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

Feuille de TD 2

Exercice 1
Soit $d \geqslant 3$ un entier. Montrer que, dans l'anneau $\mathbf{Z}\left[i\sqrt{d}\right]$, 2 est irréductible et l'idéal engendré par 2 n'est pas premier. L'anneau $\mathbf{Z}\left[i\sqrt{d}\right]$ est-il un anneau factoriel ?

Dans $\mathbf{Z}\left[i\sqrt{5}\right]$, 11 est-il irréductible ? L'idéal engendré par 11 est-il premier ?

Exercice 2
Rappelons que l'égalité

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

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

Plus généralement, montrer que si d est sans facteur carré et vérifie $-d \equiv 3\,[4]$ et $d > 1$, l'anneau des entiers de $\mathbf{Q}\left[i\sqrt{d}\right]$ (à savoir $\mathbf{Z}\left[i\sqrt{d}\right]$) n'est pas un anneau factoriel (chercher deux décompositions de $1 + d$, et montrer que 2 est irréductible dans $\mathbf{Z}\left[i\sqrt{d}\right]$).

Exercice 3
Soit m et n des entiers, avec n impair et $n \geqslant 3$, et $n = p_1 \ldots . p_r$ la décomposition de n en facteurs premiers. Le *symbole de Jacobi* $\left(\frac{m}{n}\right)$ est défini par

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right).$$

En particulier si n est premier $\left(\frac{m}{n}\right)$ coïncide avec le symbole de Legendre ce qui justifie la notation.

1. Vérifier que $\left(\frac{m}{n}\right)$ vaut ± 1 si m et n sont premiers entre eux et 0 sinon.
2. Montrer que pour tout entier n impair supérieur à 3, on a

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

et

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

3. Si m et n sont impairs et au moins égaux à 3, montrer qu'on a

$$\left(\frac{m}{n}\right) = (-1)^{\frac{(n-1)(m-1)}{4}} \left(\frac{n}{m}\right).$$

4. En déduire un nouvel algorithme de calcul du symbole de Legendre.

5. Trouver des entiers n et m tels que $\left(\frac{m}{n}\right) = 1$ et m n'est pas un carré dans $(\mathbf{Z}/n\mathbf{Z})^*$.

Exercice 4
Calculer les symboles de Legendre suivant :

$$\left(\frac{19}{229}\right), \left(\frac{2}{229}\right), \left(\frac{28}{229}\right), \left(\frac{51}{229}\right)$$

1. en utilisant l'algorithme vu en cours

2. en utilisant le symbole de Jacobi, étudié à l'exercice 3.

Exercice 5
Montrer qu'un nombre premier p supérieur à 5 est congru à 1 modulo 3 si et seulement si -3 est un carré dans $\mathbf{F}_p$:

1. en utilisant la loi de réciprocité quadratique

2. en démontrant les équivalences (pour p premier supérieur à 5)

$$\begin{aligned} & p \equiv 1 \quad [3] \\ \iff & \mathbf{F}_p \text{ contient une racine primitive cubique de l'unité} \\ \iff & X^2 + X + 1 \text{ a une racine dans } \mathbf{F}_p \\ \iff & -3 \text{ est un carré dans dans } \mathbf{F}_p. \end{aligned}$$

Exercice 6

1. Soit n un entier. Montrer que tout facteur premier distinct de 3 de n^2+n+1 est congru à 1 modulo 3 (cf. l'exercice 5).

2. Soit $p_1, \ldots, p_r$ des nombres premiers congrus à 1 modulo 3. Que peut-on dire des facteurs premiers de

$$(3.p_1 \ldots p_r)^2 + 3.p_1 \ldots p_r + 1 \quad ?$$

En déduire qu'il y a une infinité de nombres premiers congrus à 1 modulo 3.

