



TD 2 — De l'arithmétique ailleurs que sur $\mathbb{Z}$

Gonzalo Romero-García

d'après Uli Fahrenberg
et Bashar Dudin

Résumé

Cette feuille de travaux dirigés prolonge la réflexion menée sur les structures d'anneaux. Vous étudierez les quotients d'anneaux de polynômes, les anneaux d'entiers quadratiques, et l'arithmétique modulaire sur des quotients polynomiaux finis. Elle met en évidence les mécanismes communs à ces constructions : division euclidienne, irréductibilité, existence d'inverses et factorisation.

Table des matières

1	Quotients d'anneaux de polynômes	1
2	De l'arithmétique sur des anneaux d'entiers	4

1 Quotients d'anneaux de polynômes

Cette section est consacrée au fait de vous faire étendre la construction du quotient d'un anneau que vous avez rencontrée dans $\mathbb{Z}/n\mathbb{Z}$ au cas des anneaux de polynômes.

Question 1-1 On note $\mathcal{Q}_{X^2-1}$, $\mathcal{Q}_{X^2-3}$ les anneaux quotients de $\mathbb{Q}[X]$ respectivement par $(X^2 - 1)$ et $(X^2 - 3)$.

1. Vérifier si $\mathcal{Q}_{X^2-1}$ et $\mathcal{Q}_{X^2-3}$ sont intègres : si ce n'est pas le cas décrire les diviseurs de zéro, si c'est bien le cas en apporter une preuve.
2. Quel est l'inverse de X^2 dans $\mathcal{Q}_{X^2-1}$ et $\mathcal{Q}_{X^2-3}$?
3. Est-ce que l'un des anneaux $\mathcal{Q}_{X^2-1}$ ou $\mathcal{Q}_{X^2-3}$ est un corps ? Justifier votre réponse.

Question 1-2 Trouver l'inverse de

1. $[4]X^3 + [2]X + [1]$ dans $\mathbb{Z}/5\mathbb{Z}[X]/(X^2 + X + 1)$.
2. $[6]X^5 + [2]X^2 + [3]$ dans $\mathbb{Z}/7\mathbb{Z}[X]/(X^3 + X + 1)$.

$\forall P \in \mathbb{Q}_{X^2-1}$ $[P] = [a+bx]$ etc $a+bx$ est le rest de la division euclidienne de P par X^2-1 : $P = A \cdot (X^2-1) + (a+bx)$
 $\Rightarrow \mathbb{Q}_{X^2-1}$ etc

si $[a+bx] = [c+dx]$ si $(a+bx) = (c+dx) + \text{multiple de } (X^2-1)$

si $(a+bx) - (c+dx) = \text{multiple de } (X^2-1)$
 $\deg \leq 1$ multiple d'un polynôme de $\deg 2$

le seul multiple d'un polynôme de $\deg 2$ qui soit de $\deg \leq 1$ est le multiple nul

$\Leftrightarrow a+bx - c+dx = 0 \Leftrightarrow a=c$ et $b=d$

On aimerait définir une "taille" \$N\$ pour les polynômes de \$\mathbb{Q}[x^2-3]\$

tg $N(P.Q) = N(P) \cdot N(Q)$ où $N(P) \in \mathbb{Q}$
 et $N(0) = 0$ et $P=0 \Leftrightarrow N(P)=0$

mon a sa: m $P.Q=0$ ds $\mathbb{Q}[x^2-3]$

alors $N(P.Q) = N(0) = 0$
 $= N(P) \cdot N(Q)$
 $\in \mathbb{Q} \quad \in \mathbb{Q}$
 $\Rightarrow N(P)=0$ ou $N(Q)=0$
 $\Rightarrow \dots P=0$ ou $Q=0$

