Magistère de mathématiques (l'ENS de Lyon) 2004/2005, 2e semestre "Algèbre 2" Jeudi de 10h15 à 12h15, Amphi A à partir du 20 janvier 2005

A. A. Pantchichkine

Institut Fourier, B.P.74, 38402 St.–Martin d'Hères, FRANCE
e-mail : panchish@mozart.ujf-grenoble.fr, FAX : 33 (0) 4 76 51 44 78

Résumé

Le présent cours est centré sur les corps et la théorie de Galois. Il est considéré comme la suite du cours "Algèbre1" de Prof. G.Tomanov, et on utilise comme prérequis les notions de groupe, d'homomorphisme, d'actions des groupes sur un ensemble, ainsi que des généralités sur les anneaux factoriels, la classification des modules de type fini sur les anneaux principaux, et en particulier, la structure des groupes abéliens de type fini.

La théorie de Galois donne un lien entre le problème de solution d'une équation algébrique d'une indéterminée à coefficients dans un corps commutatif K, et le problème de la détermination d'un groupe (dit "le groupe de Galois d'un polynôme") qui opère sur l'ensemble des racines du polynôme correspondant, et cette action est donnée par automorphismes de certaines extensions du corps K.

Les corps finis donnent des exemples importants d'extensions galoisiennes, et on étudie en détail les polynômes irréductibles sur les corps finis et la méthode de factorisation de Berlekamp.

D'autres exemples proviennent des extensions cyclotomiques, extensions cycliques et extensions de Kummer, obtenue par adjonction de radicaux aux extension cyclotomiques

Dans la dernière partie on montre que la résolubilité par radicaux d'un équation algébrique sur un corps de caractéristique nulle est équivalente à la résolubilité du groupe de Galois de l'extension des corps correspondante. Si le temps le permet, on donne une introduction à la théorie d'Artin-Schreier, qui fournit un analogue de la théorie de Kummer dans le cas de la caractéristique positive, et les premières notions de la cohomologie galoisienne en exemples.

Des applications de la théorie de Galois dans la théorie des nombres sont indiquées dans le cours (le théorème de Kronecker-Weber, sommes de Gauss, etc.) On donne des exemples numériques avec des logiciels (Maple, PARI).

Je remercie vivement Brice Boyer, Jérémy Larochette et François Japiot (l'ENS de Lyon) pour les corrections !

Certificat "Algèbre 2"

1. Extensions finies et extensions algébriques d'un corps commutatif
2. Corps de rupture et corps de décomposition d'un polynôme. Prolongement d'un isomorphisme des corps
3. Caractères d'un groupe, le théorème d'Artin sur l'indépendance linéaire des caractères
4. Extensions galoisiennes, exemples, le théorème d'injectivité
5. Correspondance de Galois
6. Extensions séparables et extensions normales
7. Exemple : structure des corps finis
8. Polynômes irréductibles sur les corps finis et la factorisation de Berlekamp. Exemples
9. Eléments primitifs. Théorème de la base normale. Exemples
10. Extensions cyclotomiques et extensions cycliques
11. La norme, la trace, et le théorème 90 de Hilbert
12. Extensions de Kummer
13. Résolubilité par radicaux et extensions résolubles
14. Premières notions de la cohomologie galoisienne (exemples)
15. Théorie d'Artin-Schreier (option facultative)

Table des matières

Cours N°1. Le jeudi 20 janvier 2005

(disponible sur : `http ://www-fourier.ujf-grenoble.fr /~panchish`)

0 Motivations et contenu du cours

Le présent cours est centré sur les corps et la théorie de Galois. Il est considéré comme la suite du cours "Algèbre1" de Prof. G.Tomanov, et on utilise comme prérequis les notions de groupe, d'homomorphisme, d'actions des groupes sur un ensemble, ainsi que des généralités sur les anneaux factoriels, la classification des modules de type fini sur les anneaux principaux, et en particulier, la structure des groupes abéliens de type fini.

La théorie de Galois donne un lien entre le problème de la solution d'une équation algébrique d'une indéterminée à coefficients dans un corps commutatif K, et le problème de la détermination d'un groupe (dit "le groupe de Galois d'un polynôme") qui opère sur l'ensemble des racines du polynôme correspondant, et cette action est donnée par automorphismes de certaines extensions du corps K.

Exemples de la solution d'une équation algébrique

$f(x) = 0$, où $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$.

$n = 2$ $f(x) = x^2 + px + q = (x - x_1)(x - x_2)$, avec $x_i \in \mathbb{C}$, $x_1 + x_2 = -p$, $x_1x_2 = q$. On utilise le discriminant $D = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = p^2 - 4q$, donc on obtient un système $\begin{cases} x_1 - x_2 = \pm\sqrt{D}, \\ x_1 + x_2 = -p \end{cases} \Longrightarrow x_1, x_2 = \frac{-p \pm \sqrt{D}}{2}$.

$n = 3$ Formule de Cardano. Cette formule pour résoudre par radicaux une équation générale de troisième degré $z^3 + rz^2 + sz + t = 0$ a été publiée en 1545 par un mathématicien et médecin italien Girolamo Cardano (1501-76) dans son livre "Ars Magna", mais la formule a été trouvée en 1515 par Scipione del Ferro (1465-1526). En substituant $z = x - 1/3r$ on obtient la forme réduite $x^3 + px + q = 0$, dans laquelle le terme quadratique a disparu. Ici $p = s - r^2/3$ et $q = 2r^3/27 - sr/3 + t$. On utilise le discriminant de l'équation cubique :

$$D = [(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)]^2 = -4p^3 - 27q^2$$

donc l'équation possède des racines multiples si et seulement si $D = 0$.

Si D est négatif, l'unique solution réelle de l'équation réduite est

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

et si D est positif, il y a trois solutions réelles. Rappellons les formules de Vieta : $\begin{cases} x_1 + x_2 + x = 3 = 0, \\ x_1x_2 + x_1x_3 + x_2x_3 = p, \\ x_1x_2x_3 = -q \end{cases}$

(Francois Viete ou Franciscus Vieta (1540-1603)).

L'expression $\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ est invariante par permutation cyclique des trois racines $\{x_1, x_2, x_3\}$, mais elle change le signe par l'action d'une transposition. Il existe d'autres

expressions invariantes par permutation cyclique des $\{x_1, x_2, x_3\}$: on considère $j = \exp(2i\pi/3)$, et les résolvante de Lagrange $(j, x_1) = x_1 + jx_2 + j^2x_3$, $(j^2, x_1) = x_1 + j^2x_2 + jx_3$, alors

$$A = (j, x_1)^3 = (x_1 + jx_2 + j^2x_3)^3 = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\delta, \tag{0.1}$$

$$B = (j^2, x_1)^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\delta \in \mathbb{Q}(\delta, j), \tag{0.2}$$

Les expressions A et B suffisent pour conclure :

$$\left\{\begin{array}{l}(j, x_1) = x_1 + jx_2 + j^2x_3\\ (j^2, x_1) = x_1 + j^2x_2 + jx_3\\ 0 = x_1 + x_2 + x_3\end{array}\right. \Longleftrightarrow \left\{\begin{array}{l}3x_1 = (j, x_1) + (j^2, x_1)\\ 3x_2 = j(j^2, x_1) + j^2(j, x_1)\\ 3x_3 = j(j, x_1) + j^2(j^2, x_1)\end{array}\right.$$

Pour voir (0.1), on remarque que $(x_1 + x_2 + x_3)^3 = x_1^3 + x_2^3 + x_3^3$
$+3(x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) - 3x_1x_2x_3 \Rightarrow$

$$(j, x_1)^3 = (x_1 + jx_2 + j^2x_3)^3 = \sum_i x_i^3 - \frac{3}{2}\sum_{i\neq j} x_i^2x_j + 6x_1x_2x_3 + \frac{3}{2}\sqrt{-3}\sqrt{D}.$$

En utilisant les fonctions élémentaires symétriques $\sigma_1 = x_1 + x_2 + x_3$,
$\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$, $\sigma_3 = x_1x_2x_3$, on obtient

$$\sigma_1^3 = \sum_i x_i^3 + 3\sigma_1\sigma_2 - 3x_1x_2x_3 = 0 \Rightarrow \sum_i x_i^3 = -3q \text{ car } \sigma_1 = 0, \sigma_2 = p, \sigma_3 = -q,$$

$$-\frac{3}{2}\sigma_1\sigma_2 = -\frac{3}{2}\sum_{i\neq j} x_i^2x_j - \frac{9}{2}x_1x_2x_3 = 0 \text{ car } \sigma_1 = 0$$

$$\frac{9}{2}\sigma_3 = \frac{9}{2}x_1x_2x_3 = -\frac{9}{2}q,$$

donc $\sum_i x_i^3 - \frac{3}{2}\sum_{i\neq j} x_i^2x_j + 6x_1x_2x_3 = -\frac{9}{2}q - 9q = -\frac{27}{2}q$, et $(j, x_1)^3 = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\delta$.

J.-L. Lagrange a remarqué que $\boxed{(x_1 + jx_2 + j^2x_3)\cdot(x_1 + j^2x_2 + jx_3) = -3p,}$ donc il n'y a que trois choix de signes possibles pour les radicaux

$$(j, x) = \sqrt[3]{A} = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}, (j^2, x) = \sqrt[3]{B} = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}$$

(et non 9 choix). Il vient

$$\left\{\begin{array}{l}3x_1 = (j, x) + (j^2, x)\\ 3x_2 = j(j^2, x) + j^2(j, x)\\ 3x_3 = j(j, x) + j^2(j^2, x)\end{array}\right. \Longleftrightarrow \left\{\begin{array}{l}x_1 = \dfrac{\sqrt[3]{A} + \sqrt[3]{B}}{3}\\ x_2 = \dfrac{j^2\sqrt[3]{A} + j\sqrt[3]{B}}{3}\\ x_3 = \dfrac{j\sqrt[3]{A} + j^2\sqrt[3]{B}}{3}\end{array}\right.$$

Une solution géométrique pour les équations cubiques générales à l'aide de sections coniques a été trouvée par Omar Khayam (1048-1131). Scipione del Ferro (1465-1526) a résolu cette équation en 1515, mais il a gardé sa solution secrète. Avant sa mort il l'a transmise à son élève Antonio Fior (né en 1506). Ce dernier a été défié par Niccolo Fontana (1499-1557) connu comme Tartaglia ("bégayer"), pour résoudre 30 problèmes sur les équations cubiques, toutes résolues par Tartaglia, et le nom de Fior a été oublié.

Il existe une implémentation de la formule de Cardano en Maple :

```
> solve(x^3+p*x+q,x );
```

$$x_1 = 1/6\,\sqrt[3]{-108\,q+12\,\sqrt{12\,p^3+81\,q^2}}-2\,\frac{p}{\sqrt[3]{-108\,q+12\,\sqrt{12\,p^3+81\,q^2}}},$$

$$x_2 = -1/12\,\sqrt[3]{-108\,q+12\,\sqrt{12\,p^3+81\,q^2}}+\frac{p}{\sqrt[3]{-108\,q+12\,\sqrt{12\,p^3+81\,q^2}}}$$

$$+1/2\,i\sqrt{3}\left(1/6\,\sqrt[3]{-108\,q+12\,\sqrt{12\,p^3+81\,q^2}}\right.$$

$$\left.+2\,\frac{p}{\sqrt[3]{-108\,q+12\,\sqrt{12\,p^3+81\,q^2}}}\right),$$

$$x_3 = -1/12\,\sqrt[3]{-108\,q+12\,\sqrt{12\,p^3+81\,q^2}}+\frac{p}{\sqrt[3]{-108\,q+12\,\sqrt{12\,p^3+81\,q^2}}}$$

$$-1/2\,i\sqrt{3}\left(1/6\,\sqrt[3]{-108\,q+12\,\sqrt{12\,p^3+81\,q^2}}+2\,\frac{p}{\sqrt[3]{-108\,q+12\,\sqrt{12\,p^3+81\,q^2}}}\right)$$

$n = 4$ Il y a une solution correspondante pour une équation générale quartique, associée aux noms de Ludovico Ferrari (1522-1565) et Cardano. On procède en produisant une équation cubique résolvante, pour laquelle la formule précédente s'applique.

Girolamo Cardano (1501-76)

après avoir décliné plusieurs propositions de poste de médecin de cour, parmi les savants de sa génération, il fut celui qui eut la contribution la plus importante dans les domaines des mathématiques et de la médecine.
Il fut le premier à identifier le typhus. Il écrivit un livre sur la probabilité, et résolut les équations cubiques (basé sur les travaux de N. Tartaglia et S.del Ferro), ainsi que les équations de quatrième degré en 1540 (avec son étudiant L.Ferrari). Ses travaux sur les sciences, la philosophie et l'astrologie ont joui d'un grand succès. Il a été emprisonné pour hérésie en 1570 et privé de son poste.

$n \geq 5$ Il n'existe aucune formule générale pour les racines $\{x_1, \cdots, x_n\}$, et on peut montrer que les racines d'équations concrètes ne peuvent pas être obtenues par l'extraction successive des radicaux, comme dans le cas : $f(x) = x^5 - 10x - 2$, mais parfois c'est possible : $x^5 - 2$.

Pendant 300 ans après Cardano, la majorité des mathématiciens pensait que l'équation quintique générale est aussi résoluble par radicaux. En 1799, le mathématicien italien Paolo Ruffini (1765-1822) essayait de prouver qu'elle n'est pas résoluble en utilisant les idées de la théorie des groupes, mais sa démonstration contenait un trou. En 1824, Niels Henrik Abel (1802-1829) a donné une première démonstration correcte de ce résultat. Évariste Galois a prouvé indépendamment la non-résolubilité par radicaux en utilisant sa théorie de Galois, basée sur la théorie des groupes et la théorie des corps commutatifs. Cette théorie a eu beaucoup d'implications au-dessus de son but de départ. En particulier, on peut utiliser cette théorie pour déterminer, quelles équations peuvent être résolues par radicaux.

Galois, Évariste (1811-32)

un génie mathématique français ayant eu une contribution significative dans la théorie des fonctions, la théorie des équations, et la théorie des nombres, et son travail fut à la base de la théorie des groupes (terme qu'il a introduit). Il a développé ces sujets en essayant de démontrer (déjà en école) l'impossibilité de solution par radicaux d'une équation générale de cinquième degré (ce que connaissait déjà Abel). Quoiqu'il avait déjà publié quelques articles au moment où il soumettait un travail à l'Académie des Sciences en 1829, un exemplaire de celui-ci fut perdu par Cauchy, et l'autre par Fourier. Il a essayé par deux fois d'entrer à l'École Polytechnique, mais il n'a pas été reçu (une fois à cause d'une dispute survenue avec son examinateur lors de son examen d'entrée) ; cependant il fut admis à l'Ecole Normale.

L'idée de la méthode de Galois

On associe à un polynôme $f(x) = x^n + a_{n-1}x^{n-1} + \cdots a_0 = (x - x_1)\cdot\ldots\cdot(x - x_n) \in \mathbb{Q}[x]$ le groupe G_f, dit "le groupe de Galois", un sous-groupe du groupe des permutations $S(x_1, \cdots x_n)$ des racines $x_1, \cdots, x_n$:

$$G_f \subset S(x_1, \cdots, x_n),$$

induites par certains automorphismes d'un corps commutatif contenant $x_1, \cdots, x_n$.

Pour trouver $x_1, \cdots x_n$, on cherche les expressions fixées par toutes les permutations dans G_f. Par exemple, si $n = 3$, on utilise $\delta, (j, x)^3, (j^2, x)^3$, invariantes par le sous-groupe $H = A_3 \subset S_3$, qui permet de trouver x_1, x_2, x_3 par radicaux. Dans le cas général, le sous-groupe $G_f \subset S(x_1, \cdots, x_n)$ peut être plus petit que S_n (pour une équation particulière), alors il est plus facile de résoudre $f(x) = 0$ en utilisant les expressions convenables de $x_1, \cdots, x_n$.

Exemples

EXEMPLES 0.0.1 *(a) Si* $f(x) = x^5 - 2$, $|G_f| = 20$, $|S_5| = 120$, $x_k = \sqrt[5]{2}(\cos(2\pi k/5) + i\sin(2\pi k/5))$, $k = 0, 1, 2, 3, 4$.

Dans ce cas l'équation $f(x) = 0$ *est résoluble par radicaux, et on va montrer que*

$$G_f \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_5^*, b \in \mathbb{F}_5 \right\}$$

(b) Si $h(x) = x^5 - 10x - 2$, *alors* $G_h \cong S_5$, *et on va montrer que* $h(x) = 0$ *n'est pas résoluble par radicaux.*

Pour montrer a) et b), on utilisera les factorisations du polynôme $f(x) \bmod p$:

$$(x^5 - 2) \bmod 7 = (x^4 + 4\,x^3 + 2\,x^2 + x + 4)\,(x + 3),\ (x^5 - 2) \bmod 11 = x^5 + 9 \text{ (irréductible)}$$

$$(x^5 - 10x - 2) \bmod 3 = x^5 + 2\,x + 1 \text{ (irréductible)}$$
$$(x^5 - 10x - 2) \bmod 11 = (x^4 + x^3 + x^2 + x + 2)\,(x + 10)$$
$$(x^5 - 10x - 2) \bmod 13 = (x^2 + 10\,x + 5)\,(x^3 + 3\,x^2 + 4\,x + 10)$$

On montrera que ces factorisations correspondent aux types cycliques d'éléments du groupe de Galois G_f, vu comme un sous-groupe de S_n.

Des exemples de calcul en Maple sont disponibles à l'adresse cachée :
`http ://www-fourier.ujf-grenoble.fr /~panchish/05ensl-maple` **dans le fichier 5ensl-gal-perm4.mws :**
Factorisation mod p et la structure du groupe de Galois

```
> Factor(x^5-2) mod 3;
```
$$(x^4 + 2\,x^3 + x^2 + 2\,x + 1)\,(x + 1)$$
```
> Factor(x^5-2) mod 5;
```
$$(x + 3)^5$$
```
> Factor(x^5-2) mod 7;
```
$$(x^4 + 4\,x^3 + 2\,x^2 + x + 4)\,(x + 3)$$
```
> Factor(x^5-2) mod 11;
```
$$x^5 + 9$$
```
> for n from 2 to 31
> do if(isprime(n)=true) then  print(n, Factor(x^5-2) mod n);fi;od;
```
$$2,\ x^5$$
$$3,\ (x^4 + 2\,x^3 + x^2 + 2\,x + 1)\,(x + 1)$$
$$5,\ (x + 3)^5$$
$$7,\ (x + 3)\,(x^4 + 4\,x^3 + 2\,x^2 + x + 4)$$
$$11,\ x^5 + 9$$
$$13,\ (x + 7)\,(x^4 + 6\,x^3 + 10\,x^2 + 8\,x + 9)$$

$$17,\ (x+2)\,(x^4+15\,x^3+4\,x^2+9\,x+16)$$
$$19,\ (x^2+18\,x+16)\,(x+4)\,(x^2+16\,x+16)$$
$$23,\ (x+17)\,(x^4+6\,x^3+13\,x^2+9\,x+8)$$
$$29,\ (x+8)\,(x^2+10\,x+6)\,(x^2+11\,x+6)$$
$$31,\ x^5+29$$

```
> for n from 2 to 31
> do if(isprime(n)=true) then  print(n, Factor(x^5-10*x-2) mod n);fi;od;
```

$$2,\ x^5$$
$$3,\ x^5+2\,x+1$$
$$5,\ (x+3)^5$$
$$7,\ (x+2)^2\,(x+1)\,(x^2+2\,x+3)$$
$$11,\ (x^4+x^3+x^2+x+2)\,(x+10)$$
$$13,\ (x^2+10\,x+5)\,(x^3+3\,x^2+4\,x+10)$$
$$17,\ (x+5)\,(x+4)\,(x^2+2\,x+15)\,(x+6)$$
$$19,\ (x^2+8\,x+1)\,(x+10)\,(x+13)\,(x+7)$$
$$23,\ (x^2+15\,x+5)\,(x^3+8\,x^2+13\,x+18)$$
$$29,\ (x+4)\,(x+20)\,(x^2+11\,x+11)\,(x+23)$$
$$31,\ x^5+21\,x+29$$

Groupes résolubles et résolubilité par radicaux

Rappelons :

DÉFINITION 0.0.2 (a) *Un sous-groupe $H \subset G$ d'un groupe G est dit* distingué, *si pour tout $g \in G$ on a $gH = Hg$, notation $H \triangleleft G$. Dans ce cas on définit le groupe quotient*

$$G/H = \{gH \mid g_1H \cdot g_2H = g_1g_2H\}$$

(b) *G est dit* résoluble *s'il existe une série*

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\}$$

telle que G_{k-1}/G_k sont tous abéliens $(k = 1, 2, \cdots, n)$

On montrera dans le cours que la résolubilité de l'équation $f(x) = 0$ en radicaux $\Longleftrightarrow$ la résolubilité du groupe de Galois G_f du polynôme f.

EXEMPLES 0.0.3 *Les groupes*

$$G = S_2, S_3, A_4, S_4$$

et

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_5^*, b \in \mathbb{F}_5 \right\}$$

sont résolubles, mais les groupes

$$G = S_n \text{ et } A_n \subset S_n (n \geq 5)$$

ne sont pas résolubles.

NOTATIONS. On notera

$\mathbb{Z}$ l'ensemble des entiers relatifs,

$\mathbb{N}$ l'ensemble des nombres naturels,

$\mathbb{Q}$ l'ensemble des nombres rationnels,

$\mathbb{R}$ l'ensemble des nombres réels et

$\mathbb{C}$ l'ensemble des nombres complexes.

Si X est un ensemble, on note $\#X$ son cardinal :

$$\#X = \text{Card}\,(X) = |X|.$$

On écrit $|X| < \infty$, si X est un ensemble fini.

Si a est un nombre réel, on note $|a| = \sup(a, -a)$ sa valeur absolue.

Donc,

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\},\ \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

La notation $\mathbb{Z}$ vient de l'allemand ("**Z**ahlen") (depuis le 19^{e} siècle).

Un nombre entier positif p est dit premier s'il est strictement supérieur à 1 et si ses seuls diviseurs positifs sont 1 et p.

On notera $\mathcal{P}$ l'ensemble de tous les nombres premiers.

Une application très essentielle de la théorie de Galois pour l'arithmétique vient du fait que tout nombre premier p fournit une classe d'automorphismes dans des groupes de Galois, provenant des automorphismes de Frobenius sur la réduction des nombres entiers algébriques. L'utilisation des nombres premiers permet souvent de calculer le groupe de Galois.

Réciproquement, le connaissance des propriétés galoisiennes permet de déduire des propriétés de nombres premiers, comme la densité dans une progression arithmétique, la représentabilité par des formes quadratiques etc.

Deux résultats de base de la théorie des nombres

(1) L'ensemble $\mathcal{P}$ de tous les nombres premiers est *infini*;

(2) THÉORÈME FONDAMENTAL DE L'ARITHMÉTIQUE :

Tout entier positif n se décompose de façon unique sous la forme

$$m = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_t^{k_t} \text{ avec } p_i \in \mathcal{P},\ \ p_1 < p_2 < \cdots < p_t,\ k_i \in \mathbb{N}$$

Exercices

0.1 Résoudre l'équation $x^3 - x - 1 = 0$ par radicaux

0.2 Trouver le discriminant du polynôme $z^3 + rz^2 + sz + t = 0$.

0.3 Montrer que les polynômes $(x^5 - 2) \bmod 11 = x^5 + 9$ et $(x^5 - 10x - 2) \bmod 3 = x^5 + 2x + 1$ sont irréductibles.

0.4 Soit p un nombre premier. Montrer que le groupe $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_p^*, b \in \mathbb{F}_p \right\}$ est résoluble.

Première partie
Extensions de corps commutatifs

1 Extensions et algébricité

1.1 Polynômes irréductibles.

Rappelons que si K est un corps l'anneau des polynômes $K[X]$ est euclidien, donc principal et factoriel, en particulier tout polynôme non nul s'écrit de manière unique comme produit de son coefficient dominant et de polynômes irréductibles unitaires.

Et on obtient la définition suivante pour les éléments irréductibles de $K[X]$:

Définition 1.1.1 *Soit K un corps. Un polynôme $P \in K[X]$ est dit* irréductible, *s'il vérifie les deux conditions suivantes :*

Irr1. $P \notin K$

Irr2. *Si $P = QR$ avec $Q, R \in K[X]$ alors $Q \in K^\times$ ou $R \in K^\times$.*

Exemples 1.1.2 *Soit K un corps.*

(i) Un polynôme $P \in K[X]$ de degré un est irréductible.

(ii) Un polynôme $P \in K[X]$ de degré 2 ou 3 est irréductible si et seulement s'il n'admet pas de racine dans K.

(iii) Tout polynôme irréductible sur $\mathbb{C}$ est de degré un.

(iv) Tout polynôme irréductible sur $\mathbb{R}$ est de degré ≤ 2.

Proposition 1.1.3 *Soit K un corps. Un polynôme $f \in K[X]$ est irréductible si et seulement si l'anneau quotient $K[X]/(f)$ est un corps.*

1.2 Extensions, degré.

Définition 1.2.1

(i) Soit K un corps et L un autre corps, contenant K. On dit que L est une extension *de K. C'est un espace vectoriel sur K.*

(ii) Soit L une extension d'un corps K. On appelle degré de L sur K la dimension $\dim_K L$ de L considéré comme espace vectoriel sur K. On le note $[L : K]$, le degré est éventuellement infini. Si le degré $[L : K]$ est fini on dit que L est une extension finie *de K.*

(iii) Si L est une extension de K et $A = (\alpha_i)_{i \in I}$ une partie de L, on appelle extension de K engendrée par A *le sous-corps minimal $K(A)$ de L contenant K et A. Les α_i s'appellent les* générateurs *de $K(A)$ sur K. Tout élément de $K(A)$ s'écrit comme une fraction rationnelle à coefficients dans K d'élément α_i.*

Par exemple, $\mathbb{C}$ est une extension finie de $\mathbb{R}$ de degré 2.

De plus $\mathbb{C} = \mathbb{R}(i)$

Théorème 1.2.2 *Si K, L et E sont trois corps emboîtés tels que $K \subset L \subset E$, alors*

$$[E : K] = [E : L] \cdot [L : K]$$

PREUVE : On note $(a_i)_{i\in I}$ une base de E sur L, et $(b_j)_{j\in J}$ une base de L sur K.

Pour tout $x \in E$, il existe une famille finie $(\alpha_i)_{i\in I_1}$, $I_1 \subset I$, d'éléments de L tels que $x = \sum_{i\in I_1} \alpha_i a_i$. Mais chaque α_i est combinaison linéaire à coefficients dans K d'éléments b_j : $\alpha_i = \sum_{j\in J_1} \beta_{i,j} b_j$, pour une famille finie $\beta_{i,j} \in K$. Ceci implique que $x = \sum_{(i,j)\in I_1\times J_1} \beta_{i,j} a_i b_j$, et donc la famille $(a_i b_j)_{i\in I, j\in J}$ est génératrice pour le K-espace vectoriel E.

C'est une famille libre : si $(\beta_{i,j})_{(i,j)\in X}$, $X \subset I_1 \times J_1 \subset I \times J$ est une famille finie d'éléments de K telle que $\sum_{(i,j)\in X} \beta_{i,j} a_i b_j = 0$, alors les images I_1 et J_1 de X par projection sur I et J sont finies et on a :

$$\sum_{(i,j)\in X} \beta_{i,j} a_i b_j = \sum_{i\in I_1} \left(\sum_{j\in J_1} \beta_{i,j} b_j \right) a_i = 0$$

et comme pour tout i $\sum_{j\in J_1} \beta_{i,j} b_j$ appartiennent à L, on trouve $\sum_{j\in J_1} \beta_{i,j} b_j = 0$ pour tout $i \in I_1$, puis $\beta_{i,j} = 0$ pour tout $(i,j) \in X$. □

COROLLAIRE 1.2.3 *Pour n corps emboîtés*

$$K \subset K_1 \subset \cdots \subset K_n,$$

on a l'égalité

$$[K_n : K] = [K_1 : K] \cdot [K_2 : K_1] \cdot \ldots \cdot [K_n : K_{n-1}].$$

EXEMPLE 1.2.4 *On considère le sous-corps $K = \mathbb{Q}(\sqrt[3]{2}, i)$ de $\mathbb{C}$, il contient $\mathbb{Q}(\sqrt[3]{2})$, et $K = \mathbb{Q}(\sqrt[3]{2})(i)$, donc*

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2})(i) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

Le polynôme $X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$ et le polynôme $X^2 + 1$ l'est dans $\mathbb{Q}(\sqrt[3]{2})[X]$. Donc,

$$[\mathbb{Q}(\sqrt[3]{2})(i) : \mathbb{Q}(\sqrt[3]{2})] = 2, [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3, \text{ et } [K : \mathbb{Q}] = 6.$$

1.3 Éléments algébriques

Soit E une extension d'un corps K.

DÉFINITION 1.3.1

(i) Un élément α de E est dit algébrique *sur K s'il existe un polynôme non nul P de $K[X]$ tel que $P(\alpha) = 0$.*

(ii) Une extension E de K est dite algébrique *si tout élément α de E est algébrique sur K.*

(iii) Si $\alpha \in E$ est un élément algébrique sur K l'ensemble des polynômes $P \in K[X]$ tels que $P(\alpha) = 0$, forme un idéal de $K[X]$, non réduit à (0). Cet idéal est principal, et son générateur unitaire s'appelle le polynôme minimal *de α sur K.*

PROPOSITION 1.3.2 *Soit E une extension d'un corps K, et soit α un élément de E algébrique sur K de polynôme minimal P.*

i) Si $Q \in K[X]$ admet α comme racine, alors P divise Q dans $K[X]$.

(ii) Le polynôme P est irréductible dans $K[X]$.

(iii) Le sous-anneau $K[\alpha]$ de E est un corps $K(\alpha)$ et on a $[K(\alpha) : K] = \deg P$. La famille $(1, \alpha, \cdots, \alpha^{n-1})$, où $n = \deg P$, est une base de $K(\alpha)$ sur K.

PREUVE : L'assertion (i) traduit que P engendre l'idéal des éléments de $K[X]$, ayant α comme racine.

(ii) Si P se factorise en QR dans $K[X]$, alors on a $P(\alpha) = Q(\alpha)R(\alpha) = 0$ dans le corps E, donc $Q(\alpha) = 0$ ou $R(\alpha) = 0$, et P divise Q ou R. □

(iii) Le sous-anneau $K[\alpha]$ est l'image de l'homomorphisme d'évaluation $Q \mapsto Q(\alpha)$ de $K[X]$ dans E, dont le noyau est l'idéal (P), maximal d'après (ii) Par le théorème d'isomorphisme, l'anneau $K[\alpha]$ est donc isomorphe au quotient $K[X]/(P)$, qui est un corps. Si $n = \deg P$, la famille $(1, \alpha, \cdots, \alpha^{n-1})$ est libre sur K car P est le polynôme non nul de plus petit degré qui annule α. Elle est génératrice car pour tout $Q \in K[X]$ on a $Q(\alpha) = R(\alpha)$, où R est le reste de la division euclidienne de Q par P, et donc $R(\alpha) = \sum_{i=0}^{n-1} r_i \alpha^i$, $r_i \in K$. La famille est donc une base de $K(\alpha)$ sur K. En particulier on a $[K(\alpha) : K] = n = \deg P$. □

PROPOSITION 1.3.3 *Soit E une extension finie d'un corps K ($[E : K] = n \in \mathbb{N}$), alors E est algébrique sur K.*

PREUVE. Soit α un élément de E. Si $n = [E : K]$, la famille de $n + 1$ éléments $(1, \alpha, \cdots, \alpha^n)$ n'est pas libre, donc il existe $P(X) = \sum_{i=0}^{n} a_i X^i$ non nul dans $K[X]$ tel que $\sum_{i=0}^{n} a_i \alpha^i = P(\alpha) = 0$. □

REMARQUE. L'assertion réciproque est fausse : l'extension $E = \overline{\mathbb{Q}} \subset \mathbb{C}$ de $\mathbb{Q}$, formée par tous les nombres complexes algébriques sur $\mathbb{Q}$ (E est bien un corps, exercice), est algébrique par définition, mais $[E : \mathbb{Q}]$ n'est pas finie. En effet, on vérifie qu'il existe des polynômes irréductibles sur $\mathbb{Q}$ de tout degré $n \geq 1$, par exemple $X^n - 2$ (exercice).

1.4 Corps de rupture, corps de décomposition

Remarquons que pour un corps arbitraire K et pour tout polynôme P non constant de $K[X]$ on peut construire une extension L de K dans laquelle P possède une racine : quitte à factoriser P on peut le supposer irréductible, auquel cas on a vu que l'anneau quotient $K[X]/(P)$ est un corps. La classe $X + (P)$ est alors une racine de P dans $K[X]/(P)$.

THÉORÈME 1.4.1 (SUR L'ISOMORPHISME) *Soient L une extension de K et $\alpha \in L$ une racine d'un polynôme irréductible P de $K[X]$. Alors l'anneau $K[\alpha]$ est un corps isomorphe à $K[X]/(P)$.*

C'est clair d'après le paragraphe précédent, proposition 1.3.2 et sa preuve, puisque P est à un facteur constant près le polynôme minimal de α sur K.

DÉFINITION 1.4.2 *Soit K un corps, et P un polynôme irréductible. On dit qu'un corps L contenant K est un* corps de rupture *de P sur K s'il existe un $\alpha \in L$ tel que $L = K(\alpha)$ et $P(\alpha) = 0$.*

REMARQUE 1.4.3 *Avec les notations de la proposition, on peut donner une construction matricielle de l'anneau $K[X]/(P)$, corps de rupture de P sur K.*

En effet, on écrit $P = \sum_{j=0}^{n} a_j X^j$, et on suppose que $a_n = 1$, alors dans la base

$$(\overline{1}, \overline{X}, \cdots, \overline{X^{n-1}}) \bmod (P)$$

de $K[X]/(P)$ la multiplication $\mu : Q \mapsto \overline{X}Q \bmod (P)$ a pour matrice

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix},$$

dont le polynôme minimal est P. Il vient que $K[A] \simeq K[X]/\operatorname{Ker}(\mu)$ est isomorphe à $K[X]/(P)$.

En itérant la construction de corps de rupture ci–dessus (on choisit à chaque étape un facteur irréductible de P de degré > 1 sur le corps obtenu), on peut construire pour tout polynôme $P \in K[X]$ une extension finie L' de K dans laquelle P s'écrit comme produit de facteurs du premier degré. La construction implique que l'extension L' peut être choisie de telle façon que $[L' : K] \leq n!$.

