U.P.S. 2010-2011, L3 Maths Fonda Algèbre, feuille 7
Anneaux euclidiens, principaux, factoriels

Exercice 1.

a) Soient A un anneau, I un idéal de A et π la projection canonique $A \to A/I$. Montrer que les idéaux premiers de A/I sont en bijection avec les idéaux premiers de A contenant I.

b) Quels sont les idéaux premiers de $\mathbf{R}[X]/(X^2+X+1)$?

Exercice 2. Soit A un anneau intègre.

a) Montrer que les éléments inversibles de $A[X]$ sont les inversibles de A.

b) Montrer que tout élément irréductible de A est un élément irréductible de $A[X]$.

c) Trouver un élément inversible de $(\mathbf{Z}/4\mathbf{Z})[X]$ de degré non nul.

Exercice 3. Soient A un anneau commutatif unitaire intgre, s un élément non nul de A, et A_s le sous-anneau du corps des fractions de A formé des éléments de la forme $\frac{a}{s^n}$ avec $a \in A$ et $n \in \mathbf{N}$.

a) Montrer que si A est factoriel alors A_s aussi.

b) Montrer que si A est euclidien alors A_s aussi.

Exercice 4.

a) Montrer que $\mathbf{Z}[i]$ est euclidien et factoriel.

b) Expliquer pourquoi les égalités $(2+i)(2-i) = 5 = (-1-2i)(-1+2i)$ ne mettent pas en défaut la factorialité de $\mathbf{Z}[i]$.

c) Calculer le pgcd de $1-13i$ et de $4+i$ et celui de $1+7i$ et de $-8-i$.

Exercice 5. *Le théorème des deux carrés.* Dans cet exercice, on considère p un nombre premier et on note $\Sigma = \{a^2+b^2, a, b \in \mathbf{N}\}$. On sait maintenant que $\mathbf{Z}[i]$ est un anneau euclidien.

a) Montrer l'équivalence suivante :

$$p \in \Sigma \Leftrightarrow p \text{ n'est pas irréductible dans } \mathbf{Z}[i].$$

b) En déduire que

$$p \in \Sigma \Leftrightarrow p = 2 \text{ ou } p \cong 1 \bmod 4.$$

(Indication : on remarquera que $\mathbf{Z}[i]/p\mathbf{Z}[i]$ *est isomorphe à* $(\mathbf{Z}/p\mathbf{Z})[X]/(X^2+1)$*.)*

c) Soit $n \in \mathbf{N}$ et $n = \Pi p^{v_p(n)}$ sa décomposition en facteurs premiers. Montrer que :

$$n \in \Sigma \Leftrightarrow v_p(n) \text{ pair pour } p \equiv 3 \bmod 4$$

d) Déterminer les irréductibles de $\mathbf{Z}[i]$.

Exercice 6.

a) Montrer que $\mathbf{Z}[X,Y]$ est un anneau factoriel.

b) Montrer que X^2+Y^2+1 est irréductible dans $\mathbf{Z}[X,Y]$.

c) Calculer le pgcd de $X^3Y^2+XY^4+XY^2$ et de $X^3+X^2+XY^2+Y^2+X+1$.

Exercice 7.

a) Montrer que pour tout nombre premier p, le polynôme $X^p + p$ est irréductible dans $\mathbf{Z}[X]$.

b) Montrer que $3X^4 + 10X + 15$ est irréductible dans $\mathbf{Z}[X]$ mais pas dans $\mathbf{R}[X]$.

c) Montrer que $X^2 + X + 2$ est irréductible dans $\mathbf{Z}[X]$ en faisant un changement de variable simple (une translation).

Exercice 8. Dans l'anneau $\mathbf{Z}[\sqrt{10}]$, montrer que 2 est irréductible, mais pas premier.

Exercice 9. Dans l'anneau $\mathbf{Z}[i\sqrt{5}]$, montrer que 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.

Exercice 10. Soit A un anneau commutatif intègre dans lequel tout élément non nul est produit d'irréductibles et toute paire d'éléments non nuls a un ppcm.

a) Montrer que toute paire d'éléments non nuls a aussi un pgcd et que $ab = \text{ppcm}(a, b) \times \text{pgcd}(a, b)$.

b) Montrer que $(a) \cap (b) = (\text{ppcm}(a, b))$.

c) Montrer que A vérifie le lemme d'Euclide, donc que A est factoriel.

Exercice 11. Soit A un anneau factoriel vérifiant le théorème de Bézout (i.e. pour tous $a, b \in A$, l'idéal (a, b) est principal). Montrer que A est principal.

Exercice 12. Soient K un corps, P un polynôme de degré p, Q un polynôme de degré q. On considère l'application :

$$R_{P,Q} : K_{q-1}[X] \times K_{p-1}[X] \to K_{p+q-1}[X],\ (A, B) \mapsto AP + BQ\ .$$

On appelle $Res(P, Q)$ le déterminant de $R_{P,Q}$.

a) Que peut-on dire de P et de Q lorsque $Res(P, Q) = 0$?

b) On appelle nombre algébrique tout nombre complexe qui est la racine d'un polynôme à coefficients dans $\mathbf{Q}$. Montrer que si α et β sont deux nombres algébriques alors leur somme $\gamma = \alpha + \beta$ l'est aussi en déterminant un polynôme qui s'annule en γ. *(Indication : Il faut ici considérer le résultant prenant en argument les polynômes $P(X)$ et $Q(\gamma - X)$ où P et Q sont les polynômes à coefficients rationnels qui vérifient $P(\alpha) = 0$ et $Q(\beta) = 0$.)*