10. Exercices

On commence par quelques exercices sur les entiers de Gauss.

EXERCICE 7.1. *Factoriser $-3+15i$ et $4+7i$ en irréductibles dans $\mathbb{Z}[i]$.*

EXERCICE 7.2. *Trouver tous les $(x,y)\in\mathbb{Z}^2$ avec $y^2=x^3-1$.*

EXERCICE 7.3. (Un choix de représentants des irréductibles de $\mathbb{Z}[i]$)

(i) Montrer que l'idéal $(2+2i)$ de $\mathbb{Z}[i]$ admet pour $\mathbb{Z}$-base $4, 2(1+i)$.

(ii) En déduire un isomorphisme de groupes abéliens bien défini

$$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\xrightarrow{\sim}\mathbb{Z}[i]/(2+2i),\ (\overline{a},\overline{b})\mapsto\overline{a+bi}.$$

À quelle condition sur $a,b\in\mathbb{Z}$ a-t-on $a+bi\equiv 3 \bmod 2+2i$?

(iii) On munit $A:=\mathbb{Z}[i]/(2+2i)\mathbb{Z}[i]$ de sa structure d'anneau quotient. Montrer que l'application naturelle $\mathbb{Z}[i]^\times\to A^\times$ est un isomorphisme de groupes.

(iv) Montrer que l'ensemble des irréductibles de $\mathbb{Z}[i]$ de la forme $1+i$, ou congrus à 3 modulo $2+2i$, est un système de représentants de tous les irréductibles.

Dans l'exercice suivant, on dira qu'une fonction $f:\mathbb{N}_{\geqslant 1}\to\mathbb{C}$ est *arithmétiquement multiplicative* si on a $f(mn)=f(m)f(n)$ pour $m,n\geqslant 1$ avec $m\wedge n=1$.

EXERCICE 7.4. *Pour n un entier $\geqslant 1$ on pose $\Sigma_n=\{(a,b)\in\mathbb{Z}^2\mid n=a^2+b^2\}$. On se propose de montrer $|\Sigma_n|=4(\mathrm{d}_1(n)-\mathrm{d}_3(n))$, où $\mathrm{d}_i(n)$ désigne le nombre de diviseurs $d\geqslant 1$ de n vérifiant $d\equiv i \bmod 4$.*

(i) Montrer que l'on a $\Sigma_n\neq\varnothing$ si, et seulement si, on a $\mathrm{v}_p(n)\equiv 0 \bmod 2$ pour tout facteur premier p de n avec $p\equiv 3 \bmod 4$.

(ii) Montrer que les deux fonctions $n\mapsto\frac{1}{4}|\Sigma_n|$ et $n\mapsto\mathrm{d}_1(n)-\mathrm{d}_3(n)$ sont arithmétiquement multiplicatives.

(iii) Conclure.

On s'intéresse maintenant aux anneaux $\mathbb{Z}[\sqrt{d}]$ généraux.

EXERCICE 7.5. *On se propose de montrer que l'anneau $\mathbb{Z}[\sqrt{d}]$ est non principal pour $d<-2$. On pose $\alpha=\sqrt{d}$ si d est pair, $\alpha=1+\sqrt{d}$ sinon.*

(i) Traiter directement les cas $d=-3,-4$.

(ii) Montrer $(2,\alpha)=2\mathbb{Z}+\alpha\mathbb{Z}$.

(iii) Montrer que pour $d<-4$, les éléments de $\mathbb{Z}[\sqrt{d}]$ de norme $\leqslant 4$ sont $\pm 1,\pm 2$.

(iv) En déduire que l'idéal $(2,\alpha)$ n'est pas principal.

EXERCICE 7.6. (Noethérianité de $\mathbb{Z}[\sqrt{d}]$) *Soient $d\in\mathbb{Z}$ non carré et $A=\mathbb{Z}[\sqrt{d}]$.*

(i) Montrer que tout idéal non nul I de A contient un entier $n\in\mathbb{Z}_{>0}$.

(ii) Montrer qu'il n'y a qu'un nombre fini d'idéaux de A contenant un entier $n\in\mathbb{Z}_{>0}$ donné.

(iii) Montrer que A est noethérien, et que tout idéal non nul y est d'indice fini.