Cours N°2. Le jeudi 27 janvier 2005

(disponible sur : `http ://www-fourier.ujf-grenoble.fr /~panchish`)

1.4. Corps de rupture, corps de décomposition (rappels et suite)

THÉORÈME 1.4.1 (SUR L'ISOMORPHISME) *Soient L une extension de K et $\alpha \in L$ une racine d'un polynôme irréductible P de $K[X]$. Alors l'anneau $K[\alpha]$ est un corps isomorphe à $K[X]/(P)$.*

DÉFINITION 1.4.2 Soit K un corps, et P un polynôme irréductible. On dit qu'un corps L contenant K est un corps de rupture de P sur K s'il existe un $\alpha \in L$ tel que $L = K(\alpha)$ et $P(\alpha) = 0$.

DÉFINITION 1.4.4 (CORPS DE DÉCOMPOSITION) *On considère un polynôme P de $K[X]$ de degré supérieur ou égal à 1, et une extension E de K, dans laquelle P s'écrit $P(X) = (X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n)$. Alors le corps $L = K(\alpha_1, \cdots, \alpha_n)$ s'appelle* corps de décomposition *de P dans E. C'est l'extension minimale de K dans E, dans laquelle P se décompose en produit de facteurs linéaires.*

On va vérifier que ce corps est uniquement déterminé à isomorphisme près :

THÉORÈME 1.4.5 (SUR UN PROLONGEMENT D'ISOMORPHISME) *On considère un isomorphisme de corps $\sigma : K \to K'$, et un polynôme irréductible $P(X) = \sum_{j=0}^{n} a_j X^j \in K[X]$. On note $P^\sigma = \sum_{j=0}^{n} \sigma(a_j) X^j \in K'[X]$. On choisit une extension de K contenant une racine β de P, et une extension de K', contenant une racine β' de $P^\sigma(X)$. Alors il existe un isomorphisme de corps*

$$\tilde{\sigma} : K(\beta) \to K'(\beta'),$$

qui prolonge σ et tel que $\tilde{\sigma}(\beta) = \beta'$.

PREUVE. Comme σ est un isomorphisme de corps de K dans K', l'application

$$\varphi : K[X] \to K'[X], \quad Q(X) = \sum_{j=0}^{n} b_j X^j \mapsto Q^\sigma(X) = \sum_{j=0}^{n} \sigma(b_j) X^j$$

est un isomorphisme d'anneaux. On en déduit

$$\begin{array}{rccc} \tilde{\sigma} : & K(\beta) & \to & K'(\beta') \\ & \uparrow & & \uparrow \\ \overline{\varphi} : & K[X]/(P) & \to & K'[X]/(P^\sigma), \\ & Q + (P) & \mapsto & Q^\sigma + (P^\sigma) \end{array}$$

Cela montre à la fois que P^σ est un élément irréductible de $K'[X]$ (par le théorème sur l'isomorphisme 1.4.1, $K'[X]/(P^\sigma)$ est un corps), et que si $\theta = Q(\beta) \in K(\beta)$, son image par $\tilde{\sigma}$ est bien définie par l'égalité $\tilde{\sigma}(\theta) = Q^\sigma(\beta')$. □

THÉORÈME 1.4.6 (DE L'UNICITÉ) *Soient $\sigma : K \xrightarrow{\sim} K'$ un isomorphisme de corps, $P(X) = \sum_{j=0}^{n} a_j X^j$ un polynôme de $K[X]$, et notons $P^\sigma = \sum_{j=0}^{n} \sigma(a_j) X^j \in K'[X]$.*

À P, on associe une extension E de K, dans laquelle il se factorise en produit de termes du premier degré, $P(X) = a(X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n)$, et on note $B = K(\alpha_1, \cdots, \alpha_n)$ le corps de décomposition de P dans E.

On définit de même E' et B' pour le polynôme P^σ. Il existe alors un isomorphisme de corps

$$\tau : B \xrightarrow{\sim} B',$$

dont la restriction à K est égale à σ.

PREUVE. Le polynôme P s'écrit $P(X) = a(X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n)$, les α_i étant des éléments de E. Raisonnons par récurrence sur le nombre N d'éléments α_i, qui n'appartiennent pas à K.

Si $N = 0$, tous les α_i appartiennent à K, donc $B = K$ est isomorphe à $B' = K'$, et $\tau = \sigma$.

Pour $N \geq 1$, supposons que α_1 n'appartienne pas à K.

C'est un élément algébrique sur K, de polynôme minimal S, et il existe $Q \in K[X]$ tel que $P = SQ$.

Dans $E'[X]$, on a les égalités

$$P^\sigma = S^\sigma Q^\sigma = a'(X-\alpha'_1)\cdot\ldots\cdot(X-\alpha'_n).$$

Si β est une racine de S^σ dans une extension de E', il vient

$$P^\sigma(\beta) = 0 = a'(\beta-\alpha'_1)\cdot\ldots\cdot(\beta-\alpha'_n),$$

donc il existe un indice i, qu'on peut supposer égal à 1, tel que $\beta = \alpha'_1 \in E'$. On utilise le théorème 1.4.5 pour le polynôme irréductible S : il existe un isomorphisme de corps

$$\tau : K(\alpha_1) \xrightarrow{\sim} K'(\alpha'_1),$$

qui prolonge σ.

On considère maintenant P comme un polynôme à coefficients dans $L = K(\alpha_1)$.

Le nombre de racines de P qui n'appartiennent pas à L est strictement inférieur à N, et l'hypothèse de récurrence nous donne l'existence d'un prolongement de τ,

$$\pi : L(\alpha_2, \cdots, \alpha_n) \xrightarrow{\sim} L'(\alpha'_2, \cdots, \alpha'_n),$$

avec $L' = K'(\alpha'_1)$. On termine en remarquant que $L(\alpha_2, \cdots, \alpha_n) = K(\alpha_1, \alpha_2, \cdots, \alpha_n)$, et que $L'(\alpha'_2, \cdots, \alpha'_n) = K'(\alpha'_1, \alpha'_2, \cdots, \alpha'_n)$. □

COROLLAIRE 1.4.7 (DE L'UNICITÉ) *Soient K un corps, P un polynôme de $K[X]$, et L, L' deux corps de décomposition de P sur K. Alors il existe un isomorphisme de corps de L sur L' dont la restriction à K est l'identité.*

En effet, il suffit d'utiliser le résultat précédent pour $\sigma = \mathrm{id} : K \to K$.

2 Caractères d'un groupe et morphismes de corps

2.1 Indépendance linéaire des caractères

DÉFINITION 2.1.1 *Étant donné un groupe G et un corps K, on appelle* caractère *de G dans K tout morphisme de groupes de G dans K^*.*

EXEMPLE 2.1.2 *Pour tout corps K on a $\mathrm{Hom}(\mathbb{Z}, K^*) = K^*$ (tout caractère est déterminé par l'image du générateur 1 du groupe additif $\mathbb{Z}$ dans le groupe multiplicatif K^*).*

NOTATIONS. Si G est abélien, on note $X^*(G) = \mathrm{Hom}(G, \mathbb{C}^*)$ le groupe des caractères de G dans $\mathbb{C}$ avec la loi

$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g).$$

On utilise les caractères des groupes pour étudier les morphismes des corps. Soient E et E' deux corps, alors tout morphisme $\sigma \in \mathrm{Hom}(E, E')$ de E dans E' donne un caractère du groupe $G = E^*$ dans $K = E'$,

EXEMPLE 2.1.3 *Si $G = \mathbb{Z}/n\mathbb{Z}$, un* morphisme *de G dans $\mathbb{C}^*$ est déterminé par l'image de $\overline{1}$ qui vérifie*

$$\chi(\overline{1})^n = \chi(n\overline{1}) = \chi(\overline{0}) = 1.$$

C'est donc une racine n-ième de l'unité dans $\mathbb{C}^*$.

Inversement si ζ est une racine n-ième de l'unité, l'application

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^\times, \quad \overline{x} \mapsto \zeta^x$$

est un caractère de $\mathbb{Z}/n\mathbb{Z}$; on a ainsi obtenu une bijection du groupe $\mu_n(\mathbb{C})$ sur $X^*(\mathbb{Z}/n\mathbb{Z})$. Notons en outre que l'exponentielle complexe fournit un isomorphisme de groupes

$$\mathbb{Z}/n\mathbb{Z} \to \mu_n(\mathbb{C}), \quad \overline{x} \mapsto \exp(\frac{2i\pi x}{n})$$

THÉORÈME 2.1.4 (D'INDÉPENDANCE LINÉAIRE DE CARACTÈRES (E.ARTIN))
Soient $\sigma_1, \cdots, \sigma_n \in \mathrm{Hom}(G, K^*)$ n caractères distincts *d'un groupe G dans un corps K. Alors ce sont n éléments linéairement indépendants du K-espace vectoriel des applications de G dans K.*

PREUVE : On raisonne par récurrence sur l'entier n. Un caractère n'étant jamais nul, l'assertion est vraie pour $n = 1$.

Pour $n \geq 2$, supposons l'assertion vraie pour tout $i < n$, et choisissons dans K des éléments a_i $(1 \leq i \leq n)$ tels que pour tout $x \in G$ on ait l'égalité

$$e(x) = a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0$$

Si α appartient à G, on a aussi pour tout x de G

$$e(\alpha x) - \sigma_n(\alpha)e(x) = 0,$$

soit

$$a_1(\sigma_1(\alpha)-\sigma_n(\alpha))\sigma_1(x)+\cdots+a_{n-1}(\sigma_{n-1}(\alpha)-\sigma_n(\alpha))\sigma_{n-1}(x)=0.$$

Comme les σ_i sont distincts, il existe un α dans G tel que $\sigma_1(\alpha)-\sigma_n(\alpha)$ soit non nul ; et d'après l'hypothèse de récurrence, les caractères $\sigma_1,\cdots,\sigma_{n-1}$ sont linéairement indépendants, donc on a

$$a_1(\sigma_1(\alpha)-\sigma_n(\alpha))=0=a_{n-1}(\sigma_{n-1}(\alpha)-\sigma_n(\alpha))$$

d'où $a_1=0$. On utilise de nouveau l'hypothèse de récurrence avec les caractères $\sigma_2,\cdots,\sigma_n$, d'où $a_2=\cdots=a_n=0$, ce qui prouve que $\sigma_1,\cdots,\sigma_n$ sont linéairement indépendants.

COROLLAIRE 2.1.5 *Soient E et E' deux corps, et $\sigma_1,\cdots,\sigma_n\in\mathrm{Hom}(E,E')$ n morphismes* distincts *de E dans E'. Alors ce sont n éléments linéairement indépendants du E'-espace vectoriel des applications de E dans E'.*

PREUVE : il suffit de poser $G=E^*$, $K=E'$, et d'utiliser le théorème 2.1.4.

NOTATIONS. Si X est un ensemble fini, on considère la forme

$$\mathbb{C}^X\times\mathbb{C}^X\to\mathbb{C},\quad (f,g)\to\langle f,g\rangle=\frac{1}{\#X}\sum_{x\in X}\overline{f(x)}g(x).$$

PROPOSITION 2.1.6 *Si G est un groupe fini et χ, χ' deux caractères de G, dans $\mathbb{C}$, alors*

$$\langle\chi,\chi'\rangle=\begin{cases}1, & \text{si } \chi=\chi'\\ 0, & \text{sinon.}\end{cases}$$

COROLLAIRE 2.1.7 *Si G est un groupe fini, la famille $(\chi)_{\chi\in X^*(G)}$ est une famille libre du $\mathbb{C}$-espace vectoriel $\mathbb{C}^G$*

EXERCICES

2.1 Soit $K\subset E$ une extension de corps. Montrer que $\overline{K_E}=\{x\in E, x \text{ est algébrique sur } K\}$ est un sous-corps de E.

2.2 Montrer qu'il existe des polynômes irréductibles sur $\mathbb{Q}$ de tout degré $n\geq 1$, par exemple X^n-p, où p est un nombre premier.

2.3 Soit K un corps. En considérant l'ordre des éléments d'un groupe cyclique, montrer que $n=\sum_{d|n}\varphi(d)$. En déduire une autre preuve que tout sous-groupe d'ordre n de K^* est cyclique.

2.4 Soit K un corps à q éléments, $q\geq 4$. Montrer que $\sum_{x\in K}x^2=0$. Plus généralement, calculer, pour $s\geq 1$, la somme $\sum_{x\in K}x^s$.

2.5 Si H est un sous-groupe de $\mathbb{C}^*$ tel que $\mathbb{C}^*/H$ est fini, monter que $H=\mathbb{C}^*$.

2.6 Soit G un groupe abélien. Montrer que $\mathrm{Hom}(G,K^*)$ est un groupe abélien avec la multiplication $\chi_1\chi_2(g)=\chi_1(g)\chi_2(g)$

2.7 Si $|G|<\infty$, montrer que $|\mathrm{Hom}(G,K^*)|\leq|G|$.

2.8 Soient $K=\mathbb{C}$, G un groupe abélien. On pose $G^\vee=\mathrm{Hom}(G,\mathbb{C}^*)=X^*(G)$.

a) Montrer qu'il existe un isomorphisme (non-canonique) $G^\vee \xrightarrow{\sim} G$, donc $|G^\vee| = |G|$.

b) Démontrer les relations d'orthogonalité :

$$\sum_{g\in G}\chi(g) = \begin{cases}|G|, & \text{si } \chi \equiv 1\\ 0, & \text{sinon}\end{cases}, \quad \sum_{\chi\in G^\vee}\chi(g) = \begin{cases}|G|, & \text{si } g = e\\ 0, & \text{sinon}\end{cases}$$

2.9 Soit

$$1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1$$

une suite exacte de trois groupes abéliens finis ; c'est-à-dire, que $\mathrm{Im} f = \mathrm{Ker}\, g$, $\mathrm{Ker}\, f = \{1\}$, $\mathrm{Im} g = C$. Montrer qu'il existe une suite exacte des groupes des caractères :

$$1 \to C^\vee \xrightarrow{g^\vee} B^\vee \xrightarrow{f^\vee} A^\vee \to 1,$$

où $g^\vee$, $f^\vee$ sont définis pour tout $\chi \in C^\vee$, $\psi \in B^\vee$ et pour tout $b \in B$, $a \in A$ par

$$g^\vee(\chi)(b) = \chi(g(b)), \quad f^\vee(\psi)(a) = \psi(f(a)).$$

2.2 Application : corps des fixes

Définition 2.2.1 *On considère n morphismes $\{\sigma_1, \cdots, \sigma_n\}$ du corps E dans le corps E', et l'ensemble*

$$F = \{a \in E \mid \sigma_1(a) = \cdots = \sigma_n(a)\}.$$

On vérifie facilement que F est un sous-corps de E ; F s'appelle corps des fixes *par l'ensemble $\{\sigma_1, \cdots, \sigma_n\}$, et on le note $E^{\{\sigma_1,\cdots,\sigma_n\}}$.*

Théorème 2.2.2 *Soient $\{\sigma_1, \cdots, \sigma_n\}$ n morphismes distincts du corps E dans le corps E', F leur corps des fixes. On a alors l'inégalité $[E : F] \geq n$.*

Preuve : Posons $[E : F] = r$, et soit $\{\omega_1, \cdots, \omega_r\}$ une base de E sur F : tout $\alpha \in E$ s'écrit $\alpha = a_1\omega_1 + \cdots + a_r\omega_r$, avec $a_i \in F$.

Considérons ensuite une solution $(x_1, \cdots, x_n)$ du système

$$\begin{cases} \sigma_1(\omega_1)x_1 + \cdots + \sigma_n(\omega_1)x_n = 0\\ \sigma_1(\omega_2)x_1 + \cdots + \sigma_n(\omega_2)x_n = 0\\ \cdots\cdots\cdots\cdots\cdots\\ \sigma_1(\omega_r)x_1 + \cdots + \sigma_n(\omega_r)x_n = 0 \end{cases} \tag{2.1}$$

Comme pour tout $a \in F$, on a les égalités $\sigma_1(a) = \cdots = \sigma_n(a)$, on en déduit les relations :

$$\begin{cases} \sigma_1(a_1\omega_1)x_1 + \cdots + \sigma_n(a_1\omega_1)x_n = 0\\ \sigma_1(a_2\omega_2)x_1 + \cdots + \sigma_n(a_2\omega_2)x_n = 0\\ \cdots\cdots\cdots\cdots\cdots\\ \sigma_1(a_r\omega_r)x_1 + \cdots + \sigma_n(a_r\omega_r)x_n = 0 \end{cases}$$

Et en sommant, on en déduit que pour tout $\alpha \in E$, on a

$$(x_1\sigma_1 + \cdots + x_n\sigma_n)(\alpha) = 0.$$

Grâce au corollaire 2.1.5, il vient que $x_1 = \cdots = x_n = 0$.

Le système linéaire homogène (2.1), de r équations à n inconnues, n'admet que la solution nulle : $r \geq n$. □

COROLLAIRE 2.2.3 *Soient $\{\sigma_1, \cdots, \sigma_n\}$ n automorphismes distincts du corps E, et $F = E^{\{\sigma_1,\cdots,\sigma_n\}}$ leur corps des fixes. On a alors l'inégalité $[E : F] \geq n$.*

On montrera qu'on a souvent l'égalité $[E : F] = n$.

EXEMPLE 2.2.4 *$E = \mathbb{C}$, $\sigma_1(z) = z$ et $\sigma_2(z) = \overline{z}$. Alors*

$$F = \{z \in \mathbb{C} \mid z = \overline{z}\} = \mathbb{R}, \text{ et } [\mathbb{C} : \mathbb{R}] = 2.$$

EXEMPLE 2.2.5 *Il se peut que l'égalité $[E : F] = n$ ne soit pas atteinte : on considère $E' = E = \mathbb{Q}(\sqrt[3]{2}, j)$, $\sigma_1 = \mathrm{id}$, $\sigma_2(\alpha) = j\alpha$, et $\sigma_2(j) = j$, où $\alpha = \sqrt[3]{2}$, et $n = 2$. On considère les corps intermédiaires $E_1 = \mathbb{Q}(\sqrt[3]{2})$, $E_2 = \mathbb{Q}(j)$. Alors*

$$[E : \mathbb{Q}] = [E : E_1][E_1 : \mathbb{Q}] = 2 \cdot 3 = [E : E_2][E_2 : \mathbb{Q}] = 3 \cdot 2.$$

Pour tout $\gamma \in E$ il existe donc un unique triplet $a_0, a_1, a_2 \in E_2$ tel que $\gamma = a_0 + a_1\alpha + a_2\alpha^2$, et l'action de σ_2 est donnée par $\sigma_2(a_0 + a_1\alpha + a_2\alpha^2) = a_0 + ja_1\alpha + j^2a_2\alpha^2$. Ceci montre que

$$F = \{\gamma \in E \mid \gamma = a_0 \in E_2\} = \mathbb{Q}(j), \text{ et } [E : F] = 3.$$

On a donc $r = [E : F] = 3 > 2 = n$.

Cours N°3. Le jeudi 3 février 2005

(disponible sur : `http ://www-fourier.ujf-grenoble.fr /~panchish`)

Deuxième partie

Correspondance de Galois

3 Groupes de Galois

3.1 Extensions galoisiennes

Rappelons qu'une extension de corps E/F est un couple, formé par deux corps $E \supset F$ (c'est une notation traditionnelle, ne pas confondre avec le groupe quotient !)

DÉFINITION 3.1.1 *On se donne un corps E, et le groupe* Aut$E$ *de tous les automorphismes de E. Soit*

$$G = \{\sigma_1, \cdots, \sigma_n\}$$

un sous-groupe fini de Aut$E$. *On appelle* extension galoisienne *de groupe de Galois G l'extension E/F, où $F = E^G$ est le corps des fixes par G.*

Le groupe G est souvent noté $\mathrm{Gal}(E/F)$. Comme il contient l'identité, pour tout $y \in F$ et pour tout $\sigma \in G$ on a $\sigma(y) = y$.

EXEMPLE. Soient $n \geq 3$ un nombre naturel, $\zeta = \exp(2i\pi/n)$. On montrera que l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est galoisienne de groupe de Galois $G \cong (\mathbb{Z}/n\mathbb{Z})^*$, avec les automorphismes σ_a $(a \in (\mathbb{Z}/n\mathbb{Z})^*)$, donnés par

$$\sigma_a(\zeta) = \zeta^a \quad (\text{pour tout } a \bmod n, \mathrm{pgcd}(a, n) = 1)$$

Par contre, on verra que l'extension $\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$ n'est pas galoisienne pour $n \geq 3$ (exercice à faire)

THÉORÈME 3.1.2 *Soient $G = \{\sigma_1, \cdots, \sigma_n\}$ un sous-groupe fini de* Aut$E$ *et E/F extension galoisienne associée. Alors $[E : F] = n$.*

PREUVE : Grâce au théorème 2.2.2, il suffit de démontrer l'inégalité $[E : F] \leq n$.

À tout $x \in E$, associons sa trace

$$\mathrm{Tr}(x) = \sigma_1(x) + \cdots + \sigma_n(x).$$

Comme G est un groupe, pour tout $\sigma_i \in G$, on a :

$$\sigma_i(\mathrm{Tr}(x)) = \mathrm{Tr}(x) = \sigma_1(\mathrm{Tr}(x)) \text{ (si } \sigma_1 \text{ est le neutre de } G).$$

Donc $\mathrm{Tr}(x)$ est un élément de F. On en déduit que l'application trace $(\mathrm{Tr} : x \mapsto \mathrm{Tr}(x))$ est une forme F-linéaire sur E ; d'après le corollaire 2.1.5, sur l'indépendance linéaire des σ_i, cette forme est non nulle : soit $y \in E$ un élément de trace non-nulle.

Considérons maintenant une famille $\{\alpha_1, \cdots, \alpha_{n+1}\}$ de $n+1$ éléments de E. On lui associe le système homogène de n équations à $n+1$ inconnues dans le corps E :

$$\left\{\begin{array}{l} x_1\sigma_1^{-1}(\alpha_1) + \cdots + x_{n+1}\sigma_1^{-1}(\alpha_{n+1}) = 0 \\ x_1\sigma_2^{-1}(\alpha_1) + \cdots + x_{n+1}\sigma_2^{-1}(\alpha_{n+1}) = 0 \\ \cdots\cdots\cdots\cdots\cdots \\ x_1\sigma_n^{-1}(\alpha_1) + \cdots + x_{n+1}\sigma_n^{-1}(\alpha_{n+1}) = 0 \end{array}\right. \tag{3.1}$$

Comme le système est homogène, et comme le nombre d'équations est inférieur au nombre d'inconnues, l'ensemble des solutions est un espace vectoriel sur E de dimension au moins égale à 1.

Soit donc $(x'_1, \cdots, x'_{n+1})$ une solution non nulle ; quitte à changer l'indexation, on peut supposer $x'_1 \neq 0$. En posant $x_i = \frac{x'_i}{x'_1} y$, on obtient une solution $(x_1, \cdots, x_{n+1})$ avec $x_1 = y$. Et on a les égalités (3.1) :

$$\left\{\begin{array}{l} x_1\sigma_1^{-1}(\alpha_1) + \cdots + x_{n+1}\sigma_1^{-1}(\alpha_{n+1}) = 0 \\ x_1\sigma_2^{-1}(\alpha_1) + \cdots + x_{n+1}\sigma_2^{-1}(\alpha_{n+1}) = 0 \\ \cdots\cdots\cdots\cdots\cdots \\ x_1\sigma_n^{-1}(\alpha_1) + \cdots + x_{n+1}\sigma_n^{-1}(\alpha_{n+1}) = 0 \end{array}\right.$$

Prenons l'image de la i-ème ligne par σ_i :

$$\left\{\begin{array}{l} \sigma_1(x_1)\alpha_1 + \cdots + \sigma_1(x_{n+1})\alpha_{n+1} = 0 \\ \sigma_2(x_1)\alpha_1 + \cdots + \sigma_2(x_{n+1})\alpha_{n+1} = 0 \\ \cdots\cdots\cdots\cdots\cdots \\ \sigma_n(x_1)\alpha_1 + \cdots + \sigma_n(x_{n+1})\alpha_{n+1} = 0 \end{array}\right.$$

Et en sommant, on obtient l'égalité :

$$\mathrm{Tr}(x_1)\alpha_1 + \cdots + \mathrm{Tr}(x_{n+1})\alpha_{n+1} = 0, \text{ avec } \mathrm{Tr}(x_1) = \mathrm{Tr}(y) \neq 0.$$

Toute famille de $n+1$ éléments de E est liée sur F, d'où $[E : F] \leq n$. ∎

Corollaire 3.1.3 ("maximalité du groupe de Galois") *Soit E/F une extension galoisienne finie du groupe $G = \{\sigma_1, \cdots, \sigma_n\}$. Tout automorphisme $\sigma \in \mathrm{Aut}(E)$ de E dont la restriction à F est l'identité, appartient à G.*

Preuve : Soit n le cardinal du groupe G ; d'après le théorème 3.1.2, on a $[E : F] = n$. Si σ n'appartenait pas à G, F serait le corps des fixes de $n+1$ automorphismes distincts de E, et d'après le corollaire 2.1.5, $[E : F] \geq n+1$, contradiction. ∎

Propriété d'injectivité

Corollaire 3.1.4 ("injectivité") *Soit E/F une extension galoisienne du groupe G, et soient H_1, H_2 deux sous-groupes de G. Si $B_1 = E^{H_1}$, $B_2 = E^{H_2}$, l'égalité des corps $B_1 = B_2$ entraîne l'égalité des groupes H_1 et H_2.*

PREUVE : Soit H_3 le sous-groupe de G engendré par H_1 et H_2 ; son corps des fixes $B_3 = E^{H_3}$ est inclus dans le corps $B_1 = B_2$. Mais tout élément de H_3 est un produit fini d'éléments de H_1 et H_2 : il fixe les éléments de $B_1 = B_2$, et on a donc $B_1 = B_2 = B_3$. On utilise alors le théorème 3.1.2 :

$$[E : B_3] = \operatorname{Card} H_3 = [E : B_1] = \operatorname{Card} H_1 = [E : B_2] = \operatorname{Card} H_2,$$

et les inclusions $H_3 \supset H_1$, $H_3 \supset H_2$ fournissent les égalités $H_1 = H_2 = H_3$. ∎

EXEMPLE 3.1.5 *On considère* $E = \mathbb{Q}(\sqrt[3]{2}, j)$, $\alpha = \sqrt[3]{2}$,

$$\begin{cases} \tau(\alpha) = \alpha, \\ \tau(j) = j^2, \end{cases} \quad \begin{cases} \sigma(\alpha) = j\alpha, \\ \sigma(j) = j. \end{cases}$$

Alors les morphismes $\{\mathrm{id}, \sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma\}$ *sont distincts :*

$$\begin{cases} \sigma\tau(\alpha) = j\alpha, \\ \sigma\tau(j) = j^2, \end{cases} \quad \begin{cases} \tau\sigma(\alpha) = j^2\alpha, \\ \tau\sigma(j) = j^2, \end{cases}$$

donc ils forment un groupe non commutatif G *d'ordre 6, car* $[E : \mathbb{Q}] = 6$. *Les sous-groupes* $H_1 = \{\mathrm{id}, \sigma\tau\}$ *et* $H_2 = \{\mathrm{id}, \tau\sigma\}$ *sont des sous-groupes distincts d'ordre 2, et leurs corps des fixes sont* $B_1 = \mathbb{Q}(\alpha + j\alpha)$ *et* $B_2 = \mathbb{Q}(\alpha + j^2\alpha)$. *En effet,* $\sigma\tau(\alpha + j\alpha) = \alpha + j\alpha = -j^2\alpha$, $\tau\sigma(\alpha + j^2\alpha) = \alpha + j^2\alpha = -j\alpha$.

Problème de Fermat : Pierre de Fermat (1601–1665)

a soulevé son problème célèbre (c.1637) dans la marge d'une traduction des "Arithmétiques" de Diophante :
"Décomposer un cube en deux autre cubes, une quatrième puissance, et généralement, une puissance quelconque, en deux puissances de même nom au-dessus de la seconde puissance, est une chose impossible et j'en ai assurément trouvé l'admirable démonstration. La marge trop exiguë ne la contiendrait pas".
En langage moderne :

$$\text{pour } n > 2 \quad \begin{cases} x^n + y^n = z^n \\ x, y, z \in \mathbb{Z} \end{cases} \quad \Longrightarrow xyz = 0 \qquad (FLT(n))$$

("Fermat's Last Theorem").

Cas $n = 4$ (Fermat lui-même dans une lettre à Huygens)

cas $n = 3$ (Euler en1753) ;

cas $n = 5$ (Dirichlet, Legendre, c.1825) ;

cas $n = 7$ (G.Lamé, 1839 ; $n = 14$ a déjà été fait par Dirichlet en 1832) ;

Le 11 mars 1847 G.Lamé informait l'Académie des Sciences de Paris d'une démonstration complète à la base de l'identité

$$x^p + y^p = (x+y)(x+\zeta y)\cdot\cdots\cdot(x+\zeta^{p-1}y), \quad \zeta = \zeta_p = \exp(2\pi i/p), p \neq 2$$

admettant la factorialité de l'anneau $\mathbb{Z}[\zeta_p]$ (c'est-à-dire, que la décomposition en facteurs premiers dans cet anneau soit unique).
Immédiatement J.Liouville dit : "N'y a-t-il pas là une lacune à remplir ?" (et quelques mois après A.Cauchy publia une note sur la non-factorialité de $\mathbb{Z}[\zeta_{23}]$).

L'idée de divisibilité dans les anneaux a beaucoup influencé la théorie des nombres.

Travail de E.Kummer

E.Kummer en 1847 a défini un *p régulier* :

$$\text{pout tout idéal } I \subset \mathbb{Z}[\zeta_p] \quad \Big(I^p \text{ principal} \Longrightarrow I \text{ principal}\Big).$$

(en langage moderne), et il a démontré FLT(p) pour tout p régulier (la Médaille d'Or de l'Académie des Sciences en 1850). Le plus petit nombre premier irrégulier est $p = 37$, voir [He97].

3.2 Extensions séparables

Définition 3.2.1 (i) *Soit K un corps ; on dit qu'un polynôme $P \in K[X]$ est séparable, s'il n'existe pas d'extension L de K, dans laquelle P admet une racine multiple.*

(ii) *Soit E/K une extension de corps. L'élément $\alpha \in E$ est dit séparable sur K s'il existe un polynôme $P \in K[X]$ séparable tel que $P(\alpha) = 0$.*

(iii) *Enfin, l'extension E/K est séparable si tout élément $\alpha \in E$ est séparable sur K*

Proposition 3.2.2 *Soient K un corps, et P un élément de $K[X]$.*

(i) *Si P est premier avec son polynôme dérivé P', alors le polynôme P est séparable.*

(ii) *Si P est irréductible et K de caractéristique nulle, le polynôme P est séparable.*

Preuve : (i) Soit α une racine de P dans une extension L de K ; dans $L[X]$, on a les égalités :

$$P(X) = (X-\alpha)^m g(X), \text{ avec } m \geq 1, g(\alpha) \neq 0$$

et

$$P'(X) = (X-\alpha)^{m-1}[mg(X) + (X-\alpha)g'(X)].$$

D'autre part, comme P et P' sont premiers entre eux dans $K[X]$, il existe u et v dans $K[X]$ tels que

$$uP + vP' = 1$$

On obtient l'égalité dans $L[X]$:

$$u(X)(X-\alpha)^m g(X) + v(X)(X-\alpha)^{m-1}[mg(X) + (X-\alpha)g'(X)] = 1.$$

On constate, en donnant à X une valeur α, que pour $m \geq 2$ on a une contradiction : $0 = 1$. Dans toute extension de K , P ne possède que des racines simples, c'est un polynôme séparable.

(ii) Rappelons que si K est un corps d'élément unité 1_K, sa caractéristique est l'entier $q \geq 0$ qui engendre l'idéal $\operatorname{Ker}\varphi$ de $\mathbb{Z}$, où φ est le morphisme d'anneaux de $\mathbb{Z}$ dans K défini par $\varphi(n) = n1_K$. Donc si K est un corps de caractéristique nulle, le polynôme dérivé d'un polynôme non constant est non nul, et si P est un élément irréductible de $K[X]$, il est premier avec son polynôme dérivé. ∎

Exemple. On considère le corps $K = \mathbb{Z}/p\mathbb{Z}$, et un entier naturel n. Le polynôme $P(X) = X^{p^n} - X$ de $K[X]$, de polynôme dérivé -1, est séparable. Mais pour tout $a \in K$, le polynôme $g(X) = X^{p^n} - a$ ne l'est pas : $g(X) = (X - a)^{p^n}$.

Théorème 3.2.3 *Toute extension galoisienne est algébrique et séparable. Plus précisément, soit E/F une extension galoisienne de groupe de Galois $G = \{\sigma_1, \cdots, \sigma_r\}$. Si α est un élément de E, on note $\alpha_1 = \alpha$, $\alpha_2, \cdots, \alpha_r$ les* images distinctes *de α par les $\sigma_i \in G$.*

Alors $p(X) = (X - \alpha_1)\cdot\ldots\cdot(X - \alpha_r)$ est un polynôme séparable de $F[x]$ de racine α, et c'est le polynôme minimal de α sur F.

Preuve : Comme G est un groupe d'automorphismes du corps E, chacun de ses éléments σ_i permute les α_j, donc les coefficients de p appartiennent à $E^G = F$; et par construction, le polynôme p est séparable.

Si $P \in F[X]$ est tel que $P(\alpha)$ soit nul, pour tout $\sigma_i \in G$ on a $P(\sigma_i(\alpha)) = \sigma_i(P(\alpha)) = 0$, donc P admet comme racines les éléments $\alpha_1, \cdots, \alpha_r$ de E, et p divise P. Le polynôme p est bien le polynôme minimal de α sur F, et il est irréductible dans $F[X]$ d'après la proposition 1.3.2. ∎

Corollaire 3.2.4 *Soit E/F une extension galoisienne de groupe de Galois $G\{\sigma_1, \cdots, \sigma_r\}$. Si $\alpha \in E$ est de polynôme minimal p sur F, tout polynôme irréductible dans $F[X]$ de racine α est de la forme $ap(X)$ avec $a \in F^*$.*

Exercices

3.1 On considère les sous-corps $E_1 = \mathbb{Q}(\sqrt[3]{2})$, $E_2 = \mathbb{Q}(j)$ de $E = \mathbb{Q}(\sqrt[3]{2}, j)$, $\alpha = \sqrt[3]{2}$. Trouver les sous-groupes U_1 et U_2 de $\operatorname{Aut}(E)$ tels que $E^{U_1} = E_1$, $E^{U_2} = E_2$.

