Université Paris 7 - Denis Diderot **Ch. BLANCHET – M. DIMITROV – R. MNEIMNÉ.**

(Algèbre M1 – 2009)

Corrigé du Partiel de Mathématiques du Vendredi 06 novembre 2009, établi par R.M.

Exercice I.

1. Déterminer pour chacun des anneaux qui suivent le groupe des éléments inversibles.

   (a) L'anneau quotient $R = \mathbb{R}[X]/(X^5)$

   La classe $\overline{P}$ est inversible si, et seulement si, les polynômes $P(X)$ et X^5 sont premiers entre eux, comme il résulte de l'identité de Bezout.

   Le groupe multiplicatif $R^\star$ de éléments inversibles est formé donc des classes $\overline{P}$ telles que $P(0) \neq 0$. Nous allons établir que ce groupe est isomorphe à $(\mathbb{R}^\star, \cdot) \times (\mathbb{R}^4, +)$. L'anneau R s'identifie à l'anneau $\mathbb{R}[J_5]$ des polynômes en le bloc de Jordan J_5, c'est-à-dire à l'anneau des matrices de la forme

$$\begin{bmatrix} a & b & c & d & e \\ 0 & a & b & c & d \\ 0 & 0 & a & b & c \\ 0 & 0 & 0 & a & b \\ 0 & 0 & 0 & 0 & a \end{bmatrix},$$

   avec a, b, c, d et e dans $\mathbb{R}$. Le groupe multiplicatif $R^\star$ est clairement isomorphe au produit direct $\mathbb{R}^\star \times N$, où N est le groupe des matrices de la forme ci-dessus avec $a = 1$. L'application exp : $(\mathbb{R}^4, +) \to (N, \cdot)$ *qui à la matrice* $X = \begin{bmatrix} 0 & x & y & z & t \\ 0 & 0 & x & y & z \\ 0 & 0 & 0 & x & y \\ 0 & 0 & 0 & 0 & x \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$ *associe son exponentielle* $\exp X = I_5 + X + X^2/2! + X^3/3! + X^4/4!$ *est un isomorphisme de groupes (abéliens).*

   (b) L'anneau de fractions $R = \mathbb{Z}_{(5)} := S^{-1}\mathbb{Z}$, où S est la partie multiplicative $\mathbb{Z} \setminus 5\mathbb{Z}$.

   Les éléments de l'anneau R s'identifient aux fractions m/n de $\mathbb{Q}$ tells que $5 \wedge n = 1$. Un tel élement est inversible dans R si, et seulement si, m et aussi premier avec 5.

   Le groupe $R^\star$ est un sous-groupe du groupe multiplicatif $\mathbb{Q}^\star$ et l'application

$$\frac{m}{n} \mapsto \big(sgn(mn), (v_p(m) - v_p(n))_{p \in \mathcal{P}*}\big)$$

   établit un isomorphisme entre le groupe $R^\star$ et le produit direct $\{\pm 1\} \times \mathbb{Z}^{(\mathcal{P}*)}$, où le second facteur est le groupe additif formé des suites d'entiers nuls à partir d'un certain rang, et indexés par l'ensemble $\mathcal{P}*$ de tous les nombres premiers à l'exception du nombre 5. La notation $v_p(n)$ désigne, bien sûr, la valuation de l'entier n par rapport au nombre premier p ; quant au symbole sgn, il désigne évidemment le signe d'une entier. L'isomorphisme ci-dessus résulte de la décomposition d'un entier en facteurs premiers.

2. On dit qu'un anneau R *commutatif* est local s'il possède un unique idéal maximal.

   (a) Montrer qu'un anneau est local si, et seulement si, le sous-ensemble de ses éléments non inversibles est un idéal.

   • Si M est l'unique idéal maximal de l'anneau R que nous supposons local, alors M coïncide avec l'ensemble $R\backslash R^\star$. En effet, un élément d'un idéal distinct de R ne peut être inversible, et, inversement un élément non inversible (étant contenu, d'après le théorème de Krull, dans un idéal maximal) ne peut être que dans M (qui est le seul idéal de R à être maximal).

   • Réciproquement, nous partons plus généralement d'un anneau (non réduit à zéro) dans lequel la somme de deux éléments non inversibles est non inversible. L'ensemble non vide $M = R\backslash R^\star$ de ses éléments non inversibles est alors un idéal : en effet, si xy est inversible, cela force x et y à l'être (si $zxy = 1$, par l'inverse par exemple de x est zy). Cet idéal est clairement l'unique idéal maximal, car tout idéal maximal est formé d'éléments non inversibles, car à défaut, il serait égal à l'anneau tout entier.

