et $R = \mathbb{Z}[X]/P(X)$.

Exemple :

• $d = 2$, $K = \mathbb{Q}[X]/(X^2+1)$

$$x = a + bX \qquad y = c + dX$$

$$x + y = a + c + (b+d)X$$

$$x \times y = ac + (bc+da)X + bdX^2 = ac - bd + (bc+da)X \mod X^2+1$$

Rq : On représente les éléments de K par les pdgs de $\mathbb{Q}[X]$ de deg $\leq d-1$.
$K \leftrightarrow \{a(X) \in \mathbb{Q}[X] \mid \deg(a) < d\}$
Si $P = X^d + 1$, $R \leftrightarrow \{a(X) \in \mathbb{Z}[X] \mid \deg(a) < d\}$

Comme X^d+1 est irréductible, $\gcd(a, X^d+1) = 1$.

Par Bezout, il existe $u, v \in \mathbb{Q}[X]$ t.q.

$$au + v(X^d+1) = 1$$

$$\Leftrightarrow \quad a \times u = 1 \mod X^d+1$$

$\Leftrightarrow$ a est inversible dans K, d'inverse u.

On en conclut que K est un corps. □

2) Plongements :

Définition : Le plongement canonique de K est défini par

$$K \longrightarrow \mathbb{C}^d$$

$$\tau : \quad a = \sum_{i=0}^{d-1} a_i X^i \longmapsto \left(a(\rho_1), \dots, a(\rho_d)\right)$$

où $\rho_1, \dots, \rho_d$ sont les d racines de P dans $\mathbb{C}$.

Lemme : Les racines complexe de X^d+1 sont les racines primitives $2d$-ième de l'unité, i.e. $\exp\left(2i\pi \times \frac{k}{2d}\right)$ pour $1 \leq k < 2d$ avec k impair.

Preuve : Si α racine de X^d+1, alors $\alpha^d = -1$

$$\Rightarrow \alpha^{2d} = 1$$

et $\forall \underset{k \neq 2d}{k \mid 2d}$, $\alpha^k \neq 1$ (sinon on aurait $\alpha^d = 1$ car $k \mid d$)

Lemme : $\tau(a)$ ne dépend pas du choix du représentant de $a \in K$ dans $\mathbb{Q}[X]$. En d'autres termes, si $a, a' \in \mathbb{Q}[X]$ et $a = a' \bmod P$, alors $\tau(a) = \tau(a')$.

Preuve : Si $a' = a + P \times Q$ avec $Q \in \mathbb{Q}[X]$.

Soit β une racine de P dans $\mathbb{C}$.

Alors $a'(\beta) = a(\beta) + \underbrace{P(\beta)}_{=0} Q(\beta) = a(\beta)$

Donc $\tau(a') = \tau(a)$ comme demandé. □

Exemple : $P = X^2 + 1$, $a = a_0 + a_1 X \in K$

$$\tau(a) = (a_0 + a_1 i, \; a_0 - a_1 i)$$

(racines de $X^2+1 = \{i, -i\}$)

Lemme : Soient $a, b \in K$. Si $\tau(a) = (\alpha_1, \dots, \alpha_d)$ et $\tau(b) = (\beta_1, \dots, \beta_d)$, alors $\tau(ab) = (\alpha_1\beta_1, \dots, \alpha_d\beta_d)$

et $\tau(a+b) = (\alpha_1 + \beta_1, \dots, \alpha_d + \beta_d)$

Preuve : Soit β une racine de P dans $\mathbb{C}$, on a

$(a \times b)(\beta) = a(\beta) \times b(\beta)$ et $(a+b)(\beta) = a(\beta) + b(\beta)$. □

Définition : Le plongement par coefficients de K est défini par

$$\Sigma : \begin{array}{ccc} K & \longrightarrow & \mathbb{Q}^d \\ a = \sum_{i=0}^{d-1} a_i X^i & \longmapsto & (a_0, \dots, a_{d-1}) \end{array}$$

⚠ Ici, il faut vraiment choisir pour a le représentant de $\mathbb{Q}[X]/P$ de degré $< d$.

Exemple : $P = X^2+1$, $a = a_1 + a_2 X$, $\Sigma(a) = (a_1, a_2)$

Lemme : Soient $a, b \in K$, alors $\Sigma(a+b) = \Sigma(a) + \Sigma(b)$

⚠ En général on n'a pas que $\Sigma(a \times b)$ est la multiplication coeff par coeff de $\Sigma(a)$ et $\Sigma(b)$.

Par exemple : $(1+X)(2+X) = 2+3X+X^2 = 1+3X$

Σ ↙ ↓Σ ↓Σ

$(1,1) \otimes (2,1) \neq (1,3)$

↑ produit par coordonnées

Taille d'un élément de K (ou de R) : grâce à τ et Σ (→ "norme euclidienne"), on peut définir 2 notions de "taille" pour un élément $a \in K$: soit $\|\Sigma(a)\|_2$, soit $\|\Sigma(a)\|_2$

↑ norme 2 sur $\mathbb{R}^d$; ↑ norme 2 sur $\mathbb{Q}^d$

Lemme : τ et Σ sont injectifs. + Σ est bijectif

Preuve : Soient $a = \sum_{i=0}^{d-1} a_i X^i$ et $b = \sum_{i=0}^{d-1} b_i X^i \in K$

- Si $\tau(a) = \tau(b) \iff a(\beta_i) = b(\beta_i) \quad \forall i \in \{1, \dots, d\}$

  a et b sont des polys de deg $\leq d-1$ qui coincident en d points distincts $\Rightarrow$ il sont égaux.

- Si $\Sigma(a) = \Sigma(b) \iff a_i = b_i \quad \forall i \in \{0, \dots, d-1\}$

  $\iff a = b$

Correction exo 1 : $M = \begin{pmatrix} 1 & \beta_1 & \cdots & \beta_1^{d-1} \\ \vdots & & & \\ 1 & \beta_d & \cdots & \beta_d^{d-1} \end{pmatrix}$

$$\left\langle \begin{pmatrix} \beta_1^k \\ \vdots \\ \beta_d^k \end{pmatrix}, \begin{pmatrix} \beta_1^\ell \\ \vdots \\ \beta_d^\ell \end{pmatrix} \right\rangle = \sum_{i=1}^{d} \beta_i^{\ell-k}$$

si $k \neq \ell$, $\beta_i^{\ell-k} = \exp\left(2i\pi \times \frac{(2i+1)(\ell-k)}{2d}\right)$

racine primitive

$$\sum_{k=0}^{d-1} \left(\beta_i \overline{\beta_j}\right)^k$$

Remarque : Le plongement par coefficient est utile car il vit dans $\mathbb{Q}^d$ (voire $\mathbb{Z}^d$ si $a \in R$), ce qui le rend facile à manipuler ⇝ il est surtout utilisé pour les constructions.

Le plongement canonique a plein de propriétés mathématiques sympatiques (entre autre, la multiplication) ⇝ il est surtout utilisé pour la cryptanalyse.

Si $P = X^d + 1$

Lemme : Pour tout $a \in K$, on a $\|\sigma(a)\| = \sqrt{d} \times \|\Sigma(a)\|$.

