Université Côte d'Azur
Année 2020-2021

Fiche thématique : Polynômes irréductibles, corps de rupture

1. Quelques rappels

1.1. **Généralités sur les polynômes irréductibles (voir** [Per82, Dem97] **pour plus de détails).** Notations : A désigne un anneau factoriel et K désigne son corps de fractions.

Définition 1. Un polynôme $P \in A[X]$ est dit *irréductible* si
- $P \notin A^*$,
- $P = QR \Rightarrow Q \in A^*$ ou $R \in A^*$.

Définitions 2. Un *contenu* d'un polynôme non nul de $A[X]$ est un pgcd de ses coefficients.
Un polynôme P est *primitif* si 1 est un contenu de P.

***Lemme* 3** (Lemme de Gauss, [FGN07], §5.16, pages 188-189)**.** — *Soient P et Q dans $A[X] \setminus \{0\}$. Soient c un contenu de P et c' un contenu de Q. Alors cc' est un contenu de PQ.*

***Proposition* 4.** — *Les polynômes P de $A[X]$ irréductibles dans $A[X]$ sont*
- *les constantes $p \in A$, irréductibles dans A,*
- *les polynômes P, de degré $\geqslant 1$, primitifs et irréductibles dans $K[X]$.*

1.2. **Corps de rupture et le corps de décomposition d'un polynôme (**[Per82]**).** Nous allons résoudre les deux problèmes suivants :
- étant donné $P \in K[X]$ irréductible de degré $d > 1$, construire une extension dans laquelle P admet une racine a ;
- étant donné $P \in K[X]$ construire une extension dans laquelle P soit décomposé en produit de facteurs de degré 1.

Un énoncé fondamental est le suivant :

***Lemme* 5.** — *Si $P \in K[X]$ est irréductible, alors la K-algèbre $K[X]/(P)$ est un corps.*

Définition 6. Soient K un corps et soit $P \in K[X]$ un polynôme irréductible. Une extension L de K est appelée *corps de rupture* de P sur K si L est une extension monogène $L = K(\alpha)$ avec $P(\alpha) = 0$.

***Théorème* 7** ([Per82], Chapitre III, Théorème 1.27, page 70)**.** — *Soit $P \in K[X]$ un polynôme irréductible. Il existe un corps de rupture de P sur K, unique à isomorphisme (non unique) près.*

Exemple 8. $\mathbb{C}$ peut être défini comme un corps de rupture de $X^2 + 1 \in \mathbb{R}[X]$.

Définition 9. Soit $P \in K[X]$ un polynôme de degré n. On appelle *corps de décomposition* de P sur K une extension L de K telle que
- P est produit de facteurs de degré 1 dans $L[X]$,
- le corps L est minimal pour cette propriété, *i.e.* les racines de P engendrent L.

***Théorème* 10** ([Per82], Chapitre III, Théorème 1.30, page 71)**.** — *Pour tout $P \in K[X]$ il existe un corps de décomposition de P sur K unique à isomorphisme (non unique) près.*

Définition 11. Une extension $\overline{K}$ de K est appelée une clôture algébrique si elle vérifie que
- ◇ $\overline{K}$ est algébriquement clos,
- ◇ et $\overline{K}$ est algébrique sur K.

Exemple 12. $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$: c'est le théorème de d'Alembert-Gauss.

***Théorème* 13** (Théorème de Steinitz, [Goz97], Théorème V.34)**.** — *Tout corps (commutatif) K admet une clôture algébrique.*

1.3. **En appliquant ces résultats à la théorie des corps finis nous obtenons ce qui suit.**

***Théorème* 14** ([Per82], Chapitre III, Théorème 2.5, page 73)**.** — *Soient p un nombre premier et $n \geqslant 1$ un entier. Posons $q = p^n$.*
- ◇ *Il existe un corps $\Bbbk$ à q éléments ; il est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$.*
- ◇ *Si $\Bbbk$ et $\Bbbk'$ sont deux corps à q éléments, alors ils sont isomorphes.*

***Théorème* 15** ([Goz97], Théorème VII.12.)**.** — *Considérons l'extension $L = \mathbb{F}_{p^n}$ de $K = \mathbb{F}_p$. Il existe $\alpha \in L$ tel que $L = K[\alpha]$.*

En prenant le polynôme minimal de α sur K on en déduit la :

***Proposition* 16** ([Goz97], Théorème VII.24.)**.** — *Pour tout corps K à $q = p^n$ éléments il existe un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré n tel que $K \simeq {}^{\mathbb{F}_p[X]}\!/_{(P)}$.*

Remarque 17. Il n'existe pour l'instant pas d'algorithme permettant de trouver ce polynôme.

