Corps ordonnés, corps réels clos, etc.

Déf Un anneau/corps totalement ordonné R est un anneau/corps muni d'un ordre total ($\forall x, y \;\; x<y \vee y=x \vee y<x$; $\forall x,y,z \;\; x \leq y$ et $y \leq z \to x \leq z$) et compatible avec les opérations : (non $x<x$).

$$x \leq y \to x+z \leq y+z.$$
$$0 \leq x,\; 0 \leq y \to 0 \leq xy.$$

On lui associe le cône positif $P = \{a \mid a \geq 0\}$, qui satisfait alors :

$$P+P \subseteq P$$
$$P \times P \subseteq P$$
$$P \cap -P = \{0\}$$
$$P \cup -P = R$$

Déf Cône pré-positif sur R : $P+P \subseteq P$, $P \times P \subseteq P$, $-1 \notin P$, $R^2 \subseteq P$.

$\rightsquigarrow$ pré-ordre partiel. On peut avoir $P \cap -P \neq \{0\}$.

Lemme 1 Soit R un anneau, P_0 un cône pré-positif. Alors il existe $P \supseteq P_0$, cône pré-positif, tq $P \cap -P$ soit un idéal premier, et $P \cup \{-P\} = R$.

Dém Par Zorn, soit $P \supseteq P_0$ cône pré-positif maximal.

Claim : $\forall x \in R \;\; Px \cap (1+P) = \emptyset$ ou $-Px \cap (1+P) = \emptyset$.

Sinon, soient $p_1, q_1, p_2, q_2 \in P$ tels que $p_1 x = 1 + q_1$, $-p_2 x = 1 + q_2$. Alors $-p_1p_2x^2 \in 1+P$, ie $-1 = P + p_1p_2x^2$ #.

Soit $a \in R$, et supposons $Pa \cap (1+P) = \emptyset$. Posons $P' = P - Pa$.

Alors $P \subset P'$, $-a \in P'$, $P'+P' \subseteq P'$, $P' \cdot P' \subseteq P'$. ($0 \in P$)

Comme $Pa \cap (1+P) = \emptyset$, on a : $-1 \cap P' = \emptyset$
(Si $-1 = p - qa$ alors $qa = 1+p$)

Donc $P = P'$ par maximalité, i.e, $-a \in P$. $\rightsquigarrow P \cup \{-P\} = R$

Soit $J = P \cap -P$. C'est un idéal. Soient $a, b \in R$, $ab \in J$, $a \notin J$, $b \notin J$. Comme $-ab \in J$, on peut supposer $-a$ et $-b \notin P$.

Alors $Pa \cap (1+P) \neq \emptyset \neq Pb \cap (1+P)$: $p_1 a = 1+q_1$, $p_2 b = 1+q_2$
[On a montré : $Pa \cap (1+P) = \emptyset \to -a \in P$] $\rightsquigarrow$ $p_1p_2ab \in 1+P$,

ie $-1 \in P - p_1 p_2 ab \subseteq P - J \subseteq P$ #.

Cor 2 Si R est un corps, alors tout cône pré-positif peut être étendu à un cône positif.

Cor 3 Tt cône pré-positif P_0 d'un corps F est l'$\cap$ des cônes positifs le contenant.

Pf Soit $a \notin P_0$; alors $P_0 a \cap (1+P_0) = \emptyset$ ($pa = 1+q$ $\to a = \frac{(q+1)p}{p^2} \in P_0$). Alors $P' = P_0 - P_0 a$ est un cône pré-positif, contenant $-a$. Donc $a \notin P'$.

Remarque Soit $S_F = \{$sommes de carrés$\}$.
Clos par $+$ et $\times$, et $S_F \setminus \{0\}$: par $^{-1}$.
$(\sum a_i^2)^{-1} = \sum \left(\frac{a_i}{\sum a_i^2}\right)^2$.

Déf F est formellement réel/ordonnable s'il peut être ordonné

Thm 4 Soit F un corps. Sont équivalents :

(a) F est fr.

(b) $-1 \notin S_F$

(c) $\sum_{i=1}^{n} a_i^2 = 0 \to a_i = 0 \; \forall i$

(d) $F \neq S_F$ et car$(F) \neq 2$.

Facile. $a = \left(\frac{a+1}{2}\right)^2 + (-1)\left(\frac{a-1}{2}\right)^2$.

Si car$(F) > 0$, alors $-1 \in S_F$.

Extension d'un ordre du corps F à un surcorps.

Lemme 5. Soient $F \subset F_1$ des corps. Alors un ordre sur F s'étend à un ordre sur F_1 ssi $\forall n \in \mathbb{N}, \forall a_1, \dots, a_n \in F^{>0}$, $\sum a_i x_i^2 = 0$ n'a pas de sol^n non triviale dans F_1.

