Exercices d'Algèbre générale.

- 1)* (C04) Soit $(G, *)$ un groupe et A une partie de G , finie et stable par $*$. Montrer que A est en fait un sous-groupe de G .
- 2)** (X01) Soit G un groupe tel que pour tout élément x de G , $x^2 = e$.
- Montrer que G est abélien.
 - Montrer que si G est fini, son cardinal est une puissance de 2. *Indication* : On pourra considérer le plus petit entier p tel qu'il existe une famille génératrice (au sens des groupes) de G de cardinal p .
- 3)** (M00) Combien y a-t-il de morphismes de groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(\mathbb{Z}/m\mathbb{Z}, +)$?
- 4)** Soit G un groupe fini. Si g est un élément de G , on note $C(g) = \{hgh^{-1}, h \in G\}$ sa classe de conjugaison.
- Montrer que $|C(g)|$ divise $|G|$ (où $|A|$ désigne le cardinal d'un ensemble fini A).
 - On note $Z(G) = \{x \in G, \forall y \in G, xy = yx\}$, appelé le centre de G . Etablir que $Z(G)$ est un sous-groupe de G , et que si $|G| = p^\alpha$, où p est un nombre premier et $\alpha \geq 2$, alors $|Z(G)| \neq 1$.
 - On suppose dorénavant que $|G| = p^2$, avec p premier. Montrer que G est abélien, puis qu'il est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$.
- 5)** (U06) Soit $(G, \cdot)$ un groupe, $D = \text{gr}\{xyx^{-1}y^{-1}, (x, y) \in G^2\}$ (appelé groupe *dérivé* de G), et $C = \text{gr}\{x^2, x \in G\}$.
- Montrer que $D \subset C$.
 - On suppose que G est engendré par $\{x \in G, x = x^{-1}\}$. Montrer que $C = D$.
 - Soit $G = \mathcal{O}_2(\mathbb{Q})$, groupe des matrices 2×2 orthogonales à coefficients dans $\mathbb{Q}$. Montrer que D est un sous-groupe strict de $\mathcal{SO}_2(\mathbb{Q})$, sous-groupe de $\mathcal{O}_2(\mathbb{Q})$ formé des matrices de déterminant 1.
- 6)** (U08) Montrer qu'il existe une infinité de puissances de 2 commençant par 7 en base 10. Quelle est la probabilité pour que cela se produise?
- 7)** (C07) a) Montrer que les sous-groupes finis de $(U, \times)$ sont cycliques.
b) Trouver tous les sous-groupes finis de $\mathcal{SO}_2(\mathbb{R})$, groupes des matrices de rotation de $\mathbb{R}^2$.
c) Soit G un sous-groupe fini de $SL_2(\mathbb{R}) = \{M \in \mathcal{M}_2(\mathbb{R}), \det(M) = 1\}$. Etablir qu'il existe un produit scalaire φ dans $\mathbb{R}^2$ tel que les endomorphismes canoniquement associés aux éléments de G soient des isométries pour ce produit scalaire. En déduire que G est cyclique.
- 8)** Soit $(G, \cdot)$ un groupe abélien fini et P le produit de tous ses éléments. Montrer que $P = e$ (le neutre) sauf dans un cas très particulier à préciser. *Indication* : introduire $H = \{x \in G / x^2 = e\}$ et étudier sa structure ; on pourra montrer que si K est un sous-groupe de H et a un élément de $H \setminus K$ alors $K \cup aK$ est un sous-groupe de H .
- 9)** (C05) **Théorème de Cauchy.** On se propose de montrer que dans tout groupe abélien d'ordre $n = p^\alpha m$ avec p premier et $p \nmid m$ il existe un élément d'ordre p . On appelle exposant d'un groupe abélien G tout entier $q > 0$, s'il existe, tel que $x^q = e$ pour tout x de G .
- Soit un exposant q de G . Montrer que l'ordre n de G divise une puissance de q . *Indication* : faire une récurrence sur n .
 - En déduire qu'il existe $x \neq e$ tel que $x^{p^\alpha} = e$.
 - Conclure.
- 10)** **Structure d'un groupe cyclique.** Démontrer que les sous-groupes d'un groupe cyclique d'ordre n sont cycliques et qu'il y a bijection entre les diviseurs de n et ces sous-groupes. En déduire la relation dite d'Euler-Moebius : $n = \sum_{d|n} \varphi(d)$.
- 11)** (U95) **Unicité de décomposition de produits de cycliques.** Soient $(a_1, \dots, a_n)$ et $(b_1, \dots, b_m)$ des entiers strictement positifs tels que chacun soit multiple du précédent : $a_1 | a_2 | \dots | a_n$ et $b_1 | b_2 | \dots | b_m$. On suppose aussi que les groupes $\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \dots \times \mathbb{Z}/a_n\mathbb{Z}$ et $\mathbb{Z}/b_1\mathbb{Z} \times \mathbb{Z}/b_2\mathbb{Z} \times \dots \times \mathbb{Z}/b_m\mathbb{Z}$ sont isomorphes. Montrer qu'alors $m = n$ et que $a_1 = b_1, a_2 = b_2, \dots, a_n = b_n$. *Indication* : récurrence ; utiliser le cardinal et l'exposant de ces groupes.
- 12)** (X04) **Fonction de Möbius.** Soit $\mu(n)$ la somme des racines primitives n -ièmes de l'unité.
- Montrer que si m et n sont premiers entre eux, on a $\mu(mn) = \mu(m)\mu(n)$.
 - Que vaut $\mu(n)$ si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec p_i premiers?
- 13)** Soit G un sous-groupe additif de $\mathbb{R}$ tel qu'il existe un nombre fini d'ensembles distincts de la forme $x + G = \{x + g, g \in G\}$, lorsque x décrit $\mathbb{R}$. Montrer que $G = \mathbb{R}$.
- 14)** (U08) **Un groupe de pavage.** Soit P l'ensemble des nombres complexes de la forme $a + bj$ avec $a, b \in \mathbb{Z}$ et $j = \exp(\frac{2i\pi}{3})$ (on note habituellement cet ensemble $\mathbb{Z}[j]$). Quelles sont les isométries affines f du plan telles que $f(P) = P$? *Indication* : Commencer par les isométries directes. Utiliser une représentation complexe des isométries.
- 15)** (M03) **Isométries du cube.**
- Montrer que l'ensemble des rotations de l'espace $\mathbb{R}^3$ qui laissent globalement invariant le cube formé par les 8 points de coordonnées $(\pm 1, \pm 1, \pm 1)$ forme un groupe isomorphe à S_4 .

