ATN 2010 - Correction des exercices 7, 8, 9, 10, 11, 12 et 13 du TD n°7.

Je ferai quelques commentaires : *ils seront en italique.*

Rappels.

1. Soit P un polynôme de $\mathbb{Z}[X]$. On a l'équivalence suivante :
   P est irréductible $\iff$ P est primitif (i.e. son contenu est 1) et P est irréductible sur $\mathbb{Q}$.

2. Soit a un élément d'un anneau A.
   a est irréductible ssi, par définition, il est non inversible et si lorsqu'on l'écrit $a = a_1 a_2$ alors l'un des a_i est inversible.

   Étant donné un anneau A, un polynôme $P \in A[X]$ est inversible ssi c'est un polynôme constant $P = a$ et a est inversible dans A (démontrez le).

3. Étant donné un corps $\mathbb{K}$ commutatif, soit $P \in \mathbb{K}[X]$ un polynôme *de degré au plus 3.*
   P est réductible si et s. si P admet une racine (démontrez le).

   L'exemple suivant montre que cette équivalence n'est pas vrai si le polynôme P est de degré ≥ 4 :
   $P = (X^2+1)(X^2+2) \in \mathbb{R}[X]$ est réductible mais n'admet aucune racine (dans $\mathbb{R}$ bien entendu).

Exercice 7.7. *Je ne vais traîter que la première question.*
Notons $P = 3X^3 + 2X^2 + X + 4$. Nous allons montrer que P est irréductible sur $\mathbb{Q}$.

Par l'absurde supposons P réductible sur $\mathbb{Q}$. Alors par le rappel 1, P est réductible sur $\mathbb{Z}$. Ainsi il existe deux polynômes $S, T \in \mathbb{Z}[X]$ tels que $P = ST$. Étant donné que P est primitif, les polynômes S et T sont non constants. Ainsi l'un de ces deux polynômes est de degré 1 et l'autre de degré 2. Il existe donc $a, b, c, d, e \in \mathbb{Z}$ tels que

$$P = (bX - a)(cX^2 + dX + e).$$

Si on développe et qu'on identifie termes à termes, on constate que $bc = 3$ et $-ae = 4$. Ainsi 3 divise b et 4 divise a. On en déduit que $b \in \{1, -1, 3, -3\}$ et $a \in \{1, -1, 2, -2, 4, -4\}$.

En conséquence le polynôme P admet une racine rationnelle $\frac{a}{b}$ telle que :

$$\frac{a}{b} \in \{1, \frac{1}{3}, 2, \frac{2}{3}, 4, \frac{4}{3}, -1, -\frac{1}{3}, -2, -\frac{2}{3}, -4, -\frac{4}{3}\}.$$

Or, P n'a que des coefficients positifs donc il ne peut admettre de racines positifs d'où

$$\frac{a}{b} \in \{-1, -\frac{1}{3}, -2, -\frac{2}{3}, -4, -\frac{4}{3}\}.$$

Après calcul on obtient :

$$P(-1) = 2,\ P(-\frac{1}{3}) = \frac{34}{9},\ P(-2) = -14,\ P(-\frac{2}{3}) = \frac{10}{3},\ P(-4) = -160,\ P(-\frac{4}{3}) = -\frac{8}{9}.$$

La contradiction recherchée est acquise.

Exercice 7.8.

1. Le cas de P_1 a été fait en TD. Voyons pour P_2. Le contenu de P_2 (i.e. pgcd dans $\mathbb{Z}$ de ses coefficients) est 3 donc P_2 n'est pas irréductible dans $\mathbb{Z}[X]$. En effet on peut le décomposer comme : $P_2(X) = 3 \cdot Q_2(X)$ où $Q_2(X) = X^4 - 5X^2 + 10$.

   Le polynôme constant 3 étant inversible dans $\mathbb{Q}[X]$, $P_2(X)$ est irréductible dans $\mathbb{Q}[X]$ si et s. si $Q_2(X)$ l'est. Si on applique le critère d'Eisenstein avec $p = 5$ on obtient l'irréductibilité de Q_2 (donc de P_2) sur $\mathbb{Q}$.