(iv) Montrer que A n'a qu'un nombre fini d'idéaux principaux zA avec $\mathrm{N}(z)$ fixé.

EXERCICE 7.7. (Unités de $\mathbb{Z}[\sqrt{d}]$ avec $d > 0$) *Soit $d > 0$ un entier non carré. On se propose de montrer que $\mathbb{Z}[\sqrt{d}]^\times$ est infini.*

(i) Montrer que pour tout $\alpha \in \mathbb{R}$, et tout entier $N \geqslant 1$, il existe $p \in \mathbb{Z}$ et $1 \leqslant q \leqslant N$ tels que $|p - q\alpha| < 1/N$ (principe de Dirichlet).

(ii) Montrer qu'il existe une suite d'éléments $x_n \in \mathbb{Z}[\sqrt{d}]$ non nuls avec $x_n \to 0$ dans $\mathbb{R}$ et $(\mathrm{N}(x_n))_{n\geqslant 1}$ bornée.

(iii) (suite) Montrer que quitte à extraire une sous-suite de x_n, on peut supposer qu'il existe $k \in \mathbb{Z}$ tel que $\mathrm{N}(x_n) = k$ et $x_n\overline{x_m} \in k\mathbb{Z}[\sqrt{d}]$, pour tout $n, m \geqslant 1$.

(iv) Conclure.

EXERCICE 7.8. *(i) Soient (a, b) et $(c, d) \in \mathbb{Z}^2$ avec $ad - bc$ non nul. Montrer que le sous-groupe de $\mathbb{Z}^2$ qu'ils engendrent est d'indice fini, égal à $|ad - bc|$.*

(ii) Soit $d \in \mathbb{Z}$ non carré, $A = \mathbb{Z}[\sqrt{d}]$ et $z \in A$ non nul. Montrer que le groupe additif quotient A/zA est fini de cardinal $|\mathrm{N}(z)|$.

Dans les deux exercices suivants, on se propose d'examiner les idéaux d'une poignée de $\mathbb{Z}[\sqrt{d}]$ non principaux. Si A est un anneau commutatif intègre, et si I et J sont deux idéaux non nuls de A, on dira que I et J sont *équivalents*, et on notera $I \sim J$, s'il existe $a, b \in A \smallsetminus \{0\}$ avec $aI = bJ$. C'est clairement une relation d'équivalence sur les idéaux non nuls de A, dont on notera $\mathrm{Cl}(A)$ l'ensemble des classes.

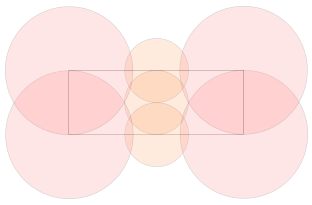
EXERCICE 7.9. *Soit A un anneau commutatif intègre.*

(i) Montrer qu'un idéal non nul de A est principal si, et seulement si, il est équivalent à A.

(ii) En déduire que A est principal si, et seulement si, on a $|\mathrm{Cl}(A)| = 1$.

EXERCICE 7.10. *On considère $A = \mathbb{Z}[\sqrt{d}]$ avec $-7 \leqslant d \leqslant -3$.*

(i) Soit $t \in \mathbb{R}$ avec $0 < t < 1+\sqrt{3}$. En observant la figure ci-dessous, montrer que pour tout $z \in \mathbb{C}$, il existe $v \in \mathbb{Z}+\mathbb{Z}\,i$ tel que soit $|z-v| < 1$, soit $|z-v/2| < 1/2$.



(ii) En déduire que pour tout $a, b \in A$ avec $b \neq 0$, il existe des éléments $q, r \in A$ avec $\mathrm{N}(r) < \mathrm{N}(b)$ et soit $a = qb + r$, soit $2a = qb + r$.

(iii) Montrer que tout idéal non nul de A est équivalent à un idéal contenant $2A$.

(iv) Montrer que les idéaux de A contenant $2A$ sont $2A$, J et A, où J est l'idéal $(2, \alpha)$ introduit à l'Exercice 7.5.

(v) (suite) Démontrer $\mathrm{Cl}(A) = \{[A], [J]\}$ et que J est non équivalent à A.