$\rightarrow$ un tel \$N\$ n'existe pas pour $\mathbb{Q}[x^2-1] \Rightarrow$ intègre

dans $\mathbb{C}$, on pose $N(z) = z\bar{z} = (a+ib)(a-ib) = a^2 + b^2 \geq 0$

$N(z)=0$ m $z=0$

$N(z_1 z_2) = (z_1 z_2) \cdot \overline{(z_1 z_2)} = z_1 z_2 \cdot \overline{z_1} \overline{z_2} = \overline{z_1} z_1 \cdot \overline{z_2} z_2 = N(z_1) \cdot N(z_2)$

inspire de $\mathbb{C}$ $N(a+bx) = (a+bx)(a-bx) = a^2 - (bx)^2 = a^2 - b^2 x^2 = a^2 - 3b^2 \in \mathbb{Q}$
 ds $\mathbb{Q}[x^2-3]$
 $= a^2 - b^2 x^2 = a^2 - 3b^2 \in \mathbb{Q}$
 $= 3 \text{ ds } \mathbb{Q}[x^2-3]$

on pose $\overline{a+bx} = a-bx$

on va montrer que $\overline{(a+bx)(c+dx)} = \overline{(a+bx)} \cdot \overline{(c+dx)}$

$\overline{(a+bx)(c+dx)} = \overline{(ac+bdx^2 + x(bc+ad))} = ac+3bd - x(bc+ad)$
 $(ac+3db + x(bc+ad))$ //

$\overline{(a+bx)} \cdot \overline{(c+dx)} = (a-bx)(c-dx) = ac + bdx^2 - x(bc+ad) = ac + 3bd - x(bc+ad)$

Pt i: $\forall P, Q$ on a $\overline{P.Q} = \overline{P} \cdot \overline{Q}$

Cor: $\forall P, Q$ on a $N(P.Q) = N(P) \cdot N(Q)$

dém: $N(P.Q) = (P.Q) \cdot \overline{(P.Q)} = P.Q \cdot \overline{P} \cdot \overline{Q} = \overline{P} \cdot P \cdot Q \cdot \overline{Q} = N(P) \cdot N(Q)$
 commutative

Pt i: ds $\mathbb{Q}[x^2-3]$ $P=0$ m $N(P)=0$

dém: m $P=0 \Rightarrow N(P) = 0 \cdot \overline{0} = 0$

m $N(P)=0$ alors posons $P = a+bx$

ds $\mathbb{Q}[x^2-3]$ $N(P)=0 = (a+bx)(a-bx) = a^2 - (bx)^2 = a^2 - b^2 x^2 = a^2 - 3b^2$

alors $0 = a^2 - 3b^2$

càd $a^2 = 3b^2$ ou $a, b \in \mathbb{Q}$

$\Rightarrow$ m $b=0$ alors $a=0 \checkmark$

m $b \neq 0$: $\sqrt{3} = \frac{a}{b} \in \mathbb{Q}$ contradiction
 $\notin \mathbb{Q}$

$\Rightarrow$ m $N(P)=0$ alors $P=0$

Requis: ds $\mathbb{Q}[x^2-3]$ on définit $\overline{a+bx} = a-bx$
 alors (1) $\overline{P.Q} = \overline{P} \cdot \overline{Q}$
 (2) m $N(P) = P \cdot \overline{P} = a^2 - 3b^2 \in \mathbb{Q}$
 et $\forall P, Q$ $N(P.Q) = N(P) \cdot N(Q)$
 $\forall P$ $P=0 \Leftrightarrow N(P)=0$

cl: $\mathbb{Q}[x^2-3]$ est intègre

$N(P) = P \cdot \overline{P}$ m $P \neq 0$ alors $N(P) \neq 0$
 $\in \mathbb{Q}$

$N(P) = P \cdot \overline{P} \rightarrow P \cdot \left(\frac{\overline{P}}{N(P)} \right) = 1$
 $\neq 0$
 $= P^{-1}$

$\forall P \neq 0$ Pa en inverse qui est $\frac{\overline{P}}{N(P)}$

$(a+bx)^{-1} = \frac{a-bx}{a^2-3b^2}$ ds $\mathbb{Q}[x^2-3]$

$\mathbb{Q} \quad \mathbb{Q}^2$

$x^2-1=0$

$x^2=3$ $(x=\sqrt{3}) \notin \mathbb{Q}$

$\mathbb{Z}_5$
5

$\mathbb{Z}_5[x^2-3]$
5²

thm Bezout: si A et B sont premiers entre eux alors $\exists U, V \text{ tq } AU + BV = 1$

