Extensions de corps, corps finis

Salim Rostam

Décembre 2024

Références : Escofier et Gozard (Théorie de Galois), Gourdon (algèbre), RDO 1, Ulmer (Anneaux, corps, résultants)

1 Corps

Définition. Un corps est un anneau commutatif dans lequel tout élément non nul est inversible.

Soit k un corps. L'anneau $\mathbb{Z}$ étant monogène, il existe un unique morphisme d'anneau $c : \mathbb{Z} \to k$ donné par $1 \mapsto 1_k$ (on a alors $c(n) = n1_k$). Le noyau est un idéal de $\mathbb{Z}$ donc de la forme $n\mathbb{Z}$ pour $n \geq 0$, et par le théorème d'isomorphisme on a donc un morphisme d'anneaux injectif $\mathbb{Z}/n\mathbb{Z} \to k$. Puisque k est intègre on en déduit que $\mathbb{Z}/n\mathbb{Z}$ également et donc $n = 0$ ou $n = p$ est premier.

Définition. L'entier n précédent est la *caractéristique* de k.

En particulier, si la caractéristique p d'un corps est > 0 alors dans k on a « $p = 0$ ».

Exemple.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps de caractéristique 0, tout comme $\mathbb{Q}(X)$ ou $\mathbb{R}(X, Y)$.
- Si p est premier alors $\mathbb{Z}/p\mathbb{Z}$ est un corps de caractéristique p (et $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier ssi $\mathbb{Z}/n\mathbb{Z}$ est intègre). Le corps $\mathbb{Z}/p\mathbb{Z}(X)$ également.

La définition fonctionne pour n'importe quel anneau commutatif ; ici ce qui est important est que la caractéristique d'un corps est un nombre premier.

Proposition. *Soit k de caractéristique $p > 0$. L'application $k \to k$ donnée par $x \mapsto x^p$ est un morphisme de corps (i.e. morphisme d'anneaux).*

Démonstration. Il suffit de remarquer que $p \mid \binom{p}{k}$ si $k \in \{1, \dots, p-1\}$. Pour cela, on peut utiliser la formule $k\binom{p}{k} = p\binom{p-1}{k-1}$ (que l'on montre par exemple avec les factorielles). Remarquons que p et k sont premiers entre eux puisque p est premier et $k \in \{1, \dots, p-1\}$. □

Le morphisme précédent est le *morphisme de Frobenius*. Ce morphisme est nécessairement injectif, mais ça n'est pas spécifique à ce morphisme.

Proposition. *Tout morphisme de corps $k \to k'$ est injectif.*

Démonstration. On rappelle que « morphisme de corps » n'est rien d'autre qu'un morphisme d'anneaux unitaires donc $1 \mapsto 1$, en particulier un tel morphisme f n'est pas nul. Le noyau $\ker f$ est un idéal de k, donc est soit $\{0\}$ soit k (s'il contient un élément non nul, cet élément est inversible donc l'idéal contient 1). Le noyau n'est pas k par la remarque précédente donc c'est $\{0\}$. □

2 Extensions de corps

Définition. Soient k, k' deux corps. On dit que k' est une *extension* de k, et on note k'/k, s'il existe un morphisme de corps $k \to k'$.

En particulier, si k est un sous-corps de k' alors k'/k est une extension. (Remarque au passage : la notation n'a rien à voir avec celle du quotient !)

Proposition. *Si k'/k est une extension alors k et k' ont la même caractéristique.*

Démonstration. Soit $c : \mathbb{Z} \to k$ le morphisme caractéristique pour k (et $c' : \mathbb{Z} \to k'$) pour k'. La caractéristique de k (resp. k') est l'unique entier $n \geq 0$ (resp. $n' \geq 0$) tel que $\ker c = n\mathbb{Z}$ (resp. $\ker c' = n'\mathbb{Z}$). Si $\iota : k \to k'$ est le morphisme d'extension alors $\iota(1_k) = 1_{k'}$. Ainsi, pour tout $a \in \mathbb{Z}$ on a $c'(a) = a1_{k'} = a\iota(1_k) = \iota(a1_k)$ (car ι est un morphisme de groupes donc $c'(a) = \iota(c(a))$. Ainsi, puisque ι est injectif on a $c'(a) = 0$ ssi $c(a) = 0$ donc $n' = n$. □

Si k'/k est une extension de corps, alors k' peut être vu comme un k-espace vectoriel. Plus précisément, si $\iota : k \to k'$ est le morphisme d'extension alors la loi externe est $\lambda \cdot x \coloneqq \iota(\lambda)x$ (les axiomes sont bien vérifiés car $\iota(k)$ est un sous-corps de k' ; les axiomes sont $1x = x$, $(\lambda + \mu)x = \lambda x + \mu x, \lambda(\mu x) = (\lambda\mu)x$ et $\lambda(x + y) = \lambda x + \lambda y$).

Définition. On note $[k' : k] \coloneqq \dim_k k'$ et on dit que c'est le *degré* de k' sur k.

Exemple. L'extension $\mathbb{C}/\mathbb{R}$ est de degré 2 mais l'extension $\mathbb{R}/\mathbb{Q}$ est (de degré) infinie (si elle était finie alors on aurait $\mathbb{R} \simeq \mathbb{Q}^n$ en tant que $\mathbb{Q}$-ev donc $\mathbb{R}$ serait dénombrable).

2.1 Corps de rupture

Le résultat suivant est fondamental.

Proposition. *Soit $P \in k[X]$ un polynôme irréductible. Alors $k_P \coloneqq k[X]/(P)$ est une extension de k de degré $\deg P$. De plus, si $x \in k_P$ est l'image de X par la projection canonique alors $(1, x, \ldots, x^{\deg(P)-1})$ est une k-base de k_P.*

Démonstration. Il faut tout d'abord montrer que $k[X]/(P)$ est un corps. C'est le cas car (P) est maximal car premier non nul ($k[X]$ est principal car euclidien car k corps ; on peut aussi le montrer directement en disant que si $I \supsetneq (P)$ est un idéal de $k[X]$ alors $I = (Q)$ est principal, or par hypothèse $Q \mid P$ donc $Q = P$ ou $Q = 1$ (en prenant Q unitaire) car P est irréductible (déf irréd : si $P = ab$ alors a ou b est inversible) donc $I = (P)$ ou $I = k[X]$). Ensuite, c'est bien une extension de k car on a une composition de morphismes d'anneaux unitaires $k \to k[X] \to k[X]/(P)$.