Donnons encore d'autres résultats sur les polynômes irréductibles des corps finis.

***Théorème* 18** ([Goz97], Théorème VII.27.)**.** — *Soient p un nombre premier et n un entier naturel non nul. Pour $j \in \mathbb{N}^*$ désignons par $\mathcal{K}(p,j)$ l'ensemble des polynômes irréductibles de degré j sur $\mathbb{F}_p$. Alors*

$$X^{p^n} - X = \prod_{d|n} \prod_{Q \in \mathcal{K}(p,j)} Q(X).$$

***Corollaire* 19** ([Goz97], Définition VII.28.)**.** — *Soient p un nombre premier et n un entier naturel non nul. Pour $j \in \mathbb{N}^*$ désignons par $\mathcal{I}(p,j)$ le cardinal de $\mathcal{K}(p,j)$. Alors*

$$p^n = \sum_{d|n} d\mathcal{I}(p,d).$$

L'algorithme de Berlekamp permet grâce à des techniques d'algèbre linéaire et des calculs de pgcd de décomposer les polynômes $P \in \mathbb{F}_p[X]$ en facteurs irréductibles. Soit p un nombre premier. Soit $P \in \mathbb{F}_p[X]$ un polynôme unitaire. Considérons tout d'abord le cas des polynômes sans facteurs carrés, *i.e.* de la forme $P = P_1 P_2 \dots P_r$ où les P_i sont irréductibles, unitaires et deux à deux distincts. Posons $n = \deg P$. Considérons $K_i = {}^{\mathbb{F}_p[X]}\!/_{(P_i)}$ pour $1 \leqslant i \leqslant r$; les P_i étant irréductibles ce sont des corps. La projection canonique

$$\mathbb{F}_p[X] \to {}^{\mathbb{F}_p[X]}\!/_{(P_1)} \times \dots \times {}^{\mathbb{F}_p[X]}\!/_{(P_r)}$$

passe au quotient et fournit un isomorphisme entre $A = {}^{\mathbb{F}_p[X]}\!/_{(P)}$ et ${}^{\mathbb{F}_p[X]}\!/_{(P_1)} \times \dots \times {}^{\mathbb{F}_p[X]}\!/_{(P_r)}$ (c'est le théorème chinois). Ainsi l'équation

$$Q^p \equiv Q[P] \tag{1.1}$$

a exactement p^r solutions, chacune correspondant à un unique r-uplet $(\alpha_1, \alpha_2, \ldots, \alpha_r) \in (\mathbb{F}_p)^r$ tel que $Q \equiv \alpha_i [P_i]$; en effet c'est le théorème chinois ajouté au fait que $A^p \equiv A\ [P_i]$ implique que A est une constante de $\mathbb{F}_p$. Remarquons ensuite qu'on a le

***Lemme* 20.** — *La décomposition* $P = \prod_{\alpha \in \mathbb{F}_p} \operatorname{pgcd}(P, Q - \alpha)$ *est valable pour tout polynôme* Q *non constant vérifiant (1.1).*

Démonstration. Pour tout i il existe un et un seul $\alpha_i \in \mathbb{F}_p$ tel que $Q \equiv \alpha_i\ [P_i]$. Ainsi P_i divise $Q - \alpha$ si et seulement si $\alpha = \alpha_i$.

