

# TD3 : IDÉAUX PREMIERS ET MAXIMAUX ; POLYNÔMES ; APPROXIMATION

Diego Izquierdo

*Les exercices 1, 4 et 5 sont à préparer avant le TD. Pendant la séance de TD, les exercices seront traités dans l'ordre suivant : 1, 4, 5, 11, 12, 15. Si le temps le permet nous traiterons aussi l'exercice 8.*

Pour ce TD, on rappelle que :

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \{(x_n)_n \in \prod_n \mathbb{Z}/p^n\mathbb{Z} \mid \forall n \in \mathbb{N}, x_{n+1} \equiv x_n \pmod{p^n}\},$$

$$A[[T]] = \varprojlim_n A[T]/(T^n) = \left\{ \sum_{i=0}^{\infty} a_i T^i \mid a_i \in A \right\}.$$

### Exercice 1 (à préparer) : Vrai ou faux ?

Soit  $A$  un anneau.

1. Si  $A$  est factoriel, alors tout idéal premier non nul est maximal.
2. Le quotient d'un anneau factoriel par un idéal premier est factoriel.
3. Si  $A$  est un anneau factoriel et  $a$  et  $b$  sont des éléments non nuls de  $A$ , on a  $(a, b) = (a \wedge b)$ .
4. Si  $A$  est un anneau factoriel et  $a$  et  $b$  sont des éléments non nuls de  $A$ , on a  $(a) \cap (b) = (a \vee b)$ .
5. Dans  $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$ , l'idéal (3) n'est pas premier, mais il est contenu dans exactement deux idéaux premiers, qui sont maximaux.
6. L'anneau  $\mathbb{Z}[(X_n)_{n \in \mathbb{N}}]$  est factoriel.
7. Le polynôme  $(X + Y)^{100} + 2(X + 5)^{98}Y + 57X^{87}Y^5 \in \mathbb{C}[X, Y]$  est irréductible.
8. Il existe un morphisme d'anneaux injectif de  $\mathbb{Z}[X]/(2X^2 + 3X + 2)$  dans  $\mathbb{C}$ .

### Exercice 2 : Vrai ou faux ? Le retour

Soit  $A$  un anneau.

1. Si  $A$  est intègre, tout élément irréductible engendre un idéal premier.
2. Si  $A$  est factoriel et si  $a$  et  $b$  sont deux éléments de  $A$  premiers entre eux, alors il existe un isomorphisme  $A/(ab) \cong A/(a) \times A/(b)$ .
3. L'idéal (89) est premier dans  $\mathbb{Z}[i]$ .
4. Si  $P \in \mathbb{C}[X, Y]$  est tel que  $P(X, 0)$  et  $P(0, Y)$  sont irréductibles, alors  $P$  est irréductible.

5. L'anneau des nombres décimaux est isomorphe à  $\mathbb{Z}[X]/(10X - 1)$ .
6. On a un isomorphisme d'anneaux  $(\mathbb{R}[X]/(X^5(X^4 - 1)))^{\text{red}} \cong \mathbb{R}^3 \times \mathbb{C}$ .

### Exercice 3 : Corps et idéaux

Soit  $A$  un anneau commutatif unitaire.

1. On suppose  $A$  intègre et que  $A$  possède un nombre fini d'idéaux. Montrer que  $A$  est un corps.
2. On suppose que  $A$  possède un nombre fini d'idéaux. Montrer que tout idéal premier de  $A$  est maximal.
3. On suppose que tout idéal propre de  $A$  est premier. Montrer que  $A$  est un corps.

### Exercice 4 (à préparer) : Anneaux principaux et anneaux factoriels de dimension au plus 1

Soit  $A$  un anneau factoriel tel que tout idéal premier non nul est maximal.

1. Soient  $x, y$  des éléments non nuls de  $A$ , que l'on suppose premiers entre eux. Montrer qu'il existe  $u, v \in A$  vérifiant  $ux + vy = 1$ .
2. Soit  $I$  un idéal non nul de  $A$ . Montrer qu'il existe  $d \in I$  non nul qui est un pgcd de tous les éléments de  $I$ .
3. Conclure que  $A$  est principal.

### Exercice 5 (à préparer) : Produits d'idéaux premiers

Considérons les anneaux  $A = \mathbb{Z}[i\sqrt{11}]$  et  $B = \mathbb{Z}[i\sqrt{13}]$ .

