Dans tout ce cours, K désigne $\mathbb{R}$ ou $\mathbb{C}$.

I) DÉFINITIONS

1) Fonctions polynômes.

DEF : une application f d'une partie I de K dans K est dite *polynomiale* (ou appelée une *fonction polynôme*) si

$$\exists n \in \mathbb{N}\ \exists (a_0, a_1, ..., a_n) \in K^{n+1} \ / \ \forall x \in I \ \ f(x) = \sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + ... + a_n x^n$$

L'ensemble des fonctions polynomiales de I dans K est noté $\mathcal{P}(I, K)$.

PROP : $\mathcal{P}(I, K)$ est à la fois un sous-espace vectoriel et un sous-anneau de $\mathcal{A}(I, K) = K^I$ (muni de l'addition et de la multiplication externe dans le premier cas, et muni de l'addition et de la multiplication interne dans le deuxième).
D1

2) Polynômes formels.

DEF : un polynôme (formel, à une indéterminée) sur le corps K est une suite définie sur $\mathbb{N}$ d'éléments de K, nulle à partir d'un certain rang ; l'ensemble de ces polynômes est noté $K[X]$:

$$K[X] = \left\{ (a_k)_{k \geqslant 0} \ / \ \left\{ \begin{array}{l} \forall k \in \mathbb{N} \ \ a_k \in K \\ \exists n \in \mathbb{N} \ / \ \forall k > n \ a_k = 0 \end{array} \right. \right\}$$

a_k est le *coefficient d'indice* k (ou de *rang* k) du polynôme $P = (a_k)$ (mais attention : a_k est le $k+1-$ième coefficient).
En particulier, le polynôme nul, noté par abus 0, est $(0, 0, ...)$, et l'*indéterminée*, notée X, est $(0, 1, 0, 0, ...)$.

DEF :

- le *degré* d'un polynôme non nul est l'indice maximum d'un coefficient non nul ; par convention, le degré du polynôme nul est $-\infty$.

$$\text{pour } P = (a_k)_{k \geqslant 0}, \deg P = \max_{a_k \neq 0} k$$

- la *valuation* d'un polynôme non nul est l'indice minimum d'un coefficient non nul ; par convention, la valuation du polynôme nul est $+\infty$.

$$\text{pour } P = (a_k)_{k \geqslant 0}, \operatorname{val} P = \min_{a_k \neq 0} k$$

E1

DEF :

- les polynômes de degré 0 et le polynôme nul sont dits *constants*.
- P est appelé un *monôme* si $\deg P = \operatorname{val} P$ (un seul coefficient non nul).
- si $n = \deg P$, le coefficient de rang n est appelé le coefficient *dominant* ou "*de tête*" du polynôme.
- un polynôme dont le coefficient dominant est égal à 1 est dit *normalisé*, ou *unitaire*.

Exemple : le monôme unitaire de degré 1 est $X = (0, 1, 0, 0...)$.

II) ESPACE VECTORIEL ET ANNEAU $K[X]$.

1) Espace vectoriel $K[X]$.

Remarquons que $K[X]$ est un sous-ensemble de $K^{\mathbb{N}}$, qui, muni de l'addition et de la multiplication à opérateurs dans K, est un K-espace vectoriel ; si $P = (a_k)_{k \geqslant 0}$ et $Q = (b_k)_{k \geqslant 0}$, par définition, $P + Q = (a_k + b_k)_{k \geqslant 0}$ et $\lambda P = (\lambda a_k)_{k \geqslant 0}$.

PROP : $K[X]$ est un sous-espace vectoriel de $K^{\mathbb{N}}$.
D2

2) Multiplication des polynômes ; anneau $K[X]$.

DEF : si $P = (a_k)$ et $Q = (b_k)$, par définition, $PQ = (c_k)$ avec

$$c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i} = a_0 b_k + a_1 b_{k-1} + ... + a_i b_{k-i} + ... + a_{k-1} b_1 + a_k b_0$$

REM : pour que ceci définisse bien une loi de composition interne dans $K[X]$, il faut vérifier que la suite (c_k) est bien nulle à partir d'un certain rang ; ceci vient de ce que :

PROP : si (a_k) est nulle à partir du rang $n+1$ et (b_k) est nulle à partir du rang $m+1$, (c_k) est nulle à partir du rang $n+m+1$; de plus $c_{n+m} = a_n b_m$.
D3

PROP : $(K[X], +, \times)$ est un anneau commutatif intègre.

