Exercice 9 *Soit E/K une extension algébrique. Alors tout $K-$morphisme $E \to E$ est un isomorphisme !*

5.2 Corps de décomposition

Soit $0 \neq P \in K[X]$. On suppose que $E \geq K$ est un corps où P est scindé : $P = c(X - x_1)...(X - x_n)$, $c \in K^\times$. On dit que $K(x_1, ..., x_n)$ est le *corps de décomposition* de P dans E.

Proposition 5.2 *Un cops de décomposition existe toujours.*

Démonstration : Par récurrence sur $\deg P$ en utilisant l'existence de corps de rupture. q.e.d.

Nous allons voir qu'il y a unicité à isomorphisme près.

Théorème 5.3 (prolongement d'isomorphisme) *Soit $\sigma : K \to K'$ un isomorphisme de corps. Soit $P \in K[X]$ un polynôme irréductible. Alors $P^\sigma \in K'[X]$ est irréductible. Si α, α' sont des racines de P et P^σ dans des extensions de K, K', alors σ se prolonge en un isomorphisme $K(\alpha) \simeq K'(\alpha')$ qui envoie α sur α'.*

Théorème 5.4 (unicité du corps de décomposition) *Soit $\sigma : K \to K'$ un isomorphisme de corps. Soit $P \in K[X]$. Soit $E \geq K$ un corps où P est scindé :$P = c(X - x_1)...(X - x_n)$. Soit $E' \geq K'$ un corps où P^σ est scindé : $P^\sigma = c'(X - x'_1)....(X - x'_n)$. Soient $B := K(x_1, ..., x_n), B' := K'(x'_1, ..., x'_n)$. Alors σ se prolonge en un isomorphisme $B \simeq B'$.*

Corollaire 5.4.1 *Soient L, L' deux corps de décomposition de P sur K. Alors il existe un $K-$isomorphisme $L \simeq L'$.*

Autre démonstration de l'unicité des corps de décomposition à isomorphisme près. Soit $P = X^n - a_1X^{n-1} + ... + (-1)^n a_n \in K[X]$. On suppose qu'il existe L_1, L_2 des corps contenant K, $x_1, .., x_n \in L_1$, $y_1, ..., y_n \in L_2$ tels que $P = (X - x_1)...(X - x_n)$ dans $L_1[X]$ et $P = (X - y_1)...(X - y_n)$ dans $L_2[X]$ et $L_1 = K(x_1, ..., x_n)$ et $L_2 = K(y_1, ..., y_n)$. Alors on a des $K-$isomorphismes :

$$L_1 \simeq L_1 \otimes_K L_2/m \simeq L_2$$

où m est un idéal maximal quelconque de $L_1 \otimes L_2$.

Sans utiliser les produits tensoriels, on peut faire ainsi :

Soit I_1 l'idéal des polynômes $P \in K[X_1, ..., X_n]$ tels que $P(x_1, ..., x_n) = 0$ dans L_1. Soit I_2 l'idéal des polynômes $P \in K[Y_1, ..., Y_n]$ tels que $P(y_1, ..., y_n) = 0$ dans L_2. Soit M un idéal maximal de l'anneau

$$K[X_1, ..., X_n, Y_1, ..., Y_n]$$

qui contient $I_1 + I_2$ (aucun problème car $1 \notin I_1 + I_2$ ‡ et car $K[X, Y]/I_1 + I_2$ est de dimension finie, il suffit donc de choisir $M \geq I_1 + I_2$ tel que $\dim_K K[X, Y]/K$ est minimal ≥ 1).

Alors $L_1 \simeq K[X]/I_1 \xrightarrow{\varphi} K[X, Y]/M$, $P \bmod I_1 \mapsto P \bmod M$ est un morphisme $K-$linéaire de corps donc injectif. Or $L = K[X, Y]/M$ est engendré par les $\overline{X_i}$ et les $\overline{Y_j}$, classes des $X_i, Y_j \bmod M$.

*Dans $L_1[X]$, on a $(X-x_1)...(X-x_n) = X^n + \sum_{k=1}^n \sigma_k(x_1, ..., x_n)(-1)^k X^{n-k} = P(X)$ Donc $\sigma_k(x_1, ..., x_n) = a_k \Rightarrow \sigma_k(X_1, ..., X_n) = a_k \bmod M$*i.e. *$\sigma_k(\overline{X_1}, ..., \overline{X_n}) = a_k$ dans L. De même, $\sigma_k(\overline{Y_1}, ..., \overline{Y_n}) = a_k$ dans L et donc*

$$\prod_i (X - \overline{X_i}) = \prod_i (X - \overline{Y_i})$$

dans $L[X]$ et donc $\{\overline{X_i} \ : \ 1 \leq i \leq n\} = \{\overline{Y_i} \ : \ 1 \leq i \leq n\}$. Or $\overline{X_i} \in \operatorname{Im} \varphi$. Donc $\overline{Y_i}$ aussi et φ est un isomorphisme. De même, on a un isomorphisme $L_2 \simeq K[X, Y]/M$. **Q.e.d.**

Exemples des corps finis : soient q une puissance d'un nombre premier p ; le corps $\mathbb{F}_q$ est un corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ et on a donc l'unicité à isomorphisme près des corps finis de cardinaux donnés. De plus $\mathbb{F}_q$ est l'ensemble des racines de $X^q - X$.

6 Corps finis

Soit K un corps fini. Sa caractéristique est un nombre premier p et son cardinal q une puissance de p. De plus si $q = p^n$, alors $(K, +) \simeq (\mathbb{Z}/p)^n$ et $(K^\times, \times) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$.

