Université Nice Sophia Antipolis
Année 2019-2020

Fiche thématique: Polynômes irréductibles, corps de rupture

Contents

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
- $\diamond$ $P \notin A^*$,
- $\diamond$ $P = QR \Rightarrow Q \in A^*$ 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*
- $\diamond$ *les constantes $p \in A$, irréductibles dans A,*
- $\diamond$ *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:
- $\diamond$ étant donné $P \in K[X]$ irréductible de degré $d > 1$, construire une extension dans laquelle P admet une racine a;
- $\diamond$ 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

- $\diamond$ P est produit de facteurs de degré 1 dans $L[X]$,
- $\diamond$ 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

- $\diamond$ $\overline{K}$ est algébriquement clos,
- $\diamond$ 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 $q = p^n$.*

- $\diamond$ *Il existe un corps $\Bbbk$ à q éléments; il est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$.*
- $\diamond$ *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

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

passe au quotient et fournit un isomorphisme entre $A = {}^{\mathbb{F}_p[X]}\!/_{(P)}$ et ${}^{\mathbb{F}_p[X]}\!/_{(P_1)} \times \ldots \times {}^{\mathbb{F}_p[X]}\!/_{(P_r)}$ (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).*

Proof. 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. Factoriser $P(X) = X^9 + X^6 - X + 1$ sur $K = \mathbb{F}_3$.

Commençons par remarquer que P n'a pas de racine dans K.

Appliquons maintenant l'algorithme:

- ◇ $P' = -1$;
- ◇ $\operatorname{pgcd}(P, P') = 1$ car $P' = -1$;

◇ l'algèbre qui nous intéresse est

$$A = {}^{K[X]}\!/_{X^9+X^6-X+1}.$$

C'est un K-espace vectoriel de dimension 9 dont une base est $\{1, X, X^2, \ldots, X^8\}$. Pour calculer la matrice de l'endomorphisme $S-I$ nous aurons besoin des puissances de X^3 jusqu'à X^{24}. Nous avons

$$\begin{aligned}
X^9 &= -X^6+X-1\\
X^{10} &= -X^7+X^2-X\\
X^{11} &= -X^8+X^3-X^2\\
X^{12} &= -(-X^6+X-1)+X^4-X^3 = X^6+X^4-X^3-X+1\\
X^{15} &= (-X^6+X-1)+X^7-X^6-X^4+X^3 = X^7+X^6-X^4+X^3+X-1\\
X^{18} &= (-X^7+X^2-X)+(-X^6+X-1)-X^7+X^6+X^4-X^3 = X^7+X^4-X^3+X^2-1\\
X^{21} &= (-X^7+X^2-X)+X^7-X^6+X^5-X^3 = -X^6+X^5-X^3+X^2-X\\
X^{24} &= -(-X^6+X-1)+X^8-X^6+X^5-X^4 = X^8+X^5-X^4-X+1
\end{aligned}$$

Alors la matrice de $S-I$ est

$$\begin{pmatrix}
0 & 0 & 0 & -1 & 1 & -1 & -1 & 0 & 1\\
0 & -1 & 0 & 1 & -1 & 1 & 0 & -1 & -1\\
0 & 0 & -1 & 0 & 0 & 0 & 1 & 1 & 0\\
0 & 1 & 0 & -1 & -1 & 1 & -1 & -1 & 0\\
0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & -1\\
0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 1\\
0 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
\begin{matrix}
1\\ X\\ X^2\\ X^3\\ X^4\\ X^5\\ X^6\\ X^7\\ X^8
\end{matrix}$$

Le noyau contient la droite engendrée par la première colonne ; il faut déterminer s'il est plus gros. Uilisons le pivot de Gauss; nous trouvons par exemple le vecteur $(0, 1, -1, -1, 1, 1, -1, 0, 1)$. Un représentant polynôme est

$$Q(X) = X^8 - X^6 + X^5 + X^4 - X^3 - X^2 + X.$$

Calculons $\operatorname{pgcd}(P, Q-\alpha)$. On utilise l'algorithme d'Euclide: la première division est

$$X^9+X^6-X+1 = \Big(X^8-X^6+X^5+X^4-X^3-X^2+X-\alpha\Big)X+\Big(X^7-X^5+X^4+X^3-X^2+(\alpha-1)X+1\Big);$$

la seconde est

$$X^8-X^6+X^5+X^4-X^3-X^2+X-\alpha = \Big(X^7-X^5+X^4+X^3-X^2+(\alpha-1)X+1\Big)X-\alpha(X^2+1)$$

C'est gagné car si $\alpha = 0$ nous avons un reste nul donc $X^7-X^5+X^4+x^3-X^2-X+1$ divise P:

$$P(X) = (X^7-X^5+X^4+X^3-X^2-X+1)(X^2+1).$$

On pourrait imaginer continuer l'algorithme avec $\alpha \neq 0$ mais on ne trouverait rien d'autre car on poursuivrait avec X^2+1 comme reste, or on sait déjà qu'il divise P.

