

Groupes. Anneaux. Arithmétique

Un peu d'histoire : Les mathématiques arabes.

Le moyen âge européen se distingue par une régression scientifique, conséquence de la censure religieuse. C'est dans d'autres civilisations que se retrouve alors l'héritage grec, plus particulièrement les civilisations arabes de Bagdad et de Cordoue du 9ème au 13ème siècle de notre ère. On connaît bien sur l'invention des chiffres « arabes » qui remplacent aujourd'hui les chiffres romains, plus généralement les travaux arabes portent sur l'algèbre (mot provenant de l'arabe Al-Jabr qui signifie en gros : faire passer de l'autre côté du signe égal). Les deux plus grand mathématicien de cette époque sont Al-Khwarismi dont le nom a donné le mot algorithme, et Al Khayyam aussi connu pour être un grand poète. On leur doit surtout la résolution des équations du second degré, des systèmes linéaires et un premier pas dans la résolution des équations d'ordre supérieur. C'est aussi à cette époque qu'apparaît la notion de polynôme, avec en particulier la formule du binôme de... Newton !

*Généralités sur les groupes*

1. Soit  $A$  un ensemble fini muni d'une loi associative et régulière. Montrer que  $A$  est un groupe.  
on montera que l'application  $x \mapsto ax$  est injective.
2. Soient  $H$  et  $K$  deux sous groupes d'un groupe  $G$ . On pose  $HK = \{hk, h \in H, k \in K\}$ .  
Montrer que  $HK$  est un sous groupe de  $G$  si et seulement si  $HK = KH$
3. Soit  $G$  un groupe et  $S$  une partie de  $G$ . On note  $S^{-1}$  l'ensemble des inverses des éléments de  $S$   
Montrer que le sous groupe engendré par  $S$  est l'ensemble des produits  $x_1 \dots x_p$  où les  $x_i$  sont dans  $S \cup S^{-1}$
4. Soit  $G$  un groupe dont tous les éléments sont d'ordre 2
  - (a) Montrer que  $G$  est abélien.  
Désormais, on suppose que  $G$  est fini de cardinal  $n$ .
  - (b) Soit  $H$  un sous groupe strict de  $G$ . Soit  $x$  un élément de  $G - H$ . Démontrer que  $H \cup xH$  est un sous groupe dont le cardinal est égal au double de celui de  $H$
  - (c) Montrer que le cardinal de  $G$  est de la forme  $2^p$  et que  $G$  est isomorphe à  $(\frac{\mathbb{Z}}{2\mathbb{Z}})^p$
5. Théorème de Cayley.  
Soit  $G$  un groupe de cardinal  $n$ .
  - a) Montrer que pour tout élément  $a$  de  $G$  l'application  $s_a : x \rightarrow ax$  de  $G$  dans lui même est une permutation de  $G$ .
  - b) En déduire que  $G$  est isomorphe à un sous groupe de  $\mathfrak{S}_n$ .
6. Morphismes du groupe  $(\mathbb{Q}, +)$  dans le groupe  $(\mathbb{Z}, +)$ .  
soit  $\phi$  un morphisme de  $(\mathbb{Q}, +)$  dans  $(\mathbb{Z}, +)$ .
  - (a) Montrer qu'il existe  $a \in \mathbb{Z}$  tel que  $\text{Im } \phi = a\mathbb{Z}$
  - (b) : Soit  $x_0$  tel que  $\phi(x_0) = a$ . Que dire de  $\phi(\frac{x_0}{2})$ ?
  - (c) Déterminer  $\phi$ .
7. *difficile*. Sous groupes de  $(\mathbb{Z}^n, +)$ .  
On se propose de démontrer que tout sous groupe  $G$  de  $(\mathbb{Z}^n, +)$  est isomorphe à  $(\mathbb{Z}^p, +)$  pour un certain entier  $p$ .
  - (a) Traiter le cas  $n = 1$
  - (b) Soit  $\pi$  la projection sur le dernier facteur qui à  $(x_1, \dots, x_n)$  associe  $x_n$ .  
Montrer qu'il existe  $a \in \mathbb{Z}$  tel que  $\pi(G) = a\mathbb{Z}$
  - (c) Si  $a$  est non nul, soit  $\omega$  un antécédent de  $a$  par  $\pi$  Montrer que l'application
 
$$x \mapsto (x - \frac{\pi(x)}{a}\omega, \frac{\pi(x)}{a})$$
 est un isomorphisme de  $G$  sur  $(\ker \pi \cap G) \times \mathbb{Z}$
  - (d) Déduire des questions précédentes l'existence de  $p$ . (on peut montrer que  $p$  est unique)