D4
3) Notation classique $\sum\limits_{k \geqslant 0} a_k X^k$ des polynômes.

a) On remarque que si $\lambda \in K$

$$\begin{array}{rcl} (\lambda, 0, 0...) + (a_0, a_1, ...) & = & (\lambda + a_0, a_1, ...) \\ (\lambda, 0, 0...) \times (a_0, a_1, ...) & = & (\lambda a_0, \lambda a_1, ...) \end{array}$$

Il n'y a donc pas de contradiction à confondre le polynôme constant $(\lambda, 0, 0...)$ avec le scalaire λ, ce que l'on fait dorénavant ; le corps K est maintenant confondu avec l'ensemble des polynômes constants (donc $K \subset K[X]$).

b) On remarque que si $k \in \mathbb{N}$, $(a_0, a_1, ...) \times X = (0, a_0, a_1, ...)$ et donc $(0, 0, ..., 0, 1, 0, 0, ..)$ (avec le 1 au rang k) est égal à X^k (par convention, $X^0 = 1$).

c) On en déduit que $(a_0, a_1, ...)$ peut s'écrire sous la forme

$$\boxed{(a_0, a_1, ...) = a_0 + a_1 X + a_2 X^2 + ... = \sum_{k \geqslant 0} a_k X^k}$$

(cette dernière somme n'étant qu'en apparence infinie puisque les a_k sont nuls APCR).

D5

donc dorénavant $K[X] = \left\{ \sum\limits_{k \geqslant 0} a_k X^k / \left\{ \begin{array}{l} \forall k \in \mathbb{N} \;\; a_k \in K \\ \exists n \in \mathbb{N} \;/\; \forall k > n \;\; a_k = 0 \end{array} \right. \right\}$

REM : la propriété

$$\boxed{\left(\sum_{k \geqslant 0} a_k X^k = \sum_{k \geqslant 0} b_k X^k \right) \Rightarrow \forall k \in \mathbb{N} \;\; a_k = b_k}$$

est alors une évidence
(alors que

$$\boxed{\left(\forall x \in K \;\; \sum_{k \geqslant 0} a_k x^k = \sum_{k \geqslant 0} b_k x^k \right) \Rightarrow \forall k \in \mathbb{N} \;\; a_k = b_k}$$

n'en est pas une : voir plus loin).

4) Propriétés du degré et de la valuation vis-à-vis de la somme et du produit.

PROP : si $P, Q \in K[X]$

$\deg(P+Q) \leqslant \max(\deg P, \deg Q)$ avec égalité assurée si $\deg P \neq \deg Q$	$\operatorname{val}(P+Q) \geqslant \min(\operatorname{val} P, \operatorname{val} Q)$ avec égalité assurée si $\operatorname{val} P \neq \operatorname{val} Q$
$\deg PQ = \deg P + \deg Q$	$\operatorname{val} PQ = \operatorname{val} P + \operatorname{val} Q$

D6

5) Espace vectoriel des polynômes de degré inférieur ou égal à n.

PROP : pour tout naturel n, l'ensemble des polynômes de degré inférieur ou égal à n, noté $K_n[X]$ est un sous-espace vectoriel de $K[X]$; la famille $\left(1, X, X^2, ..., X^n\right)$ en est une base, appelée la *base canonique* ; la dimension de $K_n[X]$ est donc $n+1$.

D7

ATTENTION 1 : $\dim K_n[X] = n+1$ et non n !
ATTENTION 2 : $K_n[X]$ n'est pas un sous-anneau de $K[X]$, sauf pour $n = 0$.
ATTENTION 3 : l'ensemble des polynômes de degré n n'est pas stable par addition !

REM : $K_0[X] = K = \{\text{polynômes constants}\} = \{\text{polynômes de degré } 0\} \cup \{0\}$ est une droite vectorielle.

PROP : toute famille de polynômes de degrés distincts (ou de valuations distinctes) est libre. On en déduit que si (P_k) est une suite de polynômes telle que $\deg P_k = k$, alors $(P_0, P_1, ..., P_n)$ est une base de $K_n[X]$.
D8

III) SUBSTITUTION D'UNE VALEUR DÉTERMINÉE À L'INDÉTERMINÉE X.
1) Définition.