⚠ Cette égalité n'est en général pas vraie si on remplace X^d+1 par un autre polynôme irreductible.

Preuve : exo 1.

Lemme : $\forall\, a, b \in K$, on a

$$\|\sigma(a+b)\| \leq \|\sigma(a)\| + \|\sigma(b)\|$$

(dire que je baisse tomber le 2 en indice de la norme)

$$\|\sigma(ab)\| \leq \|\sigma(a)\|_\infty \times \|\sigma(b)\|$$

Preuve :

- $\|\sigma(a+b)\| = \|\sigma(a)+\sigma(b)\| \leq \|\sigma(a)\| + \|\sigma(b)\|$.
- Si $\sigma(a) = (\alpha_1, \dots, \alpha_d)$ et $\sigma(b) = (\beta_1, \dots, \beta_d)$, alors

$$\|\sigma(ab)\|^2 = \sum_{i=1}^{d} |\alpha_i|^2 |\beta_i|^2 \leq \left(\max_i |\alpha_i|\right)^2 \times \sum_{i=1}^{d} |\beta_i|^2 = \|\sigma(a)\|_\infty^2 \times \|\sigma(b)\|_2^2$$

3) Idéaux et réseaux idéaux :

Lemme : R est un $\mathbb{Z}$-module de rang d : il existe $\alpha_1, \dots, \alpha_d \in R$ t.q. tout $x \in R$ s'écrit de façon unique $x = \sum_{i=1}^{d} x_i \alpha_i$ avec $x_i \in \mathbb{Z}$. On dit que $(\alpha_i)_i$ est une $\mathbb{Z}$-base de R.

Preuve : admis

Exemple : $P = X^d + 1$, $R = \mathbb{Z}[X]/X^d+1$.

On peut vérifier que $1, X, \dots, X^{d-1}$ est une $\mathbb{Z}$-base de R :

Ht élément de R s'écrit de façon unique $\sum_{i=0}^{d-1} x_i X^i$ avec $x_i \in \mathbb{Z}$.

Lemme : $\Sigma(R) \subseteq \mathbb{Q}^d$ et $\tau(R) \subseteq \mathbb{C}^d$ sont des réseaux de dimension d, de base respective $\Sigma(1), \dots, \Sigma(X^{d-1})$ et $\tau(1), \tau(X), \dots, \tau(X^{d-1})$

(notation : $\Sigma(R) = \{ \Sigma(a) \mid a \in R \}$)

Preuve : Soient $b_i = \Sigma(\alpha_i) \in \mathbb{Q}^d$ (α_i $\mathbb{Z}$-base de R)

On a vu que $\forall x \in R$, $\Sigma(x) = \Sigma\left(\sum_i x_i \alpha_i\right) = \sum x_i \Sigma(\alpha_i)$
$= \sum x_i b_i \quad x_i \in \mathbb{Z}$

Donc $\Sigma(R)$ est un réseau engendré par les b_i. Pour voir qu'il est de rg d et que les b_i forment une base du réseau, il suffit de prouver que les $\Sigma(b_i)$ sont $\mathbb{Z}$-linéairement indep.

Soient $y_1, \dots, y_d \in \mathbb{Z}$ t.q. $\sum y_i b_i = 0$. Alors $\Sigma\left(\sum_i y_i \alpha_i\right) = 0$

Comme Σ est injectif, $\sum y_i \alpha_i = 0 \Rightarrow y_1 = \dots = y_d = 0$.

Idem pour τ.

Exemple : $P = X^d + 1$, $R = \mathbb{Z}[X]/X^d+1$.

- Alors $\Sigma(R) = \mathbb{Z}^d$ (base $\Sigma(1), \dots, \Sigma(X^{d-1}) = \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}, \dots, \begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix}$)

- $\tau(R) \underset{\uparrow}{\sim} \sqrt{d}\mathbb{Z}^d$,

à une "rotation" près

$\uparrow$ mult par $U \in GL_n(\mathbb{C})$ t.q. $\overline{U}^T U = I_d$

Définition : Un idéal $\mathcal{A}$ est un sous-ensemble de R tel que :

- $\forall x, y \in \mathcal{A}$, $x+y \in \mathcal{A}$
- $\forall x \in \mathcal{A}$ et $r \in R$, $x \times r \in \mathcal{A}$

Exemple : $d=2$, • $\mathcal{A} = \{2x \times | x \in R\}$ est un idéal.

• $\mathcal{I}_b = \{a + bX \mid a = b \ [2]\}$ est un idéal

Preuve : si $a+bX \in \mathfrak{b}$ et $c+dX \in R$

$$(a+bX)(c+dX) = ac-bd+(ad+bc)X$$

$$= a(c-d)+a(c+d)X \quad [2]$$

↗ $a=b$ [2]

$$= a(c+d)+a(d+c)X \quad [2]$$

↗ $1=-1$ [2]

Lemme : Soit $\mathfrak{a} \subseteq R$ un idéal, alors $\sigma(\mathfrak{a}) \subseteq \mathbb{C}^d$ est un réseau de rang d. De plus, $\lambda_1(\sigma(\mathfrak{a})) = \dots = \lambda_d(\sigma(\mathfrak{a}))$

si $P = X^d+1$ ↗ $\sigma(\mathfrak{a})$ est appelé un réseau idéal

Preuve : exercice 2.

4) Modules et réseaux modules :

Définition : Un module* M de rang m est un sous-ensemble de R^m t.q. $\exists\, b_1, \dots, b_r \in K^m$ t.q.

$$M = \left\{ \sum_{i=1}^{r} x_i b_i \mid x_i \in R \right\}.$$ et $\mathrm{Span}_K(b_i) = K^m$ (i.e., $\{\sum x_i b_i \mid x_i \in K\} = K^m$)

(* c'est en fait un cas très particulier de ce qu'est un module en mathématique. Mais c'est la définition qu'on va utiliser dans ce cours. Terminologie utilisée par les cryptographes mais non approuvée par les mathématiciens)

Remarque : • Les $b_1, \dots, b_r$ ne sont pas forcément K-linéairement indépendants, et la représentation $\sum x_i b_i$ n'est pas forcément unique.

- Il n'existe pas forcément de base d'un module M.

Définition : le rang de M est la dimension du K-ev engendré par M.

Lemme :

M est un module de rang 1 ssi M est un idéal.

Preuve :

- M idéal $\Rightarrow$ M module : admis ($\forall$ a idéal, $\exists\, a_1, a_2 \in R$ t.q. $a = \{x_1 a_1 + x_2 a_2 \mid x_1, x_2 \in R\}$)

- M module $\Rightarrow$ M idéal : soient $x, y \in M$ et $r \in R$.

M module : $\exists\, b_1, \dots, b_k \in R$ t.q. $M = \{\sum_{i=1}^{k} z_i b_i \mid z_i \in R\}$

$\Rightarrow x = \sum x_i b_i$, $y = \sum y_i b_i$

- $x + y = \sum (x_i + y_i) b_i \in M$. ✓
- $r \times x = \sum \underbrace{(r x_i)}_{\in R} b_i \in M$. ✓

Lemme : Soit $M \subseteq R^m$ un module de rang m.