Nous avons alors

$$\operatorname{pgcd}(P, Q - \alpha) = \prod_{i \mid \alpha = \alpha_i} P_i$$

(avec la convention $\prod_{\emptyset} = 1$). □

Il suffit donc de résoudre

$$Q^p \equiv Q [P] \tag{1.2}$$

puisque nous disposons d'un algorithme performant (l'algorithme d'Euclide) pour calculer des pgcd. Il est plus facile de résoudre (1.2) que de chercher à la main la décomposition en facteurs premiers de P car $S \colon A \to A$, $Q \mapsto Q^p$ est linéaire. Il s'agit donc de déterminer le noyau de $S - I$ ce qui se fait en utilisant les techniques usuelles d'algèbre linéaire (écrire la matrice de S dans la base $\{1, X, X^2, \ldots, X^{n-1}\}$ de $\mathbb{F}_p[X]/(P)$). Remarquons enfin que $r = \dim \ker(S - I) = n - \operatorname{rg}(S - I)$ car $Q^p \equiv Q\ [P]$ a p^r solutions. Nous avons alors l'algorithme suivant :

- ◇ Premier pas : calculer $D = \operatorname{pgcd}(P, P')$. Si $D \neq 1$, alors on arrête (on a un facteur non trivial de P) ;
- ◇ Deuxième pas : résoudre $Q^p \equiv Q\ [P]$ en déterminant le noyau de $S - I$;
- ◇ Troisième pas : si $r = 1$, alors on arrête (P est irréductible). Si $r \geqslant 2$, alors il existe Q non constant modulo P solution de $Q^p \equiv Q\ [P]$. Le Lemme 20 assure que $P = \prod_{\alpha \in \mathbb{F}_p} \operatorname{pgcd}(P, Q - \alpha)$ avec une décomposition non triviale.

En itérant cet algorithme un nombre de fois suffisant on obtient la décomposition cherchée.

Exemple 21. Cet algorithme permet de trouver la décomposition en facteurs unitaires irréductibles de $X^6 + X^5 + X^4 + X^3 + 1 \in \mathbb{F}_2[X]$.

1.4. **Moyens effectifs pour s'assurer de l'irréductibilité de polynômes.**

***Théorème* 22** (Critère d'Eisenstein, [Per82], Chapitre III, Théorème 3.2, Page 76)**.** — *Soient* $P(X) = a_n X^n + \ldots + a_0 \in A[X]$ *un polynôme et* $p \in A$ *un élément irréductible. Supposons que*

- ◇ p *ne divise pas* a_n,
- ◇ p *divise* a_i *pour* $0 \leqslant i \leqslant n - 1$,
- ◇ p^2 *ne divise pas* a_0.

Alors P *est irréductible dans* $K[X]$.

Exemple 23. Si p est un nombre premier, alors le polynôme $X^{p-1} + X^{p-2} + \ldots + X + 1$ est irréductible sur $\mathbb{Z}$ (poser $X = Y + 1$ et appliquer le critère d'Eisenstein avec p).

Exemple 24. Soit $a \in \mathbb{Z}$; écrivons-le sous la forme $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. Supposons que l'un des α_i vaut 1 ; alors $X^n - a$ est irréductible sur $\mathbb{Z}$.

Exemple 25. Soit $\lambda \in K$, $\lambda \notin \{0, 1\}$. Le polynôme $Y^2 - X(X-1)(X-\lambda)$ est irréductible.

***Théorème* 26** (Critère de réduction, [Per82], Chapitre III, Théorème 3.5, Page 77)**.** — *Soit I un idéal premier de A. Alors $B = {}^{A}\!/_{I}$ est un anneau intègre ; soit L son corps de fractions. Soit $P(X) = a_n X^n + \ldots + a_0 \in A[X]$; notons $\overline{P}$ sa réduction modulo I.*

Supposons que $\overline{a_n}$ soit non nul dans B. Si $\overline{P}$ est irréductible sur B ou L, alors P est irréductible sur K.

Exemple 27. Le polynôme X^2+Y^2+1 est irréductible dans $\mathbb{R}[X, Y]$ (passer au quotient par l'idéal (Y)).