DEF : soit x un élément d'un anneau commutatif A qui est en même temps un K-espace vectoriel et $P = \sum_{k=0}^{n} a_k X^k$; on appelle *résultat de la substitution de x à l'indéterminée X* l'élément de A :

$$\boxed{P(x) = \sum_{k=0}^{n} a_k x^k = a_0 1_A + a_1 x + a_2 x^2 + ... + a_n x^n}$$

Exemples : $A = \mathbb{R}, A = \mathbb{C},\ A = \mathcal{M}_2(K)$, $A = K[X]$, $A = K^I$.

REM 1 : $P(X)$ est donc égal à P.

REM 2 : $P(Q)$ (résultat de la substitution de Q à X) dans P peut être confondu avec $P.Q$; quand il y a ambiguité, on le notera $P \circ Q$.
E3 polynômes de Tchebychev :
la suite de polynômes (T_n) définie par $T_0 = 1$, $T_1 = X$ et $T_{n+1} = 2XT_n - T_{n-1}$ pour $n \geqslant 1$ est telle que

$$\forall n \in \mathbb{N}\ \forall \theta \in \mathbb{R} \quad T_n(\cos\theta) = \cos(n\theta).$$

De plus, T_n est de degré n et son coefficient dominant est 2^{n-1} (pour $n \geqslant 1$).
2) Relations entre $K[X]$ et $\mathcal{P}(I, K)$.

PROP :

$$\forall P, Q \in K[X]\ \ \forall x \in K\ \left\{\begin{array}{c} (P+Q)(x) = P(x) + Q(x) \\ (PQ)(x) = P(x)\,Q(x) \\ (P \circ Q)(x)\,[\text{ou } (P(Q))(x)] = P(Q(x)) \end{array}\right.$$

D9

DEF : si P est un polynôme formel $\in K[X]$, la fonction polynôme définie sur I *associée* à P est la fonction f : $\left\{\begin{array}{l} I \to K \\ x \mapsto P(x) \end{array}\right.$

PROP : l'application Φ de $K[X]$ dans $\mathcal{P}(I, K)$ qui à tout polynôme associe cette fonction polynôme, qui est surjective par définition, est aussi un morphisme d'anneaux.

D10
IV) DIVISIBILITÉ DANS $K[X]$.

1) Relation de divisibilité.

DEF : soit A, B deux polynômes ; on dit que A *divise* B (ou que A est un *diviseur* de B ou encore que B est *multiple* de A) si

$$\exists Q \in K[X] \ / \ B = AQ$$

Notation : $A \mid B$.
E2 : déterminer les diviseurs normalisés de $X^4 - 1$

PROP : la relation $\mid$ est réflexive et transitive, mais non antisymétrique : ($A \mid B$ et $B \mid A$) équivaut à

$$\exists \lambda \in K^* \ / \ B = \lambda A$$

D11

DEF : deux polynômes qui se divisent mutuellement (ce qui équivaut à ce qu'ils diffèrent d'une constante multiplicative) sont dits *associés*.
REM : tout polynôme non nul est associé à un unique polynôme unitaire.

CORO : la relation $\mid$ est une relation d'ordre sur l'ensemble des polynômes unitaires.

2) Division euclidienne des polynômes.

TH : étant donné deux polynômes $A, B \neq 0$, il existe un unique couple (Q, R) de polynômes vérifiant

$$A = BQ + R, \text{ avec } \deg R < \deg B$$

Q et R sont appelés respectivement le *quotient* et le *reste* de la division euclidienne de A par B.

D12 : utilisant, pour l'existence, le lemme : si $\deg A \geqslant \deg B$, il existe Q_1 et A_1 tels que $A = BQ_1 + A_1$ avec $\deg A_1 < \deg A$.

3) Polynômes premiers entre eux, PGCD, PPCM.
a) Polynômes premiers entre eux (ou étrangers).
Si A est un polynôme, on note $\mathcal{M}_A = \{AU \ / \ U \in K[X]\}$ l'ensemble des multiples de A.

LEMME FONDAMENTAL : si A et B sont deux polynômes non nuls, il existe un unique polynôme D unitaire tel que $\mathcal{M}_A + \mathcal{M}_B = \mathcal{M}_D$.

D13

On note $\mathcal{D}_A$ l'ensemble des diviseurs normalisés d'un polynôme A.

DEF : deux polynômes A et $B \in K[X]$ sont dits *premiers entre eux* ssi leur seul diviseur commun normalisé est 1 (i. e. $\mathcal{D}_A \cap \mathcal{D}_B = \{1\}$).

