Polynômes irréductibles: exercices corrigés

Exercice 1. *Soit $A = \mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2} \ / \ (a,b) \in \mathbb{Z}^2\}$. On définit pour $z = a + ib\sqrt{2} \in A$, $N(z) = a^2 + 2b^2$.*

(a) Montrez que A est euclidien et donc factoriel.

(b) Soient $(x,y) \in \mathbb{Z}^2$, vérifiant l'équation $y^2 + 2 = x^3$. Montrez que x est impair puis que dans A, $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux. En déduire qu'il existe $(a,b) \in \mathbb{Z}^2$ tels que $x = a^2 + 2b^2$ et $y + i\sqrt{2} = (a + ib\sqrt{2})^3$, puis décrire les solutions de l'équation précédente.

(c) Etudier comme dans l'exercice 3 de la feuille 1 $S = \{n \in \mathbb{N} \ / \ \exists (x,y) \in \mathbb{Z}^2, \ n = x^2 + 2y^2\}$.
Indication: on utilisera que -2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1, 3 \mod 8$.

(d) Etudier de même l'ensemble $\{n \in \mathbb{Z} \ / \ \exists (x,y) \in \mathbb{Z}^2, \ n = x^2 - 2y^2\}$.

Preuve: (a) On raisonne comme dans l'exercice précédent; soit $N(a + ib\sqrt{2}) = a^2 + 2b^2$ la norme qui est une fonction multiplicative, et soit $z \in A^\times$; on a $zz' = 1$ soit $N(z)N(z') = 1$ et donc $N(z) = 1$, soit $z = \pm 1$.
Pour montrer que A est euclidien, on remarque à nouveau que z_1/z_2 peut s'écrire sous la forme $q + e$ avec $q \in A$ et $e \in \mathbb{C}$ de norme strictement plus petite que 1. Ainsi on a $z_1 = qz_2 + r$, avec $r = z_1 - qz_2 \in A$ et $N(r) < N(z_2)$.

(b) Si x est pair, on a $y^2 \equiv -2 \mod 8$, ce qui ne se peut pas, car les carrés dans $\mathbb{Z}/8\mathbb{Z}$, sont $0, 1, 4$. On factorise ensuite dans A: $x^3 = (y + i\sqrt{2})(y - i\sqrt{2})$ et soit δ un pgcd de $y + i\sqrt{2}$ et $y - i\sqrt{2}$; on a $\delta = (y + i\sqrt{2}, (i\sqrt{2})^3)$, or $i\sqrt{2}$ est irréductible car de norme 2, et la seule factorisation de 2 est 1×2, de sorte que $i\sqrt{2} = zz'$ implique que $N(z) = 1$ soit z inversible (ou z'). Or $i\sqrt{2}$ ne divise pas y car sinon y^2 serait pair et donc y pair soit x pair, ce qui n'est pas; ainsi $\delta = 1$. On en déduit donc que $(y \pm i\sqrt{2})$ sont des cubes parfaits: $(y \pm i\sqrt{2}) = (a \pm i\sqrt{2})^3$ et $x = a^2 + 2b^2$. En séparant partie réelle et imaginaire, on trouve alors $y = a^3 - 6ab^2$ et $1 = b(3a^2 - 2b^2)$ soit $b = \epsilon = \pm 1 = 3a^2 - 2$, ce qui donne $b = 1$ et $a = \pm 1$ soit $y = \pm 5$ et $x = 3$ qui est bien une solution de l'équation.

(c) On a à nouveau $n \in S$ si et seulement si il existe $z \in A$ tel que $n = N(z)$. On étudie à nouveau les irréductibles de B; p est irréductible si et seulement si $A/(p)$ est intègre, i.e. $X^2 + 2$ n'a pas de racine dans $\mathbb{Z}/p\mathbb{Z}$, i.e. si et seulement si -2 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, i.e. si et seulement si $p \equiv 5, 7 \mod 8$. En raisonnant comme dans l'exercice précédent, on trouve que les irréductibles de A, outre les premiers $p \equiv 5, 7 \mod 8$, sont les $z \in A$ tels que $N(z)$ est premier. Toujours en suivant la même démarche, on trouve alors que $n \in S$ si et seulement si $v_p(n)$ est pair pour $p \equiv 5, 7 \mod 8$.

