I) Groupes

A) Groupe symétrique

Exercice 1: ★★ *b.03.007*

Soit $n \geqslant 3$. Déterminer l'ensemble des permutations de $\mathfrak{S}_n$ commutant avec tous les éléments de $\mathfrak{S}_n$.

Exercice 2: ★★★ *b.03.009*

Pour $\sigma \in \mathfrak{S}_n$, on note $\varepsilon(\sigma)$ sa signature et $\nu(\sigma)$ son nombre de points fixes. Calculer $\displaystyle\sum_{\sigma\in\mathfrak{S}_n} \frac{\varepsilon(\sigma)}{\nu(\sigma)+1}$.

Exercice 3: ★★★ *b.03.009*

1. Donner le nombre minimal de permutations nécessaires pour engendrer $\mathfrak{S}_n$.
2. Donner le nombre minimal de transpositions nécessaires pour engendrer $\mathfrak{S}_n$.
3. On suppose que pour toute transposition τ de $\mathfrak{S}_n$, et tout n-cycle c de $\mathfrak{S}_n$, les permutations τ et c engendrent $\mathfrak{S}_n$. Montrer que n est premier.
4. Réciproquement, montrer que si n est premier alors pour toute transposition τ de $\mathfrak{S}_n$, et tout n-cycle c de $\mathfrak{S}_n$, les permutations τ et c engendrent $\mathfrak{S}_n$.
5. Soient $n \geqslant 2$ un entier, a et b deux éléments distincts de $[\![1\,,n]\!]$, et $G_{a,b}$ le sous-groupe de $\mathfrak{S}_n$ engendré par $(a\ \ b)$ et $(1\ \ 2\ \ \ldots\ \ n)$. A quelle condition a-t-on $G_{a,b} = \mathfrak{S}_n$?

B) Ordre et sous-groupes

Exercice 4: ★ *d.51.001*

Montrer que
$$\{x + y\sqrt{3}, x \in \mathbb{N}, y \in \mathbb{Z}, x^2 - 3y^2 = 1\}$$
est un sous-groupe de $(\mathbb{R}_+^*, \times)$.

Exercice 5: ★ *d.51.002*

Un sous-groupe d'un groupe produit est-il nécessairement produit de deux sous-groupes ?

Exercice 6: ★ *d.51.054*

Décrire les sous-groupes finis de $(\mathbb{C}^*, \times)$.

Exercice 7: ★ *d.51.033*

Montrer que le sous-ensemble formé des éléments d'ordre fini d'un groupe abélien en est un sous-groupe.

Exercice 8: ★★ *d.51.004*

Soit E un espace euclidien. On note $\mathcal{S}$ l'ensemble des endormorphismes f de E vérifiant

$$\forall (x,y) \in E^2, \langle x \mid y \rangle = 0 \iff \langle f(x) \mid f(y) \rangle = 0$$

Montrer que $\mathcal{S}$ est un groupe pour la loi de composition des applications.

Exercice 9: ★★ *d.51.039*

Pour tout $(a,b) \in \mathbb{C}^* \times \mathbb{C}*$, on considère

$$f_{a,b} : \begin{cases} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & az+b \end{cases}$$

1. Montrer que l'ensemble $\{f_{a,b}, a \in \mathbb{C}^*, b \in \mathbb{C}\}$ est muni d'une structure de groupe pour la loi $\circ$.
2. Déterminer les éléments d'ordre fini de ce groupe.

Exercice 10: ★★ *d.51.044*

Soit $(G,.)$ un groupe de cardinal $2n$.

1. Justifier que l'on définit une relation d'équivalence $\sim$ sur G en posant

$$x \sim y \iff x = y \text{ ou } x = y^{-1}$$

2. En déduire l'existence dans G d'un élément d'ordre 2.

Exercice 11: ★★ *d.51.057*

Soient H et K deux sous-groupes d'un groupe fini G noté multiplicativement. On note $HK = \{hk \mid h \in H, k \in k\}$. Montrer

$$|HK||H \cap K| = |H||K|$$

Exercice 12: ★★★ *d.51.011*

1. Montrer que tout sous-groupe additif de $\mathbb{R}$ qui n'est pas monogène est dense dans $\mathbb{R}$.
2. Soit $x \in \mathbb{R} \backslash \mathbb{Q}$. Montrer qu'il existe une infinité de $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que

$$|x - \frac{p}{q}| < \frac{1}{q^2}$$

3. Montrer la divergence de la suite de terme général

$$u_n = \frac{1}{n \sin n}$$

Exercice 13: ★★★ *d.51.061*

Lemme de Cauchy.
Soient $(G, .)$ un groupe fini et $p \in \mathbb{P}$ tel que $p \mid n = |G|$. On souhaite montrer qu'il existe un élément d'ordre p dans G. On introduit :

$$E = \{(g_1, g_2, \ldots, g_p) \in G^p \mid g_1 g_2 \ldots g_p = 1\}$$

et la relation d'équivalence $\mathcal{R}$ donnée par :

$$(g_1, g_2, \ldots, g_p)\mathcal{R}(h_1, h_2, \ldots, h_p) \iff \exists k \in \mathbb{Z}, \forall i \in [\![1\,, p]\!]\,, h_i = g_{\overline{i+k}^p}$$

où l'on adopte une notation circulaire : $g_{\overline{p+1}^p} = g_1$. . . .

1. Déterminer $|E|$.
2. Montrer qu'une classe d'équivalence pour la relation $\mathcal{R}$ est de cardinal 1 ou p.
3. En déduire l'existence d'un élément $g \in G$ différent de 1 et vérifiant $g^p = 1$.

C) Groupes cycliques et monogènes

Exercice 14: ★ *b.003.015*

Soit G un groupe cyclique de cardinal n. Quel est le nombre de sous-groupes de G ?

Exercice 15: ★ *d.51.013*

1. Vérifier que $\frac{1}{3}\mathbb{Z} + \frac{3}{5}\mathbb{Z}$ est un sous-groupe monogène de $(\mathbb{Q}, +)$.
2. Même question avec $\frac{2}{3}\mathbb{Z} + \frac{4}{5}\mathbb{Z}$.

Exercice 16: ★ *d.51.014*

Dans $(\mathbb{C}^*, \times)$, déterminer le sous-groupe $\langle \mathbb{P} \rangle$ engendré par l'ensemble $\mathbb{P}$ des nombres premiers.

