AVERTISSEMENT : Il y a peut-être des erreurs et/où coquilles dans ce que j'ai écrit, gardez un esprit critique.

1 Introduction

Pour $n \in \mathbb{N}^*$, $\mathcal{P}(n)$: Soit $p_1, p_2, ..., p_n \geq 2$ des entiers naturels sans diviseurs carrés et premiers entre eux. On note $\mathbb{Q}_n = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n})$ (et par convention $\mathbb{Q}_0 = \mathbb{Q}$).
Alors on a :
i)$(1, \sqrt{p_n})$ est une $\mathbb{Q}_{n-1}$ base de $\mathbb{Q}_n$.
ii)$[\mathbb{Q}_n : \mathbb{Q}] = 2^n$.

2 Développement

Théorème 1 *$\forall n \in \mathbb{N}^*, \mathcal{P}(n)$ est vraie.*
De plus, une $\mathbb{Q}$ base de $\mathbb{Q}_n$ est $(\prod_{i\in I} \sqrt{p_i})_{I\subseteq\{1,...,n\}}$.

3 Preuve

Initialisation : $n = 1$ On va montrer $(1, \sqrt{p_1})$ est libre sur $\mathbb{Q}$. Soit $a, b \in \mathbb{Q}$, tel que $a + b\sqrt{p_1} = 0$. Si $b \neq 0$, alors $\sqrt{p_1} = \frac{-a}{b} \in \mathbb{Q}$. Ainsi $\sqrt{p_1} \in \mathbb{Q}$ donc $\sqrt{p_1} = \frac{p}{q}$ où $p, q \in \mathbb{N}$ et $pgcd(p, q) = 1$.
Alors en mettant l'égalité au carré on obtient que $q^2 p_1 = p^2$ donc $q^2 \mid p^2$ comme $pgcd(p, q) = 1$, $q = 1$, donc $p_1 = p^2$, absurde car p_1 est sans diviseurs carrés.
D'où $b = 0$, puis $a = 0$, ainsi $(1, \sqrt{p_1})$ est libre sur $\mathbb{Q}$. Donc on a $[\mathbb{Q}_1 : \mathbb{Q}] \geq 2$ et comme $X^2 - p_1 \in \mathbb{Q}[X]$ annule $\sqrt{p_1}$, $[\mathbb{Q}_1 : \mathbb{Q}] \leq 2$. On conclut l'initialisation : $[\mathbb{Q}_1 : \mathbb{Q}] = 2$ et $(1, \sqrt{p_1})$ est une $\mathbb{Q}$ base de $\mathbb{Q}_1$ en tant que famille libre à deux éléments.

Hérédité : Soit $n \in \mathbb{N}^*$, on suppose $\mathcal{P}(k)$ vraie pour $k \in \{1, 2, ..., n\}$. Montrons que $\mathcal{P}(n + 1)$ est vraie.

Soit $p_1, p_2, ..., p_{n+1} \geq 2$ des entiers naturels sans diviseurs carrés et premiers entre eux. On va montrer $(1, \sqrt{p_{n+1}})$ est une famille de $\mathbb{Q}_{n+1}$, libre sur $\mathbb{Q}_n$.

Soit $a, b \in \mathbb{Q}_n$, tel que $a + b\sqrt{p_{n+1}} = 0$. Si $b \neq 0$, alors $\sqrt{p_{n+1}} \in \mathbb{Q}_\ltimes$ dont $(1, \sqrt{p_n})$ est une $\mathbb{Q}_{n-1}$. Ainsi $\exists (c, d) \in \mathbb{Q}_n^2$ tel que $\sqrt{p_{n+1}} = c + d\sqrt{p_n}$. En élevant au carré, $\underbrace{p_{n+1}}_{\in\mathbb{Q}_n} = \underbrace{c^2 + d^2 p_{n+1}}_{\in\mathbb{Q}_n} + 2cd\sqrt{p_n}$.
Donc $2cd\sqrt{p_n} \in \mathbb{Q}_n$. Alors $cd = 0$ [1]. Deux cas se présentent alors :

