Quelques indications de la feuille de TD n°7

Exo. 7. en effet, pour $n \in S$ un élément nilpotent (c-à-d, il existe $r \in \mathbb{Z}_{\geq 1}$ tel que $n^r = 0$), on a

$$(1-n)^{-1} = \sum_{i=0}^{+\infty} n^i = 1 + n + n^2 + \cdots + n^r.$$

Pour généralement, soit $x \in A$ inversible, $a \in A$ nilpotent tels que a et x commutent. Alors $x^{-1}a \in A$ est encore nilpotent, et on a $(x^{-1}a)^i = x^{-i}a^i$. Par suite,

$$(x-a)^{-1} = (x(1-x^{-1}a))^{-1} = (1-x^{-1}a)^{-1}x^{-1} = (\sum_{i=0}^{+\infty} x^{-i}a^i) \cdot x = \sum_{i=0}^{+\infty} x^{1-i}a^i.$$

Remarquons que, comme a est nilpotent, la somme ci-dessus est une somme *finie*.

Exo. 8. Pour tout $u \in (\mathbb{Z}/p\mathbb{Z})^*$, on a l'égalité suivante d'ensembles :

$$\mathbb{Z}/p\mathbb{Z} - \{0\} = \{x | x \in \mathbb{Z}/p\mathbb{Z} - \{0\}\ \} = \{u \cdot x | x \in \mathbb{Z}/p\mathbb{Z} - \{0\}\ \}.$$

Ainsi, on a

$$S_\alpha = \sum_{k=1}^{p-1} \bar{k}^\alpha \in \mathbb{Z}/p\mathbb{Z} = \sum_{x \in \mathbb{Z}/p\mathbb{Z}-\{0\}} x^\alpha = \sum_{ux \in \mathbb{Z}/p\mathbb{Z}-\{0\}} (ux)^\alpha = \sum_{x \in \mathbb{Z}/p\mathbb{Z}-\{0\}} u^\alpha x^\alpha = u^\alpha S_\alpha.$$

D'où la première assertion. En suite, lorsque $(p-1)|\alpha$, on a $x^\alpha = 1$ pour tout $x \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ (car le groupe $(\mathbb{Z}/\mathbb{Z})^*$ est cyclique d'ordre $p-1$). Par suite, on a

$$S_\alpha = \sum_{x \in \mathbb{Z}/p\mathbb{Z}-\{0\}} x^\alpha = \sum_{x \in \mathbb{Z}/p\mathbb{Z}-\{0\}} 1 = p - 1 = -1 \in \mathbb{Z}/p\mathbb{Z}.$$

D'où (2). Montrons ensuite (3). Soit α un entier tel que $0 < \alpha < p-1$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, le polynôme $X^\alpha - 1$ a au plus α racines dans $\mathbb{Z}/p\mathbb{Z}$. Or comme $|\mathbb{Z}/p\mathbb{Z} - \{0\}| = p - 1 > \alpha$, il peut trouver donc un élément $u \in \mathbb{Z}/p\mathbb{Z} - \{0\}$ tel que $u^\alpha \neq 1$. Par suite, en vertu de la formule dans la question (1), on a $(u^\alpha - 1)S_\alpha = 0 \in \mathbb{Z}/p\mathbb{Z}$. Or $\mathbb{Z}/p\mathbb{Z}$ est un corps avec $u^\alpha - 1 \neq 0$, on a donc $S_\alpha = 0$. Ceci finit (3). Pour la dernière question, remarquons que pour tout $\alpha \in \mathbb{Z}$ et pour tout $x \in \mathbb{Z}/p\mathbb{Z} - \{0\}$, on a $x^{\alpha+(p-1)} = x^\alpha x^{p-1} = x^\alpha$. Ainsi, on trouve $S_\alpha = S_{\alpha+(p-1)}$. Soit maintenant $\alpha \in \mathbb{Z}$ tel que $(p-1)$ ne divise pas α. Par la division euclidienne, on peut trouver un entier $k \in \mathbb{Z}$, et r $\mathbb{Z}/p\mathbb{Z}$ tel que $0 < r < p-1$, et que $\alpha = k \cdot (p-1) + r$. Par suite on a $S_\alpha = S_{k\cdot(p-1)+r} = S_r = 0$, ici la dernière égalité résulte de la question (3). Ceci achève la preuve.

Exo. 11. Notons n le nombre de pièces de ce trésor. Alors cet entier n vérifie le système de congruences suivant

$$(S) \quad \begin{cases} n & \equiv & 3 & [17] \\ n & \equiv & 4 & [11] \\ n & \equiv & 5 & [6] \end{cases}.$$

Comme les trois entiers $17, 11, 6$ sont deux à deux premiers entre eux, pour résoudre ce système de congruences, on regard d'abord le sous-système suivant

$$(S_1) \quad \begin{cases} n & \equiv & 3 & [17] \\ n & \equiv & 4 & [11] \end{cases}.$$