- b) Démontrer que l'ensemble des isométries de l'espace $\mathbb{R}^3$ qui laissent globalement invariant un tétraèdre régulier est un groupe isomorphe à S_4 ; que peut-on dire des isométries directes qui laissent ce tétraèdre invariant?
- 16)***(E99) On appelle groupe dérivé $D(G)$ d'un groupe G le sous-groupe de G engendré par les éléments de la forme $aba^{-1}b^{-1}$, où $(a, b) \in G^2$.
- a) Que peut-on dire de $D(G)$ si G est abélien?
- b) Montrer que les 3-cycles engendrent A_n , pour $n \geq 3$.
- c) Etablir que deux 3-cycles sont conjugués dans S_n , pour $n \geq 3$. Est-ce encore vrai dans A_n ?
- d) En déduire $D(S_n)$.
- 17)**(U09) Trouver tous les morphismes de $(\mathbb{Q}, +)$ dans $(\mathbb{Q}_+^*, \times)$.
- 18)**(X08) Soit $E = \{(x + y\sqrt{2}, x \in \mathbb{N}^*, y \in \mathbb{Z}, x^2 - y^2 = 1)\}$.
- a) Montrer que E est un sous-groupe de $(\mathbb{R}_+^*, \times)$.
- b) Montrer que $E = \{(x_0 + y_0\sqrt{2})^n, n \in \mathbb{Z}\}$ où $x_0 + y_0\sqrt{2}$ est le plus petit élément de E strictement supérieur à 1.
- 19)**(M09) **Anneaux euclidiens.** On dit qu'un anneau commutatif A est euclidien si et seulement s'il existe une application $v : A \setminus \{0\} \rightarrow \mathbb{N}$ telle que pour tout $(a, b) \in A^2$ tel que $b \neq 0$, il existe $(q, r) \in A^2$ tel que : $a = bq + r$, avec $r = 0$ ou $v(r) < v(b)$.
- a) Donner des exemples.
- b) Montrer que $\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$ est euclidien.
- c) Prouver que tout anneau euclidien est principal.
- d) Montrer que tout sous-anneau de $\mathbb{Q}$ est principal; et dans $\mathbb{C}$? *Indication : voir $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}, (a, b) \in \mathbb{Z}^2\}$.*
- 20)* Trouver tous les entiers n tels que $n \equiv 1 \pmod{3}$, $n \equiv 2 \pmod{5}$, $n \equiv 3 \pmod{7}$.
- 21)* L'équation $2x^2 - 5y^2 = 7$ n'a pas de solution dans $\mathbb{Z} \times \mathbb{Z}$. *Indication : Raisonner mod 7.*
- 22)**(X98) Soit p premier. Montrer que $\sum_{k=0}^p \binom{p}{k} \binom{p+k}{k} \equiv 2^p + 1 \pmod{p^2}$.
- 23)*(X98) Montrer que $10^{10^n} \equiv 4 \pmod{7}$ pour tout $n \in \mathbb{N}^*$.
- 24)*(M03) Résoudre dans $\mathbb{Z} \times \mathbb{Z} : 29x - 17y = 3$. *Indication : raisonner mod 17 Réponse : $y = -7 + 29k, x = -4 + 17k$.*
- 25)*(X06) Soit p premier, $p \geq 3$, et $\alpha \in \mathbb{N}$. Montrer que $(1 + p)^{p^\alpha} \equiv 1 + p^{\alpha+1} \pmod{p^{\alpha+2}}$. *Indication : Récurrence.*
- 26)*(M96) Résoudre $x^3 = 1$ dans $\mathbb{Z}/19\mathbb{Z}$.
- 27)***(U07) Soit un nombre premier p supérieur à 4. Soit $M = \mathbb{Z}/p\mathbb{Z} \setminus \{1\} = \{2, 3, \dots, p-1\} \subset \mathbb{Z}/p\mathbb{Z}$ et f de M dans M définie par $f(x) = 1 - x^{-1}$. Montrer que -3 est un carré modulo p si, et seulement si f a un point fixe. En déduire que -3 est un carré modulo p si, et seulement si $p \equiv 1 \pmod{3}$. *Indication : utiliser le théorème de décomposition en produits de cycles.*
- 28)**(C06) Montrer qu'il n'existe pas de quadruplet $(x, y, z, t) \in \mathbb{N}^4$ tel que $x^2 + y^2 + z^2 = (8t + 7)4^n$. *Indication : On pourra commencer par étudier le cas $n = 0$.*
- 29)**(X08) Déterminer les $n \in \mathbb{N}^*$ tels que 7 divise $n^n - 3$.
- 30)**(L93) a) Combien y a-t-il d'éléments inversibles dans $\mathbb{Z}/2^n\mathbb{Z}$? On note $\mathbb{Z}/2^n\mathbb{Z}^*$ le groupe des inversibles en question.
- b) Montrer que $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$. *Indication : récurrence.*
- c) Quel est, pour $n \geq 3$, l'ordre de 5 dans $\mathbb{Z}/2^n\mathbb{Z}^*$?
- d) Montrer que $gr(-1) \cap gr(5) = \{1\}$, et en déduire que le groupe des éléments inversibles de $\mathbb{Z}/2^n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$.
- 31)**(E98) Soit pour n entier $\pi(n) =$ le nombre de nombres premiers dans $\{2, \dots, n\}$.
- a) Montrer que la suite $(\pi(n))_{n \geq 2}$ n'est pas bornée.
- b) Montrer que $\forall n \geq 2, \pi(2^{2^n}) \geq n$.
- 32)**(X97) **Identité d'Euler.** a) Soient a et r deux entiers relatifs premiers entre eux. Montrer qu'il existe un entier $k(r) > 0$ tel que $a^{k(r)} \equiv 1 \pmod{r}$.
- b) On suppose que $a > r > 2$. Montrer que la progression arithmétique de premier terme a et de raison r contient une infinité de termes ayant les mêmes facteurs premiers.
- 33)**(X07) **Matrices inversibles entières.** a) A quelle condition une matrice à coefficients entiers relatifs est-elle inversible (dans $\mathcal{M}_n(\mathbb{Z})$)? On note $GL_n(\mathbb{Z})$ leur ensemble.
- b) Soit $u = (u_1, \dots, u_n) \in \mathbb{Z}^n$ et $\varphi(x) = \sum_{i=1}^n u_i x_i$ pour $x \in \mathbb{Z}^n$. On suppose qu'il existe au moins un "vecteur" x tel que $\varphi(x) = 1$. Montrer que $\mathbb{Z}^n = \mathbb{Z}x \oplus \text{Ker } \varphi$ (à préciser).
- c) Montrer que x est la première colonne d'une matrice de $GL_n(\mathbb{Z})$ si et seulement si les x_i sont premiers entre eux.