Les exercices qui suivent introduisent une variante importante des anneaux $\mathbb{Z}[\sqrt{d}]$. Dans le premier, on utilisera à profit l'identité suivante, valable pour $x, y \in \mathbb{R}$:

$$|x - jy|^2 = x^2 + xy + y^2 = \frac{1}{4}\left((2x + y)^2 + 3y^2\right).$$

EXERCICE 7.11. (Entiers d'Eisenstein) *On pose* $j = e^{2i\pi/3}$ *et* $\mathbb{Z}[j] = \mathbb{Z} + \mathbb{Z}j$.

(i) Montrer que $\mathbb{Z}[j]$ *est un sous-anneau de* $\mathbb{C}$.

(ii) Montrer $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\} = \mu_6$.

(iii) Montrer que $\mathbb{Z}[j]$ *est euclidien pour* $z \mapsto |z|^2$.

(iv) Soit p *un nombre premier* $\equiv 1 \bmod 3$. *Montrer que l'on a* $p = \pi\overline{\pi}$ *avec* π *et* $\overline{\pi}$ *des irréductibles non associés de* $\mathbb{Z}[j]$.

(v) (suite) En déduire qu'il existe exactement 12 *couples* $(a, b) \in \mathbb{Z}^2$ *tels que* $p = a^2 + ab + b^2$.

(vi) (suite) Retrouver qu'il existe un unique $(a, b) \in \mathbb{N}^2$ *avec* $p = a^2 + 3b^2$.

Pour $d \in \mathbb{Z}$ non carré et $d \equiv 1 \bmod 4$, on pose

$$\tau_d = \frac{1 + \sqrt{d}}{2} \quad \text{et} \quad \mathrm{A}_d = \mathbb{Z} + \mathbb{Z}\tau_d \subset \mathbb{Q}[\sqrt{d}].$$

La relation $\tau_d^2 = \tau_d + \frac{d-1}{4} \in \mathbb{Z} + \mathbb{Z}\,\tau_d$ montre que c'est un sous-anneau de $\mathbb{Q}[\sqrt{d}]$ contenant strictement $\mathbb{Z}[\sqrt{d}]$. Par exemple, on a $\tau_{-3} = e^{2i\pi/6} = -j^2$ et donc $\mathrm{A}_{-3} = \mathbb{Z}[j]$ est l'anneau des entiers d'Eisenstein (Exercice 7.11). On a aussi $\overline{\tau_d} = \frac{1-\sqrt{d}}{2} = 1 - \tau_d \in \mathbb{Z}[\sqrt{d}]$, de sorte que $z \mapsto \overline{z}$ préserve A_d, et pour $x, y \in \mathbb{Q}$, on a enfin

$$\mathrm{N}(x + y\,\tau_d) = x^2 + xy + \frac{1-d}{4}\,y^2,$$

et en particulier $\mathrm{N}(\mathrm{A}_d) \subset \mathbb{Z}$.

EXERCICE 7.12. *(i) Montrer* $\mathrm{A}_d^\times = \{z \in \mathrm{A}_d \mid \mathrm{N}(z) = \pm 1\}$ *puis* $\mathrm{A}_{-3}^\times = \mu_6$ *et* $\mathrm{A}_d^\times = \{\pm 1\}$ *pour* $d < -3$.

(ii) Montrer que les résultats de l'Exercice 7.8 (ii) et de l'Exercice 7.6 sont encore vrais pour $A = \mathrm{A}_d$.

EXERCICE 7.13. *Montrer que* A_{-3}, A_{-7} *et* A_{-11} *sont euclidiens pour* N.

EXERCICE 7.14. *On se propose de montrer que l'anneau* A_{-19} *est principal.*

(i) Montrer que pour tout $a, b \in \mathrm{A}_{-19}$ *on a soit* $a = bq + r$ *avec* $\mathrm{N}(r) < \mathrm{N}(b)$, *soit* $2a = bq + r$ *avec* $\mathrm{N}(r) < \mathrm{N}(b)$.

(ii) Montrer que les seuls idéaux de A_{-19} *contenant* 2 *sont* A_{-19} *et* $2\,\mathrm{A}_{-19}$.

(iii) En déduire que A_{-19} *est principal.*

On peut montrer que A_d est encore principal pour $d = -43, -67$ et -163.

