TD0 : Anneaux et Idéaux

11/09/2024

Sauf mention explicite du contraire, les anneaux seront toujours supposés commutatifs, unitaires et non réduits à 0. Un morphisme d'anneaux $f : A \to A'$ vérifiera toujours $f(1_A) = 1_{A'}$.

On rappelle les définitions suivantes :

Définition 1. Un idéal I d'un anneau A est un sous-groupe additif de A stable par multiplication par A. On dit qu'un idéal est

— *premier* si c'est un idéal propre et $\forall a, b \in A, ab \in I \Rightarrow (a \in I) \vee (b \in I)$.

— *maximal* si c'est un élément maximal de l'ensemble des idéaux propres de A pour la relation $\subseteq$.

— *de type fini* si il est engendré par un nombre fini d'élements, et *principal* si il est engendré par un seul élément.

Exercice 1 : Idéaux premiers et maximaux

1. Soit A un anneau et I un idéal. Montrer que I est premier (resp. maximal) si et seulement si A/I est un anneau intègre (resp. un corps).

2. Soit A un anneau et I un idéal. Montrer que I est premier (resp. maximal) si et seulement si il est le noyau d'un morphisme (resp. d'un morphisme surjectif) $\phi : A \to B$ où B est un anneau intègre (resp. un corps).

Correction :

Voir cours. On peut aussi remarquer pour la question 2, que I est premier ssi il est le noyau d'un morphisme dont le but est un corps. En effet on peut écrire $A \to A/I \to \mathrm{Frac}(A/I)$ où $\mathrm{Frac}(A/I)$ est le corps des fractions de l'anneau intègre A/I.

Exercice 2 : Etude de $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geqslant 2$.

1. Quels sont les éléments inversibles, les éléments nilpotents, les diviseurs de 0 de $\mathbb{Z}/n\mathbb{Z}$?

2. Quels sont les idéaux, les idéaux premiers, les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$?

3. Quels sont les morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$? de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$? de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ pour $n, m \in \mathbb{N}$?

Correction :

1. On note $\pi : k \in \mathbb{Z} \mapsto [k] \in \mathbb{Z}/n\mathbb{Z}$ la projection canonique.

Soit $k \in \mathbb{Z}$. On montre que $[k]$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi $n \wedge k = 1$ (ca ne dépend bien que de la classe $[k]$). Par Bézout $n \wedge k = 1$ ssi $\exists u, v \in \mathbb{Z}, nu + kv = 1$ ssi $\exists v \in \mathbb{Z}, [k][u] = 1$ dans $\mathbb{Z}/n\mathbb{Z}$, ie ssi $[k]$ est inversible.

On appelle radical de n et noté $\mathrm{rad}(n)$ le produit des nombres premiers qui divisent n. On montre que $[k]$ est nilpotent ssi $\mathrm{rad}(n)|k$ (comme $\mathrm{rad}\,(n)\,|n$ c'est toujours bien indépendant du choix de k). Si $\mathrm{rad}(n)|k$, on a $n|rad(n)^l$ pour $l = \max\{\nu_p(n), p \in \mathcal{P}\}$, alors $n|\,\mathrm{rad}(n)^l|k^l$ donc $[k]^l = [0]$ et $[k]$ est nilpotent. Réciproquement si $[k]$ est nilpotent, alors $n|k^l$ pour l assez grand et tout premier qui divise n divise k^l et donc divise k. Par Gauss, $\mathrm{rad}(n)|k$.

On montre que $[k]$ divise 0 ssi $n \wedge k \neq 1$. Si $d = n \wedge k \neq 1$, on écrit $n = dn'$ et $k = dk'$ et alors $[k][n'] = [k'][n] = 0$ avec $[n'] \neq 0$. Réciproquement si $[k]$ divise 0 alors k est non inversible (car $\mathbb{Z}/n\mathbb{Z}$ n'est pas l'annéeau nul) et $n \wedge k \neq 1$ par la discussion précédente.

2. Soit $I \subset \mathbb{Z}/n\mathbb{Z}$ un idéal, alors $\pi^{-1}(I)$ est un idéal de $\mathbb{Z}$. Il existe alors $d \in \mathbb{Z}$ tel que $\pi^{-1}(I) = d\mathbb{Z}$. De plus $n \in \pi^{-1}([0]) \subset \pi^{-1}(I)$ donc $d|n$. Comme $I = \pi\pi^{-1}(I)$ (car π est surjectif, voir cours), $I = ([d])$. Réciproquement un tel I est bien un idéal de $\mathbb{Z}/n\mathbb{Z}$. Alors les seuls idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les idéaux principaux, les idéaux premiers sont ceux engendrés par les premier p tels que $p|n$ et tous ces idéaux premiers sont maximaux.

