Arithmétique (suite)

Arithmétique des entiers.

Exercice 1 *L'équation diophantienne $x^2 + y^2 = p$. Entiers de Gauss.*

Le problème est de déterminer les entiers qui s'écrivent comme somme de deux carrés. Dans cet exercice on résoudra le cas des entiers premiers, le cas général s'en déduisant (voir [Perrin] p.56).

Soit $\Sigma = \{n \in \mathbb{N} \mid n = x^2 + y^2,\ x, y \in \mathbb{N}\}$.

1. Déterminer les carrés de $\mathbb{Z}/4\mathbb{Z}$ et en déduire que si $n \in \Sigma$, alors $n \not\equiv 3$ [4].

2. Montrer que $2 \in \Sigma$ et que 2 n'est pas irréductible dans $\mathbb{Z}[i]$.

Pour mimer les méthodes arithmétiques utilisées dans $\mathbb{Z}$, on est naturellement conduit à étudier les éléments irréductibles de $\mathbb{Z}[i]$.

A. *La norme et les inversibles de $\mathbb{Z}[i]$.*

On considère l'application $N : \mathbb{Z}[i] \to \mathbb{N}$, appelée "norme", définie par $N(a + ib) = a^2 + b^2$.

3. Montrer que N est multiplicative : pour tout $z, z' \in \mathbb{Z}[i]$, on a $N(z\,z') = N(z)\,N(z')$.

4. Déterminer $U(\mathbb{Z}[i])$.

5. En déduire qu'un nombre premier p appartient à Σ si et seulement si il n'est pas irréductible dans $\mathbb{Z}[i]$.

B. *L'anneau $\mathbb{Z}[i]$ est euclidien (donc principal, donc factoriel).*

6. Montrer que tout nombre complexe z est à distance euclidienne inférieure ou égale à $\frac{\sqrt{2}}{2}$ d'un élément de $\mathbb{Z}[i]$.

7. En déduire qu'il existe une division euclidienne dans $\mathbb{Z}[i]$ relativement à la norme N :

$$\forall a, b \in \mathbb{Z}[i],\ b \neq 0,\ \exists c, r \in \mathbb{Z}[i] \text{ tels que } a = bc + r \text{ et } N(r) < N(b)$$

(sans nécessairement unicité).

8. Faire la divisition euclidienne de $3 + 2i$ par $1 - 3i$ dans $\mathbb{Z}[i]$.

C. *Quotient par l'idéal engendré par un élément non irréductible.*

Soit p un nombre premier.

9. Montrer que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si $\mathbb{Z}[i]/(p)$ est intègre (indication : utiliser le fait que l'anneau $\mathbb{Z}[i]$ est euclidien, donc factoriel).

10. En utilisant l'isomorphisme $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2+1)$ (voir exercice en fin de feuille), en déduire que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si le polynôme $X^2 + 1$ n'a pas de racine dans $\mathbb{F}_p$.

11. En déduire pour tout nombre premier p impair l'équivalence des propriétés suivantes :

a. p appartient à Σ

b. -1 est un carré dans $\mathbb{F}_p$

c. $(-1)^{\frac{p-1}{2}} = 1$

d. $p \equiv 1$ [4].

Les nombres premiers qui appartiennent à Σ sont donc 2 et les nombres premiers p tels que $p \equiv 1$ [4].

Arithmétique des polynômes.

Exercice 2 *Anneau des polynômes sur un anneau non intègre et lemme chinois.*

1. Montrer que si $\mathbb{K}$ est un corps et $n \in \mathbb{N}$, tout polynôme de degré n de $\mathbb{K}[X]$ possède au plus n racines dans $\mathbb{K}$.

2. Déterminer les racines du polynôme $X^2 - \overline{1}$ de $(\mathbb{Z}/15\mathbb{Z})[X]$, en remarquant qu'une racine est un élément de $U(\mathbb{Z}/15\mathbb{Z})$.

3. Soit n un entier impair, $n \geq 3$. Montrer que le nombre de racines du polynôme $X^2 - \overline{1}$ de $(\mathbb{Z}/n\mathbb{Z})[X]$ est 2^k où k est le nombre de facteurs premiers de la décomposition de n (indication : réduire l'équation $x^2 - 1 \equiv 0\ [n]$ aux diviseurs de n).

Exercice 3 *(irréductibilité et quotient)*

Soient $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$.
Montrer que $\mathbb{K}[X]/(P)$ est un corps si et seulement si P est irréductible.
Comment ce résultat se généralise-t-il ?