Le polynôme X^2+1 est irréductible sur $\mathbb{F}_3$. Il faut ensuite recommencer avec le facteur

$$X^7-X^5+X^4+X^3-X^2-X+1$$

Nous avons

$$\begin{aligned} X^7 &= X^5 - X^4 - X^3 + X^2 + X - 1 \\ X^9 &= -X^6 + X - 1 \\ X^{12} &= X^6 + X^4 - X^3 - X + 1 \\ X^{15} &= X^6 + X^5 + X^4 + X^2 - X + 1 \\ X^{18} &= X^5 + X^3 - X^2 + X + 1 \end{aligned}$$

et la matirce de $S - I$ est

$$\begin{pmatrix} 0 & 0 & 0 & -1 & 1 & 1 & 1 \\ 0 & -1 & 0 & 1 & -1 & -1 & 1 \\ 0 & 0 & -1 & 0 & 0 & 1 & -1 \\ 0 & 1 & 0 & -1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & -1 & 1 & 1 & -1 \end{pmatrix} \begin{matrix} 1 \\ X \\ X^2 \\ X^3 \\ X^4 \\ X^5 \\ X^6 \end{matrix}$$

Nous voyons que le système formé par les six colonnes de droite est de rang maximal donc la dimension du noyau est 1 et P est irréductible.

La décomposition en facteurs irréductibles de $X^9 + X^6 - X + 1$ sur $K = \mathbb{F}_3$ est donc

$$(X^7 - X^5 + X^4 + X^3 - X^2 - X + 1)(X^2 + 1)$$

Exemple 22. 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* 23** (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 24. 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 25. 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 26. Soit $\lambda \in K$, $\lambda \notin \{0, 1\}$. Le polynôme $Y^2 - X(X-1)(X-\lambda)$ est irréductible.

***Théorème* 27** (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 28. Le polynôme $X^2 + Y^2 + 1$ est irréductible dans $\mathbb{R}[X, Y]$.

Il suffit de montrer que le polynôme X^2+Y^2+1 est irréductible dans $\mathbb{C}[X,Y]$, il le sera alors dans $\mathbb{R}[X,Y]$. Si $X^2+Y^2+1=P(X,Y)Q(X,Y)$ dans $\mathbb{C}[X,Y]$ avec P et Q non inversibles on voit d'abord que la seule possibilité est que P et Q soient de degré 1 en X et en Y. Si

$$(aX+bY+c)(a'X+b'Y+c')=X^2+Y^2+1$$

alors $aa'=1$ et on peut choisir $a=a'=1$. On doit alors avoir $b+b'=0$ et $bb'=1$ d'où $b=\mathbf{i}=-b'$ par exemple. Il reste alors à satisfaire $c+c'=c-c'=0$ et $cc'=1$ ce qui n'est pas possible.

On peut aussi passer au quotient par l'idéal (Y).

Exemple 29. 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 30. Soit p un nombre premier, alors X^p-X-1 est irréductible sur $\mathbb{Z}$ (*voir* [Per82]).

***Théorème* 31** ([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 32. 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.

2. 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).

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

a) Un tel L doit être de cardinal q^d puisqu'isomorphe à K^d comme K-espace vectoriel. On sait qu'il existe un tel corps, unique à isomorphisme près. C'est alors bien une extension de K; en effet un corps fini K_2 est extension d'un corps fini K_1 si et seulement si le cardinal de K_2 est une puissance de celui de K_1 (ceci résulte par exemple du fait que dans une clôture algébrique le corps de cardinal p^k (où $k\in\mathbb{N}^*$) est l'ensemble des solutions de l'équation $x^{p^k}=x$).
b) Nous avons $K[\alpha]\subset L$. Réciproquement comme α engendre le groupe fini L^* tout élément de L^* s'écrit α^m avec $m\in\mathbb{N}$. Ainsi $L^*\subset K[\alpha]$. De plus 0 appartient à $K[\alpha]$. Par suite $L=K[\alpha]$.

c) Soit P le polynôme minimal de α. Puisque $L = K[\alpha]$ le corps L est un corps de rupture de α sur K. Comme $[L : K] = d$ le polynôme P est de degré d.

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^*).

Éléments de réponse 2

a) Soit p la caractéristique de K (et de L). On peut écrire q sous la forme p^m avec $m \in \mathbb{N}$. Par suite F est le $m$ième itéré de $F_0\colon x \mapsto x^p$. Or F_0 est un morphisme de corps[1]. En particulier F_0 est injectif. Puisque L est fini il est aussi bijectif; c'est donc bien un automorphisme de L. Par suite c'est aussi le cas de $F = F_0 \circ F_0 \circ \ldots \circ F_0$. Enfin pour tout $x \in K$ nous avons $x^q = x$ puisque K est un corps de cardinal q.
b) Raisonnons par l'absurde, c'est-à-dire supposons que $F^m(\alpha) = \alpha$ pour un certain $0 < m < d$. Cela signifie que $\alpha^{q^m} = \alpha$ et on sait alors que α est dans un corps de cardinal q^m qui est de degré m sur K. Il en résulte que $[K[\alpha] : K] \leqslant m$ ce qui contredit le fait que $L = K[\alpha]$ est de degré d.
c) Soit P le polynôme minimal de α sur K. Puisque F est un automorphisme de corps de L qui induit l'identité sur K nous observons que α, $F(\alpha)$, $F^2(\alpha)$, …, $F^{d-1}(\alpha)$ sont des racines de P; de plus b) assure qu'elles sont deux à deux distinctes. Ainsi P est scindé sur L. Par conséquent, sur un corps fini, corps de rupture coïncide avec corps de décomposition, phénomène aussi vrai sur $\mathbb{R}$ mais pas sur $\mathbb{Q}$ par exemple.
d) Puisque $16 = 4^2$ le corps fini L est une extension de degré 2 de K. Comme L^* est cyclique de cardinal 15 il contient un élément α d'ordre 5. Alors $\alpha^4 \neq \alpha$ (sinon α serait d'ordre divisant 3) ce qui montre que $\alpha \notin K$. En particulier le degré de $K[\alpha]$ sur K est $\geqslant 2$ ce qui montre finalement (comme $K[\alpha] \subset L$) que $L = K[\alpha]$ par égalité des dimensions sur K. Il s'en suit qu'on peut avoir $L = K[\alpha]$ sans que α soit 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.

