U.P.S. 2010-2011, L3 Maths Fonda Algèbre, corrigé de la 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 $\mathbf{R}[X]/(X^2+X+1)$?*
a) cf Feuille 6 exercices 5 et 10.a (qui devient une équivalence si f est surjective). b) C'est un corps, donc son seul idéal propre est $\{0\}$, qui est premier.

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.*

a) Tout inversible de A est un inversible de $A[X]$. Réciproquement, si $PQ = 1$ alors, comme le degré du produit est égal à la somme des degrés (parce que A est intègre) $P, Q \in A$ donc P, Q sont des inversibles de A.

b) Si $a = PQ$ avec a irréductible de A alors $a \neq 0$ et (à nouveau par un raisonnement sur les degrés) $P, Q \in A$, donc l'un des deux facteurs est un inversible de A (donc de $A[X]$) et l'autre est un élément de A non inversible dans A (donc non inversible dans $A[X]$ d'après a)).

c) $2X + 1$ est son propre inverse.

Exercice 3. *Soient A un anneau commutatif unitaire intègre, 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.*

a) Si A est factoriel alors, dans A_s, tout élément est (à association près) produit d'irréductibles de A ne divisant pas s, et de tels éléments sont premiers dans A_s.

b) Si v est une valuation euclidienne sur A, définissons v' sur A_s par $v'(x) = v(a_x)$ où a_x est, parmi les éléments de A associés dans A_s à x, un élément premier à s. Soient $x, y \in A$ avec $y \neq 0$. Si x divise y dans A_s alors il existe n tel que a_x divise $a_y s^n$ dans A, donc (puisque a_x est premier à s) a_x divise a_y, d'où $v'(x) = v(a_x) \leq v(a_y) = v'(y)$. Sinon, soit $a_x = a_y q + r$ une division euclidienne de a_x par a_y dans A avec $v(r) < v(a_y)$, alors il existe u, v éléments inversibles de A_s tels que $x = yqu + rv$, et $v'(rv) = v'(r) \leq v(r) < v(a_y) = v'(y)$.

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 $-8-i$.*

a) Montrons que $\mathbf{Z}[i]$ est euclidien (ce qui impliquera qu'il est principal, donc factoriel). Pour tous $a, b \in \mathbf{Z}$ (ou même $\in \mathbf{Q}$) posons $N(a+ib) = a^2 + b^2$: N définit clairement une valuation sur $\mathbf{Z}[i]$, c'est-à-dire une application de $\mathbf{Z}[i] \setminus \{0\}$ dans $\mathbf{N}$ qui vérifie $u|v \Rightarrow N(u) \leq N(v)$ (en fait elle vérifie même $N(uw) = N(u)N(w)$. De plus cette valuation est euclidienne, c'est-à-dire $\forall u, v \in \mathbf{Z}[i]$ tels que $v \neq 0$, il existe $q \in \mathbf{Z}[i]$ tel que $u - qv$ soit nul ou de valuation strictement inférieure à celle de v. En effet (par multiplicativité de N) il suffit pour cela que $N(\frac{u}{v} - q) < 1$, ce qui s'obtient en notant x, y les rationnels tels que $\frac{u}{v} = x + iy$ et en posant $q = a + ib$ avec $a, b \in \mathbf{Z}$ choisis tels que $|x - a|, |y - b| \leq 1$.

b) Remarquons d'abord que $2 + i$ est premier dans $\mathbf{Z}[i]$, puisque $uv = 2 + i \Rightarrow N(u)N(v) = 5 \Rightarrow N(u)$ ou $N(v) = 1 \Rightarrow u$ ou v est inversible. De même, $2 - i$, $-1 - 2i$ et $-1 + 2i$ sont premiers. On a donc apparemment deux décompositions distinctes de 5 en facteurs premiers dans $\mathbf{Z}[i]$,

ce qui ne contredit pas la factorialité, car ces deux décompositions sont en fait égales, à l'ordre près des facteurs et à leur produit près par des inversibles.