EXERCICE 7.15. *On se propose de montrer, suivant Samuel, que* A_d *n'est pas euclidien pour* $d < -11$ *(et ce quelque soit le stathme).*

(i) Soit A un anneau euclidien qui n'est pas un corps. Montrer qu'il existe $x \in A$ non zero ou unité, tel que l'application naturelle $\{0\} \cup A^\times \to A/xA$ est surjective.

(ii) Montrer que pour $d < -11$, A_d ne possède aucun élément de norme 2 ou 3.

(iii) Conclure (on utilisera les résultats de l'Exercice 7.12).

Ainsi, A_{-19} est un anneau principal non euclidien. Les deux exercices suivants examinent les notions de pgcd et ppcm.

EXERCICE 7.16. (Pgcd et ppcm, généralités) *Soient A intègre et $a, b, c \in A \smallsetminus \{0\}$.*

(i) Montrer $(a) \cap (b) = (c)$ si, et seulement si, c est un ppcm de a et b.

(ii) On suppose a premier et $a \nmid b$. Montrer que ab est un ppcm de a et b.

(iii) On suppose $(a) + (b) = (c)$. Montrer que c est un pgcd de a et b.

EXERCICE 7.17. (Pgcd et ppcm, exemples et contre-exemples) *On se place dans l'anneau $\mathbb{Z}[\sqrt{-5}]$.*

(i) Montrer que 2 et $1 + \sqrt{-5}$ admettent un pgcd.

(ii) Montrer que 2 et $1 + \sqrt{-5}$ n'admettent pas de ppcm.

(iii) Montrer que $3(1+\sqrt{-5})$ et $3(1-\sqrt{-5}) = (1+\sqrt{-5})(-2-\sqrt{-5})$ n'admettent pas de pgcd.

(iv) Montrer que l'idéal $I = (2, 1 + \sqrt{-5})$ admet pour $\mathbb{Z}$-base $2, 1 + \sqrt{-5}$.

(v) (suite) Montrer que I n'est pas principal, puis que la réciproque du (iii) de l'exercice précédent est fausse.

On poursuit par quelques exercices généraux sur les anneaux principaux et factoriels.

EXERCICE 7.18. *Soit A le sous-anneau des fonctions $\mathbb{R} \to \mathbb{R}$ de la forme $t \mapsto P(\cos t, \sin t)$ avec $P \in \mathbb{R}[X, Y]$ (justifier).*

(i) Montrer que A est un anneau intègre.

(ii) Montrer que les éléments $\cos t$ et $\sin t$ sont irréductibles dans A.

(iii) Montrer que A n'est pas factoriel.

EXERCICE 7.19. *(i) Montrer que si k est un corps, l'idéal (X, Y) de $k[X, Y]$ n'est pas principal.*

(ii) Montrer de même que $\mathbb{Z}[X]$ n'est pas principal.

EXERCICE 7.20. (Lemme du contenu de Gauss) *Soit A un anneau factoriel de corps de fractions K. Si $P \in A[X]$ est non nul, on note $\mathrm{c}(P)$ le pgcd des coefficients de P, c'est un élément de A bien défini aux unités près. On dit que P est primitif si $\mathrm{c}(P)$ est une unité.*

(i) Montrer $A[X]^\times = A^\times$.

(ii) Montrer que si $P, Q \in A[X]$ sont primitifs alors PQ est primitif.

(iii) En déduire que si $P, Q \in A[X]$ sont non nuls, on a $\mathrm{c}(PQ) = \mathrm{c}(P)\mathrm{c}(Q)$ (aux unités près).

(iv) Montrer que si $P \in A[X]$ est non constant, alors P est irréductible dans $A[X]$ si et seulement si $\mathrm{c}(P) = 1$ et P est irréductible dans $K[X]$.

(v) En déduire que les irréductibles de $A[X]$ sont les irréductibles de A et les polynômes primitifs non constant.

(vi) Montrer que $A[X]$ est factoriel.

(vii) En déduire que $\mathbb{Z}[X_1, \ldots, X_n]$ et $k[X_1, \ldots, X_n]$ sont factoriels si $n \geqslant 1$ et si k est un corps.

EXERCICE 7.21. *Soit A l'anneau des séries entières $\sum_{n\geqslant 0} a_n z^n$, à coefficients a_n dans $\mathbb{C}$ et de rayon de convergence infini.*

(i) Montrer que A est intègre.