3. Un morphisme d'anneaux $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ doit envoyer $1_{\mathbb{Z}/n\mathbb{Z}}$ sur $1_{\mathbb{Z}}$, mais $\phi(n[1]) = \phi([0]) = 0 \neq n\phi([1]) = n$. Alors $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = \varnothing$.

Un morphisme de $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est déterminé par l'image de 1. Il y a donc au plus un morphisme. Alors $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \{\pi\}$.

De même un morphisme de $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ est déterminé par l'image de 1, il a donc au plus un morphisme d'anneau. L'image de 1 doit être de n torsion, alors si un tel morphisme existe $m|n$. Ainsi $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \varnothing$ si m ne divise pas n et $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \{\pi\}$ sinon.

Exercice 3 : Principalité de $A[X]$

Soit A un anneau. Montrer que $A[X]$ est principal si et seulement si A est un corps.

Correction :

Si A est un corps alors $A[X]$ est principal par l'argument de la division euclidienne.

Supposons $A[X]$ principal. Alors par définition d'un anneau principal, $A[X]$ est intègre et $A \hookrightarrow A[X]$ aussi : on peut donc utiliser le degré d'un polynôme qui vérifie les propriétés attendues. On sait que A est un corps ssi son seul idéal maximal est (0). Supposons par l'absurde que m soit un idéal maximal non nul de A, et notons $mA[X] = (a)$ par hypothèse de principalité. a est alors dans m (voir par exemple le degré) et est non nul car m l'est.

Soit $I = (a, X) = (P)$. Alors d'une part $a \in (P)$ donc $P = p \in A$ et $a = pq$, et $p = aU + XV$ soit en évaluant en 0, $p = aU(0)$. Par intégrité, on a donc $a(1 - U(0)q) = 0$ ie $U(0)q = 1$, donc $(a) = (p)$, puis $X \in (a) = mA[X]$, et donc $1 \in m$ absurde. D'où $m = 0$ et A est un corps.

Remarque 2. On aurait pu regarder $A[X]/(a) = (A/m)[X]$ pour en déduire que (a) est maximal dans l'ensemble des idéaux principaux de A et donc a est irréductible et conclure, car si $(a) \subset (b) = bA[X]$, alors $A[X]/(bA[X]) = (A/(b))[X]$ et forcément $A/(b) = A/(a)$ car le second est déja un corps, donc en fait $(a) = (b)$ en tant qu'idéaux de A, puis de $A[X]$.

Exercice 4 : Éléments inversibles de $A[X]$

1. Vérifier que si A est un anneau intègre, alors $A[X]$ est intègre et $A[X]^\times = A^\times$.

2. A est désormais un anneau quelconque, et $f := \sum_{i=0..n} a_i X^i$ un élément de $A[X]$.

a. Montrer que si a_0 est inversible dans A et $a_1, \dots, a_n$ sont nilpotents, alors f est inversible dans $A[X]$.

b. Réciproquement, supposant f inversible dans $A[X]$, montrer successivement que $a_0 \in A^\times$, puis $a_n \in \mathrm{Nil}(A)$, puis $a_{n-1}, \dots, a_1 \in \mathrm{Nil}(A)$.

c. Retrouver le résultat précédent en utilisant le fait que $\mathrm{Nil}(A)$ est l'intersection des idéaux premiers de A.

Correction :

1. Si A est intègre, l'application $\deg : (A[X], \times) \to (N \cup \{-\infty\}, +)$ est un morphisme (car le coeefficient dominant de PQ est le coefficient dominant de P fois le coefficient dominant de Q donc non nul sauf si l'un des deux polynômes était déja le polynôme nul). En particulier $A[X]^\times \subset A^\times$ car si $PQ = 1$ alors $\deg P + \deg Q = 0$ et donc $\deg P = 0$ et $P \in A^\times$. Réciproquement $A^\times \subset A[X]^\times$ et on a bien l'égalité voulue.

2.

a. On utilise le Lemme suivant :

Lemme 0.3.