L'assertion sur le degré découle du fait que $(1, x, \ldots, x^{\deg P-1})$ est une k-base de $k[X]/(P)$ (où x est l'image de X). C'est clairement une famille génératrice par la définition de la division euclidienne (le reste est de degré $< \deg P$), et elle est libre car si $\lambda_0+\lambda_1 x+\cdots+\lambda_{\deg P-1}x^{\deg P-1} = 0$ alors $\lambda_0 + \lambda_1 X + \cdots + \lambda_{\deg P-1}X^{\deg P-1} \in (P)$ donc pour une raison de degré le polynôme est nul donc les λ_i aussi. □

Remarque. Si k, k' sont des corps et $P \in k[X]$ est irréductible, pour construire un morphisme $k[X]/(P) \to k'$ il suffit de considérer un morphisme de corps $\iota : k \to k'$ et de choisir une image α de X telle que $\iota(P)(\alpha) = 0$ (car alors le noyau de $k[X] \to k'$ contient (P) mais est en fait exactement (P) puisque P est irréductible).

Remarque. Pour $P \in k[X]$ irréductible, le corps $k[X]/(P)$ est appelé *corps de rupture* de P sur k. C'est, à isomorphisme près, l'unique corps R tel que si k'/k est une extension où P possède une racine alors k' est une extension de R. (Cette propriété est bien vérifiée par $k[X]/(P)$ par la remarque précédente.)

En particulier, il est bon de savoir montrer qu'un polynôme est irréductible. On donne quelques critères.

Proposition. *Soit k un corps et $P \in k[X]$ de degré 2 ou 3. Alors P est irréductible sur k ssi P ne possède pas de racine dans k.*

Démonstration. Si P possède une racine $\alpha \in k$ alors $X - \alpha$ divise P dans $k[X]$. Le quotient est de degré 1 ou 2 donc en effet P n'est pas irréductible. Réciproquement, si P n'est pas irréductible alors puisque P est non nul et non inversible (car $\deg P \geq 1$) on sait que $P = UV$ avec $U, V \in k[X]$ non nuls non inversibles (donc non constants). On a donc $\deg P = \deg U + \deg V$. Si $\deg U$ ou $\deg V = 1$ alors U ou V admet une racine dans k donc P aussi, et sinon alors $\deg U, \deg V \geq 2$ mais alors leur somme est ≥ 4 ce qui contredit $\deg P \leq 3$. □

Exemple.
- Le polynôme $X^2 + 1 \in \mathbb{R}[X]$ est irréductible (car de degré $2 \in \{2, 3\}$ sans racine) donc $k \coloneqq \mathbb{R}[X]/(X^2 + 1)$ est un corps. Ce corps est isomorphe à $\mathbb{C}$ car $i^2 + 1 = 0$ donc on a bien un morphisme $k \to \mathbb{C}$, qui est surjectif car $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$.
- Le polynôme $X^3 + X + 1 \in \mathbb{Z}/2\mathbb{Z}[X]$ est irréductible car de degré $3 \in \{2, 3\}$ sans racine. Ainsi $\mathbb{Z}/2\mathbb{Z}[X]/(X^3 + X + 1)$ est un corps de caractéristique 2, et comme il possède une $\mathbb{Z}/2\mathbb{Z}$-base de cardinal 3 ce corps est de cardinal $2^3 = 8$.

Proposition (Eisenstein)**.** *Soit $P = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ de degré $n \geq 1$. S'il existe un nombre premier p tel que :*
- *$p \mid a_i$ pour $i \in \{0, \ldots, n-1\}$;*
- *$p \nmid a_n$;*
- *$p^2 \nmid a_0$;*

alors P est irréductible dans $\mathbb{Q}[X]$.

Avant de faire la preuve on a besoin d'un petit résultat technique, utilisé dans la preuve de la factorialité de $A[X]$ quand A est factoriel. Rappelons que si $P \in \mathbb{Z}[X]$ alors son *contenu* $c(P)$ est le pgcd de ses coefficients.

Lemme (Lemme de Gauss)**.** *Soient $A, B \in \mathbb{Z}[X]$. Si $c(A) = c(B) = 1$ alors $c(AB) = 1$.*

Démonstration. Par l'absurde, on suppose qu'il existe un premier p qui divise tous les coefficients de AB. On a alors $\overline{A} \cdot \overline{B} = 0_{\mathbb{Z}/p\mathbb{Z}[X]}$. Puisque $\mathbb{Z}/p\mathbb{Z}[X]$ est intègre (puisque $\mathbb{Z}/p\mathbb{Z}$ l'est ; on regarde le degré) on en déduit que $\overline{A} = 0_{\mathbb{Z}/p\mathbb{Z}}$ ou $\overline{B} = 0_{\mathbb{Z}/p\mathbb{Z}}$ donc p divise tous les coefficients de A ou p divise tous les coefficients de A donc $p \mid c(A)$ ou $p \mid c(B)$ ce qui est absurde. □

Remarque. Cela implique le résultat suivant : si $A, B \in \mathbb{Q}[X]$ sont unitaires et tels que $AB \in \mathbb{Z}[X]$ alors $A, B \in \mathbb{Z}[X]$.

Démonstration du critère d'Eisenstein. Tout d'abord, puisque $\deg P \geq 1$ on sait que P n'est pas nul et pas non plus inversible (on rappelle que $k[X]^\times$ est exactement l'ensemble des polynômes constants non nuls, via le degré). Ensuite, quitte à considérer $\frac{1}{c(P)} P$ on peut supposer que $c(P) = 1$ (ça ne change rien puisque l'irréductibilité ne voit pas la multiplication par des inversibles). Par l'absurde, on suppose que P n'est pas irréductible *i.e.* il existe des polynômes $Q, R \in \mathbb{Q}[X]$ non inversibles tels que $P = QR$. Écrivons $Q = \frac{a}{b}\widetilde{Q}$ et $R = \frac{c}{d}\widetilde{R}$ où :
- les entiers a, b, c, d sont tels que a et b (resp. c et d) sont premiers entre eux ;
- les polynômes $\widetilde{Q}, \widetilde{R} \in \mathbb{Z}[X]$ vérifient $c(\widetilde{Q}) = c(\widetilde{R}) = 1$.

Une telle décomposition est bien possible : on met les coefficients de chaque polynôme au même dénominateur et ensuite on factorise par le plus grand diviseur commun aux numérateurs.

On a alors $bdP = a\widetilde{Q}c\widetilde{R}$. Par le lemme, on sait que $c(\widetilde{Q}\widetilde{R}) = 1$ donc en regardant les pgcd des coefficients on trouve $bd = ac$. Or a et b (resp. c et d) sont premiers entre eux donc $a \mid d$ et $b \mid c$ (resp. $d \mid a$ et $c \mid b$) donc $a = d$ et $b = c$ donc finalement $P = \widetilde{Q}\widetilde{R}$.