Alors $\tau(M) := \left\{ \begin{pmatrix} \tau(x_1) \\ \vdots \\ \tau(x_m) \end{pmatrix} \in \mathbb{C}^{dm} \mid \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \in M \right\} \subseteq \mathbb{C}^{dm}$

est un réseau de rang dm.

Preuve : admis

5) Problèmes algorithmiques :

Définition : • r-module-SVP_γ = SVP_γ restreint aux réseaux de la forme $\tau(M)$ où $M \subseteq K^r$ est un module de rk r.

• r-module-$SIVP_\gamma$ = ———————

Quand $r = 1$: 1-module-SVP_γ = ideal-SVP_γ
et 1-module-$SIVP_\gamma$ = ideal-$SIVP_\gamma$

Lemme : Pour $P = X^d + 1$, $\checkmark$ ideal-SVP_γ est équivalent à ideal-$SIVP_\gamma$

Preuve : suite de l'exo 2.

Difficulté (pire cas) → Pour $r \geq 2$:

• Pas de meilleur algorithme connu pour r-module-SVP_γ pire-cas que pour SVP_γ pire-cas dans des réseaux de rang rd

• **$r = 1$** : Si $\gamma = 2^{\sqrt{d}}$ et $P = X^d + 1$ ⇝ algo poly time quantique pour ideal-SVP_γ ⇝ alors que le meilleur algo pour SVP_γ en dim d est en $\exp(\sqrt{d})$.
⇝ ideal-SVP_γ a l'air + faible que SVP_γ en dim d quand γ est grand.
⇝ quand $\gamma = poly(d)$, pas de gain significatif pour ideal-SVP_γ.

Cas spécieux : Il existe des classes d'idéaux et de modules pour lesquels SVP$_\gamma$ est facile (mais ça ne concerne qu'une toute petite fraction des idéaux/modules)

$\rightsquigarrow$ on en reparlera au 3^e cours.

À retenir : pour $r \geq 2$: ça vaut le coup d'utiliser des modules : + efficace et ça n'a pas l'air - sûr.

(pire-cas)

Dans tte cette section : $P = X^d + 1$

II) Module-LWE : $R_q = R/qR$ pour $q \geq 2$ un entier

1) Définitions :

Définition : $n \geq 1$, $q \geq 2$ et χ distribution sur R

La distribution $D^{MLWE}_{n,q,\chi}(s)$ est la distribution sur $R_q^n \times R_q$ obtenue par l'expérience suivante :

- $a \leftarrow \mathcal{U}(R_q^n)$
- $e \leftarrow \chi$
- $b = \langle a, s \rangle + e \mod q$
- return (a, b)

Remarque : χ représente une distribution de "petits" éléments de R. Par exemple, si $e \leftarrow \chi$, alors $\tau(e) \sim D_{\tau(R), \alpha q}$ ($\tau(e)$ gaussien de petit écart-type dans $\tau(R)$).

Définition : (Module LWE).

(search) $MLWE_{n,q,\chi}$: Soit $s \leftarrow \mathcal{U}(R_q^n)$, étant donné un nombre arbitraire d'échantillons de $D^{MLWE}_{n,q,\chi}(s)$, retrouver s.

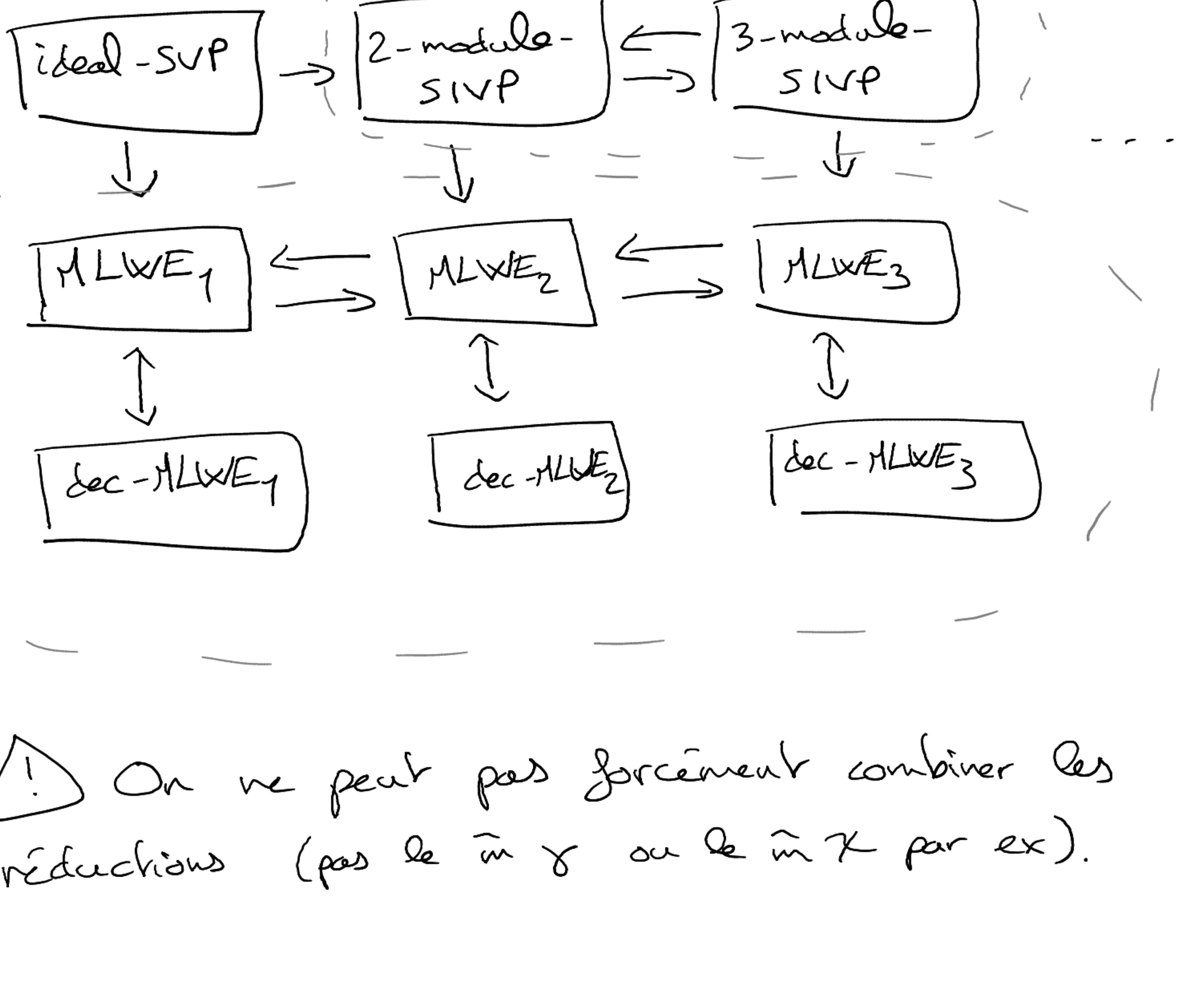
dec-$MLWE_{n,q,\chi}$ Soit $s \leftarrow \mathcal{U}(R_q^n)$, distinguer les distributions $D^{MLWE}_{n,q,\chi}(s)$ et $\mathcal{U}(R_q^n \times R_q)$.