[1] Le seul point non trivial est de voir que $(x+y)^p = x^p + y^p$ ce qui est vrai dans tout corps de caractéristique p car p divise le coefficient binomial $\binom{p}{k}$ pour tout $1 \leqslant k \leqslant p-1$.

c) Montrer que b) reste vrai si K est un corps fini[2] 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.

Éléments de réponse 3

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

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

est bijective. L'application F est un morphisme de corps[3]. En particulier F est injectif. Puisque K est fini il est aussi bijectif; c'est donc bien un automorphisme de K.

b) Le polynôme P' n'est pas nul car P n'est pas constant et K est de caractéristique zéro. Nous en déduisons l'inégalité $\deg P' < \deg P$ ce qui implique que comme P est irréductible P et P' sont premiers entre eux dans $K[X]$ ou $L[X]$ (rappelons que le pgcd ne dépend pas du corps de base). Ainsi P ne peut avoir une racine multiple dans L.

c) D'après b) le seul problème est quand $P' = 0$ ce qui signifie que P s'écrit

$$P = a_0 + a_1 X^p + \ldots + a_k X^{pk}.$$

D'après a) on peut écrire chaque a_i sous la forme b_i^p avec $b_i \in K$. Alors

$$P = (b_0 + b_1 X + \ldots + b_k X^k)^p$$

ne peut pas être irréductible.

Par contre sur $K = {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}[T]$ le polynôme $P = X^p - T$ vérifie $P' = 0$ (donc il a une racine de multiplicité P sur son corps de décomposition) bien que P soit irréductible sur K (c'est direct si $p = 2$; en général ceci résulte du critère d'Eisenstein en considérant P comme à coefficients dans l'anneau factoriel $K[T]$; à noter qu'on peut aussi utiliser l'argument général de la question d) qui suit).

d) Si K est parfait, la méthode appliquée au cas "K fini" donne le résultat.

Supposons K imparfait. Soit $a \in K^*$ tel que a ne s'écrive pas x^p avec $x \in K^*$. Soit $P \in K[X]$ défini par $P = X^p - a$. Comme $P' = 0$, toute racine de P dans un corps de décomposition est multiple d'ordre p. Il suffit donc de vérifier que P est irréductible sur K. Soit L un corps de décomposition de P sur K. Soit $b \in L$ tel que $b^p = a$. Soit π le polynôme minimal de b sur K qui est irréductible. Il suffit de montrer que $\pi = P$. Puisque $P(b) = 0$, on sait que π divise P. Mais comme $P = (X - b)^p$ dans $L[X]$ nous avons que π s'écrit $(X - b)^r$ dans $L[X]$ avec $1 \leqslant r \leqslant q$. En observant le terme constant nous obtenons que $b^r = q \in K$. Si nous avions $r < p$, alors r serait premier avec p et par Bezout nous aurions u, $v \in \mathbb{Z}$ tels que $ur + vp = 1$ ce qui impliquerait que

$$b = b^{ur+vp} = b^{ur} b^{vp} = (b^r)^u (b^p)^v = a^u a^v$$

serait dans K: contradiction avec le fait que a n'est pas une puissance $p$ième. Finalement $\pi = P$ comme nous le voulions.

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

[2]Indication: utiliser a).

[3]Le seul point non trivial est de voir que $(x + y)^p = x^p + y^p$ ce qui est vrai dans tout corps de caractéristique p car p divise le coefficient binomial $\binom{p}{k}$ pour tout $1 \leqslant k \leqslant p - 1$.

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) ?

Éléments de réponse 4

a) Posons $\alpha\bullet x=\sigma(\alpha)\cdot x$. Puisque σ est un morphisme de corps nous obtenons
   - $1\bullet x=x$ pour tout $x\in L$;
   - $\alpha\bullet(\beta\bullet x)=(\alpha\beta)\bullet x$ pour tous α, $\beta\in K$ et tout $x\in L$;
   - $\alpha\bullet(x+y)=\alpha\bullet x+\alpha\bullet y$ pour tout $\alpha\in K$ et pour tous x, $y\in L$;
   - $(\alpha+\beta)\bullet x=\alpha\bullet x+\beta\bullet x$ pour tous α, $\beta\in K$ et pour tout $x\in L$.

b) Soit $(e_1,e_2,\dots,e_d)$ une base du K-espace vectoriel M; montrons que c'est aussi une base de L'. Soient λ_1, λ_2, …, λ_d dans K tels que

$$\sum_{i=1}^{d}\lambda_i\bullet e_i=0.$$

Alors

$$\sum_{i=1}^{d}\sigma(\lambda_i)\cdot e_i=0.$$

d'où $\sigma(\lambda_i)=0$ pour tout i puis $\lambda_i=0$ puisque σ est injectif. Par conséquent $(e_1,\,e_2,\,\dots,\,e_d)$ est libre dans L'.

