Université de Rennes 1 — Master M1 de mathématiques
Année 2005-2006 — H04. Théorie algébrique des nombres

Feuille de TD 1

Exercice 1

1. Se rappeler la définition d'un anneau euclidien, principal, factoriel. Montrer qu'un anneau euclidien est principal et qu'un anneau principal est factoriel. Donner le plus grand nombre possible d'exemples d'anneaux euclidiens, d'anneaux factoriels non principaux, d'anneaux (intègres) non factoriels. Un anneau principal et non euclidien est étudié à l'exercice 17.

2. Si A est factoriel, quels sont les éléments irréductibles de $A[X]$? En déduire que $A[X]$ est factoriel.

3. Soit A un anneau factoriel vérifiant le théorème de Bézout (i.e. pour tout $a, b \in A$ l'idéal engendré par a et b est principal). Montrer que A est principal (attention, un anneau factoriel n'est pas nécessairement noethérien).

Exercice 2

Montrer que $(1-i)$ est irréductible dans $\mathbf{Z}[i]$. Vérifier que dans $\mathbf{Z}[i]$ on a

$$5 = (2+i)\,(2-i) = (1+2\,i)(1-2\,i)$$

et que ceci ne contredit pas la factorialité de $\mathbf{Z}[i]$.

Décomposer en produit d'irréductibles dans $\mathbf{Z}[i]$:

$$2,\ 7,\ 13,\ -2+2\,i,\ -11+2\,i \text{ et } 7+i.$$

Exercice 3

Décomposer en produit d'irréductibles dans $\mathbf{Z}[j]$:

$$3+j,\ 5+j,\ 3\,j, 7.$$

Exercice 4

1. Soit p un nombre premier congru à 1 modulo 4 et n un entier tel que $|n| < \frac{p}{2}$ et la classe $\overline{n}$ de n dans $\mathbf{F}_p^*$ soit d'ordre 4. Montrer que l'on peut définir un morphisme d'anneaux $\mathbf{Z}[i] \to \mathbf{F}_p$ qui envoie i sur $\overline{n}$, et que son noyau est engendré comme $\mathbf{Z}$-module par p et $n-i$. Montrer que si le noyau est engendré comme $\mathbf{Z}[i]$-module par $a + i\,b$ alors $p = a^2 + b^2$.

2. Ce qui précède donne un algorithme pour écrire p comme somme de deux carrés : on prend (cf. ci-dessous) un élément d'ordre 4 dans $\mathbf{F}_p^*$, et on calcule (comment ?) un générateur (sur $\mathbf{Z}[i]$) du noyau de la question 1. Pour trouver un élément d'ordre 4 de $\mathbf{F}_p^*$, il existe un moyen probabiliste efficace. Écrivons $p-1 = 2^r\,q$ avec q impair et $r \geqslant 2$. Montrer que pour tout x de $\mathbf{F}_p^*$, $x^{2^{r-2}\,q}$ est d'ordre 4 si et seulement si x n'est pas un carré. En déduire la probabilité pour qu'un élément x de $\mathbf{F}_p^*$ pris au hasard vérifie que $x^{2^{r-2}\,q}$ est d'ordre 4.

3. Appliquer cet algorithme à un «grand» nombre premier congru à 1 modulo 4, par exemple 1549 ou 12517.

Exercice 5
En considérant l'égalité

$$(1 + i\sqrt{5})\,(1 - i\,\sqrt{5}) = 2.3$$

montrer que $\mathbf{Z}\left[i\,\sqrt{5}\right]$ n'est pas un anneau factoriel.

Montrer que dans $\mathbf{Z}\left[i\,\sqrt{5}\right]$ 3 et $2 + i\,\sqrt{5}$ n'ont pas de ppcm et que 9 et $3\,(2 + i\,\sqrt{5})$ n'ont pas de pgcd (noter que chacun de ces deux résultats redémontre la non factorialité de $\mathbf{Z}\left[i\,\sqrt{5}\right]$).

Exercice 6
Montrer que dans un corps fini, tout élément est somme de deux carrés (si a est un élément d'un corps fini, compter le nombre d'éléments de ce corps de la forme x^2, respectivement de la forme $a - x^2$).

Exercice 7
Trouver les générateurs du groupe multiplicatif de $\mathbf{F}_p$ pour

$$p = 2, 3, 5, 7, 11, 31, 43, 71.$$

Exercice 8

1. Montrer que $X^2 + X + 1$ est l'unique polynôme irréductible de degré 2 sur $\mathbf{F}_2$. $\mathbf{F}_2[X]/(X^2 + X + 1)$ est un corps de cardinal 4. Écrire sa table d'addition et de multiplication dans la base $(cl(1), cl(X))$. Déterminer l'ordre de chacun de ses éléments non nuls, ainsi que ses automorphismes.