Cours N°4. Le jeudi 10 février 2005

(disponible à l'adresse : `http ://www-fourier.ujf-grenoble.fr /~panchish`)

4 Propriété de surjectivité

Rappelons qu'une extension de corps E/F est un couple, formé par deux corps $E \supset F$ (c'est une notation traditionnelle, ne pas confondre avec le groupe quotient !)

DÉFINITION 3.1.1(rappel). On se donne un corps E, et le groupe Aut$E$ de tous les automorphismes de E. Soit

$$G = \{\sigma_1, \cdots, \sigma_n\}$$

un sous-groupe fini de Aut$E$. On appelle extension galoisienne de groupe de Galois G l'extension E/F, où $F = E^G$ est le corps des fixes par G.

THÉORÈME 3.1.2(rappel). Soient $G = \{\sigma_1, \cdots, \sigma_n\}$ un sous-groupe fini de Aut$E$ et E/F extension galoisienne associée. Alors $[E : F] = n$.

4.1 Enoncé du résultat

THÉORÈME 4.1.1 ("SURJECTIVITÉ") *Soit E/F une extension galoisienne de groupe de Galois $G = \{\sigma_1, \cdots, \sigma_n\}$. Pour tout corps intermédiaire B, $(E \supset B \supset F)$, il existe un sous-groupe H de G tel que B soit égal à E^H.*

PREUVE : On vérifie aisément que l'ensemble des $\sigma \in G$, tels que $\sigma(b) = b$ pour tout $b \in B$, est un sous-groupe H de G. Soit $\{\sigma_1, \cdots, \sigma_s\}$ un système exact de représentants des classes à gauche de G modulo H ; les restrictions des σ_i à B sont des morphismes de corps distincts de B dans E, de corps des fixes F. Donc d'après le théorème 2.2.2 sur le corps des fixes, on a $[B : F] \geq s$. Posons $B' = E^H$: par construction de H, B' contient B. Et d'après le théorème 2.2.2,

$$[E : B] = \frac{[E : F]}{[B : F]} \leq \frac{\text{Card}\, G}{s} = \text{Card}\, H = [E : B'],$$

on en déduit l'inclusion $B' \subset B$, donc l'égalité $B = B'$. ∎

COROLLAIRE 4.1.2 *Soit E/F une extension galoisienne de groupe de Galois $G = \{\sigma_1, \cdots, \sigma_n\}$. Il existe une bijection Φ entre l'ensemble des sous-groupes H de G et l'ensemble des extensions intermédiaires B de E/F $(E \supset B \supset F)$, définie par l'égalité : $\Phi(H) = E^H$.*

PREUVE : L'injectivité de Φ découle du théorème 3.1.2, et la surjectivité de Φ découle du théorème 4.1.1).

L'application Φ est une bijection entre :

$$\Phi : \left\{ \begin{array}{c} \text{L'ensemble des} \\ \text{sous-groupes } H \subset G \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{L'ensemble des corps} \\ \text{intermédiaires } B \subset E, B \supset F \end{array} \right\}$$

4.2 Exemples : fractions rationnelles symétriques

EXEMPLE 4.2.1 *Etant donné un corps k, on considère le corps $E = k(x)$ des fractions rationnelles à coefficients dans k. On définit des applications de E dans E par :*

$$\sigma_1(f(x)) = f(x)(\sigma_1 = \mathrm{id}); \qquad \sigma_4(f(x)) = f(1 - \frac{1}{x}) = \sigma_2[\sigma_3(f(x))] \ (\sigma_4^3 = \mathrm{id});$$
$$\sigma_2(f(x)) = f(\frac{1}{x}) \ (\sigma_2^2 = \mathrm{id}); \quad \sigma_5(f(x)) = f(\frac{1}{1-x}) = \sigma_3[\sigma_2(f(x))] \ (\sigma_5^3 = \mathrm{id});$$
$$\sigma_3(f(x)) = f(1-x)(\sigma_3^2 = \mathrm{id}); \sigma_6(f(x)) = f(\frac{x}{x-1}) = \sigma_2[\sigma_3(\sigma_2(f(x)))] \ (\sigma_6^2 = \mathrm{id}).$$

Les applications $\sigma_1, \sigma_2, \sigma_3$ sont des automorphismes du corps E, et par composition, donc les applications $\sigma_4, \sigma_5, \sigma_6$ aussi (on compose les applications de droite à gauche). Soit G l'ensemble de ces σ_i, muni de la composition. Alors G est un sous-groupe non commutatif d'ordre 6 de Aut$E$ *: il est isomorphe à S_3. Posons $F = E^G$: d'après le théorème 3.1.2, on a $[E : F] = 6$. Cherchons à préciser les éléments de F.*

En effet, comme G est engendré par σ_2 et σ_3, pour vérifier qu'un élément appartient à F, il suffit de contrôler qu'il est fixé par σ_2 et σ_3 ; c'est le cas de $I = \dfrac{(x^2-x+1)^3}{x^2(1-x)^2}$. Donc $k(I)$ est inclus dans F. D'autre part, x est racine du polynôme de degré 6 à coefficients dans $k(I)$:

$$(x^2 - x + 1)^3 - Ix^2(1-x)^2.$$

Donc $[E : k(I)] \leq 6$, et comme $F \supset k(I)$, $[E : F] \geq 6$, et $6 \leq [E : F] \leq [E : k(I)] \leq 6$, il vient $[E : F] = [E : k(I)] = 6$, donc $F = k(I)$, $G = \mathrm{Aut}(E/F)$ par la maximalité (le corollaire 3.1.3).

REMARQUE 4.2.2 (L'ACTION DES HOMOGRAPHIES SUR LES FRACTIONS RATIONNELLES) *Pour toute homographie $\sigma : x \mapsto \dfrac{ax+b}{cx+d}$ $(ad - bc \neq 0)$ posons*

$$(\sigma f)(x) = f(\sigma^{-1}(x)) \ \textit{alors} \ \sigma(\tau f) = (\sigma\tau)f.$$

Le groupe G s'identifie alors avec le sous-groupe

$$G \cong \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \right\} \cong S_3,$$

et G agit sur $\{0, 1, \infty\} \subset \mathbb{P}^1_K$ par permutations.

EXEMPLE 4.2.3 *Soit $E = k(x_1, \cdots, x_n)$ le corps des fractions rationnelles en n variables sur un corps k. Le groupe symétrique S_n opère sur E par :*

$$\sigma f(x_1, \cdots, x_n) = f(x_{\sigma^{-1}(1)}, \cdots, x_{\sigma^{-1}(n)})$$

pour $f \in E$ et $\sigma \in S_n$.

Cherchons à décrire le corps F des fractions rationnelles symétriques : $F = E^{S_n}$. D'après le théorème 3.1.2, on a l'égalité $[E : F] = \mathrm{Card}\, S_n = n!$. D'autre part, le corps F contient les polynômes symétriques élémentaires

$$s_i = \sum_{1 \leq j_1 < \cdots < j_i \leq n} x_{j_1} \cdot \ldots \cdot x_{j_i}$$

des éléments $x_1, \cdots, x_n$; si l'on pose $L = k(s_1, \cdots, s_n)$, on a l'inclusion $L \subset F \subset E$. On considère le polynôme

$$f(t) = (t - x_1)\cdot\ldots\cdot(t - x_n) = t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n \in L[t] \subset F[t].$$

Pour montrer $L = F$ on introduit ensuite les corps intermédiaires :

$$L_i = L(x_{i+1}, \cdots, x_n) = L_{i+1}(x_{i+1}), \quad L = L_n \subset L_{n-1} \subset \cdots \subset L_1 \subset L_0 = E,$$

et d'après le corollaire 1.2.3 on a l'égalité :

$$[E : L] = [L_0 : L_1] \cdot [L_1 : L_2]\cdot\ldots\cdot[L_{n-1} : L_n] \geq [E : F] = n!.$$

On voit que $[L_{i-1} : L_i] \leq i$ à l'aide du polynôme

$$f_i(t) = \frac{f(t)}{(t - x_{i+1})\cdot\ldots\cdot(t - x_n)} \in L_i[t] \text{ de racine } t = x_i.$$

Comme le polynôme $f_i(t)$ de $L_i[t]$ est de degré i et admet x_i comme racine, on a
$[L_{i-1} : L_i] \leq i$, donc nécessairement $[L_{i-1} : L_i] = i$, $L = F$; $f_i(t)$ est le polynôme minimal de x_i sur L_i, et L_{i-1} est le L_i-espace vectoriel de base $\{1, x_i, \cdots, x_i^{i-1}\}$.

PROPOSITION 4.2.4 a) $[L_{i-1} : L_i] = i$, $L_{i-1} = \langle 1, x_i, x_i^2, \cdots, x_i^{i-1}\rangle_{L_i}$,
b) $E = \langle x_1^{\nu_1}\cdot\ldots\cdot x_n^{\nu_n} \mid \nu_i \leq i - 1\rangle_L$ *(une base sur $L = L_n$)*
c) *tout* polynôme $g(x_1, \cdots, x_n) \in k[x_1, \cdots, x_n]$ *est une combinaison linéaire sur L de* monômes $x_1^{\nu_1}\cdot\ldots\cdot x_n^{\nu_n}$ *avec $\nu_i \leq i - 1$, et les coefficients sont des* polynômes *de $s_1, \cdots, s_n$.*
d) $k[x_1, \cdots, x_n]^{S_n} = k[s_1, \cdots, s_n]$

PREUVE : a) On a $[L_{i-1} : L_i] \leq i$, et

$$[E : L] = [L_0 : L_n] = [L_0 : L_1][L_1 : L_2]\cdot\ldots\cdot[L_{n-1} : L_n] \leq n! = [E : F],$$

donc $[L_{i-1} : L_i] = i$ pour $i = 1, \cdots, n$.
b) Découle de la preuve du théorème 1.2.2 sur la multiplicativité du degré.
c) On montre que pour tout $l \geq i$ le monôme x_i^l est un polynôme de $x_i, \cdots, x_n$ sur l'anneau $A = k[s_1, \cdots, s_n]$ dans lequel x_j entre avec une puissance $\leq j - 1$, puisque $f_i(x_i) = 0$ (on raisonne par récurrence sur i et l). Plus précisément, on utilise la division euclidienne par un polynôme unitaire :

$$f_i(t) = \frac{f(t)}{(t - x_{i+1})\cdot\ldots\cdot(t - x_n)} = t^i + a_{1,i}t^{i-1} + \cdots + a_{i,i} \in A_i[t] \text{ où}$$
$$A_i = A[x_{i+1}, \cdots, x_n] = k[s_1, \cdots, s_n][x_{i+1}, \cdots, x_n],$$

Par exemple :

- Si $i = 1$,

$$f_1(t) = t - x_1 = t - (s_1 - x_2 \cdots - x_n) \Longrightarrow x_1 = s_1 - x_2 - \cdots - x_n \in k[x_2, \cdots, x_n][s_1, \cdots s_n].$$

- Si $i = 2$, posons

$$(t - x_3)\cdot\ldots\cdot(t - x_n) = t^{n-2} - s_1' t^{n-3} + \cdots + (-1)^{n-2} s_{n-2}' \in L_2[t], \text{ donc}$$

$$f_2(t) = t^2 - (x_1+x_2)t + x_1x_2 = t^2 - (s_1 - x_3\cdots - x_n)t + s_2 - s_2' - (x_1+x_2)(x_3+\cdots+x_n)$$
$$= t^2 - (s_1 - x_3\cdots - x_n)t + s_2 - s_2' - (s_1 - x_3 + \cdots - x_n)(x_3 + \cdots x_n)$$
$$f_2(x_2) = 0 \Longrightarrow$$
$$x_2^2 = (s_1 - x_3 - \cdots - x_n)x_2 - s_2 + s_2' + (s_1 - (x_3 + \cdots + x_n))(x_3 + \cdots + x_n), \text{ etc.}$$

d)⇐c) : on développe tout polynôme $g(x_1, \cdots, x_n) \in k[x_1, \cdots, x_n]^{S_n}$ en base $x_1^{\nu_1}\cdot\ldots\cdot x_n^{\nu_n}$ sur le corps $F = k(s_1, \cdots, s_n)$ (avec $\nu_i \leq i-1$).

Grâce à c), les coefficients de ce développement sont des polynômes de $s_1, \cdots, s_n$. Il reste à remarquer que ce développement est unique.

4.3 Étude du corps de décomposition dans $\mathbb{C}$ de $X^3 - 2$

Si l'on pose $j = \exp(2i\pi/3)$, $\alpha = \sqrt[3]{2}$, les racines de $X^3 - 2$ sont $\alpha, j\alpha, j^2\alpha$. On considère $E = \mathbb{Q}(\sqrt[3]{2}, j) = \mathbb{Q}(\alpha, j\alpha, j^2\alpha)$, et les automorphismes

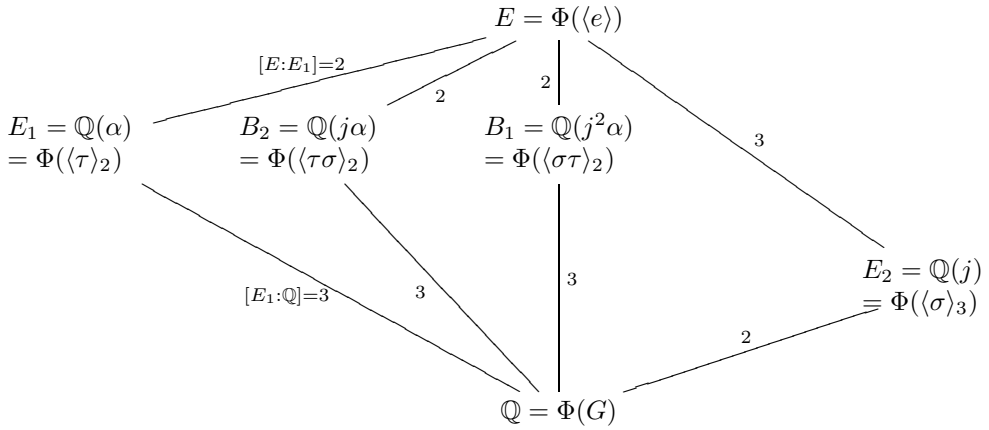
$$\begin{cases}\tau(\alpha) = \alpha,\\ \tau(j) = j^2,\end{cases} \quad \begin{cases}\sigma(\alpha) = j\alpha,\\ \sigma(j) = j.\end{cases}$$

Alors les morphismes $\{\mathrm{id}, \sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma\}$ sont distincts :

$$\begin{cases}\sigma\tau(\alpha) = j\alpha,\\ \sigma\tau(j) = j^2,\end{cases} \quad \begin{cases}\tau\sigma(\alpha) = j^2\alpha,\\ \tau\sigma(j) = j^2,\end{cases}$$

donc ils forment un groupe non commutatif G d'ordre 6, car $[E : \mathbb{Q}] = 6$. Les sous-groupes $H_1 = \{\mathrm{id}, \sigma\tau\}$ et $H_2 = \{\mathrm{id}, \tau\sigma\}$ sont des sous-groupes distincts d'ordre 2, et leurs corps des fixes sont $B_1 = \mathbb{Q}(\alpha + j\alpha)$ et $B_2 = \mathbb{Q}(\alpha + j^2\alpha)$. En effet, $\sigma\tau(\alpha + j\alpha) = \alpha + j\alpha = -j^2\alpha$, $\tau\sigma(\alpha + j^2\alpha) = \alpha + j^2\alpha = -j\alpha$.

Terminons par un dessin représentant les extensions intermédiaires de $E/\mathbb{Q}$:



Cours N°5. Le jeudi 17 février 2005

5 Correspondance de Galois

5.1 Théorème fondamental

Soit E/F une extension galoisienne de groupe $G = \{\sigma_1, \cdots, \sigma_n\}$ (un sous-groupe fini de Aut$E$). Pour tout sous-groupe $H \subset G$ on pose $B = E^H = \Phi(H)$

THÉORÈME FONDAMENTAL 5.1.1 *1) L'application Φ est une bijection entre :*

$$\Phi : \left\{ \begin{array}{c} \textit{L'ensemble des} \\ \textit{sous-groupes } H \subset G \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \textit{L'ensemble des} \\ \textit{corps intermédiaires } B \subset E \end{array} \right\}$$

2) $[E : B] = |H|$
3) Soit G/H l'ensemble des classes à gauche de G par rapport à H. Alors $[B : F] = |G/H| = (G : H) = s = n/r$, où $n = |G|$, et $r = |H|$.
4) La sous-extension B/F est galoisienne si et seulement si $H \triangleleft G$ (un sous-groupe distingué).

PREUVE : 1) $\Leftarrow$ les théorèmes d'injectivité et de surjectivité (le corollaire 3.1.4 et le corollaire 4.1.2).
2) $\Leftarrow$ la définition de Φ et le théorème 3.1.2.
3) $\Leftarrow$ la multiplicativité du degré : par le théorème 1.2.2,

$$[B : F] = \frac{[E : F]}{[E : B]} = \frac{n}{r} = s.$$

4) On considère tous les morphismes de corps $\sigma' : B \to E$ sur F, tels que $\sigma'|_B = \sigma|_B$:

$$\begin{array}{lccc} \sigma : & E & \longrightarrow & E \\ & \cup & & \cup \\ \sigma' : & B & \longrightarrow & \sigma(B) \\ & \cup & & \cup \\ & F & \longrightarrow & F \end{array} \quad \Rightarrow \quad \begin{array}{l} \forall \sigma \in G, \text{ il existe } i, \sigma = \sigma_i, \text{ et } \sigma_i H = \sigma_j H \Longleftrightarrow \\ {\sigma_j}^{-1}\sigma_i H = H \Longleftrightarrow \sigma_i|_B = \sigma_j|_B. \end{array}$$

Ceci implique qu'on dispose *d'au moins* s morphismes distincts : $|\{\sigma' : B \hookrightarrow E\}| \geq [B : F]$. D'autre part, $[B : F] \geq |\{\sigma' : B \hookrightarrow E\}|$ par le théorème 3.1.2, donc $[B : F] = |\{\sigma' : B \hookrightarrow E\}| = s$.

- Si B est galoisienne, alors $\text{Aut}(B/F) = [B : F] = s$, d'où

$$\forall \sigma \in G, \sigma|_B \in \text{Aut}(B/F) \Rightarrow \sigma(B) = B \Rightarrow \sigma H \sigma^{-1}(\sigma(B)) = B$$

  Par la bijectivité 1), on obtient $\sigma H \sigma^{-1} = H \Rightarrow H \triangleleft G$.
- Réciproquement,

$$H \triangleleft G \Rightarrow \forall \sigma \in G, \sigma H \sigma^{-1}(\sigma(B)) = B \Rightarrow \Phi^{-1}(\sigma(B)) = H = \Phi^{-1}(B)$$
$$\Rightarrow \text{Aut}(B/F) \cong G/H \Rightarrow B/F \text{ est galoisienne de groupe } G/H.$$

5.2 Composé de corps

Complétons le théorème fondamental 5.1.1 en introduisant le composé de deux extensions intermédiaires.

DÉFINITION 5.2.1 *Soient L/K une extension de corps, E et E' deux corps intermédiaires. On appelle le* composé *de E et E', noté $E \cdot E'$, le sous-corps $K(E, E')$, c'est-à-dire, le sous-corps minimal de L contenant K, E et E'.*

PROPOSITION 5.2.2 *Soient L/K une extension galoisienne de groupe de Galois G, et E et E' deux extensions intermédiaires. On note encore Φ la bijection du théorème 5.1.1.*
(i) *Si $\Phi^{-1}(E) = H$, $\Phi^{-1}(E') = H'$, alors $\Phi^{-1}(E \cdot E') = H \cap H'$, et $\Phi^{-1}(E \cap E') = H''$, le sous-groupe de G, engendré par H et H'.*
(ii) *Si l'extension E'/K est galoisienne, l'extension $E{\cdot}E'/E$ l'est aussi, de groupe de Galois* $\mathrm{Gal}(E{\cdot}E'/E)$, *isomorphe à* $\mathrm{Gal}(E'/E \cap E')$. *Un isomorphisme φ est donné par :*

$$\begin{array}{rccccc} \varphi : & \mathrm{Gal}(E \cdot E'/E) & \xrightarrow{\sim} & \mathrm{Gal}(E'/E \cap E') & \subset & \mathrm{Gal}(E'/K) \\ & \sigma & \longmapsto & \sigma|_{E'} \text{ (la restriction de } \sigma \text{ à } E') & & \end{array}$$

(iii) *Si les extensions E'/K et E/K sont galoisiennes, l'extension $E \cdot E'/K$ l'est aussi, de groupe de Galois* $\mathrm{Gal}(E \cdot E'/K)$, *isomorphe à un sous-groupe de* $\mathrm{Gal}(E/K) \times \mathrm{Gal}(E'/K)$, *par le morphisme injectif ψ donné par :*

$$\begin{array}{rccc} \psi : & \mathrm{Gal}(E \cdot E'/K) & \longrightarrow & \mathrm{Gal}(E/K) \times \mathrm{Gal}(E'/K) \\ & \sigma & \longmapsto & (\sigma|_E, \sigma|_{E'}) \end{array}$$

De plus, ψ est un isomorphisme lorsque $E \cap E' = K$.

PREUVE :
(i) Par définition du composé de deux corps, $E \cdot E'$ est inclus dans $L^{H \cap H'}$. D'autre part, le groupe de Galois $\mathrm{Gal}(L/E \cdot E')$ est inclus dans $H \cap H'$, donc $E \cdot E'$ contient $L^{H \cap H'}$. De plus, $E \cap E'$ est inclut dans $L^{H''}$. D'autre part, le groupe de Galois $\mathrm{Gal}(L/E \cap E')$ est inclut dans H'', donc $E \cap E'$ contient $L^{H''}$.
(ii) Si l'extension E'/K est galoisienne, le sous-groupe H' est distingué dans G. L'extension L/E est galoisienne de groupe de Galois H, et $E \cdot E'$ est l'extension intermédiaire, le corps des fixes de $H \cap H'$, qui est un sous-groupe distingué de H. Donc l'extension $(E \cdot E')/E$ est galoisienne par le théorème fondamental 5.1.1, 4).

L'application φ qui, à un élément de $\mathrm{Gal}(E \cdot E'/E)$ associe sa restriction à E', est bien un morphisme de groupes. Pour prouver sa surjectivité, on remarque que :

$$(E')^{\mathrm{Im}\varphi} = (E \cdot E')^{\mathrm{Gal}(E \cdot E'/E)} \cap E' = E \cap E'.$$

Enfin, si σ est un élément de $\mathrm{Gal}(E \cdot E'/E)$ d'image par φ triviale, σ fixe tout élément de E et tout élément de E', donc le corps $E \cdot E'$. L'application φ est bien injective.
(iii) Si les extensions E'/K et E/K sont galoisiennes, les sous-groupes H et H' sont distingués dans G, donc $H \cap H'$ est aussi distingué dans G (pour tout $x \in H \cap H'$ et tout $g \in G$, gxg^{-1} appartient à H et H'). Ainsi l'extension $E \cdot E'/K$ est galoisienne de groupe de Galois isomorphe à $G/(H \cap H')$. Le morphisme de l'énoncé est en fait le morphisme de groupes

$$\begin{array}{rccc} \psi : & G/(H \cap H') & \longrightarrow & G/H \times G/H' \\ & \sigma & \longmapsto & (\sigma \bmod H, \sigma \bmod H') \end{array}$$

qui est bien injectif. Si l'on suppose de plus $E \cap E' = K$, alors d'après (i) on a $H'' = G = H \cdot H'$, ce qui prouve la surjectivité de ψ. ∎

EXERCICE. Donner un exemple avec $E \cdot E' \neq L$ et $E \cap E' \neq K$.

Cours N°6. Le jeudi 3 mars 2005

Composé de corps : rappels et exemples

DÉFINITION 5.2.1 Soient L/K une extension de corps, E et E' deux corps intermédiaires. On appelle le composé de E et E', noté $E \cdot E'$, le sous-corps $K(E, E')$, c'est-à-dire, le sous-corps minimal de L contenant K, E et E'.

Soient L/K une extension galoisienne de groupe de Galois G. On note encore Φ la bijection du théorème 5.1.1 :

$$\Phi : \left\{ \begin{array}{c} \text{L'ensemble des} \\ \text{sous-groupes } H \subset G \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{L'ensemble des} \\ \text{corps intermédiaires } B \subset E \end{array} \right\}$$

REMARQUE. Si $K \subset B \subset B' \subset L$ quatre corps emboîtés, $U = \Phi^{-1}(B) \supset U' = \Phi^{-1}(B')$ alors l'extension B'/B est galoisienne si et seulement si $U' \lhd U$, et $\mathrm{Gal}(B'/B) \cong U/U'$.

PROPOSITION 5.2.2 Soient E et E' deux extensions intermédiaires. (i) Si $\Phi^{-1}(E) = H$, $\Phi^{-1}(E') = H'$, alors $\Phi^{-1}(E \cdot E') = H \cap H'$, et $\Phi^{-1}(E \cap E') = H''$, le sous-groupe de G, engendré par H et H'.
(ii) Si l'extension E'/K est galoisienne, l'extension $E \cdot E'/E$ l'est aussi, de groupe de Galois $\mathrm{Gal}(E \cdot E'/E)$, isomorphe à $\mathrm{Gal}(E'/E \cap E')$:

$$\mathrm{Gal}((E \cdot E')/E) \cong \mathrm{Gal}(E'/E \cap E') \Longleftrightarrow H/(H \cap H') \cong (H' \cdot H)/H'$$

(rappelons que $\mathrm{Gal}(E'/K) \cong G/H'$, $H' \lhd G$, $H \cap H' \lhd H$, et $H' \lhd H' \cdot H$).
(iii) Si les extensions E'/K et E/K sont galoisiennes, l'extension $E \cdot E'/K$ l'est aussi, de groupe de Galois $\mathrm{Gal}(E \cdot E'/K)$, isomorphe à un sous-groupe de $\mathrm{Gal}(E/K) \times \mathrm{Gal}(E'/K)$ par le morphisme injectif ψ :

$$\begin{array}{ccccccc} \psi : G/(H \cap H') & \hookrightarrow & G/H \times G/H' & \qquad & \mathrm{Gal}(E \cdot E'/K) & \longrightarrow & \mathrm{Gal}(E/K) \times \mathrm{Gal}(E'/K) \\ \sigma(H \cap H') & \longmapsto & (\sigma H, \sigma H') & & \sigma & \longmapsto & (\sigma|_E, \sigma|_{E'}) \end{array}$$

Dans ce cas, $H \lhd G$, $H' \lhd G$, donc $H \cap H' \lhd G$.
De plus, ψ est un isomorphisme lorsque $E \cap E' = K$, c'est-à-dire, si $H \cdot H' = G$.

EXEMPLE 5.2.3 *Soit k un corps. Considérons $L = k(x_1, x_2, x_3, x_4)$, $K = k(s_1, s_2, s_3, s_4)$. Alors $G = \mathrm{Gal}(L/K) \cong S_4$, et $E = K(x_4)$ coïncide avec le corps des fixes du sous-groupe $S_3 \subset S_4$, et $[E : K] = |G/H| = 4$, mais $H \not\lhd G$. De plus, on peut construire le corps des fixes E' du sous-groupe distingué*

$$H' = \{e, (12)(34), (13)(24), (14)(23)\} \lhd G$$

de manière suivante. Considérons les images de l'élément $\alpha = x_1 x_2^2 x_3^3 x_4^4 \in K$ par G qui sont toutes distinctes, alors

$$E' = K(\beta), \text{ où } \beta = \sum_{\sigma \in H'} \sigma(\alpha) = x_1 x_2^2 x_3^3 x_4^4 + x_1^2 x_2 x_3^4 x_4^3 + x_1^3 x_2^4 x_3 x_4^2 + x_1^4 x_2^3 x_3^2 x_4.$$

Dans ce cas $E \cdot E' = L = \Phi^{-1}(H \cap H') = \Phi^{-1}(\{e\})$, et $E \cap E' = K = \Phi^{-1}(H \cdot H') = \Phi^{-1}(G)$.

EXERCICE. Donner un exemple d'un corps intermédiaire B tel que avec $B \cdot E' \neq L$ et $B \cap E' \neq K$. (INDICATION : trouver B avec $\Phi^{-1}(B) = \langle (1,2,3,4) \rangle_4$).

5.3 Caractérisation des extensions galoisiennes

THÉORÈME 5.3.1 *Pour toute extension de corps E/K, on note* $\mathrm{Aut}(E/K)$ *le groupe des automorphismes de E dont la restriction à K est l'identité.*

L'extension finie E/K est galoisienne si et seulement si le groupe $\mathrm{Aut}(E/K)$ *est d'ordre* $[E:K]$.

PREUVE : Supposons E/K galoisienne, de groupe de Galois G, d'après le corollaire 3.1.3, G est égal à $\mathrm{Aut}(E/K)$. Donc $\mathrm{Card}\,\mathrm{Aut}(E/K) = \mathrm{Card}\,G = [E:K]$.

Réciproquement, si $[E:K] = \mathrm{Card}\,\mathrm{Aut}(E/K)$, posons $H = \mathrm{Aut}(E/K)$. Alors K est inclus dans E^H, d'après le théorème fondamental, on a $[E:E^H] = \mathrm{Card}\,H = [E:K]$, et l'extension E/K est bien galoisienne de groupe de Galois H. ∎

REMARQUE 5.3.2 *D'après le théorème 5.3.1, on a toujours* $[E:K] \geq \mathrm{Card}\,\mathrm{Aut}(E/K)$. *Donc si l'extension E/K n'est pas galoisienne, nécessairement* $[E:K] > \mathrm{Card}\,\mathrm{Aut}(E/K)$.

EXEMPLE 5.3.3 *Si $E = \mathbb{Q}(\sqrt[4]{2})$, l'extension $E/\mathbb{Q}$ n'est pas galoisienne. En effet, si $\alpha = \sqrt[4]{2}$, le polynôme minimal de α sur $\mathbb{Q}$ est $X^4 - 2$, et $[E:\mathbb{Q}] = 4$. De plus, comme $\{1, \alpha, \alpha^2, \alpha^3\}$ est une base de E sur $\mathbb{Q}$, tout élément σ de* $\mathrm{Aut}(E/\mathbb{Q})$ *est caractérisé par $\sigma(\alpha)$ qui est une racine de*

$$X^4 - 2 = (X-\alpha)(X+\alpha)(X-i\alpha)(X+i\alpha).$$

Comme E est un corps réel, $\sigma(\alpha)$ ne peut être égal qu'à $\pm\alpha$, et $\mathrm{Card}\,\mathrm{Aut}(E/K) = 2$.

THÉORÈME 5.3.4 *L'extension de corps E/K est galoisienne si et seulement si E est un* corps de décomposition *d'un polynôme séparable $P \in K[X]$.*

PREUVE : • Soit E un corps de décomposition d'un polynôme séparable, $P \in K[X]$. Si l'on note n le degré de P, et $\alpha_1, \cdots, \alpha_n$ les racines de P, dans E, on a les inclusions :

$$E = K(\alpha_1, \cdots, \alpha_n) \supset K(\alpha_1, \cdots, \alpha_{n-1}) \supset \cdots \supset K(\alpha_1) \supset K, \text{ et}$$

$$[K(\alpha_1):K] \leq n, [K(\alpha_1,\alpha_2):K(\alpha_1)] \leq n-1, \cdots [E:K(\alpha_1,\cdots,\alpha_{n-1})] = 1.$$

Par multiplicativité des degrés, on obtient $[E:K] \leq n!$, et on déduit du théorème 2.2.2 que le groupe $G = \mathrm{Aut}(E/K)$ est fini. Il reste à montrer que K est égal à E^G.

Désignons par r le nombre de racines de P n'appartenant pas à K : $r \geq 2$ (le cas $r = 1$ est impossible, car la somme des racines est un élément de K). Soit alors α_1 une racine de P non dans K, de polynôme minimal sur K P_1. Le polynôme P_1 divise P, il est donc séparable et admet s racines distinctes, qu'on note $\alpha_1, \cdots, \alpha_s$ $(2 \leq s \leq r)$. On peut donc construire s isomorphismes de corps $\sigma_i : K(\alpha_1) \to K(\alpha_i)$, tels que $\sigma(\alpha_1) = \alpha_i$, et que leur restriction à K soit l'identité. Et d'après le théorème 1.4.6, chaque σ_i se prolonge en isomorphisme τ_i de E.

Si $r = 2$, on a $s = 2$, $E = K(\alpha_1) = K(\alpha_1,\alpha_2)$, et $[E:K] = 2$. Comme on vient de construire deux automorphismes distincts de E laissant K fixe, d'après le théorème 5.3.1, l'extension E/K est galoisienne.

Raisonnons par récurrence sur $r > 2$, en supposant le résultat vrai pour tous les entiers inférieurs ou égaux à $r-1$. L'extension $E/K(\alpha_1)$ est donc galoisienne. Pour montrer l'égalité entre K et E^G, prenons un élément $\theta \in E$, fixé par tout élément de G ; θ est l'est en particulier par les éléments du groupe de Galois de $E/K(\alpha_1)$, donc il appartient à $K(\alpha_1)$:

$$\theta = c_0 + c_1\alpha_1 + \cdots + c_{s-1}\alpha_1^{s-1}, \text{ avec } c_i \in K.$$

Les prolongements τ_i, construits plus haut appartiennent à G : $\tau_i(\theta) = \theta$. Donc le polynôme de $E[X]$ de degré au plus $s-1$, $h(X) = c_{s-1}X^{s-1} + \cdots + c_1X + c_0 - \theta$, admet s racines distinctes $\alpha_1, \cdots, \alpha_s$. Cela entraîne que h est le polynôme nul, en particulier, $\theta = c_0 \in K$, $K = E^G$, et l'extension E/K est galoisienne.

• Réciproquement, supposons l'extension E/K galoisienne, et soit $\{\omega_1, \cdots, \omega_n\}$ une base de K-espace vectoriel E. Pour chaque i, on note P_i le polynôme minimal de ω_i sur K : d'après le théorème 3.2.3, si $\{\omega_i^{(j)}\}$ est l'ensemble des images distinctes de ω_i par les éléments de groupe de Galois de E/K, $P_i(X) = \prod_j (X - \omega_i^{(j)})$. Chaque P_i est séparable, tous les $\omega_i^{(j)}$ sont dans E, et E est le corps de décomposition du polynôme séparable P produit des P_i distincts. (Il est possible de construire beaucoup d'autres polynômes convenables P).