8. Soit  $G$  un sous groupe multiplicatif fini de  $\mathbb{C}^*$ . On note  $n$  le cardinal de  $G$ .
- Montrer que tous les éléments de  $G$  sont des racines  $n$  ièmes de l'unité
  - En déduire  $G$
9. classique. ordre du produit de deux éléments
- Soit  $G$  un groupe abélien fini. On suppose que  $G$  possède un élément  $x$  d'ordre 2 et un élément d'ordre 3. Montrer que  $G$  possède un élément d'ordre 6 (considérer le produit  $xy$ )
  - Dans cette question, on prend le groupe  $H = S_3$ . Montrer (sans calcul si possible) que  $G$  ne possède pas d'élément d'ordre 6 bien qu'il possède des éléments d'ordre 2 et 3.
10. Exposant d'un groupe abélien fini
- Soient  $x$  d'ordre  $p$ ,  $y$  d'ordre  $q$ , avec  $p, q$  premiers entre eux. Montrer que  $xy$  est d'ordre  $pq$ .
  - Soient  $x$  d'ordre  $p$ ,  $y$  d'ordre  $q$ , montrer qu'il existe  $z$  d'ordre  $\text{ppcm}(p, q)$ .
  - Soit  $m$  le ppcm de l'ordre de tous les éléments de  $G$ .
  - Caractériser par leur exposant les groupes cycliques. Quel est l'exposant du groupe  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ? Montrer qu'il existe un élément d'ordre  $m$ .  $m$  s'appelle l'exposant de  $G$ .
11. (X) Groupes de cardinal 8  
Soit  $G$  un groupe non commutatif de cardinal 8.
- Montrer que  $G$  possède un élément  $x$  d'ordre 4.
  - Montrer qu'il existe  $y$  tel que la famille  $(x, y)$  engendre  $G$ .
  - difficile. En déduire qu'il y a deux structures de groupe non isomorphes possibles pour un groupe non abélien de cardinal 8. indication : on pourra montrer que  $yx y^{-1} = x^3$  et que  $y^2$  est soit égal à 1 soit égal à  $x^2$ .
12. (centrale).  
cet exercice utilise la forme suivante du théorème de Lagrange : si  $H$  est un sous groupe d'un groupe fini  $G$  alors le cardinal de  $H$  divise celui de  $G$ .  
Soit  $G$  un groupe abélien fini. Soit  $C$  son centre, c'est à dire le sous groupe des éléments qui commutent avec tous les éléments de  $G$ .
- justifier que  $C$  est bien un sous-groupe.  
On suppose que  $\frac{|G|}{|C|}$  est un nombre premier
  - Déterminer pour tout  $x \notin C$  le sous groupe engendré par  $x$  et  $C$ .
  - En déduire que  $G$  est commutatif.  
Finalement que peut on penser de l'hypothèse faite plus haut?
13. classique. difficile. (Ens, centrale) Le théorème de Cauchy.  
Soit  $G$  un groupe fini et  $p$  un nombre premier qui divise le cardinal de  $G$ .  
On pose :
- $$A = \{(x_1, \dots, x_p) \in G^p, x_1 x_2 \dots x_p = e\}$$
- et on note  $f$  l'application de  $G^p$  dans lui même telle que
- $$f(x_1, \dots, x_p) = (x_p, x_1, \dots, x_{p-1})$$
- Trouver les points fixes de  $f$  et le cardinal de  $A$ .
  - Soit  $x \in G^p$ . Calculer selon  $x$  le cardinal de  $f^k(x)$ ,  $k \in \mathbb{Z}$
  - Montrer que le nombre d'éléments de  $G$  d'ordre  $p$  est congru à  $p - 1$  modulo  $p$ .
  - En déduire le théorème de Cauchy :  $G$  possède un élément d'ordre  $p$