   (b) Montrer que les deux anneaux de la question 1 sont des anneaux locaux.

   Si $f : R \to \mathbb{K}$ est un homomorphisme d'anneaux à valeurs dans le corps $\mathbb{K}$, et que $x \in R$ est inversible si, et seulement si, $f(x) \neq 0$, alors l'anneau R est local et le noyau M de f est son unique idéal maximal. Le corps R/M est isomorphe à l'image de f et s'appelle le corps résiduel de l'anneau local R.

   Mettons en évidence un tel homomorphisme pour chacun des anneaux de la question 1).

   • Pour l'anneau $\mathbb{R}[X]/(X^5)$, l'application $\overline{P} \mapsto P(0)$ répond à la question et nous donne comme corps résiduel $\mathbb{R}$.

   • Pour l'anneau $R = \mathbb{Z}_{(5)}$, nous remarquons que la surjection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ applique les éléments de $S = \mathbb{Z} \setminus 5\mathbb{Z}$ sur des éléments inversibles : elle se factorise donc à travers R. Cela définit une application surjective $f : R \to \mathbb{F}_5$, et un élément $m/n \in R$ est dans son noyau si, et seulement si, $\pi(m)\pi(n)^{-1} = 0$, c'est-à-dire m multiple de 5, autrement dit m/n est non inversible. L'idéal maximal M de R est donc l'idéal principal $5R$ et le corps résiduel est $\mathbb{F}_5$.

Exercice II.

On étudie dans cet exercice l'idéal $I = (7, X^4 + 1)$ de $\mathbb{Z}[X]$ et l'anneau quotient $R = \mathbb{Z}[X]/I$.

1. Montrer que le polynôme $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$.

   Le polynôme X^4+1 est primitif et nous allons montrer de trois façons différentes qu'il est irréductible sur $\mathbb{Q}$.

   • Il n'a pas de racine dans $\mathbb{R}$, puisque $x^4+1 \geq 1$, $\forall x$. S'il était réductible sur $\mathbb{Q}$, il se factoriserait comme produit $D_1(X)D_2(X)$ de deux polynômes du second degré. Ces polynômes ne pouvant, tout comme $X^4 + 1$, avoir de racine dans $\mathbb{R}$ donnent aussi la décomposition *de $X^4 + 1$ en facteurs irréductibles dans l'anneau factoriel $\mathbb{R}[X]$. Or*

$$X^4 + 1 = (X^4 + 2X^2 + 1) - 2X^2 = (X^2 + 1)^2 - 2X^2 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1),$$

   écriture valable dans $\mathbb{R}$. Les deux polynômes du second degré qui apparaissent sont irréductibles sur $\mathbb{R}$, car comme $X^4 + 1$ n'ont pas de racines dans $\mathbb{R}$. Ils coïncident à l'ordre près avec les précédents, et forcent donc $\sqrt{2}$ à être rationnel. D'où contradiction. (On aurait pu raisonner ainsi, et tout aussi bien, avec le corps $\mathbb{Q}(\sqrt{2})$ en place du corps $\mathbb{R}$. Par ailleurs, la décomposition donnée dans $\mathbb{R}$ s'obtient aussi en passant dans $\mathbb{C}$ et en regroupant deux à deux les racines conjuguées –voir la deuxième méthode–...)

• *On peut aussi bêtement écrire par l'absurde* $X^4+1=(X^2+aX+b)(X^2+cX+1/b)$ *dans* $\mathbb{Q}[X]$, *et en idendifiant en déduire que* $a+c=0$, $ac+b+1/b=0$ *et* $a/b+bc=0$. *On a alors d'une part* $a/b=ab$ *ou* $a(1-b^2)=0$, *et d'autre part* $1+b^2-a^2b=0$ *et donc que* $a\neq 0$ *(car* $1+b^2\geq 1$*). On a donc* $b^2=1$ *et* $2=\pm a^2$*... On n'oublie pas de répéter qu'il ne peut y avoir de facteur du premier degré.*

• *On reconnaît* X^4+1 *comme le polynôme cyclotomique* $\Phi_8(X)$, *puisque ses racines sont les racines primitives huitièmes de l'unité (car ce sont les racines huitièmes de l'unité qui ne sont pas racines quatrièmes). Il est irréductible comme tous les polynômes cyclotomiques.*

On écrit ici $\Phi_8(X+1)=(X+1)^4+1=X^4+4X^3+6X^2+4X+2$ *et on applique à ce polynôme le critère d'Eisenstein, dans l'anneau factoriel* $\mathbb{Z}$, *avec l'élément irréductible* 2.