Exercice 4

1. Quels sont les polynômes irréductibles de $\mathbb{C}[X]$? de $\mathbb{R}[X]$?

2. Montrer qu'un polynôme de degré 3 de $\mathbb{Q}[X]$ sans racine (dans $\mathbb{Q}$) est irréductible.

3. Donner un polynôme de degré 4 de $\mathbb{Q}[X]$ sans racine (dans $\mathbb{Q}$) mais pas irréductible.

On verra (de deux manières différentes) dans l'exercice suivant qu'il y a des polynômes irréductibles dans $\mathbb{Q}[X]$ de tout degré.

Exercice 5 *(irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$)*

Références : [Gourdon, Algèbre, p.58], [X-ENS algèbre 1, ex. 5.12]

A. Contenu d'un polynôme à coefficients dans $\mathbb{Z}$

1. Soient $P, Q \in \mathbb{Z}[X]$. Montrer que si un nombre premier p divise tous les coefficients du polynôme PQ, alors soit il divise tous les coefficients du polynôme P ou tous les coefficients du polynôme Q.

On appelle *contenu* d'un polynôme de $\mathbb{Z}[X]$ le pgcd (dans $\mathbb{N}$) de ses coefficients. On note $c(P)$ le contenu du polynôme P.

2. Montrer que $c(PQ) = c(P)c(Q)$ pour tous $P, Q \in \mathbb{Z}[X]$.

B. irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$ (variante de la preuve de Gourdon)

Soit $P \in \mathbb{Z}[X]$.

3. Montrer que si $c(P) \neq 1$, alors P n'est pas irréductible dans $\mathbb{Z}[X]$.

On suppose désormais que $c(P) = 1$ et que P est irréductible dans $\mathbb{Z}[X]$. On va montrer que P est irréductible dans $\mathbb{Q}[X]$. Supposons que $P = P_1 P_2$ avec $P_1, P_2 \in \mathbb{Q}[X]$.

4. Montrer qu'il existe $\alpha_1, \alpha_2 \in \mathbb{N}$ tels que $\alpha_i P_i \in \mathbb{Z}[X]$ et $\alpha_i \wedge c(\alpha_i P_i) = 1$ pour $i = 1, 2$.

5. Montrer que $\alpha_1 \alpha_2 = c(\alpha_1 P_1)c(\alpha_2 P_2)$ et en déduire que $\alpha_1 = c(\alpha_2 P_2)$ et $\alpha_2 = c(\alpha_1 P_1)$.

6. Conclure.

7. Application : soient $a_1, \dots a_n \in \mathbb{Z}$ des entiers deux à deux distincts. Montrer que le polynôme $(X - a_1) \dots (X - a_n) - 1$ est irréductible dans $\mathbb{Q}[X]$. Indication : évaluer les polynômes en $a_1, \dots a_n$.

C. Application : critère d'Eisenstein

8. Soit $P = a_n X^n + ... + a_0 \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que p divise $a_0, \dots a_n n - 1$, p ne divise pas a_n et p^2 ne divise pas a_0. En réduisant modulo p, montrer que P est irréductible dans $\mathbb{Q}[X]$.

9. Donner des polynômes irréductibles de tout degré dans $\mathbb{Z}[X]$ vérifiant le critère d'Eisenstein.

10. Montrer que les polynômes suivants sont irréductibles dans $\mathbb{Q}[X]$ (indication : pour tout $a \in \mathbb{Q}$, $P(X)$ est irréductible si et seulement si $P(X + a)$ est irréductible) :

a. $X^4 + 6X^3 - 12X^2 + 3X + 15$, **b.** $X^4 + 1$, **c.** $X^p + X^{p-1} + \dots + 1$ pour tout p premier.

Exercice 6 *Racines d'un polynôme de $\mathbb{Z}[X]$ ou $\mathbb{Q}[X]$*

Soit $P(X) = a_n X^n + \cdots + a_0$ un polynôme de $\mathbb{Q}[X]$ dont les coefficients $a_0, \ldots, a_n$ sont entiers.

1. Montrer que si un rationnel $x = \frac{p}{q}$ est racine de P, où p et q sont des entiers premiers entre eux, alors p divise a_0 et q divise a_n.

2. Les polynômes suivants de $\mathbb{Q}[X]$ ont-ils des racines dans $\mathbb{Q}$?

a. $5X^3 + X^2 - 1$ **b.** $X^4 + 3X^3 - 3X^2 - 12X - 4$

Exercice 7 *Un algorithme de factorisation dans $\mathbb{Z}[X]$ [ref ?]*

On considère le polynôme $P(X) = X^5 + X^4 + 2X^2 - 1$.

1. Montrer que si P n'est pas irréductible dans $\mathbb{Z}[X]$, alors il existe un polynôme de degré un ou deux qui divise P dans $\mathbb{Z}[X]$.

On suppose qu'il existe un tel polynôme $Q \in \mathbb{Z}[X]$.