1. En effet si $cd \neq 0$, alors $\sqrt{p_n} \in \mathbb{Q}_n$.
Donc $\mathbb{Q}_{n-1} = \mathbb{Q}_{n-1}(\sqrt{p_n}) = \mathbb{Q}_n$, absurde car $[\mathbb{Q}_n : \mathbb{Q}_{n-1}] = 2$

ou bien $c = 0$: $\sqrt{p_{n+1}} = d\sqrt{p_n}$ donc $\sqrt{p_{n+1}p_n} = dp_n \in \mathbb{Q}_{n-1}$ Donc $\mathbb{Q}_{n-1} = \mathbb{Q}_{n-1}(\sqrt{p_{n+1}p_n}) = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_{n-1}}, \sqrt{p_{n+1}p_n})$. Alors, en appliquant une première fois $\mathcal{P}(n)$ avec les nombres $p_1, ..., p_{n-1}, p_np_{n+1}$ on obtient que $[\mathbb{Q}_{n-1} : \mathbb{Q}] = 2^n$. Or par définition $\mathbb{Q}_{n-1} = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_{n-1}})$ donc en appliquant une seconde fois $\mathcal{P}(n)$ avec les nombres $p_1, ..., p_{n-1}$ on obtient que $[\mathbb{Q}_{n-1} : \mathbb{Q}] = 2^{n-1}$... absurde.

Même raisonnement si $d = 0$, $\sqrt{p_{n+1}} = c \in \mathbb{Q}_{n-1}$. Donc $\mathbb{Q}_{n-1} = \mathbb{Q}_{n-1}(\sqrt{p_{n+1}}) = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_{n-1}}, \sqrt{p_{n+1}})$. Alors, en appliquant une première fois $\mathcal{P}(n)$ avec les nombres $p_1, ..., p_{n-1}, p_{n+1}$ on obtient que $[\mathbb{Q}_{n-1} : \mathbb{Q}] = 2^n$. Or par définition $\mathbb{Q}_{n-1} = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_{n-1}})$ donc en appliquant une seconde fois $\mathcal{P}(n)$ avec les nombres $p_1, ..., p_{n-1}$ on obtient que $[\mathbb{Q}_{n-1} : \mathbb{Q}] = 2^{n-1}$... absurde.

Donc finalement, $b = 0$ puis $a = 0$. $(1, \sqrt{p_{n+1}})$ est une famille de $\mathbb{Q}_{n+1}$, libre sur $\mathbb{Q}_n$. Ainsi $[\mathbb{Q}_{n+1} : \mathbb{Q}_n] \geq 2$. Puis comme $X^2 - p_1 \in \mathbb{Q}_n[X]$ annule $\sqrt{p_{n+1}}$, $[\mathbb{Q}_{n+1} : \mathbb{Q}_n] \leq 2$.

En clair, $[\mathbb{Q}_{n+1} : \mathbb{Q}_n] = 2$. Ensuite en utilisant la récurrence forte et le théorème de la base télescopique on en déduit que : $[\mathbb{Q}_{n+1} : \mathbb{Q}_\ltimes] = [\mathbb{Q}_{n+1} : \mathbb{Q}_\ltimes] \times ... \times [\mathbb{Q}_{n+1} : \mathbb{Q}_0] = 2^{n+1}$. Ce qui conclut que l'hérédité.

Enfin pour déduire une base $\mathbb{Q}_n$ sur $\mathbb{Q}$, on se sert du théorème de la base télescopique qui nous dit que pour obtenir une base du grand corps sur le petit corps dans notre tour d'extensions , il suffit de multiplier les bases des extensions intermédiaires dans la tour d'extensions.

Les bases intermédiaires étant : $(1, \sqrt{p_n})$, $(1, \sqrt{p_{n-1}})$, ..., $(1, \sqrt{p_1})$, on obtient bien la base annoncée : $(\underbrace{\prod_{i \in I} \sqrt{p_i}}_{:=X_I})_{I \subseteq \{1,...,n\}}$.

4 Et en vrai à l'oral ça donne quoi ?

N'hésitez pas à aller voir ma vidéo youtube où j'ai présenté ce dév en mode entraînement pour l'oral, ensuite accompagné de questions de Phillipe Caldero. [2].

https://www.youtube.com/watch?v=Si9TeN9caT4

2. Et n'oubliez pas de partager,de liker et de commenter, svp

5 Bonus et goodies en tous genres pour satisfaire les goûts de chacun.

[3].

Dans toute la suite on prend pour p_i les nombres premiers (rangés dans l'ordre croissant) qui vérifient les hypothèses du théorème.

5.1 Un exemple d'extension algébrique mais qui n'est pas de dimension finie

On considère le corps $\mathbb{F} = \bigcup_{n=0}^{\infty} \mathbb{Q}_n$ [4].

Alors $\forall n \geq 0, [\mathbb{F} : \mathbb{Q}] \geq [\mathbb{Q}_n : \mathbb{Q}] = 2^n$, car $\forall n \geq 0, \mathbb{Q}_n$ est un sev de $\mathbb{F}$. D'où $[\mathbb{F} : \mathbb{Q}] = \infty$. Mais comme $\forall n \geq 0, \mathbb{Q}_n : \mathbb{Q}$ est algébrique sur $\mathbb{Q}$ on montre immédiatement que $\mathbb{F} : \mathbb{Q}$ est algébrique sur $\mathbb{Q}$.

