MP* - Compléments sur les corps

Par convention, dans le cadre du programme, tous les corps sont commutatifs.

Nous verrons, en algèbre générale, certains corps finis, les $\mathbb{Z}/p\mathbb{Z}$, p étant un nombre premier.
Au programme, théoriquement, l'algèbre linéaire, les polynômes, sont uniquement sur K sous-corps de $\mathbb{C}$.
Ce cadre n'est pas respecté par Polytechnique et les ENS, et il est bon de savoir un peu ce qui marche toujours, et ce qui tombe en défaut (sections 2 et 3).
La section 4 donne une introduction aux extensions de corps, appliquée aux nombre algébriques.

1 Caractéristique d'un corps

Définition 1: Caractéristique d'un corps
Soit K un corps. Si $n \in \mathbb{Z}$, et $x \in K$, $n \cdot x$ désigne l'itéré n-ième additif de x, et x^n l'itéré n-ième multiplicatif.
Le produit de $x, y \in K$ sera simplement noté xy, et les neutres 0 et 1.
On dit que K est de caractéristique nulle si et seulement si $\forall n \in \mathbb{N}^*$, $n \cdot 1 \neq 0$ (itéré de 1).
Si K n'est pas de caractéristique nulle, on définit sa caractéristique par $car(K) = \min\{n \in \mathbb{N}^* \mid n \cdot 1 = 0\}$.

Propriété 1:

1. Tout corps fini est de caractéristique non nulle.
2. Si K est un corps de caractéristique non nulle non réduit à un élément, $car(K)$ est un nombre premier
3. Si $car(K) = n \in \mathbb{N}^*$, $\forall x \in K^*$, $\forall m \in \mathbb{N}$, $m \cdot x = 0 \iff n|m$.

Démonstration:

1. Soit K un corps fini de cardinal n.
   Alors $1, 2 \cdot 1, ..., (n+1) \cdot 1$ sont $n+1$ éléments de K, donc deux sont égaux. Il existe $p, q \in \mathbb{N}$, $p < q$, tels que $p \cdot 1 = q \cdot 1$, et alors $(q-p) \cdot 1 = 0$.
2. On suppose $car(K) = n \in \mathbb{N}^*$.
   Si $n = 1$, $0 = 1$ et K est réduit à un élément, cas sans intérêt...
   Sinon: $n \geq 2$. Supposons n non premier. On écrit alors $n = ab$ avec $a, b \geq 2$.
   Notons qu'on a $(a \cdot 1)(b \cdot 1) = \underbrace{(1 + ... + 1)}_{a\ termes}\underbrace{(1 + ... + 1)}_{b\ termes} = n \cdot 1 = 0$.
   Par intégrité de K, $a \cdot 1 = 0$ ou $b \cdot 1 = 0$ ce qui contredit la minimalité de n.
3. Si $n|m$: $m = an$. $(an) \cdot x = a \cdot ((n \cdot 1)x) = 0$.
   Si $m \cdot x = 0$: $0 = m \cdot x = (m \cdot 1)x$. Comme $x \neq 0$, par intégrité de K, $m \cdot 1 = 0$.
   On écrit $m = pn + r$ avec $r \in [\![0, n-1]\!]$ la division euclidienne de m par n.
   $0 = m \cdot 1 = (p \cdot \underbrace{(n \cdot 1)}_{=0}) + r \cdot 1 = r \cdot 1$. Par définition de $n = car(K)$, $r = 0$.

♣

Remarque: voir fin section 4 pour la cardinalité d'un corps fini.

2 $K[X]$

La construction des polynômes ne change pas, la notion de degré et ses propriétés non plus.
$K[X]$ est intègre.
Le théorème de division euclidienne reste inchangé (même démonstration), ainsi que ses conséquences sur la factorisation, et le fait qu'un polynôme de degré n a au plus n racines.
En revanche, il y a des problèmes avec le polynôme dérivé si la caractéristique est $\neq 0$.
Si $P = a_nX^n + ... + a_1X + a_0$, $P' = na_nX^n + ... + a_1$. na_n s'entend comme l'itéré n-ième de a.
$na_n = (n \cdot 1)a_n = 0$ si $car(K)|n$.
Ainsi, si $car(K) = n$, et $P = X^n - 1$, $P' = nX^{n-1} = 0$.
Dans la formule de Taylor, $\frac{1}{n!}$ s'entend $((n!) \cdot 1)^{-1}$, et $(n!) \cdot 1$ peut être nul.
Il faut donc oublier en caractéristique non nulle formule de Taylor, caractérisation de l'ordre des racines avec les dérivées, sauf à être très prudent.