Exercice 17: ★★ *b.03.004*

1. Si $\alpha \in \mathbb{N}^*$, résoudre $x^2 = 1$ dans l'anneau $\mathbb{Z}/2^\alpha\mathbb{Z}$.
2. Pour quels $\alpha \in \mathbb{N}^*$ le groupe $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est-il cyclique ?

Exercice 18: ★★ *b.003.017*

Soient G un groupe fini de neutre 1_G et, pour d diviseur de G, $n_d(G)$ le nombre d'éléments d'ordre d de G.

1. Que vaut $\sum_{d|n} n_d(G)$, où $n = |G|$?
2. Que déduire de la question précédente si G est cyclique ?
3. Montrer que G est cyclique *si et seulement si* , pour tout diviseur d de $|G|$, l'ensemble $\{x \in G, x^d = 1_G\}$ est de cardinal majoré par d.
4. On suppose qu'il existe un corps $\mathbb{K}$ tel que G soit un sous-groupe de $\mathbb{K}^*$. Montrer que G est cyclique.
5. Que dire dans la situation précédente si $\mathbb{K} = \mathbb{C}$?

Exercice 19: ★★ *d.51.020*

Soit A une partie non vide d'un groupe $(G, \star)$. En notant, $A' = \{a^{-1}, a \in A\}$. Montrer :

$$\langle A \rangle = \{a_1 \star \cdots \star a_n \mid n \in \mathbb{N}^*, a_1, \ldots, a_n \in A \cup A'\}$$

Exercice 20: ★★ *d.51.029*

Soit $(G, \star)$ un groupe cyclique à $n \geqslant 2$ éléments engendré par a.
Pour $r \in \mathbb{N}^*$, on introduit l'application $f : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x^r \end{array} \right.$. Enfin, on pose $d = n \wedge r$.

1. Vérifier que f est un endomorphisme du groupe $(G, \star)$.
2. Déterminer le noyau de f.
3. Montrer que $\mathrm{Im}(f) = \langle a^d \rangle$ sous-groupe de G.
4. Pour $y \in G$, combien l'équation $x^r = y$ possède-t-elle de solutions ?

D) Eléments de théorie des groupes

Exercice 21: ★ *d.51.045*

Les groupes $(\mathbb{Q}, +)$ et $(\mathbb{Q}^*, \times)$ sont-ils isomorphes ?

Exercice 22: ★★ *b.03.020*

On note S une partie non vide d'un groupe multiplicatif fini G de cardinal n, contenant l'élément neutre e de G. Pour $k \in \mathbb{N}^*$, $A_k = \left\{ \prod_{i=1}^{k} s_i, (s_1, \ldots, s_k) \in S^k \right\}$ et $a_k = |A_k|$.

1. Montrer que $(a_n)_{n \in \mathbb{N}^*}$ est une suite croissante.
2. Montrer que pour tout $k \geqslant n$, $a_{k+1} = a_k$.

3. Montrer que A_n est un sous-groupe de G.

Exercice 23: ★★ *d.51.050*

On note :

$$V = \left\{ \begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix}, (a,b,c,d) \in \mathbb{Z}^4 \right\}$$

et

$$G = \{M \in V \cap GL_4(\mathbb{R}) \mid M^{-1} \in V\}$$

1. Quelle est la structure de G ?
2. Soit $M \in V$. Montrer que $M \in G$ *si et seulement si* $det(M) = \pm 1$.s
3. Donner un groupe standard isomorphe à G muni du produit.

Exercice 24: ★★★ *b.03.023*

Soir G un groupe. On note $D(G)$ le groupe engendré par les $xyx^{-1}y^{-1}$ pour $x, y \in G$. On note D^n la n-ième itérée de l'opération D, et l'on dit que G est résoluble lorsqu'il existe $n \in \mathbb{N}^*$ tel que $D^n(G) = \{e\}$ où e est le neutre de G.

1. On suppose qu'il existe deux groupes H et N, deux morphismes $f : N \longrightarrow G$ et $g : G \longrightarrow H$ respectivement injectifs et surjectifs tels que $\mathrm{Ker}(s) = \mathrm{Im}(i)$. Montrer que G est résoluble *si et seulement si* H et N le sont.
2. Montrer que le groupe des permutations $\mathfrak{S}_5$ n'est pas résoluble.

Exercice 25: ★★★ *b.03.027*

Soient $(G, .)$ un groupe, $\mathrm{Aut}(G)$ l'ensemble de ses automorphismes.

1. Montrer que $(\mathrm{Aut}(G), \circ)$ est un groupe.
2. Quels sont les groupes finis tels que $\mathrm{Aut}(G)$ soit réduit à un élément ?

E) Exemples et contre-exemples

E.1 Centre d'un groupe

On rappelle que pour G un groupe, $Z(G)$ est le sous-groupe de G des éléments commutant avec tous les autres éléments du groupe.

Exercice 26: ★ *h.2.11*

Montrer que $\mathfrak{S}_3$ est un groupe d'ordre 6 qui n'est pas commutatif.

Exercice 27: ★★ *h.2.12*

Trouver un groupe dont le centre est réduit à l'élément neutre.

E.2 Sous-groupes et ordre

Exercice 28: ★ *h.2.15*

Montrer que $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un groupe dont tous les sous-groupe stricts sont cycliques mais que G n'est pas cyclique.

Exercice 29: ★ *h.2.21*

Trouver trois éléments a, b et c du groupe $\mathfrak{S}_3$ tels que $a \circ b \circ c$ et $c \circ b \circ a$ n'ont pas le même ordre.

Exercice 30: ★★★ *h.2.20*

Trouver un groupe non commutatif dans lequel tout sous-groupe strict est commutatif et distingué.

E.3 Algèbre linéaire

Exercice 31: ★ *d.51.068*

Soit

$$M = \begin{pmatrix} 0 & 1 & & (0) \\ & \ddots & \ddots & \\ (0) & & \ddots & 1 \\ 1 & (0) & & 0 \end{pmatrix} \in \mathcal{M}_n(\mathbb{C})$$

1. Calculer le polynôme caractéristique de M. La matrice M est-elle diagonalisable ? Est-elle inversible ?
2. Soit $G = \{M^k, k \in \mathbb{Z}\}$. Montrer que G est un groupe cyclique et préciser son cardinal.