Théorème 6.1 *Soit p un nombre premier. Si $n \geq 1$, il existe, à isomorphisme près, un unique corps de cardinal $q = p^n$ c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.*

‡. en effet, si $\phi_1 : K[X_1, ..., X_n] \to K$ est une forme linéaire de noyau contenant I_1 (idem pour ϕ_2), alors on pose $\phi : K[X_1, ..., X_n, Y_1, ..., Y_n] \to K$, $cX^aY^b \to c\phi_1(X^a)\phi_2(Y^b)$. On vérifie facilement que $\phi(A(X)B(Y)) = \phi_1(A(X))\phi_2(B(Y))$ et que $I_1 + I_2$ est dans le noyau de ϕ. Si $\phi_1, \phi_2 \neq 0$, il est clair que $\phi \neq 0$ donc $I_1 + I_2 \neq k[X, Y]$ ...

Théorème 6.2 *Soit q une puissance d'un nombre premier p. Si $\mathbb{F}_q \leq K \leq \mathbb{F}_{q^n}$, alors K est de cardinal q^m où $m|n$. Réciproquement, si $m|n$, il existe un unique sous-corps K de $\mathbb{F}_{q^n}$ de cardinal q^m : c'est l'ensemble des racines de $X^{q^m} - X$ dans $\mathbb{F}_q$.*

Théorème 6.3 *Soit K un corps fini. Pour tout n, il existe une extension L/K de degré n. Cette extension est galoisienne, cyclique et unique à isomorphisme près.*

Démonstration : $K \simeq \mathbb{F}_q$ et $L \simeq \mathbb{F}_{q^n}$. q.e.d.

Remarque : si k est un corps, alors il existe une extension algébrique $\overline{k}$ de k telle que $\overline{k}$ est algébriquement clos. Ce corps $\overline{k}$ est unique à $k-$isomorphisme près. On dit que c'est une clôture algébrique de k. Pour $\mathbb{F}_p$, on a : $\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}_p} \ : \ x^{p^n} = x\}$ et $\overline{\mathbb{F}_p} = \cup_n \mathbb{F}_{p^n}$.

Dans la suite, on fixe pour tout p une clôture algébrique de $\mathbb{F}_p$: notée $\overline{\mathbb{F}_p}$ et $\mathbb{F}_{p^n} := \{x \in \overline{\mathbb{F}_p} \ : \ x^{p^n} = x\}$.

6.1 Polynômes sur les corps finis

6.1.1 Nombre de polynômes irréductibles de degré donné

Théorème 6.4 (de l'élément primitif) *Soient p un nombre premier et q une puissance de p. Pour tout $n \geq 1$, il existe $\theta \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q[\theta]$ et il existe un polynôme irréductible de degré n sur $\mathbb{F}_q$.*

Démonstration : En effet, il suffit de choisir pour θ un générateur du groupe cyclique $\mathbb{F}_{q^n}^{\times}$. q.e.d.

Lemme 6.5 *Soit $P \in \mathbb{F}_q[X]$ irréductible de degré m. Alors P divise $X^{q^n} - X$ sur $\mathbb{F}_q$ si et seulement si $m|n$.*

Démonstration : Si $m|n$, alors $q^m - 1|q^n - 1$ donc $X^{q^m-1} - 1|X^{q^n-1} - 1$ et $X^{q^m} - X|X^{q^n} - X$. Réciproquement, si $P|X^{q^n} - X$ alors si $x \in \mathbb{F}_{q^n}$ est une racine de P, on a :

$$\mathbb{F}_q \leq \mathbb{F}_q[x] \leq \mathbb{F}_{q^n}$$

donc $m = \deg P = [\mathbb{F}_q[x] : \mathbb{F}_q]$ divise $n = [\mathbb{F}_{q^n} : \mathbb{F}_q]$. Réciproquement, $m|n \Rightarrow q^m - 1|q^n - 1 \Rightarrow X^{q^m-1} - 1|X^{q^n-1} - 1 \Rightarrow X^{q^m} - X|X^{q^n} - X$. Or, si on pose $K := \mathbb{F}_q[X]/(P)$ et $x := X \bmod P$, on a $\left| \mathbb{F}_q[X]/(P) \right| = q^m \Rightarrow x^{q^m} = x \Rightarrow x^{q^m} - x = 0 \Rightarrow P|X^{q^m} - X$. q.e.d.

On a :

i)

$$X^{q^n} - X = \prod_{d|n} \prod_{P} P(X)$$

où P décrit les polynômes irréductibles unitaires sur $\mathbb{F}_q$ de degré d.

ii) $q^n = \sum_{d|n} d\nu_d(q)$; où $\nu_n(q)$ est le nombre de polynômes irréductibles sur $\mathbb{F}_q$ unitaires de degré n.

iii) $\nu_n(q) = \frac{\sum_{d|n} \mu(n/d) q^d}{n}$ où μ est la fonction de Möbius.

Rappel : si $\zeta(s) := \sum_{n\geq 1} n^{-s}$ pour $s > 1$, alors $\zeta(s)^{-1} = \sum_{n\geq 1} \mu(n) n^{-s}$ (on peut prendre cette formule comme définition de μ). Plus concrètement, on a :

$$\mu(p_1^{a_1} ... p_r^{a_r}) = \begin{cases} 0 & \text{si l'un des } a_i \geq 2, \\ (-1)^r & \text{sinon.} \end{cases}$$

Rappel : si $(G, +)$ est un groupe abélien, si $f : \mathbb{N} \to G$ est une application et si on pose $F(n) := \sum_{d|n} f(d)$, alors $f(n) = \sum_{d|n} \mu(n/d) F(d)$. En effet,

$$\begin{aligned} \sum_{d|n} \mu(n/d) F(d) &= \sum_{d|n} \mu(d) F(n/d) \\ &= \sum_{d|n,\, k|n/d} \mu(d) f(k) \\ &= \sum_{k|n,\, d|n/k} \mu(d) f(k) \\ &= \sum_{k|n} f(k) \underbrace{\sum_{d|n/k} \mu(d)}_{\substack{1 \text{ si } n/k=1 \\ 0 \text{ sinon}}} \\ &= f(n) \ . \end{aligned}$$

Exemple : dans $\mathbb{F}_3$, on a :

$$X^9 - X = X(X+1)(X+2)(X^2+X+2)(X^2+2X+2)(X^2+1)$$

et $\nu_2(3) = \frac{3^2-3}{2} = 3$.