DÉFINITION 5.3.5 *On appelle* extension normale *une extension de corps E/K telle que pour toute extension L de K et tout couple (σ, τ) de morphisme de corps de E dans L fixant K, on ait $\sigma(E) = \tau(E)$.*

THÉORÈME 5.3.6 *Une extension finie E/K est galoisienne si et seulement si elle est normale et séparable.*

PREUVE • Supposons d'abord E/K galoisienne, de groupe de Galois G d'ordre n : d'après le théorème 5.3.4, E est le corps de décomposition d'un polynôme séparable $P \in K[X]$, et $E = K(\alpha_1, \cdots, \alpha_r)$, les α_i étant les racines de P. Soient L une extension de K, et σ un morphisme de corps de E dans L laissant K fixe : $\sigma(P(\alpha_i)) = P(\sigma(\alpha_i)) = 0$, donc $\sigma(\alpha_i)$ est une racine de P dans L. Comme σ est une application injective, on en déduit que $\sigma(E)$ est la sous-extension de L/K engendrée par les racines de P dans L ; l'image est indépendante du choix de σ, et E/K est normale. C'est aussi une extension séparable, d'après le théorème 3.2.3.

• Considérons maintenant une extension E/K de degré n, *normale et séparable*. Comme dans la démonstration du théorème précédant, on introduit une base $\{\omega_1, \cdots, \omega_n\}$ de E sur K, le polynôme minimal P_i de ω_i sur K, et le polynôme séparable P de $K[X]$, produit des P_i *distincts*. Si M est un corps de décomposition de P, l'extension M/K est galoisienne (on note G son groupe de Galois), et elle contient E. Donc pour vérifier que E/K est galoisienne, il suffit de montrer que le sous-groupe H de G, qui lui est associé par la correspondance de Galois, est distingué dans G. Or comme E/K est normale, pour tout $\sigma \in G$, on a $\sigma(E) = E$; donc pour tout $\sigma \in G$ et pour tout $x \in E$, il vient $\sigma h \sigma^{-1}$ appartient à H, H est distingué dans G et E/K est galoisienne.

REMARQUE 5.3.7 *Si E/K est un extension galoisienne, son groupe de Galois s'identifie à un sous-groupe d'un groupe symétrique. En effet, E est un corps de décomposition d'un polynôme séparable $P \in K[X]$, de racines $\alpha_1, \cdots, \alpha_r$. Tout élément $\sigma \in G$ est caractérisé par les $\sigma(\alpha_i) \in \{\alpha_1, \cdots, \alpha_r\}$, et G s'identifie à un sous-groupe de S_r.*

Troisième partie
Corps finis

6 Morphisme de Frobenius, structure des corps finis

6.1 Sous-groupes finis dans K^*

6.1.1 Exposant d'un groupe fini

DÉFINITION 6.1.1 *Soit G un groupe fini. On note $\omega(G)$, et on appelle* exposant *de G le ppcm des ordres des éléments de G. C'est le plus petit entier strictement positif tel que $x^{\omega(G)} = e$ pour tout élément $x \in G$. Alors par définition du ppcm, et par le théorème de Lagrange, $\omega(G)$ divise $|G|$.*

Soient K un corps *commutatif*, et G un sous-groupe fini de $K^\times$. Alors tout $x \in G$ est racine du polynôme $X^{\omega(G)} - 1$, et ce polynôme a au plus $\omega(G)$ racines dans le corps K. Par suite $\omega(G) \geq |G|$, donc $\omega(G) = |G|$.

LEMME 6.1.2 *Soit G un groupe. On suppose que $a, b \in G$ sont deux éléments tels que $ab = ba$, et qui sont d'ordre r et s, respectivement, où r et s sont premiers entre eux. Alors ab est d'ordre rs.*

C'est un fait général sur les éléments d'un groupe qui commutent entre eux.
PREUVE : Puisque $(ab)^{rs} = a^{rs}b^{rs} = 1$, l'ordre de ab est un diviseur $r_1 s_1$ de rs, où $r_1 \mid r$ et $s_1 \mid s$. Donc

$$a^{r_1 s_1} b^{r_1 s_1} = (ab)^{r_1 s_1} = 1.$$

On élève les deux parties en la puissance r_2, où $r_1 r_2 = r$. Alors

$$a^{r_1 r_2 s_1} b^{r_1 r_2 s_1} = 1,$$

donc, puisque $a^{r_1 r_2 s_1} = (a^{r_1 r_2})^{s_1} = 1$,

$$b^{r_1 r_2 s_1} = 1.$$

Ceci implique que $s \mid r_1 r_2 s_1$, et, car $\mathrm{pgcd}(s, r_1 r_2) = 1$, il vient que $s = s_1$. Un argument similaire montre que $r = r_1$, donc l'ordre de ab est rs.

PROPOSITION 6.1.3 *Dans un groupe commutatif, l'ensemble des ordres des éléments est stable par ppcm.*

PREUVE. Soient en effet x un élément d'ordre r et y un élément d'ordre s. Il s'agit de construire un élément d'ordre $\mathrm{ppcm}(r, s)$, soit m. Or on peut écrire $m = r's'$, où r' divise r, s' divise s, et les deux entiers sont premiers entre eux, puisque $\mathrm{ppcm}(r, s)\mathrm{pgcd}(r, s) = rs$. Par exemple, si

$$r = \prod_{i=1}^{k} p_i^{\alpha_i}, s = \prod_{i=1}^{k} p_i^{\beta_i}, \text{ on pose } r' = \prod_{\substack{i=1 \\ \alpha_i > \beta_i}}^{k} p_i^{\alpha_i}, s' = \prod_{\substack{i=1 \\ \alpha_i \leq \beta_i}}^{k} p_i^{\beta_i}.$$

De là on a $x^{r/r'}$ d'ordre r', et $y^{s/s'}$ d'ordre s', on peut donc appliquer le lemme 6.1.2 et conclure.

EXEMPLE.

$$r = 120 = 2^3 \cdot 3 \cdot 5, s = 180 = 2^2 \cdot 3^2 \cdot 5,\ r' = 8 = 2^3, s = 45 = 3^2 \cdot 5.$$

REMARQUE. Voici une autre construction pour la proposition 6.1.3 : (disponible à l'adresse cachée : `http ://www-fourier.ujf-grenoble.fr /~panchish/04ma1-maple`
dans le fichier 4ma1-13ppcm.mws) Notons $d = \text{pgcd}(r, s)$.

Il s'agit de construire un diviseur s' de s qui soit premier à r/d, et tel que
$r' := \text{ppcm}(r, s)/s'$ divise r. Pour ce faire, on part de $s' = s$ et on réécrit s' en $s'/\text{pgcd}(s', r/d)$ tant que ce pgcd $\neq 1$:

```
> restart;r:=120; s:=180;sprime:=s;
> i:=0;d:=gcd (r,s);
> while (gcd(sprime, r/d)<>1) do
> gcd(sprime, d);
> sprime:=(sprime/gcd(sprime, r/d));
> printf("i=%d,lcm=%d,sprime=%d, rprime=%d\n"
> ,i,
> lcm(r,s),sprime, lcm(r,s)/sprime);
> i:=i+1;od;
```

$$i := 0$$
$$sprime := 90$$

```
i=0,lcm=360,sprime=90, rprime=4
```

$$i := 1$$
$$sprime := 45$$

```
i=1,lcm=360,sprime=45, rprime=8
```

$$i := 2$$

Autrement dit, pour $r = 120, s = 180$, $d = \text{pgcd}(120, 180) = 60$, $r/d = 2$,

$$\text{ppcm}(120, 180) = 360 = 2 \cdot 180 = 4 \cdot 90 = 8 \cdot 45.$$

Application : $x^{r/r'}$ est d'ordre r', et $y^{s/s'}$ est d'ordre s', donc on peut utiliser le lemme 6.1.2.

Cyclicité des sous-groupes finis de $K^\times$

THÉORÈME 6.1.4 *Soit K un corps. Tout sous-groupe fini G de $K^\times$ est cyclique.*

PREUVE. Par définition du ppcm, et par le théorème de Lagrange, l'exposant $\omega(G)$ divise $|G|$, et tous les $x \in G$ sont solution de $x^{\omega(G)} = 1$, mais le polynôme $X^{\omega(G)} - 1$ possède au plus $\omega(G)$ racines dans le corps K. Donc, $\omega(G) = |G|$.

Il reste à montrer qu'il existe un élément d'ordre $\omega(G) = |G|$ dans G : on conclut avec la proposition 6.1.3.

REMARQUE. Pour un corps *non commutatif* le théorème 6.1.4 n'est plus valable, par exemple, on prend le groupe des *quaternions de Cayley*

$$G = Q_8 := \{\pm 1, \pm i, \pm j, \pm k \ \mid \ ij = k = -ji, jk = i = -kj, ki = j = -ik, i^2 = j^2 = k^2 = -1\}.$$

Dans ce cas $K = \mathbb{H}$ le corps des quaternions de Cayley.

REMARQUE. Pour un groupe non commutatif, il se peut que $\omega(G) = |G|$ (mais G n'est pas cyclique), par exemple, $G = S_3$, $\text{ppcm}(2, 3) = 6$.

Cours N°7. Le jeudi 10 mars 2005

6.2 Structure des corps finis

Jusqu'ici nous avons rencontré l'exemple fondamental des corps finis $\mathbb{Z}/p\mathbb{Z}$ (p premier), quotients de $\mathbb{Z}$ par un idéal maximal. Il s'agit maintenant de décrire tous les corps finis.

PROPOSITION-DÉFINITION 6.2.1 *Soit A un anneau commutatif de caractéristique p un nombre premier. L'application*

$$\mathrm{Fr}_p : x \mapsto x^p, x \in A$$

est un morphisme d'anneaux appelé morphisme de Frobenius. Plus généralement, si A est un anneau commutatif de caractéristique p premier et si q est une puissance de p, on note $\mathrm{Fr}_q : x \mapsto x^q$.

PREUVE. Le point à montrer est l'additivité. Or si $x, y \in A$ on développe $(x+y)^p$ par la formule du binôme, et on conclut par le fait que si $1 \leq i \leq p-1$, p divise l'entier C_p^i.

THÉORÈME 6.2.2 *Soit K un corps fini. Alors K est de caractéristique p un nombre premier, K est de cardinal $q = p^d$, avec $d = [K : \mathbb{Z}/p\mathbb{Z}]$, et Fr_p est un automorphisme du corps K.*

Inversement, si p est premier et d est un entier strictement positif, il existe à isomorphisme près un unique corps à $q = p^d$ éléments, qui est le corps de décomposition de $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$. On note ce corps $\mathbb{F}_q$. De plus, le groupe $(\mathbb{F}_q, +)$ est isomorphe au groupe $((\mathbb{Z}/p\mathbb{Z})^d, +)$ et le groupe multiplicatif $\mathbb{F}_q^*$ est isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$ (groupe cyclique d'ordre $q-1$).

PREUVE. Vérifions ensuite qu'un corps K à q éléments est un corps de décomposition pour le polynôme $X^q - X$. En effet, comme K a q éléments, K^* est un groupe d'ordre $q-1$. Par conséquent,

$$\forall x \in K^*,\ x^{q-1} = 1.$$

Autrement dit, les q éléments de K sont racines de $X^q - X$. Du fait du degré, on obtient

$$X^q - X = \prod_{\alpha \in K} (X - \alpha).$$

C'est-à-dire, tous les éléments du corps K sont des racines distincts du polynôme $X^q - X$, donc ce corps est forcément un corps *minimal* contenant telles racines. En particulier, K est un corps de décomposition pour le polynôme $X^q - X$.

Soit inversement K un corps de décomposition pour le polynôme $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$, où p est premier et q est une puissance de p. Comme Fr_q est un morphisme de corps de K, l'ensemble de ses points fixes les racines de $X^q - X$ est un sous-corps de K. Comme K est engendré par ces racines sur $\mathbb{F}_p$, K est l'ensemble des racines de $P(X) = X^q - X$. Comme $P' = -1$, toutes les racines de P sont simples (par les propriétés de la dérivée formelle P' d'un polynôme), P a donc ses q racines distinctes dans K et K a exactement q éléments. D'après 1.4.7 ceci établit l'assertion d'existence et unicité à isomorphisme près du corps $\mathbb{F}_q$.

Enfin la cyclicité du groupe $\mathbb{F}_q^*$ est un cas particulier du théorème 6.1.4. ∎

THÉORÈME 6.2.3 *: Soit $q = p^n$ où p est premier. Tout sous-corps du corps $\mathbb{F}_q$ est de cardinal p^m, où m est un diviseur de n. Et pour tout diviseur m de n, $\mathbb{F}_q$ possède un unique sous-corps de cardinal p^m, qui est l'ensemble des racines du polynôme $X^{p^m} - X$ dans $\mathbb{F}_q$.*

PREUVE. Si K est un sous-corps de $\mathbb{F}_q$, alors il contient le sous-corps premier $\mathbb{F}_p$, donc c'est une extension finie et $\mathbb{F}_q$ est une extension finie de K. De là K a pour cardinal p^m, et le cardinal de $\mathbb{F}_q$ est une puissance de $(p^m)^d$ de celui de K. Ainsi $n = md$. Inversement, si m divise n, alors $p^m - 1$ divise $p^n - 1$, donc le polynôme $X^{p^m-1} - 1$ divise le polynôme $X^{p^n-1} - 1$, donc le polynôme $X^{p^m} - X$ divise $X^{p^n} - X$, ce qui entraîne que $X^{p^m} - X$ a p^m racines distinctes dans $\mathbb{F}_q$. Ces racines forment l'unique sous-corps de cardinal p^m de $\mathbb{F}_q$. ∎

THÉORÈME 6.2.4 *: Pour tout corps fini K et pour tout entier $n > 0$ il existe une extension L/K de degré n ; cette extension est galoisienne, et unique à isomorphisme près. On a $K \cong \mathbb{F}_q$, où $q = p^d$ et p est premier, et $L \cong \mathbb{F}_{q^n}$ est un corps de décomposition du polynôme $X^{q^n} - X = X^{p^{dn}} - X$, et $\mathrm{Gal}(L/K) = \langle \mathrm{Fr}_q \rangle_n$ est le groupe cyclique d'ordre n, engendré par le morphisme de Frobenius Fr_q.*

Dans la pratique, pour pouvoir faire les calculs, le corps $\mathbb{F}_{p^n}$ $(n > 1)$ sera construit comme anneau quotient de type $\mathbb{F}_p[X]/(Q)$, en choisissant un polynôme irréductible Q de degré n.

7 Polynômes sur les corps finis. Nombre de polynômes irréductibles

7.1 Nombre de polynômes irréductibles de degré donné

THÉORÈME 7.1.1 *Soient p un nombre premier et q une puissance de p. Pour tout entier $n \geq 1$, il existe $\theta \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q[\theta]$ et il existe P polynôme irréductible de degré n sur $\mathbb{F}_q$.*

PREUVE. Soient θ un générateur du groupe cyclique $\mathbb{F}_{q^n}^*$, et P son polynôme minimal sur $\mathbb{F}_q$. Alors on a $\mathbb{F}_{q^n} = \mathbb{F}_q[\theta]$ et P est un polynôme irréductible sur $\mathbb{F}_q$ dont $\mathbb{F}_{q^n}$ est un corps de rupture. Autrement dit, on a un isomorphisme

$$\mathbb{F}_q[X]/(P) \xrightarrow{\sim} \mathbb{F}_{q^n}$$

qui envoie la classe de X sur θ. En particulier, on a $\deg P = \dim_{\mathbb{F}_q}(\mathbb{F}_{q^n}) = n$.

REMARQUE 7.1.2 *Si on a un tel polynôme et α une racine de P dans $\mathbb{F}_{q^n}$, la famille $\{1, \alpha, \cdots, \alpha^{n-1}\}$ est une base du $\mathbb{F}_q$-espace vectoriel $\mathbb{F}_{q^n}$.*

PROPOSITION 7.1.3 *Soient P un polynôme irréductible sur $\mathbb{F}_q$ et α une racine de P dans une extension de $\mathbb{F}_q$. Alors, pour tout polynôme Q sur $\mathbb{F}_q$, $Q(\alpha) = 0$ si et seulement si P divise Q.*

En effet, P est alors le polynôme minimal de α sur $\mathbb{F}_q$, voir la proposition 1.3.2.

LEMME 7.1.4 *Soit P un polynôme irréductible de degré m sur $\mathbb{F}_q$. Alors P divise $X^{q^n} - X$ si et seulement si m divise n.*

PREUVE. Le corps de rupture de P sur $\mathbb{F}_q$ est de cardinal q^m, donc tout élément y vérifie $x^{q^m} = x$, donc aussi en itérant si m divise n, $x^{q^n} = x$. On conclut que P divise $X^{q^n} - X$ en appliquant la proposition précédente avec $Q = X^{q^n} - X$. Inversement si P divise $X^{q^n} - X$ alors le corps $\mathbb{F}_{q^n}$ contient un corps de rupture de P, de cardinal q^m, donc par le théorème 6.2.3, m divise n.

THÉORÈME 7.1.5 *Soit P un polynôme irréductible sur $\mathbb{F}_q$ de degré m. Alors P est scindé sur le corps $\mathbb{F}_{q^m}$ et a toutes ses racines simples. Si α est l'une d'elles, ces m racines sont $\alpha, \alpha^q, \cdots, \alpha^{q^{m-1}}$. En particulier si $P \neq X$ toutes les racines de P ont le même ordre multiplicatif dans $\mathbb{F}_{q^m}^*$.*

PREUVE. On a vu que le corps de rupture de P, $\mathbb{F}_q[X]/(P)$, de cardinal q^m, est formé de l'ensemble des racines du polynôme $X^{q^m} - X$. Par suite $X^{q^m} - X$ s'annule en une racine de P, donc par la proposition 7.1.3 il est divisible par P sur $\mathbb{F}_q$ et à fortiori sur $\mathbb{F}_{q^m}$. Ainsi puisque $X^{q^m} - X$ est scindé à racines simples sur $\mathbb{F}_{q^m}$, il en est de même pour P.

Ensuite, on écrit $P = \sum_{i=0}^m a_i X^i$ avec $a_i \in \mathbb{F}_q$. Si α est une racine de P, alors

$$\mathrm{Fr}_q(P(\alpha)) = \sum_{i=0}^m \mathrm{Fr}_q(a_i)\mathrm{Fr}_q(\alpha)^i = P(\mathrm{Fr}_q(\alpha)) = 0$$

où l'avant-dernière égalité vient du fait que $\mathrm{Fr}_q(x) = x$ pour tout $x \in \mathbb{F}_q$. Par conséquent $\alpha, \alpha^q, \cdots, \alpha^{q^{m-1}}$ sont des racines de P. Montrons par l'absurde que ces m racines sont distinctes. En effet, dans le cas contraire, il existe i, j avec $0 \leq i < j \leq m-1$ tels que $\alpha^{q^i} = \alpha^{q^j}$ et donc $\alpha^{q^j - q^i} = 1$. Par conséquent

$$\mathrm{ord}(\alpha) | q^j - q^i = q^i(q^{j-i} - 1).$$

Mais comme $\alpha \in \mathbb{F}_{q^m}^*$, l'ordre de α est premier à q donc, par le lemme de Gauss, $\mathrm{ord}(\alpha)|q^{i-j}-1$, et $\alpha^{q^{j-i}} = \alpha$, donc α appartient au corps $\mathbb{F}_{q^{j-i}}$, ce qui est en contradiction avec le fait que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \deg P = m$. Ainsi on a

$$P(X) = (X-\alpha)(X-\alpha^q)\cdot\ldots\cdot(X-\alpha^{q^{m-1}}).$$

La dernière assertion résulte de ce que Fr_q est un automorphisme du corps $\mathbb{F}_{q^m}$, donc il conserve l'ordre multiplicatif des éléments.

COROLLAIRE 7.1.6 *Le corps de décomposition de tout polynôme de degré m irréductible sur $\mathbb{F}_q$ est $\mathbb{F}_{q^m}$.*

Tout élément $t \in \mathbb{F}_{q^n}$ est racine d'un unique polynôme irréductible unitaire $P = P_t$ de $\mathbb{F}_q[X]$ de degré d divisant n, ainsi

$$X^{q^n} - X = \prod_{d|n} \prod_{\substack{P \text{ unitaire} \\ \text{irréductible sur } \mathbb{F}_q \\ \deg P = d}} P(X)$$

(dans cette formule comme dans la suite du paragraphe, on convient que la notation $d|n$ signifie que d est un diviseur POSITIF de n).

PREUVE. Puisque $\mathbb{F}_q[X]$ est factoriel, on applique le lemme 7.1.4 en utilisant que $X^{q^n} - X$ est premier avec sa dérivée, donc sa factorisation est sans multiplicité.

Soit $\nu_n(q)$ le nombre de polynômes unitaires irréductibles de degré n sur $\mathbb{F}_q$. Alors l'identité ci–dessus montre que

$$q^n = \sum_{d|n} d\nu_d(q),$$

et pour récupérer $\nu_d(q)$ de cette formule on utilise la formule d'inversion de Möbius.

Formule d'inversion de Möbius

DÉFINITION 7.1.7 *On appelle fonction de Möbius la fonction définie sur $\mathbb{N}$ par :*

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n \text{ est le produit de } k \text{ nombres premiers distincts,} \\ 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier.} \end{cases}$$

On voit que $\mu(nm) = \mu(n)\mu(m)$, si m et n sont premiers entre eux.

REMARQUE. On peut aussi définir la fonction de Möbius $\mu(n)$ par l'égalité formelle

$$\sum_{n=1}^{\infty} \mu(n) n^{-s} = \prod_{p \text{ premier}} (1-p^{-s}) = \zeta(s)^{-1}.$$

PROPOSITION 7.1.8 (FORMULE D'INVERSION) *Soient (a_n), (b_n) $(n \geq 1)$ deux suites d'entiers liées par*

$$b_n = \sum_{d|n} a_d \quad (n \geq 1).$$

Alors on a

$$a_n = \sum_{d|n} \mu(n/d) b_d \quad (n \geq 1).$$

En effet on a

$$\sum_{d|n} \mu(n/d) b_d = \sum_{d|n} \mu(n/d) \sum_{d'|d} a_{d'} = \sum_{d'|n} a_{d'} \sum_{\delta|(n/d')} \mu(\delta),$$

où $\delta = n/d$ divise n/d'. Pour $m > 1$, si s désigne le nombre de diviseurs premiers distincts positifs de m, on a

$$\sum_{\delta|m} \mu(\delta) = \sum_{t=0}^{s} C_t^s (-1)^t = (1-1)^s = 0.$$

REMARQUE. La formule d'inversion $a_n = \sum_{d|n} \mu(n/d) b_d$ résulte aussi facilement de l'identité formelle

$$\sum_{n=1}^{\infty} b_n n^{-s} = \sum_{n=1}^{\infty} a_n n^{-s} \zeta(s), \quad \zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

c'est-à-dire

$$\sum_{n=1}^{\infty} a_n n^{-s} = \sum_{n=1}^{\infty} b_n n^{-s} \zeta(s)^{-1}.$$

Une application directe de la formule d'inversion nous permet d'énoncer :

THÉORÈME 7.1.9 *Pour tout corps fini $\mathbb{F}_q$ et tout entier $n \geq 1$ on a :*

(i) $X^{q^n} - X = \prod_{d|n} \prod_{\substack{P \text{ unitaire} \\ \text{irréductible sur } \mathbb{F}_q \\ \deg P = d}} P(X),$

(ii) $q^n = \sum_{d|n} d\nu_d(q).$

(iii) Le nombre de polynômes irréductibles unitaires de degré n sur $\mathbb{F}_q$ est

$$\nu_n(q) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d.$$

REMARQUE. On voit facilement par l'absurde que l'expression à droite est non nulle, car il y a unicité de l'écriture (éventuelle) d'un entier comme somme de puissances différentes de q. Comme $\nu_n \geq 0$, on obtient $\nu_n > 0$; on a ainsi une nouvelle preuve du fait qu'il existe un polynôme irréductible de degré n sur $\mathbb{F}_q$ (théorème 7.1.1).

EXEMPLE. Soit $q = 3$, $n = 2$, alors $\nu_2(3) = \frac{1}{2}(3^2 - 3) = 3$.

```
> Factor(T^9-T) mod 3;
```

$$T\,(T+2)\,(T^2+T+2)\,(T^2+2\,T+2)\,(T+1)\,(T^2+1)$$

Cours N°8. Le jeudi 24 mars 2005

7.2 Ordre d'un polynôme, polynômes primitifs

La notion d'ordre est présentée ici comme complément, les démonstrations sont laissées en exercice (voir [Li-Ni]).

DÉFINITION 7.2.1 *Soit P un polynôme non nul sur $\mathbb{F}_q$. Si $P(0) \neq 0$, l'*ordre *de P est le plus petit entier strictement positif e tel que P divise $X^e - 1$. Si P(0)=0, alors il existe Q dans $\mathbb{F}_q[X]$ non nul en 0 et h entier positif tels que $P = X^h Q$, et dans ce cas on pose* $\mathrm{ord}(P) = \mathrm{ord}(Q)$.

EXERCICE. Montrer l'existence d'un tel nombre e, avec $e \leq q^m - 1$ si $m = \deg P \geq 1$ *Indication :* raisonner dans l'anneau fini $\mathbb{F}_q[X]/(P)$.

REMARQUE 7.2.2 *Si P est irréductible de degré m sur $\mathbb{F}_q$, alors l'ordre e de P divise $q^m - 1$. De plus d'après le lemme 7.1.4 si $e > 1$ (donc $P(X) \neq X$), m est minimal > 0 pour cette propriété, donc le degré m de P est l'ordre multiplicatif de q modulo e.*

THÉORÈME 7.2.3 *Soient $m \geq 1$ et $e > 1$. Le nombre de polynômes irréductibles unitaires sur $\mathbb{F}_q$ de degré m et d'ordre e est*

$$N_{q,m,e} = \begin{cases} \varphi(e)/m & , \text{si } m \text{ est l'ordre multiplicatif de } q \bmod e \\ 0 & , \text{sinon,} \end{cases}$$

où $\varphi(e)$ est l'indicateur d'Euler de e.

PREUVE (en exercice).

EXEMPLE 7.2.4 *On considère le groupe cyclique $\mathbb{F}_{2^{11}}^*$ d'ordre $2^{11} - 1 = 23 \cdot 89$. Soit $\alpha \in \mathbb{F}_{2^{11}}^*$ un élément d'ordre 23. La factorisation de $X^{23} - 1$ en irréductibles sur $\mathbb{F}_2$ est :*

$$X^{23} - 1 = X^{23} + 1 = (X+1)P_0(X)P_1(X) =$$
$$(X+1)\left(X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1\right)\left(X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1\right)$$

où

$$\begin{aligned} P_0(x) &= x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1 \\ &= \prod_{i \in I}(x - \alpha^i), I = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\} \\ P_1(x) &= x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1 \\ &= \prod_{j \in J}(x - \alpha^j), J = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\} \end{aligned}$$

(Notons que toute racine $\neq 1$ de $X^{23} - 1$ est d'ordre 23. Pour écrire les racines de P_0 et P_1 ci-dessus, on a noté α une racine de P_0 et appliqué le théorème 7.1.5.)

Pour $e = 23$ et $q = 2$, on a bien $\mathrm{ord}(2 \bmod 23) = 11$ *: les polynômes irréductibles d'ordre 23 sur $\mathbb{F}_2$ sont de degré 11, il y en a $\varphi(23)/11 = 2$.*

Rapellons que le degré de P irréductible sur $\mathbb{F}_q$ d'ordre e est l'ordre multiplicatif de q modulo e (par la remarque 7.2.2). En effet, on a $e|q^m-1$, avec un m minimal. Par exemple, si $e=23$, $q=2$, alors $\text{ord}(2) \bmod 23 = 11$.

DÉFINITION 7.2.5 *Un polynôme P de degré m sur $\mathbb{F}_q$ est dit* primitif *sur $\mathbb{F}_q$ s'il est le polynôme minimal sur $\mathbb{F}_q$ d'une racine primitive de $\mathbb{F}_{q^m}$ (un générateur du groupe cyclique $\mathbb{F}_{q^m}^*$).*

Une étude de l'ordre des produits de polynômes fournit la caractérisation suivante, où on voit qu'à degré m fixé ce sont les polynômes primitifs qui atteignent l'ordre maximum q^m-1 (voir l'exercice 7.2.1) :

THÉORÈME 7.2.6 *Un polynôme P de degré m est primitif sur $\mathbb{F}_q$ si et seulement si P est unitaire, non nul en 0 et d'ordre q^m-1.*

Un exemple de l'action du Frobenius sur les racines

Considérons de nouveau

$$X^{23}-1 = X^{23}+1 = (X+1)P_0(X)P_1(X) =$$
$$(X+1)\left(X^{11}+X^{10}+X^6+X^5+X^4+X^2+1\right)\left(X^{11}+X^9+X^7+X^6+X^5+X+1\right)$$

où

$$\begin{aligned} P_0(x) &= x^{11}+x^{10}+x^6+x^5+x^4+x^2+1 \\ &= \prod_{i\in I}(x-\alpha^i), I=\{1,2,3,4,6,8,9,12,13,16,18\} \\ P_1(x) &= x^{11}+x^9+x^7+x^6+x^5+x+1 \\ &= \prod_{j\in J}(x-\alpha^j), J=\{5,7,10,11,14,15,17,19,20,21,22\} \end{aligned}$$

Rappellons qu'on définit le symbole de Legendre $\left(\frac{a}{n}\right)$ pour un nombre premier $n=p$ par

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \bmod n, \\ 1 & \text{si } a \equiv b^2 \bmod n, \text{ pour un certain } b, n \nmid b, \\ -1 & \text{sinon.} \end{cases} \tag{7.1}$$

PROPOSITION 7.2.7 *Soit $n=p$ un nombre premier impair. L'application*

$$\phi : a \longmapsto \left(\frac{a}{n}\right), \quad (\mathbb{Z}/n\mathbb{Z})^* \to \{\pm 1\}$$

définit un morphisme $\phi : (\mathbb{Z}/n\mathbb{Z})^* \to \{\pm 1\}$ de groupes cycliques. Son noyau $\text{Ker}(\phi)$ coïncide avec le sous-groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^{*2}$ des carrés dans $(\mathbb{Z}/n\mathbb{Z})^*$, avec
$\text{Card}\left((\mathbb{Z}/n\mathbb{Z})^{*2}\right) = (n-1)/2$.

REMARQUE. L'ensemble $I = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$ de l'exemple 7.2.4 coïncide avec l'ensemble des résidus quadratiques modulo 23, et l'ensemble complémentaire

$$J = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$$

coïncide avec l'ensemble des non-résidus quadratiques modulo 23.

Le morphisme de Frobenius $\alpha^k \mapsto \alpha^{2k}$ laisse bien sûr les ensembles d'exposants I et J stables, et en effet on a $\left(\frac{2}{23}\right) = 1$ (En effet, on a la loi de réciprocité quadratique de Gauss : pour les nombres premiers positifs impairs p, q on a

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}, \tag{7.2}$$

et on a les deux compléments suivants de cette loi :

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}, \qquad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}). \tag{7.3}$$

De plus, l'application $\alpha^k \mapsto \alpha^{-k}$ échange les ensembles I et J puisque $\left(\frac{-1}{23}\right) = -1$; en particulier P_1 est le polynôme minimal de α^{-1} sur $\mathbb{F}_2$.

Résumé des propriétés des polynômes irréductibles sur $\mathbb{F}_q$

THÉORÈME 7.2.8 *Soit α un élément de $\mathbb{F}_{q^m}$, une extension de $\mathbb{F}_q$. Soient d le degré, et P le polynôme minimal de α sur $\mathbb{F}_q$. Alors,*

(i) P est irréductible sur $\mathbb{F}_q$ et son degré d divise m.
(ii) un polynôme Q sur $\mathbb{F}_q$ s'annule α si et seulement si P divise Q.
(iii) tout polynôme irréductible unitaire sur $\mathbb{F}_q$ nul en α est égal à P.
(iv) P divise $X^{q^d} - X$ et $X^{q^m} - X$.
(v) Les racines de P sont $\alpha, \alpha^q, \cdots, \alpha^{q^{d-1}}$ et P est le polynôme minimal sur $\mathbb{F}_q$ de toutes ces racines. Si de plus $\alpha \neq 0$, on a :
(vi) l'ordre de P est égal à celui de α dans le groupe multiplicatif $\mathbb{F}_{q^m}^*$.
(vii) P est un polynôme primitif sur $\mathbb{F}_q$ si et seulement si α est d'ordre $q^m - 1$ dans $\mathbb{F}_{q^m}^*$.

7.3 Construction d'isomorphismes à partir des polynômes irréductibles

Les calculs dans un corps fini d'ordre non premier $q = p^d$ passent par le choix d'un polynôme irréductible P sur $\mathbb{F}_p$ de sorte que $\mathbb{F}_q = \mathbb{F}_p[T]/(P)$. Il est important de savoir transposer ces calculs dans le corps construit en choisissant un autre polynôme irréductible Q. Il s'agit donc d'expliciter un isomorphisme de corps entre $\mathbb{F}_p[T]/(P)$ et $\mathbb{F}_p[T]/(Q)$.

RAPPEL :

THÉORÈME SUR L'ISOMORPHISME 1.4.1 *Soient L une extension de K et $\alpha \in L$ une racine d'un polynôme irréductible P de $K[X]$. Alors l'anneau $K[\alpha]$ est un corps isomorphe à $K[X]/(P)$.*

Pour construire un isomorphisme $\sigma : \mathbb{F}_p[T]/(Q) \xrightarrow{\sim} \mathbb{F}_p[T]/(P)$, on cherche une racine β de Q dans $\mathbb{F}_p[T]/(P) = \mathbb{F}_p[\alpha]$, et on pose $\sigma(T \bmod Q) = \beta \in \mathbb{F}_p[\alpha]$. Ici $\alpha = T \bmod P$.

