ENSEMBLES ET APPLICATIONS

Proposition 1
Soient E, F et G trois ensembles. Soit $f : E \to F$ et $g : F \to G$.
(i) Si $g \circ f$ est injective alors f est injective.
(ii) Si $g \circ f$ est surjective alors g est surjective.
(iii) Si f et g sont injectives, alors $g \circ f$ est injective.
(iv) Si f et g sont surjectives, alors $g \circ f$ est surjective.

Proposition 2
Soient E, F et G trois ensembles. Soit $f : E \to F$ et $g : F \to G$.
(i) Si f est bijective, alors f^{-1} est bijective.
(ii) Si f et g sont bijectives alors $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proposition 3
Soit E un ensemble. Soit $\mathcal{R}$ une relation sur E. On suppose que $\mathcal{R}$ est une relation d'équivalence. Les classes d'équivalences modulo $\mathcal{R}$ forment une partition de E.

ARITHMETIQUE

Théorème 1 Division euclidienne
Soient a un entier relatif et b un entier naturel non nul. Il existe un unique couple d'entiers relatifs (q, r) tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

On dit que q (resp r) est le quotient (resp le reste) de la division euclidienne de a par b.

Proposition 4
Soient a et b deux entiers non tous les deux nuls. On note d leur PGCD. Alors

$$\mathcal{D}(d) = \mathcal{D}(a) \cap \mathcal{D}(b).$$

Proposition 5
Soient a et b deux entiers, avec $b \in \mathbb{N}^*$. On note (q, r) le couple quotient reste de la division euclidienne de a par b.

$$\text{PGCD}(a, b) = \text{PGCD}(b, r).$$

Proposition 6
Soient a et b deux entiers. Soit $k \in \mathbb{N}^*$. $\text{PGCD}(ka, kb) = k\text{PGCD}(a, b)$.

Théorème 2 (**Relation de Bézout**)
Soient a et b deux entiers relatifs non tous les deux nuls. On note d leur PGCD.
Il existe deux entiers relatifs u et v tels que

$$au + bv = d.$$

Théorème 3 (**Identité de Bézout**)
Soient a et b deux entiers relatifs. Il y a équivalence entre les énoncés :
(i) a et b sont premiers entre eux.
(ii) Il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Théorème 4 (**Lemme de Gauss**)
Soient a, b, c trois entiers relatifs. Si a divise bc et si a est premier avec b, alors a divise c.

Proposition 7
Soient a et b deux entiers relatifs. Soit $n \in \mathbb{Z}$.
Si a et b sont premiers entre eux et divisent n, alors ab divise n.

Proposition 8
Soient a et b deux entiers relatifs. Soit $n \in \mathbb{Z}$.
Si a et b sont premiers à n, alors ab est premier à n.

Proposition 9
Soient a et b deux entiers non nuls. On note d leur PGCD et m leur PPCM. Alors $|ab| = dm$.

Théorème 5
L'ensemble des nombres premiers est infini.

Théorème 6
Tout entier naturel supérieur ou égal à 2 se décompose de manière unique (à l'ordre près) en un produit de facteurs premiers.

Proposition 10
Soient n et m dans $\mathbb{N}^*$. Soit p un nombre premier. $v_p(nm) = v_p(n) + v_p(m)$.

Théorème 7 (**Petit théorème de Fermat**)
Soit p un nombre premier. Soit $n \in \mathbb{Z}$. Alors $n^p \equiv n\ [p]$.

STRUCTURES ALGEBRIQUES USUELLES

Proposition 11
Soit $((G_i, \star_i))_{1 \leq i \leq n}$ une famille finie de groupes. On définit $\star$ sur $G_1 \times \cdots \times G_n$ par :

$$\begin{array}{rcl} (G_1 \times \cdots \times G_n) \times (G_1 \times \cdots \times G_n) & \to & G_1 \times \cdots \times G_n \\ ((x_1, \ldots, x_n), (y_1, \ldots, y_n)) & \mapsto & (x_1 \star_1 y_1, \ldots, x_n \star_n y_n) \end{array}.$$

$\star$ est une loi de composition interne et $(G_1 \times \cdots \times G_n, \star)$ est un groupe.

Proposition 12
Soit $(G, \star)$ un groupe. Soit $H \subset G$. H est un sous-groupe de G si et seulement si

$$H \neq \emptyset \qquad \text{et} \qquad \forall (x, y) \in H^2,\ x \star y^{-1} \in H.$$

Proposition 13
Soit $(G, \star)$ un groupe. Soit $H \subset G$. H est un sous-groupe de G si et seulement si
H est stable par $\star$ et H est un groupe pour la loi induite par $\star$.