14. Donner un exemple de groupe fini commutatif qui n'est pas cyclique.
15. Soit  $G$  un groupe. On suppose que  $\text{card } G$  est un nombre premier. Montrer que  $G$  est cyclique.
16. Soit  $G$  un groupe abélien fini (ayant au moins deux éléments). Montrer que le groupe  $G \times G$  n'est jamais cyclique.
17. Soit  $G$  le groupe des racines  $n$ èmes de l'unité.
- Montrer que pour tout diviseur  $d$  de  $n$   $G$  a exactement un sous groupe de cardinal  $d$  (on pourra utiliser un exercice précédent)
  - En déduire le théorème suivant : Tout sous groupe d'un groupe cyclique est cyclique.
  - Soit  $x$  un élément de  $G$ . Montrer que  $x$  est générateur d'un (unique) sous groupe de  $G$
  - En déduire que

$$\sum_{d|n} \varphi(d) = n$$

18. Résoudre l'équation  $\varphi(n) = 2$ . Existe-t-il un groupe cyclique ayant 3 générateurs ?

Groupe des permutations

19. Ordre d'une permutation.  
Soit  $\sigma$  la permutation de  $[[1, 10]]$  telles que

$$\sigma([[1, 10]]) = [2, 4, 7, 1, 9, 8, 3, 5, 10, 6]$$

Calculer  $\sigma^{1000}$

20. (mines) Le cycle  $(1, 2, \dots, n)$  a-t-il une racine carrée dans  $\mathfrak{S}_n$  ?
21. Conjugaison.
- Montrer que deux cycles de même longueur sont conjugués.
  - Donner une condition nécessaire et suffisante pour que deux permutations soient conjuguées
  - (difficile.) Soient  $M$  et  $N$  deux matrices de permutation. Donner une condition nécessaire et suffisante pour qu'elles soient semblables.
22. Familles génératrices
- Montrer que le groupe des permutations  $\mathfrak{S}_n$  est engendré par les  $n - 1$  transpositions  $(i, i + 1)$ .
  - Montrer qu'une autre famille génératrice est  $\{(1, 2), (1, 2, \dots, n)\}$
  - On suppose que  $n$  est premier. Soit  $\tau$  une transposition et  $s$  un  $n$ -cycle. Montrer que la famille  $\{\tau, s\}$  engendrent  $\mathfrak{S}_n$
23. Montrer que le groupe alterné  $\mathfrak{A}_n$  est engendré par les 3-cycles.
24. difficile. Montrer qu'on ne peut pas trouver  $n - 2$  transpositions qui engendrent  $\mathfrak{S}_n$
25. difficile. Soit  $\phi$  un automorphisme du groupe des permutations. On se propose de montrer que  $\phi$  est intérieur si  $n \neq 6$ , c'est à dire s'écrit  $\phi(s) = \sigma^{-1}s\sigma$  pour un certain  $\sigma$

Soit  $\phi$  un automorphisme.

- Montrer que l'image par  $\phi$  d'une transposition est un produit de  $k$  transpositions à cycles disjoints
- Montrer que  $k$  ne dépend pas de la transposition choisie
- Calculer, pour  $j \in 1..n$  le cardinal de l'ensemble des produits de  $j$  transpositions à cycles disjoints, en déduire que  $k = 1$ .
- En considérant les produits  $(1, i)(1, j)$  établir l'existence d'une permutation  $\sigma$  telle que  $\phi((1, i)) = (\sigma(1), \sigma(i))$
- Conclure

1. On note  $A$  l'anneau  $\mathbb{R}^2$  ( muni des lois addition et produit terme à terme)

- (a) Démontrer que les ensembles  $\{0\} \times \mathbb{R}$  et  $\mathbb{R} \times \{0\}$  sont des idéaux de  $A$ .
- (b) Déterminer les inversibles de  $A$ .
- (c) Soit  $I$  un idéal non trivial de  $A$ . Montrer que  $I$  contient  $(1, 0)$  ou  $(0, 1)$ .
- (d) En déduire que  $I$  est l'un des deux idéaux de la première question.

2. Soit  $A$  un anneau fini intègre. Montrer que  $A$  est un corps.

*indication : étudier les propriétés de l'application  $x \mapsto ax$*

3. (a) Soit  $A$  un anneau commutatif. Montrer que l'ensemble des éléments nilpotents de  $A$  est un idéal.