(d) De la même façon, la détermination de S se fait via l'étude de $A = \mathbb{Z}[\sqrt{2}]$, dont la norme est $a^2 - 2b^2$, avec le morphisme de corps $c(a + b\sqrt{2}) = a - \sqrt{2}b$ de sorte que N est multiplicative. Soit $z \in A^\times$, on a alors $N(z) = \pm 1$. A nouveau A est euclidien pour le stathme $|N|$. On remarque que -1 est une norme $-1 = 1^2 - 2 \times 1^2 = N(1 + \sqrt{2})$. Si n est un diviseur de $x^2 - 2y^2$ avec x, y premiers entre eux, alors au signe près n est de la forme $u^2 - 2v^2$. En effet soit $x + \sqrt{2}y = \pi_1 \cdots \pi_r$ une décomposition en produit d'irréductibles; aucun des π_i n'appartient à $\mathbb{Z}$ car x et y sont premiers entre eux, de sorte que comme précédemment les $N(\pi_i)$ sont des premiers de $\mathbb{Z}$; on a alors $x^2 - 2y^2 = N(\pi_1) \cdots N(\pi_r)$ et n au signe près, est un produit de certains de ces $N(\pi_i)$ et donc n est de la forme $N(z) = u^2 - 2v^2$.
L'égalité $-(u^2 - 2v^2) = N((1 + \sqrt{2})(u + v\sqrt{2})) = (u + 2v)^2 - 2(u + v)^2$ permet de négliger le signe $\pm$. Ainsi un premier impair p est de la forme $x^2 - 2y^2$ si et seulement si 2 est un carré modulo p ce qui est équivalent à $p \equiv \pm \mod 8$.

□

Exercice 2. ***Calculs modulaires**: d'après le lemme de Gauss, factoriser sur $\mathbb{Q}$ est essentiellement équivalent à factoriser sur $\mathbb{Z}$. On considère dans la suite $P(X) = \sum_{i=0}^n p_i X^i \in \mathbb{Z}[X]$ que l'on essaie de factoriser sur $\mathbb{Z}$.*

(1) Pour $P \in \mathbb{C}[X]$, on note $|P| = (\sum_i |p_i|^2)^{1/2}$. Soit $A = \sum i = 0^m a_i X^i$ et $B = \sum_{i=0}^n b_i X^i$ des polynômes à coefficients entiers tels que B divise A.

(i) Soit $\alpha \in \mathbb{C}$ et soient $G(X) = (X - \alpha)A(X)$ et $H(X) = (\bar{\alpha}X - 1)A(X)$. Montrer que $|G|^2 = |H|^2$.

(ii) Soit $A(X) = a_m \prod (X - \alpha_j)$ *et* $C(X) = a_m \prod_{|\alpha_j|\geq 1}(X - \alpha_j) \prod_{|\alpha_j|<1}(\bar{\alpha}_j X - 1)$. *Montrer que*

$$|A|^2 = |C^2| \geq |a_m|^2 (M(A)^2 + m(A)^2)$$

où $M(A) = \prod_{|\alpha_j|>1} |\alpha_j|$ *et* $m(A) = \prod_{-\alpha_j|<1} |\alpha_j|$.