2. Déterminer les polynômes irréductibles unitaires de degré d à coefficient dans $\mathbf{F}_p$ lorsque $(d, p) = (3, 2)$, $(4, 2)$, et $(2, 3)$. Si P est un tel polynôme, $\mathbf{F}_p[X]/(P)$ est un corps de cardinal p^d ; vérifier que les corps obtenus sont deux à deux isomorphes et exhiber un générateur de leur groupe multiplicatif.

Exercice 9
Combien y a-t-il de polynômes irréductibles de degré 17 sur $\mathbf{F}_2$?

Exercice 10
Soit p un nombre premier, $n \geqslant 1$ un entier et K un corps à p^n éléments. Soit d un diviseur de n et $F_d : K \to K$ défini par $F_d(x) = x^{p^d}$. Montrer que F_d est un automorphisme de K, que le sous-corps de K fixé par F_d est un sous-corps de K à p^d éléments et que c'est l'unique sous-corps de K à p^d éléments. On note K_d ce sous-corps.

Montrer que le groupe de Galois de K sur K_d (i.e. le groupe des automorphisme du corps K fixant le sous-corps K_d) est cyclique d'ordre n/d, engendré par F_d.

Exercice 11
Montrer que le polynôme $X^4 + 1$ est réductible sur $\mathbf{F}_p$ pour tout p premier et est irréductible sur $\mathbf{Z}$.

Exercice 12
Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4 et qu'il existe une infinité de nombres premiers congrus à 1 modulo 4 (s'inspirer de la preuve classique de l'infinitude des nombres premiers ; pour le deuxième cas, on utilisera après l'avoir démontré le fait que tout facteur premier impair d'un nombre de la forme $n^2 + 1$ est congru à 1 modulo 4).

Exercice 13
Peut-on compléter le vecteur $(6, 15, 20)$ en une base de $\mathbf{Z}^3$? Si oui, calculer une telle base de $\mathbf{Z}^3$.

Soit M le sous $\mathbf{Z}$-module de $\mathbf{Z}^2$ engendré par $(2, 4)$ et $(4, 11)$. Calculer une base de $\mathbf{Z}^2$ adaptée à M et les facteurs invariants de $\mathbf{Z}^2/M$.

Trouver toutes les solutions entières du système d'équations diophantiennes linéaires suivant :

$$\begin{cases} 2\,x + 4\,y + 3\,z &= 3 \\ 4\,x + 5\,y + 7\,z &= 2. \end{cases}$$

Exercice 14
On considère l'équation $x^2 + y^2 = p\,z^2$ où p est un nombre premier. Vérifier qu'elle possède une solution dans $\mathbf{Q}^3$ si et seulement si elle en possède une dans $\mathbf{Z}^3$. Montrer que si -1 n'est pas un carré dans $\mathbf{F}_p$ elle n'admet pas de solution dans $\mathbf{Z}^3$. Réciproque ? Dans le cas où l'équation admet une solution, décrire toutes les solutions dans $\mathbf{Q}^3$.

Exercice 15
Donner toutes les solutions dans $\mathbf{Z}^2$ et $\mathbf{Q}^2$ des équations suivantes :

$$x^2 + 2\,y^2 = 6,$$

$$x^2 + y^2 = 11,$$

$$x^2 + 2\,y^2 = 11,$$

$$x^2 + 2\,y^2 = 7,$$

$$x^2 - 6\,y^2 = -1.$$

On pensera à réduire les équations modulo un nombre premier. On pensera aussi à la paramétrisation rationnelle des coniques.

Exercice 16
Le but de cet exercice est de montrer que $(3, 5)$ et $(3, -5)$ sont les seules solutions dans $\mathbf{Z}^2$ de l'équation

$$y^2 + 2 = x^3 \quad (*).$$

1. Montrer que l'anneau $\mathbf{Z}\left[i\sqrt{2}\right]$ est euclidien (donc factoriel). On s'inspirera de la preuve du fait que $\mathbf{Z}[i]$ est euclidien.

2. En déduire que si $(x, y) \in \mathbf{Z}^2$ est une solution de $(*)$, il existe des entiers a et b vérifiant
$$y + i\sqrt{2} = \left(a + i\,b\,\sqrt{2}\right)^3.$$

3. Conclure.

4. Pouvez-vous donner un autre exemple d'équation diophantienne résolvable par une méthode similaire ?

Exercice 17
Le but de cet exercice est de montrer que l'anneau $\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais non euclidien.