*indication : calculer  $(x + y)^{n+p}$  si  $x$  est nilpotent d'ordre  $n$  et  $y$  d'ordre  $p$ .*

- (b) Déterminer l'idéal nilpotent de  $\frac{\mathbb{Z}}{n\mathbb{Z}}$  lorsque  $n = 6$  et lorsque  $n = 8$ .

4. (X)

Soit  $A$  une matrice carrée. Montrer que l'ensemble des polynômes tels que  $P(A)$  est nilpotente est un idéal de  $K[X]$ . Quel est son générateur en fonction de  $A$  ?

5. Soit  $A$  un anneau commutatif,  $I$  un idéal. On définit le radical de l'idéal  $I$  en posant :

$$\sqrt{I} = \{x, \exists n, x^n \in I\}$$

- (a) Montrer que  $\sqrt{I}$  est un idéal.
- (b) Démontrer  $\sqrt{\sqrt{I}} = \sqrt{I}$ ,  $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$  lorsque  $I$  et  $J$  sont deux idéaux de  $A$ .
- (c) On dit que  $I$  est primaire si  $I = \sqrt{I}$ . Déterminer les idéaux primaires de  $\mathbb{Z}$

6. Déterminer les inversibles de l'anneau des entiers de Gauss :

$$\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$$

7. *classique. difficile.* Inversibles de l'anneau  $\mathbb{Z}[\sqrt{d}]$ .

Soit  $d$  un entier positif qui n'est pas un carré. On pose  $A = \mathbb{Z}[\sqrt{d}] = \{n + m\sqrt{d}, (m, n) \in \mathbb{Z}^2\}$ .

Pour  $z = n + m\sqrt{d}$  on pose  $\bar{z} = n - m\sqrt{d}$  et  $N(z) = z\bar{z} = n^2 - dm^2$ .

- (a) Montrer que  $N(zz') = N(z)N(z')$ . Montrer que  $z$  est inversible si et seulement si  $N(z) = \pm 1$ .
- (b) Montrer qu'un élément  $z = n + m\sqrt{d}$  inversible est  $> 1$  si et seulement si  $n > 0$  et  $m > 0$ .
- (c) En admettant qu'un tel élément existe, montrer que  $\{z \text{ inversibles}, z > 1\}$  possède un plus petit élément  $z_0$ . Cet élément est appelé unité fondamentale de  $A$
- (d) Montrer qu'alors  $A^* = \{\pm z_0^n, n \in \mathbb{Z}\}$ .
- (e) Déterminer l'unité fondamentale de  $\mathbb{Z}[\sqrt{2}]$  et résoudre dans  $\mathbb{Z}$  les équations  $n^2 - 2m^2 = 1$  et  $n^2 - 2m^2 = -1$  (équations de Pell Fermat)

8. Déterminer les inversibles de  $\frac{\mathbb{Z}}{8\mathbb{Z}}$  et  $\frac{\mathbb{Z}}{9\mathbb{Z}}$ . Forment ils un groupe cyclique ?

9. Trouver le chiffre des unités de  $7^{7^7}$ .

10. Résoudre le système d'équations

$$3x = 2[5], 5x = 1[6]$$

11. Résoudre modulo 37 le système :

$$\begin{aligned} 6x + 7y &= 30 \\ 3x - 7y &= 0 \end{aligned}$$

Plus généralement étudier ce système modulo  $p$  premier.

12. Déterminer les classes des carrés modulo 8. En déduire qu'il existe une infinité d'entiers qui ne sont pas somme de trois carrés.

13. Déterminer les solutions de l'équation  $x^2 + x + 1 = 0$  dans  $\mathbb{Z}/n\mathbb{Z}$

a) pour  $n = 7$

b) pour  $n = 21$

14. (mines) Autour du petit théorème de Fermat.

(a) Soient  $m$  et  $n$  deux entiers.

Montrer que  $m^{19}n = n^{19}m[798]$

(b) On suppose que  $n$  et  $a$  sont deux entiers ayant les propriétés :

$$- a^{n-1} = 1[n]$$

$$- a^k \neq 1[n] \text{ si } k < n - 1$$

Montrer que  $n$  est premier.