Soit maintenant $x\in L'$. Écrivons x sous la forme $\sum_{i=1}^{d}\mu_i e_i$ dans L avec $\mu_i\in K$. Nous obtenons que $x=\sum_{i=1}^{d}\sigma^{-1}(\mu_i)\bullet e_i$ dans L' ce qui montrer que la famille $(e_1,\,e_2,\,\dots,\,e_d)$ est également génératrice dans L'.

c) Par hypothèse le morphisme de corps

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

est un automorphisme de K. Soit L une extension finie de K, qu'on peut voir comme un K-espace vectoriel. Notons L' le K-espace vectoriel défini comme en a). Alors l'application $u\colon x\mapsto x^p$ est un morphisme du K-espace vectoriel L dans le K-espace vectoriel L'. En effet puisque nous sommes en caractéristique p, nous avons $u(x+y)=u(x)+u(y)$. Si α appartient à K et x à L, alors

$$u(\alpha\cdot x)=\alpha^p x^p=\sigma(\alpha)\cdot u(x)=\alpha\bullet x.$$

Comme $\ker u=0$, u est injective. De plus $\dim L=\dim L'$ est finie. Il en résulte que u est donc bijective. Ceci signifie exactement que $x\mapsto x^p$ est bijective de L dans L et donc que L est parfait.

d) Oui. Si F est une extension algébrique de K et si x appartient à F, alors $L:=K[x]$ est une extension finie de K puisque x est algébrique sur K. Nous appliquons c) à L, nous obtenons qu'il existe $y\in L\subset F$ tel que $y^p=x$. Il s'en suit que F est parfait.

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 ?

Éléments de réponse 5

a) Pour tout $n \in \mathbb{N}$ l'ensemble $\mathbb{Q}_n[X]$ des polynômes de degré au plus n est dénombrable car en bijection avec $\mathbb{Q}^{n+1}$. L'ensemble Z_n des éléments de $\overline{\mathbb{Q}}$ qui annulent un polynôme non nul de $\mathbb{Q}_n[X]$ est donc dénombrable puisque chaque polynôme non nul de $\mathbb{Q}_n[X]$ n'a qu'un nombre fini de racines. Nous en déduisons que $\overline{\mathbb{Q}}$ qui est réunion dénombrable des Z_n pour $n \in \mathbb{N}$ est dénombrable.
b) Soit $P = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ un polynôme unitaire à coefficients dans $\overline{\mathbb{Q}}$. Alors $\mathbb{Q}(a_0)$ est un $\mathbb{Q}$-espace vectoriel de dimension finie car a_0 est algébrique sur $\mathbb{Q}$. Par récurrence $K = \mathbb{Q}(a_0, a_1, \ldots, a_{n-1})$ est de dimension finie sur $\mathbb{Q}$ (en effet chaque a_i est algébrique sur $\mathbb{Q}$ donc a fortiori sur $\mathbb{Q}(a_0, a_1, \ldots, a_{i-1})$). Soit x une racine de P, alors x est algébrique sur K par définition donc $K(x)$ est de dimension finie sur K. Comme K est de dimension finie sur $\mathbb{Q}$ nous obtenons que $K(x)$ est de diemnsion finie sur $\mathbb{Q}$ ce qui signifie que x est algébrique sur $\mathbb{Q}$, *i.e.* x appartient à $\overline{\mathbb{Q}}$.
c) Nous venons de voir que $\overline{\mathbb{Q}}$ est un sous-corps algébriquement clos de $\mathbb{C}$ qui contient $\mathbb{Q}$. C'est le plus petit: si L est un tel corps, il contient les racines de tous les polynômes non nuls à coefficients dans $\mathbb{Q}$ donc il contient $\overline{\mathbb{Q}}$. Plus généralement si $\mathbb{F}$ est un corps inclus dans un corps algébriquement clos $\mathbb{F}'$ nous obtenons la clôture algébrique de $\mathbb{F}$ en prenant l'ensemble des éléments de $\mathbb{F}'$ algébriques sur $\mathbb{F}$. La difficulté pour montrer l'existence de la clôture algébrique est qu'il faut d'abord montrer l'existence d'un tel $\mathbb{F}'$ ce qui nécessite entre autres le Lemme de Zorn.
d) Il suffit pour voir cela de trouver des polynômes irréductibles de $\mathbb{Q}[X]$ de degré d arbitrairement grand car une racine x d'un tel polynôme verifiera $[\mathbb{Q}[x] : \mathbb{Q}] = d$ arbitrairement grand (alors que ce nombre serait majorée par la dimension $[\overline{\mathbb{Q}} : \mathbb{Q}]$ si celle-ci était finie). Or le critère d'Eisenstein assure que pour p premier le polynôme $X^d - p$ est irréductible.

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

Éléments de réponse 6

a) Considérons la norme
$$N(a+\mathbf{i}b\sqrt{2}) = a^2+2b^2$$
qui est une fonction multiplicative. Soit $z \in A^\times$. Nous avons $zz' = 1$ soit $N(z)N(z') = 1$ et donc $N(z) = 1$ soit $z = \pm 1$. Pour montrer que A est euclidien remarquons que $\frac{z_1}{z_2}$ 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 $z_1 = qz_2+r$ avec $r = z_1 - qz_2 \in A$ et $N(r) < N(z_2)$.

b) Raisonnons par l'absurde: supposons que x soit pair; alors $y^2 \equiv -2 \bmod 8$: contradiction avec le fait que dans $\mathbb{Z}/8\mathbb{Z}$ les carrés sont 0, 1 et 4.

Dans A nous avons $x^3 = (y+\mathbf{i}\sqrt{2})(y-\mathbf{i}\sqrt{2})$. Soit δ un pgcd de $y+\mathbf{i}\sqrt{2}$ et de $y-\mathbf{i}\sqrt{2}$. Nous avons $\delta = (y+\mathbf{i}\sqrt{2}, (\mathbf{i}\sqrt{2})3)$. Or $\mathbf{i}\sqrt{2}$ est irréductible car de norme 2 et la seule factorisation possible de 2 est 1×2 de sorte que $\mathbf{i}\sqrt{2} = zz'$ implique que $N(z) = 1$ soit z inversible (ou z'). Or $\mathbf{i}\sqrt{2}$ ne divise pas y car sinon y^2 serait pair et donc y pair soit x pair contradiction. Ainsi $\delta = 1$.