34)**(X02) Soit p un nombre premier, $(a_0, \dots, a_{p-1}) \in \mathbb{Z}^p$. Montrer que le déterminant
$$\begin{vmatrix} a_0 & a_1 & \dots & a_{p-1} \\ a_{p-1} & a_0 & \dots & a_{p-2} \\ \vdots & & \ddots & \vdots \\ a_1 & \dots & a_{p-1} & a_0 \end{vmatrix}$$
 est congru modulo p à $\sum_{k=0}^{p-1} a_k$.

35)*(X04) Montrer qu'un réel x est rationnel si et seulement si son développement décimal est périodique au-delà d'un certain rang.

36)**(X08) Soit p un nombre premier ≥ 5 , et a tel que $1 + \frac{1}{2} + \dots + \frac{1}{p-1} = \frac{1}{(p-1)!}$. Prouver que p^2 divise a .

37)**(U09) **Sommes de deux carrés.** Soit p un nombre premier supérieur ou égal à 3. On note F_p le corps $\mathbb{Z}/p\mathbb{Z}$. On appelle résidu quadratique tout carré dans $F_p^* = F_p \setminus \{0\}$. On note R l'ensemble des résidus quadratiques.

a) Montrer que R est un groupe d'ordre $(p-1)/2$ et que : $a \in R$ si et seulement si $a^{(p-1)/2} = 1$.

b) Soit p premier impair ; montrer que si $p = a^2 + b^2$ avec a et b entiers alors $p = 4k + 1$. *Indication : montrer que -1 est résidu quadratique.*

c) Lemme de Thue : Etablir que dans F_p^* on peut représenter tout élément par $\bar{a}/\bar{b}$ avec $|a|$ et $|b|$ inférieurs à $\sqrt{p}$ (a et b dans $\mathbb{Z}$, $\bar{a}$ et $\bar{b}$ classes modulo p).

Indication : prendre k entier $1 \leq k \leq p-1$ et considérer $(a, b) \mapsto (a - kb)$ avec a et b entiers ≥ 0 et $\leq \sqrt{p}$. Montrer que cette application est non injective et conclure.

d) Soit $p = 4k + 1$ premier. En utilisant le lemme de Thue en particulier montrer que p est somme de 2 carrés.

e) Dans l'anneau des entiers de Gauss $\mathbb{Z}[i]$ montrer que les irréductibles sont les (à unité près) p premiers du type $4k - 1$ et les $a + ib$ avec $a^2 + b^2 = p$ (p premier : $p = 2$ ou $p = 4k + 1$).

f) En utilisant $\mathbb{Z}[i]$ montrer que $n \in \mathbb{N}$ est somme de deux carrés si, et seulement si on a : $n = m^2 p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec p_i premier somme de deux carrés.

38)**(X03) Soit n un nombre à six chiffres divisible par 13. Montrer qu'en mettant le premier chiffre de n à la fin (exemple : $123456 \leftarrow 234561$), on obtient un nombre divisible par 13.

39)**(C03) On désigne par $v_p(n)$ l'exposant de p dans la décomposition en facteurs premiers de n .

a) Montrer que $v_p(n!) = \sum_{k \geq 1} E\left(\frac{n}{p^k}\right)$.

b) Montrer que $\binom{2n}{n}$ divise $\prod_{p \text{ premier}, p \leq 2n} p^{E(\ln 2n / \ln p)}$.

c) Montrer que $\binom{2n}{n} \leq (2n)^{\pi(2n)}$, où $\pi(k)$ désigne le nombre de premiers $\leq k$.

d) Montrer que $\frac{k}{\ln k} = \mathcal{O}(\pi(k))$.

40)**(C03) Pour $n \in \mathbb{N}^*$, on note $S(n)$ le nombre de diviseurs de n dans $\mathbb{N}^*$.

a) Exprimer $S(n)$ à l'aide de la décomposition primaire de n . On pourra commencer par n puissance d'un nombre premier.

b) On note E l'ensemble des $n \in \mathbb{N}^*$ tels que $S(n) = 2p$. Montrer que si p et $2^p - 1$ sont premiers, alors $2^{p-1}(2^p - 1)$ est dans E .

c) Soit n pair dans E . Montrer qu'il existe un nombre premier p tel que $2^p - 1$ soit premier et $n = 2^{p-1}(2^p - 1)$.

41)**(L03) Soit $n \in \mathbb{N}^*$ et $d(n)$ le nombre de diviseurs de n . Soit $\varepsilon > 0$, montrer que $\lim_{n \rightarrow +\infty} \frac{d(n)}{n^\varepsilon} = 0$.

On considérera dans un premier temps le cas où n est une puissance d'un nombre premier.

Soit p premier et $n' = np$; que peut-on dire de $d(n)$?

42)*(X91) P et Q étant deux points de $\mathbb{R}^n$, soit (*) la propriété : il n'existe pas de point à coordonnées entières appartenant au segment $[P, Q]$ privé de P et Q . Montrer que si $P(a, b)$ et $Q(m, n)$ sont deux points de $\mathbb{Z}^2$, P et Q vérifient (*) si et seulement si $(a - m) \wedge (b - n) = 1$.

43)*(L09) **Nombres de Fermat.** On pose $F_n = 2^{2^n} + 1$.

a) Montrer que $\prod_{k=0}^{n-1} F_k = F_n - 2$.

b) Si $n \neq m$, quel est le p.g.c.d. de F_n et F_m ?

c) En déduire que l'ensemble des nombres premiers est infini.

44)**(L09) Soit p un nombre premier ≥ 3 . Montrer que $x \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$ est un carré si et seulement si $x^{p-1/2} = \bar{1}$. En déduire qu'il existe une infinité de nombres premiers congruents à 1 modulo 4.