Cor: si A est premier avec B alors $\underline{U = A^{-1}}$ dans $\mathcal{A}/B$

$$\underline{1 = AU} + \underbrace{V \cdot B}_{\substack{\text{multiple de B} \\ = 0 \text{ ds } \mathcal{A}/B}} \Rightarrow \underline{1 = AU} \text{ ds } \mathcal{A}/B \text{ et donc } \underline{U = A^{-1}}$$

$\Rightarrow$ Conséquence: Pour trouver l'inverse dans un anneau quotient par B
 $\downarrow$
 on peut utiliser l'algorithme de Bezout appliqué à A et B.

$\underline{4x^3 + 2x + 1}$ dans $\mathbb{Z}_5[x^2 + x + 1]$
 $\underline{= P}$

x	0	1	2	3	4
$1/x$	*	1	3	2	4

dans $\mathbb{Z}_5$: $\frac{1}{3} + \frac{1}{2} = 2 + 3 = 5 = 0$
 $\frac{2+3=5}{6=1} = \frac{5}{1} = 5 = 0$
 $-\frac{1}{2} = \frac{1}{3}$
 $\frac{1}{3} + \frac{1}{2} = -\frac{1}{2} + \frac{1}{2} = 0$

$\underline{P}$

$$\begin{array}{r} \underline{4x^3 + 2x + 1} \\ -4x^3 - 4x^2 - 4x \\ \hline x^2 + 3x + 1 \\ -x^2 - x - 1 \\ \hline \underline{2x} \end{array}$$

$$\begin{array}{r} \underline{x^2 + x + 1} \\ \underline{4x + 1} \end{array}$$

$P = (4x+1)(x^2+x+1) + 2x \quad (1)$
 $= 2x$

$$\begin{array}{r} x^2 + x + 1 \\ -6x^2 \\ \hline x + 1 \\ -6x \\ \hline \underline{1} \end{array}$$

$$\begin{array}{r} 2x \\ \hline 3x + 3 \end{array}$$

$x^2 + x + 1 = (3x+3)(2x) + 1 \quad (2)$
 $= 0 \text{ ds } \mathbb{Z}_5[x^2 + x + 1]$

(1) $P = 2x$

(2) $1 = - (3x+3) \underbrace{(2x)}_{=P} = - (3x+3)(P)$

$\boxed{P^{-1} = -3x - 3 = 2x + 2}$

Vérification:

$(4x^3 + 2x + 1)(2x + 2) = 8x^4 + 8x^3 + 4x^2 + 4x + 2x + 2$

$\boxed{x^2 + x + 1 = 0} \quad \boxed{x^2 = -x - 1}$

$\mathbb{Z}_5[x^2 + x + 1]$

$(x^2)^2 = (x^2)(x^2) = (-x-1)(-x-1) = x^2 + 2x + 1 = x$
 $-x-1$

$x^3 = x^2 \cdot x = (-x-1) \cdot x = -x^2 - x$
 $= +x + 1 - x = 1$

$D = 8x + 8 + 4(-x-1) + 4x + 2x + 2$

$= \underbrace{10}_{=0} \cdot x + \underbrace{6}_{=1} = 1 \quad \checkmark$

$$\frac{6x^5 + 2x^2 + 3}{P} \text{ in } \mathbb{Z}_7[x^3 + x + 1]$$

$$\mathbb{Z}_7 \begin{array}{r} 2 \ 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \\ 1/2 \ * \ 1 \ 4 \ 5 \ 2 \ 3 \ 6 \end{array}$$