(iii) Montrer que si $1 \leq x_1 \leq x_m$ *sont des réels dont le produit est égal à* M *alors les fonctions symétriques* $\sigma_{m,k} = \sum x_{i_1} \cdots x_{i_k}$ *vérifient*

$$\sigma_{m,k} \leq \binom{m-1}{k-1} + \binom{m-1}{k}$$

(iv) En déduire que

$$|b_j| \leq \binom{n-1}{j} |A| + \binom{n-1}{j-1} |a_m|$$

(2) Considérons $A(X) = X^6 - 6X^4 - 2X^3 - 7X^2 + 6X + 1$. *Supposons que* A *n'est pas irréductible de sorte qu'il possède un facteur irréductible de degré* ≤ 3 *avec* $|b_j| \leq 23$ *d'après (1). On choisit alors* $p \geq 2.23$ *et tel que* A *modulo* p *est sans facteur carré, par exemple* $p = 47$.

(i) Montrer que A *modulo* 47 *se factorise comme suit*

$$A(X) = (X - 22)(X - 13)(X - 12)(X + 12)(X^2 - 12X - 4)$$

(ii) En déduire que A *n'a pas de facteurs irréductibles de degré* 1 *ou* 2.

(iii) En déduire qu'un facteur irréductible de degré 3 *de* A *est soit* $X^3 + 23X^2 - X + 1$ *soit* $X^3 - 7X - 1$.

(iv) Factoriser A *sur* $\mathbb{Z}$.

(3) En général la borne donnée par (1) est très grande; plutôt que de raisonner avec un p *grand on raisonne modulo* p^e *pour* e *assez grand en relevant de proche en proche les solutions: c'est le lemme de Hensel suivant:*

Soit p *premier et soient* C, A_e, B_e, U, V *des polynômes à coefficients entiers tels que*

$$C(X) \equiv A_e(X) B_e(X) \mod p^2 \qquad U(X) A_e(X) + V(X) B_e(X) \equiv 1 \mod p$$

On suppose $e \geq 1$, A_e *unitaire,* $\deg U < \deg B_e$, $\deg V < \deg B_e$. *Alors il existe des polynômes* A_{e+1} *et* B_{e+1} *vérifiant les mêmes conditions en remplaçant* e *par* $e + 1$ *et tels que*

$$A_{e+1}(X) \equiv A_e(X) \mod p^e \qquad B_{e+1}(X) \equiv B_e(X) \mod p^e$$

En outre ces polynômes sont uniques modulo p^{e+1}.

(4) En déduire un algorithme de factorisation sur $\mathbb{Z}$.

Remarque: Sur $\mathbb{F}_p$, *on ne connait pas d'algorithme de factorisation en temps polynomial; cependant on a des algorithmes probabilistes en temps polynomial. Sur* $\mathbb{Z}$, *Lenstra a trouvé un algorithme en temps polynomial!*

Preuve : (1) (i) On a

$$\begin{aligned} |G|^2 &= \sum |a_{i-1} - \alpha a_i|^2 = \sum (|a_{i-1}|^2 + |\alpha a_i|^2 - 2Re(\alpha a_i \bar{a}_{i-1})) \\ &= \sum (|\alpha a_{i-1}|^2 + |a_i|^2 - 2Re(\alpha a_i \bar{a}_{i-1})) \\ &= \sum |\bar{\alpha} a_{i-1} - a_i|^2 = |H|^2 \end{aligned}$$

(ii) L'égalité découle directement de (i); le terme de droite de l'inégalité provient du coefficient de X^m et du coefficient constant, d'où le résultat.

(iii) Si on change la paire (x_{m-1}, x_m) par $(1, x_{m-1} x_m)$, toutes les contraintes sont encore satisfaites quitte a réordonner et $\sigma_{m,k}$ augmente de

$$\sigma_{m-2,k-1}(x_{m-1} - 1)(x_m - 1)$$

Ainsi si $x_{m-1} > 1$, le point $(x_1, \cdots, x_m)$ ne réalise pas un maximum. Le maximum est donc atteint pour $x_{m-1} = 1$ ce qui implique $x_i = 1$ pour tout $i < m$ de sorte que $x_m = M$. Le reste du calcul est alors élémentaire: le terme $\binom{m-1}{k-1}$ correspond aux k-uplets contenant x_m et $\binom{m-1}{k}$ à ceux qui ne le contienne pas.