1. Montrer que  $A$  et  $B$  ne sont pas des anneaux factoriels.
2. Faire la liste des idéaux premiers de  $A$  qui contiennent l'idéal (2). En déduire que l'idéal (2) ne s'écrit pas comme produit d'idéaux premiers de  $A$ .
3. À l'inverse, montrer que les idéaux (2), (3) et (7) s'écrivent bien comme des produit d'idéaux premiers de l'anneau  $B$ .

### Exercice 6 : Idéaux premiers d'un anneau de polynômes

Soit  $A$  un anneau principal de corps des fractions  $K$ . Nous allons caractériser les idéaux premiers et maximaux de  $A[X]$ .

1. Soit  $I$  un idéal premier non nul de  $A[X]$ .
  - (a) Montrer que  $I \cap A$  est un idéal maximal de  $A$ .
  - (b) On suppose  $I \cap A = 0$ .
    - (i) Soit  $J$  l'idéal de  $K[X]$  engendré par  $I$ . Montrer que  $I = J \cap A[X]$ .
    - (ii) Montrer que  $I$  est principal, engendré par un polynôme non constant, irréductible et primitif.
  - (c) On suppose que  $I \cap A$  est non nul, et on pose  $k = A/(I \cap A)$ .

Montrer que soit  $I$  est engendré par  $I \cap A$ , soit  $I$  est engendré par  $I \cap A$  et par un polynôme  $P \in A[X]$  dont l'image dans  $k[X]$  est irréductible.

- (d) Dédurre de ce qui précède que les idéaux premiers de  $A[X]$  sont :  
 (0) ; les idéaux principaux engendrés par un polynôme non constant, irréductible et primitif ; les idéaux engendrés par un idéal maximal de  $A$  ; les idéaux engendrés par un idéal maximal  $\mathfrak{m}$  de  $A$  et un polynôme de  $A[X]$  dont la réduction modulo  $\mathfrak{m}$  est irréductible. Lesquels sont maximaux ?
2. Quels sont les idéaux premiers (resp. maximaux) de  $\mathbb{C}[X, Y]$  ?
  3. Quels sont les idéaux premiers (resp. maximaux) de  $\mathbb{Z}[X]$  ?
  4. Soit  $\alpha$  un entier algébrique, c'est-à-dire un élément de  $\mathbb{C}$  racine d'un polynôme unitaire irréductible à coefficients dans  $\mathbb{Z}$ . Montrer que tout idéal premier non nul de  $\mathbb{Z}[\alpha]$  est maximal.

### Exercice 7 : Idéaux premiers de $\mathcal{C}([0, 1], \mathbb{R})$

1. Soient  $A$  un anneau et  $I$  un idéal de  $A$ . Notons  $J$  l'intersection des idéaux premiers de  $A$  contenant  $I$ . Le but de cette question est de montrer que  $\sqrt{I} = J$ .
  - (a) Montrer que  $\sqrt{I}$  est contenu dans  $J$ .
  - (b) Réciproquement, soit  $a \in A \setminus \sqrt{I}$ , et considérons  $\mathcal{E}$  la famille constituée des idéaux qui contiennent  $I$  mais qui ne contiennent aucune puissance de  $a$ . Montrer que  $\mathcal{E}$  possède un élément maximal (pour l'inclusion), qui est un idéal premier de  $A$ . En déduire que  $a \notin J$ .
  - (c) Conclure.

Soit  $\mathcal{C}$  l'anneau des fonctions continues de  $[0, 1]$  dans  $\mathbb{R}$ .

2. Quels sont les idéaux maximaux de  $\mathcal{C}$  ? Sont-ils principaux ?
3. Soit  $I = \{f : [0, 1] \rightarrow \mathbb{R} \mid \forall m \in \mathbb{N}, \lim_{x \rightarrow 0} \frac{f(x)}{x^m} = 0\}$ . Montrer que  $I = \sqrt{I}$  (on dit que  $I$  est un idéal radical). L'idéal  $I$  est-il premier ?
4. En déduire que  $\mathcal{C}$  possède des idéaux premiers non maximaux.

### Exercice 8 : Points en géométrie algébrique

1. On considère les anneaux :

$$\mathbb{C}[X], \mathbb{R}[X]/(X^2 + X + 1), \mathbb{R}[X]/(X^3 - 6X^2 + 11X - 6), \mathbb{R}[X]/(X^4 - 1).$$

Déterminer les morphismes de  $\mathbb{R}$ -algèbres de ces anneaux à valeurs dans  $\mathbb{R}$  (resp.  $\mathbb{C}$ ).