(ii) Montrer que les unités de A sont les fonctions qui ne s'annulent pas, et que les irréductibles de A sont, aux unités près, les $z - a$ avec $a \in \mathbb{C}$.

(iii) En déduire que A n'a pas la propriété de factorisation (en particulier, A n'est pas noethérien).

EXERCICE 7.22. *Soient k un corps et $k[[X]]$ l'anneau des séries formelles $\sum_{n\geqslant 0} a_n X^n$ à coefficients $a_n \in k$ pour tout $n \geqslant 0$.*

(i) Expliquer pourquoi une définition possible de l'anneau $k[[X]]$ est de considérer les fonctions $a : \mathbb{N} \to k$ munies du produit de convolution

$$(a \star b)(n) = \sum_{0\leqslant p\leqslant n} a(p)b(n-p).$$

(ii) Montrer qu'une série formelle $f = \sum_{n\geqslant 0} a_n X^n$ est inversible dans $k[[X]]$ si, et seulement si, on a $a_0 \neq 0$.

(iii) Montrer que X est l'unique irréductible de $k[[X]]$, modulo association.

(iv) Montrer que pour tout $f \in k[[X]]$ non nul, il existe un unique entier $n \geqslant 0$ (appelé valuation *de f) et un unique $u \in k[[X]]^\times$ tels que $f = X^n u$.*

(v) En déduire que $k[[X]]$ est principal.

(vi) Montrer que la valuation est un stathme euclidien sur $k[[X]]$.

Les deux exercices suivants introduisent la notion d'anneau *intégralement clos*. Soit A un anneau intègre de corps de fractions K. On note $\widetilde{A}$ l'ensemble des éléments $x \in K$ tels qu'il existe $P \in A[X]$ unitaire avec $P(x) = 0$. On a clairement $A \subset \widetilde{A}$ (considérer les $X - a$ avec $a \in A$). On dit que A est intégralement clos si on a $A = \widetilde{A}$.

EXERCICE 7.23. *Montrer qu'un anneau factoriel est intégralement clos.*

EXERCICE 7.24. (Exemples et contre-exemples d'anneaux intégralement clos)

(i) Montrer[12] *que si $\mathbb{Z}[\sqrt{d}]$ est intégralement clos, alors d est sans facteur carré et on a $d \equiv 2, 3 \bmod 4$.*

12. On peut montrer que la réciproque est aussi vraie.

(ii) Soient k un corps et A le sous-anneau des $P \in k[X]$ vérifiant $P(0) = P(1)$ (justifier). Montrer que A n'est pas intégralement clos.

(iii) Soient k un corps et A le sous-anneau des $P \in k[X]$ vérifiant $P'(0) = 0$ (justifier). Montrer que A n'est pas intégralement clos.

On termine par quelques exercices sur les anneaux euclidiens.

EXERCICE 7.25. (Deux (autres) stathmes euclidiens sur $\mathbb{Z}$). *Montrer que les deux fonctions suivantes $\varphi : \mathbb{Z} \to \mathbb{N}$ définissent des stathmes euclidiens sur $\mathbb{Z}$:*

(i) $\varphi(n) = |n|$ si n est pair, $\varphi(n) = \frac{|n|-1}{2}$ sinon.

(ii) (Samuel) *$\varphi(n) = |n|$ si $n \neq 2$, et $\varphi(2)$ est un entier arbitraire $\geqslant 2$.*

Les deux exercices suivants exposent quelques uns des résultats de Mozkin [13] et Samuel [14] sur les anneaux euclidiens.

EXERCICE 7.26. *Un stathme euclidien $\varphi : A\backslash\{0\} \to \mathbb{N}$ est dit* fort *s'il satisfait de plus : si $a, b \neq 0$ et si b divise a alors $\varphi(b) \leqslant \varphi(a)$.*

(i) Donner des exemples de stathmes forts, et des exemples qui ne le sont pas.