1. On établit d'abord une condition nécessaire pour qu'un anneau soit euclidien. Montrer que si A est un anneau euclidien. il existe un élément x de A non inversible tel que la restriction du morphisme naturel $A \to A/(x)$ à l'ensemble $A^* \cup \{0\}$ soit surjective (considérer un élément de stathme minimal). Exhiber un tel élément dans les cas $A = \mathbf{Z}$, $A = k[X]$, $A = \mathbf{Z}[i]$.

2. Dans toute la suite de l'exercice, A désigne l'anneau $\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$. Déterminer le groupe des éléments inversibles de A (on utilisera la norme $N : z \mapsto z\,\overline{z}$).

3. En remarquant que $\alpha = \frac{1+i\sqrt{19}}{2}$ satisfait la relation $\alpha^2 - \alpha + 5 = 0$, déduire de ce qui précède que A n'est pas un anneau euclidien.

4. Le but du reste de l'exercice est de montrer que A est principal. On considère à nouveau la norme $N : z \mapsto z\,\overline{z}$. Contrairement à ce qui se passe pour $\mathbf{Z}[i]$, N n'est pas un stathme euclidien pour A. Montrer cependant l'existence d'une pseudo division euclidienne sur A au sens suivant : si $a \in A$ et $b \in A \setminus \{0\}$, il existe $q, r \in A$ vérifiant les deux conditions suivantes :
i. $r = 0$ ou $N(r) < N(b)$
ii. $a = b\,q + r$ ou $2\,a = b\,q + r$
(s'inspirer de la preuve du fait que $\mathbf{Z}[i]$ est euclidien pour N ; on écrira $\frac{a}{b} = u + v\,\alpha$ avec u et v rationnels ; si n est la partie entière de v, on distinguera les cas $v \notin \left]n + \frac{1}{3}, n + \frac{2}{3}\right[$ et $v \in \left]n + \frac{1}{3}, n + \frac{2}{3}\right[$, en considérant $2\frac{a}{b}$ dans ce dernier cas).

5. Déduire de la question précédente que A est principal. On utilisera, après l'avoir démontré, le fait que (2) est un idéal maximal de A.

Exercice 18

Le but de cet exercice est de démontrer la version (énoncée en cours) du théorème de Fermat où l'anneau $\mathbf{Z}$ est remplacé par un anneau de polynômes. Soit $n \geqslant 3$ un entier. On cherche les triplets (A, B, C) d'éléments de $\mathbf{C}[T]$, premiers entre eux (un tel triplet est dit primitif) et vérifiant l'équation

$$A^n + B^n = C^n \quad (E).$$

Un tel triplet solution sera dit trivial si ses éléments sont des constantes. On va montrer que les seuls triplets primitifs d'éléments de $\mathbf{C}[T]$ solutions de (E) sont les triplets triviaux. Pour cela on utilise la méthode de descente infinie. Pour tout triplet (A, B, C) de $\mathbf{C}[T]^3$ on pose

$$h(A, B, C) = \max(\deg(A), \deg(B), \deg(C)).$$

On suppose que l'ensemble $\mathcal{E}$ des triplets primitifs non triviaux solutions de (E) est non vide. On peut alors toujours choisir $(A_0, B_0, C_0) \in \mathcal{E}$ tel que

$$h(A_0, B_0, C_0) = \min_{(A,B,C)\in\mathcal{E}} h(A, B, C).$$

On va alors construire à partir de (A_0, B_0, C_0) un élément (A'_0, B'_0, C'_0) de $\mathcal{E}$ vérifiant

$$h(A'_0, B'_0, C'_0) < h(A_0, B_0, C_0)$$

d'où une contradiction.

1. On note μ_n l'ensemble des racines $n^{\text{èmes}}$ de l'unité de $\mathbf{C}$. Montrer que les polynômes $(C_0 - \zeta\, B_0)_{\zeta\in\mu_n}$ sont premiers entre eux deux à deux, et que pour tout $\zeta \in \mu_n$ il existe un polynôme P_ζ vérifiant $P_\zeta^n = C_0 - \zeta\, B_0$.

2. Soit ζ_1, ζ_2 et ζ_3 trois éléments distincts de μ_n. Posons pour $i = 1, 2, 3$ $P_i = P_{\zeta_i}$. Montrer qu'il existe un triplet (a_1, a_2, a_3) d'éléments de $\mathbf{C}$ tel qu'on ait
$$(a_1\, P_1)^n + (a_2\, P_2)^n = (a_3\, P_3)^n\,.$$
Conclure.