2. Calculer $P(0)$, $P(1)$ et $P(-1)$. En déduire toutes les valeurs possibles pour $Q(0)$, $Q(1)$ et $Q(-1)$, donc toutes les valeurs possibles de Q.

3. Factoriser P dans $\mathbb{Z}[X]$.

Exercice 8 *(irréductibilité par réduction modulo 2)*

[Gourdon, Algèbre, ex.11 p.69]

Soit $P = a_n X^n + ... + a_0 \in \mathbb{Z}[X]$ et p un nombre premier. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$ et $\overline{P} = \overline{a_n} X^n + ... + \overline{a_0} \in \mathbb{F}_p[X]$ l'image du polynôme P dans $\mathbb{F}_p[X]$.

1. Montrer que si $\overline{P}$ est irréductible, alors P l'est aussi. La réciproque est-elle vraie ?

2. Montrer que le polynôme $X^4 + X + 1$ de $\mathbb{Z}[X]$ est irréductible (indication : le réduire modulo 2).

Exercice 9 *(irréductibilité et réduction modulo p)*

On rappelle que le polynôme $P = X^4 + 1$ est irréductible sur $\mathbb{Z}$ (et sur $\mathbb{Q}$). Nous allons montrer qu'il est réductible modulo p pour tout nombre premier p.

1. Montrer que P est réductible modulo 2.

2. Soit p un nombre premier tel que -1 est un carré modulo p (c'est-à-dire $p \equiv 1[4]$ d'après l'exercice 1). Montrer que P est réductible modulo p.

3. Soit p un nombre premier tel que 2 est un carré modulo p. Montrer que P est réductible modulo p. Indication : utiliser le fait que $X^4 + 1 = (X^2 + 1)^2 - 2X^2$).

4. Soit p un nombre premier tel que -2 est un carré modulo p. Montrer que P est réductible modulo p.

5. Montrer que si -1 et 2 ne sont pas des carrés modulo p, alors -2 est un carré modulo 2 (indication : caractériser les carrés de $\mathbb{F}_p$ comme dans l'exercice 1).

6. Conclure.

Exercice 10 *Quotients et isomorphismes.*

Pour tout $\omega \in \mathbb{C}$, on note $\mathbb{Z}[\omega] = \{P(\omega),\ P \in \mathbb{Z}[X]\}$.

1. Décrire les éléments de $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{5}]$, $\mathbb{Z}[j]$, $\mathbb{Z}[\pi]$.

2. Montrer que les anneaux suivants sont isomorphes :

a. $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[X]/(X^2 - 2)$. **b.** $\mathbb{Z}[i]$ et $\mathbb{Z}[X]/(X^2 + 1)$.

3. Décrire les anneaux $\mathbb{Z}[j]$, $\mathbb{Z}[1 + i]$ comme des quotients de l'anneau $\mathbb{Z}[X]$.

4. Décrire l'anneau $\mathbb{Z}[X]/(10X - 1)$ comme un sous-anneau de $\mathbb{C}$.

5. Montrer que $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{R}[X]/(X^2 + X + 1)$.

6. Que peut-on dire de $\mathbb{R}[X]/(X - a)$, $a \in \mathbb{R}$? $\mathbb{R}[X]/(X^2 + 1)$?

7. Montrer que $\mathbb{R}[X]/(X^2 - 1)$ est isomorphe à $\mathbb{R} \times \mathbb{R}$ muni de la loi + habituelle et de la loi $\times$ définie par $(a, b) \times (a', b') = (aa' + bb', ab' + a'b)$. Est-ce un corps ?

8. Décrire les quotients $\mathbb{Q}[X]/(X^2 + 1)$, $\mathbb{Q}[X]/(X^2 - 2)$. Sont-ils isomorphes ?

9. Montrer les isomorphismes suivants pour p premier et d entier, $d \geq 1$:

$$\mathbb{Z}[i\sqrt{d}]/(p) \simeq \mathbb{Z}[X]/(X^2 + d, p) \simeq \mathbb{F}_p[X]/(X^2 + d).$$

Exercice 11 *(Construction de corps finis, [Skandalis, exercice 4.16])*

1. Montrer que tout corps fini est de cardinal p^α pour un nombre premier p et un entier $\alpha \geq 1$.

2. Soit K un corps fini à q éléments. Combien y a-t-il de polynômes irréductibles unitaires de degré 2 dans $K[X]$? de degré 3 ?

3. Déterminer les polynômes irréductibles unitaires de degre 2 et 3 dans $\mathbb{F}_2[X]$ et $\mathbb{F}_3[X]$.

4. **a.** Construire des corps à 4, 8, 9, 27 éléments.

b. Construire des corps à 25, 49, 121 éléments.