COURS DU JEUDI 19 OCTOBRE 2017

3 Qu'est-ce qu'un corps

Définition 2 *Un corps est un anneau $(K, +, \cdot)$ avec unité, non nul, où tous les éléments $\neq 0$ sont inversibles pour la multiplication $\cdot$. Un corps non commutatif est aussi appelé un corps gauche.*

Exemple (non commutatif) : le corps gauche des quaternions :

$$\mathbb{H} := \left\{ \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} \ : \ a, b \in \mathbb{C} \right\} \ .$$

Exemples commutatifs : $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ (p premier), $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{C}(X, Y), \mathbb{C}(T)$, $\mathbb{C}((T)) = \{\sum_{n \geq n_0} a_n T \ : \ n_0 \in \mathbb{Z}, {}^{\forall} n \geq n_0, \ a_n \in \mathbb{C}\}$,
$\mathbb{Z}[i]/7, \mathbb{Z}[\sqrt{2}]/3, \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \ : \ b \in \mathbb{F}_5 \right\}$ sont des corps finis à $49, 9$ et 25 éléments.

3.1 Construction en quotientant par un idéal maximal

Plus généralement si A est un anneau commutatif avec unité, alors si $m \leq A$ est un idéal propre, m est maximal $\Leftrightarrow$ A/m est un corps (exo).

Rappels sur les idéaux : idéaux premiers, maximaux. Soit A un anneau commutatif non nul. Un idéal propre $I < A$ est premier si $ab \in I$, $a, b \in A \Rightarrow a$ ou $b \in I$. Un idéal propre $I < A$ est maximal s'il n'existe pas d'idéal propre $I < J < A$ (avec les inclusions strictes.

Proposition 3.1 *Soit $I < A$ un idéal propre d'un anneau commutatif. Alors I premier $\Leftrightarrow$ A/I intègre et I maximal $\Leftrightarrow$ A/I corps.*

Corollaire 3.1.1 *maximal $\Rightarrow$ premier.*

Ex. : les idéaux premiers de $\mathbb{Z}$ sont les $p\mathbb{Z}$ avec p premier ou $p = 0$. Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ avec p premier.

3.2 Corps des fractions d'un anneau intègre

Définition 3 *Soit A un anneau commutatif avec unité non nul et intègre (*i.e. *$ab = 0 \Leftrightarrow a$ ou $b = 0$).*

Si $(a,b),(c,d) \in A \times A \setminus \{(0)\}$, *on pose* $(a,b) \sim (c,d)$*si* $ad = bc$. *C'est une relation d'équivalence. On pose* a/b *la classe d'équivalence de* (a,b).

addition : $a/b + c/d := (ad+bc)/bd$,

multiplication : $a/bc/d := ac/bd$,

zéro : $0/1$,

unité : $1/1$.

Remarque : $a/b \neq 0 \Leftrightarrow a \neq 0$ *et dans ce cas l'inverse est* b/a.

Proposition 3.2 *On a obtenu un corps noté* Frac$A$ *et l'aaplication* $A \to \text{Frac}A$, $a \mapsto \frac{a}{1}$ *est injective.*

Exemples : $\mathbb{Q} = \text{Frac}\mathbb{Z}$, $\mathbb{Q}(X) = \text{Frac}\mathbb{Q}[X]$, $\text{Frac}\mathbb{C}[[T]] \simeq \mathbb{C}((T))$.

3.3 le groupe des inversibles

Notation importante : Soit K un corps. On note K^* le groupe $(K \setminus \{0\}, \cdot)$.