Un exemple de calcul en Maple (disponible à l'adresse cachée :
`http ://www-fourier.ujf-grenoble.fr /~panchish/04ma1-maple`
dans le fichier 4ma1-14irr.mws).

```
> Factor(T^27-T) mod 3;
```

$$T\,(T+2)\,(T+1)\,(T^3+2\,T+2)\,(T^3+T^2+2\,T+1)\,(T^3+T^2+T+2)\,(T^3+2\,T+1)$$
$$(T^3+T^2+2)\,(T^3+2\,T^2+1)\,(T^3+2\,T^2+T+1)\,(T^3+2\,T^2+2\,T+2)$$

```
> P:=T^3+2*T^2+T+1;
```

$$P := T^3+2\,T^2+T+1$$

```
> alias(alpha = RootOf(P)) ;
```

$$\alpha$$

```
> Q:=T^3+T^2+2*T+1;
```

$$Q := T^3+T^2+2\,T+1$$

```
> Factor(Q, alpha) mod 3;
```

$$(T+2\,\alpha^2+1)\,(T+\alpha+2)\,(T+\alpha^2+2\,\alpha+1)$$

```
> Factor(T^27-T, alpha) mod 3;
```

$$T\,(T+2\,\alpha^2+1)\,(T+2\,\alpha^2)\,(T+\alpha^2+2)\,(T+2\,\alpha^2+\alpha)\,(T+2)\,(T+\alpha^2)\,(T+1)$$
$$(T+\alpha^2+2\,\alpha+2)\,(T+2\,\alpha^2+2)\,(T+2\,\alpha)\,(T+\alpha^2+2\,\alpha)\,(T+2\,\alpha+1)\,(T+\alpha)$$
$$(T+2\,\alpha^2+2\,\alpha+2)\,(T+\alpha+2)\,(T+\alpha^2+\alpha+1)\,(T+2\,\alpha^2+\alpha+2)$$
$$(T+\alpha^2+2\,\alpha+1)\,(T+2\,\alpha+2)\,(T+\alpha^2+\alpha)\,(T+\alpha+1)\,(T+\alpha^2+1)$$
$$(T+2\,\alpha^2+2\,\alpha)\,(T+2\,\alpha^2+2\,\alpha+1)\,(T+2\,\alpha^2+\alpha+1)\,(T+\alpha^2+\alpha+2)$$

Les polynômes $P(T) = T^3 + 2T^2 + T + 1$ et $Q(T) = T^3 + T^2 + 2T + 1$ sont irréductibles sur $\mathbb{F}_3$, car sans racines.

EXEMPLE 7.3.1 *Construire un isomorphisme entre les corps $\mathbb{F}_3[T]/(P)$ et $\mathbb{F}_3[T]/(Q)$.*

Soit $\alpha = T \bmod P$, c'est une racine de P dans $\mathbb{F}_3[T]/(P)$.

On utilise le fait que Q a aussi une racine dans $\mathbb{F}_3[T]/(P)$, par exemple $\beta = \alpha^2 - 1$ (voir le calcul en Maple ci-dessus). On obtient un isomorphisme $\sigma : \mathbb{F}_3[T]/(Q) \xrightarrow{\sim} \mathbb{F}_3[T]/(P)$ en posant $\sigma(T \bmod Q) = \beta = \alpha^2 - 1$.

Pour trouver β "à la main", on peut le chercher sous la forme $c_0 + c_1\alpha + c_2\alpha^2$ avec $c_0, c_1, c_2 \in \mathbb{F}_3$ (faire l'exercice).

7.4 Algorithme de factorisation de Berlekamp dans $\mathbb{F}_q[X]$

On va présenter une méthode classique de factorisation d'un polynôme $P \in \mathbb{F}_q[X]$ non constant (la méthode de Berlekamp). On suppose que P n'a pas de facteurs multiples (c'est-à-dire $\operatorname{pgcd}(P, P') = 1$; dans le cas contraire, on vérifie en exercice que soit $\operatorname{pgcd}(P, P')$ est un diviseur propre D de P et le polynôme P/D est sans facteurs multiples, soit P est la puissance p-ième d'un polynôme qu'on factorise à son tour). Soit donc $P = P_1 \cdot \ldots \cdot P_s$ une factorisation inconnue de P en produit d'irréductibles non associés. Soit $\mathcal{A} = \mathbb{F}_q[X]$, et considérons l'anneau quotient

$$\mathcal{A}/(P) \simeq \mathcal{A}/(P_1) \times \cdots \times \mathcal{A}/(P_s), \tag{7.4}$$

où chaque $\mathcal{A}/(P_i)$ est un corps fini à q^{d_i} éléments, $d_i = \deg P_i$, l'isomorphisme résultant du théorème chinois. L'anneau $\mathcal{A}/(P)$ est en particulier un espace vectoriel sur $\mathbb{F}_q$, de dimension $d = \deg P$, et l'endomorphisme de Frobenius $\mathrm{Fr}_q : x \mapsto x^q$ y opère $\mathbb{F}_q$–linéairement. Par l'isomorphisme (7.4) cette opération se traduit en une action linéaire diagonale de Fr_q sur la somme directe des espaces $\mathcal{A}/(P_i)$. Soit $\mathcal{K}$ le corps de décomposition de P sur $\mathbb{F}_q$, alors chaque corps $\mathcal{A}/(P_i)$ est isomorphe à un sous-corps $\mathcal{K}_i$ de $\mathcal{K}$ tel que $\mathcal{K}_i \supset \mathbb{F}_q$, $[\mathcal{K}_i : \mathbb{F}_q] = d_i$.

De plus $\mathcal{A}/(P_i) \simeq \mathcal{K}_i \simeq \mathbb{F}_{q^{d_i}}$ est donné par la condition :

$$\mathcal{K}_i = \{x \in \mathcal{K} \mid x^{q^{d_i}} = x\} \simeq \mathbb{F}_{q^{d_i}},$$

et son sous–corps des constantes (les points fixes sous Fr_q) est $\mathbb{F}_q = \{x \in \mathcal{A}/(P_i) \mid x^q = x\}$. Alors

$$\mathrm{Ker}(\mathrm{Fr}_q - \mathrm{Id})_{|\mathcal{A}/(P)} \simeq \mathrm{Ker}(\mathrm{Fr}_q - \mathrm{Id})_{|\mathcal{A}/(P_1)} \oplus \cdots \oplus \mathrm{Ker}(\mathrm{Fr}_q - \mathrm{Id})_{|\mathcal{A}/(P_s)} \simeq \mathbb{F}_q^s, \tag{7.5}$$

où s est le nombre des facteurs irréductibles P_i.

On obtient ainsi un critère d'irréductibilité de P :

Théorème 7.4.1 (Critère d'irréductibilité) *Soit P un polynôme de degré d sur $\mathbb{F}_q$, premier avec sa dérivée. Alors P est irréductible si et seulement si le rang r de l'endomorphisme $\mathrm{Fr}_q - \mathrm{Id}$ du $\mathbb{F}_q$-espace vectoriel $A/(P)$est égal à $d-1$.*

En pratique on écrit la matrice de $\mathrm{Fr}_q - \mathrm{Id}$ dans une base de $\mathcal{A}/(P)$, par exemple dans la base

$$1 + (P),\ X + (P),\ X^2 + (P),\ \ldots\ ,\ X^{d-1} + (P).$$

Supposons maintenant $r < d - 1$; pour trouver les facteurs P_i inconnus on cherche tout d'abord un polynôme Q tel que

$$Q + (P) \in \mathrm{Ker}(\mathrm{Fr}_q - \mathrm{Id}) \subset \mathcal{A}/(P)$$

et $Q + (P)$ n'est pas une constante $\mathrm{mod}(P)$. Cela est possible grâce au fait que

$$\dim(\mathrm{Ker}(\mathrm{Fr}_q - \mathrm{Id})) = s = d - r \geq 2, \text{ puisque } r = \mathrm{rg}(\mathrm{Fr}_q - \mathrm{Id}) = \dim(\mathrm{Im}(\mathrm{Fr}_q - \mathrm{Id})) = d - s < d - 1.$$

Alors $P | Q^q - Q$ puisque $Q + (P) \in \mathrm{Ker}(\mathrm{Fr}_q - \mathrm{Id}) \subset \mathcal{A}/(P)$, on a

$$Q^q - Q = \prod_{\alpha \in \mathbb{F}_q} (Q - \alpha),$$

mais $Q - \alpha \not\equiv 0 \bmod (P)$. Ceci implique que

$$P = \mathrm{pgcd}(P, Q^q - Q) = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, Q - \alpha),$$

où la deuxième égalité vient de ce que les facteurs $Q - \alpha$ sont deux à deux premiers entre eux ; de plus la factorisation à droite n'est pas triviale car tous les $\mathrm{pgcd}(P, Q - \alpha)$ sont distincts de P.

En pratique on cherche Q (un "polynôme décomposant") sous la forme
$Q(X) = a_1 X + a_2 X^2 + \cdots + a_{d-1} X^{d-1}$, et on trouve les coefficients $a_i \in \mathbb{F}_q$ comme une solution non triviale du système des $d - 1$ équations linéaires qui traduisent que $(\mathrm{Fr}_q - \mathrm{Id})(Q) = 0$ dans $\mathcal{A}/(P)$.

Des exemples de calcul en Maple avec l'algorithme de Berlekamp sont disponibles à l'adresse cachée :
`http ://www-fourier.ujf-grenoble.fr /~panchish/04ma1-maple`
dans le fichier 4ma1-15berl.mws, voir aussi Annexe A.

EXERCICES

7.1 Dans l'algorithme ci-dessus, expliquer précisément où on a utilisé que P n'a pas de facteurs multiples. Donner un contre-exemple au théorème 7.4.1 lorsque cette hypothèse est en défaut [on pourra montrer plus précisément que le rang de l'endomorphisme $\mathrm{Fr}_q - \mathrm{Id}$ de l'anneau quotient est $d-s$, où s désigne le nombre des facteurs irréductibles unitaires distincts de P].

7.2 Soit $P \in \mathbb{F}_q[X]$ un polynôme ayant des facteurs multiples. Montrer que, soit $pgcd(P, P')$ est un diviseur propre D de P et le polynôme P/D est sans facteurs multiples, soit P est la puissance p-ième d'un polynôme $Q \in \mathbb{F}_q[X]$.

7.3 Ecrire la factorisation de $T^9 - T$ (resp. $T^8 - T$) en irréductibles sur $\mathbb{F}_3$ (resp. sur $\mathbb{F}_2$). Quels sont les facteurs primitifs ?

7.4 Montrer que $X^4 + 2$ est irréductible sur $\mathbb{F}_5$ et trouver son ordre.

7.5 Un polynôme P de degré m sur $\mathbb{F}_q$ est dit primitif sur $\mathbb{F}_q$ s'il est le polynôme minimal sur $\mathbb{F}_q$ d'une racine primitive de $\mathbb{F}_{q^m}$ (un générateur du groupe cyclique $\mathbb{F}_{q^m}^*$). Trouver le nombre des polynômes primitifs de degré m sur $\mathbb{F}_q$.

7.6 DÉTERMINANT DE MOORE. Soit k un corps contenant $\mathbb{F}_q$, $\beta_1, \cdots, \beta_n \in k$. Montrer que

$$\begin{vmatrix} \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \cdots & \beta_2^{q^{n-1}} \\ \cdots & \cdots & \cdots & \cdots \\ \beta_n & \beta_n^q & \cdots & \beta_n^{q^{n-1}} \end{vmatrix} = \beta_1 \prod_{j=1}^{n-1} \prod_{c_1,\cdots,c_n \in \mathbb{F}_q} (\beta_{j+1} - \sum_{i=1}^{j} c_i \beta_i).$$

7.7 PRODUIT DE POLYNÔMES IRRÉDUCTIBLES. Tout élément $t \in \mathbb{F}_{q^n}$ est racine d'un polynôme irréductible unitaire $f = f_t$ de $\mathbb{F}_q[T]$ de degré d divisant n, En déduire

$$T^{q^n} - T = \prod_{d|n} \prod_{\substack{f \text{ irréductible} \\ \deg f = d}} f(T).$$

On utilisera la notation $[n] := T^{q^n} - T$

7.8 PRODUIT DES POLYNÔMES UNITAIRES. En déduire que

$$P_n := \prod_{\substack{f \text{unitaire} \\ \deg f = n}} f(T) = \prod_{m=1}^{n} [m]^{q^{n-m}} = \prod_{m=1}^{n} (T^{q^m} - T)^{q^{n-m}}.$$

On utilisera la notation $[n] := T^{q^n} - T$

7.9 FACTORIEL DE CARLITZ. Soit

$$D_t = \prod_{\substack{f \text{unitaire} \\ \deg f \leq t}} f(T)$$

Montrer que

$$D_t = \prod_{n=1}^{t} P_n = \prod_{n=1}^{t} \prod_{m=1}^{n} [m]^{q^{n-m}} = \prod_{n=1}^{t} \prod_{m=1}^{n} (T^{q^m} - T)^{q^{n-m}}.$$

7.10 Déterminer l'exposant des groupes abéliens $(\mathbb{Z}/60\mathbb{Z})^*, (\mathbb{Z}/100\mathbb{Z})^*, (\mathbb{Z}/187\mathbb{Z})^*$. Trouver pour chacun un élément d'ordre l'exposant.

7.11 En considérant l'ordre des éléments dans le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$, montrer que $n = \sum_{d|n} \varphi(d)$. En déduire une autre preuve du fait que tout sous-groupe d'ordre n de K^*, où K est un corps, est cyclique.

7.12 Soit K un corps à q éléments, $q \geq 4$. Montrer que $\sum_{x \in K} x^2 = 0$. Plus généralement, calculer, pour $s \geq 1$, la somme $\sum_{x \in K} x^s$.

7.13 Soit G l'ensemble de toutes les racines de l'unité dans $\mathbb{C}$. Montrer que G est un sous-groupe infini de $\mathbb{C}^\times$, non monogène. Pour tout $n \geq 1$, montrer que G possède un unique sous-groupe cyclique d'ordre n.

7.14 Soit $P \in \mathbb{F}_{q^m}[X]$. Montrer que $P \in \mathbb{F}_q[X]$ si et seulement si $P(X)^q = P(X^q)$.

7.15 Soit p premier. Calculer "directement" le nombre de polynômes irréductibles de degré 5 sur $\mathbb{F}_p$.

7.16 Soit P polynôme de degré m sur le corps $\mathbb{F}_q$. Démontrer que P est irréductible si et seulement si les deux conditions suivantes sont vérifiées :
(i) P divise $X^{q^m} - X$,
(ii) pour tout diviseur premier l de m, P est premier avec $X^{q^{m/l}} - X$.

7.17 Ecrire tous les polynômes irréductibles unitaires de degré 4 sur $\mathbb{F}_2$ et trouver leur ordre.

7.18 Montrer que $X^4 + 2$ est irréductible sur $\mathbb{F}_5$ et trouver son ordre.

7.19 Soit p premier impair. Montrer que le polynôme $X^4 + 1$ admet une racine α dans $\mathbb{F}_{p^2}$. Montrer que $y = \alpha + \alpha^{-1}$ vérifie $y^2 = 2$. En déduire que 2 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \bmod 8$.

7.20 Soit $m \geq 1$. (a) Trouver le nombre de polynômes primitifs de degré m sur $\mathbb{F}_q$.
(b) Montrer qu'un polynôme P de degré m est primitif sur $\mathbb{F}_q$ si et seulement si P est unitaire, non nul en 0 et d'ordre $q^m - 1$ [Indication : pour la condition suffisante, on montrera que P est sans facteur multiple, et n'est pas produit de polynômes non constants premiers entre eux].

Cours N°9. Le jeudi 31 mars 2005

8 Éléments primitifs et la base normale

8.1 Éléments primitifs

Soit E/K une extension de corps.

DÉFINITION 8.1.1 *Rappelons qu'on appelle* élément primitif *de l'extension E/K un élément $\theta \in E$ tel que $E = K(\theta)$.*

THÉORÈME 8.1.2 *Si $\alpha_1, \cdots, \alpha_n$ sont n éléments algébriques et séparables sur un corps K ($n \in \mathbb{N}^*$), l'extension $E = K(\alpha_1, \cdots, \alpha_n)$ de K admet un élément primitif.*

DÉMONSTRATION. Par multiplicativité des degrés, l'extension E/K est finie. Donc si K est un corps fini, il suffit d'appliquer le théorème 6.2.2 pour conclure : $E^* = \langle\theta\rangle$ donc $E = K(\theta)$.

Supposons K infini. Il est clair qu'il suffit d'examiner le cas $n = 2$: $E = K(\alpha, \beta)$. Notons P le polynôme minimal de α sur K, Q celui de β, et L un corps de décomposition de PQ : L contient E. Comme P et Q sont séparables, P admet r racines distinctes dans L, $\alpha_1 = \alpha$, $\alpha_2, \cdots, \alpha_r$ et Q admet s racines distinctes dans L, $\beta_1 = \beta$, $\beta_2, \cdots, \beta_s$; on se place dans le cas $s > 1$ (sinon il n'y a rien à démontrer).

Pour chaque couple $(i, k) \in [\![1, r]\!] \times [\![2, s]\!]$, il existe au plus un élément $x \in K$ tel que $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$. Comme K est infini, on peut donc trouver $c \in K$ tel que pour tout $(i, k) \in [1, r] \times [2, s]$, $\alpha_i + c\beta_k$ soit distinct de $\alpha_1 + c\beta_1$.

Posons $\theta = \alpha + c\beta$, et montrons que β appartient à $K(\theta)$. Pour cela, considérons dans $K(\theta)[T]$ les deux polynômes Q et $P(\theta - cT)$, et notons δ leur pgcd : toute racine de δ est racine de Q. Par choix de $c \in K$, $\beta_1 = \beta$ est racine de δ ; mais pour $k \geq 2$, $\theta - c\beta_k = \alpha_1 + c(\beta_1 - \beta_k)$, n'est pas racine de δ et δ est égal à $T - \beta$. Comme δ appartient à $K(\theta)[T]$, β est un élément de $K(\theta)$; et $\alpha = \theta - c\beta$ aussi, d'où

$$E = K(\alpha, \beta) = K(\theta). \quad \blacksquare$$

Le théorème 8.1.2 a une conséquence très importante :

THÉORÈME 8.1.3 (D'ALEMBERT-GAUSS) *Le corps $\mathbb{C}$ est algébriquement clos (c'est-à-dire que tout polynôme à coefficients dans $\mathbb{C}$, de degré au moins un, a une racine dans $\mathbb{C}$).*

DÉMONSTRATION : On utilisera les affirmations élémentaires suivantes :

– tout polynôme $P \in \mathbb{R}[T]$ de degré impair admet une racine réelle ;

– pout tout réel $a \geq 0$, il existe un réel b tel que $a = b^2$.

Soit $P \in \mathbb{C}[T]$ un polynôme de degré n. Si $n = 2$, pour vérifier que P admet une racine dans $\mathbb{C}$, il suffit de mettre P sous la forme canonique $T^2 - z$, avec $z = x + iy \in \mathbb{C}$, ($x$ et y réels). On cherche ensuite deux réels a et b tels que $(a + ib)^2 = x + iy$. On obtient le système :

$$\begin{cases} x = a^2 - b^2 \\ y = 2ab, \end{cases}$$

d'où l'égalité $x^2 + y^2 = (a^2 + b^2)^2$. Comme un réel positif admet une racine carrée, on trouve $a^2 = \frac{1}{2}x + \frac{1}{2}\sqrt{x^2 + y^2}$ et $b^2 = -\frac{1}{2}x + \frac{1}{2}\sqrt{x^2 + y^2}$, et P admet une racine dans $\mathbb{C}$.

Si P est de degré quelconque, soit α une racine de P dans une extension de $\mathbb{C}$: α est algébrique sur $\mathbb{C}$, et comme $[\mathbb{C} : \mathbb{R}] = 2$, α est algébrique sur $\mathbb{R}$. A l'aide du polynôme minimal de α sur $\mathbb{R}$, et de $x^2 + 1$, on construit un polynôme séparable de $\mathbb{R}[T]$, dont le corps de décomposition est une extension galoisienne L de $\mathbb{R}$ contenant $\mathbb{C}(\alpha)$. Si G désigne le groupe de Galois de $L/\mathbb{R}$, on a :

$$[L : \mathbb{R}] = [L : \mathbb{C}][\mathbb{C} : \mathbb{R}] = \operatorname{Card} G = 2^k m, \text{ avec } (2, m) = 1, \text{ et } k \geq 1.$$

Si H est un 2-sous-groupe de Sylow de G, son corps des fixes L^H est une extension de degré m de $\mathbb{R}$: d'après le théorème 8.1.2, il existe $\theta \in L^H$ tel que $L^H = \mathbb{R}(\theta)$; θ est racine d'un polynôme irréductible de $\mathbb{R}[T]$ de degré impair m, ce qui n'est pas possible que pour $m = 1$.

Donc G est d'ordre 2^k. Il contient un sous-groupe $\tilde{H}$ d'ordre 2^{k-1}, associé à $\mathbb{C}$ par la correspondance de Galois. Si $\tilde{H}$ n'est pas trivial, $\tilde{H}$ contient à son tour un sous-groupe d'ordre 2^{k-2}, dont le corps des fixes est une extension de degré 2 sur $\mathbb{C}$. Ceci est impossible, puisque $\mathbb{C}[T]$ ne contient pas d'élément irréductible de degré 2. D'où $L = \mathbb{C}$, et tout polynôme de $\mathbb{C}[T]$ de degré au moins 1 a une racine dans $\mathbb{C}$. ∎

REMARQUE 8.1.4 *Dire que $\mathbb{C}$ est algébriquement clos, c'est aussi dire que toute extension finie L de $\mathbb{C}$ est égale à $\mathbb{C}$.*

EXEMPLE 8.1.5 *Soit k un corps. Considérons $L = k(x_1, \cdots, x_n)$, $K = k(s_1, \cdots, s_n)$. Alors $G = \operatorname{Gal}(L/K) \cong S_n$, et $E = K(x_n)$ coïncide avec le corps des fixes du sous-groupe $S_{n-1} \subset S_n$, et $[E : K] = |G/H| = n$, mais $H \not\lhd G$. Considérons les images de l'élément $\alpha = x_1 x_2^2 \cdot \ldots \cdot x_n^n \in E$ par G qui sont toutes distinctes, alors $L = K(\alpha)$, puisque le polynôme minimal de α est de degré $n! = [L : K] = |G|$.*

Donc α est l'élément primitif de L/K, et x_n est l'élément primitif de $L^{S_{n-1}}/K$.

8.2 Théorème de la base normale

DÉFINITION 8.2.1 *Soit E/K une extension galoisienne de degré n et de groupe de Galois G. Une base $\{w_1, \cdots, w_n\}$ du K-espace vectoriel E est dite normale si pour tout $i \in [\![1, n]\!]$, il existe $\sigma \in G$ tel que $w_i = \sigma(w_1)$.*

EXEMPLE 8.2.2 *Considérons le polynôme $P(T) = T^4 + T + 1$. Il est primitif sur $\mathbb{F}_2$ et toute racine α de P dans son corps de décomposition $\mathbb{F}_{16}$ est un élément primitif de $\mathbb{F}_{16}$:*

$$\alpha^4 = 1 + \alpha, \alpha^5 = \alpha + \alpha^2, \alpha^6 = \alpha^2 + \alpha^3, \alpha^7 = 1 + \alpha + \alpha^3, \alpha^8 = 1 + \alpha^2,$$
$$\alpha^9 = \alpha + \alpha^3, \alpha^{10} = 1 + \alpha + \alpha^2, \alpha^{11} = \alpha + \alpha^2 + \alpha^3, \alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3,$$
$$\alpha^{13} = 1 + \alpha^2 + \alpha^3, \alpha^{14} = 1 + \alpha^3, \alpha^{15} = 1.$$

On a une base $\{1, \alpha, \alpha^2, \alpha^3\}$ de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$. Les éléments

$$\alpha, \operatorname{Fr}_2(\alpha) = \alpha^2, \operatorname{Fr}_2^2(\alpha) = \alpha^4 = 1 + \alpha, \operatorname{Fr}_2^3(\alpha) = \alpha^8 = 1 + \alpha^2$$

sont toutes les racines de $P(T) = T^4 + T + 1$. On observe que ces éléments sont linéairement dépendants : $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$ n'est pas une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$.

On a cependant le résultat suivant :

THÉORÈME 8.2.3 (DE LA BASE NORMALE : CORPS FINI) *Soient p un nombre premier et $q = p^d$. Alors il existe un élément θ de $\mathbb{F}_q$ pour lequel $(\theta, \operatorname{Fr}_p(\theta), \cdots, \operatorname{Fr}_{p^{d-1}}(\theta))$ est une base de $\mathbb{F}_q$ sur $\mathbb{F}_p$.*

PREUVE. On considère le morphisme d'anneaux

$$\varphi : \mathbb{F}_p[T] \to \mathrm{End}_{\mathbb{F}_p}(\mathbb{F}_q),\ \sum_{i=0}^{n} a_i T^i \longmapsto \sum_{i=0}^{n} a_i \mathrm{Fr}_p^i$$

et on pose pour tout P de $\mathbb{F}_p[T]$ et tout x de $\mathbb{F}_q$, $P \cdot x = \varphi(P)(x)$. En particulier, $T \cdot x = \mathrm{Fr}_p(x) = x^p$. On note $\mathfrak{a}$ le noyau de φ. Comme tout x de $\mathbb{F}_q$ est solution de $X^q - X = 0$, on a que $\mathrm{Fr}_q = \mathrm{Id}_{\mathbb{F}_q}$, et donc $T^d - 1$ appartient au noyau $\mathfrak{a}$. Inversement, si $P(T) = \sum_{i=0}^{m} a_i T^i$ appartient à ce noyau avec $m < d$, on a la relation

$$\sum_{i=0}^{m} a_i \mathrm{Fr}_p^i = 0,$$

donc le polynôme $\sum_{i=0}^{m} a_i X^{p^i}$ s'annule sur tout $\mathbb{F}_q$. Or son degré est strictement inférieur à p^d, donc c'est le polynôme nul, et on a $P = 0$. Ceci prouve que $\mathfrak{a} = (T^d - 1)$ (autrement dit $T^d - 1$ est le polynôme minimal de Fr_p sur $\mathbb{F}_q$).

La factorisation de $\mu(T) = T^d - 1$ en polynômes irréductibles de $\mathbb{F}_p[T]$ donne une décomposition de l'espace $\mathbb{F}_q$ en somme directe de $\mathbb{F}_p$-sous-espaces stables par Fr_p :

$$\mu = \prod_{i=1}^{s} P_i^{r_i} \text{ et } \mathbb{F}_q = \bigoplus_{i=1}^{s} \mathrm{Ker}(P_i(\mathrm{Fr}_p)^{r_i}).$$

Chaque $E_i = \mathrm{Ker}(P_i(\mathrm{Fr}_p)^{r_i})$ est un $\mathbb{F}_p$-sous-espace stable par Fr_p, et par l'indépendance linéaire des Fr_p^i établie ci-dessus, il contient un élément α_i tel que $\left(\frac{\mu}{P_i}\right)(\mathrm{Fr}_p)(\alpha_i)$ soit non nul. Pour un tel α_i, on pose $\beta_i = \left(\frac{\mu}{P_i^{r_i}}\right)(\mathrm{Fr}_p)(\alpha_i)$; alors la famille

$$\beta_i, P_i(\mathrm{Fr}_p)(\beta_i), \cdots, P_i^{r_i-1}(\mathrm{Fr}_p)(\beta_i),$$

est libre, en effet, pour tous $a_0, a_1, \cdots, a_{r_i-1}$ dans $\mathbb{F}_p$ on a

$$\begin{aligned}
&a_0\beta_i + a_1 P_i(\mathrm{Fr}_p)(\beta_i) + \cdots + a_{r_i-1} P_i^{r_i-1}(\mathrm{Fr}_p)(\beta_i) = 0\\
&\text{donc } a_0 P_i^{r_i-1}(\mathrm{Fr}_p)(\beta_i) + a_1 P_i^{r_i}(\mathrm{Fr}_p)(\beta_i) + \cdots + a_{r_i-1} P_i^{2r_i-1}(\mathrm{Fr}_p)(\beta_i) = 0.\\
&\text{De là } a_0 = 0 \text{ puis } a_1 = 0 \cdots \text{ puis } a_{r_i-1} = 0,
\end{aligned}$$

puisque $P_i^{r_i}(\mathrm{Fr}_p)(\beta_i) = \mu(\mathrm{Fr}_p)(\beta_i) = 0$. Ceci dit que l'ensemble des polynômes Q de $\mathbb{F}_p[T]$ tels que $Q(\mathrm{Fr}_p)(\beta_i) = 0$, est l'idéal de $\mathbb{F}_p[T]$ engendré par $P_i^{r_i}$.

Considérons l'élément $\theta = \beta_1 + \cdots + \beta_s$ de $\mathbb{F}_q$. Si des éléments (a_k) de $\mathbb{F}_p$ vérifient $\sum_{k=0}^{d-1} a_k \mathrm{Fr}_p^k(\theta) = 0$, alors le polynôme $\sum_{k=0}^{d-1} a_k T^k \in \mathbb{F}_p[T]$ est divisible par $P_i^{r_i}$ pour tout i tel que $1 \le i \le s$, donc par μ, et donc les a_k sont tous nuls. Cela signifie que l'élément θ engendre bien une base normale de $\mathbb{F}_q$ sur $\mathbb{F}_p$.

REMARQUE 8.2.4 *Pour les corps finis de caractéristique 2, les bases normales permettent de calculer les carrés et donc les puissances. En effet, si $(\theta, \theta^2, \cdots, \theta^{2^{d-1}})$ est une base de $\mathbb{F}_{2^d}$ sur $\mathbb{F}_2$, alors pour tout $(a_0, a_1, \cdots, a_{d-1}) \in \mathbb{F}_2^d$ on a*

$$\begin{aligned}
(a_0\theta + a_1\theta^2 + \cdots + a_{d-1}\theta^{2^{d-1}})^2 =& a_0^2\theta^2 + a_1^2\theta^4 + \cdots + a_{d-1}^2\theta^{2^d} =\\
& a_{d-1}\theta + a_0\theta^2 + \cdots + a_{d-2}\theta^{2^{d-1}},
\end{aligned}$$

où la dernière égalité est obtenue en notant que $\theta^{2^d} = \theta$.

Autrement dit le carré s'obtient par permutation circulaire *des coordonnées. Pour un corps fini arbitraire, on a une expression similaire pour le calcul du Frobenius.*

Un exemple de calcul en Maple d'une base normale est disponible à l'adresse cachée :
`http ://www-fourier.ujf-grenoble.fr /~panchish/04ma1-maple`
dans le fichier 4ma1-16base-n.mws

THÉORÈME 8.2.5 (DE LA BASE NORMALE : CORPS INFINIS) *Si K est un corps infini, toute extension galoisienne E/K possède une base normale.*

DÉMONSTRATION : D'après le théorème 8.1.2, E admet un élément primitif θ, et le polynôme minimal P de θ sur K possède n racines distinctes $\theta = \theta_1, \theta_2, \cdots, \theta_n$. Si G désigne le groupe de Galois de E/K, notons σ_k l'élément de G, défini par $\sigma_k(\theta) = \theta_k$. Rapellons que pour tout polynôme $P \in E[T]$, on désigne par P^σ le polynôme dont les coefficients sont les images par σ des coefficients de P. Posons alors

$$Q_k(T) = \prod_{i \neq k} \frac{(T - \theta_i)}{(\theta_k - \theta_i)} = \frac{P(T)}{(T - \theta_k)P'(\theta_k)} = Q_1^{\sigma_k}(T).$$

On remarque que $Q_k(\theta_i)$ vaut 1 pour $i = k$, et 0 sinon (c'est un polynôme de Lagrange).

Considérons ensuite le polynôme de $E[T]$,

$$D(T) = \det(Q_1^{\sigma_i\sigma_k}(T))_{i,k=1,\cdots,n}$$

Remarquons que le polynôme $Q_1 + \cdots + Q_n - 1$ est de degré $n-1$ et admet n racines, les θ_i ; il est donc nul. De plus Q_iQ_k est divisible par P pour i distinct de k car il admet les n racines θ_i. Et dans l'anneau $E[T]$, on a :

$$Q_i = Q_i(Q_1 + \cdots + Q_n) \equiv Q_i^2 \bmod P.$$

Ceci implique la congruence suivante modulo P :

$$\begin{pmatrix} Q_1^{\sigma_1} & Q_1^{\sigma_2} & \cdots & Q_1^{\sigma_n} \\ Q_2^{\sigma_1} & Q_2^{\sigma_2} & \cdots & Q_2^{\sigma_n} \\ \cdots & \cdots & \ddots & \cdots \\ Q_n^{\sigma_1} & Q_n^{\sigma_2} & \cdots & Q_n^{\sigma_n} \end{pmatrix} \begin{pmatrix} Q_1^{\sigma_1} & Q_2^{\sigma_1} & \cdots & Q_n^{\sigma_1} \\ Q_1^{\sigma_2} & Q_2^{\sigma_2} & \cdots & Q_n^{\sigma_2} \\ \cdots & \cdots & \ddots & \cdots \\ Q_1^{\sigma_n} & Q_2^{\sigma_n} & \cdots & Q_n^{\sigma_n} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \ddots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

En passant aux déterminants, on obtient que dans l'anneau $E[T]$, D^2 est congru à 1 modulo P ; en particulier, D n'est pas égal à 0, et comme le corps K est infini, il existe un élément a de K tel que $D(a)$ soit non nul.

Soit donc $a \in K$ tel que $D(a) \neq 0$. Posons $w_1 = Q_1(a), \cdots, w_n = Q_n(a)$, on a donc

$$w_i = Q^{\sigma_i}(a) = \sigma_i(w)$$

et

$$\det(\sigma_i\sigma_k(w_1)) = D(a) = \det(Q^{\sigma_i\sigma_k}(a)) \neq 0.$$

Si $(x_1, \cdots, x_n) \in K^n$ vérifie l'égalité $x_1 w_1 + \cdots + x_n w_n = 0$ alors

$$\begin{cases} x_1\sigma_1(w_1) + \cdots + x_n\sigma_1(w_n) = 0, \\ \cdots\cdots\cdots\cdots\cdots \\ x_1\sigma_k(w_1) + \cdots + x_n\sigma_k(w_n) = 0, \\ \cdots\cdots\cdots\cdots\cdots \\ x_1\sigma_n(w_1) + \cdots + x_n\sigma_n(w_n) = 0, \end{cases}$$

et $(x_1, \cdots, x_n)$ est une solution du système linéaire de n équations à n inconnues :

$$1 \leq k \leq n \ : x_1\sigma_k\sigma_1(w_1) + \cdots + x_n\sigma_k\sigma_n(w_1) = 0.$$

Par choix de w_1, ce système de déterminant non nul, est un système de Cramer : il possède une unique solution dans K^n, $(0, 0, \cdots, 0)$. Ceci prouve que les w_i sont linéairement indépendants, et donc que w_1 engendre une base normale de E/K.

EXEMPLE 8.2.6 *Soit k un corps. Considérons $L = k(x_1, \cdots, x_n)$, $K = k(s_1, \cdots, s_n)$. Alors $G = \mathrm{Gal}(L/K) \cong S_n$. Considérons les images de l'élément $\alpha = x_1x_2^2 \cdot \ldots \cdot x_n^n \in E$ par G qui sont toutes distinctes, alors $L = K(\alpha)$, puisque le polynôme minimal de α est de degré $n! = [L : K] = |G|$.*

Donc α est l'élément primitif de L/K, et

$$\{\sigma \in S_n \mid \sigma(x_1x_2^2 \cdot \ldots \cdot x_n^n)\}$$

est une base normale.