c) Appliquons l'algorithme d'Euclide. $\frac{1-13i}{4+i} = \frac{(1-13i)(4-i)}{17} = \frac{-9-53i}{17}$ est approximé dans $\mathbf{Z}[i]$ par $-1-3i$, et $(1-13i)-(4+i)(-1-3i) = 2$. Puis $\frac{4+i}{2}$ est approximé (par exemple) par 2, et $(4+i)-2.2 = i \in \mathbf{Z}[i]$, inversible. Donc dans $\mathbf{Z}[i]$, $1-3i$ et $4+i$ sont premiers entre eux et "le" pgcd est 1 (ou n'importe quel autre inversible : $-1, i, -i$). Même méthode pour $1+7i$ et $-8-i$: $\frac{-8-i}{1+7i} = \frac{-3+11i}{10} \simeq i$, $(-8-i)-i(1+7i) = -1-2i$, $\frac{1+7i}{-1-2i} = -3-i \in \mathbf{Z}[i]$ donc "le" pgcd (au produit près par les inversibles $\pm 1, \pm i$) est $-3-i$.

Exercice 5. *Soient p un nombre premier et $\Sigma = \{a^2+b^2 \mid a, b \in \mathbf{N}\}$.*

a) *Montrer l'équivalence suivante :*

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

b) *En déduire que*

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

(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 $\mathbf{Z}[i]$.*

a) Si $p \in \Sigma$ alors il existe $z \in \mathbf{Z}[i]$ tel que $p = N(z) = z\overline{z}$, donc p est produit de deux éléments z et $\overline{z}$, qui sont non inversibles puisque leur norme est différente de 1, donc p est réductible. Réciproquement, si $p = uv$ avec u et v non inversibles alors $p^2 = N(u)N(v)$ avec $N(u)$ et $N(v)$ entiers différents de 1, donc $p = N(u) \in \Sigma$.

b) Compte tenu de la question a) et de l'indication (justifiée par le fait que ces deux quotients sont isomorphes à $\mathbf{Z}[X]/(p, X^2+1)$, cf feuille 6 exercice 6), et compte tenu du fait que dans $\mathbf{Z}[i]$ et $(\mathbf{Z}/p\mathbf{Z})[X]$ (euclidiens donc factoriels) tout irréductible est premier, $p \in \Sigma$ ssi p est non premier dans $\mathbf{Z}[i]$, donc ssi X^2+1 est non premier dans $(\mathbf{Z}/p\mathbf{Z})[X]$, donc ssi X^2+1 est réductible dans $(\mathbf{Z}/p\mathbf{Z})[X]$, i.e. ss'il existe dans $\mathbf{Z}/p\mathbf{Z}$ une racine carrée de -1. Pour $p = 2$ c'est vrai. Pour $p \neq 2$, comme -1 est le seul élément d'ordre 2, cela équivaut à : il existe dans le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ un élément d'ordre 4. Si c'est vrai alors 4 divise $p-1$. Réciproquement, si 4 divise $p-1$ alors le groupe contient un élément d'ordre 4 parce que ce groupe est cyclique (le groupe multiplicatif de tout corps fini est cyclique).

c) $\Leftarrow$ résulte immédiatement de b). Pour $\Rightarrow$, soient $n \in \Sigma$ et p un diviseur premier de n congru à 3 mod 4. Alors $n = a^2+b^2$ avec a et b entiers, et modulo p, $a^2+b^2 \equiv 0$ donc $a \equiv b \equiv 0$ (car sinon on en déduirait une racine carrée mod p de -1, ce qui est impossible vu le choix de p), donc p^2 divise n et $n/p^2 \in \Sigma$. En itérant on en déduit que $v_p(n)$ est pair.

d) Soit z un irréductible de $\mathbf{Z}[i]$. Comme $\mathbf{Z}[i]$ est factoriel, z est premier. Or z divise $N(z)$, qui se décompose en produit d'éléments premiers de $\mathbf{Z}$, donc z divise l'un de ces facteurs, notons-le p. Il existe donc $m \in \mathbf{N}$ tel que $N(z) = pm$ et $w \in \mathbf{Z}[i]$ tel que $p = zw$, d'où $z\overline{z} = N(z) = pm = zwm$, donc $\overline{z} = wm$, donc $z = \overline{wm}$ donc (par irréductibilité de z) exactement l'un des deux facteurs est inversible, autrement dit : ou bien w est inversible (et alors $z = p$ à cet inversible près) ou bien $m = 1$ (i.e. $N(z) = p$). De plus, d'après b), dans le premier cas p est congru à 3 mod 4, alors que dans le second cas, il ne l'est pas.