$$P = 6x^5 + 2x^2 + 3$$

$$\underline{-6x^5 - 6x^3 - 6x^2}$$

$$x^3 + 3x^2 + 3$$

$$\underline{-x^3 - x - 1}$$

$$3x^2 + 6x + 2$$

$$x^3 + x + 1$$

$$6x^2 + 1$$

$$\textcircled{0} \quad P = (6x^2 + 1)(x^3 + x + 1) + \boxed{3x^2 + 6x + 2}$$

$$x^3 + x + 1$$

$$\underline{-15x^3 - 30x^2 - 10x}$$

$$5x^2 + 5x + 1$$

$$\underline{-12x^2 - 24x - 8}$$

$$(2x)$$

$$3x^2 + 6x + 2$$

$$5x + 4$$

$$\textcircled{1} \quad x^3 + x + 1 = (5x + 4)(3x^2 + 6x + 2) + 2x$$

$$x \begin{array}{r} 1 \ 2 \ 3 \ 4 \ 5 \ 6 \\ 1/2 \ 1 \ 4 \ 5 \ 2 \ 3 \ 6 \end{array}$$

$$3x^2 + 6x + 2$$

$$\underline{-10x^2}$$

$$6x + 2$$

$$\underline{-6x}$$

$$2$$

$$2x$$

$$5x + 3$$

$$\textcircled{2} \quad 3x^2 + 6x + 2 = (5x + 3)(2x) + 2$$

$$\textcircled{2} \quad 2 = -(5x + 3)(2x) + P$$

$$= -(5x + 3)(-(5x + 4))P + P$$

$$\textcircled{1} \quad 2x = -P(5x + 4)$$

$$\boxed{2 = P * [(5x + 3)(5x + 4) + 1]}$$

$$x^4 \hookrightarrow \frac{1}{2} = P \cdot 4 \left[\underbrace{25x^2}_{=4} + \underbrace{35x}_{=0} + \underbrace{12 + 1}_{=-1} \right]$$

$$1 = P \cdot (2x^2 + 3)$$

$$(6x^5 + 2x^2 + 3)(2x^2 + 3) = 12x^7 + 18x^5 + 4x^4 + 6x^2 + 6x^2 + 9$$

$$x^3 = -x - 1$$

$$x^4 = -x^2 - x$$

$$x^5 = -x^3 - x^2 = -x^2 + x + 1$$

$$x^7 = (x^3)^2 \cdot x = (x + 1)^2 \cdot x = x^3 + 2x^2 + x = 2x^2 - 1$$

$$5(2x^2 - 1) + 4(-x^2 + x + 1) + 4(-x^2 - x) + 5x^2 + 2$$

$$x^2 + 0x + 2 = 1$$

$$N(3) = 3\bar{3}$$

$$N(a+ib) = (a+ib)(a-ib) = a^2 + b^2 \in \mathbb{N}$$

2 De l'arithmétique sur des anneaux d'entiers

$$N(z_1 z_2) = N(z_1) \cdot N(z_2)$$

$$i(i) = 1$$

Question 2-3 On s'intéresse à l'arithmétique de l'anneau $(\mathbb{Z}[i], +, \cdot)$ où l'addition et la multiplication correspondent à celle des complexes. L'ensemble $\mathbb{Z}[i]$ est donné par

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}.$$

1. Donner des exemples de nombre premiers dans $\mathbb{Z}$ qui ne sont pas irréductibles dans $\mathbb{Z}[i]$.
2. La norme d'un élément $x = a + ib$ est donnée par

$$N(x) = a^2 + b^2.$$

Donner tous les éléments inversibles de $\mathbb{Z}[i]$.

3. Donner une condition nécessaire et suffisante sur un nombre premier p , en terme de N , pour que celui-ci ne soit pas irréductible dans $\mathbb{Z}[i]$.
4. L'anneau $\mathbb{Z}[i]$ est euclidien pour la norme N , donc factoriel. Est-ce que tous les $\mathbb{Z}[i\sqrt{d}]$ pour d premier sont factoriels?

$$5 = (1+2i)(1-2i) = (2+i)(2-i)$$

$$2 = (1-i)(1+i)$$

$$21 = (4+3i)(4-3i) \\ 13 = (3+2i)(3-2i)$$

Question 2-4 On s'intéresse à l'arithmétique de l'anneau $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ où l'addition et la multiplication correspondent à celle des réels. L'ensemble $\mathbb{Z}[\sqrt{2}]$ est donné par

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

1. Donner des exemples de nombres premiers dans $\mathbb{Z}$ qui ne sont pas irréductibles dans $\mathbb{Z}[\sqrt{2}]$.
2. La norme d'un élément $x = a + b\sqrt{2}$ est donnée par

$$N(x) = a^2 - 2b^2.$$

Décrire les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ à l'aide de N . Semblerait-il y en avoir un nombre fini?

