



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
- 2 De l'arithmétique sur des anneaux d'entiers

$$a^2 - 3b^2 = N(P) = P \cdot \bar{P} \quad 1 = \frac{N(P)}{N(P)} = \frac{P \bar{P}}{N(P)} = P \cdot \frac{\bar{P}}{N(P)} = P \cdot P^{-1}$$

$N(P) \neq 0$

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.

Non pas intègre

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 $\mathbb{Z}/7\mathbb{Z}[X]/(X^3 + X + 1)$.

1-1-1 : @ ds $\mathcal{Q}_{X^2-1}$: $X^2 - 1 = 0 = (X-1)(X+1) \Rightarrow \mathcal{Q}_{X^2-1}$ n'est pas intègre

$$([0] + \alpha X) = [0] = [a + bX]$$

$$(a, b) \neq (c, d)$$

$$[a + bX] \neq [c + dX] \quad \text{si } a + bX \neq c + dX \pmod{X^2 - 1}$$

$$\text{def 1} \quad a - c + (b - d)X = \text{multiple de } X^2 - 1$$

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

$$\text{ce fait } a - c + (b - d)X = 0 \text{ ds } \mathbb{Q}[X]$$

$$\Rightarrow a = c \text{ et } b = d$$

⑥ Être intègre si $(a+bX)(c+dX) = 0$ alors $(a,b) = (0,0)$ ou $(c,d) = (0,0)$
 ds $\mathbb{Q}_{X^2=3}$

$$(a+bX)(c+dX) = ac + \underbrace{bd}_{=3}X^2 + X(bc+ad) = ac + 3bd + X(bc+ad) = 0 \Rightarrow \begin{cases} ac + 3bd = 0 \\ bc + ad = 0 \end{cases}$$

$X^2=3$

$(\cancel{X^2=3} + 3)$

$X^2=3=0 \Leftrightarrow X^2=3$

$\Downarrow ?$
 $\begin{cases} (a,b) = (0,0) \\ \text{ou} \\ (c,d) = (0,0) \end{cases}$

Norme $z \in \mathbb{C} \quad z = a + ib \quad |z| = \sqrt{a^2 + b^2}$

$\bar{z} = a - ib$

$|z|^2 = z\bar{z} = \underline{(a+ib)(a-ib)} = a^2 - (ib)^2 = a^2 + b^2$

$N(z) = |z|^2 = z\bar{z}$

$|z_1 z_2|^2 = (z_1 z_2)(\overline{z_1 z_2}) = z_1 z_2 \bar{z}_1 \bar{z}_2 = \underbrace{z_1 \bar{z}_1}_{=|z_1|^2} \underbrace{z_2 \bar{z}_2}_{=|z_2|^2} = |z_1|^2 |z_2|^2$

$\forall z, z' \in \mathbb{C} \quad N(z z') = \underline{N(z) N(z')}$

$\mathbb{Q}_{X^2=3}$ on définit le **conjugue** de $a+bX$ par $\overline{a+bX} = a-bX$

Prp: $\forall P, Q \in \mathbb{Q}_{X^2=3} \quad \overline{PQ} = \overline{P} \cdot \overline{Q}$ ✓

démon: $P = a+bX$
 $Q = c+dX$

$P \cdot Q = (a+bX)(c+dX) = ac + \underbrace{bd}_{=3}X^2 + X(bc+ad) = (ac + 3bd) + X(bc+ad)$ ds $\mathbb{Q}_{X^2=3}$

$\overline{P \cdot Q} = (ac + 3bd) + X(-bc - ad)$

en remplaçant b par -b et d par -d

$\overline{P \cdot Q} = ac + 3(-b)(-d) + X((-bc) + a(-d)) = ac + 3bd + X(-bc - ad) = \overline{P \cdot Q}$ ✓

Cor: $\forall P, Q \in \mathbb{Q}_{X^2=3} \quad N(P \cdot Q) = N(P) \cdot N(Q)$ où $N(a+bX) = a^2 - 3b^2$

démon: $P \cdot \overline{P}$ où $P = a+bX$

$\underline{P \cdot \overline{P}} = (a+bX)(a-bX) = a^2 - (bX)^2 = a^2 - b^2 X^2 = a^2 - 3b^2 = \underline{N(P)}$

$N(P \cdot Q) = (P \cdot Q)(\overline{P \cdot Q}) = P \cdot Q \cdot \overline{P} \cdot \overline{Q} = \underbrace{P \cdot \overline{P}}_{N(P)} \cdot \underbrace{Q \cdot \overline{Q}}_{N(Q)} = N(P) \cdot N(Q)$ ✓
 x commutatif

Résumé: Pour $P = a+bX$ ds $\mathbb{Q}_{X^2=3}$ on définit $N(P) = a^2 - 3b^2 \in \mathbb{Q}$
 alors $\forall P, Q \in \mathbb{Q}_{X^2=3} \quad N(PQ) = N(P) \cdot N(Q)$

