

Feuille 4

Anneaux – Polynômes

- 1.a. Soient  $P \in \mathbf{C}[X]$  et  $F \in \mathbf{C}(X)$  tels que  $P(F(X)) \in \mathbf{C}[X]$ . Montrer que  $P$  est constant ou que  $F \in \mathbf{C}[X]$ .
  - 1.b. Soit  $P \in \mathbf{C}[X]$  qui vérifie  $P(X^2) = P(X)P(X+1)$ . Montrer que les racines de  $P$  sont toutes égales à 0 ou 1. Montrer que  $P$  est nul ou une puissance de  $X(X-1)$ .
  - 1.c. Existe-t-il une fraction rationnelle  $F \in \mathbf{C}(X)$  telle que  $F(X)^2 = (X^2+1)^3$  ?
  2. Soit  $A$  un anneau commutatif. Posons  $P = X(1-X) \in A[X]$ .
    - 2.a. Donner un exemple où on a  $P(a) = 0$  ( $a \in A$ ).
    - 2.b. Peut-on trouver un tel exemple avec  $A$  de cardinal 2, 3, 4 ?
    - 2.c. Peut-on trouver un tel exemple avec  $A$  infini ?
    - 2.d. Peut-on trouver un tel exemple avec  $A$  infini et intègre ?
  3. Soient  $a, b$  des entiers  $> 0$  et  $d = \text{pgcd}(a, b)$ . Montrer que, dans  $\mathbf{Z}[X]$ ,  $\text{pgcd}(X^a - 1, X^b - 1) = X^d - 1$ .
  4. Soit  $A$  un anneau commutatif. Si  $A$  est un corps, on sait que  $A[X]$  est un anneau principal. Supposons que  $A$  ne soit pas un corps. Soit  $a \in A$  un élément non inversible et non nul.
    - 4.a. Montrer que l'idéal engendré par  $a$  est distinct de  $A$ .
    - 4.b. Soit  $I$  l'idéal de  $A[X]$  engendré par  $a$  et  $X$ . Montrer que cet idéal n'est pas principal.
  5. Soit  $P = aX^3 + bX^2 + cX + d \in \mathbf{Z}[X]$ .
    - 5.a. Montrer que si  $P$  est réductible, il admet une racine  $u/v \in \mathbf{Q}$  (où  $u$  et  $v$  sont des entiers premiers entre eux). Montrer qu'alors  $u|d$  et  $v|a$ .
    - 5.b. En déduire un algorithme pour déterminer si  $P$  est irréductible.
    - 5.c. Montrer que le polynôme  $X^3 + 274X^2 + 721X + 13$  est irréductible sur  $\mathbf{Q}$ .
  - 6.a. Donner la décomposition en polynômes irréductibles de  $X^5 - 1 \in \mathbf{F}_2[X]$ .
  - 6.b. Soit  $P \in \mathbf{F}_{11}[X]$  un polynôme irréductible de degré 2. Montrer que  $k = \mathbf{F}_{11}[X]/(P)$  est un corps à 121 éléments, puis que tout élément non nul de  $k$  est d'ordre divisant 120.
  - 6.c. Montrer que 7 n'est pas une puissance cinquième dans  $k$ .
  - 6.d. En déduire que  $X^5 - 7 \in \mathbf{Q}[X]$  est irréductible.
7. Soit  $p$  un nombre premier. Soit  $\mathbf{F}_q$  un corps à  $q = p^k$  éléments.
    - 7.a. Montrer que  $8|q^2 - 1$  (lorsque  $p \neq 2$ ). En déduire que le polynôme  $X^4 + 1 \in \mathbf{F}_p[X]$  est réductible.
    - 7.b. Montrer que  $X^4 + 1 \in \mathbf{Q}[X]$  est irréductible.
    - 7.c. Soit  $n$  un entier  $\geq 1$ . Montrer que si le groupe  $(\mathbf{Z}/n\mathbf{Z})^*$  n'est pas cyclique, le polynôme cyclotomique  $\Phi_n$  est réductible dans  $\mathbf{F}_p[X]$  pour tout nombre premier  $p$ .
