

Corps

(version chantier)

Marc SAGE

6 février 2018

Table des matières

1	Corps ssi tout idéal est premier	2
2	critère isomorphismes d'extension quadratiques de $\mathbb{Q}$	2
3	Sur les corps ordonnés (théorème d'Artin-Schreier)	2
4	Tout corps est engendré par ses commutateurs	3
5	Sous-corps finis	4
6	extension algébriques	4
7	Valeur absolue non archimédienne	4
8	Valeur absolue indépendante sur $\mathbb{Q}$	4

1 Corps ssi tout idéal est premier

(0) *premier* $\iff A$ *intégrale*.

Soit $a \in A$. (a^2) est premier, donc $a \in (a^2)$, donc $a = xa^2$, on simplifie, $1 = xa$, donc a inversible, CQF.

2 critère isomorphisme d'extensions quadratiques de $\mathbb{Q}$

Soit $a, b \in \mathbb{N}^*$

mq $\mathbb{Q}(\sqrt{a}) \simeq \mathbb{Q}(\sqrt{b})$ ssi $\sqrt{ab} \in \mathbb{N}$

soit f un iso. Il est iso d'anneau, donc préserve $\mathbb{Q}$, donc $f(u + v\sqrt{a}) = u + vf(\sqrt{a})$. notons $f(\sqrt{a}) = i + j\sqrt{b}$ (avec $j \neq 0$ sinon $\sqrt{b}$ pas atteint). Elevant au carré, $a = f(a) = f(\sqrt{a})^2 = i^2 + bj^2 + 2ij\sqrt{b}$, d'où $i = 0$ et $a = bj^2$ et $\sqrt{ab} = a|j|$.

3 Sur les corps ordonnés (théorème d'Artin-Schreier)

On dit que l'on peut ordonner un corps K si on peut trouver une relation d'ordre total $\leq$ sur K vérifiant les propriétés suivantes :

$$\begin{aligned} \forall a, b &\in K, \forall c \geq 0, (a \leq b \implies ac \leq bc) \\ \forall a, b, c &\in K, (a \leq b \implies a + c \leq b + c) \end{aligned}$$

1. Montrer qu'ordonner un corps revient à se donner une partie $P \subset K$ tel que $P \cdot P \subset P$, $P + P \subset P$, $P \cap (-P) = \{0\}$, $P \cup (-P) = K$.
2. Montrer que, dans un corps K ordonnable, -1 n'y est pas somme de carrés. Exemple ?
On s'attèle à la réciproque, qui est l'objet du **théorème d'Artin-Schreier**. Soit k corps où $1 \notin \sum k^2$.
3. Montrer que k admet une extension¹ maximale K pour la propriétés « -1 n'est pas somme de carrés ». (On pourra appliquer le lemme de Zorn à ces extensions, ordonnées par « $K' \geq K$ ssi K' est une extension de K ».)
4. Soit dans K un élément μ (comme « moins un ») qui n'est pas un carré. Montrer que le groupe additif $L := K^2$ muni de la multiplication $\begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} ax + \mu by \\ ay + bx \end{pmatrix}$ est une extension de K dans laquelle μ est un carré. En déduire que $-\mu$ est une somme de carrés dans K .
5. En déduire que K est ordonnable et conclure.

Solution proposée.

1. Supposons notre corps K ordonné. Noter que la seconde propriété énoncée est équivalente à la même en mettant les inégalités au sens strict. Montrons alors que $\forall a \in K, (a > 0 \iff -a < 0)$. Soit par l'absurde un $a > 0$ vérifiant $-a \geq 0$. Alors par somme, $0 = a - a \geq 0$, d'où égalité $a = 0 = -a$, exclu.
Au vu des propriétés souhaitées, il est naturel de prendre $P = \{a \in K ; a \geq 0\}$ (p comme "positif"). La propriété $PP \subset P$ vient de la première propriété vérifiée par $\geq$, le fait que $P + P \subset P$ vient de la seconde, celui que $P \cap (-P) = \{0\}$ est une reformulation de $\forall a \in K, (a > 0 \iff -a < 0)$ tandis que $P \cup (-P) = K$ traduit la comparabilité de tout $a \in K$ par rapport à 0.
Réciproquement, à P fixé, on définit $a \leq b \iff b - a \in P$.
2. Si -1 est somme de carrés, alors $-1 \in P$, donc $1 = (-1)^2 \in P$, donc $1 \in P \cap -P$, contradiction.
Penser à $\mathbb{C}$: s'il est ordonnable, $-1 = i^2$ serait dans P .