Exercice 32: ★★ *d.51.070*

Soit G une partie de $\mathcal{M}_n(\mathbb{R})$ non réduite à la matrice nulle.
On suppose que $(G, \times)$ est un groupe. Montrer qu'il existe $r \in \mathbb{N}^*$ tel que le groupe $(G, \times)$ soit isomorphe à un sous-groupe de $(\mathrm{GL}_r(\mathbb{R}), \times)$.

II) Anneaux, point de vue arithmétique

A) Révisions d'arithmétique

Exercice 33: ★ *b.04.001*

Démontrer que pour tout entier $n \in \mathbb{N}^*$, $3^{2n} - 2^n$ est divisible par 7, $2^{4^n} + 5$ est divisible par 21, $3^{2n} + 2^{6n-5}$ est divisible par 11.

Exercice 34: ★ *b.04.002*

Résoudre : $\left\{ \begin{array}{l} x \equiv 2[3] \\ x \equiv 3[5] \end{array} \right., \left\{ \begin{array}{l} x \equiv 6[17] \\ x \equiv 4[15] \end{array} \right., \left\{ \begin{array}{l} x \equiv 2[11] \\ x \equiv 7[13] \end{array} \right.$ et $\left\{ \begin{array}{l} x \equiv 2[11] \\ x \equiv 7[13] \end{array} \right.$.

Exercice 35: ★ *b.04.003*

1. Déterminer l'ensemble des entiers naturels p, tels que les trois nombres p, $p+2$ et $p+4$ soient des nombres premiers.
2. Déterminer l'ensemble des entiers naturels premiers qui sont à la fois somme et différence de deux entiers naturels premiers.

Exercice 36: ★ *b.04.004*

Résoudre dans $\mathbb{Z}$: $2x + 3y = 1$ et $14x - 18y = 2$. Quelles sont les solutions de cette deuxième dans $\mathbb{N}$?

Exercice 37: ★ *b.04.005*

Montrer : $\forall (a,b) \in \mathbb{Z}^2, \forall n \in \mathbb{N}, a \equiv b[n] \Rightarrow a^n \equiv b^n[n^2]$.

Exercice 38: ★ *b.04.006*

Montrer que l'ensemble des nombres premiers est infini. Montrer que l'ensemble des nombres premiers congrus à -1 modulo 4 est infini.

Exercice 39: ★ *b.04.007*

Montrer qu'il existe des intervalles de $\mathbb{N}$ aussi longs que l'on veut qui ne contiennent aucun nombre premier.

Exercice 40: ★ *b.04.008*

Résoudre dans $\mathbb{Z}$ la congruence $9x \equiv 6[24]$.

Exercice 41: ★ *b.04.009*

Soient $a \geqslant 2$ et $r \geqslant 2$ des entiers. Montrer que si $(a^r - 1)$ est premmier alors $a = 2$ et r est premier. Montrer que si $a^n + 1$ est premier, avec $n \geqslant 1$ et $a \geqslant 2$, alors a est pair et n est une puissance de 2.

Exercice 42: ★ *b.04.010*

Pour tout $n \in \mathbb{N}$, on pose $M_n = 2^n - 1$.

1. Montrer que si $n \geqslant 2$, et si M_n est premier, alors n est premier.
2. Etudier la réciproque de cette propriété.

Exercice 43: ★ *b.04.011*

Déterminer les nombres premiers tels que p divise $2^p + 1$.

Exercice 44: ★ *b.04.012*

Déterminer l'ensemble des entiers relatifs n tels que $n^{13} \equiv n[42]$.

B) Valuation, nombres premiers

Exercice 45: ★★ *d.52.038*

Théorème de WILSON.
Soit $p \in \mathbb{P}$.

1. Quels sont les éléments de $\mathbb{Z}/p\mathbb{Z}$ égaux à leur inverse ?
2. En déduire que $p \mid (p-1)! + 1$.

Exercice 46: ★★ *b.04.013*

Formule de LEGENDRE.
Soit p un nombre premier. Pour tout $n \in \mathbb{N}^*$, notons $v_p(n!)$ l'exposant de p dans la décomposition en facteurs premiers de $n!$. Montrer que $v_p(n!) = \sum_{k\geqslant 1} \lfloor \frac{n}{p^k} \rfloor$.

En déduire le nombre de zéros à la fin de l'écriture décimale de 2023!.

Exercice 47: ★★ *b.04.014*

Nombres de Fermat. Pour tout $n \in \mathbb{N}$, on note $F_n = 2^{2^n} + 1$.

1. Montrer que, pour tout $k \in \mathbb{N}^*$: $(F_n - 1)^{2^k} + 1 = F_{n+k}$.
2. Montrer qu'il existe $q \in \mathbb{N}$ tel que $F_{n+k} = qF_n + 2$.
3. En déduire que pour $n \neq m$, F_n et F_m sont premiers entre eux.
4. Soit p un diviseur premier de F_k. Montrer que $p \wedge 2 = 1$. Trouver l'ordre de 2

dans le groupe $(\mathbb{Z}/p\mathbb{Z})^*$.

5. Soit $t \in [\![1\,,k+1]\!]$. Quelle est la classe de p modulo 2^t ?
6. Montrer que pour tout $t \in \mathbb{N}^*$, il existe une infinité de nombres premiers congrus à 1 modulo 2^t.

Exercice 48: ★★ *b.04.19*

Soient $a \geqslant 2$, n et m des entiers.

1. Montrer que si $m \in n$ alors $(a^m - 1) \mid (a^n - 1)$.
2. Montrer que $(a^m - 1) \wedge (a^n - 1) = (a^{m \wedge n} - 1)$.

C) Indicatrice d'Euler

Exercice 49: ★ *d.52.055*

Combien y a-t-il d'éléments inversibles dans $\mathbb{Z}/99\mathbb{Z}$?

Exercice 50: ★ *d.52.057*

Montrer :

$$\forall a \in (\mathbb{Z}/n\mathbb{Z})^*, a^{\varphi(n)} = 1$$

Exercice 51: ★★ *b.04.018*

Trouver tous les entiers naturels $n \geqslant 2$ tels que $\varphi(n) \mid n$.

