Partiel du 30 octobre 2014

Exercice 1 (Questions de cours)**.** Soit A un anneau factoriel, et soit $f \in A[X] \setminus \{0\}$. Rappeler la définition du contenu $c(f)$, et montrer que $c(fg) = c(f).c(g)$ modulo unités.

Corrigé. On peut montrer que si f et g sont primitifs alors fg l'est aussi. On écrit :

$$f = \sum_{i=0}^{n} a_i X^i, \qquad g = \sum_{j=0}^{m} b_j X^j.$$

Soit p un premier de A et posons :

$$r = \max\{i \in \mathbb{N} \mid p \nmid a_i\},$$
$$s = \max\{j \in \mathbb{N} \mid p \nmid b_j\}.$$

Ces ensembles d'entiers ne sont pas vides car $c(f) = c(g) = 1$. Donc $i > r$ implique $p \mid a_i$ et $j > s$ implique $p \mid a_j$. Écrivons le produit fg :

$$fg = \sum_{k=0}^{n+m} c_k X^k = \sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_j X^k.$$

Alors on regarde c_{r+s}, soit :

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j.$$

On voit que $i > r$ si et seulement si $j \leq s$. Ainsi :

$$i > r \Rightarrow p \mid a_i b_j, \qquad i < r \Rightarrow j > s \Rightarrow p \mid a_i b_j.$$

Par contre si $i = r$ alors $j = s$ ainsi $p \nmid a_i b_j$. Donc p divise tous les coefficients sauf un de la somme définissant c_{r+s}, ce qui signifie que $p \nmid c_{r+s}$. Comme ce raisonnement peut être répété pour n'importe quel premier, nous avons que fg est primitif.

Exercice 2. Les anneaux sont commutatifs avec unité.

1. Montrer que ni $\mathbb{Z}[X]$ ni $\mathbb{Q}[X,Y]$ ne sont principaux.
2. Dire lesquels parmi les anneaux suivants sont intègres, principaux.
   (a) L'anneau $\mathbb{Z}/n\mathbb{Z}[X]$ selon le choix de $n \in \mathbb{N}$.
   (b) L'anneau $\mathbb{C}(Y)[X]$ des polynômes en X à coefficients dans le corps $\mathbb{C}(Y)$ des fractions polynomiales en Y à coefficients complexes.
   (c) L'anneau $A(\mathbb{R}^n, \mathbb{R})$ des fonctions polynomiales en n variables à valeurs dans $\mathbb{R}$, selon la valeur de n.

Corrigé.

1. Montré en classe : $(2,X)$ et (X,Y) ne sont pas principaux.
2. Facile :
   (a) Si n premier alors $\mathbb{Z}/n\mathbb{Z}$ est un corps ainsi cet anneau est intègre et principal. Si n n'est pas premier cet anneau n'est évidemment pas intègre.
   (b) C'est un anneau de polynômes sur un corps.

(c) Les fonctions polynomiales en n variables sur un corps infini peuvent être identifiées aux polynômes en n variables, d'après un exercice traité en classe. Donc cet anneau est toujours intègre. Il est principal si et seulement si $n = 1$.

Exercice 3. Soit $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

1. Lister les polynômes de $R = \mathbb{F}_2[X]$ de degré au plus 2.
2. Écrire tous les polynômes irréductibles de degré 2 et 3 de $\mathbb{F}_2[X]$.
3. Montrer que $F = X^4 + X^3 + 1$ est irréductible sur $\mathbb{F}_2[X]$ puis sur $\mathbb{Q}[X]$. Que pouvez-vous dire de $\mathbb{F}_2[X]/(F)$?
4. Soit $P = X^5 + X^3 + X + 1$ et $Q = X^4 + X^3 + X + 1$ dans $\mathbb{F}_2[X]$. Trouver $U, V \in \mathbb{F}_2[X]$ tels que $UP + VQ = (X + 1)$.

Corrigé. On néglige d'écrire des classes dans $\mathbb{F}_2$. Posons $A = \mathbb{F}_2[X]$.

1. Éléments de $\mathbb{F}_2 = \{0, 1\}$.

$$\begin{array}{llllll} A_0 : & 0, & 1, & & & \\ A_1 : & X, & X+1, & & & \\ A_2 : & X^2, & X^2+X, & X^2+X+1, & X^2+1. & \end{array}$$

2. On a vu en classe que les polynômes de degré 2 et 3 sont irréductibles si et seulement si ils n'ont pas de racine. En faisant le test avec 0 et 1, on voit que les polynômes suivants sont irréductibles dans $\mathbb{F}_2$ (et donc dans $\mathbb{Q}$ d'après le théorème de réduction modulo p) :

$$\begin{array}{lll} A_2 : & X^2+X+1, & \\ A_3 : & X^3+X^2+1, & X^3+X+1, \end{array}$$

   Tous les autres polynômes de degré jusqu'à 3 ont des racines dans $\mathbb{F}_2$.

3. Ces polynômes n'ont pas de racine sur $\mathbb{F}_2$. De plus, ils ne sont divisibles par aucun polynôme de degré 2 ou 3, comme on peut voir en faisant la division par les polynômes trouvés lors de la question précédente. Ils sont donc irréductibles. Comme on est dans un anneau principal, le quotient par un idéal premier est un corps.
4. On a les décompositions éléments irréductibles :

$$P = (X+1)(X^4+X^3+1),$$
$$Q = (X+1)^2(X^2+X+1).$$

   Ces décompositions peuvent être trouvées en cherchant les racines sur $\mathbb{F}_2$ de P et de Q. Les facteurs sont bien irréductibles d'après les questions précédentes. D'après Bézout, on a alors U, V tels que :

$$UP + VQ = \text{pgcd}(P, Q) = X + 1.$$

   Par conséquent, on a évidemment U, V tels que :

$$UP + VQ = (X+1)^n,$$

   quelque soit $n \geq 1$.