Théorème 3.3 *Soit* K *un corps commutatif. Si* $G \leq K^\times$ *est fini alors* G *est cyclique !*

Démonstration : Posons $\varphi(k) = |\{1 \leq k \leq n \ : \ k \wedge n = 1\}|$. Alors :

$$\sum_{k|n} \varphi(k) = n$$

si $n \geq 1$ [†]. Supposons que G est d'ordre n. Soit N_d le nombre d'éléments d'ordre d dans G. On a $\sum_{d|n} N_d = n$ car tout élément de G a un ordre qui divise n. Si $N_d \neq 0$, il existe $g \in G$ d'ordre d. Alors tout élément de $\langle g \rangle$ est solution de $X^d = 1$ dans K. Or cette équation a au plus d solution dans K [‡]. Comme il ya d éléments dans $\langle g \rangle$ les solutions de $X^d = 1$ dans K sont exactement les éléments de $\langle g \rangle$. Or dans $\langle g \rangle$, les éléments d'ordre d sont précisément $\varphi(d)$ (ce sont les g^k où $1 \leq k \leq d$ et $k \wedge d = 1$. En résumé, $N_d = 0$ ou $N_d = \varphi(d)$. En particulier, $0 \leq N_d \leq \varphi(d)$ pour tout d.

Comme $\sum_{d|n} N_d = \sum_{d|n} \varphi(d)\,(= n)$, on a forcément $N_d = \varphi(d)$ pour tout d et donc $N_n = \varphi(n) \neq 0$ et G est cyclique ! *q.e.d.*

†. En effet toute fraction dans $\left\{\frac{1}{n}, ..., \frac{n}{n}\right\}$ s'écrit d'une manière irréductible $\frac{a}{k}$ pour un $k|n$ et un a premier avec k. Le nombre de fractions irréductible ayant pour dénominateur k est exactement $\varphi(k)$ et il y a exactement n fractions dans la liste ...

‡. FAUX si K n'est pas commutatif. Par exemple $X^2 = -1$ a une infinité de solutions dans
mathbbmH ...

Contre-exemple : $\{\pm 1, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\}$ forme un sous-groupe d'ordre 8 dans $\mathbb{H}^\times$ non commutatif donc non cyclique..

Exercice 1 *On a un isomorphisme de groupes :* $\mathbb{Q}^\times \simeq \mathbb{F}_3(X)^\times$. *En effet, tout élément de* $\mathbb{Z}$ *s'écrit :* $\pm 1. \prod_{i=1}^s p_i^{\alpha_i}$ *pour certains* p_i *premiers* > 0 *deux à deux distincts et des* $\alpha_i \in \mathbb{N}$. *De plus cette écriture est unique. On en déduit en numérotant les nombres premiers* $p_1, ..., p_n, ...$ *un isomorphisme*

$$\mathbb{Q}^* \xrightarrow{\sim} \{\pm 1\} \times \mathbb{Z}^{(\mathbb{N})}$$

$$\epsilon \prod_{i\in\mathbb{N}} p_i^{\alpha_i} \longmapsto (\epsilon, (\alpha_i)_{i\in\mathbb{N}})$$

Comme les inversibles de $\mathbb{F}_3[X]$ *sont* ± 1, *comme les irréductibles de* $\mathbb{F}_3[X]$ *sont en nombre dénombrable, on a aussi :* $\mathbb{F}_3(X)^* \simeq \{\pm 1\} \times \mathbb{Z}^{(\mathbb{N})}$

3.4 Sous-corps premier, caractéristique

Soit K un corps.

Définition 4 *Soit* $p \geq 0$ *tel que* $p\mathbb{Z} = \ker(\varphi : \mathbb{Z} \to K,\ n \mapsto n1_K)$. *Le nombre* p *est la caractéristique du corps* K.

Proposition 3.4 *La caractéristique de* K *est* 0 *ou un nombre premier* > 0.

Remarque : si $p = 0$, $\mathbb{Q}$ est le plus petit sous-corps de K. Si $p > 0$, c'est $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Remarque importante : si K est de caractéristique p, alors $K \mapsto K$, $x \mapsto x^p$ est un morphisme de corps !