15. Soient  $a$  et  $n$  des entiers au moins égaux à 2. Montrer que  $n$  divise  $\varphi(a^n - 1)$

16. (a) Soit  $a$  un entier non nul,  $n$  un entier et  $m$  un nombre premier. Montrer que si  $n$  divise  $a^m - 1$  alors  $n$  divise  $a - 1$  ou  $m$  divise  $\varphi(n)$ .

(b) Soit  $M_m = 2^m - 1$  un nombre de Mersenne ( $m$  est premier). Montrer que tout facteur premier de  $M_n$  est congru à 1 modulo  $2m$ .

17. Soit  $n$  un entier premier à 10

(a) Démontrer qu'il existe un entier  $p$  tel que  $10^p = 1[9n]$ .

(b) Montrer qu'il existe un multiple de  $n$  dont tous les chiffres sont des 1.

18. (centrale)difficile.

(a) Déterminer le nombre d'éléments inversibles modulo 49.

(b) Calculer le plus petit entier  $k$  tel que  $10^k = 1[49]$  (on pourra remarquer que cet entier divise 42).

(c) Déterminer la somme  $\sum_1^{42} \cos\left(\frac{2\pi 10^k}{49}\right)$

19. *classique. difficile.* Carrés modulo  $p$   
Soit  $p$  un nombre premier impair.

(a) Dénombrer les carrés de  $\mathbb{Z}/p\mathbb{Z}^*$ .

*Indication : pour tout  $x$ ,  $-x$  est différent de  $x$*

(b) Montrer que l'ensemble des éléments de  $\mathbb{Z}/p\mathbb{Z}^*$  qui vérifient  $x^{(p-1)/2} = 1$  a un cardinal ne pouvant excéder  $(p-1)/2$ .

(c) Si  $x \in \mathbb{Z}/p\mathbb{Z}^*$ , montrer que  $x$  est un carré si et seulement si  $x^{(p-1)/2} = 1$ .

(d) Montrer que  $-1$  est un carré modulo  $p$  si et seulement si  $p$  est congru à 1 modulo 4.

*Fonctions arithmétiques.*

20. *classique.* On dit qu'une application  $f : \mathbb{N} \rightarrow \mathbb{C}$  est multiplicative si elle vérifie

$$n \wedge m = 1 \implies f(n)f(m) = f(mn)$$

(a) Montrer que si  $n \wedge m = 1$  tout diviseur de  $nm$  s'écrit de façon unique comme produit d'un diviseur de  $n$  et d'un diviseur de  $m$

(b) Montrer que si  $f$  et  $g$  sont multiplicatives, la fonction

$$f * g : n \mapsto \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

l'est aussi (produit de Dirichlet)

(c) Montrer que la somme des diviseurs (resp le nombre de diviseurs) de  $n$  est une fonction multiplicative de  $n$ .

(d) Soit  $\varphi$  l'indicateur d'Euler. On sait que  $\varphi$  est multiplicative. Démontrer à l'aide de ce qui précède que pour tout  $n$  on a :

$$\sum_{d|n} \phi(d) = n$$

*indication : on démontrera que cette relation est vraie lorsque  $n$  est de la forme  $p^k$  avec  $p$  premier*

21. *classique.* Fonction de Möbius (utiliser l'exercice précédent).

La fonction  $\mu$  est définie sur  $\mathbb{N}^*$  par  $\mu(1) = 1$ ,  $\mu(n) = 0$  si  $n$  est divisible par un carré, et  $\mu(n) = (-1)^r$  si  $n$  est le produit de  $r$  nombres premiers distincts.