En utilisant la division euclidienne, on trouve une identité de Bézout sous la forme suivante

$$2 \times 17 - 3 \times 11 = 1$$

Ainsi, les solutions pour le système (S_1) snt les entiers de la forme suivante

$$3 \times (-3 \times 11) + 4 \times (2 \times 17) + k \times 17 \times 11 = 37 + 187 \cdot k, \quad k \in \mathbb{Z}.$$

Pour résoudre le système (S), il suffit maintenant regarder le système suivant

$$(S_2) \quad \begin{cases} n & \equiv & 37 & [187] \\ n & \equiv & 5 & [6] \end{cases}.$$

Par division euclidienne, on a l'identité de Bézout de la forme suivante

$$187 - 31 \times 6 = 1$$

Ainsi, les solutions pour (S_2) sont

$$37 \times (-31 \times 6) + 5 \times 187 + k \times 187 \times 6 = -5947 + 1122 \cdot k, \quad k \in \mathbb{Z}$$

le plus petit entier non négatif parmi ces entiers est

$$-5947 + 1122 \times 6 = 785.$$

Donc, la fortune minimale est 785 pièces.

Exo. 12 :

- Pour $A = \mathbb{Z}$. Les éléments inversibles sont ± 1, et les éléments irréductibles sont $\pm p$ avec $p \in \mathbb{Z}$ un premier.
- Pour $A = \mathbb{C}[X]$. Les éléments inversibles sont les $u \in \mathbb{C}^*$ (c-à-d : les fonctions constantes non nulles). Les éléments irréductibles sont $\lambda \cdot (X - c)$ avec $\lambda \in \mathbb{C}^*$, et $c \in \mathbb{C}$.
- Pour $A = \mathbb{R}[X]$. Les éléments inversibles sont les $u \in \mathbb{R}^*$ (c-à-d : les fonctions constantes non nulles). Les éléments irréducibles sont :
  * $\lambda \cdot (X - c)$ avec $\lambda \in \mathbb{R}^*$, et $c \in \mathbb{R}$.
  * $\lambda(X^2 + a \cdot X + b)$ avec $\lambda \in \mathbb{R}^*$, et $a, b \in \mathbb{R}$ tels que le discriminant $\Delta = a^2 - 4b < 0$ (ce qui entraîne que ce polynôme n'admet pas de racine réelle).

Exo. 13.

1. Vérification directe.
2. Montrons d'abord que l'application

   $$N \colon \mathbb{Z}[i] \to \mathbb{Z}, \quad z = a + ib \mapsto a^2 + b^2$$

   est multiplicative, c-à-d : $N(z \cdot w) = N(z)N(w)$ pour tout $z, w \in \mathbb{Z}[i]$. En effet, écrivons $z = a + ib$, et $w = c + id$ avec $a, b, c, d \in \mathbb{Z}$. Alors $zz' = (a + ib)(c + id) = (ac - bd) + i(ad + bc)$. Par suite

   $$N(z \cdot w) = (ac - bd)^2 + (ad + bc)^2 = a^2c^2 + b^2d^2 - 2abcd + a^2d^2 + b^2c^2 + 2abcd = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2.$$

   D'autre part, $N(z) = a^2 + b^2$, et $N(w) = c^2 + d^2$. Ainsi

   $$N(z) \cdot N(w) = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2.$$

   D'où $N(z \cdot w) = N(z) \cdot N(w)$. Soit maintenant $z \in \mathbb{Z}[i]^*$ inversible. Par suite, on peut trouver $w \in \mathbb{Z}[i]$ tel que $zw = 1$. Ainsi $1 = N(1) = N(zw) = N(z)N(w)$. Or comme $N(z) \in \mathbb{Z}_{\geq 0}$, on a donc $N(z) = 1$. Réciproquement, soit $z = a + ib \in \mathbb{Z}[i]$ tel que $N(z) = a^2 + b^2 = 1$. Par suite, on a

   $$1 = a^2 + b^2 = (a + ib)(a - ib).$$

   Donc l'élément $z = a + ib$ est bien inversible. Ainsi

   $$\mathbb{Z}[i]^* = \{\ a + ib \in \mathbb{Z}[i] \mid a^2 + b^2 = 1\ \} = \{1, -1, i, -i\}.$$

   En particulier, c'est un sous-groupe cyclique d'ordre 4, engendré par i.
3. L'élément $2 \in \mathbb{Z}[i]$ n'est pas irréductible. En effet, on a $2 = (1 + i)(1 - i)$ avec $1 + i, 1 - i \in \mathbb{Z}[i]$ *non inversibles*. Par suite, 2 n'est pas irréductible dans $\mathbb{Z}[i]$.

   Par contre, l'élément $3 \in \mathbb{Z}[i]$ est irréductible. On va raisonner par l'absurde : supposons $3 = z \cdot w$ avec $z, w \in \mathbb{Z}[i]$ *non inversibles*. On aurait alors

   $$9 = N(3) = N(z)N(w).$$

Comme $z, w \in \mathbb{Z}[i]$ non inversibles, d'après (2), on a $N(z) > 1$, et $N(w) > 1$. Par suite, on a $N(z) = N(w) = 3$. Ecrivons ensuite $z = a + ib$, on aurait alors

$$3 = N(z) = a^2 + b^2.$$

Mais on peut vérifier aisément que l'équation $a^2 + b^2 = 3$ n'admet pas de solution dans $\mathbb{Z}$, d'où une contradiction. Donc 3 est irréductible.