Par conséquent $y+\mathbf{i}\sqrt{2}$ et $y-\mathbf{i}\sqrt{2}$ sont des cubes parfaits: $(y\pm\mathbf{i}\sqrt{2}) = (a\pm\mathbf{i}\sqrt{2})^3$ et $x = a^2+2b^2$. En séparant parties réelle et imaginaire nous trouvons alors $y = a^3-6ab^2$ et $1 = b(3a^2-2b^2)$ soit $b = \varepsilon = \pm 1 = 3a^2-2$ ce qui conduit à $b = 1$ et $a = \pm 1$ soit $y = \pm 5$ et $x = 3$ qui est bien une solution de l'équation.

c) 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 $c(a+b\sqrt{2}) = a-b\sqrt{2}$ de sorte que N est multiplicative. Soit $z \in A^\times$; nous avons $N(z) = \pm 1$. Nous pouvons vérifier que A est euclidien pour le stathme $|N|$. Remarquons 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 $x+\sqrt{2}y = \pi_1\pi_2\ldots\pi_r$ 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 $\mathbb{Z}$. Nous avons alors $x^2-2y^2 = N(\pi_1)N(\pi_2)\ldots N(\pi_r)$ et n, au signe près, est un produit de certains de ces $N(\pi_i)$. Il s'ensuit que n est de la forme $N(z) = u^2-2v^2$.

L'égalité $-(u^2-2v^2) = N((1+\sqrt{2})(u+v\sqrt{2}))$ 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 $\equiv \pm 1 \bmod 8$.

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

Éléments de réponse 7 Soit par exemple $x = \sqrt{3}+\sqrt{7}$. Nous pouvons trouver son polynôme minimal comme suit.

Soient A et B deux polynômes irréductibles unitaires sur $\mathbb{Q}$. Le système d'équations
$$A(X) = B(Y-X) = 0$$
possède comme solutions les couples (x_a, x_b+x_a) où x_a (resp. x_b) décrit les solutions de $A(X) = 0$ (resp. $B(X) = 0$). Considérons les polynômes $A(X)$ et $B(Y-X)$ comme des polynômes à valeurs dans $K[Y]$ et introduisons leur résultant qui est un polynôme en Y dont les zéros sont d'après ce qui précède exactement les sommes des zéros de A avec ceux de B.

Ici $A(X) = X^2-3$ et $B(X) = X^2-7$. Le résultant en question est donné par le déterminant
$$\begin{vmatrix} 1 & 0 & -3 & 0 \\ 0 & 1 & 0 & -3 \\ 1 & -2Y & Y^2-7 & 0 \\ 0 & 1 & -2Y & Y^2-7 \end{vmatrix}$$

soit après calcul $Y^4 - 20Y^2 + 16$.

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[4] n'est pas inutile.

Éléments de réponse 8 Montrons pour commencer que si a est un élément d'un corps L de caractéristique p non nulle qui n'a pas de racine $p$ième dans L le polynôme $U = T^p - a$ est irréductible sur L: si b est une racine de U dans une extension N de L le polynôme U se factorise comme $(T - b)^p$ dans $N[T]$. Ainsi si $U = PQ$ est une factorisation non triviale de U en polynômes unitaires de $L[X]$, nous avons $P = (T - b)^k$ avec $0 < k < p$. Le coefficient constant $\pm b^k$ de P appartient à L. Puisque b^p appartient aussi à L, il en est de même pour $b = (b^k)^u \times (b^p)^v$: contradiction.

Posons $N = K(X, Y^p)$. D'après ce qui préceède ${}^{N}\!/_{L}$ et ${}^{M}\!/_{N}$ sont de degré p. Si $\alpha = R(X, Y)$ est un élément quelconque de M, sa puissance $p$ième s'écrit $S(X^p, Y^p)$ où S est la fraction rationnelle obtenue en élevant à la puissance $p$ième chacun des coefficients de R. Par conséquent α^p appartient à L, le degré de α sur L est au plus p. Il s'en suit que ${}^{M}\!/_{L}$ n'est pas monogène d'où le résultat.

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.

a) Montrer que χ_u est irréductible si et seulement si V n'a pas de sous-espace stable par u;
b) Montrer que u est cyclique avec π_u une puissance d'un polynôme irréductible si et seulement si V est indécomposable sous u;
c) Proposer un algorithme pour tester si u est semi-simple.

Éléments de réponse 9

a) Montrons que χ_u est irréductible si et seulement si V n'a pas de sous-espace stable par u.

   Si V a un sous-espace stable W par u, alors en complétant une base de W en une base de V la matrice de u y est diagonale par bloc et son polynôme caractéristique est divisible par celui de $u_{|W}$.

   Réciproquement si χ_u est de la forme PQ avec P et Q premiers entre eux, alors le lemme des noyaux décompose l'espace en une somme directe de $\ker P(u)$ et de $\ker Q(u)$. Si $\chi_u = P^r$ avec P irréductible, nous avons alors $E = \ker P$, *i.e.* $\pi_u = P$. Soit x quelconque non nul; l'espace vectoriel engendré par x, $u(x)$, $u^2(x)$, ... est donc au plus de dimension $\deg P$ et par hypothèse est donc égal à l'espace tout entier, c'est-à-dire $r = 1$.

b) Montrons que u est cyclique avec π_u une puissance d'un polynôme irréductible si et seulement si V est indécomposable sous u.