(a) Calculer

$$\sum_{d|n} \mu(d)$$

(b) Montrer que le produit de Dirichlet

$$f * g : n \mapsto \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

est associatif sur l'ensemble  $E$  des fonctions de  $\mathbb{N}^*$  dans  $\mathbb{C}$

(c) Montrer que si  $f(n) = \sum_{d|n} g(d)$  alors  $g$  s'exprime simplement en fonction de  $f$  et  $\mu$

(d) Exprimer l'indicateur d'Euler  $\phi$  en fonction de  $\mu$

(e) *difficile.* Calculer la somme des racines primitives  $p$  ièmes de 1 à l'aide de  $\mu$

*Facteurs premiers, divisibilité, algorithme d'Euclide.*

22. (centrale)

Déterminer les entiers  $n$  tels que  $n(n+1)(n+2)$  soit un carré parfait

23. (centrale) *classique. difficile.*

Soient  $a, p, q$  des entiers. Montrer

$$a^p - 1 \wedge a^q - 1 = a^{p \wedge q} - 1$$

24. (mines) *classique*. Nombres de Fermat.

a) Montrer que si  $1 + 2^n$  est premier, alors il existe  $k$  tel que  $n = 2^k$ .

b) On pose  $f(k) = 1 + 2^{2^k}$ . Conjecturer puis établir une relation entre  $f(n+1)$  et  $\prod_{k=0}^n f(k)$ .

c) Montrer que  $f(n)$  et  $f(m)$  sont premiers entre eux pour  $n \neq m$ .

25. *classique*. Valuation  $p$  adique.

Pour tout nombre premier  $p$  et tout entier  $n$  on note  $v_p(n)$  la valuation  $p$  adique de  $n$ . Montrer la formule

$$v_p(n!) = \sum_k \lfloor \frac{n}{p^k} \rfloor$$

26. (Ens) (conséquence du précédent)

Montrer que

$$A_n = \frac{(30n)!n!}{(15n)!(10n)!(6n!)}$$

est un entier, et donner un équivalent de  $A_n$  quand  $n$  tend vers l'infini.

27. ppcm, évaluation du nombre de nombres premiers.

On note  $d_n$  le ppcm des entiers  $1, 2, \dots, n$

(a) On pose  $I_n = \int_0^1 t^n(1-t^n)dt$ . démontrer que  $I_n$  est un nombre rationnel dont le dénominateur est un diviseur de  $d_{2n+1}$ .

(b) En déduire que  $d_{2n+1} > 4^n$  puis l'existence d'une constante  $a$  telle que  $d_n \geq a2^n$  pour tout  $n$ .

(c) On note  $\pi(n)$  le nombre de nombres premiers inférieurs ou égaux à  $n$ . Démontrer que  $d_n \leq \prod_{p \in \mathbb{P}, p \leq n} p^{\frac{\ln(n)}{\ln p}}$

(d) Etablir l'existence d'une constante  $C$  telle que pour tout  $n$ ,  $\pi(n) \geq c \frac{n}{\ln n}$

### Polynômes et fractions rationnelles

La fin de cette fiche d'exercice propose quelques exercices tous classiques et souvent assez difficiles sur les polynômes.

28. *classique*. (mines) Déterminer les polynômes vérifiant

$$P(X^2) = P(X)P(X-1)$$

*indication* : raisonner sur les racines en remarquant que leur ensemble est stable par les transformations  $a \rightarrow a^2$  et  $a \rightarrow (a+1)^2$

29. *classique*.

Soit  $P \in \mathbb{R}[X]$ . On suppose que  $P(x) \geq 0$  pour tout  $x$  réel. Montrer qu'il existe  $R, S \in \mathbb{R}[X]$  tels que  $P = R^2 + S^2$

*indication* : montrer que c'est vrai pour les polynômes de degré 2 et utiliser la factorisation  $(A^2 + B^2)(C^2 + D^2) = (AC + BD)^2 + (AD - BC)^2$

30. *classique*. (mines)

(a) Trouver explicitement un polynôme  $P_n$  tel que pour tout  $\theta \in ]0, \frac{\pi}{2}[$ ,

$$P_n(\cot^2 \theta) = \frac{\sin(2n + 1\theta)}{(\sin \theta)^{2n+1}}$$

(b) Calculer ses racines et leur somme

(c) *difficile*. En déduire  $\sum_1^\infty \frac{1}{n^2}$

31. *classique.*

(a) Montrer que le polynôme

$$P_n = \frac{X(X-1)\dots(X-n+1)}{n!}$$

ne prend que des valeurs entières sur  $\mathbb{Z}$

(b) Montrer qu'un polynôme à coefficients réels vérifie  $P(\mathbb{Z}) \subset \mathbb{Z}$  si et seulement si il est combinaison linéaire à coefficients entiers des polynômes  $P_n$

(c) Si  $P$  de degré  $n$  prend des valeurs entières en  $n+1$  entiers consécutifs, alors  $P(\mathbb{Z}) \subset \mathbb{Z}$

*Polynômes à coefficients entiers ou rationnels*

32. (centrale)

Montrer que  $\sqrt[3]{2}$  n'est pas rationnel et qu'il n'est racine d'aucun polynôme à coefficients rationnels de degré 2.