Exercice 52: ★★ *b.04.022*

1. Montrer que $\forall n \in \mathbb{N}^*, \varphi(n) \geqslant \dfrac{\sqrt{n}}{2}$
2. Existe-t-il $C > 0$ tel que $\forall n \in \mathbb{N}^*, \varphi(n) \geqslant Cn$?

Exercice 53: ★★ *d.52.061*

Montrer :

$$\forall n \geqslant 3, \varphi(n) \geqslant \frac{n\ln(2)}{\ln(n) + \ln(2)}$$

Exercice 54: ★★ *d.52.065*

Déterminant de S*MITH*.
Calculer $\det((i \wedge j)_{(i,j)\in[\![1\,,n]\!]^2})$.

D) Equations

Exercice 55: ★ *d.52.034*

Résoudre les équations suivantes :

1. $3x + 5 = 0$ dans $\mathbb{Z}/10\mathbb{Z}$.
2. $x^2 = 1$ dans $\mathbb{Z}/8\mathbb{Z}$.
3. $x^2 + 2x + 2 = 0$ dans $\mathbb{Z}/5\mathbb{Z}$.

Exercice 56: ★★★ *b.04.015*

Soient $(x, y, z) \in (\mathbb{N}^*)^3$ tels que : $x^2 + y^2 = z^2$ et $x \wedge y \wedge z = 1$.

1. Montrer qu'il existe $n > m$ entiers premiers entre eux tels que, à permutation près de x et y, on ait : $x = 2nm, y = n^2 - m^2, z = n^2 + m^2$.
2. En déduire que l'aire du triangle de côté x, y et z n'est pas le carré d'un entier.

Exercice 57: ★★★ *b.04.027*

1. Soit α un nombre réel irrationnel. Montrer que, pour tout $n \in \mathbb{N}^*$, il existe $(p, q) \in \mathbb{Z} \times [\![1\,, n]\!]$ tel que $|\alpha - \dfrac{p}{q}| < \dfrac{1}{qn}$.
2. Soit $d \in \mathbb{N}^*$. On suppose que d n'est pas carré parfait.
   Montrer que l'équation $a^2 - db^2 = 1$ possède une solution $(a, b) \in \mathbb{Z}^2$ telle que $b \neq 0$.

Exercice 58: ★★★ *b.04.035*

Pour $n \in \mathbb{N}^*$, on note $C_n = \{(x, y) \in (\mathbb{Q}^*)^2, x^2 + y^2 = n\}$.

1. Montrer que C_1 est non-vide.
2. Montrer que C_7 est vide.
3. Soit $n \in \mathbb{N}^*$. On suppose que C_n est non-vide. Montrer que C_n est infini.

III) Anneaux, point de vue structurel

A) Généralités sur les anneaux

Exercice 59: ★ *d.52.001*

Soit a un élément d'un anneau $(A, +, \times)$.
Montrer que si a est nilpotent alors $1_A - a$ est inversible.

Exercice 60: ⋆ *d.52.002*

Montrer qu'un anneau $(A,+,\times)$ n'a pas de diviseurs de zéro *si et seulement si* tous ses éléments non nuls sont réguliers.

Exercice 61: ⋆ *d.52.003*

Soient a, b deux éléments d'un anneau $(A,+,\times)$ tels que ab soit inversible et b non diviseur de 0.
Montrer que a et b sont inversibles.

Exercice 62: ⋆ *d.51.063*

Justifier que les éléments inversibles de l'anneau $\mathbb{Z}/11\mathbb{Z}$ constituent un groupe cyclique.

Exercice 63: ⋆ *d.52.033*

Soit $\mathbb{K}$ un corps fini. Calculer $\displaystyle\prod_{x\in\mathbb{K}^*} x$.

Exercice 64: ⋆ *d.52.042*

Soit $n \in \mathbb{N}$ impair. Calculer $\displaystyle\sum_{\overline{x}\in\mathbb{Z}/n\mathbb{Z}} \overline{x}$.

Exercice 65: ⋆ *d.52.043*

Soit $p \in \mathbb{P}$. Calculer dans $\mathbb{F}_p$:

1. $\displaystyle\sum_{k=1}^{p} \overline{k}$
2. $\displaystyle\sum_{k=1}^{p} \overline{k}^2$

Exercice 66: ⋆⋆ *d.51.062*

Déterminer les morphismes de groupes entre $(\mathbb{Z}/n\mathbb{Z},+)$ et $(\mathbb{Z}/m\mathbb{Z},+)$.

Exercice 67: ⋆⋆ *d.52.004*

Soient $(A,+,\times)$ un anneau commutatif intègre et G une partie finie non vide de $A\backslash\{0\}$ stable par multiplication.
Montrer que G est un sous-groupe du groupe $(A^\times,\times)$ constitué des éléments inversibles de l'anneau A.

B) Idéaux

Exercice 68: ★ *d.52.018*

Soient A un anneau commutatif et e un élément idempotent de A (*id est* $e^2 = e$).

1. Montrer que $J = \{x \in A \mid xe = 0\}$ est un idéal de A.
2. On note $I = Ae$ l'idéal principal engendré par e. Déterminer $I + J$ et $I \cap J$.
3. Etablir que pour tout idéal K de A :

$$(K \cap I) + (K \cap J) = K$$

Exercice 69: ★★ *d.52.010*

On note $\mathbb{D} = \left\{\dfrac{p}{10^n} \mid p \in \mathbb{Z}, n \in \mathbb{N}\right\}$ l'ensemble des nombres décimaux.

1. Montrer que $\mathbb{D}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.
2. Montrer que les idéaux de $\mathbb{D}$ sont principaux (c'est-à-dire de la forme $a\mathbb{D}$ avec $a \in \mathbb{D}$).

Exercice 70: ★★ *d.52.011*

Nilradical d'un anneau.
On appelle nilradical d'un anneau commutatif $(A, +, \times)$ l'ensemble N formé des éléments nilpotents de A, c'est-à-dire des $x \in A$ tels qu'il existe $p \in \mathbb{N}^*$ vérifiant $x^p = 0_A$.

1. Montrer que N est un idéal de $(A, +, \times)$.
2. Déterminer N lorsque $A = \mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}^*$.