TH de Bézout : A et B sont premiers entre eux si et seulement s'il existe deux polynômes U et V tels que $AU + BV = 1$.
D14 (application du lemme).

COROLLAIRE : TH de Gauss : si A divise BC et A et B sont premiers entre eux, alors A divise C.
D15

b) PGCD.

TH : Soient A, B 2 polynômes non nuls, et D l'unique polynôme normalisé tel que $\mathcal{M}_A + \mathcal{M}_B = \mathcal{M}_D$ alors
1) D divise A et B et tout diviseur commun à A et B divise D
2) D est l'unique polynôme normalisé de degré maximum divisant A et B.
3) A/D et B/D sont premiers entre eux.

D16

DEF : ce polynôme D est appelé le PGCD de A et B.
Notation : $PGCD\,(A,B)$ ou $A \wedge B$.

PROP : A et B sont premiers entre eux ssi leur PGCD est 1.
D17

REM 1 : on peut poser $A \wedge 0 = 0 \wedge A = A$.

REM 2 : mutatis mutandis, l'algorithme d'Euclide fonctionne chez les polynômes exactement comme chez les entiers.

c) PPCM.

TH et définition : si A et B sont deux polynômes non nuls, il existe un unique polynôme M unitaire tel que $\mathcal{M}_A \cap \mathcal{M}_B = \mathcal{M}_M$. M est appelé le PPCM de A et B. Notation : $PPCM\,(A,B)$ ou $A \vee B$.

TH : a) pour A, B, M polynômes non nuls, M normalisé, on a $M = PPCM(A,B)$ ssi l'une des propriétés suivantes est réalisée :
1) M est multiple de A et B et tout multiple de A et B est multiple de M
2) M est un multiple de A et B ayant un degré minimal.
3) M divise AB et $D = (AB)/M$ est associé au $PGCD$ de A et B.

D18
Pour 3) utiliser : si D_1 divise A et B alors A et B divisent AB/D_1.
REM : on a donc $PPCM\,(A,B)\,.PGCD\,(A,B) = AB$ si A et B sont normalisés.

V) RACINES (OU ZÉROS) DES POLYNÔMES.

1) Définition et premiers exemples.
DEF : soit $P \in K[X]$ et $x_0 \in K$; on dit que x_0 est une racine (ou un zéro) de P si $P\,(x_0) = 0$.

PROP : x_0 est une racine de P ssi le polynôme $X - x_0$ divise P dans $K[X]$.
D19 (deux méthodes).

Exemples classés suivant le degré n de P :

▲ $n = 0$:

▲ $n = 1$: $aX + b$ a une unique racine : $-\dfrac{b}{a}$.

▲ $n = 2$:

$$\begin{aligned} P &= aX^2 + bX + c = a\,(\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots) = a\left((\ldots\ldots\ldots\ldots)^2 + \ldots\ldots\ldots\ldots\right) \\ &= \boxed{a\left(\left(X + \frac{b}{2a}\right)^2 - \frac{\Delta}{(2a)^2}\right) = \frac{1}{4a}\left((2aX+b)^2 - \Delta\right)} \\ \text{(forme canonique de } P, \text{ avec } \Delta &= b^2 - 4ac) \end{aligned}$$

PROP : P possède des racines ssi Δ est un carré dans K ; si c'est le cas, $\Delta = \delta^2$ et $P = a\,(X - x_1)\,(X - x_2)$ avec

$$x_1 = \frac{\ldots\ldots\ldots\ldots}{}, x_2 = \frac{\ldots\ldots\ldots\ldots\ldots}{}$$

▲ $n = 3$: donner un exemple avec $0, 1, 2$ ou 3 racines distinctes. E3

REM : on démontre en analyse à partir du théorème des valeurs intermédiaires que tout polynôme à coefficients réels de degré impair possède au moins une racine réelle ; par contre, si $n = 2p$ est pair, il existe toujours un polynôme réel de degré n sans racine réelle : ....

2) Nombre de racines d'un polynôme.

PROP : un polynôme non nul a toujours un nombre fini de racines distinctes, inférieur ou égal à son degré.
D20

CORO 1 (contraposée de la prop. précédente) : un polynôme ayant une infinité de racines est nul :

$$\exists A \text{ infini } \subset K \ / \ \forall x \in A \ \ P(x) = 0 \Rightarrow \boxed{P = 0} \ (\Rightarrow P(x) = 0 \ \forall x \in K)$$

Un polynôme qui s'annule en une infinité de points s'annule donc partout.