  8. Montrer que le polynôme  $X^3 + X + 1$  est irréductible sur le corps  $\mathbf{Q}(i)$ .
    - 9.a. À quelle condition sur le nombre rationnel  $a$ , le polynôme  $X^4 - a$  est-il irréductible ?
    - 9.b. À quelle condition sur le nombre entier  $a$ , le polynôme  $X^4 - aX - 1$  est-il irréductible ?
  - 10.a. Soit  $P \in \mathbf{Z}[X]$  un polynôme unitaire de degré  $d$ . Notons  $T$  l'ensemble composé de 1,  $-1$ , des nombres premiers et des opposés des nombres premiers. Supposons que  $\{n \in \mathbf{Z}/P(n) \in T\}$  possède au moins  $2d + 1$  éléments. Montrer que  $P$  est irréductible sur  $\mathbf{Q}$ .
  - 10.b. Montrer que  $P(X) = X^4 - 10X^2 + 1$  est irréductible sur  $\mathbf{Q}$  en calculant ses valeurs en 0, 2, 4, 6 et 8.
11. Considérons l'ensemble  $E$  des polynômes  $P \in \mathbf{Q}[X]$  tels que  $P(n) \in \mathbf{Z}$  pour tout  $n \in \mathbf{Z}$ . Posons, pour  $n$  entier  $\geq 1$ ,  $B_n(X) = X(X-1)\dots(X-n+1)/n! \in \mathbf{Q}[X]$ .
    - 11.a. Montrer que  $B_n \in E$  ( $n$  entier  $\geq 0$ ).
    - 11.b. Montrer que  $E$  est un  $\mathbf{Z}$ -module.
    - 11.c. Quels sont les éléments de  $E$  de degré 1, de degré 2, de degré 3 ?

- 11.d. Montrer que pour tout  $Q \in \mathbf{Q}[X]$  de degré  $d$ , il existe un unique  $(c_0, c_1, \dots, c_d) \in \mathbf{Q}^n$  tel que  $Q = c_0B_0 + \dots + c_nB_n$ . Donner le lien entre  $c_0, c_1, \dots, c_n$  et  $Q(0), Q(1), \dots, Q(n)$ .
- 11.e. Montrer que  $Q \in E$  si, et seulement si, on a  $c_0, c_1, \dots, c_n \in \mathbf{Z}$ .
- 11.f. Soit  $P \in \mathbf{Q}[X]$  de degré  $d$ . Montrer que  $P \in E$  si et seulement si  $P(0), P(1), \dots, P(n)$  sont tous entiers. En déduire que  $P \in E$  si et seulement si  $P$  prend des valeurs entières en  $n + 1$  entiers consécutifs.
- 11.g. Soit  $P \in \mathbf{Q}[X]$ . Montrer que  $P \in E$  si et seulement si  $P$  prend des valeurs entières en un nombre infini d'entiers consécutifs.
12. Soit  $x \in \mathbf{R}$ . Considérons la fonction  $f_x$  de classe  $\mathcal{C}^\infty$  qui au nombre réel  $t$  associe  $te^{tx}/(e^t - 1)$ .
- 12.a. Montrer que le développement en série entière de  $f_x$  en 0 est de la forme  $f_x(t) = \sum_{k=0}^{\infty} B_k(x)t^k/k!$ , où  $B_k$  est un polynôme de degré  $k$  de  $\mathbf{Q}[X]$  (c'est le  $k$ -ème *polynôme de Bernoulli*).
- 12.b. Calculer  $B_0, B_1, B_2$ .
- 12.c. Soient  $k$  et  $n$  des entiers  $> 0$ . Montrer la formule  $B_k(X) = n^{k-1} \sum_{a=0}^{n-1} B_k((X+a)/n)$  (on pourra traduire cette formule en une formule sur  $f_x$ ).
- 12.d. Soit  $k$  un entier  $> 0$ . Montrer la formule  $B_k(X+1) - B_k(X) = kX^{k-1}$  (le polynôme  $B_k$  est la "primitive discrète" de  $kX^{k-1}$ ). Montrer que  $\int_x^{x+1} B_k(u) du = x^k$ . Cette dernière formule caractérise-t-elle uniquement  $B_k$  ?