   Commençons par montrer que si u est cyclique avec π_u une puissance d'un polynôme irréductible, alors V est indécomposable sous u. En utilisant la structure de $K[X]$-module sur V induite par u nous avons $V \simeq {}^{K[X]}\!/_{(\pi_u)}$. Si V était indécomposable il serait en tant que $K[X]$-module isomorphe à un produit direct ${}^{K[X]}\!/_{P_1} \times {}^{K[X]}\!/_{P_2}$ ce qui impose $P_1 = P^r$ et

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

$P_2 = P^s$ avec P irréductible et $\pi_u = P^{r+s}$. Or le polynôme minimal de ce produit direct est $P^{\max(r,s)}$ soit donc $\min(r,s) = 0$.

Réciproquement si V est indécomposable alors u est cylique. Par ailleurs si son polynôme minimal n'était pas une puissance d'un polynôme irréductible, alors le lemme des noyaux[5] contredirait l'indécomposabilité de V.

c) L'endomorphisme u est semi-simple si et seulement si π_u est sans multiplicité, *i.e.* si et seulement si π_u est premier avec π'_u. Nous pouvons tester si u est semi-simple de manière algorithmique: nous calculons le polynôme caractéristique χ_u et nous testons si $\frac{\chi_u}{\chi_u \wedge \chi'_u}$ annule u.

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

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

(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

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

---

[5]Lemme des noyaux. Soient E un espace vectoriel sur un corps commutatif K et f un endomorphisme de E. Si P_1, …, $P_n \in K[X]$ (avec n entier strictement positif) sont premiers entre eux deux à deux, alors les sous-espaces vectoriels $V_i = \ker(P_i(f))$ (où $1 \leqslant i \leqslant n$) sont en somme directe et

$$\bigoplus_{i=1}^{n} \ker\big(P_i(f)\big) = \ker\left(\big(\prod_{i=1}^{n} P_i\big)(f)\right).$$

De plus, la projection de la somme directe V sur V_i parallèlement à $\bigoplus_{j \neq i} V_j$ est la restriction à V d'un polynôme en f.

(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

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

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

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

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

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

Éléments de réponse 10

(1) (i) Nous avons

$$\begin{aligned} |G|^2 &= \sum |a_{i-1} - \alpha a_i|^2 \\ &= \sum \left(|a_{i-1}|^2 + |\alpha a_i|^2 - 2\mathrm{Re}(\alpha a_i \overline{a_{i-1}}) \right) \\ &= \sum \left(|\alpha a_{i-1}|^2 + |a_i|^2 - 2\mathrm{Re}(\alpha a_i \overline{a_{i-1}}) \right) \\ &= \sum |\overline{\alpha} a_{i-1} - a_i|^2 \\ &= |H|^2 \end{aligned}$$

(ii) L'égalité découle directement de (i). Le terme de droite de l'inégalité provient du coefficient de X^m et du coefficient constant.

(iii) Si nous changeons le couple (x_{m-1}, x_m) en $(1, x_{m-1}x_m)$ toutes les contraintes sont encore satisfaites quitte à 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 $(x_1, \ldots, x_m)$ 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 $x_m = M$.
De plus le terme $\binom{m-1}{k-1}$ correspond aux k-uplets contenant x_m et $\binom{m-1}{k}$ à ceux qui ne le contiennent pas.

(iv) Nous en déduisons alors que

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

Ainsi

$$|b_j| \leqslant |b_n|\Big(\binom{n-1}{j}M(B)+\binom{n-1}{j-1}\Big)$$

et donc

$$|b_j| \leqslant |a_m|\Big(\binom{n-1}{j}M(A)+\binom{n-1}{j-1}\Big);$$

en effet comme B divise A, nous avons $M(B) \leqslant M(A)$ et $|b_n| \leqslant |a_m|$. Le résultat découle alors de (ii) qui assure que $M(A) \leqslant \frac{|A|}{|a_m|}$.

(2) (i) Nous pouvons appliquer l'algorithme de Berlekamp pour trouver la factorisation.

(ii) Le terme constant de A étant égal à 1, nous en déduisons que les termes constants de ses facteurs irréductibles sont égaux à ± 1.
Par ailleurs les coefficients de ces facteurs appartiennent à $\{-23, -22, \ldots, 22, 23\}$ 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 nous avons modulo 47

$$12 \times 22 = -18 \qquad 12 \times 13 = 15 \qquad 12 \times 12 = 3.$$

Nous ne trouvons pas ± 1 d'où le résultat.

(iii) Un raisonnement analogue pour les facteurs de degré 3 conduit aux possibilités données par l'énoncé.

(iv) Notons que la première éventualité est exclue car $b_2 \leqslant 12$ d'après les majorations de (1). Testons alors la divisibilité de la seconde possibilité, nous trouvons

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

(3) Posons

$$D = \frac{C - A_e B_e}{p^e} \in \mathbb{Z}[X].$$

Nous cherchons

$$A_{e+1} = A_e + p^e S \qquad \text{et} \qquad B_{e+1} = B_e + p^e T$$

avec S, $T \in \mathbb{Z}[X]$. La condition $C(X) \equiv A_{e+1}(X)B_{e+1}(X) \bmod p^{e+1}$ est équivalente, puisque $2e \geqslant e+1$, à $A_e T + B_e S \equiv D \bmod p$. La solution générale est alors $S \equiv VD + WA_e \bmod p$ et $T \equiv UD - WB_e \bmod p$ 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) Choisissons p tel que A modulo p soit sans facteur carré. Factorisons via Berlekamp. Avec le Lemme de Hensel nous remontons la factorisation modulo p^e pour e assez grand tel que p^e soit supérieur à deux fois la borne trouvée dans (1). Nous essayons alors les différentes combinaisons possibles de factorisation comme dans (3).