N mesure la "taille" d'un polynôme produit comme le produit des tailles

Mq $\mathbb{Q}_{X^2=3}$ est intègre: Soient P, Q tq $P \cdot Q = 0$ ds $\mathbb{Q}_{X^2=3}$

Comme $P \cdot Q = 0$, on a $N(P \cdot Q) = N(0) = 0^2 - 3 \cdot 0^2 = 0$

$\underbrace{N(P)}_{\in \mathbb{Q}} \cdot \underbrace{N(Q)}_{\in \mathbb{Q}}$

$\Rightarrow N(P) = 0$ ou $N(Q) = 0$ car $\mathbb{Q}$ est intègre

Qu'il s'agit d'échanger P et Q on a $N(P) = 0$ mpx $P = a+bX$ où $a, b \in \mathbb{Q}$

$N(P) = 0 = a^2 - 3b^2 \Rightarrow 3 = \frac{a^2}{b^2} \Rightarrow \sqrt{3} = \frac{a}{b} \in \mathbb{Q} \rightarrow$ absurde.

$\boxed{mb=0 \text{ alors } a=0}$

$3b^2 = a^2$
 #impair 3 ds le comp des nombres

$\Rightarrow b=0$ donc $a=0$
 donc $P=0$ ✓

m $PQ=0$ alors $P=0$ ou $Q=0$ - ✓ intègre

Inverse de $4x^3 + 2x + 1$ module $\underline{x^2 + x + 2}$ de $\mathbb{Z}_5[x]$

$$\frac{1}{3} + \frac{1}{2} = 2 + 3 = 5 = 0$$

$$\frac{2 \times 1 + 1 + 3}{6} = \frac{5}{1} = 5$$

$$\pi_5: \begin{array}{cccccc} x & 0 & 1 & 2 & 3 & 4 \\ \hline 1/x & * & 1 & 3 & 2 & 4 \end{array}$$

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

$$\begin{array}{ccc} \textcircled{-4}x^2 & \textcircled{-2}x & +1 \\ \text{= 2} & \text{= 3} & \end{array}$$

$$x^2 + 3x + 1$$

$$-x^2 - x - 1$$

$2x$

$$x^2 + x + 1$$

$$4x + 1$$

$$(1) \mid 4x^3 + 2x + 1 = (4x+1)(x^2+x+1) + 2x$$

$$\begin{array}{cccccc} x & 1 & 2 & 3 & 4 \\ \hline 1/2 & 1 & 3 & 2 & 4 \end{array}$$

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

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

$$x^2 + x + 1 = (3x + 3)(2x) + 2 \quad (2)$$

$$1 = \underbrace{(x^2 + x + 1)}_0 - \underbrace{(2x)}_1 \underbrace{(3x + 3)}_2$$

$$\stackrel{(1)}{=} \underbrace{(4x^3 + 2x + 1)} - \cancel{(4x+1)(x^2 + x + 1)}_0$$

$$\hookrightarrow 245 \mid x^2 + x + 2$$

$$1 = - \underbrace{(4x^3 + 2x + 1)}_P (3x + 3) \Rightarrow P^{-1} = -3x - 3 = 2x + 2$$

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

$$= 3x^4 + 3x^3 + 4x^2 + x + 2$$

$$x^2 + x + 1 = 0 \quad x^2 = -x - 1 = 4x + 4$$

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

$$\begin{aligned} x^3 &= x^2 \cdot x = (-x-1)x = -x^2 - x \\ &= 4(-x-1) + 4x = -4 \\ &= 1 \end{aligned}$$

$$= 3x + 3 + 4(-x - 1) + 2 + x$$

$$= 0.7 \times 1 = 1$$

Inverse $\frac{6x^5 + 2x^2 + 3}{x^3 + x + 1} \stackrel{d}{=} \frac{2x}{x^3 + x + 1}$

$$\begin{array}{r} 6x^5 + 2x^2 + 3 \\ - 6x^5 - 6x^3 - 6x^2 \\ \hline x^3 + 3x^2 + 3 \\ - x^3 - x - 1 \\ \hline 3x^2 + 6x + 2 \end{array}$$

$$\begin{array}{r} x^3 + x + 1 \\ 6x^2 + 1 \end{array}$$

$$\frac{2x}{x^3 + x + 1} \begin{array}{r} x^3 + x + 1 \\ 2x \end{array}$$

$$P = 6x^5 + 2x^2 + 3 = (6x^2 + 1)(x^3 + x + 1) + 3x^2 + 6x + 2 = 3x^2 + 6x + 2$$

$$\begin{array}{r} x^3 + x + 1 \\ - 15x^3 - 30x^2 - 10x \\ \hline 5x^2 + 5x + 1 \\ - 12x^2 - 24x - 8 \\ \hline 2x \end{array}$$