3. Donner une condition nécessaire et suffisante sur p , en terme de N , pour que celui-ci ne soit pas irréductible dans $\mathbb{Z}[\sqrt{2}]$.

$$2 = \sqrt{2} \cdot \sqrt{2} \\ 7 = (3+\sqrt{2})(3-\sqrt{2}) = 9-2=7$$

$$N(a+b\sqrt{2}) = (a+b\sqrt{2})(a-b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Z}$$

② si $x \in \mathbb{Z}[\sqrt{2}]$ est inversible il existe y tel que $xy = 1$

$$\underbrace{N(x)}_{\in \mathbb{Z}} \cdot \underbrace{N(y)}_{\in \mathbb{Z}} = N(xy) = N(1) = 1$$

$$\Rightarrow N(x) = N(y) = \pm 1$$

$$\boxed{x \text{ est inversible} \Rightarrow N(x) = \pm 1}$$

Réciproque : si $N(x) = \pm 1$, $x = a + b\sqrt{2}$ $N(x) = \underbrace{(a+b\sqrt{2})}_x \cdot \underbrace{(a-b\sqrt{2})}_y = \pm 1$

$$\Rightarrow x \text{ est inversible et son inverse est } N(x) \cdot (a-b\sqrt{2})$$

$$\boxed{\text{Thm: } x \text{ inversible dans } \mathbb{Z}[\sqrt{2}] \text{ si } N(x) = \pm 1}$$

[STA]

$$N(x) = a^2 - 2b^2$$

$$N(x) = 1 \Rightarrow a = \sqrt{2b^2 + 1} \\ a \approx \sqrt{2} \cdot b$$



$$N \ni F_n = F_{n-1} + F_{n-2}$$

$$= \left(\frac{1+\sqrt{5}}{2} \right)^n + \left(\frac{1-\sqrt{5}}{2} \right)^n \sim \oplus^n$$

les inversibles de $\mathbb{Z}[i]$: si x est inversible il existe $y \in \mathbb{Z}[i]$

$$\text{tq } xy = 1$$

$$\begin{aligned} \text{donc } N(xy) &= N(1) = 1 \\ &= \underbrace{N(x)}_{\in \mathbb{N}} \underbrace{N(y)}_{\in \mathbb{N}} \end{aligned} \quad \left. \begin{aligned} &\Rightarrow N(x) = N(y) = 1 \\ &N(x) = 1 = a^2 + b^2 \text{ où } a, b \in \mathbb{Z} \\ &x = a + ib \end{aligned} \right\}$$

$$\Rightarrow |a| = 1 \text{ et } b = 0$$

$$\text{ou } a = 0 \text{ et } |b| = 1$$

$$\Rightarrow x \in \{1, -1, i, -i\}$$

et réciproquement

$$\begin{aligned} 1^2 &= 1 \\ (-1)^2 &= 1 \\ i(-i) &= 1 \end{aligned}$$

$1, -1, i$ et $-i$ sont inversibles -

Supposons que p premier n'est pas irréductible, c'est qu'il existe x et y non inversibles et non nuls tq $xy = p$

$$\begin{aligned} &\downarrow \\ N(x) &\neq 1 \\ N(y) &\neq 1 \end{aligned}$$

$$\begin{aligned} &\downarrow N(xy) = N(p) = p^2 \\ &= \\ &\underbrace{N(x)}_{\in \mathbb{N}} \underbrace{N(y)}_{\in \mathbb{N}} \\ &\neq 0, 1 \end{aligned}$$

$$\Rightarrow N(x) = N(y) = p$$

$$x = a + ib \Rightarrow p = a^2 + b^2$$

per irréductible si $\nexists a, b$ tq $p = a^2 + b^2$

Trouver une division euclidienne de $\mathbb{Z}[i\sqrt{d}]$ par d premier.