Soit B un anneau, u un inversible et h un élément nilpotent. Alors $u-h$ est inversible.

Démonstration. On peut supposer $u=1$ quitte à multiplier par u^{-1}. Alors si n est tel que $h^n=0$, on a $\left(\sum_{k=0}^{n-1} h^k\right)(1-h)=1-h^n=1$. □

D'après le Lemme, comme $f=\underbrace{a_0}_{\in A^\times}+\underbrace{\left(\sum_{i\geqslant 1} a_i X^i\right)}_{\text{nilpotent}}$ alors f est inversible.

b. Supposons $fg=1$ dans $A[X]$ avec $f=\sum_{k=0}^n a_k X^k$. Alors en regardant le coefficient en X^0 de $fg=1$, on en déduit $a_0 b_0=1$ où $g=\sum_{i=0}^m b_i X^i$. Ecrivons les autres relations que nous donne l'écriture par coordonnée de $fg=1$:

$$\begin{cases} X^{n+m}: & a_n b_m=0 \\ X^{n+m-1}: & a_n b_{m-1}+a_{n-1}b_m=0 \\ \vdots & \vdots \\ X^{n+m-k}: & \sum_{i=0}^k a_{n-i}b_{m-k+i}=0 \end{cases}$$

En particulier, en multipliant la ligne 2 par a_n, comme par ligne 1 $a_n b_m=0$, on en déduit $a_n^2 b_{m-1}=0$. Supposons qu'on ait $a_n^i b_{m-(i-1)}=0$ pour $i\leqslant k$. Alors $0=a_n^k\left(\sum_{i=0}^k a_{n-i}b_{m-k+i}\right)=a_n^{k+1}b_{m-k}+\sum_{i=1}^k a_{n-i}\underbrace{a_n^k b_{m-k+i}}_{=0 \text{car } k-i<k}$ d'où $a_n^{k+1}b_{m-k}=0$. On a donc montré le résultat par récurrence, jusqu'à $k=m$ qui fournit $a_n^{m+1}b_0=0$ et comme b_0 est inversible, a_n est nilpotent. Finalement, comme a_nX^n est nilpotent, $f-a_nX^n$ est aussi inversible par le Lemme et donc par récurrence immédiate on en déduit que $a_{n-1},\dots,a_1$ sont nilpotents.

c. Soit $\mathfrak{p}$ un idéal premier. Notons $\pi: A\to A/\mathfrak{p}$ la réduction modulo $\mathfrak{p}$, et de même $\pi: A[X]\to A/\mathfrak{p}[X]$ la réduction modulo $\mathfrak{p}$ des coefficients. Alors si f est inversible, $\pi(f)$ l'est aussi. Mais $A/\mathfrak{p}$ est intègre, donc $\pi(f)$ est inversible ssi $\pi(f)$ est constant et inversible dans $A/\mathfrak{p}$. En particulier, a_0 n'est pas dans $\mathfrak{p}$ et $a_1,\dots,a_n\in\mathfrak{p}$. Comme cela est valable pour tout idéal premier, on en déduit que $a_1,\dots,a_n\in\bigcap_{\mathfrak{p}\in\operatorname{Spec}A}\mathfrak{p}$ ie sont nilpotents, et a_0 n'appartient à aucun idéal maximal donc est inversible.

Exercice 5 : Un exemple d'idéal premier mais non maximal

Montrer que l'idéal (x^2-2) est premier mais pas maximal dans $\mathbb{Z}[x]$.

Correction :

On calcule le quotient $\mathbb{Z}[X]/(X^2-2)=\mathbb{Z}[\sqrt{2}]$. Soit $\phi:\mathbb{Z}[X]\to\mathbb{Z}[\sqrt{2}]$ le morphisme définit par $X\mapsto\sqrt{2}$. Clairement ϕ est surjectif, pour avoir l'isomorphisme voulu, il suffit de vérifier que $\ker(\phi)=(X^2-2)$. Soit $P\in\ker(\phi)$, on écrit la DE de P par X^2-2 dans $\mathbb{Z}[X]$ comme $P=(X^2-2)Q+R$ et R est de degré $\leqslant 1$. D'où $R=a+bX$, comme $(1,\sqrt{2})$ est $\mathbb{Q}$-libre, on a $a=b=0$.