2) Reductions :

$A \longrightarrow B$: il y a une réduction polynomiale (potentiellement quantique) du problème A vers le problème B.

r-module-SIVP $=$ r-module-SIVP$_\gamma$ pour un certain γ

MLWE$_n$ $=$ MLWE$_{n,q,\chi}$ pour certains q et χ



⚠ On ne peut pas forcément combiner les réductions (pas de $\widetilde{m}_\gamma$ ou de $\widetilde{m}_\chi$ par ex).

3) Albrecht-Deo's reduction : (Asiacrypt 2017)

Definition : On note $D_{R,\sigma}$ la distribution sur R telle que si $X \sim D_{R,\sigma}$, alors $\tau(X) \sim D_{\tau(R),\sigma}$ où $D_{\tau(R),\sigma}$ est la distribution gaussienne discrète sur le réseau $\tau(R)$, de paramètre σ et centrée en 0.

Thm [Albrecht-Deo, AC'17]
Il existe une réduction en temps polynomial depuis le problème $MLWE_{n,q,D_{R,\alpha q}}$ vers le problème $MLWE_{1,q',\alpha' q'}$

où
- $q' = q^n$
- $\alpha' = \alpha \times poly(d,n)$

On va prouver une version plus faible de ce théorème.

Definition : On dit qu'une distribution χ sur R est β-bounded si $\forall x$ dans le support de χ, $\|\tau(x)\| \leq \beta$.

Lemme : Soient $q \geq 2$, $n \geq 2$ des entiers, et χ une distribution β-bounded pour un $\beta > 0$.
Il existe un algorithme polynomial A qui prend en entrée des échantillons $(a,b) \leftarrow D^{MLWE}_{n,q,\chi}(s)$ pour un $s \in R^n$ fixé t.q. $\|\tau(s_i)\| \leq \beta$, et renvoie $(\tilde{a}, \tilde{b}) \in R_{q'} \times R_{q'}$ avec :

- $q' = q^n$
- $\tilde{a}$ uniforme dans $R_{q'}$
- $\tilde{b} = \tilde{a}\tilde{s} + \tilde{e}$ où :
  - $\tilde{s} = \sum_{i=1}^{n} s_i q^{i-1}$
  - $\|\tau(\tilde{e})\| \leq \beta' := 3nd^{3/2} q^{n-1} \beta$

↳ LWE

Preuve : Soient $(a, b) \leftarrow D^{MLWE}_{n,q,\chi}(s)$.

On a $b = \underline{\quad}\,|\,s + e \ [q]$, avec $\|\tau(e)\| \leq \beta$ (car χ est β-bornée)

Soit $a = (a_1, \dots, a_n) \in R_q^n$. Pour chaque coordonnée $a_i \in R_q$, on construit un représentant $\bar{a}_i \in R$ t.q. $\bar{a}_i = a_i \ [q]$ et $\|\tau(\bar{a}_i)\| \leq q d^{3/2}$. Si $a_i = \sum_{j=0}^{d-1} x_j X^i$ avec $x_j \in \mathbb{Z}/q\mathbb{Z}$, on prend $\bar{a}_i = \sum_{j=0}^{d-1} \bar{x}_j X^i$ avec $\bar{x}_j \in \{0, \dots, q-1\}$ et $\bar{x}_j = x_j \ [q]$.

On a $\|\tau(\bar{a}_i)\| \leq \sum_{j=0}^{d-1} \bar{x}_j \|\tau(X^i)\| \leq \sum_j q \times \sqrt{d} = d^{3/2} q$.

- On construit $\bar{a} = \sum_{i=1}^{n} \bar{a}_i q^{n-i}$. Chaque $\bar{a}_i$ est uniforme modulo q, donc $\bar{a}$ est uniforme modulo $q' = q^n$.

$i = n-1+j-k$

$k = n-1+j-i$

- Calculons $\tilde{a} \times \tilde{s}$:

$$\tilde{a} \times \tilde{s} = \left(\sum_{i=1}^{n} \bar{a}_i q^{n-i}\right) \times \left(\sum_{j=1}^{n} s_j q^{j-1}\right) = \sum_{i,j=1}^{n} a_i s_j q^{\overbrace{n-1+j-i}}$$

$$= \sum_{k=0}^{2n-2} \sum_{j=1}^{k+1} \bar{a}_{n-k-1+j} s_j q^k$$

$$= \sum_{k=0}^{n-1} q^k \sum_{j=1}^{k+1} s_j \overline{a}_{n-k-1+j} \mod q'$$

$$= q^{n-1} \times \sum_{j=1}^{n} s_j \overline{a}_j + \sum_{k=0}^{n-2} q^k \sum_{j=1}^{k+1} s_j \overline{a}_{n-k-1+j}$$

On sait que $\sum_{j=1}^{n} s_j \overline{a}_j = \langle s, \overline{a} \rangle = \langle s, a \rangle \mod q$

$$= b - e \mod q$$

Donc $q^{n-1} \times \sum_{j=1}^{n} s_j \overline{a}_j = q^{n-1}(b - e + qr)$

$$= q^{n-1} b - q^{n-1} e \mod q'$$

On définit $\tilde{b} = q^{n-1} b$.

On a $\tilde{a} \times \tilde{s} = \tilde{b} - \underbrace{q^{n-1} e + \sum_{k=0}^{n-2} q^k \sum_{j=1}^{k+1} s_j \overline{a}_{n-k-1+j}}_{\tilde{e}} \; [q']$

Majorons $\| \tau(\tilde{e}) \|$:

$$\| \tau(\tilde{e}) \| \leq q^{n-1} \| \tau(e) \| + \sum_{k=0}^{n-2} q^k \sum_{j=1}^{k+1} \| \tau(s_j) \| \times \| \tau(a_{n-k-1+j}) \|$$

$$\leq q^{n-1} \beta + \sum_{k=0}^{n-2} q^k \times n \times \beta \times q \times d^{3/2}$$

$$\leq q^{n-1} \beta + n \beta d^{3/2} q \times \frac{q^{n-1} - 1}{q - 1}$$

$q \geq 2$
$\Rightarrow \frac{1}{q-1} \leq \frac{2}{q}$

$$\leq q^{n-1} \beta + 2 n \beta d^{3/2} q^{n-1}$$

$$\leq q^{n-1} (3 n \beta d^{3/2})$$

□

Corollaire : Soient $q \geq 2$ premier, $n \geq 2$ des entiers et χ une distribution β-bornée pour un $\beta > 0$.
Il existe une réduction en temps polynomiale depuis le problème $MLWE_{n,q,\chi}$ vers le problème $MLWE_{1,q',\chi'}$ où

- $q' = q^n$
- χ' est la distribution uniforme sur $\{x \in R \mid \|\Sigma(x)\|_\infty \leq \beta'\}$
  avec $\beta' = 2^{d+1} \times 3nd^{5/2} q^{n-1} \beta$

La perte de l'avantage de la réduction est $\leq 2^{-t}$.