On réduit alors modulo p l'égalité précédente pour trouver $\lambda \bar{X}^n = \overline{\widetilde{Q}}\,\overline{\widetilde{R}} \in \mathbb{Z}/p\mathbb{Z}[X]$, où $\lambda \neq 0$ puisque $p \nmid a_n$. On remarque alors les choses suivantes.

— Les polynômes $\overline{\widetilde{Q}}$ et $\overline{\widetilde{R}}$ sont non constants. En effet, si par exemple $\overline{\widetilde{Q}}$ était constant, on aurait $\deg \overline{\widetilde{R}} = n = \deg P$ donc nécessairement $\deg R \geq P$ donc $\deg R = P$ donc $\deg Q = 0$, ce qui est impossible puisque Q est supposé non inversible.

— Les polynômes $\overline{\widetilde{Q}}$ et $\overline{\widetilde{R}}$ sont tous deux des puissances de $\bar{X}$. Par exemple, on peut raisonner par récurrence sur n et utiliser le fait que 0 est racine, ou bien utiliser la factorialité de $\mathbb{Z}/p\mathbb{Z}[X]$.

Ainsi, les coefficients constants de $\overline{\widetilde{Q}}$ et $\overline{\widetilde{R}}$ sont nuls donc les coefficients constants de $\widetilde{Q}$ et $\widetilde{R}$ sont multiples de p donc $p^2 \mid a_0$, ce qui contredit l'hypothèse. □

Par exemple, le polynôme $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$ (Eisenstein avec $p = 2$ donc $\mathbb{Q}[X]/(X^n - 2)$ est de degré n sur $\mathbb{Q}$ pour tout $n \geq 1$.

2.2 Algébricité

Un autre résultat clé pour calculer la dimension d'un extension est le suivante.

Proposition (Base télescopique ; multiplicativité des degrés)**.** *Soient k'/k et k''/k' deux extensions. Alors k'' est une extension de k, de plus k''/k est finie ssi k''/k' et k'/k sont finies, auquel cas :*

$$[k'' : k] = [k'' : k'][k' : k],$$

plus précisément, une base de k''/k est obtenue en « multipliant » (avec deux indices) une base de k''/k' et k'/k.

Démonstration. Il suffit de montrer que si $(e_i)_{1\leq i\leq m}$ est une base de k' comme k-ev et si $(e'_j)_{1\leq j\leq n}$ est une base de k'' comme k'-ev alors $(e_i e'_j)_{i,j}$ est une base de k'' comme k-ev.

— (Liberté) Si $\sum_{i,j} \lambda_{ij} e_i e'_j = 0$ alors $\sum_j (\sum_i \lambda_{ij} e_i) e'_j = 0$ donc par liberté $\sum_i \lambda_{ij} e_i = 0$ pour tout j donc par liberté $\lambda_{ij} = 0$ pour tous i, j.

— (Générateur) Soit $x \in k''$. On sait que $x = \sum_j \lambda_j e'_j$ pour $\lambda_j \in k'$. Maintenant on sait aussi que $\lambda_j = \sum_i \lambda_{ij} e_i$ et on trouve donc $x = \sum_{i,j} \lambda_{ij} e_i e'_j$.

□

Avant de donner des exemples d'applications, il nous faut introduire une notation.

Définition. Soit k'/k une extension et soient $\alpha_1, \ldots, \alpha_n \in k'$. On note $k(\alpha_1, \ldots, \alpha_n)$ le sous-corps de k' engendré par (l'image de) k et $\alpha_1, \ldots, \alpha_n$, c'est-à-dire, le plus petit sous-corps de k' qui contient k et $\alpha_1, \ldots, \alpha_n$.

Ce plus petit sous-corps existe car une intersection de sous-corps est un sous-corps.

Proposition. *Soit k'/k une extension et $\alpha, \beta \in k'$. On a $k(\alpha)(\beta) = k(\beta)(\alpha) = k(\alpha, \beta)$.*

Démonstration. Par définition on a $k(\alpha, \beta) = k(\beta, \alpha)$ donc il suffit de montrer que $k(\alpha)(\beta) = k(\alpha, \beta)$.

— Par minimalité on a $k(\alpha) \subseteq k(\alpha, \beta)$ car $k(\alpha, \beta)$ est un corps qui contient k et α, ainsi par construction on a $k(\alpha)(\beta) \subseteq k(\alpha, \beta)$.

— Le corps $k(\alpha)(\beta)$ est un sous-corps de k' qui contient k, α, β donc par minimalité il contient $k(\alpha, \beta)$, ce qui conclut par double inclusion.

□

Définition. Soit k'/k une extension.
— On dit que k'/k est *finie* si $[k' : k] < \infty$.
— On dit que $\alpha \in k'$ est *algébrique* sur k s'il existe $P \in k[X] \setminus \{0\}$ tel que $P(\alpha) = 0$.
— On dit que k'/k est *algébrique* si tous les éléments de k' sont algébriques sur k.

Exemple. L'extension $\mathbb{C}/\mathbb{R}$ est finie car de degré $2 < \infty$, de plus $i \in \mathbb{C}$ est algébrique sur $\mathbb{R}$ puisque $i^2 + 1 = 0$. Plus généralement, tout $z = a + ib \in \mathbb{C}$ est algébrique sur $\mathbb{R}$ puisque $(z - a)^2 + b^2 = 0$.

Proposition. *Soit k'/k une extension. Un élément $\alpha \in k'$ est algébrique sur k ssi $[k(\alpha) : k] < \infty$. Dans ce cas, on a $[k(\alpha) : k] = \deg P$, où P est l'unique générateur unitaire de l'idéal $\{Q \in k[X] : Q(\alpha) = 0\}$. De plus, le polynôme P est irréductible et on $k(\alpha) = \{Q(\alpha) : Q \in k_{\deg P - 1}[X]\} \simeq k[X]/(P)$ (isomorphisme de corps).*

Démonstration. Supposons α est algébrique sur k et montrons que $k[X]/(P) \simeq k(\alpha)$. Tout d'abord, le polynôme P est irréductible puisque si $P = QR$ alors $0 = P(\alpha) = Q(\alpha)R(\alpha)$ alors par minimalité on a $\deg Q = 0$ ou $\deg R = 0$. On considère le morphisme de k-algèbres $f : k[X] \to k(\alpha)$ donné par $f(X) = \alpha$. On a $P \in \ker(f)$ donc f se factorise en un morphisme de corps $k[X]/(P) \to k(\alpha)$. Le morphisme est injectif, de plus son image est un corps qui contient k et α donc par minimalité l'image contient $k(\alpha)$, donc le morphisme est surjectif.