Proposition 14
Soient $(G, \star)$ et (G', T) deux groupes d'éléments neutres respectifs e et e'. Soit f un morphisme de groupes de $(G, \star)$ vers (G', T).
(i) $f(e) = e'$.
(ii) $\forall x \in G$, $(f(x))^{-1} = f(x^{-1})$.
(iii) $\forall x \in G$, $\forall n \in \mathbb{Z}$, $(f(x))^n = f(x^n)$.

Proposition 15
Soient $(G, \star)$ et (G', T) deux groupes. Soit f un morphisme de groupes de $(G, \star)$ vers (G', T).
(i) Si H est un sous-groupe de G, $f(H)$ est un sous-groupe de G'.
(ii) Si H' est un sous-groupe de G', $f^{-1}(H')$ est un sous-groupe de G.

Proposition 16
Soient $(G, \star)$ et (G', T) deux groupes. Soit f un morphisme de groupes de $(G, \star)$ vers (G', T).
$\mathrm{Ker}(f)$ est un sous-groupe de G et $\mathrm{Im}(f)$ est un sous-groupe de G'.

Proposition 17
Soient $(G, \star)$ et (G', T) deux groupes. Soit f un morphisme de groupes de $(G, \star)$ vers (G', T).

$$f \text{ est injectif} \quad \Longleftrightarrow \quad \mathrm{Ker}(f) = \{e\}.$$

Proposition 18
Soient $(G, \star)$ et (G', T) deux groupes. Soit f un isomorphisme de groupes de $(G, \star)$ vers (G', T).
Alors f^{-1} est un isomorphisme de groupes de (G', T) vers $(G, \star)$.

Proposition 19
Soit $(A, +, \times)$ un anneau, non réduit à $\{0\}$. L'ensemble des unités de A muni de $\times$ est un groupe, appelé groupe des inversibles de A ou groupe des unités de A.

Proposition 20
Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux et $f : A \to B$ un morphisme d'anneaux.
(i) L'image par f d'un sous-anneau de A est un sous-anneau de B.
(ii) L'image réciproque par f d'un sous-anneau de B est un sous-anneau de A.

Proposition 21
Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux et $f : A \to B$ un morphisme d'anneaux.
(i) $\mathrm{Im}(f)$ est un sous-anneau de B.
(ii) $\mathrm{Ker}(f)$ n'est pas en général un sous-anneau de A.
(iii) f est injectif $\iff \mathrm{Ker}(f) = \{0\}$.

Proposition 22
Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux et $f : A \to B$ un isomorphisme d'anneaux.
Alors f^{-1} est un isomorphisme d'anneaux de $(B, +_B, \times_B)$ vers $(A, +_A, \times_A)$.

Proposition 23
Soit $(A, +, \times)$ un anneau intègre. Alors pour $a \in A$, $a \neq 0$,

$$\forall (x, y) \in A^2, \quad ax = ay \quad \Longrightarrow \quad x = y.$$

Proposition 24
Soit $(K, +, \times)$ un corps. Alors $(K, +, \times)$ est un anneau intègre.

POLYNOMES

Proposition 25 (**Opérations sur les degrés**)
Soient P et Q deux polynômes de $\mathbb{K}[X]$.
(i) $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$.
Si $\deg(P) \neq \deg(Q)$, alors $\deg(P+Q) = \max(\deg(P), \deg(Q))$.
(ii) $\deg(PQ) = \deg(P) + \deg(Q)$.
(iii) $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Proposition 26
L'anneau $(\mathbb{K}[X], +, \times)$ est intègre.

Proposition 27
Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes de degré 0, i.e. les polynômes constants non nuls.