Exemple 28. Le cas le plus fréquent d'utilisation de l'énoncé précédent est le cas $A = \mathbb{Z}$, $I = (p)$ avec p premier, $B = \mathbb{F}_p$ est alors un corps. Ainsi le polynôme $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$: on le réduit modulo 2, il reste $X^3 + X + 1$ qui est irréductible sur $\mathbb{F}_2$ (sinon il aurait une racine dans $\mathbb{F}_2$).

Exemple 29. Soit p un nombre premier, alors $X^p - X - 1$ est irréductible sur $\mathbb{Z}$ (*voir* [Per82]).

***Théorème* 30** ([Per82], Chapitre III, Théorème 3.9, Page 77)**.** — *Soit $P \in K[X]$ un polynôme de degré $n > 0$. Les deux assertions suivantes sont équivalentes :*

- *P est irréductible sur K ;*
- *P n'a pas de racine dans les extensions L de K qui vérifient $[L : K] \leqslant \frac{n}{2}$.*

Exemple 31. Le polynôme $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$. Il suffit de vérifier qu'il n'a pas de racines dans $\mathbb{F}_2$, ni dans $\mathbb{F}_4$. Pour $\mathbb{F}_2$ c'est clair. Pour $\mathbb{F}_4$ notons que $\mathbb{F}_4 = \mathbb{F}_2[\mathbf{j}]$ avec $\mathbf{j}^2 + \mathbf{j} + 1 = 0$. Si x appartient à $\mathbb{F}_4 \smallsetminus \mathbb{F}_2$, nous avons $x = \mathbf{j}$ ou $x = \mathbf{j} + 1 = -\mathbf{j}^2$ donc $x^3 = 1$ et $x^4 + x + 1 = 2x + 1 = 1 \neq 0$.

1.5. **Théorie de Galois.** La théorie de Galois a tout-à-fait sa place ici puisque la définition de ses concepts (extension normale, ...) utilise la notion de polynôme irréductible.

Exercices

Exercice 1 Soit K un corps fini de cardinal q. Soit $d > 0$ un entier.

a) Montrer qu'il existe une extension de corps L de K de degré d, unique à isomorphisme près. Quel est le cardinal de L ?

b) Rappelons que le groupe multiplicatif L^* est cyclique. Soit α un générateur de ce groupe. Montrer que $L = K[\alpha]$.

c) En déduire qu'il existe un polynôme irréductible P dans $K[X]$ avec $\deg P = d$ (notons que trouver explicitement un tel P est un problème algorithmique difficile).

Exercice 2 Soit K un corps fini de cardinal q. Soit $P \in K[X]$ un polynôme irréductible de degré d. Soit $L = K[\alpha]$ un corps de rupture de P.

a) Montrer que l'application $F \colon x \mapsto x^q$ est un automorphisme du corps L qui induit l'identité sur K. Notons $F^m = F \circ F \circ \ldots \circ F$ le m-ième itéré de F.

b) Montrer que d est le plus petit entier $m > 0$ tel que $F^m(\alpha) = \alpha$ (raisonner par l'absurde en montrant que si on avait $m < d$, alors α appartiendrait à une extension de corps de K strictement incluse dans L).

c) En déduire que L est aussi un corps de décomposition de P.

d) Posons $K = \mathbb{F}_4$ et $L = \mathbb{F}_{16}$, corps respectivement à 4 et 16 éléments. Montrer que L est une extension de degré 2 de F qui peut s'écrire $L = K[\alpha]$ où α est un élément d'ordre 5 de L^* (ici α n'est donc pas un générateur de L^*).

Exercice 3 Soit K un corps.

a) Montrer que si K est fini de caractéristique p, alors l'application

$$K \to K, \qquad x \mapsto x^p$$

est bijective.

b) Supposons maintenant que K soit de caractéristique zéro. Montrer que si $P \in K[X]$ est irréductible dans $K[X]$ et si L est une extension de corps de K, alors toute racine de P dans L est simple.

c) Montrer que b) reste vrai si K est un corps fini [1] mais que b) est faux si $K = {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}(T)$.

d) Un corps K de caractéristique $p > 0$ est dit parfait si le morphisme

$$K \to K, \qquad x \mapsto x^p$$

est bijectif. Montrer que b) reste vrai plus généralement si K est un corps parfait et que b) est faux si K est un corps imparfait.