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 ?

Éléments de réponse 11

(1) Le corps K est corps de rupture du polynôme $P = X^2 + 13$.

La première assertion découle du calcul de l'anneau des entiers d'un corps quadratique.

Pour calculer la décomposition des idéaux premiers il suffit (cf cours) de réduire le polynôme P. Nous avons $P \equiv (X+1)^2 \bmod 2$, $P \equiv X^2 \bmod 13$ et P est 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) La constante de Minkowski de K vaut

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

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 nous avons 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 $\mathfrak{d} \,|\, 2\sqrt{13}\mathcal{O} = \mathfrak{p}2\mathfrak{q}$. Ainsi les seuls (idéaux) diviseurs premiers de $\mathfrak{d}$ sont au plus $\mathfrak{p}$ et $\mathfrak{q}$.

(4) Nous avons

$$(y - \sqrt{-13})\mathcal{O} = \sigma\big((y + \sqrt{-13})\mathcal{O}\big) = \sigma\big(\mathfrak{c}\mathfrak{p}^\alpha\mathfrak{q}^\beta\big) = \sigma(\mathfrak{c})\mathfrak{p}^\alpha\mathfrak{q}^\beta.$$

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) Écrivons $(y+\sqrt{-13})\mathcal{O} = \mathfrak{c}'\mathfrak{p}^\alpha\mathfrak{q}^\beta$ où $\mathfrak{c}'$ est un idéal de $\mathcal{O}$ qui n'est divisible ni par $\mathfrak{p}$, ni par $\mathfrak{q}$. Nous avons

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

cette dernière décomposition étant en quatre facteurs premiers entre eux deux à deux. Nous en déduisons 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 donc 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) Notnos $u+v\sqrt{-13}$ un générateur de l'idéal $\mathfrak{c}\mathfrak{p}^a\mathfrak{q}^b$. Le cube de cet entier est un générateur de $(y+\sqrt{-13})\mathcal{O}$, *i.e.* il vaut $\pm(y+\sqrt{-13})$. En changeant si besoin les signes de u et v nous choisissons le signe positif d'où l'équation $y+\sqrt{-13} = (u+v\sqrt{-13})^3$ qui donne celles de l'énoncé.

(8) La deuxième équation impose $v=-1$ 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.

Exercice 12

(1) Le critère d'irréductibilité d'Eisenstein. Si ℓ est un nombre premier et si $x \in \mathbb{Q}\smallsetminus\{0\}$, 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 $T(X)=\sum_i t_iX^i \in \mathbb{Q}[X]\smallsetminus\{0\}$, 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 $\mathbb{Z}[X]$.

Éléments de réponse 12

(1) a) Le contenu de A' vaut 1. Ainsi pour tout $\ell \in P$ nous avons $v_\ell(a'_i) \geqslant 0$ et $a_i \in \mathbb{Z}$. Enfin puisque $v_p(a_n) = 0$ et $v_p(a_i) \geqslant 0$ il suit que $v_p(\mathrm{Cont}(A)) = 0$. Par suite $v_p(a'_i) = v_p(a_i)$ pour tout $0 \leqslant i \leqslant n$.

b) C'est la propriété universelle des anneaux de polynômes. L'inégalité sur les degrés est immédiate.

c) Le lemme de Gauss assure que $\mathrm{Cont}(A) = \mathrm{Cont}(B)\mathrm{Cont}(C)$ donc $A' = B'C'$ et $\pi(A') = \pi(a'_n)X^n = \pi(B')\pi(C')$. Comme X est irréductible dans $\mathbb{F}_p[X]$ nous obtenons

$$\pi(B') = \beta X^{t'} \qquad \pi(C') = \gamma X^{s'} \qquad \text{avec } t' + s' = n.$$

Or $t + s = n$ et puisque $t' \leqslant t$, $s' \leqslant s$ nous avons $t' = t$ et $s' = s$.

d) L'évaluation en $X = 0$ de l'égalité $A' = B'C'$ donne $a_0 = B'(0)C'(0)$. Si $s > 0$, $t > 0$, alors d'après la question précédente $p \,|\, B'(0)$, $p \,|\, C'(0)$. Ainsi $p^2 \,|\, a_0$: contradiction.

(2) a) Nous avons $X^p - 1 = \Phi_1(X)\Phi_p(X)$. Ainsi

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + 1 \in \mathbb{Z}[X].$$

b) L'égalité $\Phi_p(1) = p$ découle de la formule précédente. Enfin

$$\Phi_p(X + 1) = \frac{(X + 1)^p - 1}{X}$$

et puisque $\binom{p}{i} = 0 \bmod p$ pour $0 < p < i$ nous avons

$$(X + 1)^p = 1 + X^p + pXR(X) \in \mathbb{Z}[X]$$

où $R \in \mathbb{Z}[X]$.

c) Le critère d'Eisenstein permet de montrer l'irréductibilité dans $\mathbb{Q}[X]$. De plus le contenu vaut 1 d'où l'irréductibilité dans $\mathbb{Z}[X]$.