45)**(E96) Soit $P = \sum_{i=0}^n \frac{a_i}{b_i} X^i \in \mathbb{Q}[X]$, où les a_i et b_i sont des entiers relatifs ; on définit le contenu de P : $c(P) = \frac{\text{p.g.c.d.}_{i=0}^n(a_i)}{\text{p.p.c.m.}_{i=0}^n(b_i)}$.

a) (Lemme de Gauss) Montrer qu'on a $P = c(P)P_1$, où P_1 est un polynôme de $\mathbb{Z}[X]$ dont les coefficients sont premiers entre eux dans leur ensemble, et qu'une telle écriture est unique.

b) Soient $(P, Q) \in \mathbb{Q}[X]^2$; prouver que $c(PQ) = c(P)c(Q)$. En déduire que si $P \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Z}[X]$, il l'est aussi sur $\mathbb{Q}[X]$. La réciproque est-elle vraie ?

- c) (Critère d'Eisenstein) Soit un polynôme $P = \sum_{i=0}^d a_i X^i \in \mathbb{Z}[X]$ de degré d et un nombre premier p tel que p divise tous les a_i excepté a_d , et que p^2 ne divise pas a_0 . Montrer que P est irréductible dans $\mathbb{Q}[X]$.
- d) En déduire que $\sum_{i=0}^{p-1} X^i$ est irréductible dans $\mathbb{Z}[X]$.
- e) Quelle est la dimension de $\mathbb{Q}[e^{2i\pi/p}]$ comme espace vectoriel sur $\mathbb{Q}$? *Indication : relire le cours sur les éléments algébriques pour savoir ce que désigne $\mathbb{Q}[a]$. Réponse : $p - 1$.*
- 46)***(U07) Soient a, b, c des entiers relatifs ($\mathbb{Z}$) tels qu'il existe α et β complexes non réels, et n, p entiers ($\mathbb{N}$) avec : $a\alpha + b\beta + c = 0$; $\alpha^n = 1$; $\beta^p = 1$. Déterminer ces nombres. En déduire qu'en général (exceptions à préciser) $1, \alpha, \beta$ sont linéairement indépendants sur $\mathbb{Q}$. Quels sont les triangles à côtés de longueurs entières et angles rationnels (en degrés)? *Indication : éliminer β , se ramener au problème des racines rationnelles du polynôme de Tchebychev T_n tel que $T_n(2 \cos \varphi) = 2 \cos n\varphi$.*
- 47)**(M96) Soit $N = \sum_{k=0}^{p-1} \left(2 \cos \frac{k\pi}{p}\right)^n \cos\left(\frac{nk\pi}{p}\right)$ (n, p entiers strictement positifs fixés). Montrer que $N \in p\mathbb{Z}$.
- 48)**(M97) Calculer le nombre de relations réflexives et symétriques sur un ensemble à n éléments.
- 49)**(X08) Pour $(k, n) \in \mathbb{N}^* \times \mathbb{N}^*$, on note $s(k, n)$ le nombre de surjections de $\{1, \dots, k\}$ dans $\{1, \dots, n\}$.
- a) Montrer que $n!$ divise $s(k, n)$.
- b) Lier le nombre des applications de $\{1, \dots, k\}$ dans $\{1, \dots, n\}$ aux $s(k, j)$, où $j \in \{1, \dots, n\}$.
- c) Calculer $s(k, 1)$ et $s(k, 2)$.
- 50)*(E00) Calculer $\sum_{k=0}^n \binom{a}{k} \binom{b}{n-k}$. *Indication : deux méthodes : formule du binôme ou tirage de boules dans une urne.*
- 51)**(U01) Soit $A = \{e_1, \dots, e_n\}$ un ensemble fini de cardinal $n \geq 2$. Soit $U_1, \dots, U_p$, p parties non vides de A , deux à deux distinctes, et telles qu'il existe $a \geq 0$ vérifiant $\forall (i, j) \in [1, n]^2, i \neq j \Rightarrow \text{Card}(U_i \cap U_j) = a$. Montrer que $p \leq n$. *Indication : Introduire la matrice $M \in \mathcal{M}_{np}(\mathbb{R})$ définie par $m_{ij} = 1$ si $e_i \in U_j$, puis la matrice $G = {}^t M M$.*
- 52)**(C04) **Un corps de nombres algébriques.** a) Montrer que toute algèbre de dimension finie et intègre, sur un corps K commutatif, est un corps.