(iv) On en déduit alors que

$$\begin{aligned} |a_j| &\leq |a_m|\Big(\tbinom{m-1}{m-j-1}M(A) + \tbinom{m-1}{m-j}\Big) \\ &\leq |a_m|\Big(\tbinom{m-1}{j}M(A) + \tbinom{m-1}{j-1}\Big) \end{aligned}$$

Ainsi on a $|b_j| \leq |b_n|((\binom{n-1}{j})M(B) + (\binom{n-1}{j-1}))$ et donc $|b_j| \leq |a_m|((\binom{n-1}{j})M(A) + (\binom{n-1}{j-1}))$ car comme B divise A, on a $M(B) \leq M(A)$ et $|b_n| \leq |a_m|$. Le résultat découle alors de (ii) qui donne $M(A) \leq |A|/|a_m|$.

(2) (i) On peut appliquer l'algorithme de Berlekamp pour trouver la factorisation.

(ii) Le terme constant de A étant égal à 1, on en déduit que les termes constants de ses facteurs irréductibles sont égaux à ± 1. Par ailleurs les coefficients de ces facteurs appartiennent à $\{-23, \cdots, 23\}$ de sorte que leur réduction modulo 47 doit être des facteurs de degré 1 écrit dans la factorisation de A modulo 47 dont les coefficients constants ne sont pas égaux à ± 1. De même pour les facteurs de degré 2, on a modulo 47, $12.22 = -18$, $12.13 = 15$, $12.12 = 3$ et $12.22 = 4$; on ne trouve donc pas ± 1 d'où le résultat.

(iii) le même raisonnement pour les facteurs de degré 3 donnent comme seules possibilités celles de l'énoncé.

(iv) On remarque que la première possibilité est exclue car $b_2 \leq 12$ d'après les majorations de (1). On teste alors la divisibilité du deuxième cas et on trouve

$$A(X) = (X^3 - 7X - 1)(X^3 + X + 1).$$

(3) Posons $D = (C - A_e B_e)/p^e \in \mathbb{Z}[X]$. On cherche $A_{e+1} = A_e + p^e S$ et $B_{e+1} = B_e + p^e T$ avec $S, T \in \mathbb{Z}[X]$. La condition $C(X) \equiv A_{e+1}(X)B_{e+1}(X) \mod p^{e+1}$ est équivalent, comme $2e \geq e + 1$, à $A_e T + B_e S \equiv D \mod p$. La solution générale est alors $S \equiv VD + WA_e \mod p$ et $T \equiv UD - WB_e \mod p$ pour un polynôme W. La condition sur le degré impose que S et T sont uniques modulo p et donc A_{e+1} et B_{e+1} sont uniques modulo p^{e+1}.

(4) On choisit p tel que A modulo p soit sans facteur carré. On factorise via Berlekamp, avec le lemme de Hensel on remonte la factorisation modulo p^e pour e assez grand tel que p^e soit supérieur à deux fois la borne trouvée dans (1). On essaie alors les différentes combinaisons possibles de factorisation comme dans (3)

Exercice 3. ***Une équation diophantienne pour les experts de théorie des nombres.*** *On considère le corps quadratique imaginaire $K = \mathbf{Q}(\sqrt{-13})$, et on note σ son automorphisme non trivial.*

(1) Démontrer les assertions suivantes:

- *(a) L'anneau des entiers de K est $\mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\sqrt{-13}$ et son discriminant vaut -52.*
- *(b) $2\mathcal{O} = \mathfrak{p}^2$, où $\mathfrak{p} = \sigma(\mathfrak{p})$ est un idéal premier de $\mathcal{O}$ qui n'est pas principal.*
- *(c) $13\mathcal{O} = \mathfrak{q}^2$, où $\mathfrak{q} = \sigma(\mathfrak{q})$ est l'idéal premier engendré par $\sqrt{-13}$.*
- *(d) $3\mathcal{O}$ est un idéal premier de $\mathcal{O}$.*
- *(e) Les seules unités de $\mathcal{O}$ sont 1 et -1.*

(2) Montrer que toute classe d'idéaux de K admet parmi ses représentants un idéal entier de norme inférieure à 5. Déduire de ce qui précède que le nombre de classes de K vaut 2.