Théorème 8 (**Division euclidienne**)
Soient A et B deux polynômes à coefficients dans $\mathbb{K}$, avec $B \neq 0$.
Il existe un unique couple (Q, R) de polynômes à coefficients dans $\mathbb{K}$ tel que

$$A = BQ + R \qquad \text{et} \qquad \deg(R) < \deg(B).$$

Proposition 28 (**Relations coefficients-racines, formules de Viète**)
Soit $P \in \mathbb{K}[X]$, qui s'écrit $P = \sum_{k=0}^{n} a_k X^k$, avec $n \in \mathbb{N}^*$ et $a_n \neq 0$. On suppose P scindé et on note $(x_i)_{1 \leq i \leq n} \in \mathbb{K}^n$ ses racines. On a :

$$\forall p \in [\![1, n]\!] \quad \sum_{i_1 < \cdots < i_p} x_{i_1} \cdots x_{i_p} = (-1)^p \frac{a_{n-p}}{a_n}.$$

En particulier

$$\sum_{i=1}^{n} x_i = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad \prod_{i=1}^{n} x_i = (-1)^n \frac{a_0}{a_n}.$$

Pour $n = 2$, si $P = aX^2 + bX + c$ est scindé de racines x_1 et x_2, on a

$$x_1 + x_2 = -\frac{b}{a} \qquad \text{et} \qquad x_1 x_2 = \frac{c}{a}.$$

Proposition 29 (**Méthode de Horner**)
Soit $P = \sum_{k=0}^{n} a_k X^k$, avec $n \in \mathbb{N}^*$. Soit $a \in \mathbb{K}$.
On définit $b_n = a_n$ puis pour $k = n-1 \ldots 0$, $b_k = a_k + b_{k+1} a$. Alors $b_0 = P(a)$.

Proposition 30 (**Degré et dérivation**)
Soient $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.
(i) $\deg(P') = \begin{cases} -\infty & \text{si } \deg(P) \leq 0 \\ \deg(P) - 1 & \text{si } \deg(P) \geq 1. \end{cases}$
(ii) On a l'équivalence : $\deg(P) \leq n \iff P^{(n+1)} = 0$.

Proposition 31 (**Formule de Leibniz**)
Soient P et Q deux polynômes de $\mathbb{K}[X]$ et $n \in \mathbb{N}$. On a :

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Théorème 9 (**Formule de Taylor**)
Soient $P \in \mathbb{K}[X] \setminus \{0\}$, $n = \deg(P)$ et $a \in \mathbb{K}$. On a les égalités :

$$P(a+X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} X^k \qquad \text{et} \qquad P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k.$$

Proposition 32
Un polynôme non nul de degré $n \in \mathbb{N}$, possède au plus n racines deux à deux distinctes.

Proposition 33 (**Caractérisation des racines multiples**)
Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}^*$. a est zéro de P de multiplicité exactement m si et seulement si :

$$\forall k \in [\![0, m-1]\!], \quad P^{(k)}(a) = 0 \quad \text{et} \quad P^{(m)}(a) \neq 0.$$

Théorème 10 (**de d'Alembert-Gauss**)
Soit $P \in \mathbb{C}[X]$, de degré supérieur ou égal à 1. Alors P admet au moins une racine dans $\mathbb{C}$.

Proposition 34
Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Proposition 35
Tout polynôme non nul de $\mathbb{C}[X]$ est scindé dans $\mathbb{C}[X]$.

Théorème 11
Les polynômes irréductibles de $\mathbb{R}[X]$ sont :
(i) les polynômes de degré 1,
(ii) les polynômes de degré 2, de discriminant strictement négatif.

Proposition 36
Tout polynôme de $\mathbb{R}[X]$ se décompose de manière unique à l'ordre près en le produit de polynômes unitaires irréductibles et de son coefficient dominant.

Proposition 37
Deux racines complexes conjuguées d'un polynôme de $\mathbb{R}[X]$ ont la même multiplicité.

Théorème 12 (**Interpolation de Lagrange**)
Soit $n \in \mathbb{N}^*$. Soient $(x_1, \ldots, x_n)$ une famille d'éléments deux à deux distincts de $\mathbb{K}$ et $(y_1, \ldots, y_n)$ une famille d'éléments de $\mathbb{K}$.
Il existe un unique polynôme $P \in \mathbb{K}_{n-1}[X]$ tel que pour tout $i \in [\![1, n]\!]$, $P(x_i) = y_i$.

ARITHMETIQUE DES POLYNOMES

Proposition 38
Soient A et B deux polynômes non tous les deux nuls. On note D un PGCD de A et de B. Alors

$$\mathcal{D}(D) = \mathcal{D}(A) \cap \mathcal{D}(B).$$

Proposition 39
Soient A et B deux entiers, avec $B \in \mathbb{N}^*$. On note (Q, R) le couple quotient reste de la division euclidienne de A par B.

$$\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(B) \cap \mathcal{D}(R).$$

Théorème 13 (**Relation de Bézout**)
Soient A et B deux polynômes non tous les deux nuls. On note D leur PGCD.
Il existe deux polynômes U et V tels que

$$AU + BV = D.$$

Théorème 14 (**Identité de Bézout**)
Soient A et B deux polynômes. Il y a équivalence entre les énoncés :
(i) A et B sont premiers entre eux.
(ii) Il existe deux polynômes U et V tels que $AU + BV = 1$.