3 Algèbre linéaire sur un corps quelconque

Les résultats du cours sont inchangés, dont les résultats sur diagonalisation/trigonalisation et polynôme minimal, polynôme caractéristique, polynômes annulateurs.
Le théorème de Cayley-Hamilton subsiste.
Mais on ne peut pas nécessairement trigonaliser, $P \in K[X]$ n'étant pas nécessairement scindé.
On peut faire certaines choses en utilisant des dénombrements sur les corps finis.
Un exemple:

Propriété 2:
Soit K un corps de cardinal q. Alors card$(GL_n(K)) = (q^n - 1)(q^n - q)(q^n - q^2)...(q^n - q^{n-1})$

Démonstration:
Définir $A \in GL_n(K)$ revient à définir ses colonnes, ie une famille libre $(C_1, ..., C_n)$ dans K^n.
On commence par choisir $C_1 \neq 0$: $q^n - 1$ choix.
Ensuite, ayant choisi C_1, il faut choisir $C_2 \in \mathbb{K}^n \backslash vect(C_1)$. card$(K^n) = q^n$. $vect(C_1) = KC_1$ est de cardinal q, car $k \to kC_1$ est injective.
D'où $q^n - q$ choix pour C_2.
Ensuite, comme (C_1, C_2) est libre, $(k_1, k_2) \mapsto k_1C_1 + k_2C_2$ est injective, $vect(C_1, C_2)$ est de cardinal q^2, et il y a $q^n - q^2$ choix pour C_3.
Etc... D'où $(q^n - 1)(q^n - q)(q^n - q^2)...(q^n - q^{n-1})$ choix.
♣

4 Extension de corps

Nous nous limiterons ici aux prémisses, bien loin d'aller jusqu'à la théorie de Galois.
En fait, essentiellement le lemme de la base télescopique, et les conséquences sur les nombres algébriques.

La remarque fondamentale de départ est que si K_1 et K_2 sont deux corps avec $K_1 \subset K_2$, K_2 a une structure naturelle de K_1-ev, le produit extérieur $\lambda \cdot x$, avec $\lambda \in K_1$ et $x \in K_2$ étant simplement le produit λx dans K_2.
On note $[K_2 : K_1] \in \mathbb{N}^* \cup \{\infty\}$ la dimension de K_2 comme K_1-ev.

Propriété 3: Soient $K_1 \subset K_2 \subset K_3$ trois corps tels que $[K_3 : K_1] < \infty$.
Alors $[K_2 : K_1] \leq [K_3 : K_1]$.

Démonstration:
Soit $n = [K_3 : K_1] < \infty$. Si $[K_2 : K_1] > n$, on peut se donner $(e_1, ..., e_{n+1})$ famille d'éléments de K_2 qui est K_1-libre.
Alors a fortiori, c'est une famille de $n + 1$ éléments de K_3 qui est K_1-libre, ce qui contredit $n = [K_3 : K_1]$.

Propriété 4: Base télescopique
Soient trois corps K_1, K_2, K_3 tels que $[K_3 : K_2]$ et $[K_2 : K_1]$ soient finis.
Alors $[K_3 : K_1]$ est finie, et $[K_3 : K_1] = [K_3 : K_2][K_2 : K_1]$.

Démonstration Soient $(e_1, ..., e_d)$ une base de K_3 comme K_2-ev, et $(f_1, ..., f_n)$ une base de K_2 comme K_1-ev.
Montrons que $B = (e_i f_j)_{\substack{1 \leq i \leq d \\ 1 \leq j \leq n}}$ est une base de K_3 comme K_1-ev, ce qui donnera le résultat par cardinalité des bases. (B est appelée base télescopique)
Caractère générateur: Soit $x \in K_3$. x s'écrit $x = \sum_i y_i e_i$ avec $y_1, ..., y_d \in K_2$. Ensuite, pour tout i, y_i s'écrit $y_i = \sum_j k_{i,j} f_j$ avec $k_{i,j} \in K_1$.
Il en résulte $x = \sum_{i,j} k_{i,j} f_j e_i$.
Liberté: Si $\sum_{i,j} k_{i,j} f_i e_j = 0$ avec $\forall i, j,\ k_{i,j} \in K_1$: $\sum_j \underbrace{\left(\sum_i k_{i,j} f_i \right)}_{\in K_2} e_j = 0$.
Par K_2-liberté de $(e_1, ..., e_d)$, $\forall j,\ \sum_i \underbrace{k_{i,j}}_{\in K_1} f_i = 0$, puis par K_1-liberté de $(f_1, ..., f_n)$, $\forall j, i,\ k_{i,j} = 0$.