2. (a) $Q(X) = X^2 + X + 2$. Ici l'idée est de considérer le polynôme : $\tilde{Q}(X) = Q(X+3)$.
On voit facilement que Q est réductible si et s. si $\tilde{Q}$ est réductible. (Faire les détails en exercice).
Ensuite, on applque le critère d'Eisenstein avec $p = 7$ pour

$$\tilde{Q}(X) = Q(X+3) = X^2 + 7X + 14$$

pour conclure que Q est irréductible dans $\mathbb{Z}[X]$ et donc dans $\mathbb{Q}[X]$ (car Q est primitif).

(b) $R(X) = 10X^2 + X - 4$. Suivre l'indication et appliquer Eisenstein avec $p = 7$.

(c) $S(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$.
Soit $T(X) = S(X+1)$. Alors $T(X)$ est la somme de
$(X+1)^{p-1} = \sum_{k=0}^{p-1} \binom{p-1}{k} X^k$ et
$(X+1)^{p-2} = \sum_{k=0}^{p-2} \binom{p-2}{k} X^k$ et
$\cdots$.
Ainsi pour $k_0 \in \{1, \ldots, p-2\}$ le coefficient devant X^{k_0} est

$$\sum_{j=k_0}^{p-1} \binom{j}{k_0} = \binom{p}{1+k_0}.$$

Ainsi p divise tous ces coefficients. De plus p divise le coefficient "constant" (i.e. devant X^0) qui est p sans que p^2 ne le divise. Enfin p ne divise pas le coefficient dominant (i.e. devant X^{p-1}) qui est 1. Par Eisenstein T et donc S est irréductible sur $\mathbb{Q}$ (donc sur $\mathbb{Z}$ car S est primitif).

Exercice 7.9.
On sait que $\mathbb{Z}/6\mathbb{Z}$ est un groupe monogène donc tout sous-groupe est aussi monogène (voir les fiches de TD sur les groupes) et donc tout idéal de $\mathbb{Z}/6\mathbb{Z}$ est principal. On peut donc faire la liste complète de ses idéaux.
$I_1 = \langle 1 \rangle = \mathbb{Z}/6\mathbb{Z}$,
$I_2 = \langle 2 \rangle = \{0, 2, 4\}$,
$I_3 = \langle 3 \rangle = \{0, 3\}$.
Ce sont les seuls car on voit facilement que les idéaux engendrés par $4 = -2$ ou $5 = -1$ sont parmi les précédents.

Rappel.
Un idéal (propre) I est premier ssi A/I est intègre et I (propre) est maximal ssi A/I est un corps.

Ainsi I_1 n'étant pas propre n'est pas premier (et donc pas maximal).

Juste en regardant son cardinal on voit que $(\mathbb{Z}/6\mathbb{Z})/I_2$ est isomorphme au corps à deux éléments $\{0, 1\} \simeq \mathbb{Z}/2\mathbb{Z}$. Ainsi I_2 est maximal (et donc premier).

Pour finir on a un morphime naturel de $\mathbb{Z}$ vers $(\mathbb{Z}/6\mathbb{Z})/I_3$. Ce morphisme est surjectif. De plus on obtient facilement que son noyau est $3\mathbb{Z}$ d'où un isomorphisme

$$(\mathbb{Z}/6\mathbb{Z})/I_3 \simeq \mathbb{Z}/3\mathbb{Z}.$$

Ainsi par le rappel I_3 est maximal.

Exercice 7.10
Rappelons que $\mathbb{F}_5$ n'est rien d'autre que le corps $\mathbb{Z}/5\mathbb{Z}$ de cardinal 5. Notons $P = X^2+1$ et $Q = X^3+X+1$.

En utilisant le rappel 3, il suffit de vérifier si ces polynômes ont une racine dans $\mathbb{Z}/5\mathbb{Z}$.

Concernant P : $P(\bar{0}) = \bar{0}$, $P(\bar{1}) = \bar{2}$, $P(\bar{2}) = \bar{5} = \bar{0}$. Ainsi P admet $\bar{2}$ comme racine, il est donc réductible. On a en fait $P = (X - \bar{2})(X - \bar{3})$.

Concernant Q : $Q(\bar{0}) = \bar{1}$, $Q(\bar{1}) = \bar{3}$, $Q(\bar{2}) = \overline{11} = \bar{1}$, $Q(\bar{3}) = \bar{1}$, $Q(\bar{4}) = Q(\overline{-1}) = \overline{-1} = \bar{4}$. Ainsi Q est irréductible.

