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 $F_1 \models ACF$. $(\Delta = 16c^2 + d^2)$

$(4) \to (2)$. $\forall c, d \in F\ \exists a, b \in F$ 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 a 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 changt 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 $\alpha_1, \ldots, \alpha_n$ 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 $\rho_f(X_1, \ldots, X_n) = \sum_{1 \leq r, s \leq n} \sigma_{r+s-2} X_r X_s$.

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 $\text{sgn}_P\, \rho_f = \#\{i \mid b_i \in P\} - \#\{i \mid b_i \in -P\}$

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

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

Soient $\beta_1, \ldots, \beta_m$ les racines de f dans R, et $\gamma_1, \overline{\gamma}_1, \ldots, \gamma_\ell, \overline{\gamma}_\ell$ celles dans $\overline{F} \setminus R$.

[Algorithme de Sturm : Lang's Algebra]

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

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

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

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

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

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

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

D'où le résultat

<u>Lemme</u> 9 bis 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 ce que nous venons de montrer, 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>Théo 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 $\#\{\text{ordres } P' \supset P \text{ sur } F(\alpha)\} = \#\{F\text{-plong}^{ts} \text{ de } F(\alpha) \text{ ds } R\}$.

Cor 12 R réel clos, $F \subset R$ sous-corps. Alors $\bar{F} \cap R$ est réel clos. Clair par Thm 8.

Thm 13 (Tarski). La théorie des corps réels clos ($RCF_<$) (dans le langage $\{+,-,\cdot,0,1,<\}$) admet l'éq.

C'est à dire : étant donnée une formule $\varphi(x_1,\dots,x_m)$, il existe une formule $\psi(x_1,\dots,x_m)$ sans quantificateurs, telle que $Th(\mathbb{R}) \vdash \forall \bar{x}\ \varphi(\bar{x}) \leftrightarrow \psi(\bar{x})$.

Dém Critère d'éq : il suffit de montrer que si (R_1, R_1^2) et (R_2, R_2^2) contiennent le corps ordonné $(\mathbb{Q}(a_1,\dots,a_n), P)$, et si $\varphi(x,\bar{a})$ est une formule sans quanteurs (et sans autres paramètres que $\bar{a}$); alors $R_1 \models \exists x\, \varphi(x,\bar{a})$ ssi $R_2 \models \exists x\, \varphi(x,\bar{a})$.

Formule sans quanteurs : $\vee \wedge$ de formules de la forme
$$f(x,\bar{a}) = 0,\quad f(x,\bar{a}) > 0,\quad f(x,\bar{a}) < 0$$
où $f \in \mathbb{Z}[X, Y_1,\dots,Y_m]$.

Une réduction facile montre qu'il suffit de montrer quand
$$\varphi(x,\bar{a}) = \bigwedge_i f_i(x,\bar{a}) = 0 \ \wedge\ \bigwedge_j g_j(x,\bar{a}) > 0.$$

Lemme 13bis C'est vrai : si $b \in R_1$ satisfait $\varphi(x)$, alors $R_2 \models \exists x\, \varphi(x)$

Soient $F_i' = \bar{F} \cap R_i$. On peut supposer $R_1 = R_2$.

Si l'une des f_i est non-triviale, et $b \in R_1$ satisfait φ, alors $b \in F_1$, et donc $R_2 \models \varphi(b)$. On peut donc supposer $\varphi(x,\bar{a}) = \bigwedge g_j(x,\bar{a}) > 0$. On regarde l'ensemble A des zéros des g_j dans F_1. Si $A = \emptyset$, alors $\bigwedge g_j(0) > 0$, et c'est OK. Autrement, comme A est fini, $R_1 \setminus A$ est une union finie d'intervalles ouverts, disons $A = \{c_1,\dots,c_m\}$; et pour tout j , le signe de g_j sur