♣

Définition 2: Nombres algébriques
$x \in \mathbb{R}$ est dit algébrique si et seulement si il existe $Q \in \mathbb{Q}[X]$ non nul tel que $Q(x) = 0$.

Définition 3: polynôme minimal
Si $x \in \mathbb{R}$, $Ann(x) = \{Q \in \mathbb{Q}[X] \mid Q(x) = 0\}$ est facilement un idéal de $\mathbb{Q}[X]$.
Si x est algébrique, $Ann(x) \neq \{0\}$, donc il existe un unique $P \in \mathbb{Q}[X]$ unitaire tel que $Ann(x) = P\mathbb{Q}[X]$, et ce polynôme P est appelé polynôme minimal de x. Nous le noterons π_x.

Propriété 5: Avec les mêmes notations, si x est algébrique, π_x est un irréductible de $\mathbb{Q}[X]$.

Démonstration: Par l'absurde, sinon, il existe $A, B \in \mathbb{Q}[X]$ non constants tels que $\pi_x = AB$. Alors $A(x)B(x) = 0$, et par intégrité de $\mathbb{R}$, $A(x) = 0$ ou $B(x) = 0$, disons $A(x) = 0$. Alors π_x divise A, mais $1 \leq deg(A) < deg(\pi_x)$. C'est absurde.

Définition 4: Soit $x \in \mathbb{R}$, et K un sous-corps de $\mathbb{R}$. On note $K(x) = \bigcap_{\substack{K_2 \ sous-corps \ de \ \mathbb{R} \\ contenant \ \{x\} \cup K}} K_2$.
L'intersection de sous-corps étant un sous corps, $K(x)$ est un sous-corps de $\mathbb{R}$, et de par sa définition, le plus petit (au sens de l'inclusion) sous-corps de $\mathbb{R}$ contenant K et x.
Dit plus simplement, $K(x)$ est tout ce qui peut s'obtenir à partir de $K \cup \{x\}$ en utilisant un nombre quelconque de fois les opérations $+$, $\times$, passage à l'inverse et à l'opposé.
De ce fait, $K(x)$ est en fait facilement l'ensemble des évaluations en x des fractions rationnelles à coefficients dans K qui n'ont pas x comme pôle: $K(x) = \{F(x) \mid F \in K(X),\ x \text{ non pôle de } F\}$.

La propriété essentielle est la suivante:

Propriété 6:

$x \in \mathbb{R}$ est algébrique si et seulement si $[\mathbb{Q}(x) : \mathbb{Q}] < \infty$.
De plus, si x est algébrique, $n := [\mathbb{Q}(x) : \mathbb{Q}]$ est le degré de π_x, et $\mathbb{Q}(x) = \mathbb{Q}_{n-1}[x] = \{P(x) \mid P \in \mathbb{Q}_{n-1}[X]\}$.

Démonstration:
Supposons x algébrique. Notons $\pi_x = X^n + a_{n-1}X^{n-1} + ... + a_0$. $a_i \in \mathbb{Q}$.
En premier, voyons que $\mathbb{Q}(x) = \mathbb{Q}[x]$. Il n'y a qu'une inclusion non triviale.
$\mathbb{Q}[x]$ est facilement un anneau.
Soit $F \in \mathbb{Q}(X)$, $F = \dfrac{A}{B}$, $A, B \in \mathbb{Q}[X]$, avec $B(x) \neq 0$.
Si on montre que $\dfrac{1}{B(x)} \in \mathbb{Q}[x]$, on aura $F(x) = A(x) \times \dfrac{1}{B(x)} \in \mathbb{Q}[x]$.
π_x ne divise pas B, et est irréductible dans $\mathbb{Q}[X]$, donc, dans $\mathbb{Q}[X]$, $B \wedge \pi_x = 1$.
Donc (Bezout), il existe $U, V \in \mathbb{Q}[X]$ tels que $UB + V\pi_x = 1$. Alors $U(x)B(x) = 1$, et $\dfrac{1}{B(x)} = U(x) \in \mathbb{Q}[x]$.
Ainsi $\mathbb{Q}(x) = \mathbb{Q}[x]$.
Ensuite, par division euclidienne par π_x, on a $\mathbb{Q}[X] = \mathbb{Q}_{n-1}[x]$.
$\mathbb{Q}_{n-1}[x] = vect_{\mathbb{Q}}(1, x, ..., x^{n-1})$. $(1, ..., x^{n-1})$ est $\mathbb{Q}$-libre sans quoi on aurait un $P \in \mathbb{Q}[X]$ non nul de degré $< n$ annulant x, donc divisé par π_x, ce qui est impossible.
Donc $[\mathbb{Q}(x) : \mathbb{Q}] = n$.