Réciproquement, tout entier premier congru à 3 mod 4 est irréductible dans $\mathbf{Z}[i]$, et tout élément de $\mathbf{Z}[i]$ dont la norme est un entier premier (qui, nécessairement, sera alors non congru à 3 mod 4) est irréductible dans $\mathbf{Z}[i]$ (puisque si $N(u)N(v) = N(uv) = p$ premier alors soit $N(u)$ soit $N(v)$ vaut 1).

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 $X^3+X^2+XY^2+Y^2+X+1$.*

a) $\mathbf{Z}$ est (euclidien donc principal donc) factoriel, donc $\mathbf{Z}[X]$ est (non principal mais) factoriel, donc $\mathbf{Z}[X][Y]$ aussi.

b) Vu comme polynme en Y, $Y^2+(X^2+1)$ est irréductible car il est de degré 2 et sans racine dans $\mathbf{Z}[X]$, car il n'existe pas de F dans $\mathbf{Z}[X]$ tel que $F^2 = -X^2-1$. En fait, il n'en existe même pas dans $\mathbf{R}(X)$, pour des raisons de signe de la fonction rationnelle associée. (Ni même dans $\mathbf{C}(X)$, car si $A, B \in \mathbf{C}[X]$ non nuls, les facteurs irréductibels $X+i$ et $X-i$ apparaissent chacune à une puissance impaire dans $-(X^2+1)B^2(X)$ et à une puissance paire dans $A^2(X)$, ce qui exclut que $A/B = -X^2-1$.)

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).*

a) et b) sont des applications directes du critère d'Eisenstein (avec $p = 5$ dans b)). Dans c), remarquons d'abord qu'une translation de la variable est un automorphisme de l'anneau, donc préserve le fait d'être irréductible ou pas. Pour pouvoir appliquer Einsenstein à $(X+n)^2+(X+n)+2 = X^2+(2n+1)X+(n^2+n+2)$ il faut qu'il existe un nombre premier p divisant $2n+1$ et n^2+n+2 (ou ce qui est équivalent : divisant à la fois $2n+1$ et $(n^2+n+2)-2(2n+1) = n(n-3)$, ou encore : tel que p divise à la fois $n-3$ et $2\times 3+1 = 7$), mais dont le carré ne divise pas n^2+n+2. Les solutions possibles sont donc : $p = 7$ et $n \in 7\mathbf{Z}+3$, par exemple $n = 3$.

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

(Ceci prouvera que cet anneau n'est pas factoriel.) Irréductibilité : $2 = uv$ alors $N(u)N(v) = 4$ donc exactement l'un des deux u ou v est inversible, sauf dans l'éventualité où l'on aurait $N(u) = N(v) = 2$, mais ce cas est impossible car pour $a, b \in \mathbf{Z}$, a^2-10b^2 est un carré modulo 5 alors que 2 n'en est pas un. Non primalité : 2 ne divise pas $z := \sqrt{10}$ mais $z^2 = 10 = 2\times 5$, donc 2 divise un produit sans diviser aucun des deux facteurs.

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.*

(Ceci prouvera que cet anneau n'est pas factoriel.) Remarquons d'abord (cela servira pour les deux questions) que pour tout diviseur commun z de 9 et $3(2+i\sqrt{5})$ on a $N(z) = 1$ ou 9. En effet, d'une part 9 et $3(2+i\sqrt{5})$ ont même norme (81) sans être associés (les seuls inversibles de l'anneau étant ± 1) donc $N(z)$ est un diviseur strict de 81 dans $\mathbf{Z}$, d'autre part, mod 5, $N(z)$ est un carré donc est congru à -1, 0 ou 1.