$$x^3 + x + 1 = (5x + 4)(3x^2 + 6x + 2) + 2x$$

$$\frac{2x}{x^3 + x + 1} \begin{array}{r} x^3 + x + 1 \\ 2x \end{array}$$

$$\begin{array}{r} 3x^2 + 6x + 2 \\ 6x + 2 \\ + 2 \end{array} \begin{array}{r} 2x \\ \frac{3}{2}x + \frac{6}{2} = 3 \\ \hline = 3x + 4 = 12 = 5 \end{array}$$

$$3x^2 + 6x + 2 = (2x)(5x + 3) + 2$$

$$\begin{aligned} 2 &= P - (2x)(5x + 3) = P - (-P)(5x + 4)(5x + 3) \\ &= P \cdot [1 + (5x + 4)(5x + 3)] \\ &= P \cdot (1 + 25x^2 + 35x + 12) \\ &= P \cdot (4x^2 + 6) \end{aligned}$$

$$\Rightarrow P \cdot (4x^2 + 6) = 2 \Rightarrow P^{-1} = \frac{(4x^2 + 6)}{2} = 2x^2 + 3$$

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

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

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

$$\begin{aligned} x^7 &= (x-1)^2 x = (x^2 + 2x + 1)x \\ &= x^3 + 2x^2 + x \\ &= (2x^2 - 1)x^5 \end{aligned}$$

$$\begin{aligned} x^5 &= (x-1)x^2 = -x^3 - x^2 \\ &= (-x^2 + x + 1)x^4 \end{aligned}$$

$$x^4 = (x-1)x = (-x^2 - x)x^4$$

$$\begin{aligned} 10x^2 - 5 - 4x^2 + 4x + 4 - 4x^2 - 4x + 5x^2 + 2 \\ = 7x^2 + 0x + 1 = 1 \end{aligned}$$

$$a = (a \cdot x) \cdot (x^{-1})$$

ni a inversible

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

$$13 = (2+3i)(2-3i) = 2^2 + 3^2 = 4 + 9$$

2 De l'arithmétique sur des anneaux d'entiers

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

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

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

$$= (a+ib)(a-ib)$$

1. Donner des exemples de nombres 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

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

$$N(uv) = N(u)N(v)$$

$$\in \mathbb{Z}$$

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 ?

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

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

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

$$N(a+b\sqrt{2}) = (a+b\sqrt{2})(a-b\sqrt{2})$$

$$= a^2 - 2b^2 \in \mathbb{Z}$$

3. Décrire les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ à l'aide de N . Semble-t-il y en avoir un nombre fini ?

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

Tous les els inversibles de $\mathbb{Z}[i]$

$$\text{Soit } x \text{ tq } \exists y \text{ tq } \boxed{xy = 1} \rightarrow \underbrace{N(xy)}_{=1} = \underbrace{N(1)}_{=1} = 1$$
$$\underbrace{N(x)}_{\in \mathbb{N}} \underbrace{N(y)}_{\in \mathbb{N}}$$

$$(a+ib)(a-ib) = 1$$
$$\underbrace{N(a+ib)}_{=1}$$

$$\text{donc } \underline{N(x) = N(y) = 1}$$

$$\text{si } x = a+ib \quad \underline{N(x) = a^2 + b^2 = 1} \Rightarrow |a|=1 \text{ et } b=0$$
$$\text{ou } a=0 \text{ et } |b|=1$$

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

et de + tous les els ± 1 et $\pm i$ sont inversibles: $(-1)^2 = 1$
 $i \cdot (-i) = 1$

les els inversibles de $\mathbb{Z}[i]$: $\{1, -1, i, -i\}$ ✓

si p est irréductible $p = xy \Rightarrow \underbrace{N(p)}_{=p^2} = \underbrace{N(xy)}_{=1,0} = \underbrace{N(x)}_{\in \mathbb{N}} \underbrace{N(y)}_{\in \mathbb{N}}$
 $x, y \notin \text{inversible} \quad \underbrace{= p^2}_{\neq 1,0}$
 $\Rightarrow N(x), N(y) \neq 1$

$$\Rightarrow \underline{N(x) = p} \text{ et } \underline{N(y) = p}$$

$$x = a+ib \quad \boxed{N(x) = a^2 + b^2 = p}$$

$$\text{si } \exists a, b \in \mathbb{Z} \text{ tq } p = a^2 + b^2 \quad p = N(a+ib) = \underbrace{(a+ib)(a-ib)}_{\in \mathbb{Z}[i]}$$

de plus $\underline{a+ib}$ est non inversible

$$\text{car } N(a+ib) = p > 1$$

THM: p est divisible par irréductible si $\exists a, b \in \mathbb{N}$ tq $p = a^2 + b^2$