Supposons maintenant $n := [\mathbb{Q}(x) : \mathbb{Q}] < \infty$.
Comme $1, x, ..., x^n$ sont $(n+1)$ éléments de $\mathbb{Q}(x)$, la famille est $\mathbb{Q}$-liée, ce qui donne un polynôme non nul $P \in \mathbb{Q}[X]$ tel que $P(x) = 0$, et x est algébrique.
♣.

La propriété précédente s'étend sans changement de démonstration à des corps quelconques, et on a notamment:

Propriété 7: Soit $K_1 \subset K_2$ deux corps, et $x \in K_2$. Il existe $P \in K_1[X]$ non nul tel que $P(x) \neq 0$ si et seulement si $[K_1(x) : K_1] < \infty$.

Propriété 8: L'ensemble A des réels algébriques est un sous-anneau de $\mathbb{R}$.

Démonstration: Remarque: on l'a déjà vu avec le résultant.
Soient $x, y \in A$. $-x \in A$ trivialement (on change des signes dans π_x).
$(\mathbb{Q}(x))(y)$ est un corps contenant x et y, donc xy et $x + y$.
On a les inclusions de corps $\mathbb{Q} \subset \mathbb{Q}(x) \subset (\mathbb{Q}(x))(y)$.
$[\mathbb{Q}(x) : \mathbb{Q}] < \infty$ car x est algébrique.
y est algébrique, d'où l'existence de $\pi_y \in \mathbb{Q}[X]$. A fortiori, $\pi_y \in \mathbb{Q}(x)[X]$, et annule y, donc par la propriété 7, $[(\mathbb{Q}(x))(y) : \mathbb{Q}(x)] < \infty$.
Alors, par la propriété 4, $[(\mathbb{Q}(x))(y) : \mathbb{Q}] < \infty]$.
$\mathbb{Q} \subset \mathbb{Q}(x+y) \subset (\mathbb{Q}(x))(y)$, et $[(\mathbb{Q}(x))(y) : \mathbb{Q}] < \infty]$, donc par la propriété 3, $[\mathbb{Q}(x+y) : \mathbb{Q}] < \infty$, et $x + y$ est algébrique.
Idem pour xy.
♣.

Une dernière chose, lié à des considérations d'algèbre linéaire:

Propriété 9:
Soit K un corps fini de cardinal ≥ 2.
Alors il existe p nombre premier et $n \in \mathbb{N}^*$ tels que $\mathrm{card}(K) = p^n$.

Remarque: réciproquement, pour tous p, n il existe un corps de cardinal p^n.

Démonstration:
Soit $p = car(K)$. On a vu que p est un nombre premier.
Notons $K_2 = \{0, 1, 2 \cdot 1, ..., (p-1) \cdot 1\}$.
K_2 est de cardinal p car s'il existait $1 \leq n < m \leq p-1$ tels que $n \cdot 1 = m \cdot 1$, on aurait $(m-n) \cdot 1 = 0$, avec $1 \leq m - n < p$, ce qui contredirait la définition de p.
K_2 est un sous-corps de K: stable par somme, produit, passage à l'opposé, en utilisant des divisions euclidiennes par p, comme dans la démonstration de la propriété 1.
Il reste à voir la stabilité par passage à l'inverse: soit $n \in [\![1, p-1]\!]$.
On a $n \wedge p = 1$ car p est premier. On écrit une relation de Bezout $1 = un + vp$.
Alors $1 = 1 \cdot 1 = (un + vq) \cdot 1 = (un) \cdot 1 + \underbrace{(vp) \cdot 1}_{=0} = (u \cdot 1)(n \cdot 1)$.

Donc l'inverse de $n \cdot 1$ est $u \cdot 1$, qui est dans K_2 comme dit précédemment, en faisant la division euclidienne de u par p.
$K_2 \subset K$, donc K est un K_2-ev, de dimension finie car fini. Notons $n = [K : K_2]$.
Soit $(e_1, ..., e_n)$ une base de K comme K_2-ev.
Par liberté et caractère générateur, $\begin{cases} K_2^n \to K \\ (k_1, ..., k_n) \mapsto k_1 e_1 + ... + k_n e_n \end{cases}$ est bijective, donc card$(K) = p^n$.
♣