Université d'Évry Val d'Essonne 2009-2010

M54 algèbre et arithmétique

Indications pour la feuille 5

Exercice 1. 1. Traité en cours. C'est aussi une conséquence de la question suivante : si A est fini, alors il n'a qu'un nombre fini de parties, et *a fortiori* un nombre fini d'idéaux.

2. Soit x un élément non nul de A ; on veut montrer que x est inversible. Pour tout $n \in \mathbf{N}$, on considère l'idéal (x^n). Comme A n'a qu'un nombre fini d'idéaux, il existe deux entiers distincts, mettons $n < m$, tels que $(x^n) = (x^m)$. En particulier, $x^n \in x^m$ donc il existe $a \in A$ tel que $x^n = ax^m$. Comme A est intègre, tout ses éléments sont simplifiables ; en outre, $m > n$, on simplifie donc par x^n, on a

$$1 = ax^{m-n} = (ax^{m-n-1})x$$

et x est inversible. Ainsi, A est un corps.

Exercice 5. 1. Soient P et Q dans $I[X]$. Chaque coefficient de la somme $P+Q$ est la somme d'un coefficient de P et d'un coefficient de Q : 'est donc la somme de deux éléments de I, donc un élément de I. Ainsi, $P+Q \in I[X]$.

Soit par ailleurs $R \in A[X]$. Chaque coefficient du produit PR est une somme dont les termes sont le produit d'un coefficient de R par un coefficient de Q (c'est plus difficile à dire qu'à comprendre). C'est une combinaison linéaire d'éléments de I, donc un élément de I. Ainsi, $PR \in I[X]$, et $I[X]$ est un idéal de $A[X]$.

2. Si a est un élément de A, notons $\overline{a}$ sa classe dans A/I. On définit alors un morphisme :

$$\begin{gathered}\phi\colon A[X] \to (A/I)[X] \\ a_0 + a_1X + \cdots + a_nX^n \mapsto \overline{a_0} + \overline{a_1}X + \cdots + \overline{a_n}X^n\end{gathered}$$

Pour montrer qu'il passe au quotient par $I[X]$ en donnant un isomorphisme, il suffit de montrer que son noyau est exactement $I[X]$. Or en notant $P = a_0 + a_1X + \cdots + a_nX^n$, on a

$$\begin{aligned}\phi(P) = 0 &\Leftrightarrow \overline{a_0} + \overline{a_1}X + \cdots + \overline{a_n}X^n = 0 \\ &\Leftrightarrow \overline{a_0} = 0 \text{ et } \overline{a_1} = 0 \text{ et } \ldots \text{et } \overline{a_n} = 0 \\ &\Leftrightarrow a_0 \in I \text{ et } a_1 \in I \text{ et } \ldots \text{et } a_n \in I \\ &\Leftrightarrow P \in I[X]\ .\end{aligned}$$

3. Supposons I premier. On peut essayer de montrer directement que si $PQ \in I[X]$, alors $P \in I[X]$ ou $Q \in I[X]$, mais ça risque d'être difficile. Ici, il faut bien mieux

utiliser l'autre caractérisation des idéaux premiers : un idéal est premier si et seulement si le quotient par cet idéal est intègre.

Ici, comme I est premier, A/I est intègre donc $(A/I)[X]$ aussi. Compte tenu de la question précédente, $A[X]/I[X]$ est donc intègre, et $I[X]$ est premier.

4. $\mathbf{Z}[X]/(p) = \mathbf{Z}[X]/p\mathbf{Z}[X] \approx (\mathbf{Z}/p\mathbf{Z})[X] = \mathbf{F}_p[X]$.

Exercice 6. 1. Pour commencer, il est clair que pour qu'un élément de $\mathbf{Z}$ soit irréductible sur $\mathbf{Z}[\sqrt{-5}]$, il faut qu'il le soit déjà sur $\mathbf{Z}$, c'est-à-dire que ce soit être un nombre premier. Nous avons donc un condition nécessaire, mais peut-être pas suffisante. Cherchons à voir si un nombre premier p peut être le produit de deux éléments de $\mathbf{Z}[\sqrt{-5}]$.

Soient $a+b\sqrt{-5}$ et $c+d\sqrt{-5}$ deux éléments de $\mathbf{Z}[\sqrt{-5}]$. Supposons que leur produit est un nombre premier p. Posons $\alpha = \mathrm{pgcd}(a,b)$ et $\beta = \mathrm{pgcd}(c,d)$, puis $a' = a/\alpha$ et ainsi de suite de sorte que a', b', c' et d' sont des entiers et que

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = \alpha\beta(a' + b'\sqrt{-5})(c' + d'\sqrt{-5}) \ .$$

Alors, $(a' + b'\sqrt{-5})(c' + d'\sqrt{-5})$ est un diviseur de p, c'est donc 1 ou p.

Par ailleurs, ce produit étant réel, ses deux facteurs complexes ont des arguments opposés, c'est-à-dire qu'il existe $\lambda \in \mathbf{R}_+$ tel que $c' + d'\sqrt{-5} = \lambda(a' - b'\sqrt{-5})$. Mais, comme c' et d' sont premiers entre eux, de même que a' et b', on a forcément $\lambda = 1$. Ainsi on a un produit de la forme $(a' + b'\sqrt{-5})(a' - b'\sqrt{-5}) = a^2 + 5b^5$, qui vaut 1 ou p.

Si $a^2+5b^2 = 1$, on a forcément $a = 1$ et $b = 0$. En particulier, $a+b\sqrt{-5}$ et $c+d\sqrt{-5}$ étaient déjà dans $\mathbf{Z}$. Ce cas n'est pas intéressant.