Remarque : si $\beta = \alpha q$ et $\beta' = \alpha' q'$, on voit que $\alpha' = \alpha \times 2^t \times \text{poly}(n,d)$. La perte de notre réduction est significativement plus grasse que celle de Albrecht et Deo.
Une autre différence (moins importante) est qu'on n'utilise pas les $\mathbb{Z}$-modules.

Preuve : exo 3.

Lemme 1 : Supposons q premier. Il y a une réduction de $MLWE_{n,q,\chi}$ vers $HNF\text{-}MLWE_{n,q,\chi}$ où le secret s est tiré selon χ.

Preuve : Tirer les $(a_i, b_i) \leftarrow D^{MLWE}_{n,q,\chi}$ jusqu'à ce qu'on ait n vecteurs $a_1, \dots, a_n$ t.q. $\overline{A} = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \in GL_n(R_q)$.
On note $\overline{b} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$ le vec correspondant

Ensuite, pour chaque échantillon $(a, b) \leftarrow D^{\text{LWE}}_{n,q,\chi}$,

on calcule $\underline{a} \times \boxed{\bar{A}^{-1}} = a'$

$$\boxed{\bar{A}}\ \underline{a}\ \Big|\, s + \Big|\, e = \Big|\, \bar{b}$$
$$\Big|\, b$$

$$\boxed{\bar{A}}\ \underline{a}\ \Big|\, \overbrace{\boxed{\bar{A}^{-1}} \times \boxed{\bar{A}} \times \Big|\, s}^{s'} + \Big|\, e = \Big|\, \bar{b}$$
$$\Big|\, b$$

$$\boxed{I_n}\ \underline{a'}\ \Big|\, s' + \Big|\, \bar{e} = \Big|\, \bar{b}$$
$$\Big|\, e \qquad\quad \Big|\, b$$

$$\underline{a'}\ \Big|\, s' + e = b$$
$$\Big|\, s' = \bar{b} - \bar{e}$$
$$\underline{a'}\ \Big|\, \bar{b} - \underline{a'}\ \Big|\, \bar{e} + e = b$$
$$-e + \underline{a'}\ \Big|\, \bar{e} = \underbrace{\underline{a'}\ \Big|\, \bar{b} - b}_{b'}$$

$b' = \langle a', \bar{e} \rangle - e$

Lemme 2 : Soit $e \in R$ t.q. $\|\tau(e)\| \leq \beta_1$ et soit χ' la distrib unif sur $\{x \in R \mid \|\tau(x)\| \leq \beta'\}$ avec

$\beta' =$

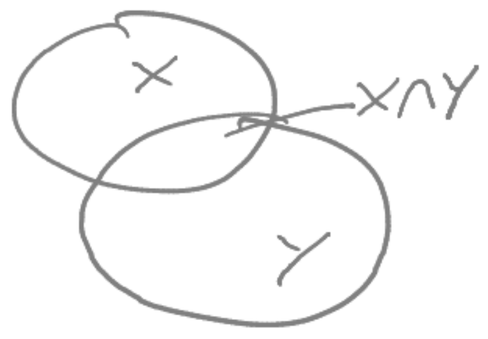
Alors $SD(\chi', \chi' + e) \leq 2^{-d}$.

Preuve : $X = \{ x \in R \mid \|\Sigma(x)\|_\infty \leq \beta' \}$

$$Y = \{ y \in R \mid \|\Sigma(y-e)\|_\infty \leq \beta' \}$$

$$SD(U(X), U(Y)) = \sum_{x \in X \setminus Y} \frac{1}{|X|} + \sum_{x \in Y \setminus X} \frac{1}{|Y|}$$

$$= 2 \sum_{x \in X \setminus Y} \frac{1}{|X|}$$



$$= 2 \times \frac{|X| - |X \cap Y|}{|X|}$$

Obj : $|X \cap Y| \geq c \times |X|$

$X \cap Y = \{ x \in R \mid \|\Sigma(x)\|_\infty \leq \beta' \text{ et } \|\Sigma(x) - \Sigma(e)\|_\infty \leq \beta' \}$

$\|\Sigma(e)\|_\infty \leq \|\Sigma(e)\|$
$\leq \|\Sigma(e)\|$

$\supseteq \{ x \in R \mid \|\Sigma(x)\|_\infty \leq \beta' - \beta \}$

$\Rightarrow |X \cap Y| \geq (\beta' - \beta)^d$

$X = \{ x \in R \mid \|\Sigma(x)\|_\infty \leq \beta' \}$ $\Rightarrow |X| \leq (\beta')^d$

$$\frac{|X \cap Y|}{|X|} \geq \left(1 - \frac{\beta}{\beta'}\right)^d \geqslant \left(1 - \frac{1}{2d \times 2^d}\right)^d \geqslant 1 - \frac{1}{2^{d+1}}$$

$$SD(U(X), U(Y)) \leq 2\left(1 - \left(1 - \frac{1}{2^{d+1}}\right)\right) \leq 2^{-d}$$

III) Cryptanalyse : Dans cette partie encore, $K = \mathbb{Q}[X]/X^4+1$

1) Sous-corps et théorie de Galois :

Définition : Un sous-corps K_1 de K est un sous-ensemble $K_1 \subseteq K$ tel que
- $\mathbb{Q} \subseteq K_1$
- K_1 est un corps.

Définition-Lemme : Tout corps K_1 contenant $\mathbb{Q}$ est un $\mathbb{Q}$-espace vectoriel. Le degré de K_1 est sa dimension en tant que $\mathbb{Q}$-ev (elle est finie si $K_1 \subseteq K$ car K est un $\mathbb{Q}$-ev de dimension d). $\exists P_1$ irred de deg d_1 t.q. $K_1 \sim \mathbb{Q}[X]/P_1(X)$

Exemple : $d = 4$, $K = \mathbb{Q}[X]/X^4+1$.

$K_1 = \{a + bX^2 \mid a, b \in \mathbb{Q}\}$ satisfait :
- $\mathbb{Q} \subseteq K_1 \subseteq K$
- K_1 est un corps : $(a+bX^2) + (c+dX^2) = (a+c) + (b+d)X^2$

$$(a+bX^2) \times (c+dX^2) = ac - db + (bc+ad)X^2$$

$$(a+bX^2)^{-1} = \frac{1}{a^2+b^2}(a - bX^2)$$

Définition : un automorphisme de K est une bijection :

$K \to K$ qui est :

* un morphisme d'anneau $\left(\begin{array}{l}\varphi(a+b)=\varphi(a)+\varphi(b)\\ \varphi(ab)=\varphi(a)\times\varphi(b)\end{array}\right)$

* qui fixe $\mathbb{Q}$: $\varphi(x)=x \quad \forall x \in \mathbb{Q}$

Si $P=X^d+1$, alors

Lemme : K admet d automorphismes $\varphi_1, \dots, \varphi_d$ définis par

$$\varphi_i : X \longmapsto X^{2i-1}$$

Preuve : Comme φ est un morphisme d'anneaux fixant $\mathbb{Q}$, et que $K = \left\{ \sum_{i=0}^{d-1} x_i X^i \mid x_i \in \mathbb{Q} \right\}$, φ est déterminé de façon unique par la valeur de $\varphi(X)$.