Dém → clair ; soit $P_0 = \{ \sum_{i=1}^{m} a_i b_i^2 \mid m \in \mathbb{N}, a_i \in F^{>0}, b_i \in F_1 \}$.

Alors $P_0 + P_0 \subseteq P_0$, $P_0 \times P_0 \subseteq P_0$, $P_0 \cap -P_0 = \{0\}$.

Lemme 6 Soit F_1 une ext^n alg. de F de degré impair, et soient $a_1, \dots, a_n \in F^{\times}$. Si l'eq^n $\sum a_i X_i^2 = 0$ a une sol^n $\neq \vec{0}$ dans F_1, elle en a une dans F.

Dém On écrit $F_1 = F(\alpha)$, et $g(X) \in F[X]$ le poly. minimal (unitaire) de α sur F. Soient $f_1(X), \dots, f_n(X) \in F[X]_{\leq 2m}$
$\deg(g) = 2m+1$ tels que $\sum a_i f_i(\alpha)^2 = 0$. Ops : $(f_1, \dots, f_n) = 1$.
Donc, il existe $h(X) \in F[X]$ tel que $\sum a_i f_i(X)^2 = g(X) h(X)$.
Alors $\deg(h) \leq 2m-1$. De plus, ops que $\deg_X \sum a_i f_i(X)^2$ est pair :
sinon les coefficients dominant des poly. de plus grand degré donnent une sol^n.
Soit h_1 un facteur premier de $h(X)$ de d° impair, et soit F_2 une ext^n de F engendrée par une racine β de $h_1(X) = 0$.
On a donc : $\sum a_i f_i(X)^2 = h_1(X) g(X) h_2(X)$, et $h_1(X)$ ne divise pas tous les $f_i(X)$. Donc l'eq^n a une sol^n non triviale dans F_2. Comme $\deg h_1(X)$ impair, on a une sol^n non triviale dans F_2. OK par induction.

Thm 7. Soit P un cône positif du corps F. Alors P s'étend à un cône positif de F_1 dans les cas suivants :

(a) $F_1 = F(\sqrt{a})$, $a \in P$

(b) $F_1 = F(\alpha)$, $[F_1 : F]$ impair

Dém (b) est clair par les 2 lemmes précedents.

Pour (a) : Supposons $\sum a_i X_i^2 = 0$ a une sol^n non triviale dans $F(\sqrt{a})$. On l'écrit $b_i + c_i\sqrt{a}$, et on obtient

$$0 = \sum_{i=1}^{n} a_i b_i^2 + a_i a c_i^2 + \sqrt{a}\, d .$$

Comme P est un ordre, et les $a_i \in F^{>0}$, on a $b_i = c_i = 0$ $\forall i$.

Déf Un corps ordonné est max^t ordonné, ssi il n'admet pas d'ext^n alg. propre ordonnée.

Un corps F est réel clos si F est formellement réel, et n'admet pas d'ext^n alg. propre qui soit formellement réelle (ie : si $F < F_1 \leq \bar{F}$, alors $S_{F_1} \ni -1$).

Rem Max^t ordonné $\to$ tt élément positif est un carré.

$\to$ l'ordre est unique.

Thm 8 Soit F un corps. Sont eq^{ts} :

(1) F a un seul ordre et est max^t ordonné

(2) F est réel clos

(3) F^2 est un cône positif de F et tt poly. de d° impair a une racine ds F

(4) $F(\sqrt{-1})$ est alg^t clos, $F \neq F(\sqrt{-1})$.

Dém (1) $\to$ (2) : Soit P l'ordre de F. Alors $F^2 \cap -F^2 = \{0\}$, $P = F^2$.

Si $F_1 \geqslant F$ est ordonnable, avec ordre $P_1 \supset P$ (néc^t, par ! de P)

Donc $F_1 = F$.

(2) $\to$ (1) : clair : soit P un ordre sur F ; par la remarque, $P = F^2 \subset F_1$, et $F = F_1$.

(1) $\to$ (3) : clair par Thm 7 ; (3) $\to$ (4) : Soit F_1 une ext^n alg. de F contenant $\sqrt{-1}$ et Galois sur F, $Gal(F_1/F) = G$.

Si L est le sscorps de F_1 fixé par un 2-Sylow de G, alors $[L:F]$ est impair, d'où $L = F$. Si $Gal(F_1/F(\sqrt{-1}))$ n'est pas trivial, il a un ssgpe d'indice 2, fixant un ss corps F_2 de F_1, de la forme $F(\sqrt{-1})(\sqrt{A})$.