En effet, Si $(x_\sigma)_{\sigma \in S_n} \in K^{S_n}$ vérifie l'égalité $\sum_{\sigma \in S_n} x_\sigma \sigma(\alpha)) = 0$ alors

$$\left\{ \ \sum_{\sigma \in S_n} x_\sigma \tau^{-1}\sigma(\alpha)) = 0 \quad (\tau \in S_n) \right.$$

et $(x_\sigma)_{\sigma \in S_n} \in K^{S_n}$ est une solution du système linéaire de $n!$ équations à $n!$ inconnues. Ce système de déterminant non nul, est un système de Cramer : il possède une unique solution dans K^n, $(0, 0, \cdots, 0)$: $\det(\tau^{-1}\sigma(\alpha))_{\sigma,\tau \in S_n} \neq 0$ (les termes diagonaux (avec $\sigma = \tau$) sont strictement plus grands que les autres pour l'ordre lexicographique inverse, et ils ne peuvent pas se simplifier). Ceci prouve que les $\sigma(\alpha)$ sont linéairement indépendantes, et donc que α engendre une base normale *de E/K.*

Cours N°10. Le jeudi 7 avril 2005

Quatrième partie
Extensions résolubles

9 Extensions cyclotomiques

9.1 Racines primitives n-ièmes

Définition 9.1.1 (Racines primitives n-ièmes) *On considère un entier naturel $n \in \mathbb{N}^*$, et un corps K dont la caractéristique ne divise pas n. D'après la proposition 3.2.2, le polynôme $T^n - 1$ de $K[T]$ est séparable car son polynôme dérivé est nT^{n-1}. On note par $\mu_n(K)$ l'ensemble des racines de $T^n - 1$ dans K. Si L est une extension de K contenant un corps de décomposition de $T^n - 1$, ce polynôme admet n racines distinctes dans L, qui forment un sous-groupe multiplicatif fini $\mu_n(L)$ de L^* ; $\mu_n(L)$ est donc un groupe cyclique, et on appelle* racines primitive n-ième de l'unité *tout générateur ζ_n de ce groupe cyclique. Il y a donc $\varphi(n)$ générateurs de ce groupe cyclique, φ désignant la fonction d'Euler.*

Théorème 9.1.2 (Automorphismes d'une extension cyclotomique) *Soient n un élément de $\mathbb{N}^*$, K un corps de caractéristique première à n, et ζ_n une racine primitive n-ième de l'unité dans une extension de K. Alors l'extension $K(\zeta_n)/K$ est galoisienne, et il existe un morphisme injectif ψ de son groupe de Galois G dans le groupe $(\mathbb{Z}/n\mathbb{Z})^*$, défini par $\psi(\sigma) = m \bmod n$, avec m entier vérifiant $\sigma(\zeta_n) = \zeta_n^m$.*

Démonstration : Le corps $K(\zeta_n)$ coïncide avec le corps de décomposition du polynôme séparable $T^n - 1$: il est indépendant du choix de ζ_n parmi les racines primitives n-ièmes de l'unité, et l'extension $K(\zeta_n)/K$ est galoisienne, de groupe de Galois G.

Soit σ un élément de G, c'est un automorphisme du corps $K(\zeta_n)$ laissant fixes les éléments de K, donc il est caractérisé par l'image $\sigma(\zeta_n)$, qui est aussi une racine primitive n-ième de l'unité. On a donc $\sigma(\zeta_n) = \zeta_n^m$, avec $(n, m) = 1$, l'entier m étant défini modulo n, l'application ψ est donc injective.

Si σ_1 et σ_2 sont deux éléments de G tels que $\sigma_1(\zeta_n) = \zeta_n^{m_1}$ et $\sigma_2(\zeta_n) = \zeta_n^{m_2}$, alors $\sigma_1\sigma_2(\zeta_n) = \zeta_n^{m_1 m_2}$, et ψ est un morphisme de groupes. ∎

Remarque. L'extension $K(\zeta_n)/K$ est toujours abélienne (c'est-à-dire, galoisienne de groupe de Galois abélien ; en effet, son groupe de Galois est isomorphe à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$.

Définition 9.1.3 (corps cyclotomique) *Dans le cas particulier, où $K = \mathbb{Q}$, et où ζ_n est une racine primitive n-ième dans $\mathbb{C}$, le corps $\mathbb{Q}(\zeta_n)$, noté $\mathbb{Q}^{(n)}$, s'appelle n-ième* corps cyclotomique.

9.2 Groupe de Galois d'une extension cyclotomique

Théorème 9.2.1 (Groupe de Galois d'un corps cyclotomique) *L'extension $\mathbb{Q}^{(n)}/\mathbb{Q}$ est galoisienne, de groupe de Galois, isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.*

DÉMONSTRATION. Le théorème 9.1.2 donne déjà l'existence d'un morphisme injectif ψ du groupe de Galois G de $\mathbb{Q}^{(n)}/\mathbb{Q}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Il reste à prouver la surjectivité de ψ. On fixe une racine primitive n-ième de l'unité ζ_n dans $\mathbb{C}$, et on note P son polynôme minimal sur $\mathbb{Q}$. Le polynôme P divise T^n-1, donc il existe un $Q \in \mathbb{Q}[T]$ tel que $T^n-1 = P(T)Q(T)$. Grâce au lemme de Gauss, on obtient que P et Q appartiennent en fait à $\mathbb{Z}[T]$.

Si d est le degré de P, on a les égalités :

$$[\mathbb{Q}^{(n)} : \mathbb{Q}] = d = \operatorname{Card} G.$$

D'autre part, pour construire ψ, on a remarqué que pour tout $\sigma \in G$, $\sigma(\zeta_n)$ est aussi une racine primitive n-ième de l'unité, racine du polynôme P. Donc pour démontrer la surjectivité de ψ, il suffit de prouver que toutes les $\varphi(n) = \operatorname{Card}((\mathbb{Z}/n\mathbb{Z})^*)$ racines primitives n-ièmes sont racines de P.

Soit p un nombre premier ne divisant pas n ; alors ζ_n^p est une racine primitive n-ième de l'unité. Comme ζ_n^p est une racine de T^n-1, si ce n'est pas une racine de P, c'est que $Q(\zeta_n^p) = 0$. Donc ζ_n est une racine de $Q(T^p)$, et il existe $R \in \mathbb{Q}[T]$, tel que $Q(T^p) = P(T)R(T)$.

Toujours grâce au lemme de Gauss, on voit que R appartient à $\mathbb{Z}[T]$.

Considérons alors le morphisme d'anneaux de réduction modulo p :

$$\begin{aligned} &\mathbb{Z}[T] \longrightarrow \mathbb{F}_p[T] \\ &\phi = \sum_i c_i T^i \longmapsto \overline{\phi} = \sum_i \overline{c}_i T^i \end{aligned}$$

Dans l'anneau $\mathbb{F}_p[T]$, on a les égalités

$$\overline{Q}(T^p) = (\overline{Q}(T)^p = \overline{P}(T)\overline{R}(T),$$

et $T^n - \overline{1} = \overline{P}(T)\overline{Q}(T)$. Et comme $\overline{P}(T)$ n'est pas une unité de $\mathbb{F}_p[T]$, $\overline{P}(T)$ et $\overline{Q}(T)$ admettent un diviseur commun de degré au moins 1, et le polynôme $T^n - \overline{1}$ admet une racine multiple dans une extension de $\mathbb{F}_p$. Mais $T^n - \overline{1}$ et premier avec son polynôme dérivé nT^{n-1} car p ne divise pas n, d'où la contradiction. Donc si p est un nombre premier ne divisant pas n, ζ_n^p est une racine de P si ζ_n l'est.

Or toute racine primitive n-ième de l'unité s'écrit ζ_n^m avec $m = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$, les p_i ne divisant pas n. En utilisant plusieurs fois le raisonnement précédent, on prouve que ζ_n^m est racine de P. Donc $d = \varphi(n) = [\mathbb{Q}^{(n)} : \mathbb{Q}]$, et le morphisme ψ est bien surjectif. ∎

THÉORÈME 9.2.2 (KRONECKER-WEBER) *Toute extension abélienne $E/\mathbb{Q}$ du corps $\mathbb{Q}$ des nombres rationnels est contenue dans une extension cyclotomique $\mathbb{Q}^{(n)}/\mathbb{Q}$, et son groupe de Galois est isomorphe à un groupe quotient de $(\mathbb{Z}/n\mathbb{Z})^*$.*

REMARQUE. Le fait que toute extension quadratique de $\mathbb{Q}$ est contenue dans une extension cyclotomique $\mathbb{Q}^{(n)}/\mathbb{Q}$, est déjà non trivial. Une démonstration explicite utilise les sommes de Gauss.

On utilise le morphisme de groupes multiplicatifs $\chi_q : (\mathbb{Z}/q\mathbb{Z})^* \to \{\pm 1\}$, donné par le symbole de Legendre $a \longmapsto \left(\frac{a}{q}\right) = \chi(a)$, où q est un nombre premier, et on utilise le morphisme $x \longmapsto \zeta^x = \exp(2i\pi x/q)$ du groupe additif $\mathbb{Z}/q\mathbb{Z}$ dans $\mathbb{C}^*$, $(\zeta = \exp(2i\pi/q))$.

Nous allons considérer les sommes de Gauss comme un analogue discret de la fonction gamma $\Gamma(s)$ qui pour $\operatorname{Re}(s) > 0$ est définie par l'intégrale

$$\Gamma(s) = \int_0^\infty e^{-y} y^s \frac{dy}{y}. \tag{9.1}$$

Ici la fonction intégrée est le produit d'un caractère additif de $\mathbb{R}$ (l'homomorphisme $y \mapsto e^{-y}$, c'est-à-dire, un morphisme de groupes $\mathbb{R} \to \mathbb{C}$), et d'un caractère multiplicatif $y \mapsto y^s$ de $\mathbb{R}_+^\times$, c'est-à-dire, un morphisme $\mathbb{R}_+^\times \to \mathbb{C}$). L'intégration est effectuée par rapport à la mesure invariante multiplicative $\frac{dy}{y}$.

Pour définir la somme de Gauss, on remplace ici $\mathbb{R}$ par $\mathbb{Z}/N\mathbb{Z}$ avec un $N > 1$, e^{-y} par un caractère additif

$$\mathbb{Z}/N\mathbb{Z} \to \mathbb{C}^\times : y \mapsto \zeta_N^y, \quad \zeta_N = \exp\left(\frac{2\pi i}{N}\right),$$

(c'est-à-dire, un morphisme de groupes $\mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$), et on remplace y^s par un caractère multiplicatif $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ (c'est-à-dire, un morphisme de groupes $(\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}$). Le caractère de Dirichlet $\chi : \mathbb{Z} \to \mathbb{C}$ correspondant à χ (désigné aussi par χ) est défini par $\chi(a) = \chi(a \bmod N)$ pour $\mathrm{pgcd}(a, N) = 1$ et par $\chi(a) = 0$ pour $(a, N) > 1$. La somme de Gauss $G(\chi)$ est définie par

$$G(\chi) = \sum_{x=1}^{N-1} \chi(x)\zeta_N^x. \tag{9.2}$$

Pour $a \in \mathbb{Z}$, on utilise souvent la notation suivante :

$$G_a(\chi) = \sum_{x=1}^{N-1} \chi(x)\zeta_N^{ax}.$$

Remarquons aussi que la fonction $a \mapsto G_a(\chi)$ coïncide avec la "transformation de Fourier discrète" du caractère χ.

La similitude entre (9.1) et (9.2) implique que leurs propriétés sont similaires. Pour les décrire on introduit tout d'abord la notion importante de caractère de Dirichlet primitif.

Définition 9.2.3 *Un caractère χ est dit* primitif *modulo N s'il ne se réduit pas à un autre caractère $\chi' : (\mathbb{Z}/M\mathbb{Z})^* \to \mathbb{C}^*$ défini modulo un nombre M plus petit qui est un diviseur propre de N (par la composée avec la projection $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/M\mathbb{Z}$). De même, la restriction de χ sur un sous groupe $H_M = ((1 + M\mathbb{Z})/(1 + N\mathbb{Z}))^\times$ ne soit pas trivial.*

Par exemple, tout caractère non trivial modulo un nombre premier q, est primitif, y compris le symbole de Legendre $\chi_q : a \longmapsto \left(\frac{a}{q}\right)$.

Proposition 9.2.4 *Si χ est primitif, on a*

$$G_a(\chi) = \overline{\chi}(a)G(\chi) \ (a \in \mathbb{Z}), \tag{9.3}$$

$$\overline{G(\chi)} = \chi(-1)G(\overline{\chi}), \tag{9.4}$$

$$|G(\chi)|^2 = N. \tag{9.5}$$

Remarque 9.2.5 *La propriété (9.3) correspond à la formule*

$$\int_0^\infty e^{-ay} y^s \frac{dy}{y} = a^{-s}\Gamma(s) \ (\mathrm{Re}(s) > 0),$$

et (9.5), réécrite sous la forme $G(\chi)G(\chi^{-1}) = \chi(-1)N$, correspond à l'équation fonctionnelle de la fonction gamma

$$\Gamma(s)\Gamma(-s) = -\frac{\pi}{s \sin \pi s} \quad \left(\text{ou} \ \ \Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}\right)$$

PREUVE des égalités (9.3)–(9.5) (en exercice) est impliquée par des changements d'indice de sommation. Par exemple, si $\mathrm{pgcd}(a,N)=1$, $G_a(\chi)=\sum_{x=1}^{N-1}\chi(x)\zeta_N^{ax}=\sum_{x=1}^{N-1}\overline{\chi}(a)\chi(ax)\zeta_N^{ax}=\overline{\chi}(a)\sum_{y\in(\mathbb{Z}/N\mathbb{Z})^*}\chi(ax)\zeta_N^{ax}$. Si $(a,N)=t>1$, on utilise le fait que ζ_N^{ax} ne dépend que de $x \bmod N/t$, et que la somme $\sum_{\substack{b \bmod N\\ b\equiv c \bmod M}}\chi(b)$ s'annule pour tout caractère primitif χ, et pour tout diviseur propre M de N, donc $G_a(\chi)=0=\overline{\chi}(a)G(\chi)$ dans ce cas, d'où (9.3). En particulier, pour $a=-1$ on a (9.4), car

$$\overline{G_{-1}(\chi)}=\sum_{x=1}^{N-1}\overline{\chi(x)}\zeta_N^{-x}=\chi(-1)G(\overline{\chi}),\ \text{et}$$

$$|G(\chi)|^2=G(\chi)\overline{G(\chi)}=\chi(-1)G(\chi)G(\overline{\chi})=\sum_{x \bmod N}\overline{\chi(x)}G(\chi)\zeta_N^{-x}=$$
$$\sum_{x \bmod N}G_x(\overline{\chi})\zeta_N^{-x}=\sum_{x,z \bmod N}\overline{\chi}(z)\zeta_N^{-x+xz}=\sum_{z \bmod N}\overline{\chi}(z)\sum_{x \bmod N}\zeta_N^{x(-1+z)}=N$$

puisque la seule somme non nulle sur x correspond à $z=1$, et $\chi(1)=1$, d'où (9.5).

COROLLAIRE 9.2.6 *Pour le symbole de Legendre $\chi_q : a \longmapsto \left(\frac{a}{q}\right)$ on a : $G(\chi_q)^2=\chi_q(-1)q=\left(\frac{-1}{q}\right)q$, d'où $\sqrt{\left(\frac{-1}{q}\right)q}\in\mathbb{Q}^{(q)}$. Pour tout $d=q_1\cdot\ldots\cdot q_s$ sans facteurs carrés, et $\chi=\chi_{q_1}\cdot\ldots\cdot\chi_{q_s} \bmod d$, on obtient de la même façon $G(\chi)^2=\chi(-1)d$, and $\sqrt{\chi(-1)d}\in\mathbb{Q}^{(d)}$.*

EXEMPLE.

```
> sum(legendre(a,19)*sin(2*Pi*a/19), a=1..9);
```

$$\sin(\frac{2\,\pi}{19})-\sin(\frac{4\,\pi}{19})-\sin(\frac{6\,\pi}{19})+\sin(\frac{8\,\pi}{19})+\sin(\frac{9\,\pi}{19})+\sin(\frac{7\,\pi}{19})+\sin(\frac{5\,\pi}{19})-\sin(\frac{3\,\pi}{19})+\sin(\frac{\pi}{19})$$

```
> evalf(%);
```

$$2.179449471$$

```
> evalf(sqrt(19))/2;
```

$$2.179449472$$

EXERCICE. Calculer

$$2\sin(\frac{2\,\pi}{7})+2\sin(\frac{3\,\pi}{7})-2\sin(\frac{\pi}{7})$$

DÉFINITION 9.2.7 (POLYNÔMES CYCLOTOMIQUES) *On a démontré dans le théorème 9.2.1 que toutes les racines primitives n-ièmes de l'unité dans $\mathbb{C}$ ont même polynôme minimal sur $\mathbb{Q}$. Ce polynôme, noté Φ_n, s'appelle le n-ième polynôme cyclotomique.*

PROPOSITION 9.2.8 (PROPRIÉTÉS DES POLYNÔMES CYCLOTOMIQUES)
(i) Φ_n est un élément de $\mathbb{Z}[T]$.

(ii) Le polynôme Φ_n est de degré $d = \varphi(n) = [\mathbb{Q}^{(n)} : \mathbb{Q}]$.
(iii) $T^n - 1 = \prod_{d|n} \Phi_d$.

COROLLAIRE 9.2.9 *Grâce au lemme de Gauss, on a vu que le polynôme Φ_n est irréductible dans $\mathbb{Z}[T]$.*

EXEMPLE 9.2.10 Les premiers polynômes cyclotomiques sont donnés par

$\Phi_1(T) = T - 1,$
$\Phi_2(T) = T + 1,$
$\Phi_3(T) = T^2 + T + 1,$
$\Phi_4(T) = T^2 + 1,$
$\Phi_5(T) = T^4 + T^3 + T^2 + T + 1,$
$\Phi_6(T) = T^2 - T + 1,$
$\Phi_8(T) = T^4 + 1.$
$\Phi_{105}(T) = T^{48} + T^{47} + T^{46} - T^{43} - T^{42} - 2\,T^{41} - T^{40} - T^{39} + T^{36} + T^{35} + T^{34} + T^{33} + T^{32} + T^{31} - T^{28} - T^{26} - T^{24} - T^{22} - T^{20} + T^{17} + T^{16} + T^{15} + T^{14} + T^{13} + T^{12} - T^9 - T^8 - 2\,T^7 - T^6 - T^5 + T^2 + T + 1$

```
> with(numtheory):cyclotomic(105,T);
```

$$1 + T + T^2 - T^5 - T^8 - 2\,T^7 + T^{35} - T^{28} + T^{32} - T^{42} + T^{12} + T^{13} - T^9 + T^{47} - T^6 + T^{16} + T^{14} + T^{15} - T^{22} + T^{17} - T^{20} - 2\,T^{41} - T^{39} - T^{40} + T^{31} - T^{24} - T^{26} + T^{36} + T^{33} + T^{34} + T^{48} - T^{43} + T^{46}$$

```
> sort(%);
```

$$T^{48} + T^{47} + T^{46} - T^{43} - T^{42} - 2\,T^{41} - T^{40} - T^{39} + T^{36} + T^{35} + T^{34} + T^{33} + T^{32} + T^{31} - T^{28} - T^{26} - T^{24} - T^{22} - T^{20} + T^{17} + T^{16} + T^{15} + T^{14} + T^{13} + T^{12} - T^9 - T^8 - 2\,T^7 - T^6 - T^5 + T^2 + T + 1$$

REMARQUE 9.2.11 *Si K est un corps de caractéristique p, et si p divise n, le polynôme $T^n - 1$ n'est pas séparable. En effet, n s'écrit $p^r u$, avec* $\mathrm{pgcd}(p, u) = 1$, *et $T^n - 1 = (T^u - 1)^{p^r}$.*

10 La norme, la trace et les extensions cycliques

10.1 La norme et la trace

Soit E/K une extension finie de corps. À tout élément α de E, on associe l'application $\varphi_\alpha : E \to E$, définie pour tout x de E par $\varphi_\alpha(x) = \alpha x$.

Définition 10.1.1

La norme *de α dans l'extension E/K est* $\mathrm{N}_{E/K}(\alpha) = \det \varphi_\alpha$.

La trace *de α dans l'extension E/K est* $\mathrm{Tr}_{E/K}(\alpha) = \mathrm{tr}\, \varphi_\alpha$.

Proposition 10.1.2 *Soient E/K une extension finie de corps, et α un élément de E, de polynôme minimal $Q(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0$.*

(i) $E = K(\alpha)$, alors $\mathrm{Tr}_{E/K}(\alpha) = -a_{n-1}$ et $\mathrm{N}_{E/K}(\alpha) = (-1)^n a_0$.

(ii) Si $[E : K(\alpha)] = r$, alors $\mathrm{Tr}_{E/K}(\alpha) = -r a_{n-1}$ et $\mathrm{N}_{E/K}(\alpha) = [(-1)^n a_0]^r$.

(iii) Si E/K est galoisienne, de groupe de Galois $G = \{\sigma_1, \cdots, \sigma_m\}$, alors $\mathrm{Tr}_{E/K}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_m(\alpha)$ et $\mathrm{N}_{E/K}(\alpha) = \sigma_1(\alpha) \cdot \ldots \cdot \sigma_m(\alpha)$.

Démonstration : (i) Si α engendre E, c'est que $\{1, \alpha, \cdots, \alpha^{n-1}\}$ est une K-base de l'espace vectoriel E. La matrice de φ_α dans cette base est

$$A = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}.$$

On a donc bien $\mathrm{Tr}_{E/K}(\alpha) = -a_{n-1}$ et $\mathrm{N}_{E/K}(\alpha) = (-1)^n a_0$.

(ii) Soit $\{e_1, \cdots, e_r\}$ une base de E considéré comme $K(\alpha)$-espace vectoriel ; E s'écrit comme une somme directe $E = K(\alpha)e_1 \oplus \cdots \oplus K(\alpha)e_r$. Chacun des sous-espaces $K(\alpha)e_i$ est un sous-K-espace vectoriel, de E stable pour l'application φ_α, et la restriction de φ_α à $K(\alpha)e_i$ admet comme matrice dans la base $\{\alpha^j e_i\}_{0 \le j \le n-1}$,

$$A_\alpha = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}.$$

Donc la matrice de φ_α dans la base $\{\alpha^j e_i\}_{\substack{0 \le j \le n-1 \\ 1 \le i \le r}}$ du K-espace vectoriel E est la matrice formée de blocs de taille $n \times n$,

$$B_\alpha = \begin{pmatrix} A_\alpha & 0 & \ldots & 0 & 0 \\ 0 & A_\alpha & \ldots & 0 & 0 \\ 0 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & A_\alpha \end{pmatrix}.$$

Ceci implique les égalités (ii) : si $[E : K(\alpha)] = r$, alors

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{tr}(B_\alpha) = \mathrm{tr}\, \varphi_\alpha = r\, \mathrm{Tr}_{K(\alpha)/K}(\alpha) = -r a_{n-1},$$
$$\mathrm{N}_{E/K}(\alpha) = \det(B_\alpha) = \det \varphi_\alpha = [\mathrm{N}_{K(\alpha)/K}(\alpha)]^r = [(-1)^n a_0]^r.$$

(iii) On suppose maintenant E/K galoisienne, de groupe de Galois $G = \{\sigma_1, \cdots, \sigma_m\}$. D'après le théorème 3.2.3, si l'on note $\alpha_1 = \alpha$, $\alpha_2, \cdots, \alpha_n$ les images distinctes de α par les $\sigma_i \in G$, alors $Q(T) = (T - \alpha_1)\cdot\ldots\cdot(T - \alpha_n)$ est un polynôme séparable de $K[T]$ de racine α, et c'est le polynôme minimal de α sur K :

$$Q(T) = \prod_{\sigma_i(\alpha) \text{ distinctes}} (T - \sigma_i(\alpha));$$

α possède donc n images distinctes par les éléments de G, notées $\sigma_{j_1(\alpha)}, \cdots, \sigma_{j_n}(\alpha)$. Soit H le sous-groupe de G associé à $K(\alpha)$ par la corresponance de Galois (théorème 5.1.1) : pour tout $\sigma \in H$, on a $\sigma(\alpha) = \alpha$, $\operatorname{Card} H = [E : K(\alpha)] = r$, $m = nr$, $G = \{\sigma_{j_k}\sigma \mid \sigma \in H, k = 1, \cdots, n\}$, et chaque élément $\sigma_{j_k}(\alpha)$ apparaît r fois dans la famille $\{\sigma_1(\alpha), \cdots, \sigma_m(\alpha)\}$.

On utilise alors les résultats de (ii) :

$$\begin{aligned}
\operatorname{Tr}_{E/K}(\alpha) &= -ra_{n-1} = r(\sigma_{j_1}(\alpha) + \cdots + \sigma_{j_n}(\alpha)) = \sigma_1(\alpha) + \cdots + \sigma_m(\alpha) \\
\operatorname{N}_{E/K}(\alpha) &= [(-1)^n a_0]^r = [\sigma_{j_1}(\alpha)\cdot\ldots\cdot\sigma_{j_n}(\alpha)]^r = \sigma_1(\alpha)\cdot\ldots\cdot\sigma_m(\alpha)
\end{aligned}$$

alors $\operatorname{Tr}_{E/K}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_m(\alpha)$ et $\operatorname{N}_{E/K}(\alpha) = \sigma_1(\alpha)\cdot\ldots\cdot\sigma_m(\alpha)$. ∎

Cours N°11. Le jeudi 14 avril 2005

10.2 Extensions cycliques : définition et exemples

DÉFINITION 10.2.1 *Une extension finie de corps E/K est dite cyclique si elle est galoisienne, à groupe de Galois cyclique.*

EXEMPLE 10.2.2 *Une extension de corps E/K finis est toujours cyclique, à groupe de Galois cyclique, engendré par l'élément de Frobenius Fr_q, où $q = |K|$.*

EXEMPLE 10.2.3 *Soit p un nombre premier. Alors, l'extension cyclotomique $\mathbb{Q}^{(p)}/\mathbb{Q}$ est cyclique de degré $p-1$, à groupe de Galois cyclique, isomorphe à $(\mathbb{Z}/p\mathbb{Z})^*$.*

EXEMPLE 10.2.4 *L'extension cyclotomique $\mathbb{Q}^{(8)}/\mathbb{Q}$ n'est pas cyclique : son groupe de Galois est isomorphe à $(\mathbb{Z}/8\mathbb{Z})^* = \{\pm 1, \pm 3\}$ mod 8.*

EXEMPLE 10.2.5 *Soit $K = \mathbb{Q}(\zeta_n)$, ζ_n une racine primitive n-ième de l'unité, et on pose $E = K(\sqrt[n]{p})$ pour un nombre premier p. Alors on montrera que l'extension de corps E/K est cyclique, à groupe de Galois cyclique, isomorphe à $\mathbb{Z}/n\mathbb{Z}$:*

$$\mathbb{Z}/n\mathbb{Z} \ni a \longmapsto (\sqrt[n]{p} \mapsto \zeta_n^a \sqrt[n]{p}).$$

10.3 Éléments de norme 1 dans les extensions cycliques

THÉORÈME 10.3.1 (THÉORÈME 90 DE HILBERT) *Soient E/K une extension cyclique de corps, et b un élément de E. Les conditions suivantes sont équivalentes :*

(i) $\mathrm{N}_{E/K}(b) = 1$ *;*

(ii) il existe un $a \in E^*$ tel que $b = a\sigma(a)^{-1}$, où σ désigne un générateur du groupe de Galois de E/K.

DÉMONSTRATION. On note m le degré $[E : K]$, et σ un générateur du groupe de Galois.

(ii) $\Rightarrow$(i) : Si b s'écrit $\frac{a}{\sigma(a)}$, avec $a \in E^*$, on remarque que la norme d'un quotient est le quotient des normes, et on utilise la proposition 10.1.2, (iii) :

$$\mathrm{N}_{E/K}(b) = \frac{\prod_{i=1}^m \sigma^i(a)}{\prod_{i=1}^m \sigma^i \cdot \sigma(a)} = 1.$$

(i)$\Rightarrow$(ii) : Réciproquement, supposons b de norme 1 : $\prod_{i=1}^m \sigma^i(b) = 1$. D'après le théorème d'Artin, les morphismes σ^0, σ, $\cdots$, σ^{m-1} sont linéairement indépendants sur E ; la combinaison linéaire de caractères

$$\sigma^0 + b\sigma + b\sigma(b)\sigma^2 + \cdots + b\sigma(b)\cdot\ldots\cdot\sigma^{m-2}(b)\sigma^{m-1}$$

de E^* dans E n'est donc pas nulle, et il existe $c \in E^*$ tel que

$$c + b\sigma(c) + b\sigma(b)\sigma^2(c) + \cdots + b\sigma(b)\cdot\ldots\cdot\sigma^{m-2}(b)\sigma^{m-1}(c) = a \neq 0.$$

Donc

$$\begin{aligned} b\sigma(a) &= b\sigma(c) + b\sigma(b)\sigma^2(c) + \cdots + b\sigma(b)\cdot\ldots\cdot\sigma^{m-1}(b)\sigma^m(c) \\ &\Rightarrow b\sigma(c) + b\sigma(b)\sigma^2(c) + \cdots + c = a = b\sigma(a). \end{aligned}$$

(car $\mathrm{N}_{E/K}(b) = 1$, et $\sigma^m = \sigma^0$). ∎

Le résultat suivant, dû à Kummer, est une célèbre application du théorème 10.3.1 :

THÉORÈME 10.3.2 (KUMMER) *Soient n un entier naturel, K un corps de caractéristique ne divisant pas n et contenant une racine primitive n-ième de l'unité, ζ_n, et E une extension galoisienne de K.*

(i) *Si l'extension E/K est cyclique de degré n, il existe un élément α de E, et un élément a de K, tels que $a = \alpha^n$, et $E = K(\alpha)$.*

(ii) *S'il existe un élément α de E, et un élément a de K, tels que $a = \alpha^n$, et $E = K(\alpha)$, alors l'extension E/K est de degré un diviseur d de n, α^d appartient à K, et $T^d - \alpha^d$ est le polynôme minimal de α sur K.*

DÉMONSTRATION : (i) Comme ζ_n appartient à K, on a $\mathrm{N}_{E/K}(\zeta_n^{-1}) = \zeta_n^{-n} = 1$. D'après le théorème 90 de Hilbert (théorème 10.3.1), il existe $\alpha \in E^*$ tel que $\zeta_n^{-1} = \alpha\sigma(\alpha)^{-1}$, soit $\sigma(\alpha) = \zeta_n\alpha$, d'où $\sigma^i(\alpha) = \zeta_n^i\alpha$. Les images de α par les éléments du groupe de Galois sont toutes distinctes : le polynôme minimal de α sur K est $\prod_{i=0}^{n-1}(T - \zeta_n^i\alpha) = T^n - \alpha^n$, avec $a = \alpha^n \in K$, et α un élément primitif de l'extension E/K.

(ii) Par l'hypothèse, K^* contient le groupe cyclique $\mu_n = \langle\zeta_n\rangle$ d'ordre n des racines n-ièmes de 1. D'autre part, si σ est un élément du groupe de Galois G de E/K, il est caractérisé par $\sigma(\alpha)$, et comme $(\alpha\sigma(\alpha)^{-1})^n = 1$, $\alpha\sigma(\alpha)^{-1} = \zeta_n^{-a}$ appartient à $\mu_n = \langle\zeta_n\rangle$. Donc l'application $\psi : G \longrightarrow \mu_n$ $(\sigma^i \mapsto \dfrac{\alpha}{\sigma^i(\alpha)})$ est un morphisme injectif de groupes ; en effet,

$$\alpha\sigma(\alpha)^{-1} = \zeta_n^{-a} \Rightarrow \sigma(\alpha) = \zeta_n^a\alpha \Rightarrow \sigma^i(\alpha) = \zeta_n^{ia}\alpha \Rightarrow \alpha\sigma^i(\alpha)^{-1} = \zeta_n^{-ia}.$$

Son image est un sous-groupe d'ordre un diviseur d de n.

11 Résolubilité (par radicaux)

11.1 Définitions et exemples

DÉFINITION 11.1.1 *Soit K un corps de caractéristique nulle. Une extension L/K est dite résoluble par radicaux s'il existe un corps E contenant L, et une tour d'extensions intérmédiaires*

$$K = K_0 \subset K_1 \subset \cdots \subset K_m \supset E, K_{j+1} = K_j(\alpha_j) \text{ avec } \alpha_j^{n_j} = a_j, a_j \in K_j, \tag{11.1}$$

vérifiant les conditions suivantes : pour toute indice j ($0 \leq j \leq m-1$), il existe a_j dans K_j, $n_j \in \mathbb{N}^*$, et $\alpha_j \in K_{j+1}$ tels que α_j soit racine du polynôme $T^{n_j} - a_j$, et que l'on ait $K_{j+1} = K_j(\alpha_j)$.

EXEMPLE 11.1.2 *Les extensions cyclotomiques (par définition), et les extensions de Kummer étudiées dans le théorème 10.3.2 sont résolubles par radicaux.*

DÉFINITION 11.1.3 *Une extension L/K est dite résoluble, s'il existe une extension E sur L telle que E/K soit galoisienne à groupe de Galois résoluble.*

REMARQUE 11.1.4 (RAPPEL : DÉFINITION 0.0.2) *Un groupe G est dit* résoluble *s'il existe une série*

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\}$$

telle que G_{k-1}/G_k sont tous abéliens ($k = 1, 2, \cdots, n$). En se référant à la structure des groupes abéliens finis, on peut toujours se ramener, en allongeant la suite, au cas où G_j/G_{j+1} est cyclique d'ordre un diviseur premier p de l'ordre de G.

Le but de ce paragraphe est de comparer, lorsque K est de caractéristique nulle, ces deux notions de résolubilité. Commençons par deux lemmes techniques.