Exercice 4 Soit K un corps. Soit $\sigma\colon K \to K$ un automorphisme de K. Soit L un K-espace vectoriel.

a) Montrer que $(L, +)$ muni de la loi externe $(\alpha, x) \mapsto \sigma(\alpha) \cdot x$ est aussi un K-espace vectoriel que l'on notera L'.

b) Montrer que si L est de dimension finie d, alors L' est aussi de dimension d.

c) En déduire que si $\Bbbk$ est un corps parfait de caractéristique $p > 0$, alors toute extension finie de K est un corps parfait.

d) Le résultat de c) reste-t-il vrai pour une extension algébrique (pas nécessairement finie) ?

Exercice 5 Notons $\overline{\mathbb{Q}}$ l'ensemble des nombres complexes qui sont algébriques sur $\mathbb{Q}$. C'est un sous-corps de $\mathbb{C}$.

a) Montrer que $\overline{\mathbb{Q}}$ est dénombrable.

b) Montrer que $\overline{\mathbb{Q}}$ est algébriquement clos. On observera que si $P = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ est un polynôme unitaire à coefficients dans $\overline{\mathbb{Q}}$, alors tous les coefficients a_i vérifient que le corps $\mathbb{Q}(a_i)$ est un $\mathbb{Q}$-ev de dimension finie.

c) Montrer que $\overline{\mathbb{Q}}$ est le plus petit corps algébriquement clos (inclus dans $\mathbb{C}$) qui contient $\mathbb{Q}$. Étendre cette construction à un sous-corps K quelconque d'un corps algébriquement clos L.

d) $\overline{\mathbb{Q}}$ est-il un $\mathbb{Q}$-ev de dimension finie ?

Exercice 6 Soit $A = \mathbb{Z}[\mathbf{i}\sqrt{2}] = \left\{a + \mathbf{i}b\sqrt{2} \,|\, a, b \in \mathbb{Z}\right\}$. On définit pour $z = a + \mathbf{i}b\sqrt{2} \in A$

$$N(z) = a^2 + 2b^2.$$

a) Montrer que A est euclidien donc factoriel.

1. Indication : utiliser a).

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

c) Étudier $S=\left\{n \in \mathbb{Z} \,|\, \exists\,(x,y) \in \mathbb{Z}^2,\ n=x^2+2y^2\right\}$. Indication : on utilisera que -2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1,\ 3 \bmod 8$.

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

Exercice 7 Trouver un élément primitif de $\mathbb{Q}[\sqrt{3},\sqrt{7}]$.

Exercice 8 Montrer que si K est un corps de caractéristique p non nulle, le corps $M=K(X,Y)$ des fractions rationnelles en deux indéterminées à coefficients dans K est une extension de degré p^2 de son sous-corps $L=K(X^p,Y^p)$.

Montrer que si α est un élément de M qui n'est pas dans L, son polynôme minimal sur L est de degré p.

En déduire que le mot séparable dans l'énoncé du théorème de l'élément primitif [2] n'est pas inutile.

Exercice 9 Soit u un endomorphisme de $V \simeq K^n$ dont on note χ_u et π_u respectivement les polynômes caractéristique et minimal.

(1) Montrer que χ_u est irréductible si et seulement si V n'a pas de sous-espace stable par u ;

(2) Montrer que u est cyclique avec π_u une puissance d'un polynôme irréductible si et seulement si V est indécomposable sous u ;

(3) Proposer un algorithme pour tester si u est semi-simple.

Exercice 10 D'après le Lemme de Gauss factoriser sur $\mathbb{Q}$ est essentiellement équivalent à factoriser sur $\mathbb{Z}$. Considérons dans la suite $P(X)=\sum_{i=0}^{n} p_i X^i \in \mathbb{Z}[X]$ que nous essayons de factoriser sur $\mathbb{Z}$.

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

(i) Soit $\alpha \in \mathbb{C}$. Soient

$$G(X)=(X-\alpha)A(X) \qquad \text{et} \qquad H(X)=(\overline{\alpha}X-1)A(X).$$

Montrer que $|G|^2=|H|^2$.