Exercice 7.11.
Nous allons énoncés quelques résultats intermédiaires utiles pour répondre aux questions.
Le point (a) suivant est classique dans ce genre de situations. Un autre exemple classique est $\mathbb{Z}[i\sqrt{5}]$.

(a) Pour $z = a + b\sqrt{13} \in \mathbb{Z}[\sqrt{13}]$ (avec $a, b \in \mathbb{Z}$), on définit :
$\overline{z} = a - b\sqrt{13} \in \mathbb{Z}[\sqrt{13}]$,
$L(z) = a^2 - 13b^2 \in \mathbb{Z}$.

Avec ces définitions on a les propriétés suivantes :

- $\overline{z \cdot z'} = \overline{z} \cdot \overline{z'}$, $\overline{z + z'} = \overline{z} + \overline{z'}$.
- $L(z) = z \cdot \overline{z}$,
- $L(z) = L(-z) = L(\overline{z})$,
- $L(z \cdot z') = z\overline{z}z'\overline{z'} = (zz')\overline{zz'} = L(z) \cdot L(z')$

(b) Études des carrés de $\mathbb{Z}/13\mathbb{Z}$.
$1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 3$, $5^2 = 12$, $6^2 = 10$, $7^2 = (-6)^2 = 10$, $8^2 = (-5)^2 = 12$, etc.
Ainsi l'ensemble des carrés de $\mathbb{Z}/13\mathbb{Z}$ est $\{1,\ 3,\ 4,\ 9,\ 10,\ 12\}$.

(c) Étude des inversibles de $\mathbb{Z}[\sqrt{13}]$.
Affirmation : $z \in \mathbb{Z}[\sqrt{13}]$ est inversible $\iff L(z) \in \{-1, 1\}$.
En effet soit z inversible. Alors il existe $z' \in \mathbb{Z}[\sqrt{13}]$ tel que $zz' = 1$. Par suite, $1 = L(1) = L(zz') = L(z)L(z')$. Cette égalité ayant lieu dans $\mathbb{Z}$, on en déduit le résultat voulu. Réciproquement, supposons que $L(z) \in \{-1, 1\}$. Si $L(z) = 1$ alors par le (a), on obtient $z\overline{z} = 1$ d'où l'on déduit que z est inversible. Si $L(z) = -1$ alors $z \cdot (-\overline{z}) = 1$ et on conclut également.

Retournons à l'exercice proprement dit.

1. Soit $\alpha \in \{2, 3 - \sqrt{13}, -3 - \sqrt{13}\}$.
Alors $L(\alpha) \in \{-4, 4\}$. Soit z et z' dans $\mathbb{Z}[\sqrt{13}]$ tels que $\alpha = z \cdot z'$ le but étant de montrer que z ou z' est inversible.

On applique L à l'égalité $\alpha = z \cdot z'$ et on obtient : $L(z)L(z') \in \{-4, 4\}$. On a alors deux cas possibles :

- Cas 1. L'un parmi $L(z)$ et $L(z')$ vaut ± 1 et l'autre vaut ± 4. Dans ce cas, par (c), z ou z' est inversible.
- Cas 2. Les nombres $L(z)$ et $L(z')$ sont dans $\{-2, 2\}$.
Dans ce cas, écrivons $z = a + b\sqrt{13}$ avec $a, b \in \mathbb{Z}$. L'hypothèse signifie que

$$a^2 - 13b^2 = 2 \quad \text{ou bien} \quad a^2 - 13b^2 = -2.$$

Modulo 13 on obtient

$$a^2 \equiv 2\ [13] \quad \text{ou bien} \quad a^2 \equiv -2 \equiv 11\ [13].$$

En utilisant le point (b), on voit que ce cas est impossible.

Ainsi on est nécessairement dans le cas 1. On en conclut que α est irréductible par (c).

2. L'égalité suivante
$$2 \cdot 2 = (3 - \sqrt{13})(-3 - \sqrt{13})$$
montre que l'élément 4 s'écrit de deux façons différentes comme produit de deux irréductibles. Ainsi l'anneau $\mathbb{Z}[\sqrt{13}]$ n'est pas factoriel.

Exercice 7.12.