Exercice :

Donner un sens au produit infini $\prod_P (1 - t^{\deg P})^{-1}$ où P décrit l'ensemble des polynômes irréductibles unitaires sur $\mathbb{F}_q$ et montrer que :

$$\prod_P (1 - t^{\deg P})^{-1} = (1 - qT)^{-1} \ .$$

L'égalité précédente s'écrit :

$$\prod_{n\geq 1}(1-t^n)^{-\nu_n(q)} = (1-qT)^{-1} \ .$$

Exercice : Vérifier : $\nu_n(q) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right)$. En déduire

$$\left| \{P \in \mathbb{F}_q[X] \ : \ P \text{ irréductible unitaire } \deg P \leq n\} \right| \sim \frac{q}{q-1}\frac{q^n}{n} \ .$$

6.2 Symbole de Legendre

Soit p un nombre premier impair.

Définition 9 *Si $x \in \mathbb{F}_p^\times$, alors on pose $\left(\frac{x}{p:=1}\right)$ si x est un carré et -1 sinon.*

Proposition 6.6 $\left(\frac{x^{\frac{p-1}{2}} = x}{p \bmod p}\right)$. *en particulier, $\mathbb{F}_p^\times \to \{\pm 1\}$, $\left(\frac{x\mapsto x}{p}\right)$ est un morphisme de groupes de noyau l'ensemble des carrés de $\mathbb{F}_p^\times$.*

Exercice 10 *En déduire que le polynôme X^4+1 est réductible* $\bmod p$ *pour tout p premier. Solution : si $p=2$, alors $X^4+1=(X+1)^4$ et si p est impair, on a :*

$$\left(\frac{-1}{p}\right)\left(\frac{-2}{p}\right)\left(\frac{2}{p}\right) = 1$$

donc $-1, -2$ ou 2 est un carré $\bmod p$. *Si $-1 = x^2$, alors $X^4+1 = (X^2 - x)(X^2+x)$ et si 2 (ou -2) $= x^2$, alors $X^4+1 = (X^2-xX+1)(X^2+xX+1)$ ...*

Démonstration : Le morphisme $x \mapsto x^2$ a pour noyau $\{\pm 1 \bmod p\}$ de cardinal 2 et tout $x = y^2$ vérifie $x^{(p-1)/2} = y^{p-1} = 1$. Cela donne $(p-1)/2$ solutions et donc on les a toutes ... *q.e.d.*

Théorème 6.7 (Loi de réciprocité quadratique) *(i)* $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} =$ 1 *si* $p = 1 \bmod 4$, -1 *si* $p = -1 \bmod 4$.

(ii) si p, q sont des nombres premiers impairs, alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \ .$$

(iii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1$ *si* $p = \pm 1 \bmod 8$, -1 *si* $p = \pm 3 \bmod 8$.

Exemple : 5 est un carré $\bmod 5 \Leftrightarrow p$ est un carré $\bmod 5$.

Démonstration : Admettons (ii) et démontrons (iii). On introduit le symbole de Jacobi : Si m, n sont des nombres impairs premiers entre eux, avec $n > 0$, on pose $\binom{m}{n} = \prod_i \binom{m}{p_i}^{\alpha_i}$ où $n = \prod_i p_i^{\alpha_i}$ est la décomposition de n en produit de nombre premiers. On vérifie que $\binom{m}{n}\binom{n}{m} = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$ et que $\binom{-1}{n} = (-1)^{\frac{n-1}{2}}$ et que $\binom{m}{n}$ ne dépend que de la classe de $m \bmod n$. Attention on peut avoir $\binom{m}{n=1}$ sans que m soit un carré $\bmod m$. Par exemple $\binom{2}{9} = 1$ mais 2 n'est pas un carré $\bmod 9$.

On a :

$$\binom{2}{p} = (-1)^{\frac{p-1}{2}}\binom{-2}{p} == (-1)^{\frac{p-1}{2}}\binom{p-2}{p}$$

et maintenant $p-2$ et p sont impairs et l'un des 2 est $1 \bmod 4$! Donc :

$$\binom{2}{p} = (-1)^{\frac{p-1}{2}}\binom{p}{p-2} = (-1)^{\frac{p-1}{2}}\binom{2}{p-2}$$

$$= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-3}{2}}...(-1)^1 1$$

$$= (-1)^{1+...+\frac{p-1}{2}}$$

$$= (-1)^{\frac{p^2-1}{8}} \ .$$

<u>*q.e.d.*</u>

7 Résultant

Définition 10 *Soient* $P := a_0X^p + ... + a_p, Q := b_0X^q + ... + b_q \in A[X]$ *où* A *est un anneau.*

$$\left.\begin{matrix}q \text{ lignes}\\ \\ \\ \\ \\ p \text{ lignes}\\ \\ \\ \\ \\ \end{matrix}\right\{\left(\begin{matrix} a_0 & a_1 & ... & a_p & & \\ & a_0 & a_1 & ... & a_p & \\ & & \ddots & \ddots & & \ddots \\ b_0 & b_1 & ... & b_q & & \\ & b_0 & b_1 & ... & b_q & \\ & & \ddots & \ddots & & \ddots \end{matrix}\right)$$

Soit $\mathrm{Res}_{p,q}(P, Q)$ *le déterminant de la matrice :*

Le coefficient (i, j) *de la matrice est :* a_{j-i} *si* $1 \leq i \leq q$ *et* b_{j-i+q} *si* $q + 1 \leq i \leq p + q$ *(où l'on convient que* $a_n = 0$ *si* $n < 0$.