LEMME 11.1.5 *Soient K un corps de caractéristique nulle, E/K une extension galoisienne, et F et L deux extensions intermédiaires de E/K. Si l'extension L/K est résoluble (resp. résoluble par radicaux), il en est de même de l'extension $L \cdot F/F$.*

DÉMONSTRATION : Pour la résolubilité, on se ramène au cas où L/K est galoisienne, de groupe de Galois résoluble. Il suffit d'utiliser la proposition 5.2.2, et les propriétés connues des groupes résolubles pour montrer que l'extension $L \cdot F/F$ est galoisienne, à groupe de Galois résoluble :

PROPOSITION 11.1.6 (RAPPEL) *Soit G un groupe, et H un sous groupe distingué dans G. La résolubilité d'un groupe G est équivalent à celle des groupes H et G/H.*

Pour la résolubilité par radicaux, on utilise la définition. Si l'on a :

$$K = K_0 \subset K_1 = K_0(\alpha_0) \subset \cdots \subset K_m = K_{m-1}(\alpha_{m-1}), \text{ avec } L \subset K_m,$$

α_i racine d'un polynôme $T^{n_i} - a_i$ de $K_i[T]$, alors K_m et E sont deux extensions finies de K et de L. Par le théorème 8.1.2 (d'élément primitif), $K_m = L(\theta)$ pour un élément algébrique θ sur L du polynôme minimale $P \in L[T]$. On sait qu'il existe toujours un corps de décomposition E' du polynôme P sur $E \supset L$: $E' \supset L$, Donc E' contient un sous corps, isomorphe à K_m, et contenant L (engendré sur L par une racine de P dans E'). Ceci dit, qu'on peut choisir une tour (11.1) contenue dans un corps E' contenant E et L. En particulier, *on peut toujours supposer* que tous les $\alpha_j \in K_{j+1} \subset E'$, On a aussi :

$$F = F_0 \subset F_1 = F_0(\alpha_0) \subset \cdots \subset F_m = F_{m-1}(\alpha_{m-1}), \text{ avec } F \cdot L \subset F_m, \quad \blacksquare$$

Remarque 11.1.7 *La réciproque du lemme 11.1.5 n'est pas vraie. Il suffit de voir que pour toute extension L/K, s'il on pose $F = L$, on obtient $F \cdot L = L$, et l'extension $F \cdot L/L$ est résoluble et résoluble par radicaux, tandis que L/K ne l'est pas nécessairement.*

Lemme 11.1.8 *On considère trois corps de caractéristique nulle, $K \subset L \subset M$. L'extension M/K est résoluble (resp. résoluble par radicaux), si et seulement si les extensions M/L et L/K le sont.*

Démonstration : Pour la résolubilité, comme dans la démonstration du lemme précédent, on se ramène au cas où les extensions M/K et L/K sont galoisiennes. La résolubilité du groupe $G = \mathrm{Gal}(M/K)$ est équivalente à celle des groupes $H = \mathrm{Gal}(M/L)$ et G/H, isomorphe à $\mathrm{Gal}(L/K)$.

Supposons maintenant l'extension M/K résoluble par radicaux. Il existe une tour d'extensions :

$$K = K_0 \subset K_1 = K_0(\alpha_0) \subset \cdots \subset K_m = K_{m-1}(\alpha_{m-1}), \text{ avec } M \subset K_m,$$

et pour tout j, $\alpha_j^{n_j} = a_i \in K_j$.

Comme L est inclus dans M, cette même tour convient pour prouver la résolubilité par radicaux de l'extension L/K. Et pour l'extension M/L, il suffit de prendre $L = L_0$, et $L_{j+1} = L_j(\alpha_j)$ avec les mêmes α_j que pour M/K.

Réciproquement, si les extensions M/L et L/K sont résolubles par radicaux, à partir des tours,

$$K = K_0 \subset K_1 = K_0(\alpha_0) \subset \cdots \subset K_m = K_{m-1}(\alpha_{m-1}), \text{ avec } L \subset K_m,$$

$$\text{et } L = L_0 \subset L_1 = L_0(\beta_0) \subset \cdots \subset L_n = L_{n-1}(\beta_{n-1}), \text{ avec } M \subset L_n,$$

on construit la tour composée

$$K = L_0 \subset K_1 \subset \cdots \subset K_m \subset K_m(\beta_0) = L'_1 \subset \cdots \subset L'_n = L'_{n-1}(\beta_{n-1}). \quad \blacksquare$$

Et l'on arrive au résultat essentiel de ce paragraphe.

Théorème 11.1.9 *Soit K un corps de caractéristique nulle. Une extension L/K est résoluble si et seulement si elle est résoluble par radicaux.*

Démonstration : • Supposons d'abord l'extension L/K galoisienne, à groupe de Galois résoluble G. Si N désigne l'ordre de G, on considère une racine primitive $n$ième de l'unité, ζ_N, et l'extension cyclotomique $F = K(\zeta_N)$.

Par construction, l'extension F/K est résoluble par radicaux. Comme on a les inclusions $K \subset F \subset F \cdot L$, et $L \subset F \cdot L$, pour prouver que L/K est résoluble par radicaux, d'après le lemme 11.1.8, il suffit de le faire pour l'extension $F \cdot L/F$. Or d'après la proposition 5.2.2, (ii), l'extension $F \cdot L/F$ est galoisienne, de groupe de Galois isomorphe à un sous-groupe de $G = \mathrm{Gal}(L/K)$: le groupe $\mathrm{Gal}((F \cdot L)/F)$ est résoluble, et il existe une suite de sous groupes emboîtés

$$\mathrm{Gal}((F \cdot L)/F) = G_0 \supset G_1 \supset \cdots \supset G_m = \{e\},$$

telle que G_{j+1} soit distingué dans G_j, et que le groupe quotient G_j/G_{j+1} soit d'ordre un diviseur premier q de N.

On pose alors $F_j = (F \cdot L)^{G_j}$. L'extension F_{j+1}/F_j est galoisienne de degré q, donc cyclique ; le corps F_j, qui contient F, contient une racine primitive $q$ième de l'unité.

D'après le théorème 10.3.2 (de Kummer), il existe a dans F_j et α dans F_{j+1}, avec $\alpha^q = a$, et $F_{j+1} = F_j(\alpha)$. L'extension $(F \cdot L)/F$ est donc résoluble par radicaux, de même que L/K.

• Réciproquement, supposons L/K résoluble par radicaux :

$$K = K_0 \subset K_1 = K_0(\alpha_0) \subset \cdots \subset K_m = K_{m-1}(\alpha_{m-1}), \text{ avec } L \subset K_m, \text{ et } \alpha_j^{n_j} = a_j \in K_j.$$

Raisonnons par récurrence sur la longueur m de la tour.

Si $m = 1$, on a simplement l'inclusion $L \subset K(\alpha)$, avec $\alpha^n = a \in K$. On note ζ_n une racine primitive $n$ième de l'unité, on introduit le corps $F = K(\zeta_n)$; on a alors les inclusions $L \subset F \cdot L \subset F(\alpha)$. L'extension $F(\alpha)/F$ est cyclique, d'après le théorème 10.3.2, (ii), donc l'extension $F \cdot L/F$ est aussi une extension cyclique comme F/K est une extension abélienne, grâce au lemme 11.1.8, on en déduit que l'extension $F \cdot L/K$ est résoluble, donc L/K aussi.

Pour m quelconque, on applique l'hypothèse de récurrence pour montrer que K_{m-1}/K est résoluble ; le raisonnement ci-dessus prouve que K_m/K_{m-1} l'est, donc L/K aussi. ∎

Cours N°12. Le jeudi 28 avril 2005

11 Résolubilité et résolubilité par radicaux (fin)

11.1 Rappels : définitions et exemples

DÉFINITION 11.1.3 (RAPPEL) Une extension L/K est dite résoluble, s'il existe une extension E sur L telle que E/K soit galoisienne à groupe de Galois résoluble.

REMARQUES IMPORTANTES

(i) Dans la définition 11.1.3 on ne demande pas que L/K soit galoisienne.

(ii) Si L/K et M/L sont galoisiennes, il se peut que M/K ne soit pas galoisienne. Cependant, si L/K et M/L sont résolubles, alors M/K est résoluble, *même si elle n'est pas galoisienne.*

EXEMPLE. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $M = \mathbb{Q}(\sqrt[4]{2})$, $E = \mathbb{Q}(\sqrt[4]{2}, i)$. Dans ce cas $T^4 - 2 = (T - \alpha)(T - i\alpha)(T + \alpha)(T + i\alpha)$, avec $\alpha = \sqrt[4]{2}$, et pour tout $\sigma \in \mathrm{Aut}(M/K)$, $\sigma(\alpha) = \pm\,\alpha \in M \subset \mathbb{R} \Rightarrow |\mathrm{Aut}(M/K)| = 2 \neq [M : K] = 4$, donc M/K n'est pas galoisienne. Cependant, E/K est galoisienne (comme le corps de décomposition du polynôme $T^4 - 2$ dans $\mathbb{C}$), et $|\mathrm{Gal}(E/K)| = [E : K] = 8$, ceci dit, $\mathrm{Gal}(E/K)$ est un p-groupe avec $p = 2$, donc résoluble (en fait, $\mathrm{Gal}(E/K) \xrightarrow{\sim} D_4$).

(iii) Soit M/K résoluble, avec une extension E sur M telle que E/K soit galoisienne de groupe de Galois G résoluble. Alors la sous extension minimale galoisienne dans E/K sur $M = K(\theta)$, notée $\widetilde{M}$, coïncide avec $K(\theta_1, \cdots, \theta_n)$, où θ_i sont toutes les images distinctes de $\theta = \theta_1$ par les automorphismes $\sigma \in G$, voir le théorème 3.2.3, et θ est un élément primitif de M sur K : $K \subset M = K(\theta) \subset \widetilde{M} = K(\theta_1, \cdots, \theta_n) \subset E$.

On voit que M/K est résoluble si et seulement si $\mathrm{Gal}(\widetilde{M}/K)$ est résoluble :
$\mathrm{Gal}(\widetilde{M}/K) \cong \mathrm{Gal}(E/K)/\mathrm{Gal}(E/\widetilde{M})$ (est isomorphe au groupe quotient du groupe résoluble $\mathrm{Gal}(E/K)$).

(iv) DÉFINITION 0.0.2 (RAPPEL) Un groupe G est dit résoluble s'il existe une série

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\}$$

telle que G_{k-1}/G_k sont tous abéliens ($k = 1, 2, \cdots, n$). En se référant à la structure des groupes abéliens finis, on peut toujours se ramener, en allongeant la suite, au cas où G_j/G_{j+1} est cyclique d'ordre un diviseur premier p de l'ordre de G.

DÉFINITION 11.1.1 (RAPPEL) Soit K un corps de caractéristique nulle. Une extension L/K est dite résoluble par radicaux s'il existe un corps E contenant L, et une tour d'extensions intermédiaires

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = E, E \supset L,$$

vérifiant les conditions suivantes : pour tout indice j ($0 \leq j \leq m - 1$), il existe a_j dans K_j, $n_j \in \mathbb{N}^*$, et $\alpha_j \in K_{j+1}$ tels que α_j soit racine du polynôme $T^{n_j} - a_j$, et que l'on ait $K_{j+1} = K_j(\alpha_j)$.

Résolubilité et résolubilité par radicaux

Le but de ce paragraphe est de comparer, lorsque K est de caractéristique nulle, ces deux notions de résolubilité :

THÉORÈME *Soit K un corps de caractéristique nulle. Une extension L/K est résoluble si et seulement si elle est résoluble par radicaux.*

Commençons par deux lemmes techniques.

LEMME 11.1.5 (SUR LA RÉSOLUBILITÉ DU COMPOSÉ, RAPPEL) *Soient K un corps de caractéristique nulle, E/K une extension galoisienne, et F et L deux extensions intermédiaires de E/K. Si l'extension L/K est résoluble (resp. résoluble par radicaux), il en est de même de l'extension $(L \cdot F)/F$.*

DÉMONSTRATION : • Pour la résolubilité, on considère l'extension minimale galoisienne $\widetilde{L}/K$, contenant L. D'après la remarque importante (iii), le groupe de Galois $\mathrm{Gal}(\widetilde{L}/K)$ est résoluble. Il suffit d'utiliser la proposition 5.2.2, et les propriétés connues des groupes résolubles pour montrer que l'extension $(\widetilde{L} \cdot F)/F$ est galoisienne, à groupe de Galois résoluble : $\mathrm{Gal}((\widetilde{L} \cdot F)/F) \cong \mathrm{Gal}(\widetilde{L}/(F \cap \widetilde{L})) \subset \mathrm{Gal}(\widetilde{L}/K)$.

PROPOSITION 11.1.6 (RAPPEL) Soit G un groupe, et H un sous groupe distingué dans G. La résolubilité d'un groupe G est équivalente à celle des groupes H et G/H.

• Pour la résolubilité par radicaux, on utilise la définition. Si l'on a :

$$K = K_0 \subset K_1 \subset \cdots \subset K_m \supset L, K_{j+1} = K_j(\alpha_j) \text{ avec } \alpha_j^{n_j} = a_j, a_j \in K_j, \tag{11.1}$$

alors K_m et E sont deux extensions finies de K et de L. Par le théorème 8.1.2 (d'élément primitif), $K_m = L(\theta)$ pour un élément algébrique θ sur L du polynôme minimal $P \in L[T]$. On sait qu'il existe toujours un corps de décomposition E' du polynôme P sur $E \supset L : E' \supset E$, Donc E' contient un sous corps, isomorphe à K_m, et contenant L (engendré sur L par une racine de P dans E'). Ceci dit, on peut choisir une tour (11.1) contenue dans un corps E' contenant E et L. En particulier, *on peut toujours supposer* que tous les $\alpha_j \in K_{j+1} \subset E'$,

$$F = F_0 \subset F_1 \subset \cdots \subset F_m \supset L, F_{j+1} = F_j(\alpha_j) \text{ avec } \alpha_j^{n_j} = a_j, a_j \in K_j \subset F_j. \quad \blacksquare$$

LEMME 11.1.8 (SUR LA RÉSOLUBILITÉ DANS UNE TOUR, RAPPEL) *On considère trois corps de caractéristique nulle, $K \subset L \subset M$. L'extension M/K est résoluble (resp. résoluble par radicaux), si et seulement si les extensions M/L et L/K le sont.*

DÉMONSTRATION : • Pour la résolubilité : soient $\widetilde{M}/K$, $\widetilde{L}/K$ les extensions minimales galoisiennes de M et de L dans une extension galoisienne E. Alors M/K (resp. L/K) sont résolubles si et seulement si les groupes de Galois d'extensions $\widetilde{M}/K$ (resp. $\widetilde{L}/K$) sont résolubles.

Donc si le groupe $\mathrm{Gal}(\widetilde{M}/K)$ est résoluble, alors son sous groupe $\mathrm{Gal}(\widetilde{M}/L)$ est résoluble, et $L \subset M \subset \widetilde{M}$, d'où la résolubilité de deux extensions M/L et de L/K.

Réciproquement, si les extensions M/L et L/K sont résolubles, on veut montrer que le groupe $\mathrm{Gal}(\widetilde{M}/K)$ est résoluble. Soit M'/L l'extension minimale galoisienne de L dans $\widetilde{M}$, alors le groupe de Galois $\mathrm{Gal}(M'/L)$résoluble par la remarque importante (iii).

Considérons le composé $M' \cdot \widetilde{L}$, alors nous avons la tour

$$\widetilde{M} \supset M' \cdot \widetilde{L} \supset \widetilde{L} \supset K. \tag{$\star$}$$

On veut montrer que dans cette tour chaque "étage" est résoluble.
On sait par la proposition 5.2.2, (ii), que

$$\mathrm{Gal}(M'\cdot\widetilde{L}/\widetilde{L})\cong\mathrm{Gal}(M'/\widetilde{L}\cap M')\subset\mathrm{Gal}(M'/L)\text{ est résoluble,}$$
$$\text{et }\mathrm{Gal}(\widetilde{L}/K)\cong\mathrm{Gal}(\widetilde{M}/K)/\mathrm{Gal}(\widetilde{M}/\widetilde{L})\text{ est résoluble.}$$

Donc, il suffit de montrer : $\mathrm{Gal}(\widetilde{M}/\widetilde{L})$ est résoluble (pour en déduire que le groupe $\mathrm{Gal}(\widetilde{M}/K)$ l'est).

On pose $M''=M'\cdot\widetilde{L}$, alors $M''=K(\theta)$ pour un élément primitif θ de M'' sur K. Alors $\widetilde{M}\supset M''=K(\theta)\supset M$, donc

$$\widetilde{M}=K(\theta_1,\cdots,\theta_n)=K(\sigma_1(\theta),\cdots,\sigma_n(\theta))=\sigma_1(M'')\cdot\ldots\cdot\sigma_n(M''),$$

où $\theta_i=\sigma_i(\theta)$ sont les images distinctes de θ par l'action des $\sigma_i\in\mathrm{Gal}(\widetilde{M}/K)$. Donc

$$\mathrm{Gal}(\widetilde{M}/\widetilde{L})=\mathrm{Gal}(\sigma_1(M'')\cdot\ldots\cdot\sigma_n(M'')/\widetilde{L})\subset\prod_i\mathrm{Gal}((\sigma_i(M'')/\sigma_i(\widetilde{L}))=\prod_i\mathrm{Gal}(M''/\widetilde{L}),$$

par la proposition 5.2.2, (iii), et grâce au fait que pour tout $\sigma\in\mathrm{Gal}(\widetilde{M}/K)$ on a $\sigma_i(\widetilde{L})=\widetilde{L}$. Ceci implique que $\mathrm{Gal}(\widetilde{M}/\widetilde{L})$ est résoluble comme un sous groupe du *produit* des groupes résolubles $\mathrm{Gal}(M''/\widetilde{L})=\mathrm{Gal}((M'\cdot\widetilde{L})/\widetilde{L})$. Il reste à conclure que la résolubilité du groupe $G=\mathrm{Gal}(\widetilde{M}/K)$ est équivalente à celle des groupes $H=\mathrm{Gal}(\widetilde{M}/\widetilde{L})$ et G/H, isomorphe à $\mathrm{Gal}(\widetilde{L}/K)$.

• Pour la résolubilité par radicaux : supposons maintenant l'extension M/K résoluble par radicaux. Il existe une tour d'extensions :

$$K=K_0\subset K_1\subset\cdots\subset K_m\supset M,\ K_{j+1}=K_j(\alpha_j)\text{ avec }\alpha_j^{n_j}=a_j,\ a_j\in K_j.$$

Comme L est inclus dans M, cette même tour convient pour prouver la résolubilité par radicaux de l'extension L/K. Et pour l'extension M/L, on raisonne comme dans la démonstration du lemme 11.1.5 pour pouvoir choisir K_m (et la tour) dans une extension finie de M. Ensuite, il suffit de prendre $L=L_0$, et $L_j=L\cdot K_j$ dans $L_j=L\cdot K_j$, donc $L_m=L\cdot K_m\supset M$ (le composé est pris dans M').

Réciproquement, si les extensions M/L et L/K sont résolubles par radicaux, on veut montrer que M/K l'est, à partir des deux tours :

$$K=K_0\subset K_1\subset\cdots\subset K_m\supset L,\ K_{j+1}=K_j(\alpha_j)\text{ avec }\alpha_j^{n_j}=a_j,\ a_j\in K_j,$$

$$\text{et }L=L_0\subset L_1\subset\cdots\subset L_n\supset M,\ L_{j+1}=L_j(\beta_j)\text{ avec }\beta_j^{r_j}=b_j,\ b_j\in L_j,r_j\in\mathbb{N}.$$

Ensuite, on raisonne comme dans la démonstration du lemme 11.1.5 pour pouvoir choisir K_m et L_n dans une *extension finie* M' de M. Ensuite, on construit la tour composée : on pose $L'_j=K_m\cdot L_j$ dans M', alors $L'_{j+1}=L'_j(\beta_j)$, et $\beta_j\in L'_{j+1}\subset M'$:

$$K=L_0\subset K_1\subset\cdots\subset K_m=L'_0\subset L'_1\subset\cdots\subset L'_n\supset L_n\supset M.\quad\blacksquare$$

Et l'on arrive au résultat essentiel de ce paragraphe.

THÉORÈME 11.1.9 *Soit K un corps de caractéristique nulle. Une extension L/K est résoluble si et seulement si elle est résoluble par radicaux.*

DÉMONSTRATION : • Soit L/K résoluble, alors $L \subset \widetilde{L}$, avec l'extension $\widetilde{L}/K$ galoisienne, à groupe de Galois résoluble G. Si N désigne l'ordre de G, on considère une racine primitive Nième de l'unité, ζ_N, et l'extension cyclotomique $F = K(\zeta_N)$.

Par construction, l'extension F/K est résoluble par radicaux. Comme on a les inclusions $K \subset F \subset F \cdot \widetilde{L}$, et $F \cdot \widetilde{L} \supset \widetilde{L} \supset L$, pour prouver que L/K est résoluble par radicaux, d'après le lemme 11.1.8, il suffit de le faire pour l'extension $(F \cdot \widetilde{L})/F$.

Or, d'après la proposition 5.2.2, (ii), l'extension $(F \cdot \widetilde{L})/F$ est galoisienne, de groupe de Galois isomorphe à un sous groupe de $G = \mathrm{Gal}(\widetilde{L}/K)$: le groupe $\mathrm{Gal}((F \cdot \widetilde{L})/F)$ est donc résoluble, et il existe une suite de sous-groupes emboîtés

$$\mathrm{Gal}(F \cdot \widetilde{L}/F) = G_0 \supset G_1 \supset \cdots \supset G_m = \{e\},$$

telle que G_{j+1} soit distingué dans G_j, et que le groupe quotient G_j/G_{j+1} soit d'ordre un diviseur premier q de N.

On pose alors $F_j = (F \cdot \widetilde{L})^{G_j}$. L'extension F_{j+1}/F_j est galoisienne de degré q, donc cyclique ; le corps F_j, qui contient F, contient une racine primitive q-ième de l'unité.

D'après le théorème 10.3.2 (de Kummer), il existe a dans F_j et α dans F_{j+1}, avec $\alpha^q = a$, et $F_{j+1} = F_j(\alpha)$. L'extension $F \cdot \widetilde{L}/F$ est donc résoluble par radicaux, de même que $\widetilde{L}/K$ (puisque $F = K(\zeta_N)$).

Comme $L \subset \widetilde{L}$, ceci implique que L/K est donc résoluble par radicaux.

• Réciproquement, supposons L/K résoluble par radicaux :

$$K = K_0 \subset K_1 = K_0(\alpha_0) \subset \cdots \subset K_m = K_{m-1}(\alpha_{m-1}), \text{ avec } L \subset K_m, \text{ et } \alpha_j^{n_j} = a_j \in K_j.$$

Raisonnons par récurrence sur la longueur m de la tour.

Si $m = 1$, on a simplement l'inclusion $L \subset K(\alpha)$, avec $\alpha^n = a \in K$. On note ζ_n une racine primitive $n$ième de l'unité, on introduit le corps $F = K(\zeta_n)$; on a alors les inclusions $L \subset F \cdot L \subset F(\alpha)$. L'extension $F(\alpha)/F$ est cyclique, d'après le théorème 10.3.2, (ii), donc l'extension $(F \cdot L)/F$ est aussi une extension cyclique comme F/K est une extension abélienne, grâce au lemme 11.1.8, on en déduit que l'extension $(F \cdot L)/K$ est *résoluble*, donc L/K l'est.

Pour m quelconque, on applique l'hypothèse de récurrence pour montrer que K_{m-1}/K est résoluble ; le raisonnement ci-dessus prouve que K_m/K_{m-1} l'est, donc L/K aussi. ∎

11.2 Exemples de calculs du groupe de Galois

Pour construire des exemples d'extensions non-résolubles sur $\mathbb{Q}$ (et sur autres corps), on utilise une méthode générale de calcul du groupe de Galois $\mathrm{Gal}_P = \mathrm{Gal}(L/K)$ d'un polynôme $P \in K[T]$ séparable irréductible, où L note un corps de décomposition de P.

Soient $\alpha_1, \cdots, \alpha_n$ les racines de P dans L. On considère les combinaisons linéaires

$$\theta = u_1\alpha_1 + \cdots + u_n\alpha_n \in L[u_1, \cdots, u_n],$$

avec les variables u_i, et on pose

$$F(z, u) = F(z, u_1, \cdots, u_n) = \prod_{s_u}(z - s_u\theta) \in K[u_1, \cdots, u_n, z],$$

où s_u parcourt toutes les permutations des variables $u_1, \cdots, u_n$ dans le groupe symétrique $S_n = S(u_1, \cdots, u_n)$. On considère une (unique) décomposition

$$F(z, u) = F_1(z, u) \cdot \ldots \cdot F_r(z, u) \in K[u_1, \cdots, u_n, z]$$

en polynômes irréductibles dans $K[u_1, \cdots, u_n, z]$. On définit le sous-groupe

$$\mathfrak{g} := \{s_u \in S(u_1, \cdots, u_n) \mid s_u(F_1) = F_1\} \subset S_n = S(u_1, \cdots, u_n).$$

PROPOSITION 11.2.1 *Le sous groupe $\mathfrak{g}$ est isomorphe au groupe de Galois $\mathrm{Gal}_P = \mathrm{Gal}(L/K)$.*

DÉMONSTRATION (voir §66 de [VdW71]). Les polynômes $F(z,u)$ et $F_i(z,u)$ sont scindés sur le corps $L(u_1, \cdots, u_n)$ avec les facteurs linéaires distincts $z - s_u(\sum_\nu u_\nu \alpha_\nu)$, et on peut supposer que $(z-\theta)|F_1$. Soit s_α parcourt toutes les permutaions des éléments $\alpha_1, \cdots, \alpha_n$ dans le groupe symétrique $S(\alpha_1, \cdots, \alpha_n)$, de telle façon que s_α correspond à s_u (on fixe les racines $\alpha_1, \cdots, \alpha_n$) ; donc

$$s_u s_\alpha(\sum_\nu u_\nu \alpha_\nu) = \sum_\nu u_\nu \alpha_\nu \Longleftrightarrow s_\alpha(\theta) = s_u^{-1}(\theta).$$

Alors $s_\alpha \in \mathrm{Gal}(L/K) \Longleftrightarrow s_u \in \mathfrak{g}$. En effet,

$$s_u \in \mathfrak{g} \Longleftrightarrow s_u(z-\theta)|F_1 \Longleftrightarrow (z - s_\alpha^{-1}(\theta))|F_1 \Longleftrightarrow s_\alpha \in \mathrm{Gal}(L/K),$$

parce que le polynôme $F_1(z,u) \in K(u_1, \cdots, u_n)[z]$ est irréductible et séparable avec les racines $z - \sigma(\theta)$, où $\sigma \in \mathrm{Gal}(L/K)$, et $\sigma(\theta) = u_1\sigma(\alpha_1) + \cdots + u_n\sigma(\alpha_n)$.

COROLLAIRE 11.2.2 *Soient A un anneau intègre factoriel, $\mathfrak{p} \subset A$ un idéal premier de A, $\overline{A} = A/\mathfrak{p}$, $K = \mathrm{Frac}(A)$, $\overline{K} = \mathrm{Frac}(\overline{A})$. On considère un polynôme $P \in A[T]$ séparable sur K tel que le polynôme $\overline{P} \in \overline{A}[T]$ est séparable sur $\overline{K}$. Alors le groupe $\overline{\mathfrak{g}} \subset S(u_1, \cdots, u_n)$ associé au polynôme $\overline{P}$, est un sous-groupe de $\mathfrak{g} \subset S(u_1, \cdots, u_n)$.*

PREUVE : On considère les décompositions des polynômes séparables

$$F(z,u) = F_1(z,u) \cdot \ldots \cdot F_r(z,u) \Rightarrow \overline{F}(z,u) = \overline{F}_1(z,u) \cdot \ldots \cdot \overline{F}_r(z,u),$$

où $F_i(z,u) \in A[u_1, \cdots, u_n, z]$ et $\overline{F}_i(z,u) \in \overline{A}[u_1, \cdots, u_n, z]$ par le lemme de Gauss. On obtient

$$\overline{\mathfrak{g}} \subset \mathfrak{g} \subset S(u_1, \cdots, u_n),$$

puisque $\overline{F}_1(z,u), \cdots, \overline{F}_r(z,u)$ sont premiers entre eux (mais peut-être réductibles !). D'autre part, $\overline{\mathfrak{g}}$ est isomorphe à $\mathrm{Gal}_{\overline{P}}$, donc le corollaire 11.2.2 nous dit que $\mathrm{Gal}_{\overline{P}}$ est isomorphe à un sous-groupe de Gal_P.

Cours N°13. Le jeudi 12 mai 2005

Exemples de calculs du groupe de Galois (fin)

RAPPEL : on utilise une méthode générale de calcul du groupe de Galois $\mathrm{Gal}_P = \mathrm{Gal}(L/K)$ d'un polynôme $P \in K[T]$ séparable irréductible, où L note un corps de décomposition de P.

Soient $\alpha_1, \cdots, \alpha_n$ les racines de P dans L, et $u_1, \cdots, u_n$ les variable indépendantes. On considère le polynôme linéaire

$$\theta = u_1\alpha_1 + \cdots + u_n\alpha_n \in L[u_1, \cdots, u_n],$$

et on pose

$$F(z,u) = F(z, u_1, \cdots, u_n) = \prod_{s_u}(z - s_u\theta) \in K[u_1, \cdots, u_n, z],$$

où s_u parcourt toutes les permutaions des variables $u_1, \cdots, u_n$ dans le groupe symétrique $S_n = S(u_1, \cdots, u_n)$. On considère une (unique) décomposition

$$F(z,u) = F_1(z,u)\cdot\ldots\cdot F_r(z,u) \in K[u_1, \cdots, u_n, z]$$

en polynômes irréductibles dans $K[u_1, \cdots, u_n, z]$. On définit le sous-groupe

$$\mathfrak{g} := \{s_u \in S(u_1, \cdots, u_n) \mid s_u(F_1) = F_1\} \subset S_n = S(u_1, \cdots, u_n).$$

PROPOSITION 11.2.1 *Le sous groupe $\mathfrak{g}$ est isomorphe au groupe de Galois $\mathrm{Gal}_P = \mathrm{Gal}(L/K)$.*

DÉMONSTRATION (voir §66 de [VdW71]). Les polynômes $F(z,u)$ et $F_i(z,u)$ sont scindés sur le corps $L(u_1, \cdots, u_n)$ avec les facteurs linéaires distincts $z - s_u(\sum_\nu u_\nu\alpha_\nu)$, et on peut supposer que $(z-\theta)|F_1$. Soit s_α parcourt toutes les permutations des éléments $\alpha_1, \cdots, \alpha_n$ dans le groupe symétrique $S(\alpha_1, \cdots, \alpha_n)$, de telle façon que s_α correspond à s_u (on fixe les racines $\alpha_1, \cdots, \alpha_n$) ; donc

$$s_u s_\alpha(\sum_\nu u_\nu\alpha_\nu) = \sum_\nu u_\nu\alpha_\nu \Longleftrightarrow s_\alpha(\theta) = s_u^{-1}(\theta).$$

Alors $s_\alpha \in \mathrm{Gal}(L/K) \Longleftrightarrow s_u \in \mathfrak{g}$. En effet,

$$s_u \in \mathfrak{g} \Longleftrightarrow s_u(z-\theta)|F_1 \Longleftrightarrow (z - s_\alpha^{-1}(\theta))|F_1 \Longleftrightarrow s_\alpha \in \mathrm{Gal}(L/K),$$

parce que le polynôme $F_1(z,u) \in K(u_1, \cdots, u_n)[z]$ est irréductible et séparable avec les racines $z - \sigma(\theta)$, où $\sigma \in \mathrm{Gal}(L/K) \cong \mathrm{Gal}(L(u_1, \cdots, u_n)/K(u_1, \cdots, u_n))$, et $\sigma(\theta) = u_1\sigma(\alpha_1) + \cdots + u_n\sigma(\alpha_n)$.

COROLLAIRE 11.2.2 *Soient A un anneau intègre factoriel, $\mathfrak{p} \subset A$ un idéal premier de A, $\overline{A} = A/\mathfrak{p}$, $K = \mathrm{Frac}(A)$, $\overline{K} = \mathrm{Frac}(\overline{A})$. On considère un polynôme $P \in A[T]$ séparable sur K tel que le polynôme $\overline{P} \in \overline{A}[T]$ est séparable sur $\overline{K}$. Alors le groupe $\overline{\mathfrak{g}} \subset S(u_1, \cdots, u_n)$ associé au polynôme $\overline{P}$, est un sous-groupe de $\mathfrak{g} \subset S(u_1, \cdots, u_n)$.*

PREUVE : On considère les décompositions des polynômes séparables

$$F(z,u) = F_1(z,u)\cdot\ldots\cdot F_r(z,u) \Rightarrow \overline{F}(z,u) = \overline{F}_1(z,u)\cdot\ldots\cdot\overline{F}_r(z,u),$$

où $F_i(z,u) \in A[u_1, \cdots, u_n, z]$ et $\overline{F}_i(z,u) \in \overline{A}[u_1, \cdots, u_n, z]$ par le lemme de Gauss. On obtient

$$\overline{\mathfrak{g}} \subset \mathfrak{g} \subset S(u_1, \cdots, u_n),$$

puisque $\overline{F}_1(z,u), \cdots, \overline{F}_r(z,u)$ sont premiers entre eux (mais peut-être réductibles !). D'autre part, $\overline{\mathfrak{g}}$ est isomorphe à $\mathrm{Gal}_{\overline{P}}$, donc le corollaire 11.2.2 nous dit que $\mathrm{Gal}_{\overline{P}}$ est isomorphe à un sous-groupe de Gal_P.

Utilisation du corollaire 11.2.2 pour le calcul du groupe de Galois

Soit par exemple $A = \mathbb{Z}$, $\mathfrak{p} = (p)$, p un nombre premier. Alors

$$P(T) \equiv \varphi_1(T)\cdot\ldots\cdot\varphi_h(T) \bmod p\mathbb{Z}[T] \Rightarrow \overline{P}(T) = \overline{\varphi}_1(T)\cdot\ldots\cdot\overline{\varphi}_h(T)$$

avec $\overline{\varphi}_i(T)$ irréductibles dans $(\mathbb{Z}/p\mathbb{Z})[T]$. On sait que dans ce cas le groupe $\mathrm{Gal}_{\overline{P}}$ est *cyclique*, par exemple $\mathrm{Gal}_{\overline{P}}$ est $\langle(1,2,\cdots,j)(j+1,\cdots\rangle$. Ces orbites sur l'ensemble des racines du polynôme $\overline{P}$ dans son corps de décomposition (où sur l'ensemble des symboles $u_1,\cdots,u_n$) correspondent aux facteurs irréductibles $\overline{\varphi}_i(T)$, de telle façon que chaque facteur correspond a un cycle de longueur d_i égale à son degré.