Réciproquement, si $[k(\alpha) : k] = n < \infty$ alors la famille $(1, \alpha, \dots, \alpha^n)$ est k-liée donc il existe des scalaires non tous nuls $\lambda_i \in k$ tels que $\sum_{i=0}^n \lambda_i \alpha^i = 0$. Ainsi α est annulé par le polynôme non nul $\sum_{i=0}^n \lambda_i X^i$ donc α est algébrique sur k. □

Remarque. Le polynôme P précédent est appelé *polynôme minimal* de α sur k.

Exemple. On montre que $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$ et que $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. Pour cela, on utilise de concert Eisenstein et la formule de multiplicativité des degrés. Par la démonstration de la formule de multiplicativité des degrés, une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ est $(1, \sqrt{2}, i, i\sqrt{2})$.

Exemple. On sait que $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$ est de degré au plus 2 (cf. polynôme annulateur) donc $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est de degré 2 ou 4 sur $\mathbb{Q}$. C'est 2 ssi $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ donc ssi il existe $a, b \in \mathbb{Q}$ tels que $\sqrt{3} = a + b\sqrt{2}$. On aurait alors $3 = a^2 + 2b^2 + 2\sqrt{2}ab$, donc $ab = 0$ puisque $(1, \sqrt{2})$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. On a $b \neq 0$ puisque $\sqrt{3} \notin \mathbb{Q}$, ainsi $a = 0$ et donc $3 = 2b^2$. En posant $b = \frac{u}{v}$ avec $\operatorname{pgcd}(u, v) = 1$ on a $3v^2 = 2u^2$ donc $2 \mid v$ donc $v = 2v'$ donc $3 \cdot 2^2 v'^2 = 2u^2$ donc $2 \mid u$ donc $2 \mid \operatorname{pgcd}(u, v)$.

Corollaire. *1. Une extension finie est algébrique. La réciproque est fausse.*

2. La somme, le produit de deux éléments algébriques et l'inverse d'un élément algébrique reste algébrique.

3. Si k''/k' et k'/k sont deux extensions algébriques alors k''/k est algébrique. En particulier, un élément algébrique sur une extension algébrique d'un corps k est algébrique sur k.

4. Si k'/k est une extension, l'ensemble des éléments de k' algébriques sur k est un sous-corps de k' (et une extension algébrique de k).

Démonstration. Point 1. Si k'/k est finie alors pour tout $\alpha \in k'$ on a $k(\alpha) \subseteq k'$ donc $[k(\alpha) : k] \leq [k' : k]$ (d'après les théorèmes généraux sur les espaces vectoriels) donc α est algébrique. On va faire la réciproque plus tard.

Pour le deuxième point, si $\alpha, \beta \in k'$ sont algébriques sur k alors β est algébrique sur k donc sur $k(\alpha)$ donc $k(\alpha)(\beta) = k(\alpha, \beta)$ est finie sur $k(\alpha)$, donc par la formule de multiplicativité des degrés on sait que $k(\alpha, \beta)$ est finie sur k. Ainsi $\alpha + \beta, \alpha\beta, \alpha^{-1} \in k(\alpha, \beta)$ donc $k(\alpha + \beta), k(\alpha\beta), k(\alpha^{-1}) = k(\alpha)$ sont finies sur k ce qui conclut.

Point 3. Si maintenant $\alpha \in k''$ est algébrique sur k' qui est algébrique sur k, alors il existe $P \in k'[X]$ tel que $P(\alpha) = 0$. Si $a_0, \dots, a_n$ sont les coefficients de P, par hypothèse chaque a_i est algébrique sur k. Ainsi, on a $P \in k(a_0, \dots, a_n)[X]$ et $k(a_0, \dots, a_n)/k$ est finie (par exemple par récurrence sur n : on a vu que c'était vrai pour $n = 0$ et pour $n \geq 1$ on conclut par multiplicativité des degrés puisque $k(a_0, \dots, a_{n-1})(a_n)/k(a_0, \dots, a_{n-1})$ est finie (cf. polynôme minimal de a_n sur k qui annule a_n sur $k(a_0, \dots, a_{n-1})$). Ainsi, l'extension $k(a_0, \dots, a_n)(\alpha)/k(a_0, \dots, a_n)$ est finie donc $k(a_0, \dots, a_n, \alpha)/k$ est finie donc $k(\alpha)/k$ aussi (multiplicativité des degrés) donc α est algébrique sur k.

Le point 4 découle du point 2.

Réciproque du point 1. On sait que l'ensemble $\overline{\mathbb{Q}}$ des complexes algébriques sur $\mathbb{Q}$ est une extension de $\mathbb{Q}$. Par définition chaque élément de $\overline{\mathbb{Q}}$ est algébrique sur $\mathbb{Q}$ donc $\overline{\mathbb{Q}}/\mathbb{Q}$ est algébrique, en revanche pour chaque $n \geq 1$ le réel $z_n \coloneqq \sqrt[n]{2}$ est dans $\overline{\mathbb{Q}}$ (car annulé par $X^n - 2$ et on a vu qu'il est irréductible, par Eisenstein) et $[\mathbb{Q}(z_n) : \mathbb{Q}] = n$. Ainsi, l'extension $[\overline{\mathbb{Q}} : \mathbb{Q}]$ ne peut pas être finie de degré N car puisque $\mathbb{Q}(z_n) \subseteq \overline{\mathbb{Q}}$ on aurait $n \leq N$ pour tout $n \geq 1$. □

On mentionne le résultat suivant (pas très facile mais pas très dur ; ça peut faire un développement).

Théorème (Élément primitif)**.** *Si $k/\mathbb{Q}$ est finie (i.e. $[k : \mathbb{Q}] < \infty$) alors il existe $\alpha \in k$ tel que $k = \mathbb{Q}(\alpha)$.*

Exemple. Par exemple, $\alpha \coloneqq \sqrt{2} + \sqrt{3}$ est un élément primitif de $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Remarquons tout d'abord que $\alpha \neq 0$ puisque $(1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3})$ est $\mathbb{Q}$-libre donc la sous-famille $(\sqrt{2}, \sqrt{3})$ également. On a $(\alpha - \sqrt{2})^2 = 3$ donc $\alpha^2 - 2\sqrt{2}\alpha + 2 = 3$ donc $\alpha^2 - 2\sqrt{2}\alpha = 1$ donc $\sqrt{2} = (\alpha^2 - 1)/(2\alpha) \in \mathbb{Q}(\alpha)$. Puisque $\sqrt{3} = \alpha - \sqrt{2}$ on a également $\sqrt{3} \in \mathbb{Q}(\alpha)$. Finalement on a $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha)$ donc $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha)$.

Or on sait que $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ donc $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ donc on conclut que ces deux extensions sont égales.