Remarques :

1. si $a_0 = b_0 = 0$, alors $\mathrm{Res}_{p,q} = 0$; si $\phi : A \to B$ est un morphisme d'anneaux, alors $\phi(\mathrm{Res}_{p,q}(P,Q)) = \mathrm{Res}_{p,q}(P^\phi, Q^\phi)$; $\mathrm{Res}_{p,q}(P,Q) = a_p^q b_o^p + (-1)^{(q-1)p} a_0^q b_q^p +$ des termes de degrés $< p$ en b_0 et $< q$ en a_0 (car, par exemple, la diagonale est $(\underbrace{a_0, ..., a_0}_{q}, \underbrace{b_0, ..., b_0}_{p})$).
2. $\mathrm{Res}_{p,q}(P,Q)$ est homogène de degré q en $a_0, ..., a_p$ et de degré p en $b_0, ..., b_q$.

Exemples : $\mathrm{Res}(f, f') = 4p^3 + 27q^2$ si $f = X^3 + pX + q$, $-a(b^2 - 4ac)$ si $f = ax^2 + bx + c$.

Proposition 7.1 *Si $P, Q \in K[X]$ sont de degrés respectifs p, q, alors $\mathrm{Res}_{p,q}(P,Q) = 0 \Leftrightarrow P, Q$ ont un facteur commun ($\Leftrightarrow$ ont une racine commune dans une certaine extension de K).*

Démonstration : P, Q ont un facteur en commun si et seulement si $PQ_1 = QP_1$ pour un $P_1 = \alpha_1 X^{p-1} + ... + \alpha_p \in K[X]$ de degré $< \deg P$ et un $Q_1 = \beta_1 X^{q-1} + ... + \beta_q$ de degré $< \deg Q$ avec $(P_1, Q_1) \neq (0;0)$ (en fait $P_1 = 0 \Rightarrow Q_1 = 0$).

Or $PQ_1 = P_1 Q \Leftrightarrow (\beta_1, ..., \beta_q, -\alpha_1, ..., -\alpha_p).S = 0$. Donc il existe un facteur commun si et seulement si S est non inversible ... q.e.d.

Théorème 7.2 *Si $P = a_0(X - x_1)...(X - x_p)$ et $Q = b_0(X - y_1)...(X - y_q)$, alors*

$$\mathrm{Res}(P,Q) = a_0^q b_0^p \prod_{i=1,j=1}^{i=p,j=q} (x_i - y_j) = a_0^q \prod_{i=1}^{p} Q(x_i) = (-1)^{pq} b_0^p \prod_{j=1}^{q} P(y_j) \ .$$

Démonstration : Raisonnons dans l'anneau des polynômes $\mathbb{Z}[a_0, b_0, x_1, ..., x_p, y_1, ...y_q]$ en $pq+2$ variables. Alors $P = a_0 X^p - a_0\sigma_1(x_1, ..., x_p) + ... + (-1)^p a_0 \sigma_p(x_1, ..., x_p))$ et $Q = b_0 X^q - b_0\sigma_1(x_1, ..., x_q) + ... + (-1)^q b_0 \sigma_q(x_1, ..., x_q))$. Donc $\mathrm{Res}(P,Q) = a_0^q b_0^p R(x_1, ..., x_p, y_1, ..., y_q)$ un polynôme homogène de degré q en les x_i et p en les y_j (car les σ_k sont de degré 1 en chaque x_i).

Or, dans l'anneau $\mathbb{Z}[a_0, b_0, x_1, ..., x_p, y_1, ...y_q]$, si on remplace x_i par y_j, on trouve $R(x_1, ..., \overset{\not{x_i}}{y_j}, ..., y_1, ..., y_q) = 0$ car il ya un facteur commun : $x - y_j$. Or, pour tout polynôme

$$F(x_1, ..., x_p, y_1, ..., y_q) = F(x_1, ..., \overset{\not{x_i}}{y_j}, ..., y_1, ..., y_q) \bmod x_i - y_j$$

dans $\mathbb{Z}[x_1, ..., x_p, y_1, ...y_q]$. Donc pour tous i, j, $x_i - y_j | R$ dans $\mathbb{Z}[x_1, ..., x_p, y_1, ...y_q]$. Comme ce dernier anneau est factoriel, $S = \prod_{i=1,j=1}^{i=p,j=q}(x_i - y_j)$ divise R dans $\mathbb{Z}[x_1, ..., x_p, y_1, ...y_q]$.

Or en chaque x_i, $\deg_{x_i} R \leq q$ et $\deg_{x_i} S = q$ et en chaque y_j, $\deg_{y_j} R \leq p$ et $\deg_{y_j} S = p$ donc

$$\mathrm{Res}(P, Q) = a_0^q b_0^p S\lambda$$

où $\lambda \in \mathbb{Z}$. Pour l'ordre lexicographique en les y_j, le terme dominant dans $\mathrm{Res}(P, Q)$ est $(-1)^{pq} a_0^q b_0^p (y_1...y_q)^p$. Pour l'ordre lexicographique en les y_j, le terme dominant dans $a_0^q b_0^p S$ est aussi $(-1)^{pq} a_0^q b_0^p (y_1...y_q)^p$. Donc $\lambda = 1$.

q.e.d.

Corollaire 7.2.1 $\mathrm{Res}_{p,q}(P, Q) = (-1)^{pq}\mathrm{Res}_{p,q}(Q, P)$.

Définition 11 *Si $f = a_0x^n + ... + a_n \in K[X]$, on pose $D(f) = a_0^{2n-2} \prod_{1 \leq i < j \leq n}(x_i - x_j)^2$ où $f = a_0(X - x_1)...(X - x_n)$ dans une certaine extension de K. C'est un élément de l'anneau $\mathbb{Z}[a_0, ..., a_n]$*

Exercice 11 *Vérifier que* $\mathrm{Res}_{n,n-1}(f, f') = (-1)^{n(n-1)/2} a_0 D(f)$.

7.1 Application du résultant : loi de réciprocité quadratique

Exercice 12 *Pour tout $k \geq 1$, il existe un polynôme $P \in \mathbb{Z}[X]$ tel que $X^k + \frac{1}{X^k} = P\left(X + \frac{1}{X}\right)$.*

Soit p un nombre premier impair.
On pose $T_p \in \mathbb{Z}[X]$ unitaire de degré $\frac{p-1}{2}$ tel que :

$$X^{(p-1)/2} T_p\left(X + \frac{1}{X}\right) = 1 + ... + X^{p-1} \ .$$

Exercice 13 $T_p(0) = (-1)^{(p-1)/2}$

Proposition 7.3 *Si $p \neq q$ sont premiers impairs, alors :*

i) $\mathrm{Res}(T_p, T_q) = \pm 1$ *dans* $\mathbb{Z}$ *;*

ii) $\mathrm{Res}(T_p, T_q) = \left(\frac{q}{p}\right) \bmod p$.