3. (une généralisation) Soit q un nombre premier impair. Montrer les équivalences, pour p premier distinct de q,

$$\begin{aligned} & p \equiv 1 \quad [q] \\ \iff \quad & \mathbf{F}_p \text{ contient une racine primitive } q\text{-ème de l'unité} \\ \iff \quad & \text{le polynôme } \frac{X^q-1}{X-1} = X^{q-1}+X^{q-2}+\cdots+1 \\ & \text{a une racine dans } \mathbf{F}_p. \end{aligned}$$

S'inspirant du cas $q=3$, en déduire qu'il y a une infinité de nombres premiers congrus à 1 modulo q.

Exercice 7

Déterminer les irréductibles de $\mathbf{Z}[j]$. On rappelle que $\mathbf{Z}[j]$ est factoriel. On pourra commencer par déterminer les nombres premiers p qui sont irréductibles dans $\mathbf{Z}[j]$.

Exercice 8

Déterminer les nombres premiers p irréductibles dans $\mathbf{Z}\left[\frac{1+i\sqrt{7}}{2}\right]$. Même question avec $\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$. On utilisera le fait que ces anneaux sont factoriels. On exprimera le résultat sous forme de congruence.

Exercice 9

Déterminer les nombres premiers p tels que l'équation

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

ait une solution dans $\mathbf{Z}^2$ (montrer que l'existence d'une solution équivaut au fait que p n'est pas irréductibles dans $\mathbf{Z}\left[i\sqrt{2}\right]$, et utiliser le fait que $\mathbf{Z}\left[i\sqrt{2}\right]$

est factoriel et la réciprocité quadratique pour caractériser de tels p).

Exercice 10
Montrer que l'anneau des entiers du corps quadratique imaginaire $\mathbf{Q}\left[i\sqrt{d}\right]$ est euclidien si d est dans l'ensemble $\{1, 2, 3, 7, 11\}$.

Montrer que si $d > 0$ est sans facteur carré et n'est pas dans cet ensemble, la norme $\alpha \mapsto \alpha\,\overline{\alpha}$ n'est pas un stathme euclidien sur l'anneau des entiers de $\mathbf{Q}\left[i\sqrt{d}\right]$.

Exercice 11
Montrer que si $d \neq d'$ sont deux entiers strictement positifs sans facteur carré, les corps $\mathbf{Q}\left[\sqrt{d}\right]$, $\mathbf{Q}\left[\sqrt{d'}\right]$, $\mathbf{Q}\left[i\sqrt{d}\right]$ et $\mathbf{Q}\left[i\sqrt{d'}\right]$ sont deux à deux non isomorphes.

Exercice 12
Montrer directement (i.e. sans utiliser le fait que l'ensemble des entiers algébriques est un anneau) que $\sqrt{2} + \sqrt{3}$ est un entier algébrique. Même question avec $\sqrt{2} + \sqrt[3]{3}$.

Exercice 13
Soit σ l'automorphisme non trivial du corps $\mathbf{Q}\left[\sqrt{2}\right]$, i.e. $\sigma\left(a + b\sqrt{2}\right) = a - b\sqrt{2}$ pour tous a, $b \in \mathbf{Q}$. Montrer que la fonction $\alpha \mapsto |\alpha\,\sigma(\alpha)|$ définit un stathme euclidien sur l'anneau des entiers de $\mathbf{Q}\left[\sqrt{2}\right]$.

Plus généralement, soit $d > 2$ sans facteur carré et σ l'automorphisme non trivial de $\mathbf{Q}\left[\sqrt{d}\right]$, i.e. $\sigma\left(a + b\sqrt{d}\right) = a - b\sqrt{d}$ pour tous a, $b \in \mathbf{Q}$. Pour quelles valeurs de d la fonction $\alpha \mapsto |\alpha\,\sigma(\alpha)|$ définit-elle un stathme euclidien sur l'anneau des entiers de $\mathbf{Q}\left[\sqrt{d}\right]$?

