Objectif.

On veut montrer que $\sqrt{1}+\cdots+\sqrt{n}$ est de degré $2^{\pi(n)}$ sur $\mathbb{Q}$, où $\pi(n)$ désigne le nombre de nombres premiers inférieurs ou égaux à n.

On va établir ce résultat par des moyens très élémentaires. L'intérêt, outre le résultat, est de mettre en lumière les outils développés par Évariste Galois dans ce cas très simple, et donc de s'y familiariser.

1. Généralité sur les extensions de corps.

On considère un corps k et un élément α (a priori dans un sur-corps K de k). On rappelle la notation $[K:k]$ =$\dim_k(K)$ si K est un sur-corps de k.
On considère ensuite le morphisme d'anneaux $f : \underset{P\mapsto P(\alpha)}{K[X]\to K}$.

Définition 1. —

- *Si f est injective, α est dit transcendant sur k.*
- *Sinon, α est dit algébrique sur k et $k[\alpha]$ est un k-espace vectoriel de dimension finie. Si on note π_α le polynôme minimal de α et $Im(f) = k[\alpha]$, on a alors $deg_k(\alpha)$ =$dim_k(k[\alpha])$ =$deg(\pi_\alpha)$.*

Démonstration. — $\mathrm{Ker}(f)$ est un idéal de $k[X]$. Il est donc engendré par un polynôme π_α unique à constante multiplicative près. Notons d =$\deg(\pi_\alpha)$. Comme $k_{d-1}[X]$ est un supplémentaire de $\mathrm{Kef}(f)$, $\mathrm{Im}(f)$ est isomorphe en tant qu'espace vectoriel à $k_{d-1}[X]$ Il est donc de dimension finie d. □

Rappelons que si $x=\frac{p}{q}$ est un rationnel écrit sous forme irréductible solution de $P=\sum_{i=0}^{n} a_iX^i \in \mathbb{Z}[X]$, alors $q|a_n$ et $p|a_0$.

Exemples. —

1 $deg(\alpha)=1$ si et seulement si $\alpha\in k$.
2 $P=\pi_\alpha$ si et seulement P annule α et P irréductible sur k.
3 Pour $k=\mathbb{Q}$ et $\alpha=\sqrt{2}$, on a $\pi_\alpha=X^2-2$, $deg_{\mathbb{Q}}(\alpha)=2$ et $(1,\sqrt{2})$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\sqrt{2}]$.
4 Pour $k=\mathbb{Q}$ et $\alpha=\sqrt[3]{2}$, on a $\pi_\alpha=X^3-2$, $deg_{\mathbb{Q}}(\alpha)=3$ et $(1,\sqrt[3]{2},\sqrt[3]{2}^2)$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\sqrt[3]{2}]$.
5 Pour $k=\mathbb{Q}$ et $\alpha=\sqrt{2}+\sqrt{3}$, on a $\pi_\alpha=X^2-12X^2-1$, $deg(\alpha)=4$ et $(1,\sqrt{2},\sqrt{3},\sqrt{6})$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$.

Démonstration. —

1 Dire que $\deg(\pi_\alpha) = 1$ signifie $\pi_\alpha = X - \alpha$, soit $\alpha \in k$.
2 - Si $\pi_\alpha = PQ$, alors $P(\alpha)Q(\alpha) = 0$, puis , par intégrité, par exemple, $P(\alpha) = 0$, ce qui signifie $\pi_\alpha | P$, soit $P = c\pi_\alpha$ et π_α est bien irréductible.
- Si P annule α et P irréductible, comme $\pi_\alpha | P$, on a bien $P = \pi_\alpha$.
3 $P = X^2 - 2$ est un annulateur de $\sqrt{2}$. Il est irréductible car sans racine dans $\mathbb{Q}$ (voir le rappel : si $x = p/q$ en est une avec $(p, q) = 1$, alors $q|1$ et $p|2$, soit $x = \pm 1$ ou ± 2, dont on vérifie qu'ils ne sont pas racines). Ceci signifie $(1, \sqrt{2})$ est une base puisque clairement génératrice, et $\mathbb{Q}[\sqrt{2}]$ est un $\mathbb{Q}$-espace vectoriel de dimension 2.
4 De façon analogue, $X^3 - 2$ est irréductible sur $\mathbb{Q}$ car sans racine et de degré 3. On conclut de même.
5 $\alpha^2 = 5 + 2\sqrt{6}$, puis $P = (X^2 - 5)^2 - 24 = X^4 - 10X^2 + 1$ est un annulateur de α. Il est de même sans racine dans $\mathbb{Q}$ par le rappel, donc également sans facteur de degré 3. Il reste à voir qu'il n'a pas de facteur de degré 2 à coefficients dans $\mathbb{Q}$. Pour cela, on remarque que les racines de P sont $\pm\sqrt{2} + \pm\sqrt{3}$. On vérifie que la somme ou le produit de deux d'entre elles n'est pas dans $\mathbb{Q}$. Ainsi, par exemple, $(\sqrt{2} + \sqrt{3}) + (\sqrt{2} - \sqrt{3}) = 2\sqrt{2} \notin \mathbb{Q}$, et $-(\sqrt{2} + \sqrt{3}).(\sqrt{2} + \sqrt{3}) = -5 - 2\sqrt{6} \notin \mathbb{Q}$. □