- 12.e. Soient  $k$  et  $n$  des entiers  $> 0$ . Donner une formule pour  $\sum_{i=1}^n i^{k-1}$  à l'aide de  $B_k$ . Application à  $k = 3$ .
- 13.a. Soit  $n$  un entier  $\geq 1$ . Montrer que  $X^n - Y$  est irréductible dans  $\mathbf{C}[X, Y]$ .
- 13.b. Montrer que  $X^n + Y^n - 1$  est d'Eisenstein relativement à l'élément premier  $Y - 1$ . En déduire qu'il est irréductible dans  $\mathbf{C}[X, Y]$ .
- 13.c. Montrer que la réduction modulo  $Y + 1$  de  $X^n + (Y + 5)X + (Y - 1)$  est irréductible dans  $\mathbf{Q}[X]$  est irréductible. En déduire qu'il est irréductible dans  $\mathbf{Q}[X, Y]$ .
14. Posons  $\mathbf{Z}[i] = \{a + ib \in \mathbf{C}/a, b \in \mathbf{Z}\}$ .
- 14.a. Montrer que c'est un sous-anneau de  $\mathbf{C}$ . Est-ce un anneau intègre ?
- 14.b. Montrer que l'application  $\mathbf{Z}[i] \rightarrow \mathbf{Z}[i]$  qui à  $z$  associe  $\bar{z}$  est un isomorphisme d'anneaux.
- 14.c. Posons, pour  $z \in \mathbf{C}$ ,  $N(z) = z\bar{z}$ . Montrer qu'on a  $N(zz') = N(z)N(z')$ . En déduire que si  $z \in \mathbf{Z}[i]^*$ , on a  $N(z) = 1$  ou  $-1$ .
- 14.d. Montrer que  $\mathbf{Z}[i]^* = \{1, -1, i, -i\}$ .
- 14.e. Montrer que tout nombre complexe s'écrit comme somme d'un élément de  $\mathbf{Z}[i]$  et d'un nombre complexe de module  $< 1$ . Soit  $z \in \mathbf{Z}[i]$ , et  $d \in \mathbf{Z}[i]$ ,  $d \neq 0$ . Montrer qu'il existe  $q \in \mathbf{Z}[i]$ , et  $r \in \mathbf{Z}[i]$  avec  $N(r) < N(d)$  tels que  $z = dq + r$ . en déduire que  $\mathbf{Z}[i]$  est un anneau euclidien.
- 14.f. Soit  $I$  un idéal non nul de  $\mathbf{Z}[i]$ . Soit  $a \in I$ , tel que  $N(a)$  soit minimal dans  $\{N(b)/b \in \mathbf{Z}[i], b \neq 0\}$ . Montrer que l'idéal  $I$  est engendré par  $a$ . L'anneau  $\mathbf{Z}[i]$  est-il principal ?
- 14.g. Montrer qu'on a un homomorphisme d'anneaux  $\mathbf{Z}[X] \rightarrow \mathbf{Z}[i]$  qui à  $P$  associe  $P(i)$ . Montrer que le noyau est engendré par le polynôme  $X^2 + 1$ . En déduire qu'on a un isomorphisme d'anneaux  $\mathbf{Z}[X]/(X^2 + 1)\mathbf{Z}[X] \rightarrow \mathbf{Z}[i]$ .
15. Soit  $p$  un nombre premier impair.
- 15.a. Montrer que 2 n'est pas irréductible dans  $\mathbf{Z}[i]$ .
- 15.b. Montrer que s'il existe  $a, b \in \mathbf{Z}$  tels que  $p = a^2 + b^2$ ,  $p$  n'est pas irréductible dans  $\mathbf{Z}[i]$ .
- 15.c. Montrer alors que  $a + ib$  est irréductible dans  $\mathbf{Z}[i]$ .
- 15.d. Supposons  $p$  réductible dans  $\mathbf{Z}[i]$ . Montrer qu'il existe  $a, b \in \mathbf{Z}$  tels que  $p = a^2 + b^2$ .
- 15.e. Montrer que si  $p \equiv 3 \pmod{4}$ , il n'existe pas  $a, b \in \mathbf{Z}$  tels que  $p = a^2 + b^2$ .