Exercice 14
Soit x un réel tel que $\tan(2\,\pi\,x)$ soit un rationnel distinct de 0, -1 et 1. Montrer que x est irrationnel (on pourra montrer que $e^{i\,4\,\pi\,x}$ est dans $\mathbf{Q}[i]$ et que, si x est rationnel, c'est en outre un entier algébrique ; qu'en déduire sur les valeurs de $\cos(4\,\pi\,x)$ et $\sin(4\,\pi\,x)$?).

Exercice 15
Soit A un anneau intégralement clos et K son corps des fractions. Soit f un polynôme unitaire à coefficients dans A. Montrer que si f est irréductible dans $A[X]$ alors f est irréductible dans $K[X]$ (considérer les racines de f dans une extension de K). La réciproque est-elle vraie ? Que se passe-t-il si

A n'est pas intégralement clos ?

Exercice 16
Montrer que $\mathbf{Z}\left[\sqrt{3}\right]$ est l'anneau des entiers de $\mathbf{Q}\left[\sqrt{3}\right]$, que $\mathbf{Z}\left[\sqrt{7}\right]$ est l'anneau des entiers de $\mathbf{Q}\left[\sqrt{7}\right]$, mais que $\mathbf{Z}\left[\sqrt{3},\sqrt{7}\right]$ n'est pas l'anneau des entiers de $\mathbf{Q}\left[\sqrt{3},\sqrt{7}\right]$ (regarder $\frac{\sqrt{3}+\sqrt{7}}{2}$).

Exercice 17
Soient B un anneau, A un sous-anneau de B et x un élément inversible de B. Montrer que tout élément y de $A[x] \cap A\left[x^{-1}\right]$ est entier sur A (montrer qu'il existe n tel que $A+A\,x+\cdots+A\,x^n$ soit stable par multiplication par y).

Exercice 18
Soit x un élément d'un corps de nombres K tel que $\mathrm{N}_{K/\mathbf{Q}}x = \pm 1$. Est-il vrai que x est un élément inversible de l'anneau des entiers de K ? On pourra par exemple examiner la situation où $K = \mathbf{Q}[i]$.

Exercice 19
On considère le corps de nombres $K = \mathbf{Q}\left[\sqrt{7},\sqrt{10}\right]$ et $\mathcal{O}_K$ son anneau des entiers. Le but de cet exercice est de montrer qu'il n'existe pas d'entier algébrique α dans K qui vérifie $\mathbf{Z}[\alpha] = \mathcal{O}_K$ (contrairement à ce qui se passe pour les anneaux d'entiers des extensions quadratiques de $\mathbf{Q}$).

1. On considère les éléments de $\mathcal{O}_K$

$$\begin{aligned}\alpha_1 &= (1+\sqrt{7})\,(1+\sqrt{10}),\\ \alpha_2 &= (1+\sqrt{7})\,(1-\sqrt{10}),\\ \alpha_3 &= (1-\sqrt{7})\,(1+\sqrt{10}),\\ \alpha_4 &= (1-\sqrt{7})\,(1-\sqrt{10}).\end{aligned}$$

   Montrer que pour $i \neq j$ le produit $\alpha_i\,\alpha_j$ est divisible par 3 dans $\mathcal{O}_K$.

2. Soit $i \in \{1,2,3,4\}$ et $n \geqslant 0$ un entier. Montrer que

$$\mathrm{Tr}_{K/\mathbf{Q}}(\alpha_i^n) = \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n.$$

   En utilisant la question précédente, montrer que $\alpha_1^n+\alpha_2^n+\alpha_3^n+\alpha_4^n$ est congru à $(\alpha_1+\alpha_2+\alpha_3+\alpha_4)^n$ modulo 3 dans $\mathcal{O}_K$.

   Déduire de ce qui précède que $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha_i^n)$ est congru à 1 modulo 3 dans $\mathbf{Z}$, puis que 3 ne divise pas α_i^n dans $\mathcal{O}_K$.