1. Soit $P(X) = \sum_{k=0}^{d} a_k X^k$ un polynôme quelconque de $K[X]$. Pour $\alpha \in K$, et pour $k \in \mathbb{N}$, on a :
$$X^k = (X - \alpha + \alpha)^k = \sum_{i=0}^{k} \binom{k}{i} (X - \alpha)^i \alpha^{k-i} = \alpha^k + (X - \alpha) \cdot Q_k(X)$$
avec $Q_k \in K[X]$. Ainsi
$$P(X) = \sum_{k=0}^{d} a_k \cdot (\alpha^k + (X - \alpha)Q_k(X)) = P(\alpha) + (X - \alpha)Q(X)$$
où $Q(X) = \sum_k a_k Q_k(X)$. Aurement dit
$$(\star) \qquad P(X) - P(\alpha) \in \mathbb{K}[X](X - \alpha).$$
Soit $\phi : \mathbb{K}[X] \to \mathbb{K}$ le morphisme d'évaluation en α donné par $\phi(P(X)) = P(\alpha)$. Alors ϕ est surjectif (car $\phi(c) = c$ pour tout $c \in K$). De plus la relation $(\star)$ implique que $\ker(\phi) = \mathbb{K}[X](X - \alpha)$. Le théorème d'isomorphisme de Noether nous permet de conclure.

2. Soit $P(X, Y) = \sum_{k,l} a_{kl} X^k Y^l$ un polynôme quelconque de $K[X, Y]$. Un calcul similaire au précédent nous permet d'écrire que
$$P(X, Y) - P(\alpha, Y) \in \mathbb{K}[X, Y](X - \alpha).$$
On considère le morphisme $P(X, Y) \mapsto P(\alpha, Y)$ et on raisonne de même.

3. Ici on fait encore de même en travaillant avec les deux variables; en écrivant $X = X - \alpha + \alpha$ et $Y = Y - \beta + \beta$. On obtient après calcul que
$$P(X, Y) - P(\alpha, \beta) \in \mathbb{K}[X, Y](X - \alpha, Y - \beta).$$
Le morphisme considéré est alors $P(X, Y) \mapsto P(\alpha, \beta)$. On utilise encore le théorème de Noether.

Remarquons en passant que l'idéal $K[X, Y](X - \alpha, Y - \beta)$ (engendré par les polynômes $X - \alpha$ et $Y - \beta$) n'est pas principal.
Ainsi l'anneau $K[X, Y]$ est factoriel mais non principal.

Exercice 7.13. On travaille dans l'anneau $\mathcal{A} = \{a + ib \text{ avec } a, b \in \mathbb{Z}\}$.
Remarque. *Je ne corrigerai pas tout. Je donnerai des indications et laisserai les questions faciles en exercice.*

1. Montrer que $\mathcal{A}$ est stable sous l'action de la conjugaison complexe.
Trivial : en exercice. Il s'agit de montrer que si z apprtient à $\mathcal{A}$ alors son conjugué $\bar{z}$ également.

2. Montrer que le noyau du morphisme d'anneaux
$$\begin{aligned} \phi : \mathbb{Z}[X] &\to \mathcal{A} \\ P(X) &\mapsto P(i) \end{aligned}$$

est l'idéal principal engendré par X^2+1.
Indications : Il est clair que le polynôme X^2+1 appartient au noyau de ϕ ce qui implique l'inclusion $\langle X^2+1\rangle \subset \ker\phi$. Pour l'autre inclusion, on suppose que $P \in \mathbb{Z}[X]$ est annuler par ϕ. On effectue la division euclidienne de P par X^2+1 : $P = Q\cdot(X^2+1)+R$. Le reste est de degré au plus 1. On peut donc l'écrire $R = aX+b$. Ensuite on montre que $R=0$ en evaluant en $X=i$.

Remarquons que la division euclienne de polynômes a lieu "normalement" dans un anneau de polynôme sur un corps. Aussi il n'y a, a priori, pas de division euclidienne dans $\mathbb{Z}[X]$. En fait ici, on effectue la division dans $\mathbb{Q}[X]$. Mais le polynôme X^2+1 étant unitaire, tout se passe dans $\mathbb{Z}[X]$, i.e. le quotient Q et le reste R sont à coefficients dans $\mathbb{Z}$.