$\mathbb{F}$ fournit un contre exemple pour réfuter la réciproque de la proposition selon laquelle toute extension finie est algébrique. [a]

a. La clotûre algébrique de $\mathbb{Q}$ est aussi un contre exemple.

5.2 Une somme irrationnelle

Soit $s > 2$.
On va montrer que $\sum_{k=2}^{s} \sqrt{k} \notin \mathbb{Q}$. [5]

$\sum_{k=2}^{s} \sqrt{k} = \sum_{\text{k=2,k carré parfait}}^{s} \sqrt{k} + \sum_{\text{k=2,k non carré parfait}}^{s} \sqrt{k}$.

Le premier terme est rationnel car c'est une somme d'entiers. Ainsi pour montrer ce que l'on veut, on va montrer que la seconde somme n'est pas dans $\mathbb{Q}$. Notons la T

Soit $k \in \{1, 2, ..., s\}$ un non carré parfait. On écrit sa décomposition en nombres premiers, $k = \prod_{i=0}^{N} p_i^{a_i}$. Pour tout $i \in \{1, 2, ..., N\}$, on effectue la division euclidienne de a_i par 2. Ainsi $a_i = 2q_i + \epsilon_i$, avec $\epsilon_i \in \{0, 1\}$.
Ainsi $k = \underbrace{(\prod_{i=0}^{N} p_i^{q_i})^2}_{:=\gamma_k^2} \prod_{i=0}^{N} p_i^{\epsilon_i}$, [6] d'où $\sqrt{k} = \gamma_k \times \underbrace{\prod_{i \in I_k} \sqrt{p_i}}_{=X_{I_k}}$ où $I = \{1 \leq i \leq N \,/ \epsilon_i = 1\} \in \mathcal{P}(N)$.

3. En mettre en application dans des plans d'agreg par exemple.
4. $\mathbb{F}$ est un corps en tant qu'union de corps CROISSANTS.
5. Le résultat parait quand même très intuitif, j'ai donc essayer de le montrer avec des moyens « élémentaires » sans passer par des arguments de théorie des corps. Je n'ai pas abouti. Si vous pensez avoir une solution, ca m'interesse ! Envoyer moi un mail à : jouve.adam@gmail.com
6. $\gamma_k \in \mathbb{Q}$

Ainsi $T = \sum_{\text{k=2,k non carré parfait}}^{s} \gamma_k X_{I_k}$. On regroupe les termes de cette somme où les X_{I_k} sont égaux. D'où il existe H une sous partie de $\mathcal{P}(N)$ et des $\beta_I \in \mathbb{Q}$, tels que :$T = \sum_{I\in H}^{s} \beta_I X_I$.

Si par l'absurde $T \in \mathbb{Q}$. Alors $T = q = qX_\emptyset$. Et donc ; $T - qX_\emptyset = 0$, c'est à dire $\sum_{I\in H}^{s} \beta_I X_I - qX_\emptyset = 0$. La famille $(X_I)_{I\in H} \cup X_\emptyset$ est libre sur $\mathbb{Q}$ car c'est une famille extraite de la base $(X_I)_{I\in\mathcal{P}(n+1)}$ de $\mathbb{Q}_N$. Donc $\beta_I = q = 0$.

Ainsi $T = 0$ or c'est ABSURDE car il existe des non carrés entre 2 et s. (2 est un non carré parfait par exemple).

Finalement $T \notin \mathbb{Q}$, donc $\sum_{k=2}^{s} \sqrt{k} \notin \mathbb{Q}$.

5.3 Théorie des corps et un peu de théorie de Galois.

[7]

On va montrer que $\mathbb{Q}_n/\mathbb{Q}$ est une extension galoisienne.

Premièrement $\mathbb{Q}$ est un corps parfait (car de caractéristique 0) et $\mathbb{Q}_n/\mathbb{Q}$ est une extension algébrique, donc $\mathbb{Q}_n/\mathbb{Q}$ est une extension séparable.

Secondement, le polynôme minimal des $\sqrt{p_i}$ sur $\mathbb{Q}$, noté $Irr_{\mathbb{Q}}(\sqrt{p_i})$, est égal à $X^2 - p_i$. En posant le polynôme $f = \prod_{i=1}^{n} \underbrace{Irr_{\mathbb{Q}}(\sqrt{p_i})}_{=X^2-p_i} \in \mathbb{Q}[X]$, on remarque que $\mathbb{Q}_n$ est le corps de décomposition de f sur $\mathbb{Q}$.
$\mathbb{Q}_n/\mathbb{Q}$ est donc d'une extension normale.