De plus, on sait que $\varphi(X)^d + 1 = \varphi(X^d+1) = \varphi(0) = 0$

Donc $\varphi(X)$ est une racine du polynôme Y^d+1.

Les racines de ce polynôme dans K sont exactement les

X^{2i-1} pour $1 \le i \le d$,

(on peut vérifier que $\left(X^{2i-1}\right)^d = \left(X^d\right)^{2i-1} = (-1)^{2i-1} = -1$

et il ne peut pas y avoir + de racines car ça fait d

et qu'elles sont toutes distinctes).

donc φ est l'un des φ_i.

Inversement, les φ_i sont bien des morphismes de K.

Def / Lemme : Les automorphismes de K forment un groupe pour la composition. Ce groupe est appelé groupe de Galois de K est noté $Gal(K)$.

Lemme : Soit H un sous-groupe de $Gal(K)$, et $K_H = \{x \in K \mid \varphi(x) = x \quad \forall \varphi \in H\}$. Alors K_H est un ss-corps de K.

Preuve : écrire les défs.

Théorème : Il y a une bijection entre les sous-corps de K et les sous-groupe H de $Gal(K)$, donnée par

$$H \longmapsto K_H \qquad (K_H \text{ ss-corps fixé par } H).$$

De plus, $deg(K_H) = \frac{deg(K)}{|H|}$

Exemple : exo 4

Lemme

Définition : Soit K_1 un sous-corps de K, et H le sous-groupe de $Gal(K)$ t.q. $K_1 = K_H$. On définit la trace et la norme relative par :

$$Tr_{K/K_1} : K \longrightarrow K_1, \quad x \longmapsto \sum_{\varphi \in H} \varphi(x)$$

$$N_{K/K_1} : K \longrightarrow K_1, \quad x \longmapsto \prod_{\varphi \in H} \varphi(x)$$

Preuve que $\sum_{\varphi\in H} \varphi(x) \in K_1$ (et que $\prod_{\varphi\in H} \varphi(x) \in K_1$)

Soit $\varphi_0 \in H$, alors $\varphi_0\left(Tr_{K/K_1}(x)\right) = \sum_{\varphi\in H} \varphi_0\circ\varphi(x)$

$= \sum_{\varphi'\in H} \varphi'(x) = Tr_{K/K_1}(x)$

(on utilise le fait que $H \longrightarrow H$, $\varphi \longmapsto \varphi_0\circ\varphi$ est une bijection car H est un groupe).

Par définition de $K_1 = K_H = \{y\in K \mid \varphi(y)=y \ \forall \varphi\in H\}$,

on conclut que $Tr_{K/K_1}(x) \in K_1$.

Idem pour la norme.

Lemme :

- $Tr_{K/K'}$ est $\mathbb{Q}$-linéaire ($Tr(\alpha x+\beta y)=\alpha Tr(x)+\beta Tr(y)$ pour $x,y\in K$, $\alpha,\beta\in\mathbb{Q}$) et n'est pas la fonction nulle.
- $N_{K/K'}$ est multiplicative ($N(xy)=N(x)N(y)$)

Preuve : . linéarité et multiplicativité facile.

. $Tr \neq 0$ car $Tr_{K/K'}(1) = \sum_{\varphi\in H} \varphi(1) = \sum_{\varphi\in H} 1$

$= |H|$.

Lemme : Soit $x \in K$ et $\varphi \in Gal(K)$, alors $\|\tau(x)\| = \|\tau(\varphi(x))\|$.

Preuve : $\tau(\varphi(x))$ a les $\tilde{m}$ coordonnées que $\tau(x)$ mais permutées.

Soit $\sigma_i : K \hookrightarrow \mathbb{C}$ un plongement complexe de K.

$$a(X) \longmapsto a(\xi_i)$$

On a $\sigma_i \circ \varphi : K \hookrightarrow \mathbb{C}$

$$a(X) \longmapsto \sigma_i(\varphi(a)) = \sigma_i(a(\varphi(X)))$$

$$= a(\sigma_i(\varphi(X)))$$

Mais on a vu que φ est de la forme $\varphi(X) = X^{2j-1}$ pour $j \in \{1, \dots, d\}$

Donc $\sigma_i(\varphi(X)) = \sigma_i(X^{2j-1}) = \underbrace{\xi_i^{2j-1}}_{\xi_k^{''}}$ $\xi_i = \exp\left(2i\pi \times \frac{2i-1}{2d}\right)$

pour un certain k.

Donc $\sigma_i = \sigma_k$ et $\sigma \longrightarrow \sigma \circ \varphi$ est une bijection sur l'ensemble des plongements complexes de K.

↳ exo 5

2) Un algorithme pour trouver de vecteurs courts dans certains réseaux idéaux :

Définition : Soit $\mathfrak{a}$ un idéal. Le groupe de décomposition de $\mathfrak{a}$ est $\{\varphi \in Gal(K) \mid \varphi(\mathfrak{a}) = \mathfrak{a}\}$, où $\varphi(\mathfrak{a}) = \{\varphi(x) \mid x \in \mathfrak{a}\}$.

Ce groupe contient toujours l'identité. Dans la plupart des cas, le groupe de décomposition de $\mathfrak{a}$ est $\{id\}$, mais parfois il est plus gros, et dans ce cas on peut résoudre SVP dans $\mathfrak{a}$ plus rapidement que d'habitude.

Idée principale : si $x \in K$ est tel que $\varphi(x) = x \quad \forall \varphi \in H$, alors $x \in K_H$ ($\mathbb{Z}$-corps stricts de K si $H \neq \{id\}$).
C'est pareil pour des idéaux : si $\varphi(\mathfrak{a}) = \mathfrak{a} \quad \forall \varphi \in H$, alors "moralement" $\mathfrak{a} \subseteq K_H$. On va le prouver de façon + simple.

Dans toute la suite, on fixe $\mathfrak{a}$ un idéal, H son groupe de décomposition et K_H le $\mathbb{Z}$-corps de K fixé par H.

Lemme : $\mathfrak{b} := \mathfrak{a} \cap K_H$ est un idéal de $K_H \cap R$, et le réseau idéal associé $\tau(\mathfrak{b}) \subseteq \mathbb{R}^d$ est de rang $\frac{d}{|H|}$.

Preuve : c'est vrai $\forall$ $\mathbb{Z}$-corps K_1 de K. Le fait que $\mathfrak{b}$ est stable par addition et mult par un élt de $K_H \cap R$ peut se vérifier facilement. Comme c'est un idéal de K_H qui a un degrée $d_H = \frac{d}{|H|}$, le réseau associé est de rang $d_H = \frac{d}{|H|}$.

Lemme : $\lambda_1(\tau(\mathfrak{b})) \leq |H| \times \lambda_1(\tau(\mathfrak{a}))$

Preuve : exo 6

Soit $s \in \mathfrak{a}$ t.q. $\|\tau(s)\| = \lambda_1(\tau(\mathfrak{a}))$.