Exercice 71: ★★ *d.52.013*

Soit $(A, +, \times)$ un anneau. On considère

$$R = \{x \in A \mid \forall a \in A, 1_A + ax \text{ est inversible}\}$$

Montrer que R est un idéal de A.

Exercice 72: ★★ *d.52.016*

Soit A un anneau intègre. On suppose que l'anneau A ne possède qu'un nombre fini d'idéaux.
Montrer que A est un corps.

C) Anneaux $\mathbb{Z}[\alpha]$

Exercice 73: ★★ *d.52.022*

On étudie l'ensemble $\mathbb{Z}[\mathrm{j}] = \{a + b\mathrm{j}, a, b \in \mathbb{Z}\}$.

1. Montrer que cet ensemble est un anneau.
2. Prouver qu'un élément $x \in \mathbb{Z}[\mathrm{j}]$ est inversible *si et seulement si* $|x| = 1$. Préciser alors quels sont les inversibles de $\mathbb{Z}[\mathrm{j}]$.
3. Soient $x, y \in \mathbb{Z}[\mathrm{j}]$ avec $y \neq 0$. Prouver l'existence de $(q, r) \in \mathbb{Z}[\mathrm{j}]^2$ vérifiant $x = qy + r$ et $|r| < |y|$.
4. En déduire que les idéaux de $\mathbb{Z}[\mathrm{j}$ sont de la forme $x\mathbb{Z}[\mathrm{j}]$ avec $x \in \mathbb{Z}[\mathrm{j}]$.

Exercice 74: ★★ *b.03.043*

1. Montrer que, si un nombre réel s'écrit $a + b\sqrt{2}$ avec $(a, b) \in \mathbb{Z}^2$, cette écriture est unique.
2. Montrer que l'ensemble $\mathbb{Z}[\sqrt{2}]$ des nombres réels de la forme précédente est sous-anneau de $\mathbb{R}$.
3. Déterminer les automorphismes de l'anneau $\mathbb{Z}[\sqrt{2}]$.
4. Si $(x, y) \in \mathbb{Z}^2$ et $z = x + \sqrt{2}y$, on pose $N(z) = x^2 - 2y^2$. Montrer que z est un inversible de $\mathbb{Z}[\sqrt{2}]$ *si et seulement si* $N(z) = \pm 1$.
5. Montrer que les inversibles de $\mathbb{Z}[\sqrt{2}]$ sont $\pm(1 + \sqrt{2})^k$ avec $k \in \mathbb{Z}$.

Exercice 75: ★★ *b.03.044*

On note $\mathbb{Z}[\mathrm{i}\sqrt{2}] = \{a + \mathrm{i}b\sqrt{2}, (a, b) \in \mathbb{Z}^2\}$.

1. Montrer que $\mathbb{Z}[\mathrm{i}\sqrt{2}]$ est un sous-anneau de $\mathbb{Q}$.
2. Montrer que l'anneau $A = \mathbb{Z}[\mathrm{i}\sqrt{2}]$ est euclidien, c'est-à-dire qu'il existe une fonction $N : \mathbb{Z}[\mathrm{i}\sqrt{2}] \longrightarrow \mathbb{N}$ telle que pour tout $(a, b) \in A \times (A \backslash \{0\})$, il existe un couple $(q, r) \in A^2$ tel que $a = bq + r$ et $N(r) < N(b)$.
3. Enoncer et démontrer un théorème d'existence et d'unicité d'une décomposition en facteurs irréductibles dans $\mathbb{Z}[\mathrm{i}\sqrt{2}]$.

D) Exemples et contre-exemples

Exercice 76: ★ *h.3.1*

Trouver un anneau infini puis fini qui n'est pas un anneau commutatif.

Exercice 77: ★★ *h.3.1*

Trouver un anneau commutatif non nul qui n'est pas un anneau intègre.

Exercice 78: ★★ *h.3.39*

Trouver un corps non-commutatif (*id est* un corps gauche).

Exercice 79: ★★★ *h.3.30*

Montrer que $\mathbb{Z}\left[\frac{1}{2}+\mathrm{i}\frac{\sqrt{19}}{2}\right]$ est un anneau principal qui n'est pas un anneau euclidien.

IV) Polynômes

A) Généralités et équations

Exercice 80: ★ *d.36.001*

Soit $(P_n)_{n\in\mathbb{N}^*}$ la suite de polynômes définie par

$$P_1 = X - 2 \text{ et } P_{n+1} = P_n^2 - 2 \text{ pour tout } n \in \mathbb{N}^*$$

Calculer le coefficient de X^2 dans P_n.

Exercice 81: ★ *d.36.002*

1. Pour $n \in \mathbb{N}$, développer le polynôme $(1+X)(1+X^2)(1+X^4)\dots(1+X^{2^n})$.
2. En déduire que tout entier $p > 0$ s'écrit de façon unique comme somme de puissances de 2.

Exercice 82: ★ *d.36.006*

Trouver les $P \in \mathbb{R}[X]$ tels que $P(X^2) = (X^2+1)P(X)$.

Exercice 83: ★ *d.36.008*

Résoudre les équations suivantes :

1. $Q^2 = XP^2$ d'inconnues $P, Q \in \mathbb{K}[X]$.
2. $P \circ P = P$ d'inconnue $P \in \mathbb{K}[X]$.

Exercice 84: ★ *d.36.012*

Trouver tous les polynômes $P \in \mathbb{R}[X]$ tels que

$$\forall k \in \mathbb{Z}, \int_k^{k+1} P(t)\,\mathrm{d}t = k+1$$

Exercice 85: ★ *d.36.015*

Soit $P \in \mathbb{R}[X]$. On suppose que $a \in \mathbb{R}$ vérifie

$$P(a) > 0 \text{ et } \forall k \in \mathbb{N}^*, P^{(k)}(a) \geqslant 0$$

Montrer que le polynôme P ne possède pas de racines dans $[a\,, +\infty[$.

Exercice 86: ★★ *d.36.110*

Polynômes de Legendre.
Pour tout $n \in \mathbb{N}$, on pose :

$$L_n = \frac{n!}{(2n)!}\left((X^2-1)^n\right)^{(n)}$$

1. Montrer que L_n est un polynôme unitaire de degré n.
2. Vérifier que pour tout polynôme réel Q avec $\deg Q < n$, on a
$$\int_{-1}^{1} L_n(t)Q(t)\,\mathrm{d}t = 0$$
3. En déduire que L_n possède n racines simples toutes dans l'intervalle $]-1\,,1[$.

