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

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

⑥ Être intègre si $(a+bX)(c+Xd)=0$ alors $(a,b)=(0,0)$ ou $(c,d)=(0,0)$

dans $\mathbb{Q}[X]/(X^2-3)$

$(a+bX)(c+dX) = ac+3bd+X(bc+ad)$

X^2-3 $\quad$ (X^2-3+3) $\quad$ $X^2-3=0 \hookrightarrow X^2=3$

$=0 \Rightarrow \begin{cases} ac+3db=0 \\ bc+ad=0 \end{cases}$ ⁉

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

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

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

$N(z)=|z|^2=z\bar{z}$ $\quad |z_1z_2|^2=(z_1z_2)(\overline{z_1z_2})=z_1z_2\bar{z}_1\bar{z}_2=z_1\bar{z}_1z_2\bar{z}_2=|z_1|^2|z_2|^2$ $\quad \overline{z_1z_2}=\bar{z}_1\bar{z}_2$

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

$\mathbb{Q}[X]/(X^2-3)$ on définit le **conjugué** de $a+bX$ par $\overline{a+bX}=a-bX$

Prop: $\forall P,Q\in\mathbb{Q}[X]/(X^2-3)$ $\quad \overline{PQ}=\bar{P}\cdot\bar{Q}$ ✓

dem: $P=a+bX$, $Q=c+dX$

$P\cdot Q=(a+bX)(c+dX)$

$=ac+X^2bd+X(bc+ad)$ $\quad X^2=3 \Rightarrow$ ok aussi $\forall k$

$=(ac+3bd)+X(bc+ad)$ dans $\mathbb{Q}[X]/(X^2-3)$

$\overline{P\cdot Q}=(ac+3bd)+X(-bc-ad)$ en remplaçant b par $-b$ et d par $-d$

$\overline{P}\cdot\overline{Q}=ac+3(-b)(-d)+X((-b)c+a(-d))$

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

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

dem: $P\cdot\bar{P}$ où $P=a+Xb$ $\quad P\cdot\bar{P}=(a+Xb)(a-Xb)=a^2-(Xb)^2$

$=a^2-b^2X^2$ $\quad X^2=3$

$=a^2-3b^2=N(P)$

$N(P\cdot Q)=(P\cdot Q)\overline{(P\cdot Q)}=P\cdot Q\cdot\bar{P}\cdot\bar{Q}=P\bar{P}\cdot Q\bar{Q}$ ✓ ($\times$ commutatif)

$N(P)\quad N(Q)$

$=\overline{P\cdot Q}$

Résumé: Pour $P=a+bX$ dans $\mathbb{Q}[X]/(X^2-3)$ on définit $N(P)=a^2-3b^2\in\mathbb{Q}$ $\quad \leq 0$

alors $\forall P,Q\in\mathbb{Q}[X]/(X^2-3)$ $\quad N(PQ)=N(P)\cdot N(Q)$

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

Mq $\mathbb{Q}[X]/(X^2-3)$ est intègre: Soient P,Q tq $P\cdot Q=0$ dans $\mathbb{Q}[X]/(X^2-$

Comme $P\cdot Q=0$, on a $N(P\cdot Q)=N(0)=0^2-3\cdot0^2=0$

$N(P)\cdot N(Q)$

$\in\mathbb{Q}$ $\quad \in\mathbb{Q}$

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

Quitte à échanger P et Q on a $N(P)=0$ on pose $P=a+bX$ où $a,b\in\mathbb{Q}$

$N(P)=0=a^2-3b^2 \Rightarrow 3=\frac{a^2}{b^2}$ $\quad (b\neq0)$ $\Rightarrow \sqrt{3}=\left|\frac{a}{b}\right|\in\mathbb{Q}$ → absurde.