Si on veut trouver le polynôme minimal de α, avec la relation précédente $\sqrt{2} = (\alpha^2 - 1)/(2\alpha)$ on trouve $2 = (\alpha^2 - 1)^2/(4\alpha^2)$ donc α est annulé par $(X^2 - 1)^2 - 8X^2 = X^4 - 10X^2 + 1$. Puisque $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ on sait qu'on tient le polynôme minimal.

Finalement, terminons par des résultats un peu plus difficiles.

Proposition. *Soit $P \in k[X]$. Il existe une extension k_s/k sur laquelle P est* scindé *et telle que si k'/k est une autre extension sur laquelle P est scindé alors k' est une extension de k_s.*

Une telle extension minimale sur laquelle P est scindé (*i.e.* produit de polynômes de degré 1) est un *corps de décomposition* de P sur k. L'existence découle des corps de rupture successifs pour les facteurs irréductibles de P, et l'unicité peut se montrer par récurrence sur le degré de P.

Remarque. Un corps de rupture d'un polynôme irréductible ne contient pas forcément toutes ses racines. Par exemple, le polynôme $X^3 - 2$ est irréductible sur $\mathbb{Q}$ (par Eisenstein), mais le corps $\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}[X]/(X^3 - 2)$ ne contient pas les autres racines $j^{\pm 1}\sqrt[3]{2}$.

Définition. Soit k un corps.

— Le corps k est dit *algébriquement clos* si tout polynôme non constant à coefficients dans k admet une racine dans k.

— Si k'/k est une extension algébrique où k' est algébriquement clos, on dit que k' est une *clôture algébrique* de k.

Théorème (D'Alembert–Gauss)**.** *Le corps $\mathbb{C}$ est algébriquement clos.*

Démonstration. (La preuve est celle de R.P. Boas.) Soit $P \in \mathbb{C}[X]$ de degré $d \geq 1$. Quitte à considérer le polynôme $Q \coloneqq P\overline{P} \in \mathbb{R}[X]$, on peut supposer que $P \in \mathbb{R}[X]$ (si z est une racine de Q, si c'est une racine de P c'est bon et sinon z est racine de $\overline{P}$ donc $\bar{z}$ est racine de P.) On suppose que P n'admet pas de racine dans $\mathbb{C}$. Ainsi, l'application $\phi : [0, 2\pi] \to \mathbb{C}$ donnée par $\theta \mapsto \frac{1}{P(2\cos\theta)}$ est continue et ne s'annule pas, ainsi :

$$\int_0^{2\pi} \phi(\theta) d\theta \neq 0.$$

On a de plus :

$$\begin{aligned}
\int_0^{2\pi} \frac{d\theta}{P(2\cos\theta)} &= \int_0^{2\pi} \frac{ie^{i\theta} d\theta}{ie^{i\theta} P(e^{i\theta} + e^{-i\theta})} \\
&= \frac{1}{i} \int_{|z|=1} \frac{dz}{zP(z + z^{-1})} \\
&= \frac{1}{i} \int_{|z|=1} \frac{z^{d-1} dz}{z^d P(z + z^{-1})} \\
&= \frac{1}{i} \int_{|z|=1} f(z) dz,
\end{aligned}$$

où $f(z) \coloneqq \frac{z^{d-1}}{R(z)}$ où $R(z) \coloneqq z^d P(z + z^{-1})$. Montrons que R (qui est à priori une fraction rationnelle) est un polynôme sans racine sur $\mathbb{C}$.

Si $P = \sum_{k=0}^{d} a_k X^k$ alors :

$$\begin{aligned}
R &= X^d P(X + X^{-1}) \\
&= \sum_{k=0}^{d} a_k X^d (X + X^{-1})^k \\
&= \sum_{k=0}^{d} a_k X^{d-k} X^k (X + X^{-1})^k \\
&= \sum_{k=0}^{d} a_k X^{d-k} (X^2 + 1)^k,
\end{aligned}$$

donc R est bien un polynôme, de plus on obtient son terme en 0 en regardant simplement le terme de la somme pour $k = d$ (car le X^{d-k} devient 0 quand on l'évalue en 0 si $k \in \{0, \ldots, d-1\}$) et on trouve alors $R(0) = a_d \neq 0$ puisque $\deg P = d$.

Ainsi, puisque $R = X^d P(X + X^{-1})$ on sait déjà que R ne possède pas de racine complexe non nulle sur $\mathbb{C}$ puisque P n'en possède pas, et on vient de voir que $R(0) \neq 0$ donc 0 n'est pas non plus racine de R. Ainsi R n'a pas de racine complexe, ainsi $f(z) = \frac{z^{d-1}}{R(z)}$ est holomorphe sur $\mathbb{C}$ donc $\int_{|z|=1} f(z)dz = 0$, ce qui est une contradiction. □

Théorème (Steinitz)**.** *Tout corps possède une clôture algébrique, unique à isomorphisme près.*

Exemple. Une clôture algébrique de $\mathbb{R}$ est $\mathbb{C}$ (qui est bien algébrique sur $\mathbb{R}$ puisque finie).

Proposition. *Si k'/k est une extension avec k' algébriquement clos, alors $\bar{k} \coloneqq \{x \in k' : x$ algébrique sur $k\}$ est l'unique clôture algébrique de k incluse dans k'.*

Démonstration. On a vu que $\bar{k}$ est bien un corps, qui est une extension algébrique de k.

— Montrons que $\bar{k}$ est algébriquement clos. Soit $P \in \bar{k}[X]$. On a $P \in k'[X]$ donc P possède une racine sur k'. De plus pour $P \in \bar{k}[X]$ alors $P \in k'[X]$ donc P admet une racine $\alpha \in k'$, mais α est alors algébrique sur k donc $\alpha \in \bar{k}$.

— Montrons l'unicité. Si $k'' \subseteq k'$ est une autre clôture algébrique de k, si $x \in k''$ alors x est algébrique sur k donc $x \in \bar{k}$. Réciproquement, si $x \in \bar{k}$, considérons son polynôme minimal P sur k. Par hypothèse P possède une racine dans k'', et en faisant des divisions euclidiennes successives on trouve que $x \in k''$.

□

Démonstration du théorème de Steinitz. Soit k un corps et soit $\mathcal{P}$ l'ensemble des polynômes non constants à coefficients dans k. On considère l'anneau de polynômes $A \coloneqq k[X_f : f \in \mathcal{P}]$ (chaque élément est un polynôme en un nombre fini d'indéterminées).