4 Extensions, algébricité

Définition 5 *Si* $K \leq L$ *sont des corps, on dit que* L *est une extension de* K. *On note parfois* L/K *l'extension* $K \leq L$ *(bien que l'on ne considère pas le quotient d'espaces vectoriels* L/K*).*

Notation : Dans ce cas L est aussi un $K-$espace vectoriel. On note $[L : K] := \dim_K L$: c'est le *degré de* L *sur* K.

Proposition 4.1 (multiplicativité des degrés) *Soient $K_1 \leq ... \leq K_n$ des corps. Alors $[K_n : K_1] = [K_n : K_{n-1}]...[K_2 : K_1]$.*

Démonstration : Supposons $n = 3$. Soit $(x_i)_i$ une base de K_2 comme K_1-espace vectoriel. Soit $(y_j)_j$ une base de K_3 comme K_2-espace vectoriel. Alors $(x_i y_j)_{i,j}$ est une base de K_3 comme K_1-espace vectoriel. *q.e.d.*
Exemple : $[\mathbb{Q}(\sqrt[3]{2}, j) : \mathbb{Q}] = 6$.

4.1 Éléments algébriques

Remarque : $K[X]/(P)$ est un $K-$espace vectoriel de dimension $d = \deg P$ car une base est donnée par les $X^k \bmod P$, $0 \leq k < \deg P$.

Proposition 4.2 *Soit $K \leq E$ une extension de corps. Soit $x \in E$. Sont équivalentes :*

(i) *il existe $0 \neq P \in K[X]$ tel que $P(x) = 0$;*

(ii) $\dim_K K[x]$ *est finie ;*

(iii) $K[x] = K(x)$.

Dans ce cas, on dit que x est algébrique sur K.

Dans ce cas, $K[x] = K(x)$, $K[x]$ est un $K-$espace vectoriel de dimension finie.

De plus, l'idéal $\{P \in K[X] \ : \ P(x) = 0\}$ est un idéal premier non nul engendré par un unique polynôme unitaire P_x : le *polynôme minimal* de x sur K.

Remarque, P_x est irréductible sur K et si P est un polynôme irréductible sur K qui annule x, $P = cP_x$ pour un $c \in K^\times$.

On a : $\dim_K K(x) = \deg P_x$: c'est le *degré de x sur K*.

Remarque : en particulier si x est algébrique sur K, alors tous les éléments de $K[x]$ le sont.

Remarque importante : $K[x] \simeq K[X]/(P_x)$.

Définition 6 *Une extension L/K est algébrique si tous les éléments de L sont algébriques sur K. Elle est finie si L est un $K-$ espace vectoriel de dimension finie.*

Proposition 4.3 *Si L/K est finie, alors L/K est algébrique.*

Remarque : $\overline{\mathbb{Q}}$ est une extension algébrique infinie de $\mathbb{Q}$.

Exercice 2 $e^{2i\pi/103}$ *est algébrique sur* $\mathbb{Q}$, $\cos(2\pi/7)$ *aussi,* $\sum_{k\geq 0} \frac{1\times...\times(2k-1)}{2\times...\times(2k)} t^k$ *est algébrique sur* $\mathbb{C}(t)$ *(en effet c'est* $(1-t)^{-1/2}$*).*

Proposition 4.4 *Soit $K \leq L$ une extension de corps. Si $x, y \in L$ sont algébriques sur K, alors $x+y$, xy et x/y (si $y \neq 0$) aussi !*

Démonstration : En effet, si on note $d_x = [K(x) : K]$ et $d_y = [K(y) : K]$ alors $K(x,y) = K(x)(y) = K[x,y]$ est de dimension $\leq d_x d_y$.] q.e.d.