2. Extensions successives.

On rappelle la notation $[K : k] = \dim_k(K)$, cette dimension pouvant être finie ou non. Ainsi, $k[\alpha, \beta]$ désigne $k[\alpha][\beta] = k[\beta][\alpha]$. C'est l'espace des expressions polynomiales en α et β. On considère une tour d'extensions de corps $k \subset K \subset L$.

Proposition 1. — *Multiplicativité des degrés.*
$[L : k]$ est finie si et seulement si $[K : k]$ et $[L : K]$ sont finies. Si oui, on a alors $[L : k] = [L : K][K : k]$.

Démonstration. —

- Si $[L : k]$ est finie : On a alors clairement $[K : k], [L : k] \leq [L : k]$.
- Si $[L : K]$ et $[K : k]$ sont finies : notons $(a_i)_{i\in I}$ une base du Kespace vectoriel L et $(b_j)_{j\in J}$ une base du k espace vectoriel K. Montrons que $(a_i b_j)_{(i,j)\in I\times J}$ est une base du k espace vectoriel L.
  1 Caractère générateur : on prend $x \in L$. On écrit $x = \sum_{i\in I} x_i a_i$ avec $x_i \in K$, puis $x_i = \sum_{j\in J} x_{i,j} b_j$ et on a $x = \sum_{(i,j)\in I\times J} x_{i,j} a_i b_j$.
  2 Caractère libre : on suppose $x = \sum_{(i,j)\in I\times J} x_{i,j} a_i b_j = 0$. On pose $x_i = \sum_{j\in J} x_{i,j} b_j \in K$ et on a $\sum_{i\in I} x_i a_i = 0$. Par liberté de $(a_i)_{i\in I}$, $x_i = 0$ puis, par liberté de $(b_j)_{j\in J}$, on conclut $x_{i,j} = 0$.

□

Ainsi, si α et β sont algébriques sur k, alors $\alpha+\beta$ et $\alpha\beta$ le sont également.

Exemples. —

1 $[\mathbb{Q}[\sqrt{2},\sqrt[2]{3}:\mathbb{Q}]=6$.
2 $[\mathbb{Q}[\sqrt{2},\sqrt{3}];\mathbb{Q}]=4$.
3 $\mathbb{Q}[\sqrt{2},\sqrt{3}]=\mathbb{Q}[\sqrt{2}+\sqrt{3}]$.

Remarque : comme $\deg_K(\alpha)$ est inférieur au degré d'un annulateur à coefficients dans K, alors, si $k\subset K$, on a $\deg_K(\alpha)\leq\deg_k(\alpha)$.