3. Peut-on remplacer $\mathbf{C}$ par un corps k algébriquement clos quelconque ?

4. Peut-on remplacer $\mathbf{C}$ par un corps quelconque ?

Exercice 19
Le but de cet exercice est de donner une démonstration du théorème de Lagrange : tout entier naturel est somme de quatre carrés.

1. Soit A un anneau. On note $1, i, j, k$ la base canonique du A-module libre A^4. Admettre (ou démontrer...) qu'il existe sur A^4 une loi de composition (que l'on notera multiplicativement) associative, distributive par rapport à l'addition, admettant 1 pour élément neutre, et telle que

$$i^2 = j^2 = k^2 = -1,\ i\,j = -j\,i = k,\ j\,k = -k\,j = i,\ k\,i = -i\,k = j.$$

   Cette loi munit A^4 d'une structure d'anneau non nécessairement commutatif. A^4 muni de cette structure est appelé *anneau des quaternions sur* A et noté $\mathbf{H}(A)$. Pour tout $z = a + b\,i + c\,j + d\,k \in \mathbf{H}(A)$ on définit le conjugué de z par $\overline{z} = a - b\,i - c\,j - d\,k$. Vérifier qu'on a pour tout $z, z' \in \mathbf{H}(A)$

$$\overline{z + z'} = \overline{z} + \overline{z'},\ \overline{z\,z'} = \overline{z}\,\overline{z'} \text{ et } \overline{\overline{z}} = z.$$

2. Pour $z \in \mathbf{H}(A)$, on définit la norme réduite de z, notée $N(z)$, par $N(z) = z\,\overline{z}$. Montrer que si $z = a + b\,i + c\,j + d\,k \in \mathbf{H}(A)$ on a $N(z) = a^2 + b^2 + c^2 + d^2$ et que pour tout z, $z' \in \mathbf{H}(A)$ on a $N(z\,z') = N(z)\,N(z')$. Montrer que z est inversible dans $\mathbf{H}(A)$ si et seulement si $N(z)$ est inversible dans A. En déduire que tout élément non nul de $\mathbf{H}(\mathbf{Q})$ est inversible.

3. On définit l'ensemble $\mathbf{H}$ des quaternions de Hurwitz comme le sous-ensemble de $\mathbf{H}(\mathbf{Q})$ donné par

$$\mathbf{H} = \left\{ \frac{a + b\,i + c\,j + d}{2},\ (a, b, c, d) \in \mathbf{Z}^4,\ a \equiv b \equiv c \equiv d\ [2] \right\}.$$

   Montrer que $\mathbf{H}$ est un sous-anneau (non commutatif) de $\mathbf{H}(\mathbf{Q})$ contenant $\mathbf{H}(\mathbf{Z})$. Montrer que tout idéal à gauche de $\mathbf{H}$ (respectivement à droite)(i.e. tout sous-groupe additif de $\mathbf{H}$ stable par multiplication à gauche (resp. à droite)) est de la forme $\mathbf{H}\,z$ (respectivement $z\,\mathbf{H}$) pour un $z \in \mathbf{H}$ (s'inspirer de la preuve du fait que $\mathbf{Z}[i]$ est principal).

4. Montrer que pour démontrer le théorème de Lagrange il suffit de montrer que tout nombre premier impair s'écrit comme somme de quatre carrés.

5. Montrer que sur un corps fini 0 est somme de quatre carrés *non tous nuls*. En déduire que l'anneau des quaternions sur un corps de caractéristique non nulle n'est jamais intègre.

6. Soit p un nombre premier impair. Montrer que l'on peut munir le quotient $\mathbf{H}/\mathbf{H}\,p$ d'une structure d'anneau (non commutatif) telle que l'application naturelle $\mathbf{H} \to \mathbf{H}/\mathbf{H}\,p$ soit un morphisme d'anneaux. Montrer que muni de cette structure $\mathbf{H}/\mathbf{H}\,p$ est isomorphe à $\mathbf{H}(\mathbf{F}_p)$. En considérant un élément non nul de $\mathbf{H}(\mathbf{F}_p)$ de norme réduite nulle, montrer qu'il existe un élément z de $\mathbf{H}$ tel que $\mathbf{H}\,z$ soit distinct de $\mathbf{H}$ et $\mathbf{H}\,p$ soit inclus dans $\mathbf{H}\,z$. En déduire que p est somme de quatre carrés.