- 15.f. Montrer que si  $p \equiv 1 \pmod{4}$ , le groupe  $(\mathbf{Z}/p\mathbf{Z})^*$  admet deux éléments d'ordre 4.
- 15.g. Montrer que l'homomorphisme d'anneaux  $\mathbf{Z} \rightarrow \mathbf{Z}[i]/p\mathbf{Z}[i]$  identifie par passage au quotient  $\mathbf{Z}/p\mathbf{Z}$  à un sous-anneau de  $\mathbf{Z}[i]/p\mathbf{Z}[i]$ .
- 15.h. En déduire que, si  $p \equiv 1 \pmod{4}$ , l'anneau  $\mathbf{Z}[i]/p\mathbf{Z}[i]$  admet au moins 6 éléments  $x$  vérifiant  $x^4 = 1$ .
- 15.i. Montrer que si  $p \equiv 1 \pmod{4}$ , l'anneau  $\mathbf{Z}[i]/p\mathbf{Z}[i]$  n'est pas un corps. En déduire que l'idéal  $p\mathbf{Z}[i]$  n'est pas premier.
- 15.j. Montrer que si  $p \equiv 1 \pmod{4}$ , il existe  $a, b \in \mathbf{Z}$  tels que  $p = a^2 + b^2$ .
16. Posons  $P = X^2 + Y^2 - 1$  dans  $\mathbf{R}[X, Y]$ . Notons  $A$  l'anneau quotient  $\mathbf{R}[X, Y]/(P)$  et  $B = \mathbf{R}[X]$ . Notons  $x$  et  $y$  les classes respectives de  $X$  et  $Y$  dans  $A$ .

- 16.a. Soit  $F \in \mathbf{R}[X, Y]$ . Montrer qu'il existe un unique  $(Q, R_1, R_2) \in \mathbf{R}[X, Y] \times \mathbf{R}[X] \times \mathbf{R}[X]$  tel que  $F = QP + R_1Y + R_2$ .
- 16.b. Montrer qu'on a un homomorphisme injectif d'anneaux  $\mathbf{R}[X] \rightarrow A$  qui à  $F$  associe  $F(x)$ .
- 16.c. Montrer que  $A$  est un  $\mathbf{R}[X]$ -module de base  $(1, y)$  (*i.e.* tout élément de  $A$  s'écrit de façon unique comme combinaison  $\mathbf{R}[X]$ -linéaire de 1 et  $y$ ).
- 16.d. Soient  $a, b \in \mathbf{R}[X]$ . Déterminer, dans cette base, la matrice de l'endomorphisme de  $\mathbf{R}[X]$ -modules qui à  $F \in A$  associe  $(a + by)F$ . Calculer le déterminant de cette matrice.
- 16.e. Montrer que, si  $(a, b) \neq (0, 0)$  ce déterminant est non nul. En déduire que l'anneau  $A$  est intègre, que ce n'est pas un corps, puis que  $P$  est irréductible dans  $\mathbf{R}[X, Y]$ .
- 16.f. Déterminer  $A^*$ .
- 16.g. Montrer que  $y$  est irréductible dans  $A$ .
- 16.h. Montrer que les anneaux  $A/(y)$  et  $\mathbf{R}[X]/(X^2 - 1)$  sont isomorphes.
- 16.i. Montrer que  $A$  n'est pas factoriel.
- 16.j. Le sous-anneau de l'ensemble des fonctions  $\mathbf{R} \rightarrow \mathbf{R}$  engendré par les fonctions sinus et cosinus est-il factoriel ?
17. Soit  $A$  un anneau intègre et commutatif. Considérons la suite  $(A_n)_{n \geq 0}$  de sous-ensembles de  $A$  donnée par  $A_0 = \{0\}$  et la récurrence  $A_{n+1} = A_n \cup \{x \in A, A = Ax + A_n\}$ .
- 17.a. Déterminer  $A_1$ .
- 17.b. Lorsque  $A = \mathbf{Z}$ , déterminer  $A_2, A_3$ .
- 17.c. Montrer que l'anneau  $A$  est euclidien si et seulement si  $A = \cup_{n \geq 0} A_n$ .