1) On va d'abord construire une extension k'/k sur laquelle tout élément de $\mathcal{P}$ possède une racine. Pour cela, on considère l'idéal I engendré par les $f(X_f)$ pour $f \in \mathcal{P}$. Si cet idéal coïncide avec A alors $1 \in I$ donc il existe $f_1, \dots, f_n \in \mathcal{P}$ et $a_1, \dots, a_n \in A$ tels que $1 = \sum_{i=1}^n a_i f_i$. On peut trouver une extension de k sur laquelle $f_1 \cdots f_n$ est scindé, et si x_i y est une racine de f_i alors en substituant x_i à X_{f_i} on obtient $1 = \sum_{i=1}^n a_i(\cdot) f_i(x_i) = 0$, ce qui est absurde.
2) Ainsi l'idéal I est strict, il est donc inclus dans un idéal maximal $\mathfrak{m}$ et $k' \coloneqq A/\mathfrak{m}$ est donc un corps, dans lequel k s'injecte via $k \to A \to A/\mathfrak{m}$. Pour $f \in \mathcal{P}$ on a $f(X_f) \in I \subseteq \mathfrak{m}$ donc l'image de $f(X_f)$ dans k' est nulle. Ainsi, le polynôme f possède bien une racine dans k' (une telle racine est l'image de X_f dans k').
3) On peut recommencer cette construction avec k' et finalement trouver une tour de corps $k_0 \coloneqq k \subseteq k_1 \coloneqq k' \subseteq k_2 \subseteq k_3 \subseteq \dots$. On pose alors $\Omega \coloneqq \cup_{i \geq 0} k_i$ qui est bien un corps comme union croissante de corps, et si $P \in \Omega[X]$ alors il existe i tel que $P \in k_i[X]$ (regarder P coefficients par coefficients) donc P admet une racine dans $k_{i+1} \subseteq \Omega$ et donc Ω est algébriquement clos.
4) Finalement, a déjà vu qu'alors $\overline{k} \coloneqq \{x \in \Omega : x$ algébrique sur $k\}$ est une clôture algébrique de k.

□

3 Corps finis

3.1 Prélude sur les polynômes

Soit k un corps commutatif.

Définition. Soit $P \in k[X]$ et $a \in k$. On dit que a est *racine* de P si $P(a) = 0$.

Proposition. *Un polynôme non nul de degré n sur k possède au plus n racines dans k.*

Démonstration. On montre la propriété par récurrence sur le degré n. Si $n = 0$ c'est clair car le polynôme ne possède alors pas de racine (donc bien au plus 0).

On suppose maintenant $n \geq 1$. Si P ne possède pas de racine sur k c'est gagné. Supposons donc que $x \in k$ est racine de P. On écrit la division euclidienne de P par $X - x$: il existe $Q, R \in k[X]$ avec $\deg R < 1$ tel que $P = (X - x)Q + R$. Puisque $\deg R \leq 0$ on a $R = r \in k$. En évaluant en $X = x$ on trouve $P(x) = r$ donc $r = 0$ puisque x est racine de P. Ainsi $P = (X - x)Q$.

On a $\deg Q = \deg P - 1 = n - 1 \geq 0$ donc par hypothèse de récurrence, le polynôme Q possède au plus $n-1$ racines. Puisque pour tout $y \in k$ on a $P(y) = 0 \iff (y-x)Q(y) = 0 \iff y = x$ ou $Q(y) = 0$ (car k est un corps donc intègre) on en déduit que P possède au plus $1 + (n-1) = n$ racines. □

Remarque. L'énoncé devient faux si k est non commutatif, ou si k n'est qu'un anneau (même commutatif). Par exemple, dans $\mathbb{Z}/8\mathbb{Z}$, le polynôme $X^2 - 1$ possède quatre racines ($\pm\bar{1}$ et $\pm\bar{3}$).

Proposition. *Soit $P \in k[X]$ tel que $P' \in k^\times$. Alors P est à racines simples sur k.*

Démonstration. Si P possède une racine double sur k alors il existe $\alpha \in k$ et $Q \in k[X]$ non nul tel que $P = (X-\alpha)^2 Q$. Ainsi $P' = 2(X-\alpha)Q + (X-\alpha)^2 Q'$ et donc α est racine de P'. Cela contredit le fait que P' est constant ! □

3.2 Existence (et unicité) des corps finis

On a vu que si un corps k est de caractéristique 0 alors $\mathbb{Q} \subseteq k$ donc k est infini, ainsi un corps fini est nécessairement de caractéristique première. (On rappelle que la réciproque n'est pas vrai, comme le montre par exemple le corps $\mathbb{Z}/p\mathbb{Z}(X)$.)

Proposition. *Soit k un corps fini, de caractéristique p. Il existe un entier $d \geq 1$ tel que $\#k = p^d$.*

Démonstration. On va montrer que k possède une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. Soit $\gamma : \mathbb{Z}/p\mathbb{Z} \to k$ donnée par la factorisation du morphisme caractéristique. La structure de $\mathbb{Z}/p\mathbb{Z}$-ev est alors donnée par $\lambda \cdot x \coloneqq \gamma(\lambda)x$ pour tout $\lambda \in \mathbb{Z}/p\mathbb{Z}$ et $x \in k$. On vérifie les axiomes d'espace vectoriel en utilisant les axiomes de corps et le fait que γ est un morphisme d'anneaux.

Maintenant $\{x : x \in k\}$ est une partie génératrice finie de k en tant que $\mathbb{Z}/p\mathbb{Z}$-ev donc k est de dimension finie. Si d est cette dimension alors k est en bijection avec l'ensemble des d-uplets d'éléments de $\mathbb{Z}/p\mathbb{Z}$ (les coordonnées dans une base) donc $\#k = p^d$. □

Proposition. *Soit p un nombre premier et $n \geq 1$.*
- *Soit k un corps fini, de cardinal p^n. Alors k est un corps de décomposition sur $\mathbb{Z}/p\mathbb{Z}$ du polynôme $X^{p^n} - X$.*
- *Il existe un corps fini à p^n éléments, unique à isomorphisme près. On le note $\mathbb{F}_{p^n}$.*

Démonstration. Si $\#k = p^n$ alors $k^\times$ est un groupe multiplicatif de cardinal $p^n - 1$ donc pour tout $x \in k^\times$ on a $x^{p^n-1} = 1$ donc $x^{p^n} = x$. Cette égalité est également vérifiée pour $x = 0$ donc tous les éléments de k sont des racines de $X^{p^n} - X \in \mathbb{Z}/p\mathbb{Z}[X]$. On sait que $\#k = p^n$ et que $X^{p^n} - X$ possède au plus p^n racines sur k donc finalement $X^{p^n} - X$ est bien scindé sur k. Par minimalité, on en déduit que k est bien un corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$, et il est unique à isomorphisme près par unicité du corps de décomposition.