Ce qui montre que le quotient est intègre et donc (X^2-2) est premier. On vérifie ensuite que 3 n'est pas inversible dans $\mathbb{Z}[\sqrt{2}]$. Sinon $3(a+b\sqrt{2})=1$, ce qui implique $a=\frac{1}{3}$ et $b=0$. Donc 3 n'est pas inversible dans $\mathbb{Z}[\sqrt{2}]$.

Exercice 6 : Image réciproque d'un idéal maximal

Soient $f: A\to B$ un homomorphisme d'anneaux et M un idéal maximal de B. Soit $N:=f^{-1}(M)$. Montrer que N n'est pas nécessairement un idéal maximal de A , mais que c'est le cas si f est surjectif.

Correction :

Soit $f : A \to B$ un morphisme d'anneau et $M \subset B$ un idéal maximal. La composée $A \to B \to B/M$ se factorise par A/N et l'application induite $A/N \to B/M$ est injective.

Si f est surjective, alors $A \to B/M$ l'est aussi, et par conséquent $A/N \to B/M$ aussi, donc A/N est un corps et N est maximal.

Un contre exemple est donné par l'inclusion $\mathbb{Z} \to \mathbb{Q}$, $m = 0$ et $n = 0$ n'est pas maximal.

Exercice 7 : Entiers algébriques

Soit $x \in \mathbb{C}$. Montrer que les propositions suivantes sont équivalentes :

(i) x est racine d'un polynôme non nul unitaire à coefficients dans $\mathbb{Z}$.

(ii) $\mathbb{Z}[x]$ est un groupe abélien de type fini.

En déduire que l'ensemble des entiers algébriques de $\mathbb{C}$ est un anneau.

Correction :

$(i) \Rightarrow (ii)$ Si $x^n = a_{n-1}x^{n-1} + \cdots + a_0$, alors $\mathbb{Z}[x]$ est généré par $(1, x, \ldots, x^{n-1})$ et c'est bien un groupe abélien de type fini.

$(ii) \Rightarrow (i)$ Si $\mathbb{Z}[x]$ est un groupe abélien de type fini, alors on peut extraire une famille génératrice finie de la famille de génératrice $(x^k, k \geqslant 0)$. Alors $\mathbb{Z}[x]$ est générée par $1, \ldots, x^n$ et $x^{n+1} = a_n x^n + \cdots + a_0$.

Par un raisonnement analogue on a, pour x, y des entiers algébriques, $\mathbb{Z}[x, y]$ est un groupe abélien de type fini. Alors $\mathbb{Z}[xy] \subset \mathbb{Z}[x, y]$ et $\mathbb{Z}[x + y] \subset \mathbb{Z}[x, y]$ sont des groupes abéliens de type fini et l'ensemble des entiers algébriques est un sous anneau de $\mathbb{C}$.

Exercice 8 : Division euclidienne

Soit A un anneau et $A[X]$ l'anneau des polynômes à coefficients dans A.

1. Montrer que si $D \in A[X]$ a un coefficient dominant inversible, alors pour $P \in A[X]$ il existe $R, Q \in A[X]$ tel que $P = QD + R$ et $\deg R < \deg D$. Si A est intègre, montrer que le couple P, Q est unique.

Correction :

Voir une preuve pour A un corps, et voir pourquoi on a besoin que le coefficient dominant soit inversible.

Exercice 9 : Une caractérisation de l'intégrité

Soit A un anneau distinct de $\{0\}$, de $\mathbb{Z}/4\mathbb{Z}$, et de $\mathbb{F}_2[X]/(X^2)$. Montrer que les propriétés suivantes sont équivalentes :

(i) A est intègre.

(ii) Tout polynôme unitaire de degré n à coefficients dans A a au plus n racines dans A.

(iii) Tout polynôme unitaire de degré 2 à coefficients dans A a au plus 2 racines dans A.

Correction :

L'implication $(ii) \Rightarrow (iii)$ ne pose pas de problème.

$(i) \Rightarrow (ii)$. Soit P un polynôme unitaire à coefficients dans A. Si a est une racine de P, on peut considérer la division euclidienne de P par $X - a$ qui existe car le coefficient dominant de $X - a$ est inversible, et s'écrit alors $P = (X - a)Q + b$ avec b un polynôme constant, puis $b = 0$ en évaluant en a. Par intégrité, $\deg Q = \deg P - 1$, et en particulier P a bien au plus $\deg P$ racines.