- 17.d. Supposons  $A$  euclidien. Montrer qu'il existe  $x \in A - A^*$  tel que la restriction à  $A^* \cup \{0\}$  de surjection canonique  $A \rightarrow A/Ax$  soit surjective. En déduire que  $A/Ax$  est un corps.
18. Posons  $\alpha = (1 + i\sqrt{19})/2 \in \mathbf{C}$ . Considérons  $A = \mathbf{Z}[\alpha] = \{a + b\alpha \in \mathbf{C}/a, b \in \mathbf{Z}\}$ .
- 18.a. Montrer que c'est un anneau isomorphe à  $\mathbf{Z}[X]/(X^2 - X + 5)$ .
- 18.b. Déterminer  $A^*$ .
- 18.c. Montrer que le polynôme  $X^2 - X + 5$  est irréductible sur les corps  $\mathbf{F}_2$  et  $\mathbf{F}_3$ .
- 18.d. En déduire que  $A$  n'est pas euclidien en utilisant le critère de l'exercice précédent.
- 18.e. Soient  $a$  et  $b$  deux éléments non nuls de  $A$ . Montrer qu'il existe  $q, r \in A$  tels que  $a = bq + r$  ou  $2a = bq + r$  avec  $r = 0$  ou  $N(r) < N(b)$  (où  $N(z)$  désigne la norme d'un nombre complexe  $z$ ). Pour cela on pourra écrire  $a/b = u + v\alpha$  avec  $u, v \in \mathbf{Q}$  et considérer les entiers  $s$  et  $t$  les plus proches de  $u$  et  $v$  respectivement ; dans le cas où  $|t - v| \leq 1/3$ , on posera  $q = s + t\alpha$ , sinon on étudie la division de  $2a$  par  $b$  par le même procédé.)
- 18.f. Montrer que l'idéal principal engendré par 2 est maximal.
- 18.g. Soit  $I$  un idéal de  $A$ . Soit  $b \in I$  tel que  $N(b)$  soit minimal parmi les normes des éléments non nuls de  $A$ . Montrer qu'on a les inclusions  $2I \subset bA \subset I$ , puis que  $I$  est principal.
19. On considère  $\phi : \mathbf{C}[X, Y] \rightarrow \mathbf{C}[T]$  qui à un polynôme  $P(X, Y)$  associe le polynôme  $P(T^2, T^3)$ .
- 19.a. Indiquer brièvement pourquoi  $\phi$  est un morphisme d'anneaux.
- 19.b. Montrer que pour tout  $P \in \mathbf{C}[X, Y]$ , il existe  $Q \in \mathbf{C}[X, Y], R_2, R_1, R_0 \in \mathbf{C}[Y]$  tel que  $P(X, Y) = (X^3 - Y^2)Q + R_2X^2 + R_1X + R_0$ . En déduire que le noyau de  $\phi$  est l'idéal engendré par le polynôme  $X^3 - Y^2$ .
- 19.c. Montrer que  $\text{Im}(\phi) = \mathbf{C} + T^2\mathbf{C}[T]$  et que  $T^2$  et  $T^3$  sont irréductibles dans  $\text{Im}(\phi)$ .
- 19.d. En déduire que l'anneau quotient  $\mathbf{C}[X, Y]/(X^3 - Y^2)$  n'est pas factoriel.
20. Soient  $A$  un anneau intègre et  $K$  son corps de fractions. On dit qu'un élément  $x \in K$  est *entier* sur  $A$  s'il est racine d'un polynôme unitaire de  $A[X]$ . On dit que  $A$  est *intégralement clos* si tous les éléments entiers de  $K$  sont dans  $A$ .
- 20.a. Montrer qu'un anneau factoriel est intégralement clos.
- 20.b. Soit  $d$  un entier sans facteur carré, avec  $d \equiv 1 \pmod{4}$ . Notons  $\sqrt{d}$  une racine carrée de  $d$  dans  $\mathbf{C}$ . Montrer que  $(1 + \sqrt{d})/2$  est entier sur  $\mathbf{Z}$ . En déduire que l'anneau  $\mathbf{Z}[\sqrt{d}]$  n'est pas intégralement clos.