(ii) Soient

$$A(X)=a_m\prod(X-\alpha_j) \qquad \text{et} \qquad C(X)=a_m\prod_{|\alpha_j|\geqslant 1}(X-\alpha_j)\prod_{|\alpha_j|<1}(\overline{\alpha}_j X-1).$$

Montrer que

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

où

$$M(A)=\prod_{|\alpha_j|>1}|\alpha_j| \qquad \text{et} \qquad m(A)=\prod_{|\alpha_j|<1}|\alpha_j$$

2. Théorème. Toute extension finie séparable est simple, c'est-à-dire engendrée par un seul élément, appelé élément primitif.

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

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

(iv) En déduire que

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

(2) Considérons $A(X) = X^6 - 6X^4 - 2X^3 - 7X^2 + 6X + 1$. Supposons que A ne soit pas irréductible de sorte qu'il possède un facteur irréductible de degré $\leqslant 3$ avec $|b_j| \leqslant 23$ d'après (1).

On choisit alors $p \geqslant 2.23$ tel que A modulo p soit 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 et V des polynômes à coefficients entiers tels que

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

On suppose $e \geqslant 1$, 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

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

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

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

Exercice 11 Considérons le corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-13})$. Notons σ son automorphisme non trivial.

(1) Démontrer les assertions suivantes :
(a) L'anneau des entiers de K est $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}[\sqrt{-13}]$ 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 $(y+\sqrt{-13})\mathcal{O} = \mathfrak{c}\mathfrak{p}^a\mathfrak{q}^b$ o'u $\mathfrak{c}$ 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.

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

$$Y^2 = X^3 - 13.$$

(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

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

(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 ? Si oui dans quelle ville sera célébré l'heureux événement ?

Exercice 12

1) Le critère d'irréductibilité d'Eisenstein. Si ℓ est un nombre premier et si $x \in \mathbb{Q} \setminus \{0\}$, on note $v_\ell(x)$ la valuation ℓ-adique de x (*i.e.* $x = \pm\ell^{v_\ell(x)}\frac{n}{d}$ où $n \in \mathbb{N}$ et $d \in \mathbb{N}^*$ sont premiers à ℓ)

Soit

$$A(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{Q}[X].$$

Supposons qu'il existe p premier tel que $v_p(a_n) = 0$, $v_p(a_0) = 1$ et pour $i < n$, $v_p(a_i) \geqslant 1$. Supposons que $A(X) = B(X)C(X)$ avec B, $C \in \mathbb{Q}[X]$. Désignons par $\mathcal{P}$ l'ensemble des premiers dans $\mathbb{N}$. Si $T(X) = \sum_i t_iX^i \in \mathbb{Q}[X] \setminus \{0\}$, notons $\mathrm{Cont}(T) = \prod_{\ell\in\mathcal{P}} l^{\inf_i v_p(t_i)}$ un contenu de T.

a) Posons $A' = \frac{A}{\mathrm{Cont}(A)}$.

Montrer que A' appartient à $\mathbb{Z}[X]$ et que $v_p(a'_n) = 0$, $v_p(a'_0) = 1$ et pour $i < n$, $v_p(a'_i) \geqslant 1$.

b) Montrer qu'il existe un unique morphisme d'anneaux

$$\pi\colon \mathbb{Z}[X] \to \mathbb{F}_p[X]$$

qui induit la réduction modulo p sur $\mathbb{Z}$ et tel que $\pi(X) = X$.

Montrer que $\deg(\pi(T(X))) \leqslant \deg(T(X))$.

c) Posons $B' = \frac{B}{\mathrm{Cont}(B)}$ et $C' = \frac{C}{\mathrm{Cont}(C)}$.

Montrer que $\pi(A') = \pi(a'_n)X^n$ et en déduire que $\pi(B') = \pi(b'_t)X^t$, $\pi(C') = \pi(x'_s)X^s$ où $\deg B' = t$ et $\deg C' = s$.

d) En déduire que A est irréductible dans $\mathbb{Q}[X]$.