Exo. 17.

1. Déjà vu en TD.
2. Remarquons que $F := \mathbb{Z}/3\mathbb{Z}$ est un corps à 3 éléments : $0, 1, 2 \in F$. Ici, il suffit de trouver tous les polynômes irréductibles de degrés $1, 2, 3, 4$ qui sont *unitaire*[1]. On va distinguer les 4 cas suivants :
   – Les éléments unitaires de degré 1 de $\mathbb{Z}/3\mathbb{Z}[X]$ sont : X, $X+1$, et $X+2$, qui sont bien sûr irréductibles.
   – Les éléments unitaires de degré 2 de $\mathbb{Z}/3\mathbb{Z}[X]$ sont : X^2, X^2+1, X^2+2, X^2+X, X^2+X+1, X^2+X+2, X^2+2X, X^2+2X+1, X^2+2X+2. Parmi ces 9 éléments, les irréductibles sont :

   $$X^2+1, \quad X^2+X+2, \quad X^2+2X+2$$

   Par exemple, pour vérfier que X^2+2X+2 est irréductible, il suffit de vérifier que ce polynôme n'admet pas de racine dans $\mathbb{Z}/3\mathbb{Z}$.....
   – On peut procéder d'une manière similaire, mais le calcul devient de plus en plus fastidieux....Voici donc la liste des polynômes irréductibles unitaires de degré 2 :

   $$X^3+2X+1, \quad X^3+2X+2, \quad X^3+X^2+2, \quad X^3+X^2+X+2,$$
   $$X^3+X^2+2X+1, \quad X^3+2X^2+1, \quad X^3+2X^2+X+1, \quad X^3+2X^2+2X+2.$$

   – Voici la liste des polynômes irréductibles unitaires de degré 4 :

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

Exo. 19. Remarquons que l'anneau $A = \mathbb{Z}/3\mathbb{Z}[X]$ est de caractéristique 3, par suite, pour tout $a, b \in A$, on a $(a+b)^3 = a^3 + b^3$.

1. $P(X)$ est réductible car $P(1) = 1+1+1 = 0$, donc $P(X)$ contient un facteur de degré 1 : $X-1$. Par contre $Q(X)$ est irréductible car $Q(0) \neq 0$, $Q(1) \neq 0$ et $Q(2) \neq 0$. Donc $Q(X)$ ne contient pas de facteur de degré 1. D'autre part, comme Q est de degré 2, ceci implique alors que $Q(X)$ est irréductible. Par suite, l'idéal $(Q(X)) \subset \mathbb{Z}/3\mathbb{Z}[X]$ engendré par $Q(X)$ est maximal. Ainsi, le quotient

   $$F' := \frac{\mathbb{Z}/3\mathbb{Z}[X]}{(Q(X))}$$

   est un corps, degré 3 sur $\mathbb{Z}/3\mathbb{Z}$. Ainsi, F' est un corps de 9 éléments (en effet, F' est un espace vectoriel de dimension sur $\mathbb{Z}/3\mathbb{Z}$ avec une base donnée par $1, \beta$, avec β la classe de X dans F').
2. Montrons que $\alpha \in F'$ est un élément d'ordre 8 :
   – Montrons d'abord que $\alpha \in F'$ est d'ordre divisant 8 : c-à-d, $\alpha^8 = 1$. Comme $\alpha \in F'$ est non nul (car $\alpha = 0$ signifie que $X - 1 \in (Q(X))$, ce qui n'est pas possible pour la raison de degré), il revient au même de prouver $\alpha^9 = \alpha$: remarquons que β est la classe de X dans le quotient F', alors $\alpha = \beta + 1$, et on a $\beta^2 + 1 = 0$:

   $$\alpha^9 - \alpha = (\beta+1)^9 - (\beta+1) = \beta^9 + 1^9 - (\beta+1) = \beta^9 - \beta = (\beta^2)^4 \cdot \beta - \beta = (-1)^4 \cdot \beta - \beta = 0.$$

   Ainsi $\alpha^9 = \alpha$. Par suite, $\alpha^8 = 1$. Donc α est d'ordre divisant 8.
   – Montrons que $\alpha^4 \neq 1$. En effet, comme $\alpha^4 - 1 = (\beta+1)^3(\beta+1) - 1 = (\beta^3+1)(\beta+1) - 1$. Par suite,

   $$\alpha^4 - 1 = (\beta^3+1)(\beta+1) - 1 = \beta^4 + \beta^3 + \beta = (\beta^2)^2 + \beta^2\beta + \beta = 1 - \beta + \beta = 1.$$

   En particulier, on a $\alpha^4 - 1 \neq 0$. Donc α est d'ordre 8. Comme $F'^* = F' - \{0\}$ est à 8 éléments. Par suite, F'^* est cyclique d'ordre 8, engendré par α. Ceci finit donc la preuve.

1. Soit k un corps. Un polynôme non nul $f \in k[X]$ est dit *unitaire* si son coefficient dominant est égal à 1.