- b) Montrer que $P(X) = X^3 - 2$ est irréductible sur $\mathbb{Q}[X]$.
- c) Montrer que $H = \{a + b2^{1/3} + c4^{1/3}, (a, b, c) \in \mathbb{Q}^3\}$ est un corps et une $\mathbb{Q}$ -algèbre dont on donnera une base.
- 53)**(U09) **Groupe multiplicatif d'un corps fini.** On appelle exposant m d'un groupe fini G le p.p.c.m. des ordres des éléments de G .
- a) Si G est abélien, montrer qu'il existe un élément de G d'ordre m . *Indication : On s'intéressera d'abord au cas où m est une puissance d'un nombre premier ; dans la cas général, on décomposera m en produit de puissances de facteurs premiers.*
- b) Démontrer que le groupe multiplicatif d'un corps K fini (supposé commutatif) est cyclique. *Indication : L'équation $X^d - 1 = 0$ possède au plus d solutions ; introduire le ppcm des ordres des divers éléments de K^* et l'indicateur d'Euler.*
- 54)**(U08) Soit $E = \{(x, y) \in \mathbb{R}^2, y^2 = x^3\}$. $f \in R^{E \times E}$ est dite polynomiale s'il existe une fonction polynomiale réelle $F(X, Y)$ telle que f soit la restriction de F à E . Soit $m \geq 0$; déterminer la dimension de l'espace des fonctions polynomiales $f \in R^{E \times E}$ telles que $f(x, y) = O(|x^m|)$ lorsque $|x| + |y|$ tend vers l'infini.
- 55)**(L08) a) Soit $P_0 = 1$ et $\forall n \in \mathbb{N}^*, P_n(X) = \frac{1}{n!} \prod_{i=1}^n (X + i)$. Montrer que $\forall n \in \mathbb{N}, P_n(\mathbb{Z}) \subset \mathbb{Z}$.
- b) Soit $p \in \mathbb{N}^*$ et $P \in \mathbb{Q}_p[X]$. Montrer que $P(\mathbb{Z}) \subset \mathbb{Z}$ si et seulement s'il existe $(\alpha_0, \dots, \alpha_p) \in \mathbb{Z}^p$ tels que $P = \sum_{i=0}^p \alpha_i P_i$.
- 56)*(C06) Soient $P \in \mathbb{Z}[X]$, et a et b deux entiers relatifs tels que $b > 0$ et $\sqrt{b}$ irrationnel.
- a) Montrer que si $a + \sqrt{b}$ est racine de P , alors $a - \sqrt{b}$ l'est aussi.
- b) On suppose que $a + \sqrt{b}$ est racine double de P . Montrer que $P = R.Q^2$, avec $(R, Q) \in \mathbb{Z}[X]^2$.
- 57)**(U07) Les entiers naturels non nuls k et n étant fixés, rendre maximal $x_1 \dots x_k$, avec les conditions $(x_1, \dots, x_k) \in \mathbb{N}^k$ et $x_1 + \dots + x_k = n$.
- 58)**(X07) Soit un polynôme $\in \mathbb{C}_d[X]$, n'ayant sur $\mathbb{C}$ que des racines de module inférieur ou égal à 1, et u un complexe de module 1. On pose $Q_u(z) = P(z) + uz^d \bar{P}\left(\frac{1}{z}\right)$, $\bar{P}$ désignant le polynôme dont les coefficients sont les conjugués de ceux de P . Montrer que les racines de Q_u sont toutes de module 1.
- 59)**(U08) Soit P un polynôme réel possédant au plus k coefficients non nuls. Montrer que P a au plus $2k - 1$ racines distinctes. Peut-il en avoir exactement $2k - 1$?
- 60)**(L08) Soit $(P_n)_{n \geq 0}$ une suite de polynômes non nuls de $\mathbb{R}[X_1, \dots, X_p]$. Montrer qu'il existe $(x_1, \dots, x_p) \in \mathbb{R}^p$ tel que : $\forall n \in \mathbb{N}, P_n(x_1, \dots, x_n) \neq 0$.
- 61)**(E08) **Théorème de Lucas.** Soit $P \in \mathbb{C}[X]$ établir que les racines de P' sont dans l'enveloppe convexe (c'est-à-dire sont barycentres à coefficients ≥ 0) des racines de P .