On définit $v_i = s x^{i-1}$. on a $\|\tau(v_i)\| = \|\tau(s)\| = \lambda_1(\tau(\mathfrak{a}))$

Soit $w_i = \mathrm{Tr}_{K/K_H}(v_i)$. Montrons qu'il existe $i \in [1, \dots, d]$ t.q. $w_i \neq 0$.

Supposons par l'absurde $\mathrm{Tr}_{K/K_H}(v_i) = 0 \ \forall\, i$.

Les v_i sont $\mathbb{Q}$-linéairement indep (cf exo 2) de rk d,

donc $\forall x \in K$, $\exists x_1, \dots, x_d \in \mathbb{Q}$ t.q. $x = \sum x_i v_i$.

Mais alors $\mathrm{Tr}_{K/K_H}(x) = \sum_i x_i \mathrm{Tr}_{K/K_H}(v_i) = 0$.

Or on a vu que Tr_{K/K_H} n'est pas la fct nulle : contradiction.

Soit i_0 t.q. $w_{i_0} \neq 0$. On a $w_{i_0} \in \mathfrak{a}$ car

$$w_{i_0} = \sum_{\varphi \in H} \varphi(v_{i_0}) \quad \text{et } \varphi(\mathfrak{a}) = \mathfrak{a} \text{ donc } \varphi(v_{i_0}) \in \mathfrak{a} \ \forall \varphi \in H.$$

De plus, $w_{i_0} \in K_H$, donc $w_{i_0} \in \mathfrak{b}$ (et est non nul).

Il reste à majorer sa taille :

$$\|\tau(w_{i_0})\| = \left\|\tau\left(\sum_{\varphi \in H} \varphi(v_{i_0})\right)\right\| \leq \sum_{\varphi \in H} \|\tau(\varphi(v_{i_0}))\|$$

$$= |H| \times \|\tau(v_{i_0})\|$$

$$= |H| \times \lambda_1(\tau(\mathfrak{a}))$$

□

On peut maintenant décrire l'algorithme pour calculer un vecteur court dans $\mathfrak{a}$.

Algorithme :

Entrée : $\mathfrak{a}$ un idéal

Sortie : $s \in \mathfrak{a} \setminus \{0\}$

1. Calculer H le groupe de décomposition de $\mathfrak{a}$, et K_H le ss-gp fixé par H.
2. Calculer $\mathfrak{b} = \mathfrak{a} \cap K_H$.
3. Résoudre SVP_γ dans $\tau(\mathfrak{b})$ $\rightsquigarrow$ vecteur $s \in \mathfrak{b} \setminus \{0\}$ t.q. $\|\tau(s)\| \leq \gamma \lambda_1(\tau(\mathfrak{b}))$

Renvoyer s.

Thm : l'algo tourne en temps poly sauf l'appel à SVP_γ, qui est fait pour un réseau de dim $\frac{d}{|H|}$.

Preuve : - hyps poly admis.
- $\dim(\tau(\mathfrak{b})) = \frac{d}{|H|}$ on l'a déjà vu avant.

Thm : l'algo résout $SVP_{\gamma'}$ dans $\mathfrak{a}$, avec $\gamma' = \gamma \times |H|$.

Preuve : $s \in \mathfrak{b} \subseteq \mathfrak{a}$, $s \neq 0$ et $\|\tau(s)\| \leq \gamma \lambda_1(\tau(\mathfrak{b}))$
$\leq \gamma \times |H| \times \lambda_1(\tau(\mathfrak{a}))$
par le lemme précédent

Remarque : $\tau(\mathfrak{a})$ est un réseau de dim d
$\rightsquigarrow$ l'algo est intéressant seulement si $|H| > 1$
(sinon SVP_γ en dim d dans $\tau(\mathfrak{a})$ est aussi court et meilleur)
$\rightsquigarrow$ ça concerne très peu d'idéaux.

3) Le problème NTRU :

Définition : Soit $q \geq 2$ un entier, et $B > 0$.
Une instance de $NTRU_{q,B}$ est un $h \in R$ t.q.
$\exists (f, g) \in R^2 \setminus (0,0)$ qui satisfont :

- $gh = f \ [q]$ ($h = f/g \ [q]$ si g inversible)
- $\|\tau(f)\|, \|\tau(g)\| \leq B$

Il faut imaginer $B \ll \sqrt{q}$. Dans ce cas, les instances de $NTRU_{q,B}$ sont peu fréquentes dans R.

Lemme : Si q est premier et $\neq 2$, alors la proportion d'éléments de R qui sont des $NTRU_{q,B}$ instances est $\leq \left(\frac{2^5 B^2}{q}\right)^d$.

Preuve : admis

exo 7

Lemme (plus faible) : si $K = \mathbb{Q}^r$ et q premier, la proportion d'éléments de $R = \mathbb{Z}$ qui sont des $NTRU_{q,B}$ instances est $\leq \frac{(2B+1)^2}{q}$.

On peut supposer sans perte de généralité que $B < q$ (sinon $\frac{(2B+1)^2}{q} > 1$).

Preuve : Déjà, il suffit de regarder h mod q.
Ensuite, chaque couple $(f, g) \in \mathbb{Z}^2 \setminus (0,0)$ t.q. $|f|, |g| \leq B$ ne peut servir de témoin qu'à un seul h :
si $gh = f \ [q]$, alors g inversible mod q.
s'il ne l'était pas, on aurait $g = 0 \ [q]$ (q premier)
donc $f = 0 \ [q]$ et comme $|f|, |g| \leq B < q$, $g = f = 0$.
Donc $g \neq 0$ et $h = f/g \ [q]$ est unique mod q.

Ensuite, il suffit de compter le nb de paires (f,g) comme avant pour avoir une majoration sur le nb de h qui soit des instances de NTRU.

Exo 7

Définition : Soient $q \geq 2$, $B > 0$ et ψ une distributions sur les instances de $NTRU_{q,B}$.

* (search) $NTRU_{q,B,\psi}$: étant donné $h \leftarrow \psi$, retrouver $(f',g') \in R^2$, avec $\cdot (f',g') \neq 0$
  $\cdot \|\tau(f')\|, \|\tau(g')\| \leq B$
  $\cdot f' = g'h \ [q]$

* décision dec-$NTRU_{q,B,\psi}$: distinguer ψ de $\mathcal{U}(R_q)$.

