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
$P+P\subseteq P$, $P\times P\subseteq P$
$-1\notin P$, $R^2\subseteq P$.
$\rightsquigarrow$ 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 $p_1x=1+q_1$, $-p_2x=1+q_2$. Alors $-p_1p_2x^2\in 1+P$, ie $-1=P+p_1p_2x^2$ #.

Soit $a\in A$, 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 : $-1\cap P'=\emptyset$ (translater par $-1+Pa$).
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 $Pa\cap(1+P)\neq\emptyset\neq Pb\cap(1+P)$: $p_1a=1+q_1$, $p_2b=1+q_2$
$\rightsquigarrow p_1p_2ab\in 1+P$,

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

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

<u>Cor 3</u> 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 $\underset{P'}{P_0 - P_0 a}$ est un cône pré-positif, contenant $-a$. Donc $a \notin P'$.

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

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

<u>Thm</u> 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 $\mathrm{car}(F) \neq 2$.

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

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

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

<u>Dém</u> $\to$ clair ; soit $P_0 = \{ \sum_{i=1}^{n} a_i b_i^2 \mid n \in \mathbb{N}, a_i \in F^{>0}, b_i \in F_1 \}$.

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

<u>Lemme 6</u> 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.

<u>Dém</u> On écrit $F_1 = F(\alpha)$, et $g(X) \in F[X]$ le poly. minimal (unitaire) de α sur F. Soient $f_1(X), \dots, f_n(X) \in F[X]_{\leq 2m}$ tels que $\sum a_i f_i(X)^2 = 0$. Ops : $(f_1, \dots, f_n) = 1$.

$\deg(g) = 2m+1$

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^{ré} 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.

<u>Thm 7.</u> 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 précédents.
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$^+$ 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$^+$ 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$^+$ 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$^+$ 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 $F_1 \geq F$ 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 ssgroupe 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 linéaire : $f(X) = c\prod(X - a_i)$, $c \neq 0$, $c \in F$, $a_i \in F(\sqrt{-1})$. 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 $\mathrm{char}(F) = 0$, et $F^s = F(\sqrt{-1})$]

Par le théorème 7, tout corps ordonné F a une extension algébrique ordonnée réelle close. Un tel corps est appelé une clôture réelle de F

Nous allons montrer :

- 2 clôtures réelles du corps ordonné F sont isomorphes
- La thie des corps réels clos (obtenue en axiomatisant (3) du thm 8) est complète dans le langage des anneaux. Si on rajoute $\{<\}$ au langage et l'axiome $\forall x\ x \geq 0 \to \exists y\ y^2 = x$, la théorie a l'éq.

Déf Soit (F, P) un corps ordonné, $f \in F[X]$ irréductible non constant, et $\alpha_1, \dots, \alpha_n$ ses racines dans $\overline{F}$ (= clôture alg. de F)

On pose $\sigma_r = \sum_{i=1}^{n} \alpha_i^r$, $\in F$, et on regarde la forme quadratique $\rho_f(X_1, \dots, X_n) = \sum_{1 \leq r, s \leq n} \sigma_{r+s-2} X_r X_s$.

Avec un changement de variable approprié, cette forme quadratique peut s'écrire $\sum_{i=1}^{n} b_i Y_i^2$, $b_i \in F$.

On pose $\operatorname{sgn}_P \rho_f = \#\{i \mid b_i \in P\} - \#\{i \mid b_i \in -P\}$

Thm 9 Si R est une clôture réelle $\subset \overline{F}$ de $\langle F, P \rangle$ alors

$$\operatorname{sgn}_P \rho_f = \#\{i \mid \alpha_i \in R\}.$$

Soient $\beta_1, \dots, \beta_m$ les racines de f dans R, et $\gamma_1, \overline{\gamma_1}, \dots, \gamma_\ell, \overline{\gamma_\ell}$ celles dans $\overline{F} \setminus R$.

[Algorithme de Sturm : Lang's Algebra]

On écrit : $\rho_f(X_1, \dots, X_n) = \sum_{r,s,t} \alpha_t^{r-1+s-1} X_r X_s$

$$= \sum_t \sum_{r=1}^{n} (\alpha_t^{r-1} X_r)^2$$

$$= \sum_{t=1}^{m} \left(\sum_{r=1}^{n} \beta_t^{r-1} X_r\right)^2 + \sum_{s=1}^{\ell} \left[\left(\sum_{r=1}^{n} \gamma_s^{r-1} X_r\right)^2 + \left(\sum_{r=1}^{n} \overline{\gamma_s}^{r-1} X_r\right)^2\right]$$

On pose : $Y_t = \sum_{i=1}^{n} \beta_t^{i-1} X_i$ pour $1 \leq t \leq m$,

$$Z_{2s-1} = \frac{1}{2} \sum_{i=1}^{n} (\gamma_s^{i-1} + \bar{\gamma}_s^{i-1}) X_i \qquad 1 \leq s \leq \ell$$

$$Z_{2s} = \frac{1}{2i} \sum_{i=1}^{n} (\gamma_s^{i-1} - \bar{\gamma}_s^{i-1}) X_i$$

Alors : $\rho_f(X_1, \dots, X_n) = \sum_{t=1}^{m} Y_t^2 + 2 \sum_{s=1}^{\ell} (Z_{2s-1}^2 - Z_{2s}^2)$

D'où le résultat

<u>Lemme</u> Soit R_1, R_2 2 clôtures alg. réelle de (F, P), et F_1 tel que $(F, P) \subseteq (F_1, P_1) \subseteq (R_1, R_1^2)$, avec $[F_1 : F] < \infty$. Alors il existe un F-plongement de (F_1, P_1) dans (R_2, R_2^2).

<u>Dém</u> Soit $\alpha \in F_1$ tel que $F(\alpha) = F_1$, et $f(X) \in F[X]$ son polynôme minimal. On sait que f a au moins une racine dans R_2. Soient $\varphi_1, \dots, \varphi_m : F_1 \to R_2$ les F-plongements distincts de F_1 dans R_2. Si l'on suppose qu'aucun des φ_i ne préserve P_1, cela veut dire qu'il existe $b_1, \dots, b_m \in P_1$ tels que $\varphi_1(b_1), \dots, \varphi_m(b_m) \notin R_2^2$. Cependant on sait que $F_2 = F_1(\sqrt{b_1}, \dots, \sqrt{b_m}) \subset R_1$. Par le cas précédent, il existe au moins un F-plongement φ du corps F_2 dans R_2 ; alors $\varphi|_{F_1} = \varphi_i$ pour un i, et donc $\varphi_i(b_i) \in R_2^2$, contradiction.

Comme corollaire, on obtient :

<u>Thm 10</u> (A.S) Tout corps ordonné (F, P) a une clôture réelle, et elle est unique à F-iso près.

<u>Cor 11</u> Soit R une clôture alg. réelle de (F, P), $F \subset F(\alpha) \subset R$. Alors $\#\{\text{ordres } P' \supset P \text{ sur } F(\alpha)\} = \#\{F\text{-plong}^{ts} \text{ de } F(\alpha) \text{ ds } R\}$.