Comme $P(X)\mapsto P(X+1)$ *est un automorphisme de* $\mathbb{Z}[X]$, *le polynôme* $\Phi_8(X)=X^4+1$ *est à son tour irréductible.*

2. Montrer qu'il cesse de l'être dans $\mathbb{F}_7[X]$ et donner sa décomposition en produit d'irréductibles.

   Comme 2 *est un carré modulo* 7, *puisque* $\overline{3}^2=\overline{2}$, *on écrit tout comme plus haut*

$$X^4+1=(X^2+1)^2-2X^2=(X^2-3X+1)(X^2+3X+1),$$

   Ces polynômes du second degré sont irréductibles, car leur discriminant, qui vaut $\overline{5}$, *n'est pas un carré modulo* 7. *On peut invoquer aussi le fait qu'ils n'ont pas de racines tout comme* X^4+1, *car* -1 *n'est pas un carré modulo* 7, *puisque* $7\equiv 3 \mod(4)$ *(et non point à* 1*).*

3. Quels sont les idéaux maximaux de $\mathbb{Z}[X]$ qui contiennent I ?

   Un idéal maximal M *contenant* I *contient l'idéal* $(7)=7\mathbb{Z}[X]$ *engendré par* 7. *Or les idéaux maximaux de* $\mathbb{Z}[X]$ *contenant cet idéal-là sont en correspondance bijective croissante avec les idéaux maximaux de* $\mathbb{Z}[X]/(7)=F_7[X]$, *au moyen de la surjection canonique* $s=\mathbb{Z}[X]\to\mathbb{F}_7[X]$. *Les idéaux maximaux de* $\mathbb{Z}[X]$ *qui contiennent* I *sont donc en correspondance bijective avec les idéaux maximaux de* $\mathbb{F}_7[X]$ *qui contiennent l'image* $s(I)$, *c'est-à-dire avec les idéaux maximaux qui contiennent* $X^4+1=(X^2-3X+1)(X^2+3X+1)$. *Un idéal maximal étant premier, un tel idéal maximal contiendra* X^2-3X+1 *ou bien* X^2+3X+1, *car il contient leur produit. Il contiendra donc aussi l'idéal engendré par l'un ou l'autre de ces polynômes (irréductibles), idéaux qui sont maximaux! Deux idéaux maximaux* M *sont donc possibles* $M=(7,X^2+3X+8)$ *ou bien* $M=(7,X^2+4X+1)$.

   Remarque. *Si l'on connaît par avance la forme des idéaux maximaux de* $\mathbb{Z}[X]$, *on cherchera d'abord l'intersection d'un tel idéal avec* $\mathbb{Z}$. *Comme il coupe* $\mathbb{Z}$ *suivant un idéal premier (et donc distinct de* $\mathbb{Z}$ *en particulier) contenant* $I\cap\mathbb{Z}=(7)$, *lequel est maximal, on a donc* $M\cap\mathbb{Z}=7\mathbb{Z}$. *L'idéal cherché est donc de la forme* $(7,P(X))$ *avec* P *irréductible modulo* 7. *En écrivant qu'un tel idéal contient* X^4+1, *soit* $X^4+1=7P_1+P_2P$ *et en passant modulo* 7, *on trouve que* P *modulo* 7 *est, par factorialité, l'un des deux polynômes du second degré donnés plus haut...*

4. Montrer que R est isomorphe à l'anneau $\mathbb{F}_7[X]/(X^4+1)$.

   La composée des homomorphismes surjectifs $\mathbb{Z}[X]\to F_7[X]\to\mathbb{F}_7[X]/(X^4+1)$ *a pour noyau l'idéal* I. *Le résultat découle aussitôt du théorème de factorisation d'un homomorphisme d'anneaux.*

5. Trouver le cardinal du groupe $R^\times$ des éléments inversibles.

   Le théorème des restes chinois donne $R\simeq\mathbb{F}_7[X]/(X^2-3X+1)\times\mathbb{F}_7[X]/(X^2+3X+1)$ *(on aura noté que les polynômes* X^2-3X+1 *et* X^2+3X+1 *sont premiers entre eux, car ce sont des polynômes irréductibles non associés). L'anneau* R *est produit de deux corps, de cardinal* 49 *chacun, (ce sont des espaces vectoriels de dimension deux sur* $\mathbb{F}_7$*) et son groupe d'éléments inversibles a pour cardinal* $(49-1)^2=(2^4\cdot 3)^2=256\cdot 9=2304=(50-2)^2$.