2) L'irréductibilité de $\Phi_p(X)$, le $p$ième polynôme cyclotomique.

a) Montrer que $\Phi_p(X)$ appartient à $\mathbb{Z}[X]$.

b) Montrer que $\Phi_p(1) = p$ et que $\Phi_p(X+1) = X^{p-1} \bmod p\mathbb{Z}[X]$.

c) En déduire que $\Phi_p(X)$ est irréductible dans $\mathbb{Z}[X]$.

3) L'irréductibilité de $\Phi_{p^r}(X)$ pour $r > 1$.

a) Montrer que $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$.

b) Montrer que $\Phi_{p^r}(X+1) = ^{p^{r-1}(p-1)} \bmod p\mathbb{Z}[X]$.

c) En déduire que $\Phi_{p^r}(X)$ est irréductible dans $\mathbb{Z}[X]$.

Exercice 13 Comptons les polynômes irréductibles de $\mathbb{F}_p[X]$ de degré n.
Soit L un corps fini à $q = p^n$ éléments.

(1) Soit $P \in \mathbb{F}_p[X]$ unitaire, irréductible de degré d. Supposons que P divise $X^q - X$. Montrons que d divise n.

(2) Soit $P \in \mathbb{F}_p[X]$ unitaire, irréductible de degré $d|n$. Montrons que P divise $X^q - X$.

(3) Pour $d|n$ notons I_d le cardinal de l'ensemble des $P \in \mathbb{F}_p[X]$ unitaires, irréductibles de degré d avec $P|(X^q - X)$. Montrons que $p^n = \sum_{d|n} dI_d$.

(4) En déduire que $nI_n \leqslant p^n$.

(5) Montrer que $nI_n \geqslant p^n - \sum_{1 \leqslant d \leqslant n-1} p^d$.

(6) En déduire que $nI_n \geqslant 2 + (p-2)\frac{p^n-1}{p-1}$.

Exercice 14 Il n'existe pas d'anneau A dont le groupe des inversibles $A^\times$ est d'ordre 5.
Supposons que A soit un anneau unitaire dont le groupe des inversibles $A^\times$ est d'ordre 5.

(1) Montrer que $1 = -1$ dans A. En déduire que A contient un sous-corps isomorphe à $\mathbb{F}_2$ (on le notera encore $\mathbb{F}_2$).

(2) Soit B le sous-anneau de A engendré par $A^\times$. Montrer que $A^\times = B^\times$.

(3) Soit ζ un générateur de $A^\times$. Justifier l'existence d'un morphisme de $\mathbb{F}_2$-algèbre $\rho\colon \mathbb{F}_2[X] \to A$ tel que $\rho(P(X)) = P(\xi)$.

(4) Montrer que $B = \operatorname{Im}\rho$ et que $\ker\rho = S(X)\mathbb{F}_2[X]$ avec $S(X)$ unitaire divisant $X^5 - 1$.

(5) Montrer que $\frac{X^5-1}{X-1}$ est irréductible sur $\mathbb{F}_2$. En déduire la liste des diviseurs de $X^5 - 1$ dans $\mathbb{F}_2[X]$.

(6) En remarquant que $B \simeq {}^{\mathbb{F}_2[X]}\!/_{S(X)\mathbb{F}_2[X]}$ conclure à une contradiction.

Références

[Dem97] M. Demazure. *Cours d'algèbre*, volume 1 of *Nouvelle Bibliothèque Mathématique [New Mathematics Library]*. Cassini, Paris, 1997. Primalité. Divisibilité. Codes. [Primality. Divisibility. Codes].

[FGN07] S. Francinou, H. Gianella, and S. Nicolas. *Exercices de mathématiques oraux x-ens, algèbre 1*. Cassini, 2007.

[Goz97] I. Gozard. *Théorie de Galois*. Ellipses, 1997.

[Per82] D. Perrin. *Cours d'algèbre*, volume 18 of *Collection de l'École Normale Supérieure de Jeunes Filles*. École Normale Supérieure de Jeunes Filles, Paris, 1982. Edited with the collaboration of Marc Cabanes and Martine Duchene.