$(iii) \Rightarrow (i)$ On montre d'abord le lemme suivant :

<u>Lemme</u> : Soit A un anneau non intègre tel que $\forall a, b \in A$ non nuls, $ab = 0 \Rightarrow a = b$, alors $A = \mathbb{Z}/4\mathbb{Z}$ ou $A = \mathbb{F}_2[X]/X^2$.

Démonstration. Si a un diviseur de 0, qui par hypothèse vérifie $a^2 = 0$, alors a est en particulier est nilpotent. Alors l'anneau réduit $A/\mathcal{N}(A)$ où $\mathcal{N}(A)$ est le nilradical de A est intègre (si $ab \in \mathcal{N}(A)$, $a^n b^n = 0$ pour un certain n et par l'hypothèse $a^n = b^n$, donc $a^{2n} = 0$ et $a \in \mathcal{N}(A)$). Soit $[c] \neq 0$ un élément de $A/\mathcal{N}(A)$, et a un diviseur de 0 (non nul) fixé. lors $ca^2 = 0$ donc $ca = a$ (en effet il faut vérifier que $ca \neq 0$ pour appliquer l'hypothèse mais c'est le cas car sinon $c = a$ et $[c]$ serait nul) puis $(c-1)a = 0$. On a donc soit $c = 1$, soit $c-1$ et a sont non nuls et par hypothèse $c = a+1$. Dans les deux cas $[c] = 1$, et on a la liste de tous les éléments de $A = \{0, a, 1, 1+a\}$. (en effet un élément $x \in A$ vaut soit 1 dans le quotient et on a décrit ces éléments, soit 0, mais dans ce cas $1+x$ vaut 1...). Finalement, suivant si $a = 2$ ou non, on peut conclure. □

Si A est non intègre et A différent de $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{F}_2[X]/X^2$. Alors il existe a, b distincts et non nuls tels que $ab = 0$. Alors $(X-a)(X-b)$ a trois racines distinctes $a, b, 0$.

Exercice 10 : Anneaux d'entiers

Montrer que si un nombre rationnel est racine d'un polynôme non nul unitaire à coefficients entiers, alors c'est un entier.

Correction :

Soit $r = \frac{p}{q} \in \mathbb{Q}$ avec $p \wedge q = 1$ vérifiant

$$r^n + a_{n-1}r^{n-1} + \cdots + a_0 = 0$$

On multiplie l'équation par q^n, celle-ci devient :

$$p^n + qp^{n-1}a_{n-1} + \cdots + q^n a_0 = 0$$

Si $q \neq 1$, on regarde mod q, ce qui devient $p^n = 0$ et contredit l'hypothèse $p \wedge q = 1$. Alors $q = 1$ et $r \in \mathbb{Z}$.

Exercice 11 : Théorème des deux carrés

On rappelle que les anneaux des entiers de Gauss est l'anneau $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$. On définit $N : \mathbb{Z}[i] \to \mathbb{N}$ par $N(z) := |z|^2$.

1.

a. Montrer que N est multiplicative, i.e. pour tous $z, z' \in \mathbb{Z}[i]$ on a

$$N(zz') = N(z)N(z')$$

b. Montrer que $\mathbb{Z}[i]^\times = \{z \in \mathbb{Z}[i], N(z) = 1\}$.

2. Soit p un nombre premier différent de 2.

a. Montrer que -1 est un carré modulo p si et seulement si $p \equiv 1[4]$.

b. Montrer l'équivalence des propriétés suivantes :

(i) p est irréductible dans $\mathbb{Z}[i]$.

(ii) $p \equiv 3[4]$

(iii) p n'est pas somme de deux carrés d'entiers naturels.

Correction :

1.

a. Le module complexe est multiplicatif.

b. Si z est inversible, il existe z' tel que $zz' = 1$ alors $N(z)N(z') = 1$, puis forcément $N(z) = a^2 + b^2 = 1$ donc $z \in \{\pm 1, \pm i\}$. Réciproquement ces éléments sont clairement inversibles dans $\mathbb{Z}[i]$.