Exercice 3 (transitivité)
1. *Si $x_1, ..., x_n$ sont algébriques sur K, alors $K(x_1, ..., x_n)/K$ est algébrique et finie !*
2. *Si $K_2 \geq K_1 \geq K$, alors K_2/K algébrique $\Leftrightarrow$ K_2/K_1 et K_1/K algébriques.*
3. *Si L/K est une extension de corps, alors $\overline{K}^L = \{x \in L : x$ est algébrique sur $K\}$ est un sous-corps de L.*

Exercice 4 *Soit E/K une extension algébrique. Soit $P \in K[X]$ unitaire qui annule $x \in E$. Alors $P = \pi_x \Leftrightarrow P$ irréductible.*

Exemple : trouver le polynôme minimal de $\sqrt{2 + \sqrt[3]{2}}$ sur $\mathbb{Q}$.

4.2 Polynômes irréductibles

Rappelons que l'anneau $K[X]$ est euclidien, donc principal donc factoriel (donc intégralement clos).

Rappels sur les anneaux :

Définition 7 *Soit A un anneau intègre.*
On dit que A est euclidien s'il existe une fonction $q : A \setminus \{0\} \to \mathbb{N}$ telle que :

$^{\forall} a, b \in A,\ b \neq 0, {}^{\exists} q, r \in A,\ a = bq + r$ *avec* $r = 0$ *ou* $r \neq 0$ *et* $q(r) < q(b)$.

On dit que A est principal si tout idéal de A peut être engendré par un élément.
On dit que $0 \neq a \in A$ est irréductible si a n'est pas inversible et si $bc = a, b,\ c \in A \Rightarrow b$ ou c inversible.
On dit que A est factoriel si tout $a \neq 0$ dans A s'écrit :

$$a = up_1....p_s$$

avec u inversibles et les p_i irréductibles et si cette écriture est unique au sens suivant :

$a = up_1...p_s = vp'_1...p'_{s'} \Rightarrow s = s'$ *et il existe* $\sigma \in \mathfrak{S}$ *tel que* $p'_i = u_i p_{\sigma(i)}$ *pour un certain* u

$$\text{euclidien} \Longrightarrow \text{principal} \Longrightarrow \text{factoriel} \Longrightarrow \text{intégralement clos}$$

$$\mathbb{R}[X,Y]/(X^2+Y^2+1) \xleftarrow{\times\times} \mathbb{R}[X,Y] \xleftarrow{\times\times} \mathbb{Z}[i\sqrt{5}]$$

Proposition 4.5 *Principal $\Rightarrow$ factoriel*

Exercice 5 *Même si K est fini, il y a une infinité de polynômes irréductibles deux à deux premiers entre eux.*

Proposition 4.6 *Soit K un corps. Soit $P \in K[X]$. Alors P est irréductible $\Leftrightarrow K[X]/(P)$ est un corps.*

4.3 Critères d'irréductiblité

Proposition 4.7 (Eisenstein) *Soit $P = a_n X^n + ... + a_0 \in \mathbb{Z}[X]$ de degré $n > 0$. Supposons qu'il existe p premier tel que :*

(i) $p \not| a_n$;

(ii) $p | a_0, ..., a_{n-1}$;

(iii) et $p^2 \not| a_0$.

Alors P est irréductible sur $\mathbb{Q}$.

Remarque : cette proposition reste vraie si on remplace $\mathbb{Z}$ par un anneau factoriel, p par unélément irréductible de A et $\mathbb{Q}$ par Frac$A$.

Exemple : si p est premier $1 + X + ... + X^{p-1}$ est irréductible sur $\mathbb{Q}$. (On applique le critère d'Eisenstein à $P(X+1)$!