2. On considère l'anneau  $\mathbb{R}[X]/(X^5)$ . Déterminer les morphismes de  $\mathbb{R}$ -algèbres de cet anneau à valeurs dans  $\mathbb{R}$  (resp.  $\mathbb{C}$ , resp.  $\mathbb{R}[\varepsilon]$ ).
3. (a) Soit  $k$  un corps. Montrer qu'il existe une  $k$ -algèbre  $A$  définissant

- une “variété”  $X$  telle que, pour chaque  $k$ -algèbre  $B$ , on ait une bijection  $X(B) \cong B^\times$ . Calculer  $X(k[\varepsilon])$ .
- (b) Même question pour  $X(B) \cong GL_n(B)$ .
  - (c) Même question pour  $X(B) \cong \mu_n(B)$  où  $\mu_n(B)$  désigne l’ensemble des racines  $n$ -ièmes de l’unité dans  $B$ .

**Exercice 9 : L’anneau  $\hat{\mathbb{Z}}$**

Pour  $n$  et  $m$  deux entiers naturels non nuls tels que  $n|m$ , on note  $\pi_{m,n}$  la projection naturelle  $\mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ . On pose :

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \{(x_n)_n \in \prod_n \mathbb{Z}/n\mathbb{Z} \mid \forall (n, m) \in (\mathbb{N}^*)^2, n|m \Rightarrow \pi_{m,n}(x_m) = x_n\}.$$

En notant  $\mathcal{P}$  l’ensemble des nombres premiers, montrer que  $\hat{\mathbb{Z}} \cong \prod_{p \in \mathcal{P}} \mathbb{Z}_p$ .

**Exercice 10 : Racines de l’unité dans  $\mathbb{Z}_p$**

Soit  $p$  un nombre premier impair. Sans utiliser le lemme de Hensel, montrer que le groupe des racines de l’unité dans  $\mathbb{Z}_p$  est cyclique d’ordre  $p - 1$ . Après avoir remarqué que  $\mathbb{Z}_p$  est intègre, en déduire que, si  $p$  et  $l$  sont deux nombres premiers impairs distincts, alors les corps des fractions de  $\mathbb{Z}_p$  et  $\mathbb{Z}_l$  ne sont pas isomorphes.

**Exercice 11 : Entiers  $p$ -adiques et équations**

Soit  $p$  un nombre premier. On munit  $\mathbb{Z}_p$  de la topologie induite par la topologie produit sur  $\prod_n \mathbb{Z}/p^n\mathbb{Z}$ .

1. Montrer que  $\mathbb{Z}_p$  est compact.
2. Soit  $m > 0$ . Soit  $f \in \mathbb{Z}[X_1, \dots, X_m]$ . Montrer que l’équation  $f(x_1, \dots, x_m) = 0$  a des solutions dans  $\mathbb{Z}_p$  si, et seulement si, elle a des solutions dans  $\mathbb{Z}/p^r\mathbb{Z}$  pour tout  $r$ .

**Exercice 12 : Lemme de Hensel et applications**

1. Soient  $A$  un anneau et  $I$  un idéal de  $A$ .
  - (i) Soit  $n$  entier naturel non nul. Soient  $f \in A[X]$  et  $x \in A$  tels que  $f(x) \equiv 0 \pmod{I^n}$  et  $f'(x) \in (A/I)^\times$ . Montrer qu’il existe  $y \in A$  tel que  $y \equiv x \pmod{I^n}$  et  $f(y) \equiv 0 \pmod{I^{n+1}}$ . Montrer que si  $z \in A$  est tel que  $z \equiv x \pmod{I^n}$  et  $f(z) \equiv 0 \pmod{I^{n+1}}$ , alors  $z \equiv y \pmod{I^{n+1}}$ .
  - (ii) Soient  $f \in A[X]$  et  $x \in A$  tels que  $f(x) \equiv 0 \pmod{I}$  et  $f'(x) \in (A/I)^\times$ . Déduire de la question précédente qu’il existe un unique  $y \in \varprojlim_n A/I^n$  tel que son image dans  $A/I$  coïncide avec celle de  $x$  et  $f(y) = 0$ .
2. Est-ce que 14 possède une racine carrée dans  $\mathbb{Z}_5$  ? Dans  $\mathbb{Z}_7$  ? Dans  $\mathbb{Z}_{11}$  ?

3. Soit  $p$  un nombre premier. En utilisant le lemme de Hensel, montrer que  $\mathbb{Z}_p$  possède  $p - 1$  racines  $p - 1$ -ièmes de l'unité.
4. Montrer qu'il existe  $f(T) \in \mathbb{Z}[[T]]$  tel que  $f(T)^5 + f(T) + T = 0$ . En écrivant  $f(T) = \sum_{n \geq 0} a_n T^n$ , calculer  $a_n$  pour  $n \leq 6$ .