Théorème 15 (**Lemme de Gauss**)
Soient A, B, C trois polynômes. Si A divise BC et si A est premier avec B, alors A divise C.

Proposition 40
Soient A et B deux polynômes. Soit $P \in \mathbb{K}[X]$.
Si A et B sont premiers entre eux et divisent P, alors AB divise P.

Proposition 41
Soient A et B deux polynômes. Soit $P \in \mathbb{K}[X]$.
Si A et B sont premiers avec P, alors AB est premier avec P.

Proposition 42
Deux polynômes de $\mathbb{C}[X]$ sont premiers entre eux si et seulement s'ils n'ont pas de racine commune.

Proposition 43
Soient A et B deux polynômes non nuls. On note D leur PGCD et M leur PPCM. Alors AB et DM sont associés.

FRACTIONS RATIONNELLES

Proposition 44 (**Opérations sur les degrés**)
Soient F et G deux fractions rationnelles dans $\mathbb{K}(X)$.
(i) $\deg(F+G) \leq \max(\deg(F), \deg(G))$.
(ii) $\deg(FG) = \deg(F) + \deg(G)$.

Proposition 45 (**Partie entière**)
Toute fraction rationnelle F de $\mathbb{K}(X)$ s'écrit, de façon unique, comme la somme d'un polynôme, appelé partie entière de F, et d'une fraction rationnelle de degré strictement négatif.

Théorème 16 (**Décomposition en éléments simples dans** $\mathbb{C}(X)$)
Soit $F \in \mathbb{C}(X)$ dont les pôles sont les complexes $a_1, \ldots, a_n$ distincts deux à deux et d'ordres de multiplicité respectifs $m_1, \ldots, m_n$. On note E la partie entière de F. Il existe une unique famille de complexes $(\lambda_{k,u})_{\substack{1\leq k\leq n \\ 1\leq u\leq r_k}}$ tels que :

$$F = E + \sum_{k=1}^{n} \left(\sum_{u=1}^{m_k} \frac{\lambda_{k,u}}{(X-a_k)^u} \right).$$

Théorème 17 (**Décomposition en éléments simples dans** $\mathbb{R}(X)$)
Soit $F \in \mathbb{R}(X)$ une fraction rationnelle admettant pour forme irréductible unitaire $F = \frac{A}{B}$. Il existe $(n, m) \in \mathbb{N}^2$ tel que la décomposition en produits de facteurs irréductibles de B soit de la forme :

$$B = \prod_{k=1}^{n} (X-a_k)^{m_k} \prod_{l=1}^{m} (X^2 + b_l X + c_l)^{n_l}$$

où les $a_1, \ldots, a_n$ sont les racines réelles distinctes deux à deux de B, d'ordres de multiplicité respectifs $m_1, \ldots, m_n$ et $X^2+b_1X+c_1, \ldots, X^2+b_mX+c_m$ sont des polynômes deux à deux distincts sans racine réelle, $n_1, \ldots, n_m$ sont des entiers naturels non nuls.
On note E la partie entière de F. Il existe une unique famille de réels $(\lambda_{k,u})_{\substack{1\leq k\leq n \\ 1\leq u\leq r_k}}$ et une unique famille de couples de réels $(\mu_{l,v}, \nu_{l,v})_{\substack{1\leq l\leq m \\ 1\leq v\leq n_l}}$ tels que :

$$F = E + \sum_{k=1}^{n} \left(\sum_{u=1}^{m_k} \frac{\lambda_{k,u}}{(X-a_k)^u} \right) + \sum_{l=1}^{m} \left(\sum_{v=1}^{n_l} \frac{\mu_{l,v}X + \nu_{l,v}}{(X^2+b_lX+c_l)^v} \right).$$

Proposition 46
Soit $P \in \mathbb{K}[X]$, scindé, de racines $a_1, \ldots, a_n$ de multiplicités respectives $m_1, \ldots, m_n$. Alors la décomposition en éléments simples de $\frac{P'}{P}$ dans $\mathbb{K}(X)$ est

$$\frac{P'}{P} = \sum_{k=1}^{n} \frac{m_k}{X-a_k}.$$