62)**(X09) Soit $P \in \mathbb{R}[X]$ scindé sur $\mathbb{R}$.

a) Montrer que $\forall \alpha \in \mathbb{R}, P + \alpha P'$ est scindé sur $\mathbb{R}$.

b) Soit $R = \sum_{i=0}^r \in \mathbb{R}[X]$ scindé sur $\mathbb{R}$. Montrer que $\sum_{i=0}^n a_i P^{(i)}$ aussi.

63)**(E09) Soit P un polynôme réel scindé à racines simples de degré n ; montrer que $(n-1)P'^2 \geq nPP''$.

64)**(E09) Soit $P \in \mathbb{Z}[X]$ non constant. Montrer qu'il y a une infinité de nombres premiers figurant dans la décomposition des $P(n), n \in \mathbb{N}$.

65)**(M98) Soient $x_0, \dots, x_n$ des réels distincts et $L_i(X) = \prod_{i \neq j} \frac{X-x_j}{x_i-x_j}$. Soit $P_m = \sum_{i=0}^m x_i^m L_i$ avec $m \leq n+2$. Calculer $P_m(0)$.

Indication : immédiat si $m \leq n$. Sinon soustraire X^{n+1} ou X^{n+2} .

66)*(C07) Polynômes P tels que $(X+3)P(X) = XP(X+1)$.