Application : la fonction cos n'est donc pas polynomiale.

CORO 2 : si $a_0, a_1, ..., a_n \in K$ et si $\forall x \in A$ infini $\subset K \quad a_0 + a_1 x + ... + a_n x^n = 0$ alors

$$a_0 = a_1 = ... = a_n = 0$$

D21

E4

CORO 3 : deux polynômes égaux en une infinité de points sont égaux (donc égaux en tout point de K) :

$$\exists A \text{ infini } \subset K \ / \ \forall x \in A \ \ P(x) = Q(x) \Rightarrow \boxed{P = Q} \ (\Rightarrow P(x) = Q(x) \ \ \forall x \in K)$$

D22

Application : si $P, Q \in \mathbb{R}[X]$ et $\forall \theta \in \mathbb{R} \ \ P(\cos\theta) = Q(\cos\theta)$, alors $P = Q$ (et donc $P(x) = Q(x) \quad \forall x \in \mathbb{R}$ et même $P(z) = Q(z) \ \ \forall z \in \mathbb{C}$).
A1

REM : ce corollaire est parfois appelé le *théorème de prolongation des identités algébriques* : si une identité algébrique (autrement dit, polynomiale) est vérifiée sur un ensemble infini, elle est vérifiée partout.

CORO 4 : l'application Φ définie dans III) 2) qui relie les fonctions polynômes et les polynômes formels est bijective dès que la partie I est infinie ; $\mathcal{P}(I, K)$ et $K[X]$ sont donc dans ce cas des anneaux isomorphes.
D23

REM : par contre, si $I = \{x_1, x_2, ..., x_n\}$ est finie, l'application Φ n'est pas injective (car 0 et $(X - x_1)...(X - x_n)$ ont la même image), et en fait, toute application de I dans K est polynomiale ! : $\mathcal{P}(I, K) = \mathcal{A}(I, K)$.

3) Ordre de multiplicité d'une racine.

DEF : on donne $P \in K[X], x_0 \in K, k \in \mathbb{N}$; on dit que x_0 est une racine *d'ordre de multiplicité* k de P si

$$(X - x_0)^k \text{ divise } P \text{ mais } (X - x_0)^{k+1} \text{ ne divise pas } P$$

Rem :
- "ordre de multiplicité" est raccourci en "ordre", ou "multiplicité" tout court, suivant les goûts.

- une racine d'ordre 0 n'est pas une racine... (bizarre, mais pratique).

- une racine d'ordre 1 est dite *simple*, d'ordre 2 : *double*, d'ordre 3 : *triple* etc...., d'ordre k : $k-$*uple*.

- une racine d'ordre $\geqslant 2$ est dit *multiple* (ou *au moins double*).

CNS : x_0 est une racine *d'ordre* k de P ssi $\exists Q \in K[X]$ / $P = (X - x_0)^k Q$, avec $Q(x_0) \neq 0$.

D24
PROP : tout polynôme P non nul s'écrit de façon unique sous la forme

$$P = (X - x_1)^{\alpha_1} (X - x_2)^{\alpha_2} ... (X - x_p)^{\alpha_p} Q \text{ avec } Q \in K[X] \text{ sans racine dans } K$$

D25, E5.

REM : p est le nombre de racines distinctes de P, et $q = \alpha_1 + \alpha_2 + ... + \alpha_p$, somme des ordres des racines de P est parfois appelé "*nombre de racines de P, en comptant les ordres de multiplicité*".

PROP : si n est le degré de P, $p \leqslant q \leqslant n$.
D26, E6

4) Polynôme scindé.

DEF : un polynôme *scindé* est un polynôme qui est produit de polynômes du premier degré.

CNS : avec les notations du paragraphe précédent, P est scindé $\Leftrightarrow Q$ est constant, $\Leftrightarrow q = n$ (somme des ordres = degré).

REM : si $P \in \mathbb{R}[X]$, il faut toujours préciser si P est scindé en tant que polynôme à coefficients réels (on dit : scindé sur $\mathbb{R}$), ou en tant que polynôme à coefficients complexes (on dit : scindé sur $\mathbb{C}$).

E7

VI) DÉRIVATION DES POLYNÔMES ; FORMULE DE TAYLOR.