Exercice 87: ★★ *d.36.004*

Soit $P \in \mathbb{C}[X]$ non constant et tel que $P(0) = 1$. Montrer que :

$$\forall \varepsilon > 0, \exists z \in \mathbb{C}, |z| < \varepsilon \text{ et } |P(z)| < 1$$

B) Division euclidienne, divisibilité, PGCD

Exercice 88: ★ *b.05.004*

Soit $P \in \mathbb{C}[X]$ non-nul tel que $P(X^2) = P(X+1)P(X)$.

1. Montrer que toute racine de P est soit nulle soit de module 1.
2. Déterminer P.

Exercice 89: ★ *d.36.034*

Montrer les divisibilités suivantes et déterminer les quotients correspondants :

1. $X-1 \mid X^3-2X^2+3X-2$
2. $X-2 \mid X^3-3X^2+3X-2$
3. $X+1 \mid X^3+3X^2-2$

Exercice 90: ★ *d.36.040*

En réalisant une division euclidienne, former une condition nécessaire et suffisante sur $(\lambda, \mu) \in \mathbb{K}^2$ pour que $X^2 + 2$ divise $X^4 + X^3 + \lambda X^2 + \mu X + 2$.

Exercice 91: ★ *d.36.042*

Soient $t \in \mathbb{R}$ et $n \in \mathbb{N}^*$.
Déterminer le reste de la division euclidienne dans $\mathbb{R}[X]$ de $(X \cos t + \sin t)^n$ par $X^2 + 1$.

Exercice 92: ★ *d.36.045*

Soient $a, b \in \mathbb{R}$ distincts. Montrer qu'il existe un unique endomorphisme φ de $\mathbb{R}[X]$ vérifiant :

$$\begin{cases} \varphi(1) = 1 \\ \varphi(X) = X \\ \forall X \in \mathbb{R}[X], P(a) = P(b) = 0 \Longrightarrow \varphi(P) = 0 \end{cases}$$

Exercice 93: ★★ *b.05.005*

1. Déterminer les polynômes P tels que P' divise P.
2. Déterminer les polynômes P tels que P divise XP'.

Exercice 94: ★★ *b.05.007*

Soit $n \in \mathbb{N}^*$. On pose $\omega = e^{\frac{2i\pi}{n}}$. Pour $P \in \mathbb{C}_{n-1}[X]$, on pose $\mathcal{F}(P) = \sum_{k=0}^{n-1} P(\omega^k) X^k$ et $\tilde{\mathcal{F}}(P) = \sum_{k=0}^{n-1} P(\omega^{-k}) X^k$.

1. Montrer que $\mathcal{F}$ et $\tilde{\mathcal{F}}$ sont des automorphismes de $\mathbb{C}_{n-1}[X]$.
2. Calculer $\tilde{\mathcal{F}} \circ \mathcal{F}$.
3. Soit $P \in \mathbb{Z}[X]$ tel que, pour tout $z \in \mathbb{U}_n$, $|P(z)| \leqslant 1$. On suppose que P possède une racine dans $\mathbb{U}_n$. Montrer que $X^n - 1$ divise P.

Exercice 95: ★★ *d.36.050*

Soient $A, B \in \mathbb{K}[X]$ tels que $A^2 \mid B^2$. Montrer que $A \mid B$.

Exercice 96: ★★★ *b.05.008*

Quels sont les $P \in \mathbb{Z}[x]$ tels que $\forall z \in \mathbb{U}$, $|P(z)| \leqslant 1$?

C) Racines, factorisation et irréductiblité des polynômes

Exercice 97: ★ *b.05.011*

Soit $P \in \mathbb{R}[X]$ simplement scindé sur $\mathbb{R}$.

1. Montrer que P' est simplement scindé sur $\mathbb{R}$.
2. Comparer les moyennes arithmétiques des racines de P et P'.

Exercice 98: ★ *p.05*

Soient $(\alpha_j)_{1\leqslant j\leqslant 4}$ les 4 racines de $P = X^4 - pX^3 + qX + r$. Calculer :

$$\sum_{j=1}^{4} \alpha_j^7$$

Exercice 99: ★ *d.36.021*

Justifier que tout polynôme réel de degré impair possède au moins une racine réelle :

1. en employant le théorème des valeurs intermédiaires ;
2. en employant le théorème de décomposition en facteurs irréductibles.

Exercice 100: ★ *d.36.058*

Soit $(n, p, q) \in \mathbb{N}^3$. Justifier

$$1 + X + X^2 \mid X^{3n} + X^{3p+1} + X^{3q+2}$$

Exercice 101: ★ *d.36.072*

Soit $n \in \mathbb{N}^*$.

1. Décomposer $X^n - 1$ en facteurs irréductibles dans $\mathbb{C}[X]$.
2. Décomposer $X^n - 1$ en facteurs irréductibles dans $\mathbb{R}[X]$.

Exercice 102: ★★ *b.05.013*

Soit $\Gamma = \{P \in \mathbb{R}[X], \exists (A, B) \in \mathbb{R}[X]^2, P = A^2 + B^2\}$.

1. Montrer que Γ est stable par produit.
2. Montrer l'équivalence : $\forall P \in \mathbb{R}[X], (P \in \Gamma) \iff (\forall x \in \mathbb{R}, P(x) \geqslant 0)$.
3. Montrer l'équivalence : $\forall P \in \mathbb{R}[X], (\forall x \in \mathbb{R}_+, P(x) \geqslant 0) \iff (\exists (A, B) \in \Gamma^2, P = A + XB)$.

Exercice 103: ★★ *b.05.045*

Soit $P \in \mathbb{R}[X]$ un polynôme scindé.

1. Montrer que $x \mapsto (P'(x))^2 - P(x)P''(x)$ est de signe constant sur $\mathbb{R}$.
2. Si $P = \sum_{k=0}^{n} a_k X^k$, montrer que pour tout $k \in [\![1\,, n-1]\!]$, $a_{k-1}a_{k+1} \leqslant a_k^2$.