Définition 8 *Soit $P \in \mathbb{Z}[X]$. On note $c(P)$ le pgcd des coefficients de P.*

Exercice 6 $c(PQ) = c(P)c(Q)$

Proposition 4.8 *Soit $P \in \mathbb{Z}[X]$. alors P est irréductible dans $\mathbb{Z}[X]$ $\Leftrightarrow$ $P \in \mathbb{Z}$ est irréductible dans $\mathbb{Z}$ ou* $\deg P > 0$ *et P est irréductible sur $\mathbb{Q}$.*

Plus généralement :

Proposition 4.9 *Si A est factoriel, alors l'anneau $A[X]$ aussi. Plus précisément les irréductibles de $A[X]$ sont les $a \in A$ irréductibles et les $P \in A[X]$ de degré > 0, tels que $c(P) \sim 1$ et P est irréductible dans $K[X]$.*

Exercice 7 *Le déterminant vu comme polynôme dans $K[X_{ij} : 1 \leq i, j \leq n]$ est irréductible.*

Exercice 8 *Le polynôme $X^3 + Y^3 - 1$ est irréductible dans $\mathbb{C}[X, Y]$*

Technique de la réduction $\bmod p$ *:* Soit $P = a_0 + ... + a_d X^d \in \mathbb{Z}[X]$. Soit p un nombre premier ; si $\overline{P} := \overline{a_0} + ... + \overline{a_d} X^d \in \mathbb{Z}/p\mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors P est irréductible sur $\mathbb{Q}$ (où l'on a noté $\overline{a_i} = a_i \bmod p \in \mathbb{Z}/p\mathbb{Z}$).

Exemple : $X^4 - X - 1$ est irréductible sur $\mathbb{Q}$ car l'est $\bmod 2$. *Contre-exemple :* $X^4 + 1$ est réductible $\bmod p$ pour tout p premier mais $X^4 + 1$ est irréductible sur $\mathbb{Q}$ [†].

4.4 Morphismes de corps

Exercice 9

$$\mathrm{Aut}(\mathbb{R}) = 1,$$
$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \{\mathrm{Id}, a + b\sqrt{2} \mapsto a - b\sqrt{2}\},$$
$$\mathrm{Aut}\mathbb{C}(t) \simeq \mathrm{PGL}_2(\mathbb{C}),$$
$$\mathrm{Aut}\mathbb{Q}(\sqrt[3]{2}) = 1\,,$$
$$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, j) \simeq \mathfrak{S}_3\ .$$

†. en effet, les facteurs irréductibles (unitaires) de $X^4 + 1$ sur $\mathbb{R}$ sont $X^2 \pm \sqrt{2}X + 1$ et aucun n'est dans $\mathbb{Q}[X]$

5 Corps de rupture, corps de décomposition

5.1 Corps de rupture

Soit $P \in K[X]$ un polynôme irréductible. Dans le corps $K[X]/(P)$, l'élément $\overline{X} := X \bmod P$ est une racine de P car $P(\overline{X}) = P(X) = 0 \bmod P$.

Théorème 5.1 *Soit L une extension de K et $\alpha \in L$ une racine de P telle que $K[\alpha] = L$. Alors $K[X]/(P) \to k[\alpha]$, $Q(X) \bmod P \mapsto Q(\alpha)$ est un isomorphisme de corps.*

Une extension L de K comme dans le théorème est un *corps de rupture de P sur K.*

En particulier $1, \alpha, ..., \alpha^{\deg P - 1}$ est une $K-$base de α.

Exemple : $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(j\sqrt[3]{2}), \mathbb{Q}(j^2\sqrt[3]{2})$ sont des corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.

Corollaire 5.1.1 *Si $P \in K[X]$ est irréductible, il existe toujours un corps de rupture de P sur K, unique à isomorphisme près.*

Réalisation du corps de rupture

Si $P(X) = X^n + a_1 X^{n-1} + ... + a_n \in K[X]$ est irréductible, alors $K[X]/(P) \simeq K[A]$ où A est la matrice :

$$\begin{pmatrix} 0 & & 0 & -a_n \\ 1 & \ddots & & \vdots \\ 0 & & 0 & \\ & & 1 & -a_1 \end{pmatrix} \in \mathscr{M}_n(\mathbb{K})$$

Par exemple : $\mathbb{C} \simeq \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ et $\mathbb{F}_{25} \simeq \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_5 \right\}$