1) Définition.
DEF : le polynôme dérivé du polynôme $P = \sum\limits_{k \geqslant 0} a_k X^k$ est le polynôme, noté $P' = \sum\limits_{k \geqslant 1} k a_k X^{k-1} = \sum\limits_{k \geqslant 0} (k+1) a_{k+1} X^k$.

Les polynômes dérivés successifs se notent de la même façon que pour les fonctions.
On notera D l'application : $\left\{ \begin{array}{c} K[X] \to K[X] \\ P \mapsto P' \end{array} \right.$
Propriétés :
P1 : $P \in K \Leftrightarrow P' = 0$

P2 : si $\deg(P) \geqslant 1$, $\deg P' = \deg P - 1$, et mieux, si $n \geqslant 1$, $P \in K_n[X] \Leftrightarrow P' \in K_{n-1}[X]$

P3 : $(P+Q)' = P' + Q'$; $(\lambda P)' = \lambda P'$; $(PQ)' = P'Q + PQ'$

P4 : $(P \circ Q)' = (P' \circ Q) Q'$
D27

2) Formule de Taylor.

PROP : (formule de Taylor pour les polynômes)

Si $\deg P = n$,

$$P = P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(x_0)}{k!} (X - x_0)^k = P(x_0) + P'(x_0)(X - x_0) + P''(x_0) \frac{(X - x_0)^2}{2} + .. + P^{(n)}(x_0) \frac{(X - x_0)^n}{n!}$$

ou, ce qui revient au même

$$P(x_0 + X) = \sum_{k=0}^{n} \frac{P^{(k)}(x_0)}{k!} X^k = P(x_0) + P'(x_0) X + P''(x_0) \frac{X^2}{2} + .. + P^{(n)}(x_0) \frac{X^n}{n!}$$

D28

COROLLAIRE :
un polynôme de degré n est entièrement déterminé par la connaissance de $P(x_0), P'(x_0), P''(x_0), ..., P^{(n)}(x_0)$

E8 : écrire la formule de Taylor pour $(1+X)^n$ et $x_0 = 0$.

3) Caractérisation de l'ordre de multiplicité à partir des polynômes dérivés.

On donne $P \in K[X], x_0 \in K, k \in \mathbb{N}^*$.

PROP : si x_0 est racine d'ordre k de P, alors x_0 est racine d'ordre $k-1$ de P'.
D 28 bis

REM 1 : pour $k = 1$, ceci donne : si x_0 est racine simple de P, alors x_0 n'est pas racine de P'.
REM 2 : la réciproque est fausse !
REM 3 : on en déduit évidemment : si x_0 est racine d'ordre k de P, alors

x_0 est racine d'ordre $k-1$ de P'
x_0 est racine d'ordre $k-2$ de P''
...
x_0 est racine simple de $P^{\cdots\cdots\cdots}$
x_0 n'est pas racine de $P^{\cdots\cdots\cdots}$

On en déduit la caractérisation :
TH : x_0 est une racine d'ordre k de P ssi

$$P(x_0) = P'(x_0) = ... = P^{\cdots\cdots}(x_0) = 0 \text{ et } P^{\cdots\cdots}(x_0) \neq 0$$

D29

CORO : x_0 est une racine multiple de P ssi $P(x_0) = P'(x_0) = 0$.

VII) POLYNÔMES IRRÉDUCTIBLES. RÉDUCTION.

DEF : un polynôme $P \in K[X]$ est dit *réductible* ou *factorisable* (sur K) s'il est divisible par un polynôme non constant $\in K[X]$ de degré strictement inférieur à son degré. Il est dit *irréductible* s'il est non constant et non réductible.

REM : les polynômes constants ne sont donc ni réductibles, ni irréductibles !

CNS :
1) P est réductible ssi P est produit de deux polynômes non constants.
2) P est irréductible ssi P est non constant et P n'est divisible que par λ et λP avec $\lambda \in K^*$.
3) P est irréductible ss'il a exactement deux diviseurs unitaires (1 et $\dfrac{P}{\text{coef dominant de } P}$).
D30

REM 1 : les polynômes irréductibles (resp. réductibles) sont donc aux polynômes ce que sont les nombres premiers (resp. composés) aux naturels.

REM 2 : un polynôme de $\mathbb{R}[X]$ peut être irréductible sur $\mathbb{R}$ et réductible sur $\mathbb{C}$; exemple : X^2+1.