Ainsi $\mathbb{Q}_n/\mathbb{Q}$ est une extension galoisienne de degré fini.
Quel est son groupe de Galois ? $G := Gal(\mathbb{Q}_n/\mathbb{Q}) \simeq$?

Déjà, à titre d'information, comme l'extension est galoisienne, $|G| = [\mathbb{Q}_n : \mathbb{Q}] = 2^n$.

Soit $\sigma \in G$, pour $i \in \{1, ..., n\}$, $\sigma(\sqrt{p_i})^2 = \sigma(p_i) = p_i$. Donc on en déduit que tout éléments de G, est d'ordre 2 (ou 1 pour l'identité).À isomorphisme près, il n'existe que une seul groupe d'ordre 2^n dont tous les éléments sont d'ordre 2 (sauf l'identité) : c'est le groupe additif $(\mathbb{Z}/2\mathbb{Z})^n$. [8].

7. ATTENTION, si vous parlez de théorie de Galois le jour de l'agreg, c'est à vos risques et périls ! Je le mentionne ici car j'aime bien ça, mais je ne pense pas que je l'aurais évoqué de moi même un jour d'oral d'agreg.

8. savez vous le justifier ? moi voilà ce que j'aurais dit : comme tous les éléments sont d'ordre 2, on peut voir G comme un $\mathbb{F}_2 = (\mathbb{Z}/2\mathbb{Z})$ espace vectoriel. C'est un espace vectoriel de dimension fini car G est fini. D'après la théorie de l'algèbre linéaire , cet espace G est isomorphe linéairement à un $(\mathbb{Z}/2\mathbb{Z})^p$) qui est aussi un isomorphisme de groupe. En aussi en évoquant l'égalité des cardinaux (un iso c'est en particulier une bijection) on a en particulier $2^p = 2^n$ donc $p = n$

$G = Gal(\mathbb{Q}_n/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^n$

5.3.1 Un élément primitf ?

$\mathbb{Q}_n/\mathbb{Q}$ est une extension séparable et de degré fini, donc d'après le théorème de l'élément primitif on récupère que l'extension est monogène. question : peut-on trouver un a explicite ?

Réponse : oui !

On pose $a = \sum_{i=1}^{n} \sqrt{p_i}$

Soit $\sigma \in Gal(\mathbb{Q}_n/\mathbb{Q})$ tel que $\sigma(a) = a$.
Comme expliqué précédemment $\sigma(\sqrt{p_i}) = \pm\sqrt{p_i}$.

Comme $\sigma(a) = a$, $\sum_{i=1}^{n} \pm\sqrt{p_i} = \sum_{i=1}^{n} \sqrt{p_i}$. D'où $\sigma(\sqrt{p_i}) = \sqrt{p_i}$.
Donc $H := \{g \in Gal(\mathbb{Q}_n/\mathbb{Q})/g(a) = a\} = Gal(\mathbb{Q}_n/\mathbb{Q}(a))$. Et comme $\mathbb{Q}_n/\mathbb{Q}$ est galoisienne donc $\mathbb{Q}_n/\mathbb{Q}(a))$ aussi , d'où $\mathbb{Q}_n^H = \mathbb{Q}(a)$.
$U_i = \{g \in Gal(\mathbb{Q}_n/\mathbb{Q})/g(\sqrt{p_i}) = \sqrt{p_i}\} = Gal(\mathbb{Q}_n/\mathbb{Q}(\sqrt{p_i}))$, par les mêmes arguments évoqués juste avant, $\mathbb{Q}_n^{U_i} = \mathbb{Q}(\sqrt{p_i})$.

Or$H \subseteq U_i$ donc $\mathbb{Q}_n^{U_i} \subseteq \mathbb{Q}_n^H$ c'est à dire $\mathbb{Q}(\sqrt{p_i}) \subseteq \mathbb{Q}(a)$.

Ainsi $\mathbb{Q}_n \subseteq \mathbb{Q}(a)$. Et l'inclusion réciproque est claire, a est la somme des $\sqrt{p_i}$. D'où :

$\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1} + \sqrt{p_2} + ... + \sqrt{p_n})$.

6 Référence

On peut trouver le dév (pas rédigé comme ça) dans le livre Algèbre linéaire de Michel Cognet.

Le passage sur la théorie de Galois vient de :https ://math.stackexchange.com/

7 Mes recasages

-125 Extensions de Corps -148 Dimension d'un espace vectoriel -127 Nombres remarquables (mais pour la 127 c'est sans doute abusé).