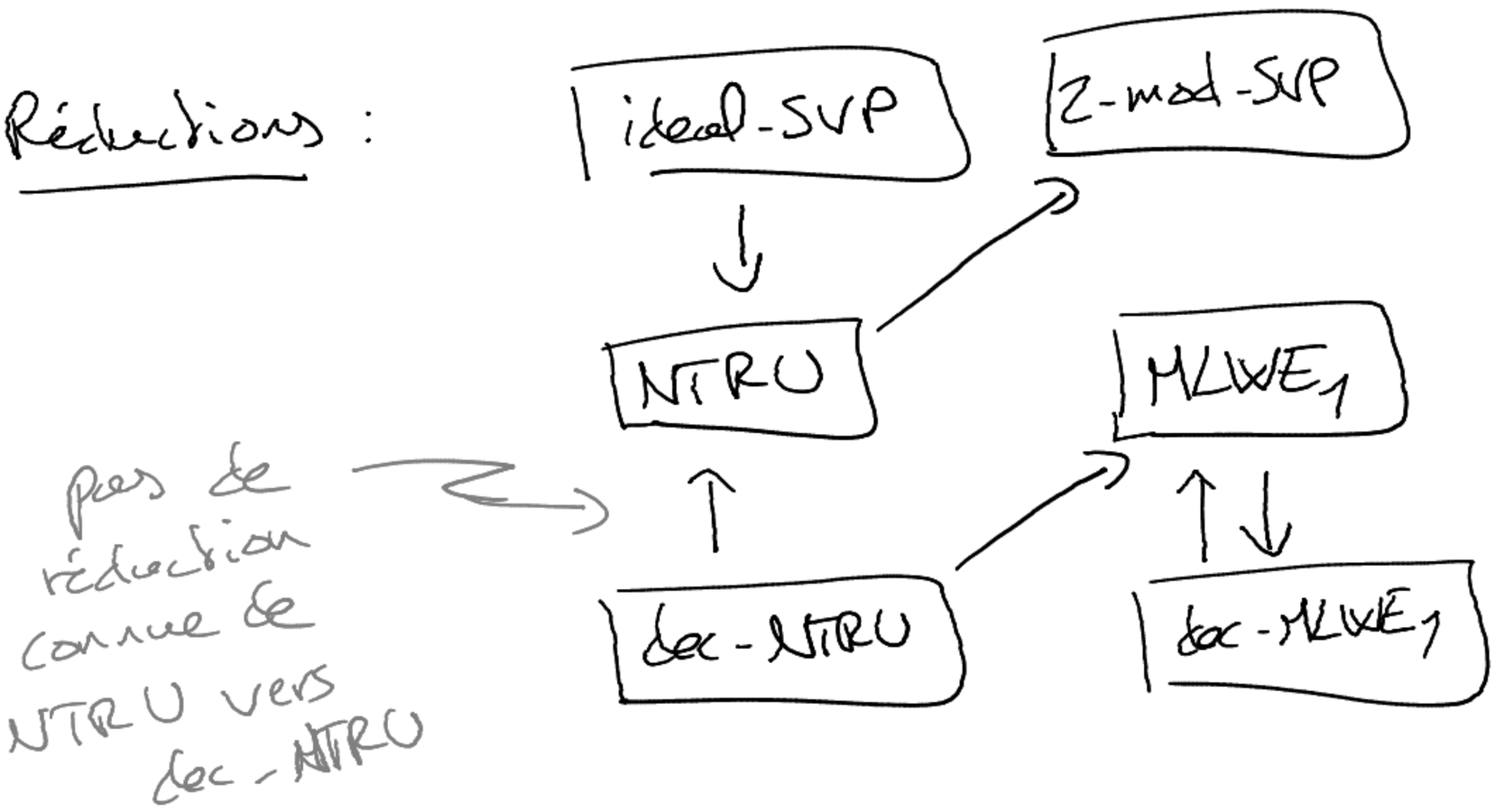
Remarque : • la solution de search-NTRU n'est pas unique.
Par ex, si (f,g) est solution, (fX, gX) aussi.

• En pratique, ψ est obtenue en choisissant χ une distrib de petits elts sur R (par ex Gaussien), puis en tirant $(f,g) \leftarrow \chi^2$ jusqu'à ce que g soit inversible mod q, puis en renvoyant $h = f/g \ [q]$.

Exo 7 suite

3.1) Propriétés de NTRU :

Réductions :



NTRU est un pb de réseau :

Définition : Soit $q \geq 2$ et $h \in R$. Le module NTRU associé à h est le module de rang 2 $\subseteq R^2$ engendré par $\begin{pmatrix}1\\h\end{pmatrix}$ et $\begin{pmatrix}0\\q\end{pmatrix}$. On note $\mathcal{M}_h$ ce module.

Lemme : $\mathcal{M}_h = \{(g,f)^T \in R^2 \mid gh = f \ [q]\}$

Preuve : • Si $gh = f \ [q]$, $\exists r \in R$ t.q. $gh = f + qr$

et alors $\begin{pmatrix}g\\f\end{pmatrix} = g \times \begin{pmatrix}1\\h\end{pmatrix} - r \times \begin{pmatrix}0\\q\end{pmatrix} \in \mathcal{M}_h$

• inversement, si $\begin{pmatrix}u\\v\end{pmatrix} = x\begin{pmatrix}1\\h\end{pmatrix} + y\begin{pmatrix}0\\q\end{pmatrix} \in \mathcal{M}_h$, $x, y \in R$

alors $x = u$ et $xh + yq = v \iff uh = v \ [q]$

⚠ Français

Corollary : Finding a trapdoor (f,g) for an NTRU instance h = solving SVP in the rk-2 module lattice $\mathcal{M}_h$.

Rk : $\mathcal{M}_h$ is a specific module lattice. NTRU is a special case of mod-SVP in rk 2, but it is a priori not equivalent to it.

3.2) Algorithme pour NTRU lorsque q est grand :

Lemme : Soit h une instance de $NTRU_{q,B}$,

alors $\lambda_1(\tau(\mathcal{M}_h)) = \lambda_2(\tau(\mathcal{M}_h)) = \cdots = \lambda_d(\tau(\mathcal{M}_h)) \leq \sqrt{2}B$

et $\lambda_{d+1}(\tau(\mathcal{M}_h)) = \cdots = \lambda_{2d}(\tau(\mathcal{M}_h)) \geq \dfrac{\det(\tau(\mathcal{M}_h))^{1/d}}{\sqrt{2}B}$

Proof : $\lambda_1 = \cdots = \lambda_d$ and $\lambda_{d+1} = \cdots = \lambda_{2d}$ par module

- $\lambda_1 \leq \left\| \begin{pmatrix} g \\ g \end{pmatrix} \right\| \leq \sqrt{2}B$
- $\prod \lambda_i \geq \det(\tau(\mathcal{M}_h))$

$\Leftrightarrow \prod_{i \geq d+1} \lambda_i \geq \dfrac{\det(\tau(\mathcal{M}_h))}{\prod_{i \leq d} \lambda_i}$

$\Leftrightarrow \lambda_{d+1}^{d} \geq \dfrac{\det(\tau(\mathcal{M}_h))}{\lambda_1^{d}}$

$\Leftrightarrow \lambda_{d+1} \geq \dfrac{\det(\tau(\mathcal{M}_h))}{\lambda_1}$

Lemme : $\det(\tau(\mathcal{M}_h)) = q^d \times d^d$

Preuve : admis

Conclusion : Si $B \ll \sqrt{q}$, alors

$$\lambda_1(\tau(\mathcal{H}_h)) = \dots = \lambda_d(\tau(\mathcal{H}_h)) \ll \lambda_{d+1}(\tau(\mathcal{H}_h)) = \dots = \lambda_{2d}(\tau(\mathcal{H}_h))$$

EC'17

Theorème (Kirchner-Fouque) : Soit $\varepsilon > 0$.

Il existe un algorithme polynomial heuristique qui résout $dec\text{-}NTRU_{q,B}$ pour $B = poly(d)$ et $q = \exp(d^{1/2+\varepsilon})$