REM 3 : les seuls polynômes scindés irréductibles sont ceux du premier degré.

REM 4 : Il faut combattre la croyance fortement ancrée consistant à penser qu'un polynôme irréductible est un polynôme sans racine ; en effet :
1) les polynômes du premier degré sont irréductibles, et pourtant ils ont une racine.
2) le polynôme $(X^2+1)(X^2+2) \in \mathbb{R}[X]$ est sans racine (réelle) et il est pourtant réductible.

Par contre :
PROP :
1) un polynôme irréductible sur K de degré $\geqslant 2$ n'a pas de racine dans K.
2) un polynôme de degré 2 ou 3 est irréductible ss'il n'a pas de racine.
D31

Exemple : un polynôme à coefficients réels de degré impair $\geqslant 3$ est toujours réductible sur $\mathbb{R}$.

E9

TH de décomposition :

Tout polynôme non constant se décompose de manière unique en produit de facteurs irréductibles.
3) Théorème de D'ALEMBERT-GAUSS.

THÉORÈME FONDAMENTAL DE L'ALGÈBRE, ou THÉORÈME de D'ALEMBERT-GAUSS (admis) :
Tout polynôme à coefficients complexes non constant possède au moins une racine complexe.

CORO 1 : tout polynôme à coefficients réels non constant possède au moins une racine complexe.

CORO 2 : Tout polynôme non nul de degré n à coefficients complexe est scindé sur $\mathbb{C}$: la somme des ordre de ses racines est égal à n (ou, selon l'expression consacrée : il possède n racines complexes en comptant les ordres de multiplicité).
D32

CORO 3 : Les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
D33

4) Application à la réduction des polynômes à coefficients réels.

a) Conjugué d'un polynôme à coefficients complexes.

DEF : le conjugué d'un polynôme à coefficients complexe est le polynôme obtenu en conjuguant les coefficients :

$$\text{si } P=\sum_{k=0}^{n} a_k X^k, \text{ le conjugué de } P \text{ est } \overline{P}=\sum_{k=0}^{n}\overline{a_k}X^k$$

Propriétés pour $P,Q\in\mathbb{C}[X]$:
P1 : $\forall z\in\mathbb{C}\ \overline{P(z)}=\overline{P}(\overline{z})$

P2 : $\overline{P+Q}=\overline{P}+\overline{Q}$, $\overline{P.Q}=\overline{P}.\overline{Q}$

P3 : $P\in\mathbb{R}[X]\Leftrightarrow P=\overline{P}$.

P4 : si $P\in\mathbb{C}[X]$, $P+\overline{P}, P\overline{P}\in\mathbb{R}[X]$.

P5 : $z_0\in\mathbb{C}$ est racine de P d'ordre $\alpha\Leftrightarrow\overline{z_0}$ est racine de $\overline{P}$ d'ordre α.
D34

COROLLAIRE : si z_0 est racine complexe non réelle d'ordre α d'un polynôme réel P , alors $\overline{z_0}$ est aussi racine de P d'ordre α et P est donc divisible par le polynôme à coefficients réels :

$$(X-z_0)^{\alpha}(X-\overline{z_0})^{\alpha}=\left(X^2-2\operatorname{Re}(z_0)X+|z_0|^2\right)^{\alpha}$$

Ex : trouver les polynomes réels de degré 4 ayant $3-i$ pour racine double.
b) Réduction des polynômes à coefficient réels

COROLLAIRE du Théorème de D'Alembert pour les polynômes à coefficients réels :

Tout polynôme de degré n, de coefficient dominant a_n à coefficients réels possède sur $\mathbb{C}$ une décomposition unique sous la forme

$$P = a_n (X - x_1)^{\alpha_1} ... (X - x_p)^{\alpha_p} (X - z_1)^{\beta_1} (X - \overline{z_1})^{\beta_1} ... (X - z_r)^{\beta_r} (X - \overline{z_r})^{\beta_r}$$