2.

a. Considérons le morphisme de groupes $\varphi : x \in (\mathbb{Z}/p\mathbb{Z})^* \mapsto x^2 \in (\mathbb{Z}/p\mathbb{Z})^*$, de noyau $\{-1, +1\}$. Alors son image est de cardinal $\frac{|(\mathbb{Z}/p\mathbb{Z})^*|}{|\ker \varphi|} = \frac{p-1}{2}$. De plus, tout élément $x \in (\mathbb{Z}/p\mathbb{Z})^*$ vérifie $x^{p-1} = 1$. En particulier, $\mathrm{im}(\varphi) \subset \{x \in (\mathbb{Z}/p\mathbb{Z})^*, x^{\frac{p-1}{2}} = 1\}$. Or ce second ensemble est précisément l'ensemble des racines du polynôme à coefficients dans le corps $\mathbb{Z}/p\mathbb{Z}$ $X^{\frac{p-1}{2}} - 1$, et est donc de cardinal au plus $\frac{p-1}{2}$. Par égalité des cardinaux, on conclue que x est un carré mod p ssi $x^{\frac{p-1}{2}} = 1$ mod p. Alors -1 est un carré mod p ssi $(-1)^{\frac{p-1}{2}} = 1$ ssi $p = 1[4]$.

b.

$(i) \Rightarrow (iii)$ Si p est une somme de deux carrés, alors $p = a^2 + b^2 = (a+ib)(a-ib)$ n'est pas irréductible dans $\mathbb{Z}[i]$.

$(iii) \Rightarrow (i)$ Si p n'est pas irréductible $p = zz'$ avec z, z' non inversibles. Mais alors $p^2 = N(z)N(z')$ et comme z et z' ne sont pas inversibles, $N(z) = N(z') = p$ et $p = N(z)$ est une écriture de p comme somme de deux carrés.

$(i) \Leftrightarrow (ii)$ Calculons $\mathbb{Z}[i]/(p) = \mathbb{Z}[X]/(p, X^2+1) = \mathbb{F}_p[X]/(X^2+1)$. Ce dernier anneau est intègre ssi -1 n'est pas un carré mod p. En effet, si $-1 = a^2$, alors $X^2 - 1 = (X-a)(X+a)$ et donc cet anneau n'est pas intègre. Si réciproquement on suppose que $\mathbb{F}_p[X]/(X^2+1)$ n'est pas intègre, on dispose d'une relation du type $(aX+b)(cX+d) = X^2 + 1[p]$ (on peut prendre des représentants de degré 1 en simplifiant avec le X^2, puis multiplier par un inverse si nécessaire) avec $aX+b$ et $cX+d$ non nuls dans $\mathbb{F}_p[X]$. Mais alors

$$\begin{cases} ac = 1 \\ ad + bc = 0 \\ db = 1 \end{cases}$$

On déduit alors $ad + ba^{-1} = 0$ et $a^2 d = -b$, et en reportant dans la dernière équation : $d^2 a^2 = -1[p]$. (on peut aussi dire que cet anneau est intègre ssi $X^2 - 1$ est irréductible ssi il n'a pas de racine car c'est un polynôme de degré 2). Finalement, on a bien l'équivalence :

p est irréductible $\iff$ (p) est premier $\iff$ $\mathbb{Z}[i]/p$ est intègre $\iff$ -1 n'est pas un carré modulo p $\iff$ $p \equiv 3[4]$.

(pour la première équivalence : si (p) est premier, et $p = zz'$, alors disons $z \in (p)$, puis $p^2 = N(z)N(z')$ avec $p^2 | N(z)$ donc $N(z') = 1$ et z' est inversible. Réciproquement, p irréductible $\iff$ (p) est maximal dans l'ensemble des idéaux principaux de $\mathbb{Z}[i]$, or $\mathbb{Z}[i]$ est principal (montrer qu'on peut faire une "division euclidienne" avec N, donc en fait (p) est maximal donc à fortiori premier.)

Exercice 12 : Exemples d'entiers algébriques ?

Parmi ces nombres algébriques, lesquels sont des entiers algébriques ?

$$\frac{3+2\sqrt{6}}{(1-\sqrt{6})}, \frac{\sqrt{3}+\sqrt{5}}{2}, \frac{\sqrt{3}+\sqrt{7}}{2}, \frac{1+^3\sqrt{10}+^3\sqrt{100}}{3}, \frac{1+i}{2}, \frac{\sqrt{a}+\sqrt{b}}{n}$$

avec $a, b \in \mathbb{Z} \backslash \{0, 1\}$ des entiers distincts sans facteur carré et $n \in \mathbb{N}^*$.

Correction :