Remarque. *On peut déterminer le cardinal du groupe des unités de l'anneau $R = \mathbb{F}_7[X]/(X^4+1)$ directement en comptant les classes modulo X^4+1 qui sont premières avec X^4+1, et sans passer par le théorème des restes chinois : une classe est représentée uniquement par un polynôme de degré ≤ 3, et des $7^4 = 49^2$ éléments de R il faut exclure les multiples par $aX+b$ de nos deux polynômes $X^2 \pm 3X + 1$, ce qui donne 7^2 éléments chaque fois, donc 2×49, mais on aura compté deux fois la classe nulle. D'où $(7^4 - 2 \cdot 7^2 + 1) = (7^2-1)^2$ inversibles. C'est quand même moins élégant.*

Exercice III. Soit A est le sous-groupe additif de $\mathbb{C}$ engendré par les deux racines, notées j et $\overline{j}$, de X^2+X+1, et soit B le sous-groupe $\mathbb{Z} + \mathbb{Z}i\sqrt{3}$.

Il est bon, avant de se lancer dans la réponse aux questions, de penser au fait que les éléments $a+bj$ de l'anneau $A = \mathbb{Z}[j]$ donnent par passage modulo 2 quatre représentants (cf. plus bas), suivant la parité des entiers a et b. De plus, il est bon d'avoir déjà rencontré le fait standard que les éléments de cet anneau s'écrivent sous la forme $x + iy\sqrt{3}$ avec x et y tous deux des entiers (ce qui donnera les éléments de $B = \mathbb{Z}[i\sqrt{3}]$), ou tous deux des demi-entiers (c'est-à-dire des éléments de $\frac{1}{2} + \mathbb{Z}$).

1. (a) Montrer que A est un sous-anneau de $\mathbb{C}$.

   Comme $\overline{j} = j^2 = -1 - j$, on voit que $A = \mathbb{Z} + \mathbb{Z}j$. Le sous-anneau $\mathbb{Z}[j]$ de $\mathbb{C}$ engendré par j est formé de tous les $P(j)$, où $P(X)$ est un polynôme quelconque de $\mathbb{Z}[X]$. En divisant un tel polynôme par le polynôme unitaire *X^2+X+1, on voit que $P(j) \in A$. On a donc $A = \mathbb{Z}[j]$. De plus, l'application $P \mapsto P(j)$ a pour noyau l'idéal engendré par X^2+X+1 : il s'ensuit que l'anneau A est isomorphe au quotient $\mathbb{Z}[X]/(X^2+X+1)$.*

   (b) Montrer que $N(z) = |z|^2$ définit une application de A dans $\mathbb{N}$ qui respecte la multiplication. On admet que N est un stathme euclidien sur A.

   $N(z) = (a+bj)(a+bj^2) = a^2+b^2-ab \in \mathbb{Z}$ et est positif, car égal à $|z|^2$. Le caractère multiplicatif résulte de la multiplicativité du module (d'un nombre complexe).

   Rappelons pourquoi N définit un stathme euclidien sur $\mathbb{Z}[j]$. Si z et $z' \neq 0$ sont donnés, le nombre complexe z/z' est au plus à une distance égale à $\sqrt{3}/3 < 1$ des points du réseau $\mathbb{Z}[j]$ (considérer le pavage du plan avec les triangles équilatéraux de côtés de longueur 1 et de sommets les points de $\mathbb{Z}[j]$). Il existe donc $q \in A$ tel que $|z/z' - q| < 1$ ou encore $z = qz' + r$ avec $0 \leq N(r) < N(q)$.

   (c) Quel est l'ensemble $A^\times$ des éléments inversibles de A ?

   Comme $N(1) = 1$, le caractère multiplicatif de N force les inversibles de A à aller sur 1. Ils sont donc sur le cercle unité dans $\mathbb{C}$, mais aussi dans le réseau A : ils sont donc, comme le montre un dessin rapide, parmi les six racines sixièmes de l'unité, lesquelles inversement sont dans $A^\times$. Le groupe $A^\times$ est donc isomorphe à U_6.