(ii) Montrer que tout anneau euclidien admet un stathme euclidien fort (Motzkin). *Un stathme euclidien φ étant donné on pourra considérer*

$$\varphi'(a) = \inf_{y \in aA} \varphi(y).$$

EXERCICE 7.27. (Caractérisation de Motzkin-Samuel des anneaux euclidiens). *Soit A un anneau* [15]*. On définit par récurrence une suite de sous-ensembles $\{\mathrm{E}_n(A)\}_{n\geqslant 0}$ de A en posant $\mathrm{E}_0(A) = \varnothing$, $\mathrm{E}'_n(A) = \mathrm{E}_n(A) \cup \{0\}$ et*

$$\mathrm{E}_{n+1}(A) = \{a \in A \mid aA + \mathrm{E}'_n(A) = A\}.$$

On pose aussi $\mathrm{Eucl}(A) = \bigcup_{n\geqslant 0} \mathrm{E}_n(A)$, et pour $a \in \mathrm{Eucl}(A)$ on note $\upsilon(a)$ le plus petit entier $n \geqslant 0$ vérifiant $a \in \mathrm{E}_{n+1}(A)$.

(i) Déterminer $\mathrm{E}_n(\mathbb{Z})$ pour tout entier $n \geqslant 1$, ainsi que υ.

(ii) Pour k un corps, déterminer $\mathrm{E}_n(k[X])$ pour tout entier $n \geqslant 1$, ainsi que υ.

(iii) Montrer $\mathrm{E}_1(A) = A^\times$ et que $\{\mathrm{E}_n(A)\}_{n\geqslant 0}$ est croissante pour l'inclusion.

(iv) On suppose A euclidien pour le stathme φ. Montrer $\upsilon \leqslant \varphi$ et

$$A = \mathrm{Eucl}(A) \cup \{0\}.$$

(v) Réciproquement, montrer que si on a $A = \mathrm{Eucl}(A) \cup \{0\}$ alors A est euclidien pour le stathme υ.

EXERCICE 7.28. *Soit A un anneau intègre. Une fonction $f : A \smallsetminus \{0\} \to \mathbb{N}$ est dite* presque euclidienne *si pour tout $a, b \in A \smallsetminus \{0\}$, on a soit $b \,|\, a$, soit il existe $c \in aA + bA$ tel que $f(c) < f(a)$. Si une telle fonction existe, on dit que A est presque euclidien.*

---

13. T. Motzkin, The Euclidean algorithm, Bull. Amer. Math. Soc. 55 (12), 1142-1146 (1949).

14. P. Samuel, *About Euclidean Rings*, Journal of Algebra 19, 282-301 (1979). Cet article est particulièrement accessible.

15. Pour coller aux conventions du cours, on pourra supposer A commutatif, mais cette hypothèse n'interviendra pas, sauf à la question (v) pour une raison de convention.

(i) Montrer que si A est presque euclidien, alors A est principal.

(ii) On suppose A principal. Montrer que la fonction $f : A \smallsetminus \{0\} \to \mathbb{N}$ associant à tout élément le nombre de ses facteurs premiers, est presque euclidienne.

(iii) En déduire que A est principal si, et seulement si, il est presque euclidien (Dedekind, Hasse).

Dans l'exercice suivant on utilisera la notion d'anneau quotient.

EXERCICE 7.29. (Idéaux premiers) *Soient A un anneau commutatif et P un idéal de A. On dit que P est premier si on a $P \neq A$ et si pour tout $x, y \in A$ tels que $xy \in P$, on a soit $x \in P$, soit $y \in P$.*

(i) Soit $f \in A$. Montrer que l'idéal fA est premier $\iff$ l'élément f est premier.

(ii) Montrer que P est premier $\iff$ l'anneau quotient A/P est intègre.

(iii) Montrer que si P est maximal alors P est premier.

(iv) Donner un exemple d'idéal premier non maximal.

(v) Montrer que si P est premier, et si A/P est fini, alors P est maximal.

L'exercice suivant montre que pour les anneaux comme $\mathbb{Z}[\sqrt{d}]$ ou A_d, factoriel équivaut à principal.

EXERCICE 7.30. *Soit A un anneau factoriel tel que pour tout $f \in A$ non nul alors A/fA est fini. On veut montrer que A est principal.*

(i) Montrer que A est noethérien.

(ii) Montrer que pour tout $f \in A$ premier, l'idéal fA est maximal.

(iii) Montrer que tout idéal maximal de A est de la forme fA avec $f \in A$ premier.

(iv) Soit $f \in A$ non nul ou unité, et $I \subset A$ un idéal non nul, montrer $fI \subsetneq I$.

(v) Conclure.