33. (mines) Montrer que le polynôme  $X^3 - 3X + 1$  est irréductible dans  $\mathbb{Q}[X]$

34. (centrale.) Montrer que le polynôme  $P = X^n - 2$  est irréductible sur  $\mathbb{Z}$ . On pourra, par exemple écrire  $P = QR$  et étudier la parité des coefficients de  $Q, R$ .

35. *difficile.* Le lemme de Cauchy pour les polynômes :

Pour un polynôme  $P$  à coefficients entiers on note  $c(P)$  le pgcd de ses coefficients.

Soient  $P$  et  $Q$  deux polynômes à coefficients entiers.

(a) On suppose que  $c(P) = c(Q) = 1$ . Montrer que  $c(PQ) = 1$ .

*Indication : on pourra considérer un nombre premier  $p$  qui divise tous les coefficients de  $PQ$  et établir une contradiction.*

(b) Montrer qu'en toute généralité  $c(PQ) = c(P)c(Q)$

(c) Soit  $P$  un polynôme unitaire à coefficients entiers. On suppose que  $P$  est irréductible dans  $\mathbb{Z}[X]$ . Montrer qu'il est irréductible dans  $\mathbb{Q}[X]$

*Relations coefficients-racines*

36. (mines)

Soient  $a, b, c$  trois nombres complexes de modules distincts. On suppose que  $a + b + c, a^2 + b^2 + c^2, a^3 + b^3 + c^3$  sont réels. Montrer que  $a, b, c$  sont réels.

37. *classique.* Déterminer toutes les triplets de nombres complexes  $a, b, c$  de module 1 et de somme nulle.

38. (centrale) Soit  $P = \sum_{k=0}^n a_k X^k$  un polynôme dont les racines sont  $x_1, \dots, x_n$ . Montrer que pour tout  $k$ ,

$$|a_k| \leq \binom{n}{k} \prod_{j=1}^n \max(1, |x_j|)$$

39. (mines) Si  $P$  est un polynôme scindé sur  $\mathbb{R}$ , montrer qu'il en est de même de son polynôme dérivé.

40. Soit  $P$  un polynôme scindé sur  $\mathbb{R}$ . Montrer qu'il en est de même de  $P + P'$ .

*indication : trouver une fonction auxiliaire judicieuse qui ramène à l'exercice précédent*

41. Un lemme de localisation :

Si  $z$  est racine de  $X^n + \sum_{k=0}^{n-1} a_k X^k$ , alors

$$|z| \leq 1 + \max_{0 \leq k \leq n-1} (|a_k|)$$

42. Calculer

$$\prod_{k=1}^n (1 + e^{\frac{2ik\pi}{n}})$$

*Utilisation de fractions rationnelles*

43. Soit  $P$  un polynôme réel scindé à racines simple de degré  $n > 1$ . Montrer que  $(n-1)P'^2 - nPP''$  est positif.

*indication : utiliser la fraction  $\frac{P'}{P}$*

44. *classique.*

Soit  $P$  un polynôme scindé à racines simples  $x_1, \dots, x_n$ . Calculer :

(a)  $\sum_1^n \frac{1}{x_k P'(x_k)}$  si 0 n'est pas racine de  $P$ .

45. *classique. Théorème de Gauss Lucas*

Soit  $P$  un polynôme à coefficients complexe. Montrer que les racines de  $P'$  sont dans l'enveloppe convexe de celles de  $P$ .

46. (mines)

Soit  $P \in \mathbb{R}[X]$  unitaire de degré  $n$ . Montrer qu'il existe  $k \in \{0, \dots, n\}$  tel que  $|P(k)| \geq \frac{n!}{2^n}$ .

*indication : considerer la fraction rationnelle  $\frac{P}{X(X-1)\dots(X-n)}$*