¹On rappelle qu'une *extension* d'un corps K est la donnée d'un morphisme de corps $K \hookrightarrow L$ (lequel est automatiquement injectif). On identifie abusivement l'extension au corps d'arrivée.

3. Considérons une chaîne d'extensions (k_i) où -1 n'est pas un carré. La réunion des k_i (en fait la limite projective) est alors un corps dans lequel -1 n'est pas un carré : sinon $-1 = \sum c^2$ et chaque c est dans un k_i donc tous sont dans un même k_i où -1 n'est pas carré.
4. Vérifions déjà que L est bien un corps. Idée : on construit à la main des éléments de la forme $a + b\sqrt{\mu}$ en les identifiant au couple (a, b) et en mettant le produit qu'il faut. Les deux coordonnées sont bilinéaires en (a, b) et (x, y) , donc $\times$ est distributif. Pour l'associativité, on s'attend à ce que le produit $\begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ vaille

$$(a + b\sqrt{\mu})(u + v\sqrt{\mu})(x + y\sqrt{\mu}) = aux + \mu(avy + buy + bvx) + \sqrt{\mu}(bux + avx + auy + \mu bvy).$$

On le vérifie. Ensuite, l'inverse d'un $a + b\sqrt{\mu}$ est (en conjuguant) $\frac{1}{a+b\sqrt{\mu}} = \frac{a-b\sqrt{\mu}}{a^2-\mu b^2}$: on le vérifie à la main ($a^2 - \mu b^2$ est non nul sinon μ serait un carré (et si de plus $b = 0$, alors $a = 0$)).

Extension : $a + 0\sqrt{\mu}$, ie $a \mapsto (a, 0)$ est bien morphisme d'anneaux. Puisque $(0, 1)$ n'est pas dans l'image (c'est dire que la racine de μ n'est pas dans K), on a une extension *stricte*, donc où -1 est somme de carré, mettons

$$-1 = \sum (a_i + b_i\sqrt{\mu})^2 = \sum a_i^2 + \mu \sum b_i^2 + 2\sqrt{\mu} \sum a_i b_i.$$

Puisque $\sqrt{\mu} \notin K$, la troisième somme est nulle. Puisque $-1 \notin \sum K^2$, la deuxième somme est non nulle ; ce qui permet d'isoler $-\mu = \frac{1 + \sum a_i^2}{\sum b_i^2}$. Puisque 1 est un carré et que $\sum K^2$ est stable par quotient ($\frac{p}{q} = (\frac{1}{q})^2 pq$), on en déduit que $-\mu \in \sum K^2$, *CQFD*.

5. L'ordre d'une question précédente montre que K est ordonnable par $P := \sum K^2$ (le point subtil était de montrer que $K = P \cup -P$). Montrons que l'ordre induit $p := k \cap P$ ordonne bien k

C'est une partie de k , stable par somme et produit (si $*$ désigne l'un ou l'autre, on a $p * p \subset k * k \subset k$ et $p * p \subset P * P \subset P$), on a $-p = -(k \cap P) = -k \cap -P = k \cap -P$, d'où $p \cap -p \subset P \cap -P = 0$ et enfin $k = k \cap K = k \cap (P \cup -P) = p \cup -p$.

Remarque. Les corps où -1 n'est pas somme de carrés, à l'instar de $\mathbb{R}$, ont beaucoup de propriété en commun avec ce dernier. Par exemple, on dispose du théorème des valeurs intermédiaires pour les polynômes et du théorème de Sturm pour compter le nombre de racines dans un intervalle donné. On renvoie pour plus de détails à LangAlg, chapitre XI *Real fields*.

4 Tout corps est engendré par ses commutateurs

1. Soient K un corps, a, b deux éléments non permutables de K . Montrer que l'on a

$$a = \left(b - \frac{1}{a-1}b(a-1)\right) \frac{1}{a^{-1}ba - \frac{1}{a-1}b(a-1)} \quad (\text{développer})$$

$$a = \left(1 - \frac{1}{a-1} \frac{1}{b} (a-1)b\right) \frac{1}{\frac{1}{a} \frac{1}{b} ab - \frac{1}{a-1} \frac{1}{b} (a-1)b} \quad (\text{développer})$$
2. Soient K un corps non commutatif, $x \in K$ qui commute avec tous ses conjugués. Mq x commute avec tous les monde (noter *kle* sou *s-corps* de K engendré par l'ensemble des conjugués de x ; montrer par l'absurde que s'il ne vaut pas tout cas alors il est commutatif, et conclure x central)
3. Dédurre de 2) que $H \hookrightarrow K$ sous-corps tel que $Z(K) \subset H \subset K$ et $aHa^{-1} = H$ pour tout $a \neq 0$ dans K , alors $H \in \{Z(K), K\}$ (théorème de Cartan-Brauer-Hua).
4. Dédurre de 1) que dans un corps non commutatif K , l'ensemble des commutateurs $aba^{-1}b^{-1}$ d'éléments $\neq 0$ de K engendre le corps K

Solution proposée.