3. Soit $n \geq 2$. En considérant les morphisme d'anneaux naturels

$$\mathbb{Z}[X] \to \mathcal{A} \to \mathcal{A}/n\mathcal{A},$$

en déduire l'isomorphisme d'anneaux

$$\mathcal{A}/n\mathcal{A} \simeq \frac{(\mathbb{Z}/n\mathbb{Z})[X]}{(X^2+1)}.$$

Le chemin que nous indique l'énoncé me semble un peu tortueux...
Considérons plutôt le morphisme suivant.

$$\begin{aligned}\psi : (\mathbb{Z}/n\mathbb{Z})[X] &\to (\mathbb{Z}/n\mathbb{Z})[i]\\ P(X) &\mapsto P(i)\end{aligned}$$

Ce morphisme est clairement surjectif. De plus comme à la question précédente, on montre que le noyau est l'idéal engendré par X^2+1. On obtient donc, via le théorème d'isomorphisme, que

$$(\mathbb{Z}/n\mathbb{Z})[X]/\langle X^2+1\rangle \simeq (\mathbb{Z}/n\mathbb{Z})[i].$$

Pour conclure on remarque que $(\mathbb{Z}/n\mathbb{Z})[i] \simeq \mathcal{A}/n\mathbb{Z}$. En fait ces anneaux sont mêmes égaux (en tant qu'ensembles). En effet ces ensembles sont des sous-ensembles de $\mathbb{Z}[i]$. Le premier $(\mathbb{Z}/n\mathbb{Z})[i]$ est

$$\{\alpha+i\beta \mid \exists a,b \in \mathbb{Z} \text{ t.q. } \alpha = a+n\mathbb{Z}, \beta = b+n\mathbb{Z}\}.$$

Le second $\mathcal{A}/n\mathbb{Z}$ est

$$\{z+n\mathbb{Z}[i] \mid z \in \mathbb{Z}[i]\}.$$

4. Pour tout $z \in \mathbb{C}$, on note $N(z) = |z|^2 = z\bar{z}$.

   (a) Montrer que $N(\alpha) \in \mathbb{N}$ pour tout $\alpha \in \mathcal{A}$.
   Trivial

   (b) Soient $\alpha, \beta \in \mathcal{A}$, $b \neq 0$. Montrer qu'il existe $\gamma \in \mathcal{A}$ tel que

   $$N(\alpha/\beta - \gamma) \leq 1/2.$$

   En déduire que $\mathcal{A}$ est euclidien.
   Question traîtée en CM

   (c) Soit $\alpha \in \mathcal{A}$. Montrer que α est inversible si et seulement si $N(\alpha)=1$.
   En déduire que les seuls inversibles de $\mathcal{A}$ sont ± 1 et $\pm i$.

   Supposons α inversible. Alors il existe $\beta \in \mathcal{A}$ tel que $\alpha\beta = 1$. On en déduit que $N(\alpha)N(\beta)=1$ d'où $N(\alpha) = \pm 1$. Réciproquement, supposons $N(\alpha) = \pm 1$. Observons que $N(\alpha) = z\bar{z}$. Ainsi $z\bar{z} = \pm 1$. Ainsi $z\bar{z} = 1$ ou bien $z(-\bar{z}) = 1$ et dans les cas α est inversible.
   On en déduit trivialement que les inversibles sont ceux annoncés.

5. Soit p un nombre premier impair.

   (a) Montrer que p est premier dans $\mathcal{A}$ si et seulement si le polynôme X^2+1 n'a pas de racines modulo p.

   p est premier dans $\mathcal{A}$ si s. si $\mathcal{A}/p\mathcal{A}$ est intègre. Par la question 3, cela équivaut au fait que $(\mathbb{Z}/p\mathbb{Z})[X]\langle X^2+1\rangle$ soit intègre.
   Or $\mathbb{Z}/p\mathbb{Z}$ est un corps donc $(\mathbb{Z}/p\mathbb{Z})[X]$ est principal (donc en particulier factoriel). Ainsi la condition précédente est équivalente au fait que $\langle X^2+1\rangle$ est premier ou encore que X^2+1 est irréductible dans $(\mathbb{Z}/p\mathbb{Z}[X])$. Ce polynôme est de degré 2 donc par le rappel 3, il est irrréductible dans $\mathbb{Z}/p\mathbb{Z}$ si et s. si il n'admet pas de racines dans $\mathbb{Z}/p\mathbb{Z}$.