(3) Montrer que pour tout entier rationnel y, l'idéal $\mathfrak{d}$ de $\mathcal{O}$ engendré par $y + \sqrt{-13}$ et $y - \sqrt{-13}$ admet au plus $\mathfrak{p}$ et $\mathfrak{q}$ comme diviseurs premiers — autrement dit, $\mathfrak{p}$ et $\mathfrak{q}$ sont les seuls idéaux premiers pouvant contenir $\mathfrak{d}$.

(4) Soient α, β des entiers naturels tels que $(y + \sqrt{-13})\mathcal{O} = \mathfrak{c}\mathfrak{p}^\alpha\mathfrak{q}^\beta$, où $\mathfrak{c}$ est un idéal de $\mathcal{O}$ qui n'est divisible ni par $\mathfrak{p}$ ni par $\mathfrak{q}$. Montrer que $\mathfrak{c}$ et $\sigma(\mathfrak{c})$ n'ont pas de diviseur premier commun.

On désigne désormais par $(x, y) \in \mathbb{Z}^2$ une solution en entiers rationnels de l'équation

$$Y^2 = X^3 - 13 \qquad (*).$$

(5) *Déduire de la relation* $(x)^3 = (y+\sqrt{-13})(y-\sqrt{-13})$ *l'existence d'un idéal* $\mathfrak{c}$ *de* $\mathcal{O}$ *et de deux entiers naturels* a *et* b *tels que*

$$(y+\sqrt{-13})\mathcal{O} = (\mathfrak{c}\mathfrak{p}^a\mathfrak{q}^b)^3.$$

(6) *Montrer que* $\mathfrak{c}\mathfrak{p}^a\mathfrak{q}^b$ *est un idéal principal.*

(7) *En déduire qu'il existe des entiers rationnels* u, v *tels que*

$$y = u^3 - 39uv^2 \quad , \quad 1 = v(3u^2 - 13v^2).$$

(8) *Dans le taxi qui l'amène à la mairie-préfecture où il doit épouser Alice, Bernard s'aperçoit qu'en soustrayant le carré du dernier nombre de la plaque minéralogique de la voiture au cube de l'âge de sa fiancée, il pourrait se croire à Marseille. Alice est-elle en âge de se marier, et si oui, dans quelle ville sera célébré l'heureux événement ?*

Preuve : Le corps K est corps de rupture du polynôme $P = X^2 + 13$.

(1) On a vu en cours le calcul de l'anneau des entiers d'uun corps quadratique. Le (a) est donc déjà connu. Pour calculer la décomposition des idéaux premiers, il suffit d'après le (complément de) cours, de réduire le polynôme P. On a $P \equiv (X+1)^2 \pmod 2$, $P \equiv X^2 \pmod{13}$, et P irréductible (mod 3). Ceci démontre les (b), (c) et (d), à part le fait que $\mathfrak{p}$ n'est pas principal. Mais s'il l'était, un générateur $x + y\sqrt{13}$ donnerait une solution entière à l'équation $x^2 + 13y^2 = 2$ qui n'en a pas. De même,, l'équation en entiers $x^2 + 13y^2 = \pm 1$ n'a que les solutions triviales $(1, 0)$ et $(-1, 0)$, d'où le v).