Les x_i sont les p racines réelles de P, d'ordres respectifs α_i.
Les z_i et $\overline{z_i}$ sont les $2r$ racines non réelles de P, d'ordres respectifs β_i.
Et on a :

$$n = \sum_{i=1}^{p} \alpha_i + 2 \sum_{i=1}^{r} \beta_i$$

D35

Sur $\mathbb{R}$ on obtient donc la décomposition

$$P = a_n (X - x_1)^{\alpha_1} ... (X - x_p)^{\alpha_p} \left(X^2 - 2\operatorname{Re}(z_1) X + |z_1|^2\right)^{\beta_1} ... \left(X^2 - 2\operatorname{Re}(z_r) X + |z_r|^2\right)^{\beta_r}$$

qui peut s'écrire, avec l'écriture exponentielle des z_i : $z_i = \rho_i e^{i\theta_i}$

$$P = a_n (X - x_1)^{\alpha_1} ... (X - x_p)^{\alpha_p} \left(X^2 - 2\rho_1 \cos\theta_1 X + \rho_1^2\right)^{\beta_1} ... \left(X^2 - 2\rho_r \cos\theta_r X + \rho_r^2\right)^{\beta_r}$$

COROLLAIRE 1 : les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes du premier degré et les polynômes du second degré de discriminant négatif.
D36

COROLLAIRE 2 : la décomposition en produit de facteurs irréductibles d'un polynôme non constant de $\mathbb{R}[X]$ est formée de polynômes du premier degré et de polynômes du second degré de discriminant négatif.

E10

VIII) RELATIONS ENTRE LES RACINES ET LES COEFFICIENTS D'UN POLYNÔME SCINDÉ.

1) Cas du degré 2

PROP : si $P = aX^2 + bX + c = a(X - x_1)(X - x_2)$ est un polynôme scindé de degré 2, alors

$s = x_1 + x_2 =$ ....
$p = x_1 x_2 =$ ....

2) Cas du degré 3

PROP : $P = aX^3 + bX^2 + cX + d = a(X - x_1)(X - x_2)(X - x_3)$ est un polynôme scindé de degré 3, alors

$s = \sigma_1 = x_1 + x_2 + x_3 =$ ....
$\sigma_2 = x_1x_2 + x_2x_3 + x_3x_1 =$ ....
$p = \sigma_3 = x_1x_2x_3 =$ ....

3) Cas général

LEMME : si $x_1, x_2, ..., x_n$ sont n éléments de K, le développement du produit $(X - x_1)(X - x_2)...(X - x_n)$ s'écrit :

$$X^n + \sum_{k=1}^{n} (-1)^k \sigma_k X^{n-k}$$

où σ_k est la somme de tous les produits k à k des scalaires $x_1, x_2, ..., x_n$:

$$\sigma_k = \sum_{1 \leqslant i_1 < i_2 < ... < i_k \leqslant n}^{n} x_{i_1} ... x_{i_k} = \sum_{\begin{cases} J \subset [|1, n|] \\ |J| = k \end{cases}} \prod_{j \in J} x_j$$

D37
DEF : le nombre σ_k s'appelle la k-ième *expression symétrique élémentaire* des nombres $x_1, x_2, ..., x_n$.
REM 1 : σ_1 est la somme des x_i et σ_n est leur produit.
REM 2 : le nombre de produits $x_{i_1}...x_{i_k}$ dans l'écriture de σ_k vaut $\begin{pmatrix} n \\ k \end{pmatrix}$.
PROP : si $P = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0 = a_n (X - x_1)(X - x_2)...(X - x_n)$ est un polynôme scindé de degré n, alors les racines de P et ses coefficients sont liés par les relations :

$s = \sigma_1 = x_1 + ... + x_n = ...$
...
$\sigma_k = \sum\limits_{1 \leqslant i_1 < i_2 < ... < i_k \leqslant n}^{n} x_{i_1}...x_{i_k} = ...$
...
$p = \sigma_n = x_1...x_n = ...$

D38

E11 : cas $n = 4$

4) Applications.

a) Calculs d'expressions symétriques des racines, sans avoir besoin de connaître ces racines.

On constatera que si $f(x_1, ..., x_n)$ est une expression symétrique des $x_1, ..., x_n$ (c'est-à dire que si on permute un x_i et un x_j le résultat ne change pas), alors on peut mettre $f(x_1, ..., x_n)$ sous la forme $g(\sigma_1, ..., \sigma_n)$.
Comme les σ_k s'expriment à partir des coefficients du polynôme par les relations ci-dessus, on peut donc calculer $f(x_1, ..., x_n)$ sans avoir besoin de connaître les valeurs des scalaires $x_1, ..., x_n$.
E12

b) Résolutions de systèmes symétriques en les inconnues $x_1, ..., x_n$ par la détermination des racines d'un polynôme.
E13

BLAGUE : M. et Mme Heaumes ont une fille....