Si 3 et $2+i\sqrt{5}$ avaient un ppcm z, celui-ci diviserait les deux multiples communs 9 et $3(2+i\sqrt{5})$, donc (d'après la remarque préliminaire) $N(z) = 1$ ou 9. Mais 3 et $2+i\sqrt{5}$ ont même norme (9) sans être associés, donc la norme de tout multiple commun doit être un multiple strict de 9 dans $\mathbf{Z}$, ce qui est incompatible avec $N(z) = 1$ ou 9.

Si 9 et $3(2+i\sqrt{5})$ avaient un pgcd z on aurait (d'après la remarque préliminaire) $N(z) = 1$ ou 9. Mais comme 3 et $2+i\sqrt{5}$ sont des diviseurs communs, ils doivent diviser le pgcd z, et même

strictement puisqu'ils ont même norme (9) sans être associés, donc 9 doit diviser strictement $N(z)$ dans $\mathbf{Z}$, ce qui est incompatible avec $N(z) = 1$ ou 9.

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 $ab = \mathrm{ppcm}(a,b) \times \mathrm{pgcd}(a,b)$. b) Montrer que $(a) \cap (b) = (\mathrm{ppcm}(a,b))$. c) Montrer que A vérifie le lemme d'Euclide, donc que A est factoriel.*

a) Soit m un ppcm de a et b, alors il existe $a', b', d \in A$ tels que $m = ab' = ba'$ et $ab = md$, ce qui implique $a = da'$ et $b = db'$. Soit x un diviseur commun de a et b, montrons que x divise d. Il existe $u, v \in A$ tels que $a = xu$ et $b = xv$, d'où $av = bu$ (multiple commun à a et b) est divisible par $m = ba'$, donc u est divisible par a' : $u = a'w$. Alors, $da' = a = xu = xa'w \Rightarrow d = xw$.

b) C'est la traduction exacte, en termes d'idéaux, de la définition du ppcm.

c) Soient p un diviseur irréductible de ab, et $d = pgcd(a,p)$. Alors d divise p qui est irréductible, donc d est soit inversible, soit associé à p. Dans le second cas, p divise a. Dans le premier cas, $ppcm(a,p) = ap$ (d'après la question précédente), donc ap divise ab, donc p divise b. On vient de montrer que tout irréductible est premier, ce qui implique l'unicité de la décomposition en produit d'irréductibles.

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.*
Soient I un idéal non nul de A, et a un élément non nul de I dont le nombre de facteurs (dans la décomposition en produit d'irréductibles) est minimum. Pour tout $x \in I$, soit $(d) = (a,x)$, alors $a \in (d)$ et $d \in I$ donc (par choix de a) d est associé à a, donc a divise x. Par conséquent, $I = (a)$.

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.
Remarquons que les K-e.v. de départ et d'arrivée de l'application (K-linéaire) $R_{P,Q}$ sont de même dimension $p+q$, donc son déterminant a un sens étant donné un choix de bases, et la nullité de ce déterminant ne dépend pas d'un tel choix.

a) Si $Res(P,Q) = 0$ alors $R_{P,Q}$ est non injectif donc son noyau n'est pas réduit à zéro, donc P, Q ne sont pas premiers entre eux. Inversement si $Res(P,Q) \neq 0$ alors $R_{P,Q}$ est surjectif donc $1 \in \mathrm{Im}(R_{P,Q})$ donc P, Q sont premiers entre eux.

b) Si $P(\alpha) = Q(\beta) = 0$ alors $P(X)$ et $Q(\gamma - X)$ ne sont pas premiers entre eux car ils ont α comme racine commune. Donc leur résolvant est nul, ce qui (en développant ce déterminant) fournit une identité polynomiale sur z. (Autre raisonnement, sans utiliser le résolvant : si α, β sont algébriques sur K (ou même si α est algébrique sur K et β algébrique seulement sur $K(\alpha)$) alors le K-e.v. $K[\alpha + \beta]$, étant inclus dans $K[\alpha, \beta]$, est de dimension finie (car ce dernier est un e.v. de dimension finie sur $K(\alpha) = K[\alpha]$, qui lui-même est un K-e.v. de dimension finie). Donc $\alpha + \beta$ est algébrique sur K.)