Démonstration. —

1 Par $\mathbb{Q}\subset\mathbb{Q}[\sqrt{2}]\subset\mathbb{Q}[\sqrt{2},\sqrt[2]{3}]$, on a comme degré pour l'inclusion de gauche 2, pour celle de droite au plus 3 par la remarque, et $[\mathbb{Q}[\sqrt{2},\sqrt[2]{3}]:\mathbb{Q}]\leq 6$, avec $[\mathbb{Q}[\sqrt{2},\sqrt[2]{3}]:\mathbb{Q}]$ divisible par 2. Mais par $\mathbb{Q}\subset\mathbb{Q}[\sqrt[3]{2}]\subset\mathbb{Q}[\sqrt{2},\sqrt[2]{3}]$, on voit que $[\mathbb{Q}[\sqrt{2},\sqrt[2]{3}]:\mathbb{Q}]$ est aussi divisible par 3. On a donc bien $[\mathbb{Q}[\sqrt{2},\sqrt[2]{3}]:\mathbb{Q}]=6$.
2 On a de même $\mathbb{Q}\subset\mathbb{Q}[\sqrt{2}]\subset\mathbb{Q}[\sqrt{2},\sqrt{3}]$, le premier degré étant égal à 2, le deuxième inférieur ou égal à 2. On va montrer que c'est bien 2, soit $\sqrt{3}\notin\mathbb{Q}[\sqrt{2}]$. On va raisonner par l'absurde : $\sqrt{3}=a+b\sqrt{2}$, avec $a,b\in\mathbb{Q}$. On obtient $3=\underbrace{a^2+2b^2}_{\in\mathbb{Q}}+2ab\sqrt{2}$. Par liberté sur $\mathbb{Q}$ de $(1,\sqrt{2})$, on en déduit $a=0$ ou $b=0$. Le premier cas donne $3/2$ est un carré dans $\mathbb{Q}$, ce qui n'est pas, le deuxième 3 est un carré dans $\mathbb{Q}$, ce qui n'est pas non plus. Ceci achève la démonstration de ce point.
3 Cela vient du fait que les dimensions des deux $\mathbb{Q}$-espaces vectoriels sont égales à 4.

□

Pour simplifier, on supposera dans la suite $K\subset\mathbb{C}$ une extension de k.

Définition 2. — *k-plongement de K dans $\mathbb{C}$.*
On appelle k-plongement de K dans $\mathbb{C}$ (ou plongement s'il n'y a pas d'ambiguïté, ou si par exemple $k=\mathbb{Q}$) un morphisme de corps entre K et $\mathbb{C}$ qui fixe k.

Exemples. —

1 Un plongement agit comme l'identité sur $\mathbb{Q}$.
2 Les seuls plongements de $\mathbb{Q}[\sqrt{2}]$ sont l'identité est la conjugaison $\sqrt{2}\mapsto-\sqrt{2}$.
3 Si α est algébrique sur k, pour tout k-plongement σ de $k[\alpha]$ dans $\mathbb{C}$, on a $\sigma(\alpha)$ est une racine de π_α.

Démonstration. —

1 C'est classique et simple. On vérifie $\sigma(n)=n$ pour $n\in\mathbb{Z}$, puis, par $1=\sigma\left(n.\frac{1}{n}\right)$, on a $\sigma(1/n)=1/n$ pour $n\in\mathbb{Z}^*$.
2 Soit $\alpha=\sqrt{2}$ qui vérifie $\alpha^2=2$. On a donc $(\sigma(\alpha))^2=2$, soit $\sigma(\alpha)=\pm\alpha$. On vérifie que $\sigma(a+b\alpha)=a-b\alpha$ est bien un morphisme pour les lois du corps $\mathbb{Q}[\alpha]$.

3 C'est analogue. $\pi_\alpha(\alpha) = 0$ donc $\pi_\alpha(\sigma(\alpha)) = 0$, puisque π_α est à coefficients dans k. □

On va maintenant établir une réciproque du troisième point.

Proposition 2. — *Prolongement d'isomorphismes.*
On fait agir σ sur $k[X]$ par $\sigma.\sum_i a_i X^i = \sum_i \sigma(a_i)X^i$.

1 Soit σ un plongement de k dans $\mathbb{C}$, soit α algébrique sur k et soit β une racine de $\sigma.\pi_\alpha$. Il existe un unique prolongement de σ sur $k[\alpha]$ qui vérifie $\sigma(\alpha) = \beta$.
2 Soit σ un plongement de k dans $\mathbb{C}$, soit K une extension finie de k Il existe un plongement sur K qui prolonge σ.
3 Il y a exactement $[K : k]$ k-plongements de K.