Exercice 104: ★★ *b.05.015*

Pour $P \in \mathbb{C}[X]$ non constant, soit $Z(P)$ l'ensemble des racines de P dans $\mathbb{C}$. Soient P et Q dans $\mathbb{C}[X]$ non constants tels que $Z(P) = Z(Q)$ et $Z(P-1) = Z(Q-1)$. Montrer que $P = Q$.

Exercice 105: ★★ *b.05.033*

Soit $P \in \mathbb{Z}[X]$. On suppose que, pour tout $n \in \mathbb{N}$, $P(n)$ est premier. Montrer que P est constant.

Exercice 106: ★★ *d.36.024*

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$. On pose $M = \sup_{|z|=1} |P(z)|$. Montrer que :

$$\forall k \in [\![0\,, n]\!]\,, |a_k| \leqslant M$$

Indication. On pourra employer des racines de l'unité.

Exercice 107: ★★ *d.36.028*

1. Montrer que $a = \cos\left(\frac{\pi}{9}\right)$ est racine d'un polynôme de degré 3 à coefficients dans $\mathbb{Z}$.
2. Justifier que le nombre a est irrationnel.

Exercice 108: ★★ *d.36.063*

Soient P un polynôme à coefficients entiers et quatre entiers $\lambda_1, \ldots, \lambda_4$ distincts tels que $P(\lambda_i) = 7$ pour $i \in [\![1\,, 4]\!]$.
Montrer que l'équation $P(n) = 14$ n'admet pas de solution entière.

Exercice 109: ★★ *d.36.076*

Pour $n \in \mathbb{N}^*$ on pose $P_n = \sum_{k=0}^{n} X^k$.

1. Donner la décomposer en facteurs irréductibles de P_n dans $\mathbb{C}[X]$.

2. En déduire la valeur de $\prod_{k=1}^{n} \sin\left(\frac{k\pi}{n+1}\right)$.

Exercice 110: ★★ *d.36.087*

Soit $P \in \mathbb{R}[X]$ scindé sur $\mathbb{R}$.
Montrer que pour tout réel α, le polynôme $P' + \alpha P$ est scindé sur $\mathbb{R}$.

Exercice 111: ★★ *d.36.092*

Déterminer les triplets $(x, y, z) \in \mathbb{C}^3$ tels que :

1. $\begin{cases} x+y+z & = 1 \\ \dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z} & = 1 \\ xyz & = -4 \end{cases}$
2. $\begin{cases} x(y+2) & = 1 \\ y(z+x) & = 1 \\ z(x+y) & = 1 \end{cases}$
3. $\begin{cases} x+y+z & = 2 \\ x^2+y^2+z^2 & = 14 \\ x^3+y^3+z^3 & = 20 \end{cases}$

Exercice 112: ★★ *d.36.098*

Déterminer les triplets $(x, y, z) \in \mathbb{C}^3$ vérfiant :

- $|x| = |y| = |z|$
- $x + y + z = xyz = 1$

Exercice 113: ★★★ *b.05.016*

Soit $P \in \mathbb{R}[X]$ unitaire de degré de n. Montrer que $\max_{x\in[-1,1]} |P(x)| \geqslant \frac{1}{2^{n-1}}$.

Exercice 114: ★★★ *b.05.021*

Soient (a_n) une suite de complexes non nuls, et $P_n = a_0 + a_1X + \cdots + a_nX^n$. Soit $r > 0$. Montrer que pour n assez grand, les racines de P_n ne sont pas toutes dans le disque $|z - r| < r$.

Exercice 115: ★★★ *d.36.104*

Sommes de Newton.

On considère le polynôme $P = \sum_{k=0}^{n} a_{n-k} X^k \in \mathbb{C}[X]$ de racines $x_1, \ldots, x_n$ comptées avec multiplicité.

Pour tout $p \in \mathbb{N}$, on pose $S_p = \sum_{j=1}^{n} x_j^p$.

Etablir :

$$\begin{cases} a_0 S_1 + a_1 & = 0 \\ a_0 S_2 + a_1 S_1 + 2a_2 & = 0 \\ \ldots & \\ a_0 S_p + a_1 S_{p-1} + \cdots + a_{p-1} S_1 + p a_p & = 0, p \in [\![1\,, n]\!] \\ \ldots & \\ a_0 S_n + a_1 S_{n-1} + \cdots + a_n S_1 & = 0 \\ a_0 S_{n+k} + a_1 S_{n+k-1} + \cdots + a_n S_k & = 0, k > 0 \end{cases}$$

D) Extensions de corps

Exercice 116: ★ *d.52.025*

On considère l'ensemble $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid (a, b) \in \mathbb{Q}^2\}$. Montrer que c'est un corps muni des opérations usuelles.

Exercice 117: ★ *d.52.029*

Soient $\mathbb{K} \subseteq \mathbb{L}$ deux corps tel que $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie. Soit E un $\mathbb{L}$-espace vectoriel de dimension finie.
Montrer que E est un $\mathbb{K}$-espace vectoriel et

$$\dim_{\mathbb{K}}(E) = \dim_{\mathbb{K}}(\mathbb{L}) \dim_{\mathbb{L}}(E)$$

Exercice 118: ★★ *d.52.030*

On considère le polynôme $P = X^3 - X + 1$.

1. Justifier que P est irréductible dans $\mathbb{Q}[X]$.
2. Montrer que le polynôme P admet une unique racine réelle x et vérifier que celle-ci n'est pas rationnelle.
3. Déterminer la dimension de $F = \mathrm{Vect}_{\mathbb{Q}}((x^k)_{k \in \mathbb{N}})$.
4. L'espace F est-il un corps ?

Exercice 119: ⋆⋆ *d.52.031*

Soit $K = \mathbb{Q} + \sqrt{2}\mathbb{Q} + \sqrt{3}\mathbb{Q} + \sqrt{6}\mathbb{Q}$.

1. Montrer que $(a, \sqrt{2}, \sqrt{3}, \sqrt{6})$ est une $\mathbb{Q}$-base du $\mathbb{Q}$-espace vectoriel K.
2. Montrer que K est un sous-corps de $\mathbb{R}$.

Exercice 120: ⋆⋆⋆ *b.05.025*

Soit $\omega = e^{\frac{2\pi}{5}}$.