(2) Avec les notations du cours, on a $n = 2$ et $t = 1$. La constante de Minkowski de K vaut donc

$$M_K = \frac{4}{\pi} \cdot \frac{2}{4} \cdot \sqrt{52} = \frac{4\sqrt{13}}{\pi} \approx 4.6 < 5,$$

d'où la première affirmation. Les seuls idéaux entiers de norme inférieure à 5 sont $\mathcal{O}$, $\mathfrak{p}$ et $2\mathcal{O}$. Il y a donc au plus une classe non principale (celle de $\mathfrak{p}$), et comme on a vu qu'elle ne l'était effectivement pas, il y a exactement deux classes distinctes.

(3) Un tel idéal doit contenir leur différence $2\sqrt{13}$, donc $\mathfrak{d} \mid 2\sqrt{13}\mathcal{O} = \mathfrak{p}^2\mathfrak{q}$, donc les seuls (idéaux) diviseurs premiers de $\mathfrak{d}$ sont au plus $\mathfrak{p}$ et $\mathfrak{q}$.

(4) On a $(y-\sqrt{-13})\mathcal{O} = \sigma((y+\sqrt{-13})\mathcal{O}) = \sigma(\mathfrak{c}\mathfrak{p}^\alpha\mathfrak{q}^\beta) = \sigma(\mathfrak{c})\mathfrak{p}^\alpha\mathfrak{q}^\beta$. Tout (idéal) premier facteur commun entre $\mathfrak{c}$ et $\sigma(\mathfrak{c})$ serait un facteur commun entre $y-\sqrt{-13}$ et $y+\sqrt{-13}$, donc $\mathfrak{p}$ ou $\mathfrak{q}$, qui ne peuvent diviser $\mathfrak{c}$.

(5) Ecrivons comme au (4) $(y+\sqrt{-13})\mathcal{O} = \mathfrak{c}'\mathfrak{p}^\alpha\mathfrak{q}^\beta$, où $\mathfrak{c}'$ est un idéal de $\mathcal{O}$ qui n'est divisible ni par $\mathfrak{p}$ ni par $\mathfrak{q}$. On a

$$(x)^3 = (y+\sqrt{-13})\mathcal{O}\sigma((y+\sqrt{-13})\mathcal{O}) = \mathfrak{c}'\mathfrak{p}^\alpha\mathfrak{q}^\beta\sigma(\mathfrak{c}'\mathfrak{p}^\alpha\mathfrak{q}^\beta) = \mathfrak{c}'\sigma(\mathfrak{c}')\mathfrak{p}^{2\alpha}\mathfrak{q}^{2\beta},$$

cette dernière décomposition étant en quatre facteurs premiers entre eux deux à deux. On en déduit que chacun des quatre facteurs est lui-même le cube d'un idéal entier, $\mathfrak{c}' = \mathfrak{c}^3$, $\alpha = 3a$ et $\beta = 3b$, d'où le résultat.

(6) Le groupe des classes d'idéaux a deux éléments; la multiplication par 3 est donc l'identité sur ce groupe: un idéal est principal si et seulement si son cube l'est. C'est donc le cas de $\mathfrak{c}\mathfrak{p}^a\mathfrak{q}^b$ dont le cube est engendré par $y+\sqrt{-13}$.

(7) Notons $u+v\sqrt{-13}$ un générateur de l'idéal $\mathfrak{c}\mathfrak{p}^a\mathfrak{q}^b$. Le cube de cet entier est un générateur de $(y+\sqrt{-13})\mathcal{O}$, c'est-à-dire qu'il vaut $\pm((y+\sqrt{-13})$. En changeant au besoin les signes de u et v, on choisit le signe $+$, d'où l'équation $y+\sqrt{-13} = (u+v\sqrt{-13})^3$ qui donne celles du texte.

(8) La deuxième équation impose $v = -1$ et $u = \pm 2$, et la première $y = \pm 70$, d'où $x = u^2 + 13v^2 = 17$. Alice a 17 ans et le mariage a lieu à Vesoul.