2. (a) Montrer que B est un sous-anneau de A et qu'il n'est pas factoriel.

   L'ensemble sous-jacent à B coïncide avec l'image de l'homomorphisme défini sur l'anneau $\mathbb{Z}[X]$ à valeurs dans $\mathbb{C}$, qui applique $P(X)$ sur $P(i\sqrt{3})$, comme le montre une division par le polynôme unitaire *X^2+3. Il est donc clair que B est un anneau et qu'il est de plus isomorphe à l'anneau quotient $\mathbb{Z}[X]/(X^2+3)$.*

   L'anneau B n'est pas factoriel, car l'élément 2 de B est irréductible et engendre pourtant un idéal non premier. En effet, $B/(2) \simeq \mathbb{Z}[X]/(2, X^2+3) \simeq \mathbb{F}_2[X]/(X^2+3) \simeq \mathbb{F}_2[X]/(X+1)^2$ est clairement pas intègre. Et de plus, si $2 = xy$, alors $4 = N(x)N(y)$ ce qui force $N(x)$ ou $N(y)$ à valoir 1 (et donc à être inversibles), car il n'y a pas dans B d'éléments de module $\sqrt{2}$ (ou s'il l'on veut, à tort, éviter de regarder un dessin parce que l'équation $x^2 - 3y^2 = 2$ n'a pas de solutions dans $\mathbb{Z}$ comme le montre un passage modulo 3).

Remarque. *L'argument de plus rapide, si l'on est un peu savant, pour nier la factorialité de l'anneau B consiste à remarquer qu'il n'est pas intégralement clos, puisque j est dans son corps de fractions, est entier sur B (puisqu'il l'est déjà sur $\mathbb{Z}$) et n'appartient pas à B.*

(b) Montrer que les corps de fractions $\mathcal{Q}(B)$ et $\mathcal{Q}(A)$ sont isomorphes.

Si $z = a + bj \in A$ est non nul, il est inversible dans le corps $\mathbb{Q}(j) = \mathbb{Q}[j]$ (et admet pour inverse $\overline{z}/N(z)$). Il existe donc un homomorphisme de $\mathcal{Q}(A)$ dans $\mathbb{Q}(j)$, obligatoirement injectif, car défini sur un corps. La surjectivité est immédiate, vu que $\mathbb{Q}(j)$ est le plus petit corps de $\mathbb{C}$ contenant j.

On procède de même pour montrer que $\mathcal{Q}(B)$ est isomorphe à $\mathbb{Q}(j)$.

Nos deux corps de fractions, isomorphes tous deux à $\mathbb{Q}(j)$, sont donc isomorphes entre eux.

3. (a) Montrer que 1 et j engendrent A comme B-module.

Il s'agit de démontrer que $A = B + Bj$, et surtout que $A \subseteq B + Bj$, mais on a déjà $A = \mathbb{Z} + \mathbb{Z}j$ et $\mathbb{Z} \subset B$.

(b) Quels sont les éléments de torsion du B-module A ?

Si $\lambda z = 0$, avec $0 \neq \lambda \in B$ et $z \in A$, on a alors que $z = 0$, car $\mathbb{C}$ est intègre ! L'anneau A est donc un B-module de type fini et sans torsion.

Remarque. *Si B était principal, le B-module A serait libre, mais cela est démenti dans la question qui suit.*

(c) Est-ce que A est un B-module libre ?

La réponse est non. En effet, dans le cas contraire $A \simeq B$ ou $A \simeq B^2$ comme B-modules. On aurait dans le second cas au niveau des groupes additifs sous-jacents $\mathbb{Z}^2 \simeq (\mathbb{Z}^2)^2 \simeq \mathbb{Z}^4$, ce qui n'est pas.

Si par contre le B-module A était isomorphe à B, cela voudrait dire que $A = zB$ pour un certain $z \in A$, et forcerait z à être inversible et d'avoir son inverse dans B, et donc $z = \pm 1$ et donc $A = B$, ce qui est faux !

(d) Déterminer le B-module quotient A/B.

On va démontrer que ce quotient contient deux classes, la classe B et la classe $j+B$. En effet, un élément z de $A = \mathbb{Z}[j]$ s'écrit $(a + bi\sqrt{3})/2$, avec a et b tous deux pairs ou tous deux impairs. Dans le premier cas, il est dans B et dans le second, c'est $z - j = (a+bi\sqrt{3})/2 - (-1+i\sqrt{(}3)/2 = \big(a + 1) + (b - 1)i\sqrt{3}\big)/2$ qui est dans B.