Cependant, comme $F = F^2 \cup -F^2$, tout élément de $F(\sqrt{-1})$ est un carré : Si $(a+bi)^2 = (c+di)$, alors $b = d/2a$ et a^2 est une racine de $4X^2 - 4cX - d^2 = 0$, qui a une sol^n ds F.
Donc $F_2 = F_1$ et $F_1 \models ACF$.

(4) → (2). $\forall c, d \in F\ \exists a, b \in F$ tq $(a+bi)^2 = (c+di)$.
$c = a^2 - b^2$, $d = 2ab$, et $c^2 + d^2 = (a^2 + b^2)^2 \in F^2$. Donc $S_F \subseteq F^2$, et $(-1) \notin S_F$, ie F formellement réel. Mais $F(\sqrt{-1})$ n'est pas f.r, et donc F est réel clos.

<u>Cor/Rem</u> Soit F réel clos, $<$ son ordre. Pour tout $f \in F[X]$.

(a) Les facteurs premiers de $f(X)$ sont de la forme $X - a$ ou $(X-a)^2 + b^2$, avec $b \neq 0$. $(\Delta = -4b^2)$.

(b) Si $a < b$ et $f(a) < 0 < f(b)$ alors il existe $c \in F$ tel que $a < c < b$ et $f(c) = 0$.

<u>Dém</u> (a) Dans $F(\sqrt{-1})$, $f(X)$ se décompose en facteurs linéaires : $f(X) = c\prod(X - a_i)$, $c \neq 0$, $c \in F$, $a_i \in F(\sqrt{-1})$. Si $a_i \notin F$
Notons $\bar{a}_i$ le conjugué de a_i ; alors $\bar{a}_i = a_j$ pour un j.
et $(X-a_i)(X-\bar{a}_i) = X^2 - (a_i + \bar{a}_i)X + a_i\bar{a}_i$ divise f, a ses coefficients dans F. $X^2 + cX + d$ n'a pas de racine ds F $\leftrightarrow c^2 - 4d < 0$.
(b). Si $f(X)$ change de signe entre a et b, alors ce chang^t de signe provient d'un facteur linéaire.

<u>Exercice</u> Montrez qu'un corps ordonné satisfaisant (b) est un corps réel clos. Et s'il ne satisfait que (a), que se passe-t-il ? [Théorème d'Artin-Schreier : Si F est un corps, et $[F^s : F] < +\infty$ alors : ou bien $F = F^s$, ou alors $char(F) = 0$, et $F^s = F(\sqrt{-1})$]

Dans le Theorème 8 : (1) peut être remplacé par :
F a un ordre pour lequel il est maximalement ordonné.
En effet, dans ce cas, S_F est un cône positif, donc l'ordre est unique par (a) du Thm 7.

J'avais donné comme exercice le fait de décrire tous les cônes positifs de $\mathbb{Q}[X]$. Si vous trouvez cela difficile, remplacez $\mathbb{Q}$ par $\overline{\mathbb{Q}} \cap \mathbb{R}$.

Théorie de Galois infinie. Soit K un corps
En caractéristique $p > 0$, on regarde la clôture séparable de K, notée K^s ; c'est l'union de toutes les extensions de Galois finies de K. Je note $\mathcal{G}$ l'ensemble des extensions de Galois finies de K.
Si $L \subset M \in \mathcal{G}$ on a une surjection $\pi_{ML} : Gal(M/K) \twoheadrightarrow Gal(L/K)$ donnée par la restriction. Cela nous donne un système inverse dirigé $(Gal(L/K) ; \pi_{ML}, L \subset M \in \mathcal{G})$ et on a $Aut(K^s/K) = Gal(K^s/K) = \varprojlim_{L \in \mathcal{G}} Gal(L/K)$

Concrètement : on regarde $\prod_{L \in \mathcal{G}} Gal(L/K)$, muni de la topologie produit, chaque $Gal(L/K)$ étant discret. Ce produit est compact, Hausdorff, totalement discontinu. On a

$$Gal(K^s/K) = \{ (g_L)_{L \in \mathcal{G}} \mid \text{si } L \subset M,\ \pi_{ML}(g_M) = g_L \}$$

un sous-groupe fermé de $\prod_L Gal(L/K)$, donc compact.

Dualité de Galois :

$$K \subset E \subset K^s \longleftrightarrow Gal(K^s/E), \text{ sous-groupe fermé de } Gal(K^s/K)$$

$$Fix(H) \longleftarrow H$$

Si $[E:K] < \infty$ alors $Gal(K^s/E)$ est ouvert