Réciproquement, soit K un corps de décomposition de $X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$ (ou plus simplement, un corps où ce polynôme se décompose) et soit $k \coloneqq \{x \in K : x^{p^n} = x\}$. En utilisant le morphisme de Frobenius on voit que k est un sous-corps de K. De plus $X^{p^n} - X \in \mathbb{Z}/p\mathbb{Z}$ est de dérivée $1 \neq 0$ donc est à racines simples dans K. Puisque $X^{p^n} - X$ est scindé sur K et que $\deg(X^{p^n} - X) = p^n$, on en déduit que $\#k = p^n$. Par ce qui précède, ce corps est unique à isomorphisme près. □

Une question demeure cependant : pour construire un corps de décomposition de $X^{p^n} - X$, on a dit qu'il fallait prendre des corps de rupture successifs pour les facteurs irréductibles. En fait, on va voir qu'il suffit de considérer un corps de rupture (on est content car la construction est beaucoup plus facile).

Théorème. *Soit k un corps fini.*

— *Le groupe multiplicatif $k^\times$ est cyclique.*
— *Si k est de cardinal p^n (avec p premier) alors il existe $P \in \mathbb{F}_p[X]$ irréductible de degré n tel que $k \simeq \mathbb{F}_p[X]/(P)$.*

Démonstration. Le premier résultat est ultra classique. On propose ici une démonstration élémentaire, par récurrence forte. En fait, on va montrer que si K est un corps (pas forcément fini) et si G est un sous-groupe de $K^\times$ de cardinal $n \geq 1$ alors G est cyclique.

— Si $\#G = p^a$ avec p premier (par forcément la caractéristique) et $a \geq 1$, si G n'est pas cyclique alors tout élément est d'ordre divisant p^{a-1} donc tout $x \in G$ vérifie $x^{p^{a-1}} = 1$ donc les éléments de G sont racines de $X^{p^{a-1}} - 1$. Ce polynôme est de degré p^{a-1} donc possède au plus p^{a-1} racines, ce qui est absurde puisque $\#G = p^a > p^{a-1}$ (car $p \geq 2$).
— Ainsi, on peut écrire $\#G = ab$ avec $1 < a, b < n$ premiers entre eux. On considère l'application $f : G \to G$ définie par $f : x \mapsto x^a$. C'est un morphisme de groupes car K est commutatif.
  — Le sous-groupe $\ker f$ est de cardinal au plus $a < n$ (car $b > 1$ et les éléments du noyau sont racines de $X^a - 1$), et les éléments de $\mathrm{im}(f)$ sont tous racines de $X^b - 1$ (car $ab = n$) donc $\#\mathrm{im}(f) \leq b < n$.
  — Puisque f est un morphisme de groupes, on a $n = ab = \#G = \#\ker f \#\mathrm{im}(f) \leq ab$ donc en fait $\#\ker f = a$ et $\#\mathrm{im}(f) = b$.
  — Par hypothèse de récurrences, les sous-groupes $\ker f$ et $\mathrm{im}(f)$ de $K^\times$ sont cycliques. Si x (resp. y) engendre $\ker f$ (resp. $\mathrm{im}(f)$) alors x (resp. y) est d'ordre a (resp. b). Ainsi x et y commutent et sont d'ordres premiers entre eux donc xy est d'ordre $ab = n$, donc G est cyclique ! (On a $(xy)^{ab} = (x^a)^b (y^b)^a = 1 \cdot 1 = 1$, et si $(xy)^k = 1$ alors $z := x^k = y^{-k} \in \langle x \rangle \cap \langle y \rangle$ donc l'ordre de z divise à la fois a et b donc divise 1, donc $x^k = 1 = y^{-k}$ donc $x^k = 1 = y^k$ donc $a \mid k$ et $b \mid k$ donc $ab \mid k$ puisque a et b sont premiers entre eux.)
— (On peut raccourcir le point précédent en utilisant le fait que les sous-groupe de Sylow de G sont tous cycliques, par hypothèse de récurrence.)

Passons maintenant au deuxième point du théorème. On vient de voir qu'il existe $x \in k^\times$ tel que $k^\times = \{x^n : n \in \mathbb{N}\}$, ainsi le morphisme d'annaux $\mathbb{F}_p[X] \to k$ donné par $X \mapsto x$ est surjectif. Le noyau est de la forme (P) avec P irréductible de degré d' (car le quotient est intègre car s'injecte dans k) et on a donc $\mathbb{F}_p[X]/(P)$ qui est isomorphe à k. Le quotient est de cardinal $p^{d'}$ donc on en déduit $d' = d$. □

Exemple. Construisons $\mathbb{F}_4$. Pour cela, il suffit de trouver un polynôme $P \in \mathbb{F}_2[X]$ irréductible de degré 2, donc sans racines (car de degré 2 ou 3). On remarque que $P = X^2 + X + 1$ convient donc $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2 + X + 1)$. Si $j \in \mathbb{F}_4$ désigne l'image de X alors $(1, j)$ est une $\mathbb{F}_2$-base de $\mathbb{F}_4$ donc $\mathbb{F}_4 = \{0, 1, j, 1 + j\}$. On remarque que $1 + j + j^2 = 0$ par définition de j, et cette égalité montre que j est un générateur de $\mathbb{F}_4^\times = \{1, j, j^2 = 1 + j\}$.

Exemple. Construisons $\mathbb{F}_{16}$. Pour cela, il suffit de trouver un polynôme $P \in \mathbb{F}_2[X]$ irréductible de degré 4. Les polynômes réductibles sont ceux avec des racines ou ceux sans racine mais qui sont produit de deux polynômes irréductibles de degré 2. On remarque qu'en fait $X^2 + X + 1$ est le seul polynôme irréductible de degré 2 sur $\mathbb{F}_2$ donc on veut juste que notre P soit sans racine et ne soit pas $(X^2 + X + 1)^2 = X^4 + X^2 + 1$. On peut donc par exemple prendre $P = X^4 + X + 1$ et alors $\mathbb{F}_{16} \simeq \mathbb{F}_2[X]/(X^4 + X + 1)$. Si $\zeta \in \mathbb{F}_{16}$ alors $(1, \zeta, \zeta^2, \zeta^3)$ est une $\mathbb{F}_2$-base de $\mathbb{F}_{16}$ et $\zeta^4 + \zeta + 1 = 0$.

Déterminons à présent un générateur de $\mathbb{F}_{16}^\times$, c'est-à-dire, déterminons un élément d'ordre $15 = 5 \times 3$. On a $\zeta, \zeta^3 \neq 1$ d'après la $\mathbb{F}_2$-base, on a $\zeta^4 = 1 + \zeta$ donc $\zeta^5 = \zeta + \zeta^2 \neq 1$ pour la même raison donc l'ordre de ζ n'est pas dans $\{1, 3, 5\}$ donc ζ est d'ordre 15 d'après le théorème de Lagrange.