   Pour trouver U et V du cas $n = 1$, on applique Euclide étendu. On commence par $R_0 = P$ et $R_1 = Q$, puis :

$$R_0 = R_1 T_1 + R_2, \qquad R_2 = X^2 + X, \qquad T_1 = X + 1.$$

   Ensuite :

$$R_1 = R_2 T_2 + R_3, \qquad R_3 = X + 1, \qquad T_2 = X^2.$$

Donc :

$$X+1 = R_1 - R_2T_2 = R_1 - (R_0 - R_1T_1)T_2 = -T_2R_0 + (1+T_1T_2)R_1.$$

Ainsi :

$$U = -X^2, \qquad V = X^3 + X^2 + 1.$$

Exercice 4. Soit $A = \mathbb{Z}[i]$ et notons $x+iy$, avec $x,y \in \mathbb{Z}$ un élément de A. Posons :

$$N(x+iy) = x^2 + y^2.$$

1. Montrer que, pour tout $a,b \in A$, on a $N(ab) = N(a)N(b)$. En déduire la liste des éléments inversibles de A.
2. Montrer que ni 2 ni 5 ne sont irréductibles dans A. Est-ce que 3 l'est ?
3. Soit p un nombre premier. Montrer l'équivalence des conditions suivantes :
   (a) p n'est pas irréductible dans A ;
   (b) il existe $a \in A$ tel que $N(a) = p$;
   (c) il existe $x,y \in \mathbb{Z}$ tel que $p = x^2 + y^2$;

4*. Soit $a \in A$ et $b \in A \setminus \{0\}$. Posons $\frac{a}{b} = \alpha + i\beta \in \mathbb{C}$. Montrer que, si on définit le quotient q de a par b comme $x+iy$ avec x,y les entiers plus proches de α,β alors $r = a - bq$ satisfait $r = 0$ ou $N(r) < N(b)$. En déduire que A est euclidien.

Corrigé 1. On a $A \subset \mathbb{C}$ donc A intègre.

1. C'est vrai que N est multiplicatif dans $\mathbb{C}$ donc aussi dans A. Alors a inversible implique $N(a) = 1$ donc $a = \pm 1$ ou $a = \pm i$.
2. On a $2 = (1+i)(1-i)$ et ni $1+i$ ni $1-i$ ne sont inversibles. De même $5 = (2+i)(2-i)$ et ni $2+i$ ni $2-i$ ne sont inversibles. On en déduit qu'un élément $a \in A$ est inversible si et seulement si $N(a) = 1$.

   En revanche 3 est irréductible. Sinon, $3 = ab$ implique $9 = N(a)N(b)$ donc $N(a) = N(b) = 3$ ou alors a ou b ont norme 1 donc sont inversibles. Mais si $a = x+iy$ a norme 3 alors $x^2 + y^2 = 3$ ce qui est visiblement impossible.
3. Soit p un nombre premier.

(a) $\Rightarrow$ (b) Si p n'est pas irréductible dans A alors p s'exprime comme un produit, plus précisément (p étant réel) le produit d'un nombre et de son conjugué : $p = (x+iy)(x-iy)$. Soit $a = x+iy$. On a alors $p^2 = N(a)N(\bar{a})$, ce qui implique $N(a) = p$ puisque $N(a) \neq 1$, sans quoi a serait inversible.

(b) $\Rightarrow$ (c) Soit $a \in A$ tel que $N(a) = p$, donc $a = x+iy$. On a $p = N(a) = x^2 + y^2$.

(b) $\Rightarrow$ (c) Soit $x,y \in \mathbb{Z}$ tel que $p = x^2 + y^2$. Alors on peut écrire $p = (x+iy)(x-iy)$. Si $a = x+iy$ est inversible, alors $a = \pm 1$ ou $a = \pm i$, ce qui veut dire $p = 1$, auquel cas p n'est pas premier.

4*. Énoncé de la question : « Soit $a \in A$ et $b \in A \setminus \{0\}$. Posons $\frac{a}{b} = \alpha + i\beta \in \mathbb{C}$. Montrer que, si on définit le quotient q de a par b comme $x+iy$ avec x,y les entiers plus proches de α,β alors $r = a - bq$ satisfait $r = 0$ ou $N(r) < N(b)$. En déduire que A est euclidien. »

Réponse. Choisissons un entier de Gauss q tel que :

$$N\left(\frac{a}{b} - q\right) \leq \frac{1}{2} < 1.$$

Ceci est vérifié par n'importe quel q tel que :

$$\begin{cases} |\Re\frac{a}{b} - \Re q| \leq \frac{1}{2}, \\ |\Im\frac{a}{b} - \Im q| \leq \frac{1}{2}, \end{cases}$$

En effet :

$$N\left(\frac{a}{b}-q\right)=(\Re\frac{a}{b}-\Re q)^2+(\Im\frac{a}{b}-\Im q)^2\leq\frac{1}{4}+\frac{1}{4}=\frac{1}{2}.$$

Pose alors :

$$r=a-bq=b\left(\frac{a}{b}-q\right).$$

Il est clair que :

$$N(r)=N(b)N\left(\frac{a}{b}-q\right)<N(b).$$

Ceci permet de définit la division euclidienne et de prouver que A est euclidien donc principal. On remarquera que, dans cette division, quotient et reste ne sont pas toujours uniques. Cependant, pour montrer que A est euclidien, on n'a pas besoin de cette unicité.