Sinon, on a $a^2 + 5b^2 = p$. On peut donc dire que les éléments de $\mathbf{Z}$ irréductible sur $\mathbf{Z}[\sqrt{-5}]$ sont les nombres premiers qui ne s'écrivent pas sous la forme $a^2 + 5b^2$. Il est difficile de donner une description plus précise. Mentionnons seulement que 29 est un exemple d'entier irréductible dans $\mathbf{Z}$, mais pas dans $\mathbf{Z}[\sqrt{-5}]$, car $29 = (3 + 2\sqrt{-5})(3 - 2\sqrt{-5})$.

2. Au vu du raisonnement tenu à la question précédent, il est clair qu'on doit chercher l'autre décomposition de 6 sous la forme $c(a + b\sqrt{-5})(a - b\sqrt{-5})$ avec a, b et c entiers, c'est-à-dire chercher une solution à $6 = c(a^5 + 5b^2)$. En essayant, on trouve rapidement que $a = 1$, $b = 1$ et $c = 1$ conviennent, de même que $a = 2$, $b = 0$ et $c = 3$. On a donc deux décompositions distinctes : $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Ainsi, $\mathbf{Z}[\sqrt{-5}]$ n'est pas factoriel. (On peut en déduire qu'il n'est pas principal, et donc pas euclidien, même si ce n'était pas demandé dans l'énoncé.)

Exercice 7. 1. Exemple traité en cours, je crois. Sinon voir par exemple la page wikipédia « Entiers de Gauss » qui contient un démonstration.

2. Par contraposée : si α n'est pas irréductible, il existe β et γ non inversibles tels que $\alpha = \beta\gamma$, donc $N(\alpha) = N(\beta)N(\gamma)$. Comme β et γ ne sont pas inversibles, leur normes non plus (par le même raisonnement), et $N(\alpha)$ n'est pas irréductible.

3. Par le même raisonnement qu'à l'exercice précédent, les nombres premiers qui restent irréductibles dans $Z[i]$ sont ceux qui ne s'écrivent pas sous la forme a^2+b^2 avec a et b entiers. On peut soit essayer à la main, soit se souvenir du résultat de l'exercice 8 de la feuille 1 : un premier p est un somme de carré si et seulement si il vaut 2, on est congru à 1 modulo 4. Ainsi, les nombres irréductibles dans la liste proposée sont : 7, 11, 19, 23, 31.
4. Non, car 2 n'est pas irréductible.

Exercice 8. Traité en cours.

Exercice 9. Notons $q = p^n$, et $x_1, \dots x_q$ les éléments de K. Posons $P = (X-x_1)\cdots(X-x_q)$. Il est clair que P est toujours nul (bien que ce ne soit pas le polynôme nul, attention). Donc $P+1$ ne s'annule jamais.

Exercice 10. 1. Traité en TD.

2. Il suffit d'écrire tous les polynômes de degré 2 (il y en a 4) puis tous les polynômes de degré 3 (il y en a 8), puis de regarder ceux qui s'annulent, d'après la question précédente (deux éléments à tester à chaque fois). On trouve

$$X^2+X+1$$
$$X^3+X^2+1 \qquad X^3+X+1\ .$$

3. Si ces polynômes n'étaient pas irréductibles dans $\mathbf{Z}[X]$ leurs réductions modulo 2 ne le seraient pas non plus. La réduction de P modulo 2 est X^3+X+1, qui est irréductible d'après la question précédente. Celle de Q est X^5+X^3+1 qui est irréductible d'après la question suivante.
4. Un polynôme de degré 4 qui n'est pas irréductible est soit le produit d'un polynôme de degré 3 par un polynôme de degré 1 (il a donc un zéro dans ce cas), soit le produit de deux polynômes irréductibles de degré 2. On peut commencer par écrire tous les polynômes de degré 4 n'ayant pas de zéro comme à la question 2. (Avec le temps, vous devriez remarquer qu'un polynôme s'annule en 0 si son terme constant est nul, et en 1 s'il a un nombre pair de termes.) Ensuite, il suffit d'éliminer ceux qui sont la produit de deux polynômes irréductibles de degré 2. D'après la question 2, il n'y en a qu'un : c'est $(X^2+X+1)^2 = X^4+X^2+1$. Tous ceux qui restent sont irréductibles.

   Pour les polynômes de degré 5, on applique un raisonnement similaire. Par le même genre de méthode (en étant un petit peu plus précis, c'est-à-dire en calculant à chaque fois une estimation nu nombre de polynômes irréductibles de degré n), on peut montrer qu'il existe des polynômes irréductibles de n'importe quel degré sur $\mathbf{F}_p$. Comparer avec le cas de $\mathbf{R}$, ou les polynômes irréductibles sont tous de degré 1 ou 2. (Et sur $\mathbf{Q}$, savez-vous exhiber un polynôme irréductible de n'importe quel degré ?)

Exercice 12. 1. Traité en TD.

2. Q est irréductible d'après l'exercice 10. Donc l'idéal qu'il engendre est premier et même maximal, puisque $\mathbf{F}_2[X]$ est un anneau principal. Le quotient est donc un corps. Par ailleurs, en notant α la classe de X dans le quotient, on voit que chaque élément s'écrit de façon unique sous la forme $a + b\alpha + c\alpha^2$, avec a, b et c dans $\mathbf{F}_2$. Le quotient est donc un corps à 8 éléments. (On le note habituellement $\mathbf{F}_8$.) Pour dresser la table de multiplication, on utilise les règles habituelles de calcul dans un anneau commutatif de caractéristique 2, et la règle additionnelle $\alpha^3 = \alpha + 1$.