Remarques.

• *Une classe du B-module A/B admet, vu la question 3 (a), un représentant de la forme zj, avec $z \in B$. Cela prouve que j est un générateur du B-module A/B, qui par ailleurs est annulé par 2 (puisque $2j = i\sqrt{3} - 1 \in B$). Le quotient $B/2B$ se surjecte donc sur A/B. On ne peut ici conclure, car $B/2B$ a quatre éléments comme on l'a vu plus haut.*

• *On peut obtenir ce résultat en comparant les surfaces des domaines fondamentaux des réseaux A et B...*

• *On pourra aussi obtenir ce résultat en considérant les fibres de l'homorphisme Φ défini plus bas.*

4. Montrer que tout élément de A est associé à un élément de B. Décomposer $56 + 14i\sqrt{3}$ en produit d'éléments irréductibles appartenant à B.

Nous allons démontrer que $A = B \cup jB \cup j^2B$. Cela résultera de l'étude des fibres de l'homomorphisme d'anneaux surjectif (défini par de passage modulo 2)

$$\Phi : A \simeq \mathbb{Z}[X]/(X^2 + X + 1) \to \mathbb{Z}[X]/(2, X^2 + X + 1) \simeq \mathbb{F}_2[X]/(X^2 + X + 1) = \mathbb{F}_4,$$

sachant que le polynôme X^2+X+1 est (le seul polynôme) irréductible de degré deux sur $\mathbb{F}_2$. Comme 1 et $2j$ engendrent le réseau B, on voit que les éléments de B s'appliquent sur $F_2 \subset \mathbb{F}_4 = \{0,1,\alpha,\alpha^2\}$, où α est la classe de X dans $\mathbb{F}_2[X]/(X^2+X+1)$, vérifiant $\alpha^3=1$. Réciproquement, un élément de A qui va sur 0 ou 1 modulo 2 s'écrit $2z$ ou $1+2z$ avec $z \in A$ et serait donc dans B puisque $2A \subset B$. Autrement dit, l'anneau B est la réunion des deux fibres au dessus de $\mathbb{F}_2$.

Si maintenant un élement z de A s'applique sur α, alors j^2z s'appliquera sur 1 et sera donc dans B ; enfin si z s'appliquait sur α^2, alors jz s'appliquerait sur 1 et serait dans B.

Remarque. *On notera que $B \cap jB = B \cap j^2B = jB \cap j^2B = (2) = ker(\Phi)$. On notera aussi que le noyau de Φ qui est $2A$ est formé des $a+ib\sqrt{3}$ tels que a et b soient tous deux pairs ou tous deux impairs. On retrouve enfin le fait que $A = B \cup (j+B) = B \cup (j^2+B)$, puisque la somme de deux éléments non nuls distincts de $\mathbb{F}_4$ est le troisième élément non nul.*

Décomposons $z = 56+14i\sqrt{3}$ en produit d'irréductibles dans l'anneau factoriel A. On écrit $z = 2\cdot(2+i\sqrt{3})(2-i\sqrt{3})(4+i\sqrt{3})$. L'élément 2 est irréductible dans A, car $A/(2) \simeq F_4$. Les éléments $2 \pm i\sqrt{3}$ et tout comme $4+i\sqrt{3}$ le sont aussi, car leurs normes sont des nombres premiers de $\mathbb{N}$.

5. Trouver un p.g.c.d. appartenant à B de $19+38i\sqrt{3}$ et $8+3i\sqrt{3}$.

   On écrit $19+38i\sqrt{3} = (4+i\sqrt{3})(4-i\sqrt{3})(1+2i\sqrt{3})$ qui est une décomposition en facteurs irréductibles. La norme de $8+3i\sqrt{3}$ vaut $64+3\cdot 9 = 91$ est un nombre premier.

   Ces deux éléments sont donc premiers entre eux et leur pgcd vaut 1.

6. Montrer que le polynôme $X^5+14X+2+i\sqrt{3}$ est irréductible dans $\mathcal{Q}(A)$.

   On applique le critère d'Eisenstein dans l'anneau factoriel A avec l'élément irréductible $2+i\sqrt{3}$, qui divise 14, comme vu plus haut.