21. Soit  $D$  une algèbre à division (*i.e.* un anneau dans lequel tout élément non nul est inversible). Supposons  $D$  fini. Notons  $p$  sa caractéristique. Notons  $\Phi_n$  le  $n$ -ième polynôme cyclotomique.
- 21.a. Notons  $Z$  le centre de  $D$ , c'est-à-dire  $\{x \in D/xy = yx \ (y \in D)\}$ . Montrer que c'est un corps fini. Notons  $q$  son nombre d'éléments. Montrer qu'il existe un entier  $n \geq 1$  tel que  $D$  possède  $q^n$  éléments.

- 21.b. Soit  $x \in D$ . Montrer que  $\{y \in D/xy = yx\}$  est une algèbre à division contenant  $Z$ . Montrer que son ordre est de la forme  $q^{m_x}$  avec  $m_x < n$  si  $x \notin Z$ . Montrer que  $m_x$  divise  $m$ .
- 21.c. Considérons l'action du groupe  $D^*$  sur lui-même par conjugaison. Écrire la formule des classes pour cette action :  $q^n - 1 = \sum_{x \in S} (q^n - 1)/(q^{m_x} - 1)$ , où  $S$  est un système de représentants des orbites sous l'action de  $D^*$  et  $m_x$  es donné ci-dessus.
- 21.d. Montrer que pour tout  $x \in D$ ,  $\Phi_n(q)$  divise  $(q^n - 1)/(q^{m_x} - 1)$ . Dédire de la formule des classes que  $\Phi_n(q)$  divise  $q - 1$ .
- 21.e. Soit  $\zeta$  une racine de l'unité dans  $\mathbf{C}$ . Montrer qu'on a  $|q - \zeta| > |q - 1|$ , si  $\zeta \neq 1$ . En factorisant  $\Phi_n$ , montrer que  $n = 1$ . En déduire que  $D$  est commutatif.
22. Soit  $K_0$  un corps de caractéristique 0. Soient  $P, Q$  et  $R \in K_0[X]$  des polynômes scindés, non constants et deux à deux premiers entre eux tels que  $P + Q = R$ . Notons  $z_0(PQR)$  le nombre de zéros distincts de  $PQR \in K_0[X]$ .
- 22.a. Les polynômes  $P, Q$  et  $R$  ont-ils des zéros communs ?
- 22.b. En posant dans  $K_0(X)$ ,  $F = P/R$  et  $G = Q/R$ , démontrer qu'on a  $F' + G' = 0$ , puis que  $Q/P = -\frac{F'/F}{G'/G}$ .
- 22.c. Posons  $P = a \prod_{i \in I} (X - a_i)^{n_i}$ ,  $Q = b \prod_{j \in J} (X - b_j)^{m_j}$  et  $R = c \prod_{k \in K} (X - c_k)^{l_k}$ , où  $a, b, c \in K_0^*$  et où les familles finies  $(a_i)_{i \in I}$ ,  $(b_j)_{j \in J}$ ,  $(c_k)_{k \in K}$  décrivent des éléments distincts de  $K_0$  et les familles  $(n_i)_{i \in I}$ ,  $(m_j)_{j \in J}$ ,  $(l_k)_{k \in K}$  décrivent des entiers  $\geq 1$ . Calculer  $P'/P$ ,  $Q'/Q$  et  $R'/R$ . En déduire  $F'/F$  et  $G'/G$ .
- 22.d. En posant alors  $N = \prod_{i \in I} (X - a_i) \prod_{j \in J} (X - b_j) \prod_{k \in K} (X - c_k)$ , montrer que  $NF'/F$  et  $NG'/G$  sont des polynômes de degrés  $< z_0(PQR)$ .
- 22.e. En déduire que les degrés de  $P, Q$  et  $R$  sont majorés strictement par  $z_0(PQR)$ .
- 22.f. En déduire que si  $U, V, W \in \mathbf{C}[X]$  sont non constants, premiers entre eux et vérifient  $U^n + V^n = W^n$ , on a  $n \leq 2$ .
23. Soit  $\mathbf{F}_q$  un corps fini à  $q$  éléments. Soit  $P \in \mathbf{F}_q[X]$  un polynôme irréductible de degré  $n$  distinct de  $X$ .