Exemple. On a $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2+1)$ (le polynôme $X^2+1 \in \mathbb{F}_3[X]$ est de degré $2 \in \{2,3\}$ sans racine). Si $\alpha \in \mathbb{F}_9$ est l'image de X, alors $\alpha^2 = -1$ donc $\alpha^4 = 1$ donc α n'engendre pas $\mathbb{F}_9^\times$ (qui est de cardinal 8). En revanche, on a $(1+\alpha)^2 = 1 + 2\alpha + \alpha^2 = -\alpha$ donc $1+\alpha$ est d'ordre 8 et est donc un générateur du groupe multiplicatif.

Corollaire. *Soit $P \in \mathbb{F}_p[X]$ irréductible de degré d. Alors P divise $X^{p^n} - X$ dans $\mathbb{F}_p[X]$, en particulier P est scindé dans $\mathbb{F}_{p^n} \simeq \mathbb{F}_p[X]/(P)$.*

Démonstration. Pour le deuxième point, on sait déjà que $\mathbb{F}_{p^n}$ est un corps de décomposition sur $\mathbb{F}_p$ de $X^{p^n} - X$. Il suffit donc de montrer le premier point, c'est-à-dire que $P \mid X^{p^n} - X$. Pour cela, il suffit de montrer que $X^{p^n} - X \equiv 0$ dans $\mathbb{F}_p[X]/(P)$, donc que $X^{p^n} \equiv X \pmod P$. Mais c'est clair car l'image x de X dans $\mathbb{F}_{p^n} \simeq \mathbb{F}_p[X]/(P)$ est non nulle (car $\{1, x, \dots, x^{d-1}\}$ est une $\mathbb{F}_p$-base) donc $x \in \mathbb{F}_{p^n}^\times$ qui est d'ordre $p^n - 1$ donc $x^{p^n-1} = 1$ donc $x^{p^n} = x$ (égalité en fait vraie pour tout $x \in \mathbb{F}_{p^n}$). □

3.3 Sous-corps

Soit p un nombre premier.

Proposition. *Soit k un corps fini de cardinal p^n.*
- *Si k' est un sous-corps de k alors il existe $n' \mid n$ tel que $\#k' = p^{n'}$.*
- *Réciproquement, pour tout $n' \mid n$, il existe un* unique *sous-corps de k de cardinal $p^{n'}$.*

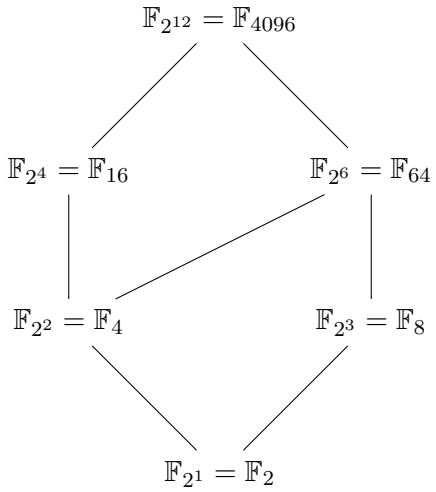
Démonstration. Si k' est un sous-corps de k alors comme au début k possède une structure de k'-espace vectoriel donc $\#k = (\#k')^d$ où $d \coloneqq \dim_{k'} k$. On sait que k' est un corps fini donc est de cardinal $p^{n'}$, et on trouve donc $p^n = (p^{n'})^d = p^{dn'}$ donc $n = dn'$ donc $n' \mid n$.

Réciproquement, si $k' \subseteq k$ est de cardinal $p^{n'}$ pour $n' \mid n$ alors tous les éléments de k' vérifient $x^{p^{n'}} = x$ donc sont tous racines de $X^{p^{n'}} - X \in k[X]$. Ce polynôme possède tous les éléments de k' comme racines, de plus il en possède au plus $p^{n'}$ donc les racines de $X^{p^{n'}} - X$ sur k sont exactement les éléments de k', ce qui prouve l'unicité. Pour l'existence, on montre que l'ensemble k' des racines de $X^{p^{n'}} - X$ dans k est un corps (on utilise le Frobenius), qui est de cardinal exactement $p^{n'}$ puisque $X^{p^{n'}} - X$ divise $X^{p^d} - X$ qui est scindé à racines simples sur k. La division provient du fait que, modulo $X^{p^{n'}} - X$, on a $X^{p^{n'}} \equiv X$ donc $(X^{p^{n'}})^{p^{n'}} \equiv X^{p^{n'}}$ donc $X^{p^{n'}p^{n'}} \equiv X^{p^{n'}}$ donc :

$$X^{p^{2n'}} \equiv X^{p^{n'}} \equiv X,$$

donc finalement en écrivant $d = dn'$ on obtient bien $X^{p^d} \equiv X$ ce qui conclut. □

Exemple. On va déterminer le treillis de sous-corps de $\mathbb{F}_{4096}$. On a $4096 = 2^{12}$. Les diviseurs de 12 sont $1, 2, 3, 4, 6, 12$ et les sous-corps sont les $\mathbb{F}_{2^n}$ correspondants. On liste les diviseurs pour chaque diviseur et ainsi de suite pour obtenir le treillis suivant (qui coïncide avec le treillis des diviseurs de 12) :



Exemple. Si q est premier alors $\mathbb{F}_{p^q}$ ne possède pas de sous-corps strict non trivial.

Proposition. *Une clôture algébrique de $\mathbb{F}_p$ est $\cup_{n\geq 0}\mathbb{F}_{p^{n!}}$.*

Démonstration. C'est bien un corps comme union croissante de corps (car $n! \mid (n+1)!$). Il reste à montrer que le corps k donné est algébriquement clos et est une extension algébrique de $\mathbb{F}_p$. Si $x \in k$ alors il existe n tel que $x \in \mathbb{F}_{p^{n!}}$ donc x est algébrique sur $\mathbb{F}_p$ (car $\mathbb{F}_{p^{n!}}/\mathbb{F}_p$ est finie de degré $n!$). Si maintenant $P \in k[X]$ est irréductible de degré d alors il existe n tel que $P \in \mathbb{F}_{p^{n!}}[X]$. On sait que P possède une racine dans $k' \coloneqq \mathbb{F}_{p^{n!}}[X]/(P)$, qui est de cardinal $(p^{n!})^n = p^{n!d}$ donc $k' \simeq \mathbb{F}_{p^{n!d}}$ est un sous-corps de $\mathbb{F}_{p^{(n!d)!}} \subseteq k$ (car $n!d \mid (n!d)!$) donc P possède une racine dans k. □