1. Déterminer le polynôme minimal de ω.
2. On pose $\mathbb{K} = \text{Vect}(1, \omega, \omega^2, \omega^3)$. Déterminer sa dimension comme $\mathbb{Q}$-espace vectoriel. Montrer que c'est un sous-corps de $\mathbb{C}$.
3. Comment trouver l'expression de l'inverse d'un élément non nul de $\mathbb{K}$?
4. Montrer qu'il existe un unique automorphisme σ de $\mathbb{K}$ tel que $\sigma(\omega) = \omega^2$.
5. Soit τ un automorphisme de $\mathbb{K}$. Montrer qu'il existe $k \in [\![1\,,4]\!]$ tel que $\tau = \omega^4$.

Exercice 121: ⋆⋆⋆ *b.05.027*

Soit $\mathcal{A}$ une $\mathbb{R}$-algèbre commutative intègre de dimension finie.

1. Montrer que $\mathcal{A}$ est un corps.
2. Montrer que, pour tout $a \in \mathcal{A}$, l'ensemble $\{P \in \mathbb{R}[X], P(a) = 0\}$ est un idéal engendré par un polynôme irréductible.
3. Montrer que $\mathcal{A}$ est isomorphe à $\mathbb{R}$ ou $\mathbb{C}$.

E) Exemples et contre-exemples

Exercice 122: ⋆ *h.3.10*

Trouver deux polynômes P et Q tels que $\deg(PQ) < \deg P + \deg Q$.

Exercice 123: ⋆ *h.3.17*

Trouver deux polynômes tels que leurs applications associées soient égales.

Exercice 124: ⋆⋆ *h.3.12, h.3.13*

Trouver un polynôme de degré 1 n'ayant pas de racine, puis un polynôme de degré 1 ayant deux racines.
Trouver un polynôme de degré 2 ayant 4 racines.

Exercice 125: ⋆⋆ *h.3.11*

Trouver deux polynômes P et Q tels que $\text{val}(PQ) > \text{val}P + \text{val}Q$.

Exercice 126: ★★ *h.3.18*

Montrer que $X^3 - 2$ est irréductible de degré 3 dans $\mathbb{Q}[X]$.

Exercice 127: ★★★ *h.3.14*

Trouver un polynôme de degré 2 ayant une infinité de racines.

V) Fractions rationnelles

Exercice 128: ★★ *b.05.048*

Soit $P \in \mathbb{C}[X]$, un polynôme scindé à racines simples. On note $x_1, x_2, \dots, x_n$ ses racines. On suppose que P ne s'annule pas en 0.

1. Montrer que : $\displaystyle\sum_{i=1}^{n} \frac{1}{x_i P'(x_i)} = -\frac{1}{P(0)}$.
2. Soit $Q \in \mathbb{C}[X]$ tel que $\deg Q \leqslant n-2$. Calculer $\displaystyle\sum_{i=1}^{n} \frac{Q(x_i)}{P'(x_i)}$.

Exercice 129: ★★★ *b.05.047*

1. Déterminer les $P \in \mathbb{C}[X]$ tels que $P(\mathbb{U}) \subseteq \mathbb{U}$.
2. Déterminer les $F \in \mathbb{C}[X]$ tels que $F(\mathbb{U}) \subseteq \mathbb{U}$.

Exercice 130: ★★★ *b.05.051, b.11.019*

Si $P \in \mathbb{C}[X]\backslash\{0\}$ et $r > 0$, soit $N_r(P)$ le nombre de racines de P de module au plus r comptées avec multiplicités. On admet dans les deux premières questions le résultat suivant : si P et Q sont dans $\mathbb{C}[X]\backslash\{0\}$ et $\mathbb{C}[X]$ respectivement, si $r > 0$ est tel que pour tout $x \in \mathbb{C}$ de module r, $|Q(z)| \leqslant |P(z)|$, alors $N_r(P+Q) = N_r(P)$.

1. Déduire de l'énoncé admis le théorème de d'Alembert-Gauss.
2. Soit $P = X^4 + 6X + 3$. Déterminer $N_2(P)$, $N_1(P)$, et $N_{\frac{1}{3}}(P)$.
3. Soient $r > 0$ et $P \in \mathbb{C}[X]\backslash\{0\}$ ne s'annulant pas sur le centre de centre 0 et de rayon r. Montrer que
$$N_r(P) = \frac{1}{2\pi}\int_{-\pi}^{\pi} \frac{P'}{P}(re^{\mathrm{i}t})re^{\mathrm{i}t}\,\mathrm{d}t$$
d'abord en utilisant d'Alembert-Gauss, puis sans.
4. Déduire de la question précédente le résultat admis en début d'énoncé.
5. Pour toute fraction rationnelle $f \in \mathbb{C}(X)$ et tout réel r tel que f n'ait ni zéro ni pôle de module r on pose $N_r(f) = \displaystyle\frac{1}{2\pi}\int_0^{2\pi} \frac{f'(re^{\mathrm{i}t})}{f(re^{\mathrm{i}t})}re^{\mathrm{i}t}\,\mathrm{d}t$. Prouver que, lorsque

$N_r(f)$ est bien défini, il est égal au nombre de zéros de f dans le disque $\overline{B}(0,r)$ diminué du nombre de pôles de f dans le disque $\overline{B}(0,r)$ (les deux étant comptés avec multiplicité).

Exercice 131: ★★★ *b.05.052*

Soit $n \in \mathbb{N}^*$. On note $\mathbb{U}_n$ l'ensemble des racines complexes de $X^n + 1$.

1. Avec la décomposition en éléments simples de la fraction rationnelle $\dfrac{1}{X^n+1}$, calculer $\displaystyle\sum_{z\in\mathbb{U}_n} \frac{z}{1-z}$.
2. Montrer que pour tout $P \in \mathbb{C}_n[X]$, $XP'(X) = \dfrac{n}{2}P(X) + \dfrac{2}{n}\displaystyle\sum_{z\in\mathbb{U}_n} \frac{zP(zX)}{(z-1)^2}$.
3. Pour $Q \in \mathbb{C}[X]$, on pose $\|Q\| = \sup\limits_{z\in\mathbb{U}} |Q(z)|$. Montrer que pour tout $P \in \mathbb{C}_n[X]$, $\|P'\| \leqslant n\|P\|$.