67)**(U95) **Polynômes positifs.** Soit $P \in \mathbb{R}[X]$ tel que $\forall x \in \mathbb{R} P(x) \geq 0$. Démontrer l'existence de deux polynômes réels A et B tels que $P = A^2 + B^2$. Indication : factoriser d'abord P dans $\mathbb{C}[X]$; distinguer les racines non réelles et réelles et surveiller la multiplicité de celles-ci.

68)*(C04) Quels sont les polynômes $P \in \mathbb{C}[X]$, tels que $P(X^2) = P(X)P(X+1)$? Indication : travailler sur l'ensemble des zéros qui est fini et stable pour des applications simples de $\mathbb{C}$ dans $\mathbb{C}$ Réponse : $P(X) = (X(X-1))^\alpha$.

69)**(X95) a) Soit f et g les applications de $\mathbb{C}$ dans $\mathbb{C}$ définies respectivement par $z \rightarrow z^2 + z + 1$ et $z \rightarrow z^2 - z + 1$. Soit A une partie finie de $\mathbb{C}$ telle que $f(A) \subset A$ et $g(A) \subset A$. Déterminer A . Indication : Considérer $a \in A$ tel que $M = |a^2 + 1|$ soit le plus grand possible, examiner $f(a)$ et $g(a)$; si M n'est pas nul, en déduire que $|a^2 + 2| \leq 1$ et que $|a| \leq \frac{1}{2}$.

b) En déduire tous les polynômes P de $\mathbb{C}[X]$ tels que $P(X^2 + X + 1) = P(X)P(X+1)$.

70)*(M02) Pour $n \in \mathbb{N}^*$, on considère le polynôme

$$P_n(X) = X^{2n} - 2X^{2n-1} + 3X^{2n-2} - \dots - 2nX + 2n + 1.$$

Combien $P_n(X)$ possède-t-il de racines réelles? Indication : réellement peu...

71)**(L04) On donne un polynôme réel scindé, de degré n , $Q(X) = \sum_{k=0}^n a_k X^{n-k}$. Montrer que $k(n-k)a_k^2 \geq (k+1)(n-k+1)a_{k+1}a_{k-1}$ pour tout $k \in \{1, \dots, n-1\}$.

72)**(U95) Soit $P = a_0 + \dots + a_n X^n \in \mathbb{R}[X]$. On suppose que P n'a que des racines réelles strictement positives. Montrer que le polynôme $Q = a_0 \cos \varphi + a_1 \cos(\varphi + \theta)X + \dots + a_n \cos(\varphi + n\theta)X^n$ a toutes ses racines réelles si $\theta \notin \frac{\pi}{2} + \pi\mathbb{Z}$. Indication : introduire le polynôme $R = a_0 \exp(i\varphi) + a_1 \exp i(\varphi + \theta)X + \dots + a_n \exp i(\varphi + n\theta)X^n$ et discuter des arguments.

73)**(C04) **Formules de Newton.** Soit P un polynôme de degré $n \geq 1$ scindé à racines simples. On note Q le polynôme $Q = X^n P(\frac{1}{X})$ et F la fraction rationnelle $F = -\frac{XQ'}{Q}$. Décomposer F en éléments simples.

En déduire une méthode pour obtenir la somme des puissances p -ièmes des racines d'un polynôme scindé à racines simples.

74)**(X04) a) Soit un entier $n \geq 1$, $Q \in \mathbb{R}[X]$, tel que $Q(X) = a_n X^n - \sum_{k=0}^{n-1} a_k X^k$ avec les a_k tous positifs. Montrer que Q admet une unique racine dans l'intervalle $]0, +\infty[$.

b) On considère $P(X) = \sum_{k=0}^n b_k X^k$ avec $0 < b_0 < \dots < b_n$ et $Q(X) = (X-1)P(X)$. Montrer que si z est une racine complexe de P , alors $Q(|z|) \leq 0$ et en déduire que $|z| \leq 1$.

75)**(L02) Soit un polynôme $P \in \mathbb{C}[X]$.

a) On suppose que P admet deux racines distinctes, et que P'' divise P . Montrer que P est à racines simples. Indication : utiliser le lemme de Gauss-Lucas.

b) On suppose de plus que $P \in \mathbb{R}[X]$. Montrer que P est scindé sur $\mathbb{R}$ à racines simples.

76)**(M07) Déterminer une condition nécessaire et suffisante liant les 3 nombres complexes p, q, r pour que l'équation $x^3 + 3px^2 + 3qx + r = 0$ ait pour racines dans $\mathbb{C}$ les affixes des 3 sommets d'un triangle équilatéral.