Démonstration :

i) On a $\mathrm{Res}(T_p, T_q) \in \mathbb{Z}$. Si $r$est un nombre premier qui divise $\mathrm{Res}(T_p, T_q)$, alors T_p et T_q ont une racine commune dans une extension de $\mathbb{F}_r$. Notons cette racine y. Comme $y \neq 0$, on peut trouver une racine x de $x+1/x = y$. Alors $1 + ... + x^{p-1} = 0 = 1 + ... + x^{q-1}$. Donc $x^p = x^q = 1$ et $x = 1$ *absurde.*
Or dans $\mathbb{F}_p$, $T_p(Y) = (Y-2)^{(p-1)/2}$. Donc $\mathrm{Res}(T_p, T_q) = (-1)^{(p-1)(q-1)/4} T_q(2)^{(p-1)/2} = q^{(p-1)/2} = \left(\frac{q}{p}\right) \bmod p$ ...

q.e.d.

Corollaire 7.3.1 $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Démonstration : En effet, $\mathrm{Res}(T_p, T_q) = (-1)^{\frac{(p-1)(q-1)}{4}} \mathrm{Res}(T_q, T_p)$. *q.e.d.*

8 Corps algébriquement clos

Définition 12 *On dit qu'un corps K est algébriquement clos si tout polynôme non constant est scindé sur K.*

Théorème 8.1 *Soit K un corps. Il existe une extension algébrique $\overline{K}$ de K qui est un corps algébriquement clos. C'est une clôture algébrique de K. L'extension $\overline{K}$ est unique à $K-$isomorphisme près.*

Démonstration :
Existence : soit $\mathscr{P}$ l'ensemble des polynômes irréductibles unitaires de $K[X]$. Pour tout $p \in \mathscr{P}$, on choisit une variable X_p. Soit $A := K[X_p : p \in \mathscr{P}]$. Soit I l'idéal de A engendré par les polynômes $p(X_p)$, $p \in \mathscr{P}$. Alors I est propre donc contenu dans un idéal maximal M. Le corps A/M est une extension algébrique de K et tout polynôme p irréductible sur K a une racine $(X_p \bmod M)$ dans A/M. Cela suffit pour dire que A/M est algébriquement clos (comme nous le verrons plus tard) ...
Unicité : on utilise le lemme de Zorn ... *q.e.d.*

Exemples : $\mathbb{C}$ (*respectivement* $\overline{\mathbb{Q}}$ (*respectivement* $\cup_{n\geq 1}\mathbb{C}((t^{1/n}))$)) est une clôture algébrique de $\mathbb{R}$ (*respectivement* de $\mathbb{Q}$ (*respectivement* de $\mathbb{C}((t))$)).

9 Éléments primitifs

Soit E/K une extension.
On dit que $x \in E$ est un élément *primitif* de E/K si $E = K(x)$.

Théorème 9.1 *Si $x, y \in E$ sont algébriques sur K, si y est séparable sur K, alors il existe $z \in E$ tel que $E = K(z)$. En particulier, si K est parfait, toutes ses extensions finies sont primitives.*

Démonstration : Si K est fini, alors $K(x,y)$ aussi donc $K(x,y)^\times$ est cyclique et il suffit de prendre pour z un générateur du groupe $K(x,y)^\times$!
Si K est infini : notons P_x, P_y les polynômes minimaux de x et y sur K. Notons y_j les racines distinctes de P_y et x_i celles de P_x (dans une extension). Soit $0 \neq t \in K$ tel que les $x_i + ty_j$ soient deux à deux distincts (il suffit que $t \in K \setminus \{\frac{x_{i'}-x_i}{y_j-y_{j'}} : i, i', j, j', y_j \neq y_{j'}\}$. Posons $z := x + ty$. Alors $P_x(z - tY) \in K(z)[Y]$ a une seule racine en commun avec $P_y(Y) : y$. Donc le pgcd de $P_x(z-tY)$ et P_y est $Y - y$. Or, $P_y, P_x(z-tY) \in K(z)[Y]$ donc $Y - y \in K(z)[Y] \Rightarrow y \in K(z) \Rightarrow x, y \in K(z) \Rightarrow K(z) = K(x,y)$. *q.e.d.*

Exercice : si E/K est finie, alors E/K admet un élément primitif si et seulement s'il existe un nombre fini de corps $K \leq L \leq E$.

Contre-exemple : si $K := \mathbb{F}_p(X^p, Y^p)$, $E := \mathbb{F}_p(X, Y)$, alors les corps $K(X + tY)$, $t \in K$ sont deux à deux distincts.

Théorème 9.2 *Soit E/K une extension algébrique telle que tout polynôme irréductible $P \in K[X]$ a une racine dans E. Alors E est algébriquement clos.*

Démonstration :

1er cas : K est parfait.

Soit $P \in E[X]$ irréductible. Soit E_1 une extension où P est scindé : $P = (X - x_1)...(X - x_n)$. Les x_i sont algébriques sur K. il existe $a \in E_1$ tel que $K(x_1, ..., x_n) = K(a)$. Soit Q le polynôme minimal de a sur K. Alors Q a une racine b dans E. une racine de P dans une extension de E. Alors, x est algébrique sur K. Soit K_1 un corps de décomposition de $\pi_{x,K}$ sur K.

2ème cas

Posons $K' = \{x \in E : {}^{\exists}n,\ x^{p^n} \in K\}$. Alors $K' = K'^p$. Et tout polynôme irréductible sur K' a une racine dans E. *(en effet, si $x \in K'$, alors il existe n tel que $x^{p^n} \in K$; le polynôme $T^{p^{n+1}} - x^{p^n}$ a une racine dans E disons y. Alors $y \in K'$ et $y^p = x$).*

q.e.d.