- 23.a. Montrer que  $P$  est sans racine multiple dans une clôture algébrique  $\bar{\mathbf{F}}_q$  de  $\mathbf{F}_q$ .
- 23.b. Montrer que les racines de  $P$  dans  $\bar{\mathbf{F}}_q$  sont des racines de l'unité, et, plus précisément que  $P$  divise  $X^{q^n - 1} - 1$  dans  $\mathbf{F}_q[X]$ .
- 23.c. Montrer que tout corps de rupture de  $P$  est un corps de décomposition.
- 23.d. Montrer que tout polynôme irréductible de  $\mathbf{F}_q[X]$  et de degré divisant  $n$  divise  $X^{q^n} - X$ .
- 23.e. Montrer que le polynôme  $X^{q^n} - X$  est sans racine multiple. En déduire la formule  $\prod_Q Q = X^{q^n} - X$ , où  $Q$  parcourt les polynômes unitaires, irréductibles de  $\mathbf{F}_q[X]$  et de degré divisant  $n$ .
- 23.f. Notons  $i_d$  le nombre de polynômes irréductibles unitaires de degré  $d$  de  $\mathbf{F}_q[X]$ . Établir la formule  $\sum_{d|n} di_d = q^n$ .
- 23.g. Calculer  $i_3$  lorsque  $q = 5$ .
- 23.h. Établir la formule, dans  $\mathbf{Z}[[X]]$ ,  $\prod_P (1 - X^{d^0(P)}) = 1 - qX$ , où le produit porte sur les polynômes irréductibles unitaires de  $\mathbf{F}_q[X]$ .
24. Soit  $\mathbf{F}_q$  un corps fini à  $q$  éléments. Soit  $P \in \mathbf{F}_q[X]$  de degré  $d$ . On va mettre au point une méthode pour factoriser  $P$ . Posons  $A = \mathbf{F}_q[X]/(P)$ .
- 24.a. Donner un moyen de déterminer les facteurs multiples de  $P$ .
- 24.b. Supposons  $P$  sans facteur multiple. Posons  $P = P_1 P_2 \cdots P_n$ , avec  $P_1, \dots, P_n \in \mathbf{F}_q[X]$  irréductibles. Soient  $A, B \in \mathbf{F}_q[X]$ . Montrer qu'on a  $A \equiv B \pmod{P}$  si, et seulement si,  $A \equiv B \pmod{P_i}$  ( $i \in \{1, 2, \dots, n\}$ ).
- 24.c. Montrer que l'image dans  $A$  de  $\{Q \in \mathbf{F}_q[X]/Q^q \equiv Q \pmod{P}\}$  est un sous-anneau  $B$  de  $A$ . C'est l'algèbre de *Berlekamp*. Montrer que les classes modulo  $P$  des polynômes constants forment un sous-anneau de  $B$  isomorphe à  $\mathbf{F}_q$ .
- 24.d. Soient  $i \in \{1, 2, \dots, n\}$  et  $Q \in \mathbf{F}_q[X]$ . Montrer qu'on a  $Q^q \equiv Q \pmod{P_i}$  si et seulement si il existe  $s_i \in \mathbf{F}_q$  tel que  $P_i$  divise  $Q - s_i$ .
- 24.e. Soit  $Q \in \mathbf{F}_q[X]$  tel que  $Q^q \equiv Q \pmod{P}$  et tel que l'image de  $Q$  dans  $B$  est non constante. Montrer que  $\text{pgcd}(P, Q - s) \neq 1$  pour au moins une valeur de  $s \in \mathbf{F}_q$ . En déduire la formule  $P = \prod_{s \in \mathbf{F}_q} (P, Q - s)$ .
- 24.f. Montrer que  $P$  est irréductible si, et seulement si,  $B$  ne contient que des éléments constants.
- 24.g. Montrer que  $A$  est un espace vectoriel sur  $\mathbf{F}_q$  de dimension  $d$  et que l'élévation à la puissance  $q$  dans  $A$  est  $\mathbf{F}_q$ -linéaire. Exprimer  $B$  comme le noyau d'une application linéaire sur  $A$  dont on écrira la matrice.