Démonstration. —

0 Par $\pi_\alpha(\alpha) = 0$, si $\overline{\sigma}$ est un tel plongement qui prolonge σ sur $k[\alpha]$, alors $\overline{\sigma}(\alpha)$ doit être une racine de $\sigma.\pi_\alpha$. Ainsi, il y a au plus $[K : k]$ k-plongements de K dans le cas $K = k[\alpha]$. Par multiplicativité des degrés, ce résultat reste vrai pour une extension finie K de k.
1 Traitons la réciproque. Soit β une telle racine. On considère le morphisme d'anneaux $f : \underset{P\mapsto\sigma.P(\beta)}{k[X] \to \mathbb{C}}$. Comme $f(\pi_\alpha) = 0$, ce morphisme passe au quotient et on peut définir $\overline{\sigma} : \underset{x=P(\alpha)\mapsto\sigma.P(\beta)}{k[\alpha] \to \mathbb{C}}$ comme annoncé. Il y a donc exactement $[k[\alpha] : k]$ prolongement de σ.
2 On procède par récurrence sur $[K : k]$ pour établir le résultat.
3 Dans le cas où $K = k[\alpha]$, par le point précédent, il y a exactement $[K : k]$ k-plongements de K. Par multiplicativité des degrés, on obtient le résultat pour une extension finie quelconque K de k.

□

Citons une application importante.

Proposition 3. — *Éléments invariants sous les plongements.*
Soit K une extension finie de k. Soit $x \in K$. On a $x \in k$ si et seulement si x est invariant sous tout k-plongement de K dans $\mathbb{C}$.

Démonstration. — Il est clair qu'un élément de k est invariant sous l'action d'un k-plongement. Pour la réciproque, soit $\alpha \notin k$. $\deg\pi_\alpha \geq 2$. Soit donc β une racine de π_α distincte de α. On pose $\sigma(\alpha) = \beta$ et on prolonge ce plongement à K. On obtient donc un k-plongement qui ne fixe pas α. □

On remarquera ici l'importance du fait que les racines d'un irréductible soient distinctes. La séparabilité n'est donc pas loin. Citons un exemple d'intérêt par la recherche d'un générateur d'une extension finie K de k.

Proposition 4. — *Générateurs de K sur k.*
Soit K une extension finie de k. $\alpha \in K$ engendre K, c'est à dire $K = k[\alpha]$ si et seulement si les $\sigma(\alpha)$ sont deux à deux distincts pour tout σ k-plongement de K.

Démonstration. — 1 Si les $\sigma(\alpha)$ sont deux à deux distincts. Il y en a exactement $[K : k]$. Ils sont racines de π_α qui est donc de degré $[K : k]$, et donc $K = k[\alpha]$.

2 Réciproquement, s'ils ne sont pas deux à deux distincts. Le polynôme $P = \prod_\sigma (X - \sigma(\alpha))$ a ses coefficients dans k car ils sont invariants sous l'action de tous les k-plongements, et il admet au moins une racine double. $\mathrm{PGCD}(P, P')$ est alors un annulateur de α de degré strictement inférieur à $[K : k]$. α n'est donc pas un générateur de K.

□

3. Le cas d'extensions quadratiques.

Notons $\mathcal{P}$ l'ensemble des nombres premiers. Le but est de donner le degré sur $\mathbb{Q}$ de l'élément $\alpha_n = \sqrt{1} + \cdots + \sqrt{n}$, ou encore de montrer que c'est un générateur de $\mathbb{Q}[\sqrt{p}]_{p\in\mathcal{P},\ 2\leq p\leq n}$.

Rappelons la valuation p-adique d'un entier puis d'un rationnel : $v_p(n)$ désigne l'exposant de p dans la décomposition de n en produits de nombres premiers. On prolonge alors v_p sur $\mathbb{Q}$ par $v_p(n/m) = v_p(n) - v_p(m)$. On dit alors que deux rationnels x et y sont *premiers entre eux* si pour tout p premier, $v_p(x) \neq 0 \Rightarrow v_p(y) = 0$.

Proposition 5. — *Cas d'extensions quadratiques successives.*
Soient $x_1, \cdots, x_n$ des rationnels deux à deux premiers entre eux. Notons $K_n = \mathbb{Q}[\sqrt{x_1} \cdots, \sqrt{x_n}]$.
1 $[K_n : \mathbb{Q}] = 2^n$.
2 Les plongements de K_n dans $\mathbb{C}$ sont paramétrés par $\varepsilon = (\varepsilon_1, \cdots, \varepsilon_n) \in \{-1, 1\}^n$. Plus précisément, un tel plongement stabilise K_n. Notons alors σ_ε l'application de K_n dans lui-même définie par $\sigma_\varepsilon(\sqrt{x_i}) = \varepsilon_i\sqrt{x_i}$ et prolongée par linéarité. Si on note G_n le groupe de ces isomorphismes (qui agissent donc sur K_n), on a un isomorphisme $\underset{\varepsilon}{\{-1, 1\}^n} \underset{\mapsto}{\to} \underset{\sigma_\varepsilon}{G_n}$.