9.1 Corps parfaits

Définition 13 *Si K est un corps de caractéristique nulle ou si K est un corps de caractéristique $p > 0$ vérifiant $K^p = K$, on dit que K est un corps parfait.*

Exercice 14 *si K est un corps parfait, alors tout polynôme irréductible est premier avec son polynôme dérivé.*

10 Un peu de théorie de Galois

10.1 Morphismes de corps

Exercice 15

$$\mathrm{Aut}(\mathbb{R}) = 1,$$

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \{\mathrm{Id}, a+b\sqrt{2} \mapsto a-b\sqrt{2}\},$$

$$\mathrm{Aut}\mathbb{C}(t) \simeq \mathrm{PGL}_2(\mathbb{C}),$$

$$\mathrm{Aut}\mathbb{Q}(\sqrt[3]{2}) = 1\,,$$

$$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, j) \simeq \mathfrak{S}_3\ .$$

10.2 Lemme d'Artin

Théorème 10.1 *Soient K, L des corps et $\sigma_1, ..., \sigma_n : K \to L$ des morphismes de corps deux à deux distincts. Alors les σ_i sont $L-$linéairement indépendants dans le $L-$espace vectoriel des fonctions $K \to L$.*

Définition 14 *Une extension (finie) galoisienne est une extension de la forme K/K^G où K un corps et $G \leq \mathrm{Aut}K$ un sous-groupe fini.*

Exemples : $\mathbb{F}_{q^n}/\mathbb{F}_q$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $Q(sqrt[3]2, j)/\mathbb{Q}$, $\mathbb{C}(t)/\mathbb{C}(t+t^{-1})$ sont galoisiennes.

Contre-exemples : $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathbb{F}_p(X)/\mathbb{F}_p(X^p)$.

10.3 Extensions résolubles

10.4 Nombres constructibles à la règle et au compas

11 Théorème de Lüroth

11.1 Sous-groupes finis de $\mathbf{PGL_2}(\mathbb{C})$

12 Un peu de théorie de Galois

12.1 Théorème d'indépendance des caractères d'Artin

Si G est un groupe et K un corps, un caractère de G dans K est un morphisme de groupes $G \to K^\times$. L'ensemble des caractères est une partie du $K-$espace vectoriel des fonctions $G \to K$.

Exemple : $G = \mathbb{Z}/n\mathbb{Z}$, $K = \mathbb{C}$, les caractères de G dans $\mathbb{C}$ sont les $k \mapsto \zeta^k$ où $\zeta = \exp(2i\pi/n)$.

12.2 Indépendance

Théorème 12.1 (Artin) *Soient $\sigma_1, ..., \sigma_n$ n caractères distincts de G dans K. Alors les σ_i sont $K-$linéairement indépendants.*

Corollaire 12.1.1 *Soient E, E' deux corps. Si $\sigma_1, ..., \sigma_n$ sont n morphismes distincts de corps $E \to E'$. Alors les σ_i sont $E'-$linéairement indépendants.*

Exercice : si G abélien, on pose $G^\vee$ le groupe des caractères de G dans $\mathbb{C}$. Montrer que $G^\vee \simeq G$ *(non canonique).*

Exercice : si G fini, $|\mathrm{Hom}(G, K^\times)| \leq |G|$.

12.3 Corps des invariants

Théorème 12.2 *Soient $\sigma_1, ..., \sigma_m$ m morphismes distincts $E \to E'$. Alors si $F := E^{\{\sigma_1,...,\sigma_m\}} := \{x \in E \ : \ \sigma_1(x) = ... = \sigma_n(x)\}$, $[E : F] \geq m$.*

Démonstration : Si $e_1, ..., e_n$ est une famille génératrice de E comme $F-$espace vectoriel, alors les lignes de la matrice $(\sigma_i(e_j))_{\substack{1\leq i\leq m \\ 1\leq j\leq n}} \in \mathscr{M}_{m,n}(E')$ sont indépendantes. Donc $m \leq n$. *q.e.d.*

Corollaire 12.2.1 *Si G est un sous-groupe fini de $\mathrm{Aut}(E)$, alors $[E : E^G] \geq |G|$.*

Remarque : comme G contient l'identité, $E^G = \{x \in E \ : \ ^\forall g \in G, \ g(x) = x\}$.

Exemple : $E = \mathbb{C}$, $G = \{1, \sigma\}$ où σ est la conjugaison complexe, $[\mathbb{C} : \mathbb{R}] = 2$.

12.4 Extensions galoisiennes

Définition 15 *Soit E un corps. Soit $G \leq \mathrm{Aut}(E)$ fini. On dit que E/E^G est une extension galoisienne de groupe de Galois G.*

Exemples : $\mathbb{C}/\mathbb{R}$, $\mathbb{F}_{q^n}/\mathbb{F}_q$, $\mathbb{Q}(\zeta)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{C}(X)/\mathbb{C}(X^3)$; *contre-exemple :* $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathbb{F}_p(X)/\mathbb{F}_p(X^p)$, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$.

Exemple : $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$.