$$\mathbb{Z}[i\sqrt{d}] \quad N(a+ib\sqrt{d}) = (a+ib\sqrt{d}) \cdot (a-ib\sqrt{d}) \\ = a^2 + d \cdot b^2$$

on veut effectuer une division euclidienne :

$$\frac{p}{q} = \frac{(a+ib\sqrt{d})(x-iy\sqrt{d})}{x^2+dy^2}$$

$\in \mathbb{Q}[i\sqrt{d}]$

$$p = a+ib\sqrt{d} \\ q = x+iy\sqrt{d}$$

$$\frac{1}{q} = \frac{\bar{q}}{|q|^2} = \frac{x-iy\sqrt{d}}{x^2+dy^2}$$

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

$$u = \lfloor \alpha \rfloor \in \mathbb{Z} \quad \text{t.q.} \quad |u - \alpha| \leq \frac{1}{2}$$

$$v = \lfloor \beta \rfloor \in \mathbb{Z} \quad \text{t.q.} \quad |v - \beta| \leq \frac{1}{2}$$

$$\text{reste} = p - q \cdot (u + i\sqrt{d}v) = q \cdot [(\alpha - u) + i\sqrt{d}(\beta - v)]$$

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

$$N(\text{reste}) = \underbrace{N(q)} \cdot \underbrace{N((\alpha - u) + i\sqrt{d}(\beta - v))}$$

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

pour $d=2$

mais pas pour $d \geq 3$

N'est ce théorème pour $d=2$ seulement

$$\mathbb{Z}[\sqrt{2}] \quad ① \quad 7 = (5+3\sqrt{2})(5-3\sqrt{2}) \\ = 25 - \underbrace{9 \times 2}_{18} = 7$$

$$2 = \sqrt{2} \cdot \sqrt{2} \\ \text{or } 1\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

② inversibles de $\mathbb{Z}[\sqrt{2}]$ si x est inversible, $\exists y \quad xy = 1$

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

$$\text{donc soit } N(x) = N(y) = 1 \rightarrow a^2 - 2b^2 = 1 \text{ si } x = a + \sqrt{2}b$$

$$\text{soit } N(x) = N(y) = -1 \rightarrow a^2 - 2b^2 = -1$$

inversible si $N(x) = \pm 1$ et $x = a + \sqrt{2}b$ ma $x \cdot \underbrace{(a - \sqrt{2}b)}_{\text{inverse de } x} = N(x) = \pm 1$

$\Rightarrow x$ est inversible

THM: x est inversible si $N(x) = 1$ ou $N(x) = -1$

Combien il y en a? $a^2 - 2b^2 = 1$ ou -1

$$a = \sqrt{2b^2 + 1} \text{ ou } a = \sqrt{2b^2 - 1}$$

$$a = \sqrt{2b^2 + 1} = \sqrt{2} \cdot b \left(\sqrt{1 + \frac{1}{2b^2}} \right) \quad \sqrt{1+x} = 1 + \frac{x}{2} + o(x)$$

$$\frac{a}{b} = \sqrt{2} = 1 + \underbrace{\left(\frac{1}{4b^2} \right)}_{\text{circled}} + o\left(\frac{1}{b^2}\right)$$

③ si p est de $\mathbb{N}$ et irréductible ma $p = xy$ de $\mathbb{Z}[\sqrt{2}]$ x, y non inversibles

$$\text{donc } N(p) = p^2 = N(xy) = \underbrace{N(x)}_{\in \mathbb{Z} \setminus \{0, \pm 1\}} \cdot \underbrace{N(y)}_{\in \mathbb{Z} \setminus \{0, \pm 1\}}$$

Ng: $N(x) = 0 \Leftrightarrow x = 0$

$$x = a + \sqrt{2}b \quad N(x) = a^2 - 2b^2$$

$$N(x) = 0 \Leftrightarrow a^2 - 2b^2 = 0 \Leftrightarrow a^2 = 2b^2$$

par unicité de la décomposition en nombres premiers si $a \neq 0$ ou $b \neq 0$, 2 apparaît un nombre impair de fois à droite et pair à gauche

$\rightarrow$ contradiction

$$N(x) = 0 \Leftrightarrow x = 0 \quad \checkmark$$

$$\text{donc } N(x) = N(y) \text{ et } N(x) = \pm p$$

inversement: si $\exists a, b \in \mathbb{Z} \quad p = a^2 - 2b^2$ ou $-p = a^2 - 2b^2$

$$p = (a + \sqrt{2}b)(a - \sqrt{2}b)$$

$$N = p \neq \pm 1 \quad N = p \neq \pm 1$$

$\rightarrow$ non inversible

$\rightarrow$ irréductible

$$p = -(a + \sqrt{2}b)(a - \sqrt{2}b)$$

$$N = \pm p \neq \pm 1$$