3. Soit α un entier algébrique de K. On suppose qu'on a $\mathbf{Z}[\alpha] = \mathcal{O}_K$. Soit f le polynôme minimal de α sur $\mathbf{Q}$. Pour tout polynôme g de $\mathbf{Z}[X]$

on note $\overline{g}$ sa réduction modulo 3. Montrer que $g(\alpha)$ est divisible par 3 dans $\mathbf{Z}[\alpha]$ si et seulement si $\overline{f}$ divise $\overline{g}$ dans $\mathbf{F}_3[X]$.

4. Pour $1 \leqslant i \leqslant 4$ soit f_i un élément de $\mathbf{Z}[X]$ tel que $\alpha_i = f_i(\alpha)$. Montrer que pour tout i, $\overline{f}$ a un facteur irréductible ne divisant pas $\overline{f_i}$ mais divisant $\overline{f_j}$ pour tout $j \neq i$.

5. En considérant le nombre de facteurs irréductibles de $\overline{f}$ sur $\mathbf{F}_3$, aboutir à une contradiction.

Exercice 20
Dans $\mathbf{Z}\left[i\sqrt{3}\right]$ on considère l'idéal $\mathfrak{a}$ engendré par 2 et $1+i\sqrt{3}$. Montrer que $\mathfrak{a}$ est distinct de (2) et que $\mathfrak{a}^2 = (2)\,\mathfrak{a}$. En déduire que les idéaux de $\mathbf{Z}\left[i\sqrt{3}\right]$ ne se factorisent pas de manière unique en produit d'idéaux premiers. Montrer que $\mathfrak{a}$ est l'unique idéal premier contenant 2. En déduire que (2) ne s'écrit pas comme un produit d'idéaux premiers.

Exercice 21
Le but de cet exercice est d'étudier un peu la décomposition des idéaux dans l'anneau $\mathbf{Z}\left[i\sqrt{5}\right]$, pour expliquer notamment les différentes factorisations non équivalentes de 6 dans cet anneau. On note $A = \mathbf{Z}\left[i\sqrt{5}\right]$.

1. Soit p un nombre premier. Montrer que $A/p\,A$ est isomorphe soit à $\mathbf{F}_{p^2}$, soit à $\mathbf{F}_p \times \mathbf{F}_p$, soit à $\mathbf{F}_p[t]/(t^2)$, et déterminer pour quels premiers p chacun des cas se produit.

2. En considérant $A/2\,A$, montrer que $\mathfrak{m}_2 = (2, 1+i\sqrt{5})$ est l'unique idéal maximal de A contenant $2\,A$. Montrer que $\mathfrak{m}_2^2 = 2\,A$.

3. Montrer que les idéaux maximaux de A contenant $3\,A$ sont $\mathfrak{m}_3 = (3, 1+i\sqrt{5})$ et $\overline{\mathfrak{m}_3} = (3, 1-i\sqrt{5})$. Montrer que $3\,A = \mathfrak{m}_3\,\overline{\mathfrak{m}_3}$.

4. En déduire la décomposition de $6\,A$ en produit d'idéaux maximaux de A. Montrer que $\mathfrak{m}_2$, $\mathfrak{m}_3$, $\overline{\mathfrak{m}_3}$ ne sont pas principaux mais que $\mathfrak{m}_2\,\mathfrak{m}_3$ et $\mathfrak{m}_2\,\overline{\mathfrak{m}_3}$ le sont, ainsi que $\mathfrak{m}_2^2$ et $\mathfrak{m}_3\,\overline{\mathfrak{m}_3}$ (et $\mathfrak{m}_3^2$). Ceci explique les différentes factorisations de 6.

5. Calculer des $\mathbf{Z}$-bases de tous les idéaux maximaux de A contenant un premier p avec $p \leqslant 19$. Déterminer lesquels sont principaux, et montrer, en calculant au cas par cas, que si deux d'entre eux ne sont pas principaux, leur produit est principal.