Théorème 12.3 *Soit E un corps. Soit $G \leq \mathrm{Aut}(E)$ un groupe fini. Alors $[E : E^G] = |G|$.*

Démonstration : On utilise la forme $F-$linéaire Tr : $E \to F$, $x \mapsto \sigma_1(x) + ... + \sigma_n(x)$ où $F = E^G$, $G = \{\sigma_1, ..., \sigma_n\}$. Soient $g_1, ..., g_n$ les éléments de G. Si $e_1, ..., e_{n+1}$ sont des éléments de E, alors les colonnes de la matrices $(g_i(e_j))_{\substack{1\leq i\leq n \\ 1\leq j\leq n+1}} \in \mathscr{M}_{n,n+1}$ sont liées. Donc $^\forall i$, $\sum_j x_j g_i(e_j) = 0$ pour certains $x_j \in E$. D'où :

$$^\forall i, \sum_j g_i^{-1}(x_j)e_j = 0$$

et $\sum_i \sum_j g_i^{-1}(x_j)e_j = 0 \Rightarrow \sum_j \mathrm{Tr}(x_j)e_j = 0$. C'est encore vrai si on remplace x_j par xx_j, $x \in E$. Donc on peut choisir les x_j tels que $x_1 \in E$ et $\mathrm{Tr}(x_1) \neq 0$ par exemple. Mais alors, les e_j sont liés sur E^G. *q.e.d.*

Exemples :

a) $k(x_1, ..., x_n)^{\mathfrak{S}_n} = k(s_1, ..., s_n)$ (où k est un corps et où les s_i sont les polynômes symétriques élémentaires) car $k(x_1, ..., x_n) \geq k(x_1, ..., x_n)^{\mathfrak{S}_n} \geq k(s_1, ..., s_n)$ et $[k(x_1, ..., x_n) : k(x_1, ..., x_n)^{\mathfrak{S}_n}] = |\mathfrak{S}_n| = n! \geq [k(x_1, ..., x_n) : k(s_1, ..., s_n)]$,

b) $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est galoisienne de groupe de Galois $G := \langle s, t\rangle \simeq \mathfrak{S}_3$ où s est le $\mathbb{Q}(j)-$automorphisme qui envoie $\sqrt[3]{2}$ sur $j\sqrt[3]{2}$ et t le $\mathbb{Q}(\sqrt[3]{2})-$automorphisme qui envoie j sur j^2 ;

c) soit G le sous-groupe des automorphismes de $\mathbb{C}(t)$ engendré par les changements de variables $t \mapsto t^{-1}$ et $t \mapsto 1 - t$. On vérifie que G est d'ordre 6, isomorphe à $\mathfrak{S}_3$.

Soit K le sous-corps des fractions rationnelles $f \in \mathbb{C}(t)$ invariantes par les changements de variables

$$t \mapsto 1 - t \text{ et } t \mapsto t^{-1} \ .$$

Montrer que $K = \mathbb{C}\left(\frac{(t^2-t+1)^3}{t^2(t-1)^2}\right)$.

En déduire que l'extension :

$$\mathbb{C}\left(\frac{(t^2 - t + 1)^3}{t^2(t - 1)^2}\right) \subset \mathbb{C}(t)$$

est galoisienne de groupe de Galois S_3.

Exercice : on pose $y_1 := x_1 + jx_2 + j^2x_3$, $y_2 := x_1 + j^2x_2 + jx_3$. Montrer que $\mathbb{C}(x_1, x_2, x_3)^{\mathfrak{A}_3} = \mathbb{C}(y_1^2/y_2, y_2^2/y_1, \sigma_1)$.

On peut retrouver les polynômes symétriques à partir des fractions rationnelles symétriques ...

Exercice On pose $L := k(s_1, ..., s_n)$ et $L_i := L(x_{i+1}, ..., x_n)$, $0 \leq i \leq n$ ($L_n = L$).

a) $[L_{i-1} : L_i] = i$ et $1, ..., x_i^{i-1}$ est une base de L_{i-1}/L_i.

b) $\{x_1^{a_1}...x_n^{a_n} \ : \ ^\forall i,\ a_i \leq i-1\}$ est une base de $k(x_1, ..., x_n)/L$.

c) tout $g \in k[x_1, ..., x_n]$ est une combinaison $k[s_1, ..., s_n]-$linéaire de monômes $x_1^{a_1}...x_n^{a_n} \ : \ ^\forall i,\ a_i \leq i-1$.

d) On retrouve que $k[x_1, ..., x_n]^{\mathfrak{S}_n} = k[s_1, ..., s_n]$.

Corollaire 12.3.1 (Maximalité du groupe de Galois) *Soit E/F galoisienne de groupe G. Alors si $E' \geq E$ et si $\sigma : E \to E'$ est un $F-$morphisme de corps, $\sigma \in G$. En particulier, $G = \mathrm{Aut}_F(E)$, groupe des automorphismes $F-$linéaires de E.*

Notation : si $F = E^G$, $G =: \mathrm{Gal}(E/F)$.

12.5 Injectivité

Corollaire 12.3.2 (Injectivité) *Si E/F est galoisienne de groupe G si $H_1, H_2 \leq G$, alors $E^{H_1} = E^{H_2} \Leftrightarrow H_1 = H_2$.*

12.6 Surjectivité

Théorème 12.4 *Soit E/F une extension galoisienne de groupe de Galois G. Si $F \leq B \leq E$, alors il existe $H \leq G$ tel que $E^H = B$.*

Démonstration : Soit $H := \mathrm{Aut}_B(E)$. On a : $B \leq E^H$. Soit $s_1, ..., s_r$ un système de représentants de G/H. On a $B^{\{s_1,...,s_r\}} = F$ donc $[B : F] \geq r$ et $[E : B] \leq [E : F]/r = |H| = [E : E^H]$ d'où $B = E^H$. q.e.d.

Exercice : donner la liste des sous-corps de $\mathbb{Q}(\sqrt[3]{2}, j)$.
(*réponse :* $\mathbb{Q}(\sqrt[3]{2}, j) \geq \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(j\sqrt[3]{2}), \mathbb{Q}(j^2\sqrt[3]{2}), \mathbb{Q}(j) \geq \mathbb{Q}$).