$3b^2=a^2$ il y a un nombre pair de 3

impair de 3 dans b^2 car on compte deux nombres de fois les

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

donc $P=0$ ✓

si $PQ=0$ alors $P=0$ ou $Q=0$ _ ✓ intègre

Inverse de $4x^3+2x+1$ modulo x^2+x+1 de $\mathbb{Z}/5\mathbb{Z}[x]$

$\mathbb{Z}/5$:

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

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

$=$

$\frac{2\times1+1+3=5}{6=1} = \frac{5}{1}=0$

$4x^3 \quad +2x+1$

$-(4x^3+4x^2+4x)$

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

$=1 \quad =3$

x^2+3x+1

$-\ x^2-x-1$

$2x$

x^2+x+1

$4x+1$

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

x	1	2	3	4
1/2	1	3	2	4

x^2+x+1

$-6x^2$

$x+1$

$-6x$

$2x$

$3x+3$

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

1

$1 = (x^2+x+1) - (2x)(3x+3)$ dans $\mathbb{Z}/5\mathbb{Z}/x^2+x+1$

(2) 0

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

(1) 0

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

P

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

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

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

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

$-x-1$

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

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

$= 1$

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

$= 0.x+1 = 1$

Inverse $\underbrace{6x^5+2x^2+3}_{=P}$ dans $\mathbb{Z}_7/x^3+x+1$

$\mathbb{Z}_7$

x	0	1	2	3	4	5	6
1/x	x	1	4	5	2	3	6

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

$P = 6x^5+2x^2+3 = (6x^2+1)\underbrace{(x^3+x+1)}_{0} + 3x^2+6x+2$

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

$$\begin{array}{r|l} x^3+x+1 & 3x^2+6x+2 \\ \hline -15x^3-30x^2-6x & 5x+4 \\ \hline 5x^2+5x+1 & \\ -12x^2-24x-8 & \\ \hline 2x & \end{array}$$

$x^3+x+1 = (5x+4)\underbrace{(3x^2+6x+2)}_{=P} + 2x$

$\underbrace{x^3+x+1}_{0} = (5x+4)(3x^2+6x+2) + 2x$

(1)

x	1	2	3	4	5	6
1/x	1	4	5	2	3	6

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

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

$\underbrace{3x^2+6x+2}_{=P} = (2x)(5x+3)+2$

$2 = \underset{(2)}{P-(2x)(5x+3)} = P-(-P)(5x+4)(5x+3)$

$= \underset{(1)}{-P(5x+4)}$

$= P\cdot[1+(5x+4)(5x+3)]$

$1+25x^2+35x+12$

$= 4x^2+6$

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

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

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

$= 5x^7+4x^5+4x^4+5x^2+2$

$x^3 = -x-1$

$x^7 = (x-1)^2x = (x^2+2x+1)x$

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

$= (2x^2-1)\times 5$

$x^5 = (x-1)x^2 = -x^3-x^2$

$= (-x^2+x+1)\times 4$

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

$10x^2-5-4x^2+4x+4-4x^2-4x+5x^2+2$

$= 7x^2+0.x+1 = 1$

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

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

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

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

   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 ?

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

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

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. Semble-t-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 $\mathbb{Z}[\sqrt{2}]$.

Tous les elts inversible de $\mathbb{Z}[i]$

Soit x tq $\exists y$ tq $xy = 1 \to N(xy) = N(1) = 1$

$N(xy) = N(x)\,N(y)$

$N(x) \in \mathbb{N}$ $\quad N(y) \in \mathbb{N}$

donc $N(x) = N(y) = 1$

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

ou $a = 0$ et $|b| = 1$

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

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

$i \cdot (-i) = 1$

les elts inversible de $\mathbb{Z}[i]$: $\{1, -1, i \text{ et } -i\}$

---

si p est reductible $\quad p = xy \Rightarrow N(p) = N(xy) = N(x)\,N(y)$

x, y ni inversible $\quad = p^2$

$\Rightarrow N(x), N(y) \neq 1$

$N(x) \in \mathbb{N}$ $\quad N(y) \in \mathbb{N}$

$\neq 1, 0$ $\quad \neq 1, 0$

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

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