77)**(X98) **Méthode de Sturm.** Soit P_0 un polynôme à coefficients réels et n'ayant pas de racine réelle multiple. On construit une suite (P_n) de polynômes selon : $P_1 = -P_0'$, $P_{i+1} = -R_i$, reste de la division euclidienne de P_{i-1} par P_i . Soit M le plus grand entier i tel que $P_i \neq 0$.

a) Majorer M .

b) Que dire des racines de P_M ?

c) Soit $\sigma(t)$ le nombre de changements de signes de la suite $(P_0(t), \dots, P_M(t))$ (compté en ignorant la présence d'éventuels termes nuls). Montrer que le nombre de racines de P_0 dans $[a, b[$ est égal à $\sigma(b) - \sigma(a)$.

78)**(X93) Soit P un polynôme à coefficients rationnels de degré 5 admettant une racine double complexe. Montrer que P a une racine rationnelle. Pour quels $n \in \mathbb{N}$ a-t-on la propriété suivante : « Tout polynôme P de $\mathbb{Q}[X]$ de degré n admettant une racine double dans $\mathbb{C}$ possède une racine rationnelle ».

79)**(C02) Soit un polynôme $P \in \mathbb{Q}[X]$ irréductible et α une racine complexe de P . Montrer que α est une racine simple de P . On factorise $P = (X - \alpha)Q$. Quels sont les coefficients rationnels de Q ? Indication : utiliser le PGCD de P et de P' .

80)** Soit $a_1, a_2, \dots, a_n$ des entiers deux à deux distincts et $P(X) = 1 + \prod_{1 \leq j \leq n} (X - a_j)^2$. Prouver que P est irréductible dans $\mathbb{Z}[X]$.

81)**(C05) Trouver P et Q tels que $P^2 + (1 - X^2)Q^2 = 1$.

82)*(M02) Calculer $\prod_{k=1}^{n-1} \frac{1}{1 - e^{2ik\pi/n}}$.

83)*(C02) Chercher successivement $\{P \in \mathbb{C}[X], P(\mathbb{Q}) \subset \mathbb{Q}\}$ puis $\{P \in \mathbb{C}[X], P(\mathbb{Q}) = \mathbb{Q}\}$.

84)**(X02) Soit n réels positifs $a_1, a_2, \dots, a_n$. On note

$$\begin{cases} \sigma_1 = a_1 + \dots + a_n \\ \sigma_2 = a_1 a_2 + a_1 a_3 + \dots + a_{n-1} a_n \\ \dots \\ \sigma_n = a_1 a_2 \dots a_n \end{cases}$$

les fonctions symétriques. On pose $\forall k \in \llbracket 1, n \rrbracket, \mu_k = \frac{\sigma_k}{\binom{n}{k}}$. Montrer que $\forall k \in \llbracket 2, n-1 \rrbracket, \mu_{k-1} \mu_{k+1} \leq \mu_k^2$. *Indication : introduire le polynôme P de racines a_i , le dériver $n - k - 1$ fois et changer x en $\frac{1}{x}$.*

85)(C98) Soit $P = \sum_{i=0}^n a_i X^i \in \mathbb{R}[X]$, scindé, à racines simples.

a) Montrer que $P'^2 - PP''$ n'a aucune racine réelle. *Indication : fractions.*

b) Montrer que $a_{k-1} a_{k+1} < a_k^2$ pour tout $k \in \llbracket 1, n-1 \rrbracket$. *Indication : $k = 1$ pour commencer.*

86)**(U95) Soit $P(\theta) = a_0 + a_1 \cos \theta x + \dots + a_n \cos n\theta x^n$. On suppose que P a des valeurs positives ou nulles sur $\mathbb{R}$. Alors il existe un polynôme $T \in \mathbb{R}[X]$ tel que $P(\theta) = |T(z)|^2$ si $z = \exp(i\theta)$. *Indication : noter que $\cos \theta = \frac{z + z^{-1}}{2}$.*

87)***(U08) **Polynômes cyclotomiques.**

a) Montrer que $\Phi_n = \prod_k \left(X - \exp \frac{2ik\pi}{n} \right)$ où k décrit l'ensemble des entiers inférieurs ou égaux à n et premiers avec n , est à coefficients entiers.

b) Que peut-on dire d'un nombre premier p divisant $\Phi_n(a)$ où a est entier, mais aucun $\Phi_d(a)$ où d décrit l'ensemble des diviseurs stricts de n ?

c) En déduire qu'il existe une infinité de nombres premiers de la forme $\lambda n + 1$.

88)***(U07) **Équation de Fermat polynomiale.** Soit $n \in \mathbb{N}, n \geq 3$. Montrer qu'il n'existe pas de polynômes P, Q, R à coefficients complexes et non tous trois proportionnels tels que : $P^n + Q^n = R^n$.

89)***(U07) Soit S une partie du plan euclidien $\mathbb{R}^2$ telle que : $\forall p \in \mathbb{R}^2, \exists s \in S, \|p - s\| \leq 1$. Montrer que si $P \in \mathbb{R}[X, Y]$ s'annule sur S , alors $P = 0$.