1. on développe, on regroupe, on trouve $1 = 1$. Nécessaire que $a, b \neq 1$ (sinon ils commuteraient). Si le denum est nul, le num aussi, d'où $b = \frac{1}{a-1}b(a-1)$, ie $(a-1)b = b(a-1)$ ie $ab = ba$. Idem pour les commutateurs.

rq : Notons $\begin{pmatrix} i_a \\ j_a \end{pmatrix} := \begin{pmatrix} a \cdot a^{-1} \\ a^{-1} \cdot a \end{pmatrix}$. Alors la première identité mq

$$a = \left[(j_1 - j_{a-1}) \frac{1}{j_a - j_{a-1}} \right] (b) \quad \text{dès que } ab \neq ba.$$

2. Le point 1. mq $\forall \lambda \in k, a\lambda = \lambda a \implies a \in \mathbb{Z}(j_a(\lambda), j_{a-1}(\lambda)) \subset k$ car k est stable par conjugaison. Si λ et μ sont deux éléments de k , passant par un élément $a \notin k$, on a d'une part $a\lambda \notin k$ (car $\lambda^{-1} \in k$) donc $a\lambda$ et a commutent à λ et $\mu : a(\lambda\mu) = (a\lambda)\mu = \mu(a\lambda) = (\mu a)\lambda = (a\mu)\lambda = a(\mu\lambda)$, d'où λ et μ comm. Ainsi k est commutatif, donc x commute à k ; mais il commute aussi à ${}^c k$ d'après 1., ce quiconclut.
3. Si K commutatif, H est coicé entre $Z(K) = K$, donc vaut les deux. Si K non comm, ou bien $H = Z(K)$, ou bien $\exists x \in H \setminus Z(K)$ et alors $K = \mathbb{Z}(\text{conj de } x) \subset \mathbb{Z}(H) \subset H$, d'où $H = K$
4. Noutons C l'engendré des commutateurs. La secnde identité mq

$$a = (1 - [a - 1, b]) \frac{1}{[a, b] - [a - 1, b]} \text{ dès que } [a, b] \neq 0.$$

Soient $[\lambda, \mu] \neq 0$ (d'où $\lambda \in C$) et $a \in K$. Si $a \notin Z(A)$, disons $[a, b] \neq 0$, alors $a \in C$. Sinon, $[a\lambda, \mu] = a[\lambda, \mu] \neq 0$ (résultat trivial si $a = 0$), donc $a\lambda \in C$ et $a \in \lambda^{-1}C \subset C$.

5 Sous-corps finis

Mq les sous-corps de $\overline{\mathbf{F}_p} =: \mathbf{F}_{p^\infty}$ sont les $\mathbf{F}_{p^n}$ pour $n \in \{1, 2, 3, \dots, \infty\}$

Soit K un tel sous corps. Si fini, c'est un $\mathbf{F}_{p^n}$. Si infini, il contient une suite (a_k) dans $\mathbb{F}_{p^{n_k}}$ où n_k croît ssttt, donc contient une racine de $X^{p^{n_k}} - X$, donc les contient toutes, ie contient $\mathbb{F}_{p^{n_k}}$. Finalement, K contient tous

6 extensino algébriques

mq tout extensino algébrique $k \subset K$ s'étend à la cloture algébrique $\bar{k}$

DEM : on ordonne les leextensions intémérédiaire $k \subset E \subset K$ muni d'un k -morphisme σ vers $\bar{k}$ par l'inclusion /commutation évidente. Alors zorn donne un élément maximal (E, σ) . Si pas tout K , il y a un $a \in K$ hors de E , algébrique sur k . On définit $\sigma' : E[a] \rightarrow \bar{k}$ par $\sum e_i a^i \mapsto \sum \sigma(e_i) \alpha^i$ où α racine ndas $\bar{k}$ d'un polynome annulateur de a et on a une contradiction.

7 Valeur absolue non arichmédienne

8 Valeur aboslur indépendante sur $\mathbb{Q}$