**Exercice 13 : Approximations plus subtiles**

1. Montrer que 28 est un cube dans  $\mathbb{Z}_3$ .
2. Montrer qu'il existe  $f(T) \in \mathbb{Q}[[T]]$  tel que  $f(T)^5 + Tf(T) + T^3 = 0$ .

**Exercice 14 : Approximation dans  $\mathbb{Z}[i]$**

Existe-t'il  $z \in \mathbb{Z}[i]/(51^{100})$  tel que  $z^2 = 2$  ?

**Exercice 15 : Partiel 2013**

Soit  $n \geq 1$  un entier. Montrer que :

1. Il existe  $u_n \in \mathbb{R}[X]$  tel que  $u_n \equiv X \pmod{(X^2 + 1)}$  et  $u_n^2 + 1 \equiv 0 \pmod{(X^2 + 1)^n}$ .
2. La classe de  $u_n$  modulo  $(X^2 + 1)^n$  est unique. Donner une formule pour la classe de  $u_{n+1}$  modulo  $(X^2 + 1)^{n+1}$  en fonction de  $u_n$ .
3. Les formules :

$$\alpha_n : \mathbb{C}[Y] \rightarrow \mathbb{R}[X]/(X^2 + 1)^n, a + bi \mapsto a + bu_n, Y \mapsto X - u_n,$$

définissent un morphisme surjectif de  $\mathbb{R}$ -algèbres.

4.  $\alpha_n$  définit un isomorphisme de  $\mathbb{R}$ -algèbres :

$$\mathbb{C}[Y]/(Y^n) \rightarrow \mathbb{R}[X]/(X^2 + 1)^n.$$

5. Pour tout polynôme non constant  $f \in \mathbb{R}[X]$ , il existe un isomorphisme :

$$\mathbb{R}[X]/(f) \cong \prod_{j=1}^N \mathbb{R}[X]/(X^{a_j}) \times \prod_{k=1}^M \mathbb{C}[Y]/(Y^{b_k}).$$

**Exercice 16 : Anneau des séries formelles**

1. Soit  $k$  un corps. Montrer que  $k[[T]]$  est un anneau euclidien possédant exactement un idéal premier.
2. Exhiber un élément de  $\mathbb{Z}[X]$  qui n'est pas irréductible, mais qui est irréductible dans  $\mathbb{Z}[[X]]$ .
3. Exhiber un élément irréductible de  $\mathbb{Z}[X]$ , qui n'est pas irréductible dans  $\mathbb{Z}[[X]]$ .
4. Les questions concernant la factorialité de  $A[[T]]$  sont difficiles. Pierre Samuel a montré en 1960 les faits suivants :

- Si  $A$  est un anneau principal et  $n$  un entier naturel, alors l'anneau  $A[[T_1, T_2, \dots, T_n]]$  est factoriel ;
- Il existe des anneaux factoriels  $A$  tels que  $A[[T]]$  n'est pas factoriel : par exemple,  $A = \mathbb{Z}/2\mathbb{Z}[X, Y, Z]/(Z^2 - X^3 - Y^7)$ .

**Exercice 17 (difficile <sup>1</sup>) : Produit de deux sous-anneaux**

Soient  $A$  un anneau et  $I$  un idéal. Montrer que, si  $A/I$  est un produit non trivial de deux sous-anneaux, il en est de même pour  $\hat{A} = \varprojlim_n A/I^n$ .

**Exercice 18 : Lemme de Hensel bis**

1. Soit  $p$  un nombre premier. Soient  $f_1, \dots, f_n$  des éléments de  $\mathbb{Z}[X_1, \dots, X_m]$ . Considérons le système d'équations (S) :

$$\begin{cases} f_1(x_1, \dots, x_m) = 0 \\ f_2(x_1, \dots, x_m) = 0 \\ \dots \\ f_n(x_1, \dots, x_m) = 0 \end{cases}$$

Soit  $x \in (\mathbb{Z}/p\mathbb{Z})^m$  une solution de (S). On suppose que le rang de la matrice jacobienne  $J(x) = \left( \frac{\partial f_i}{\partial x_j}(x) \right)_{i,j} \in \mathcal{M}_{n,m}(\mathbb{Z}/p\mathbb{Z})$  est égal à  $n$ . Montrer que le système (S) possède une unique solution dans  $\mathbb{Z}_p$  qui relève  $x$ .

2. Trouver tous les nombres premiers  $p$  tels que l'équation  $x^2 + 1 = 3y^2$  a des solutions dans  $\mathbb{Z}_p$ .
3. Combien de solutions possède le système d'équations :

$$\begin{cases} x^2 + 1 = 3y^2 \\ x^3 + 3y^5 + y = 2 \end{cases}$$

dans  $\mathbb{Z}_5$  ?