   (b) Montrer que p est irréductible dans $\mathcal{A}$ si et seulement si il n'existe pas $\alpha \in \mathcal{A}$ avec $N(\alpha) = p$.

   Supposons qu'il existe $\alpha \in \mathcal{A}$ tel que $N(\alpha) = p$. Cela signifie que $\alpha\bar{\alpha} = p$ avec $N(\alpha) \neq 1$ et $N(\bar{\alpha}) \neq 1$ donc (par 4.(c)) que p est réductible. Par contraposée, nous venons de démontrer l'implication $\Rightarrow$.
   Supposons maintenant p réductible, i.e. $p = \alpha\beta$ avec α, β non inversibles. Ainsi $N(\alpha) \neq 1$ et $N(\beta) \neq 1$. Mais on a $p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta)$ d'où l'on déduit que $N(\alpha) = N(\beta) = p$. Nous venons, par contraposé, de montre l'implication $\Leftarrow$.

   (c) En déduire le résultat suivant

   Le nombre premier p s'écrit comme somme de deux carrés d'entiers
   si et seulement $p = 2$ ou p est congru à 1 modulo 4.

   Remarquons que l'enoncé nous induit en erreur Car dans le 5, p doit être un nombre premier impair...

   L'anneau $\mathcal{A}$ est euclidien donc factoriel. Dans un tel anneau, les éléments irréductibles et premiers se confondent. Ainsi p est premier dans $\mathcal{A}$ si et s. si p est irréductible dans $\mathcal{A}$.

   - Supposons qu'il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$. Nous devons montrer que $p = 2$ ou p est congru à 1 modulo 4. Pour cela supposons $p \neq 2$ et montrons que p est congru à 1 modulo 4.
     En posant $\alpha = a + ib$, nous obtenons $p = N(\alpha)$. Donc par 5(b), p n'est pas irréductible donc n'est pas premier. Donc par 5(a), il existe $\bar{k} \in \mathbb{Z}/p\mathbb{Z}$ tel que $\bar{k}^2 + \bar{1} = 0$. Donc $\bar{k}^2 = -\bar{1}$. Rappelons que $p \neq 2$ donc $-1 \neq 1$ dans $\mathbb{Z}/p\mathbb{Z}$ et $\bar{k}^2 \neq \bar{1}$. Comme $\bar{k}^4 = 1$, cela signifie que $\bar{k}$ est d'odre 4 dans $(\mathbb{Z}/p\mathbb{Z})^*$. Or ce groupe est d'ordre $p-1$ donc $4|p-1$. On en déduit que p est bien congru à 1 modulo 4.
   - Réciproquement supposons que $p = 2$ ou $p \equiv 1[4]$. Si $p = 2$ alors $p = 1^2 + 1^2$ et le but est atteint dans ce cas. Nous supposerons donc $p \neq 2$. Notons G le groupe $(\mathbb{Z}/p\mathbb{Z})^*$, il est d'ordre $p-1$. L'hypothèse $p \equiv 1[4]$ se traduit donc par 4 divise $|G|$. Ainsi tout élément de G est d'ordre 1, 2 ou 4.
     Supposons qu'il n'existe pas d'éléments dans G qui soient d'ordre 4. Alors pout tout $g \in G$, $g^2 = 1$ ou encore $(g-1)(g+1) = 0$. Mais alors $G = \{1, -1\}$ (*n'oublions pas que nous sommes dans $\mathbb{Z}/p\mathbb{Z}$ qui est un corps donc en particulier un anneau intègre*). D'où $p - 1 = 2$ ce qui contredit le fait que $p \equiv 1[4]$.
     Ainsi, il existe $g = \bar{k}$ d'ordre 4 dans G. Pour un tel g, on a $(g^2-1)(g^2+1) = 0$ or $g^2 \neq 1$ donc $g^2 = -1$. Ainsi le polynôme X^2+1 admet une racine dans $\mathbb{Z}/p\mathbb{Z}$. En utilisant 5(a) on en déduit que p n'est pas premier dans $\mathcal{A}$. Ainsi p n'est pas irréductible dans $\mathcal{A}$ (car $\mathcal{A}$ est factoriel comme rappelé plus haut). Par 5(b), on obtient l'existence de $\alpha = a + ib \in \mathcal{A}$ (avec $a, b \in \mathbb{Z}$) tel que $N(\alpha) = p$ ce qui implique $p = a^2 + b^2$.