defini: $N(a+i\sqrt{d}.b) = \underline{(a+i\sqrt{d}.b)(a-i\sqrt{d}.b)}$
 $\underline{= a^2 + d.b^2}$

$$\frac{p}{q} =$$

$$q = x + i\sqrt{d}.y \quad \frac{1}{q} = \frac{x - i\sqrt{d}.y}{x^2 + d.y^2} \text{ dans } \mathbb{C}$$

$$\frac{p}{q} \stackrel{=}{=} \alpha + i\beta\sqrt{d} \text{ où } \alpha, \beta \in \mathbb{Q}$$

dans $\mathbb{C}$

$$\text{on pose } u = \lfloor \alpha \rfloor \in \mathbb{Z} \text{ tq } |u - \alpha| \leq \frac{1}{2}$$

$$v = \lfloor \beta \rfloor \in \mathbb{Z} \text{ tq } |v - \beta| \leq \frac{1}{2}$$

$$\underline{\underline{\text{reste}}} = \textcircled{p} - q \cdot \underbrace{(u + i\sqrt{d}.v)}_{\text{quotien arrondi}} = q \cdot [(\alpha - u) + i\sqrt{d}(\beta - v)]$$

$$p = q \cdot (\alpha + i\beta\sqrt{d}) \text{ dans } \mathbb{C}$$

$$\textcircled{N}(\text{reste}) = \underbrace{N(q)} \cdot \underbrace{N((\alpha - u) + i\sqrt{d}(\beta - v))}_{\text{je veux } < 1}$$

$$= \underbrace{(\alpha - u)^2}_{\leq \frac{1}{4}} + d \underbrace{(\beta - v)^2}_{\leq \frac{1}{4}} \leq \frac{1+d}{4} < 1$$

seulement pour $d=2$
et pas pour $d \geq 3$

$$\text{si } d=2 \quad N(\text{reste}) < N(q)$$

$$\text{si } d \geq 3 \quad \text{aucune garantie que } \cancel{N(\text{reste}) < N(q)}$$

$\mathbb{Z}[i\sqrt{2}]$ est euclidien pour $N \Rightarrow$ il est factoriel
= statisme

mais $\mathbb{Z}[i\sqrt{d}]$ pour $d \geq 3$, on sait pas ...

CNS pour p premier réductible

si p est réductible dans $\mathbb{Z}[\sqrt{2}]$: il existe x et y non-inversibles

$$\text{tq } p = xy$$

$$p^2 = N(p) = N(xy) = \underbrace{N(x)N(y)}_{\in \mathbb{Z} \setminus \{\pm 1\}}$$

$\Rightarrow N(x) = N(y) = \pm p$ par unicité de la décomposition en nombres premiers

$$\Rightarrow \boxed{\begin{array}{l} \exists a, b \text{ tq } p = a^2 - 2b^2 \\ \text{ou } -p = a^2 - 2b^2 \end{array}}$$

Réciproquement si $\exists a, b \text{ tq } (1) p = a^2 - 2b^2$ ou $(2) -p = a^2 - 2b^2$ $N=p > 1$

$$(1) \Rightarrow p = \underbrace{(a+b\sqrt{2})}_{N(1)=p > 1} \underbrace{(a-b\sqrt{2})}_{N(1)=p > 1}$$

non inversibles

$\Rightarrow p$ réductible

$$(2) \Rightarrow p = \underbrace{(a+b\sqrt{2})}_{N=p > 1} \underbrace{(a-b\sqrt{2})}_{N=p > 1}$$

$\Rightarrow p$ réductible

il faut que $(a+b\sqrt{2})$ et $(a-b\sqrt{2})$ ne soient pas inversibles

càd que leur norme soit $\neq \pm 1$ OK car $N(1)=1 \neq p$