(3) a) Remarquons que

$$X^{p^r} - 1 = \Phi_{p^r}\Phi_{p^{r-1}} \ldots \Phi_p\Phi_1 = \Phi_{p^r}(X^{p^{r-1}} - 1).$$

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

b) En utilisant (2)b) nous obtenons

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

c) Le critère d'Eisenstein permet de montrer l'irréductibilité dans $\mathbb{Q}[X]$. De plus le contenu vaut 1 d'où l'irréductibilité 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 $nI_n \geqslant 2 + (p-2)\frac{p^n-1}{p-1}$.

Éléments de réponse 13

(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.

Puisque L est l'ensemble des racines dans L de $X^q - X$, il suit que P est un produit de polynômes de degré 1 à coefficients dans L. Ainsi il existe $x \in L$ avec $P(x) = 0$. Nous avons $\mathbb{F}_p[x] \subset L$ et donc par le théorème de la base télescopique[6] $d = \dim_{\mathbb{F}_p} \mathbb{F}_p[X]$ divise $\dim_{\mathbb{F}_p} L = n$.

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

Soit $K \supset L$ un corps de décomposition de $P \in K[X]$. Soit $x \in L$ une racine de P. Alors $\mathbb{F}_p[x] \simeq {}^{\mathbb{F}_p[X]}\!/_{P\mathbb{F}_p[X]}$ est un corps fini de cardinal p^d. Ainsi $x^{p^d} = x$ et donc P divise $X^{p^d} - X$ dans $\mathbb{F}_p[X]$.

Comme $d|n$, nous avons $p^d - 1 | p^n - 1$. Par suite $X^{p^d-1} - X$ divise $X^{p^n-1} - X$. Finalement

$$P \,|\, (X^{p^d} - X) \,|\, (X^{p^n} - X).$$

(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 $p^n = \sum_{d|n} dI_d$.

On écrit la décomposition en irréductibles de $X^q - X$ dans $\mathbb{F}_p[X]$ et on en déduit une partition des racines de $X^q - X$ par leur polynôme irréductible.

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

C'est une conséquence immédiate de l'égalité précédente.

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

Nous avons

$$nI_n = p^n - \sum_{\substack{d \mid n \\ d \neq n}} dI_d \geqslant p^n - \sum_{\substack{d \mid n \\ d \neq n}} p^d \geqslant p^n - \sum_{1 \leqslant d \leqslant n-1} p^d.$$

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

Nous avons $nI_n \geqslant p^n - p\frac{p^{n-1}-1}{p-1} = 2 + (p-2)\frac{p^n-1}{p-1}$. En particulier $I_n \geqslant 1$.

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.

[6] Théorème de la base télescopique ([Per82, Chapitre III, Théorème 1.4, page 65]: soient $K \subset L \subset M$ des corps, $(e_i)_{i\in I}$ une base de L sur K, $(f_j)_{j\in J}$ une base de M sur L. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de M sur K.

Éléments de réponse 14

(1) Remarquons que $(-1)^2 = 1$, ainsi -1 appartient à $A^\times$ et son ordre est 1 ou 2. Le théorème de Lagrange assure qu'il n'est pas 2 et donc $1 = -1$ dans A. Ainsi $2 \times 1_A = 0$ et le noyau du morphisme canonique υ de $\mathbb{Z}$ dans A qui envoie $1 \in \mathbb{Z}$ sur 1_A est contenu dans $2\mathbb{Z}$. Puisque υ n'est pas le morphisme nul $\ker \upsilon = 2\mathbb{Z}$. Le théorème de factorisation assure donc que $\mathbb{F}_2$ s'injecte dans A et son image $\{0, 1_A\}$ est un sous-corps de A isomorphe à $\mathbb{F}_2$.

(2) Par construction $B \subset A$ et donc $B^\times \subset A^\times$. Puisque $A^\times \subset B$ nous obtenons $A^\times = B^\times$.

(3) Cela découle de la propriété universelle des anneaux de polynômes.

(4) Par construction $\operatorname{im} \rho = \mathbb{F}_2[\xi]$ et c'est le plus petit sous-anneau de A contenant ξ et donc $A^\times$. Il en résulte que $\operatorname{im} \rho = B$. Le noyau de ρ est un idéal monogène ($\mathbb{F}_2[X]$ est un anneau principal) non nul et comme $\rho(X^5 - 1) = 0$ le résultat suit.

(5) Nous avons
$$X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1).$$
Le polynôme $X^4 + X^3 + X^2 + X + 1$ n'a pas de racine dans $\mathbb{F}_2$ et n'est pas égal à
$$(X^2 + X + 1)^2 = X^4 + X^2 + 1.$$
Puisque X^2+X+1 est le seul irréductible de degré 2 dans $\mathbb{F}_2[X]$, le polynôme $X^4+X^3+X^2+X+1$ est irréductible dans $\mathbb{F}_2[X]$. Ainsi
$$1, \qquad X - 1, \qquad X^4 + X^3 + X^2 + X + 1, \qquad X^5 - 1$$
sont les diviseurs de $X^5 - 1$ dans $\mathbb{F}_2[X]$.

(6) Puisque $S(X) \neq 1$ l'anneau B est
- ◇ soit isomorphe à $B_1 = {}^{\mathbb{F}_2[X]}\!/_{(X-1)} = \mathbb{F}_2$,
- ◇ soit isomorphe à $B_2 = {}^{\mathbb{F}_2[X]}\!/_{(X^4+X^3+X^2+X+1)} \simeq \mathbb{F}_{2^4}$
- ◇ ou soit isomorphe à $B_3 = {}^{\mathbb{F}_2[X]}\!/_{(X^5-1)} \simeq B_1 \times B_2$ par le théorème des restes chinois.

Dans tous les cas nous avons une contradiction avec $|B^\times| = 5$.

References

[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.