**Exercice 19 (culturel) : Topologie sur les entiers  $p$ -adiques**

Soit  $p$  un nombre premier. Comme dans l'exercice 11, on munit  $\mathbb{Z}_p$  de la topologie induite par la topologie produit sur  $\prod_n \mathbb{Z}/p^n\mathbb{Z}$ . Ainsi  $\mathbb{Z}_p$  est un anneau topologique.

1. Pour  $x = (x_n)_n \in \mathbb{Z}_p$ , on pose  $v_p(x) = \max\{n \in \mathbb{N} / x_n = 0\}$ . Montrer que :

$$d_p(x, y) = p^{-v_p(x-y)}$$

définit une distance sur  $\mathbb{Z}_p$ .

---

1. Pour une version plus facile de l'exercice, on pourra aller voir l'exercice I.3.11 dans le polycopié.

2. En déduire que  $\mathbb{Z}_p$  est métrisable, puis que  $\mathbb{Z}_p$  est complet.
3. Montrer que  $\mathbb{Z}$  s'injecte dans  $\mathbb{Z}_p$ . Quelle fonction induit  $v_p$  sur  $\mathbb{Z}$  ?
4. Montrer que  $\mathbb{Z}_p$  est le complété de  $\mathbb{Z}$  (où  $\mathbb{Z}$  est bien sûr muni de la distance  $d_p$ ) ?

### Exercice 20 (culturel) : L'anneau des entiers $p$ -adiques

On garde les notations de l'exercice précédent.

1. Rappeler pourquoi  $\mathbb{Z}_p$  est un anneau intègre.
- Soit  $\mathbb{Q}_p$  le corps des fractions de  $\mathbb{Z}_p$ .
2. Montrer que la fonction  $v_p : \mathbb{Z}_p \rightarrow \mathbb{N}$  s'étend en un morphisme de groupes surjectif  $v_p : \mathbb{Q}_p \rightarrow \mathbb{Z}$ . Montrer que  $\mathbb{Z}_p = \{x \in \mathbb{Q}_p / v_p(x) \geq 0\}$  et que  $\mathbb{Z}_p^\times = \text{Ker}(v_p)$ .
  3. En déduire que l'anneau  $\mathbb{Z}_p$  est principal. Quels sont ses idéaux ? Montrer que, pour chaque  $x \in \mathbb{Z}_p$ , on a  $\mathbb{Z}_p/(x) \cong \mathbb{Z}/p^{v_p(x)}\mathbb{Z}$ .
  4. On rappelle qu'un idéal  $J$  de  $A$  est dit premier (resp. maximal) si  $A/J$  est un anneau intègre (resp. un corps). Quels sont les idéaux premiers (resp. maximaux) de  $\mathbb{Z}_p$  ?
  5. La surjection  $\pi : \mathbb{Z}_p \rightarrow \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$  induit par restriction un morphisme de groupes surjectif  $\pi : \mathbb{Z}_p^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ . Montrer qu'il possède une section, c'est-à-dire qu'il existe un morphisme de groupes  $s : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{Z}_p^\times$  tel que  $\pi \circ s = \text{Id}$ .
  6. On pose  $s(0) = 0$ . Montrer que la fonction :

$$\phi : (\mathbb{Z}/p\mathbb{Z})^\mathbb{N} \rightarrow \mathbb{Z}_p, (x_n)_n \mapsto \sum_n s(x_n)p^n$$

est une bijection. S'agit-il d'un isomorphisme d'anneaux ?

7. Il est intéressant de comprendre quelle structure d'anneau il faut mettre sur  $(\mathbb{Z}/p\mathbb{Z})^\mathbb{N}$  pour que  $\phi$  soit un isomorphisme. C'est la théorie des vecteurs de Witt qui y répond, mais elle dépasse très largement le cadre de ce cours.

### Exercice 21 (culturel) : Séries formelles

Soit  $k$  un corps. Pour  $x \in k[[T]]$  et  $y \in k[[T]]$ , on pose  $v(x) = \max\{n \in \mathbb{N} / x \in (T^n)\}$  et  $d(x, y) = e^{-v(x-y)}$ . En procédant comme dans l'exercice 19, montrer que  $d$  définit une distance sur  $k[[T]]$  et que  $k[[T]]$  est alors un anneau qui s'identifie au complété de  $k[T]$  pour la distance  $d$ . Quand  $k[[T]]$  est-il compact ?