Démonstration. —
1 On va démontrer ce point par récurrence sur n. Rédigeons le passage du rang n au rang $n+1$. On veut donc montrer $\sqrt{x_{n+1}} \notin K_n$. Supposons donc $\sqrt{x_{n+1}} = a + b\sqrt{x_n}$ avec $a, b \in K_{n-1}$. On élève au carré et donc $x_{n+1} = a^2 + b^2 x_n + 2ab\sqrt{x_n}$, écriture dans $K_{n-1}[\sqrt{x_n}]$ qui est de dimension 2^n, ce qui signifie $(1, \sqrt{x_n})$ libre sur K_{n-1}. Par l'hypothèse de récurrence, cette relation donne a ou $b = 0$. Si $a = 0$, on a x_{n+1}/x_n est un carré dans K_{n-1}, ce qui contredit l'hypothèse de récurrence appliquée à $K_{n-1}[x_{n+1}/x_n]$ puisque $x_1, \cdots, x_{n-1}, x_{n+1}/x_n$ sont premiers entre eux. Si $b = 0$, on a x_n est un carré dans K_{n-1}, ce qui contredit l'hypothèse de récurrence appliquée à $K_{n-1}[x_n]$ puisque $x_1, \cdots, x_n$ sont premiers entre eux.

2 On sait que les plongements de K_n sont au nombre de 2^n. On peut prolonger l'identité sur $\mathbb{Q}[\sqrt{x_i}]_{i\neq j}$ en un plongement σ_j sur K_n qui vérifie $\sigma_j(\sqrt{x_i}) = \sqrt{x_i}$ pour $i \neq j$ et $\sigma_j(\sqrt{x_j}) = -\sqrt{x_j}$. Ces plongements stabilisent K_n, ils fabriquent un groupe de plongements de K_n de cardinal 2^n isomorphe à $\{-1,1\}^n$, on obtient donc bien ainsi les 2^n plongements possibles de K_n.

□

Exemples. — *Le cas $K_n = \mathbb{Q}[\sqrt{p_1}, \cdots, \sqrt{p_n}]$ où les p_i sont des nombres premiers deux à deux distincts.*
Soient $a_1, \cdots, a_n$ des éléments de $\mathbb{Q}_+^*$. Soit $\alpha_n = a_1\sqrt{p_1} + \cdots + a_n\sqrt{p_n}$. On a alors $K_n = \mathbb{Q}[\alpha_n]$.

Démonstration. — Si $\varepsilon \neq (1, \cdots, 1)$, alors au moins l'un des $\sqrt{p_i}$ est changé en son opposé, et $\sigma_\varepsilon(\alpha_n) < \alpha_n$. Puis, si $\sigma_\varepsilon(\alpha_n) = \sigma_{\varepsilon'}(\alpha_n)$, alors $\sigma_{\varepsilon(\varepsilon')^{-1}}(\alpha_n) = \alpha_n$, et donc $\varepsilon\varepsilon'^{-1} = (1, \cdots, 1)$, soit $\varepsilon = \varepsilon'$. Ainsi, les $(\sigma_\varepsilon(\alpha_n))_\varepsilon$ sont deux à deux distincts, et, par la proposition 4, on conclut $\mathbb{Q}[\alpha_n] = K_n$.

□

Application : démonstration du résultat recherché par cet article.

On va adapter la démonstration précédente pour vérifier que l'élément $\sqrt{1} + \cdots + \sqrt{n}$ est un générateur de $\mathbb{Q}[\sqrt{p_1}, \cdots, \sqrt{p_k}]$ si $p_1, \cdots, p_k$ sont les nombres premiers inférieurs ou égaux à n.

Il suffit d'écrire $\alpha_n = \sqrt{1} + \cdots + \sqrt{n}$ comme une somme de termes du type $a_I \left[\prod_{i\in I} p_i\right]^{1/2}$ avec $a_i \in \mathbb{Q}_+^*$ pour $I \subset \{1, \cdots, k\}$. Par σ_ε, chacun de ces termes est donc invariant ou changé en son opposé. Mais, pour tout $1 \leq i \leq k$, il y a donc en particulier le terme $\sqrt{p_i}$, et, à nouveau, si $\varepsilon \neq (1, \cdots, 1)$ alors $\sigma_\varepsilon(\alpha_n) < \alpha_n$.

On en déduit donc le résultat annoncé au début de cet article.