12.7 Correspondance de Galois

Théorème 12.5 (fondamental) *Soit E/F une extension galoisienne de groupe G.*

i) On a 2 bijections réciproques :

$$\{H \leq G\} \overset{1:1}{\longleftrightarrow} \{F \leq B \leq E\}$$

$$H \mapsto E^H$$

$$\mathrm{Gal}(E/B) \leftarrow B \ .$$

ii) *L'extension E/B est galoisienne et $[E : B] = |\mathrm{Gal}(E/B)|$;*

iii) $[B : F] = |G/\mathrm{Gal}(E/B)|$;

iv) *l'extension B/F est galoisienne si et seulement si $\mathrm{Gal}(E/B) \triangleleft G$. Dans ce cas, $\mathrm{Gal}(B/F) \simeq G/\mathrm{Gal}(E/B)$.*

Démonstration : Si $\mathrm{Gal}(E/B) \triangleleft G$, si $\sigma \in G$, alors $\sigma(B) = B$: en effet, $\mathrm{Gal}(E/\sigma(B)) = \sigma\mathrm{Gal}(E/B)\sigma^{-1} = \mathrm{Gal}(E/B) \Rightarrow \sigma(B) = B$. Notons G' l'image du morphisme $\sigma \mapsto \sigma|_B$. On a : $B^{G'} = F$. Réciproquement si B/F est galoisienne, alors pour tout $\sigma \in G$, $\sigma|_B \in \mathrm{Gal}(B/F)$ (*cf.* le corollaire 12.3.1). On a alors $\mathrm{Gal}(E/B) = \ker(G \to \mathrm{Gal}(B/F)\,,\, \sigma \mapsto \sigma|_B)$ qui est un noyau donc distingué. *q.e.d.*

Proposition 12.6 *Soit E/K une extension galoisienne. On suppose que $K \leq B \leq B' \leq E$. On note $U := \mathrm{Gal}(E/B)$, $U' := \mathrm{Gal}E/B'$. Alors B'/B est galoisienne $\Leftrightarrow U' \triangleleft U$. Et dans ce cas, $\mathrm{Gal}(B'/B) \simeq U/U'$.*

Exercice : démontrer cette proposition.

12.8 Caractérisation des extensions galoisiennes

Théorème 12.7 *Soit E/K une extension finie. On a toujours : $|\mathrm{Aut}_K(E)| \leq [E : K]$. L'extension E/K est galoisienne $\Leftrightarrow |\mathrm{Aut}_K(E)| = [E : K]$. Dans ce cas, $\mathrm{Gal}(E/K) = \mathrm{Aut}(E/K)$.*

Contre-exemples :

a) si $E = \mathbb{Q}(\sqrt[4]{2})$, alors $|\mathrm{Aut}(E/\mathbb{Q})| = 2 < 4 = [E : \mathbb{Q}]$.

b) si p est premier et $E = \mathbb{F}_p(T)$ et $K = \mathbb{F}_p(T^p)$; alors $[\mathbb{F}_p(T) : \mathbb{F}_p(T^p)] = p$ mais $\mathrm{Aut}_{\mathbb{F}_p(T^p)}(\mathbb{F}_p(T)) = \{\mathrm{Id}\}$.

13 Éléments entiers sur un anneau

Définition 16 *Soit B un anneau commutatif avec unité. Soit $A \subseteq B$ un sous-anneau (sous-entendu qui contient 1). Si $b \in B$, sont équivalentes :*

(i) *il existe $P \in A[X]$ unitaire tel que $P(b) = 0$;*

(ii) *$A[b]$ est un $A-$module de type fini ;*

(iii) *il existe un $A[b]-$module fidèle qui est un $A-$module de type fini.*

Un b qui vérifie ces propriétés est dit entier sur A.

Exemple : $\sqrt{2}$ est entier sur $\mathbb{Z}$.

Exercice 16 *Si $z \in \mathbb{Q}$ est entier sur $\mathbb{Z}$, alors $z \in \mathbb{Z}$.*

Démonstration : iii $\Rightarrow$ *i* : soit M un $A[b]-$module fidèle qui est un $A-$module de type fini. Soient $e_1, ..., e_n$ des générateurs. Il existe des coefficients $a_{i,j} \in A$ tels que :

$$^{\forall} j,\ be_j = \sum_i a_{i,j} e_j \ .$$

On en déduit par récurrence sur n que $^{\forall} j\ b^n e_j = \sum_i (M^n)_{i,j} e_i$ où $M := (a_{i,j})$. Mais alors, $\chi_M(b)e_j = \sum_i \chi_M(M)_{i,j} e_i = 0$ pour tout j. Donc $\chi_M(b)M = 0 \Rightarrow \chi_M(b) = 0$ car M est fidèle. Or, $\chi_M(X)$ est unitaire à coefficients dans A. q.e.d.

Corollaire 13.0.1 *L'ensemble des éléments de B entiers sur A est un sous-anneau de A*

Exercice 17 *Soit $z \in \mathbb{C}$ une racine de l'unité. Alors $\mathbb{Q} \cap \mathbb{Z}[z] = \mathbb{Z}$. On dit que $\mathbb{Z}$ est intégralement clos (sous-entendu dans son corps des fractions). Contre-exemple : $\mathbb{Z}[i\sqrt{5}]$ est intégralement clos non factoriel car $6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ et $2, 3, 1 \pm i\sqrt{5}$ sont des irréductibles dans $\mathbb{Z}[i\sqrt{5}]$ deux à deux non associés ...*

Application : irréductibilité des polynômes cyclotomiques :

13.1 Polynômes cyclotomiques

Définition 17 *Soit $n \geq 1$. On pose $\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} (X - e^{2ik\pi/n}) \in \mathbb{C}[X]$.*

Théorème 13.1 *a) Pour tout n, $X^n - 1 = \prod_{d|n} \Phi_d(X)$.*

b) Pour tout n, $\Phi_n \in \mathbb{Z}[X]$.

c) Pour tout n, Φ_n est irréductible sur $\mathbb{Q}$.

Remarque : en particulier $\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$.
Démonstration :

c)

Soit ζ une racine primitive $n-$ième de l'unité. Soit $P \in \mathbb{Q}[X]$ son polynôme minimal sur $\mathbb{Q}$. Soit p un nombre premier qui ne divise pas n. Alors $P \in \mathbb{Z}[X]$ donc $P(X^p) = P(X)^p \bmod p$. En particulier, dans l'anneau $\mathbb{Z}[\zeta]$, on a $P(\zeta^p) = 0 \bmod p$.