EXEMPLE 11.2.3 *On considère le polynôme $T^5 - T - 1 \in \mathbb{Z}[T]$. On trouve la factorisation*

$$T^5 - T - 1 = (T^2 + T + 1)(T^3 + T^2 + 1) \bmod 2 \tag{11.2}$$

$$T^5 - T - 1 \textit{ irréductible } \bmod 3 \tag{11.3}$$

en utilisant par exemple la matrice de Berlekamp mod 3,

$$B_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \Rightarrow \mathrm{rg}(B_3 - I_3) = \mathrm{rg}\begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} = 4$$

(on utilise l'action du Frobenius Fr_3 sur la base $\{1, T, T^2, T^3, T^4\}$ de $(\mathbb{Z}/3\mathbb{Z})[T]/(\overline{P})$:

$$\begin{aligned} &1 \mapsto 1, T \mapsto T^3, T^2 \mapsto T^6 = T^2 + T, \\ &T^3 \mapsto T^9 = T^3 \cdot T^6 = T^3 \cdot (T^2 + T) = T^5 + T^4 = T^4 + T + 1, \\ &T^4 \mapsto T^{12} = T^3 \cdot T^9 = T^3 \cdot (T^4 + T + 1) = T^7 + T^4 + T^3 \\ &= T^2(T+1) + T^4 + T^3 = T^4 + 2T^3 + T^2 = T^4 - T^3 + T^2 \bmod 3). \end{aligned}$$

Ceci implique que Gal_P contient un 5-cycle $\sigma_5 = (1,2,3,4,5)$, et une permutation de type $\tau = (i,k)(l,m,n)$. Mais $\tau^3 = (i,k)$, et l'action sur τ^3 par conjugaison avec les puissances de σ_5 produit des transpositions de type $(i,k),(k,p),(p,q),(q,r),(r,i)$ qui engendrent le groupe symétrique S_5.
CONCLUSION : Le groupe de Galois Gal_P du polynôme $T^5 - T - 1 \in \mathbb{Z}[T]$ est isomorphe à S_5. En particulier, ce groupe n'est pas résoluble, et le théorème 11.1.9 nous dit que l'équation $T^5 - T - 1 = 0$ n'est pas résoluble par radicaux sur $\mathbb{Q}$.

REMARQUE 11.2.4 *On applique souvent le corollaire 11.2.2 dans le cas $A = \mathbb{F}_p[x]$, où $P = a_n(x)T^n + \cdots + a_1(x)T + a_0(x) \in A[T]$, $\mathfrak{p} = (f)$, $f \in \mathbb{F}_p[x]$ un polynôme irréductible sur $\mathbb{F}_p$. Si, par exemple $f = x - c \in \mathbb{F}_p[x]$, $\overline{P} = a_n(c)T^n + \cdots + a_1(c)T + a_0(c) \in \mathbb{F}_p[T]$, $\overline{A} = \mathbb{F}_p$.*

EXEMPLE 11.2.5 *Trouver Gal_P pour $P = T^3 + xT + 1 \in A[T]$, où $A = \mathbb{F}_3[x]$.*

On remarque que P est séparable et irréductible sur $K = \mathbb{F}_p(x)$, puisque $P' = x \in K^*$, $P \bmod (x+1) = T^3 - T + 1 \in \mathbb{F}_3[T]$ est irréductible. Il reste à remarqer que $P \bmod (x-1) = T^3 + T + 1 = (T-1)(T^2 + T - 1) \in \mathbb{F}_3[T]$, donc Gal_P contient un 2-cycle et un 3-cycle, ceci dit, $\mathrm{Gal}_P \cong S_3$.

EXERCICES

11.1 Construire un polynôme P de groupe de Galois S_6.

11.2 Montrer qu'un groupe transitif sur $\{1, \cdots, n\}$, contenant un 2-cycle et un $(n-1)$-cycle, coïncide avec S_n.

11.3 Quel est le groupe de Galois du polynôme $T^4 + 2T^2 + T + 3$?

Indication :

```
> galois(x^4+2*x^2+x+3);
```

"4T5", {"S(4)"}, "-", 24, {"(2 4)", "(3 4)", "(1 4)"}

11.4 Soit E le corps de décomposition du polynôme $T^4 + 2T^2 + T + 3$. Quelle est la sous extension maximale abélienne E^{ab} de E sur $\mathbb{Q}$?

Indication : $E^{\mathrm{ab}} = \mathbb{Q}(\sqrt{3877})$, en utilisant :

```
> discrim(T^4+a*T^2+b*T+c,T);
```

$$-4\,a^3\,b^2 - 27\,b^4 + 16\,a^4\,c - 128\,a^2\,c^2 + 144\,a\,c\,b^2 + 256\,c^3$$

```
> discrim(T^4+2*T^2+T+3,T);
```

3877

12 Notions de la cohomologie galoisienne

12.1 Définitions et exemples

La théorie de la cohomologie des groupes donne des moyens pour obtenir une information arithmétique à partir des groupes de Galois, opérant sur des objets assez variés comme des nombres algébriques, points de variétés algébriques (solutions d'équations algébriques sur les corps et les anneaux), en particuler, sur les groupes algébriques etc. (cf. [Se63], [Se64], [Wei74]). Pour donner un exemple important, on va formuler le théorème 90 de Hilbert à l'aide de la notion de la cohomologie galoisienne.

THÉORÈME 10.3.1 (THÉORÈME 90 DE HILBERT, RAPPEL) *Soient E/K une extension cyclique de corps, et β un élément de E. Les conditions suivantes sont équivalentes :*

(i) $\mathrm{N}_{E/K}(\beta) = 1$ *;*

(ii) il existe un $\alpha \in E^*$ tel que $\beta = \alpha\sigma(\alpha)^{-1}$, où σ désigne un générateur du groupe de Galois de E/K.

On considère un groupe fini G, noté multiplicativement, muni de l'opération $(\sigma, \sigma') \mapsto \sigma\circ\sigma'$, un groupe commutatif M, noté multiplicativement, muni de l'action de $G : G \to \mathrm{Aut}(M)$, $G\times M \to M$, et le groupe commutatif multiplicatif $\mathrm{App}(G, M) = \{f \ : G \to M\}$, muni d'action naturelle de G (la multiplication des fonctions et l'action de G se fait point-par-point). Ensuite, on définit le groupe commutatif des 1-cocycles (homomorphismes croisés) multiplicatifs $Z^1(G, M)$, et son sous groupe $B^1(G, M)$ des 1-cobords par

$$Z^1(G, M) = \{f \ : G \to M \mid \text{pour tout } \sigma, \sigma' \in G, f(\sigma \circ \sigma') = \sigma f(\sigma') \cdot f(\sigma)\} \tag{12.1}$$

$$B^1(G, M) = \{f \ : G \to M \mid \exists a \in M, \forall \sigma \in G, f(\sigma) = a\sigma(a)^{-1}\} \tag{12.2}$$

DÉFINITION 12.1.1 *On définit le premier groupe de cohomologie du groupe G à coefficients dans M comme le groupe quotient, noté $H^1(G, M) = Z^1(G, M)/B^1(G, M)$.*

Considérons une extension finie galoisienne L/K de groupe $G = \mathrm{Gal}(L/K)$, et le groupe multiplicatif $M = L^*$ muni d'action naturelle de G.

THÉORÈME 12.1.2 (THÉORÈME 90 DE HILBERT, FORME GÉNÉRALE)

$$H^1(G(L/K), L^*) = \{1\}.$$

L'idée de la preuve du théorème est la même que dans la description des extensions cycliques (cf. §10.3). Soit $f : G \to L^*$ un *homomorphisme croisé* $f \in Z^1(G(L/K), L^*)$. Dans la notation multiplicative cela signifie que pour tout σ, $\sigma' \in G$ on a $\sigma(f(\sigma')) = f(\sigma \circ \sigma')/f(\sigma) \in L^*$. On trouvera un élément $\alpha \in L^*$ tel que pour tout $\sigma \in G$ on a $f(\sigma) = \alpha/\sigma(\alpha)$.

Considérons la "série de Poincaré" $\sum_{\sigma' \in G} f(\sigma')\sigma'$, une combinaison linéaire des caractères σ'. Par le théorème 2.1.4 d'indépendance linéaire de caractères (E.Artin), il existe un $\gamma \in L$, tel que

$$\alpha = \sum_{\sigma' \in G} f(\sigma')\sigma'(\gamma) \in L \tag{12.3}$$

soit non nul. On applique aux deux parties de (12.3) un élément $\sigma \in G$. Alors

$$\sigma(\alpha) = \sum_{\sigma' \in G} \sigma(f(\sigma'))\sigma(\sigma'(\gamma)) = \sum_{\sigma' \in G} \sigma f(\sigma')(\sigma \circ \sigma')(\gamma))$$
$$= f(\sigma)^{-1} \sum_{\sigma' \in G} f(\sigma \circ \sigma')\sigma \circ \sigma'(\gamma) = f(\sigma)^{-1}\alpha$$

(par la formule de l'action à gauche de G sur L^*, $\sigma(\sigma'(\gamma)) = \sigma \circ \sigma'(\gamma)$ pour $\sigma, \sigma' \in G$). Cette méthode de la somme moyenne (la *série de Poincaré*) $\alpha = \sum_{\sigma' \in G} f(\sigma')\sigma'(\gamma) \in L$ est aussi connue comme la méthode de la *résolvante de Lagrange* dans la théorie des extensions de corps.

Pour retrouver la forme précédente du théorème 90 de Hilbert (le théorème 10.3.1 pour une extension cyclique L/K de groupe de Galois $\langle\sigma\rangle_n$), on considère un élément $\beta \in L^*$ avec $\mathrm{N}_{L/K}(\beta) = 1$, et l'application

$$f \ : \sigma^0 \mapsto 1, \sigma \mapsto \beta, \sigma^2 \mapsto \beta\sigma(\beta), \cdots, \sigma^{n-1} \mapsto \beta\sigma(\beta)\cdot\ldots\cdot\sigma^{n-2}(\beta),$$

On vérifie que f est un 1-cocycle : pour tous $0 \leq i, k \leq n-1$, on a

$$f(\sigma^i \circ \sigma^k) = \sigma^i(f(\sigma^k))f(\sigma^i)$$

Si, par exemple $i + k \leq n - 1$, on a

$$f(\sigma^i \circ \sigma^k) = \beta\sigma(\beta)\cdot\ldots\cdot\sigma^{i+k-1}(\beta) = \sigma^i(\beta\sigma(\beta)\cdot\ldots\cdot\sigma^{k-1}(\beta))\beta\sigma(\beta)\cdot\ldots\cdot\sigma^{i-1}(\beta) = \sigma^i(f(\sigma^k))f(\sigma^i),$$

et pour les autres valeurs de i, k on utilise la relation $\mathrm{N}_{L/K}(\beta) = \beta\sigma(\beta)\cdot\ldots\cdot\sigma^{n-1}(\beta) = 1$.

En utilisant le théorème 12.1.2, on trouve un $\alpha \in L^*$ telle que $\beta = f(\sigma) = \alpha/\sigma(\alpha)$.

Pour donner une définition générale des groupes de cohomologie d'un groupe fini G, noté multiplicativement, on considère un groupe commutatif A, noté additivement, muni d'action de G (c'est-à-dire, un G–module A).

Les groupes de cohomologie de G à coefficients dans A sont définis à l'aide du *complexe des cochaînes*. On considère les groupes abéliens (les G-modules) suivants :

$$C^0(G, A) = A,$$

et pour $n \geq 1$

$$C^n(G, A) = \{f : G \times \cdots \times G \to A\}$$

(l'addition des fonctions et l'action de G se fait point-par-point).

Définition 12.1.3 *La formule*

$$\begin{aligned}(d_n f)(g_1, \ldots, g_{n+1}) =& g_1 f(g_2, \ldots, g_{n+1}) \\ &+ \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\ &+ (-1)^{n+1} f(g_1, \ldots, g_n),\end{aligned} \tag{12.4}$$

définit un morphisme $d_n : C^n(G, A) \to C^{n+1}(G, A)$.

Ensuite, on vérifie l'égalité $d_{n+1} \circ d_n = 0$.

Si, par exemple $n = 1$, on a

$$\begin{aligned}&d_2 \circ (d_1 f)(g_1, g_2, g_3) = \\ &g_1(d_1 f)(g_2, g_3) - (d_1 f)(g_1 g_2, g_3) + (d_1 f)(g_1, g_2 g_3) - (d_1 f)(g_1, g_2); \\ &g_1(d_1 f)(g_2, g_3) = g_1 g_2 f(g_3) - g_1 f(g_2 g_3) + g_1 f(g_2); \\ &-(d_1 f)(g_1 g_2, g_3) = -g_1 g_2 f(g_3) + f(g_1 g_2 g_3) - f(g_1 g_2); \\ &(d_1 f)(g_1, g_2 g_3) = g_1 f(g_2 g_3) - f(g_1 g_2 g_3) + f(g_1); \\ &-(d_1 f)(g_1, g_2) = -g_1 f(g_2) + f(g_1 g_2) - f(g_1);\end{aligned}$$

l'addition des termes montre que $d_2 \circ (d_1 f) = 0$.

Exercice. Vérifier l'identité $d_n \circ d_{n-1} = 0$ pour $n \geq 2$.

DÉFINITION 12.1.4 *Le groupe* $Z^n(G,A) = \mathrm{Ker}(d_n)$ *est appelé le groupe des* n*–cocycles, et le groupe* $B^n(G,A) = \mathrm{Im}(d_{n-1})$ *est appelé le groupe des* n*–cobords. La propriété* $d_n \circ d_{n-1} = 0$ *implique que* $B^n(G,A) \subset Z^n(G,A)$*. On définit alors les groupes de cohomologie par*

$$H^n(G,A) = Z^n(G,A)/B^n(G,A) = \begin{cases} \mathrm{Ker}\, d_n/\mathrm{Im} d_{n-1} & \textit{pour } n \geq 1; \\ \mathrm{Ker}\, d_0 & \textit{pour } n = 0. \end{cases} \tag{12.5}$$

Si $n = 0$ alors

$$H^0(G,A) = A^G = \{a \in A \mid ga = a \text{ pour tout } g \in G\}. \tag{12.6}$$

La formule (12.21) montre qu'un 1-cocycle est une application $f : G \to A$ vérifiant l'identité : pour tous $g_1,\, g_2 \in G$

$$f(g_1 g_2) = f(g_1) + g_1 f(g_2). \tag{12.7}$$

On dit que f est un *homomorphisme croisé*. On dit qu'un homomorphisme croisé est un *1-cobord*, si et seulement s'il existe un $a \in A$ tel que pour tout $g \in G$ on a $f(g) = a - ga$. On identifie alors le groupe $H^1(G,A)$ avec le groupe quotient de tous les homomorphismes croisés par le sous groupe de tous les cobords. Si l'action de G sur A est triviale alors $H^1(G,A)$ coïncide avec le groupe de tous les homomorphismes de G dans A.

EXERCICE. Montrer que pour un groupe fini cyclique $G = \langle\sigma\rangle_n$, et pour tout G-module A, on a l'isomorphisme suivant :

$$H^1(G,A) = (\mathrm{Ker}\,\mathrm{Norm})(A)/(\sigma - 1)A, \text{ où } \mathrm{Norm}(a) = (1 + \sigma + \cdots + \sigma^{n-1})a$$

Indication : pour un 1-cocycle $f \in Z^1(G)$ utiliser la formule :

$$f(\sigma^i) = (1 + \sigma + \cdots + \sigma^{i-1}) f(\sigma), \text{ et } f(1) = f(\sigma^n) = 0$$

et noter que cette formule donne toujours un 1-cocycle pour un choix de $f(\sigma) \in \mathrm{Ker}\,\mathrm{Norm}$.

Un 2-cocycle est une application $f : G \times G \to A$ vérifiant l'identité : pour tous $g_1,\, g_2, g_3 \in G$

$$g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0. \tag{12.8}$$

On dit que c'est un *système de facteurs*. Les éléments de $H^2(G,A)$ correspondent bijectivement aux classes d'équivalence d'extensions de G par A. Pour le voir, considérons une extension

$$0 \longrightarrow A \xrightarrow{i} \tilde{G} \xrightarrow{\pi} G \to 1, \tag{12.9}$$

où on mélange la notation additive dans A avec la notation multiplicative dans G et $\tilde{G}$: $i(a_1 + a_2) = i(a_1)i(a_2)$. Pour tout $g \in G$ on choisit un relèvement $\tilde{g}$ dans $\tilde{G}$ (c'est-à-dire, on choisit une section $g \mapsto \tilde{g}$ de la projection $\tilde{G} \xrightarrow{\pi} G$). On définit un 2-cocycle (un système des facteurs) $f : G \times G \to A$, $f(g_1, g_2) \in A$ par

$$\tilde{g}_1 \cdot \tilde{g}_2 = i(f(g_1, g_2))\widetilde{g_1 g_2}.$$

Alors la fonction f est un 2–cocycle de G à coefficients dans A. Si on change notre choix de représentants $\tilde{g}$ (c'est-à-dire, on le choix d'une section $G \to \tilde{G}$), alors f est altéré par un 2-cobord. Donc la classe de f ne dépend que de l'extension (12.9).

Réciproquement, on peut définir une loi de groupe sur l'*ensemble* $G \times A$ par

$$(g_1, a_1) \cdot (g_2, a_2) = (g_1 g_2, a_1 + a_2 + f(g_1, g_2)),$$

(on vérifie l'associativité à partir de (12.8).

EXERCICE 12.1.5 *Montrer que pour un groupe fini G, et un G-module fini A, tels que* $\mathrm{pgcd}(|G|, |A|)) = 1$, *on a*

$$H^n(G, A) = 0 \text{ pour tout } n > 0.$$

Indication : Soit $N = |G|$. On considère un n-cocycle $f \in Z^n(G, A)$, et on cherche à construire une $(n-1)-$cochaîne $\varphi \in C^{n-1}(G, A)$, telle que $N \cdot f = d_{n-1}(\varphi)$, sous la forme suivante :

$$\varphi(g_1, \cdots, g_{n-1}) = \sum_{g_n \in G} f(g_1, \cdots, g_{n-1}, g_n) \tag{12.10}$$

12.2 Propriétés des groupes de cohomologie

(1) LONGUE SUITE EXACTE DES COHOMOLOGIES. Considérons une *suite exacte* courte de G–modules (c'est-à-dire, de groupes abéliens munis d'action de G) :

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{\pi} C \longrightarrow 0,$$

c'est-à-dire, que $\mathrm{Im}(i) = \mathrm{Ker}(\pi)$, i est injective et π est surjective. Alors la longue suite exacte suivante est définie :

$$\begin{aligned} 0 \longrightarrow H^0(G, A) \longrightarrow H^0(G, B) \longrightarrow H^0(G, C) &\xrightarrow{\Delta_0} H^1(G, A) \\ \longrightarrow H^1(G, B) \longrightarrow H^1(G, C) &\xrightarrow{\Delta_1} H^2(G, A) \longrightarrow \\ \cdots \longrightarrow H^n(G, A) \longrightarrow H^n(G, B) \longrightarrow H^n(G, C) &\xrightarrow{\Delta_n} H^{n+1}(G, A) \longrightarrow \cdots \end{aligned} \tag{12.11}$$

Pour définir les homomorphismes Δ_n, on utilise le grand diagramme commutatif (12.12). Plus précisémment, à partir d'un n-cocycle $f \in Z^n(G, C)$, on construit d'abord un relèvement $\tilde{f} \in C^n(G, B)$, qui est une n-cochaîne, de telle façon que $\pi_n(\tilde{f}) = f$.

Ensuite, on applique d_n à $\tilde{f}$: $d_n(\tilde{f}) \in C^{n+1}(G, B)$, d'où $\pi_n(d_n(\tilde{f})) = d_n(f) = 0$. Alors $d_n(\tilde{f}) \in \mathrm{Ker}(\pi_{n+1}) = \mathrm{Im}(i_{n+1})$ définie alors un $(n+1)$-cocycle $\varphi \in Z^{n+1}(G, A)$, $d_n(\tilde{f}) = i_{n+1}(\varphi)$, et on pose $\Delta_n(\text{classe}(f)) = \text{classe}(d_n(\tilde{f}))$. En effet, $i_{n+1}(d_{n+1}\varphi) = d_{n+1}(d_n(\tilde{f})) = 0$, donc φ est un $(n+1)$-cocycle puisque $d_{n+1}\varphi = 0$ (i_{n+1} est une injection).

$$\begin{array}{ccccc}
C^0(G,A) & \xrightarrow{i_0} & C^0(G,B) & \xrightarrow{\pi_0} & C^0(G,C) \\
\downarrow{\scriptstyle d_0} & & \downarrow{\scriptstyle d_0} & & \downarrow{\scriptstyle d_0} \\
C^1(G,A) & \xrightarrow{i_1} & C^1(G,B) & \xrightarrow{\pi_1} & C^1(G,C) \\
\downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_1} \\
C^2(G,A) & \xrightarrow{i_2} & C^2(G,B) & \xrightarrow{\pi_2} & C^2(G,C) \\
\downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_2} \\
\cdots & \longrightarrow & \cdots & \longrightarrow & \cdots \\
\downarrow{\scriptstyle d_{n-1}} & & \downarrow{\scriptstyle d_{n-1}} & & \downarrow{\scriptstyle d_{n-1}} \\
C^n(G,A) & \xrightarrow{i_n} & C^n(G,B) & \xrightarrow{\pi_n} & C^n(G,C) \ni f \\
\downarrow{\scriptstyle d_n} & & \downarrow{\scriptstyle d_n} & & \downarrow{\scriptstyle d_n} \\
i_{n+1}^{-1}(d_n(\tilde{f})) \in C^{n+1}(G,A) & \xrightarrow{i_{n+1}} & C^{n+1}(G,B) & \xrightarrow{\pi_{n+1}} & C^{n+1}(G,C)
\end{array} \tag{12.12}$$

(2) Théorie de Kummer

Exemple 12.2.1 *Soit K un corps contenant le groupe μ_n de toutes les racines primitives n-iémes. Puis, on suppose que la caractéristique* $\mathrm{car}K$ *ne divise pas n. Pour toute extension galoisienne L/K de groupe de Galois $G = G(L/K)$ l'application $x \mapsto x^n$ définie un homomorphisme de G–modules : $\nu : L^* \longrightarrow L^*$. Considérons un sous groupe $C \subset K^*$ du groupe multiplicatif contenant K^{*n}, tel que le groupe quotient $C/(K^*)^n$ soit fini.*

On considère l'extension galoisienne $L = K(C^{1/n})$, engendrée par toutes les racines n-ièmes $\sqrt[n]{c}$ de $c \in C$. Alors on a une injection

$$G_C = \mathrm{Gal}(K(C^{1/n})/K) \longrightarrow \prod_{c \in C/K^{*n}} \mathrm{Gal}(K(c^{1/n})/K). \tag{12.13}$$

C'est une extension abélienne d'exposante n puisque chaque groupe $\mathrm{Gal}(K(c^{1/n})/K)$ *est cyclique d'ordre un diviseur de n (voir le théorème 10.3.2).*

On utilise l'application

$$\langle \cdot, \cdot \rangle \ : G_C \times C \longrightarrow \mu_n, \ \textit{définie par } \langle \sigma, c \rangle = \frac{\sigma(c^{1/n})}{c^{1/n}} \tag{12.14}$$

On vérifie aisément que l'application (12.14) est bimultiplicative.

Proposition 12.2.2 *L'application (12.14) est* non-dégénérée, *c'est-à-dire, qu'elle induit des injections*

$$\varphi_1 : G_C \longrightarrow \mathrm{Hom}(C/K^{*n}, \mu_n), \sigma \longmapsto (\bar{c} \mapsto \langle \sigma, c \rangle) \tag{12.15}$$

$$\varphi_2 : C/K^{*n} \longrightarrow \mathrm{Hom}(G_C, \mu_n), \bar{c} \longmapsto (\sigma \mapsto \langle \sigma, c \rangle) \tag{12.16}$$

Démonstration : Pour montrer l'injectivité de φ_1, on considère un $\sigma \in G$, avec $\sigma(c^{1/n}) = c^{1/n}$ pour tous les $c \in C$. Ceci implique $\sigma(a) = a$ pour tout $a \in K(C^{1/n})$, c'est-à-dire, que $\sigma = \mathrm{id}$. Donc φ_1 est

injective. D'autre part, soit $c \in C$, avec $\sigma(c^{1/n}) = c^{1/n}$ pour tous les $\sigma \in G_C$, alors $c^{1/n} \in K^*$, donc $c \in K^{*n}$, donc φ_2 est aussi injective.

On peut observer que φ_1 et φ_2 sont en fait des isomorphismes, à partir des inégalités évidentes :

$$[K(C^{1/n}) : K] = |G_C| \leq |\mathrm{Hom}(C/K^{*n}, \mu_n) = |C/K^{*n}|$$
$$|\mathrm{Hom}(C/K^{*n}| = |G_C| = [K(C^{1/n}) : K],$$

on utilise (12.13) pour voir que $K(C^{1/n})/K$ est une extension abélienne d'exposant n.

COROLLAIRE 12.2.3 *Soit K un corps contenant le groupe μ_n de toutes les racines primitives n-iémes. Puis, on suppose que la caractéristique* car$K$ *ne divise pas n.*

Alors, il existe des bijections naturelles

$$\left\{ \begin{array}{c} \textit{Sous groupes } C \subset K^* \\ \textit{avec } K^{*n} \subset C \textit{et } C/K^{*n} \textit{fini} \end{array} \right\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \left\{ \begin{array}{c} \textit{Extensions abéliennes finies } L/K \\ \textit{avec l'exposant un diviseur de } n \end{array} \right\} \tag{12.17}$$

$$C \overset{\Phi}{\longmapsto} L = K(C^{1/n}); \qquad L \overset{\Psi}{\longmapsto} L^n \cap K^*. \tag{12.18}$$

PREUVE : Par la proposition 12.2.2, il reste à montrer que Φ et Ψ sont inverses l'un de l'autre. On commence par $\Phi \circ \Psi = \mathrm{id}$, et considérons un sous groupe $C \subset K^*$ tel que $K^{*n} \subset C$et C/K^{*n} est fini. On pose $C' = K(C^{1/n})^n \cap K^*$. Alors par la définition $C \subset C'$, et de plus $K(C^{1/n}) = K(C'^{1/n})$.

Une façon très naturelle pour obtenir l'isomorphisme de Kummer
$C/K^{*n} \cong \mathrm{Hom}(G(L/K), \mu_n)$, est à partir de la cohomologie galoisienne : on utilise la suite exacte des $G = G(L/K)$-modules

$$1 \longrightarrow \mu_n \longrightarrow L^* \xrightarrow{\nu} L^{*n} \longrightarrow 1.$$

Considérons les groupes de cohomologie (12.11) on obtient la longue suite exacte suivante

$$\begin{aligned} &H^0(G(L/K), \mu_n) \longrightarrow H^0(G(L/K), L^*) \xrightarrow{\nu} H^0(G(L/K), (L^*)^n) \longrightarrow \\ &H^1(G(L/K), \mu_n) \longrightarrow H^1(G(L/K), L^*) \xrightarrow{\nu} H^1(G(L/K), (L^*)^n) \longrightarrow \cdots . \end{aligned} \tag{12.19}$$

Puisque le groupe $G(L/K)$ opère trivialement sur μ_n, il vient que $H^1(G(L/K), \mu_n)$ coïncide avec le groupe $\mathrm{Hom}(G(L/K), \mu_n)$. Le groupe $H^0(G(L/K), L^*)$ est le sous groupe de tous les éléments fixés par le groupe de Galois, i.e. $H^0(G(L/K), L^*) = L^{*G(L/K)} = K^*$, de plus $H^0(G(L/K), L^{*n}) = K^* \cap L^{*n} \supset C$, et on a montré dans le corollaire 12.17 que $K^* \cap L^{*n} = C$.

Ensuite, $H^0(G(L/K), \mu_n) = \mu_n$, et $H^1(G(L/K), L^*) = \{1\}$ par le théorème de Hilbert 90 sous la forme générale (le théorème 12.1.2). On obtient donc la suite exacte suivante

$$1 \longrightarrow \mu_n \longrightarrow K^* \xrightarrow{\nu} C \longrightarrow \mathrm{Hom}(G(L/K), \mu_n) \longrightarrow 1,$$

équivalent à l'isomorphisme de Kummer :

$$C/K^{*n} \cong \mathrm{Hom}(G(L/K), \mu_n).$$

3) Soit H un sous groupe distingué d'un groupe fini G et soit A un G–module. Alors on a la suite exacte suivante d'"inflation - restriction"

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(H, A), \tag{12.20}$$

dans laquelle Inf désigne l'homomorphisme d'inflation, définie par l'"inflation " d'un cocycle f sur G/H à valeurs dans $A^H \subset A$ vers un cocycle f sur G ; et Res est l'homomorphisme de la restriction donné par la restriction des cocycles de G sur le sous groupe H.

REMARQUE. De façon similaire on peut donner une définition générale des groupes d'homologie d'un groupe fini G, noté multiplicativement, à coefficients dans un G–module A noté additivement.

Les groupes d'homologie de G à coefficients dans A sont définies à l'aide du *complexe des chaînes*. On considère les groupes abéliens (les G-modules) suivants :

$$C_0(G, A) = A,$$

et pour $n \geq 1$

$$C_n(G, A) = \{f : G \times \cdots \times G \to A\}$$

(l'addition des fonctions et l'action de G se fait point-par-point).

On définit le morphisme $\partial_n : C_n(G, A) \to C_{n-1}(G, A)$ de *n-bord* par la formule :

$$\begin{aligned}(\partial_n f)(g_1, \ldots, g_{n-1}) = &\sum_{g \in G} g^{-1} f(g g_1, \ldots, g_{n-1}) \\ &+ \sum_{i=1}^{n-1} (-1)^i \sum_{g \in G} f(g_1, \ldots, g_i g, g^{-1}, g_{i+1}, \ldots, g_{n-1}) \\ &+ (-1)^n \sum_{g \in G} f(g_1, \ldots, g_{n-1}, g),\end{aligned} \tag{12.21}$$

Ensuite, on vérifie l'égalité $\partial_n \circ \partial_{n+1} = 0$.

Le groupe $Z_n(G, A) = \operatorname{Ker} \partial_n$ est appelé le groupe des *n–cycles*, et le groupe $B_n(G, A) = \operatorname{Im} d_{n+1}$ est appelé le groupe des *n–bords*. La propriété $\partial_n \circ \partial_{n-1} = 0$ implique que $B_n(G, A) \subset Z_n(G, A)$. On définit alors les groupes d'homologie par

$$H_n(G, A) = B_n(G, A)/Z_n(G, A) = \begin{cases} \operatorname{Ker} \partial_n / \operatorname{Im} \partial_{n+1} & \text{pour } n \geq 1; \\ A / \operatorname{Im} \partial_1 & \text{pour } n = 0. \end{cases} \tag{12.22}$$

Si $n = 0$ alors

$$H_0(G, A) = A_G \tag{12.23}$$

le plus grand module quotient de A sur lequel G opère trivialement

Puis, on peut identifier le groupe $H_1(G, \mathbb{Z})$ avec le groupe quotient G/G', voir [Se63], p. 122.

EXERCICE. Vérifier l'identité $\partial_n \circ \partial_{n+1} = 0$ pour $n = 1$.

13 Une application : extensions d'Artin-Schreier

13.1 Une forme additive du théorème 90 de Hilbert

Considérons une extension finie galoisienne L/K de groupe $G = \mathrm{Gal}(L/K)$, et le groupe additif $M = L$ muni d'action naturelle de G.

Théorème 13.1.1 (Théorème 90 de Hilbert, forme additive)

$$H^n(G(L/K), L) = \begin{cases} K = L^G, & si\ n = 0 \\ \{0\}, & si\ n > 0. \end{cases}$$

On peut déduire ce résultat à partir de l'existence d'une base normale de L/K, qui signifie que L est un $K[G]$-module libre de rang 1, cf. [Se64].

Cependant, nous donnons une preuve directe du fait $H^n(G(L/K), L) = \{0\}$, si $n > 0$, sans utiliser une base normale. Nous utilisons de nouveau le fait que pour toute extension galoisienne L/K il existe un $a \in L$ tel que $\mathrm{Tr}_{L/K}(a) = 1 = \sigma_1(a) + \cdots + \sigma_n(a)$, où $\mathrm{Gal}(L/K) = \{\sigma_1, \cdots, \sigma_n\}$, voir la preuve du théorème 3.2.3.

Démonstration : On considère un n-cocycle $f \in Z^n(G, L)$, et on cherche à construire un $(n-1)-$cochaîne $\varphi \in C^{n-1}(G, L)$, telle que $f = d_{n-1}(\varphi)$. On va chercher φ sous la forme d'une série de Poincaré :

$$\varphi(g_1, \cdots, g_{n-1}) = \sum_{g_n \in G} f(g_1, \cdots, g_{n-1}, g_n)(g_1 \cdot \ldots \cdot g_{n-1} g_n)(a) \tag{13.1}$$

Si, par exemple, $n = 1$ on considère l'élément

$$b = \sum_{g \in G} f(g) g(a) \in L. \tag{13.2}$$

On applique aux deux parties de (13.2) (avec la notation $g = \sigma' \in G$) un élément $\sigma \in G$. Alors

$$\begin{aligned} \sigma(b) &= \sum_{\sigma' \in G} \sigma(f(\sigma'))\sigma(\sigma'(a)) = \sum_{\sigma' \in G} \sigma' f(\sigma')(\sigma \circ \sigma')(a) \\ &= \sum_{\sigma' \in G} f(\sigma \circ \sigma')(\sigma \circ \sigma')(a) - f(\sigma) \sum_{\sigma' \in G} \sigma'(a) \\ b - \mathrm{Tr}_{L/K}(a) f(\sigma) &= b - f(\sigma). \end{aligned}$$

(par la formule de l'action gauche de G sur $L^\times$, $\sigma(\sigma'(\gamma)) = \sigma \circ \sigma'(\gamma)$ for $\sigma, \sigma'(\gamma) \in G$).

Cette méthode de la somme moyenne (série de Poincaré) $b = \sum_{\sigma' \in G} f(\sigma')\sigma'(\gamma) \in L$ est aussi connue comme la méthode de la *résolvante de Lagrange* dans la théorie des extensions de corps.

Exercice. Vérifier l'identité $d_{n-1}\varphi = f$ à partir de la définition (13.1) pour $n \geq 2$.

13.2 Théorie d'Artin-Schreier pour un exposant première

Soit K un corps de caractéristique $\mathrm{car}K = p > 0$. Pour toute extension galoisienne L/K de groupe de Galois $G = G(L/K)$ l'application $x \mapsto \wp(x) = x^p - x$ définie un homomorphisme de G–modules : $\wp : L \longrightarrow L$. Considérons un sous groupe $C \subset K$ du groupe additif contenant $\wp(K)$, tel que le groupe quotient $C/\wp(K)$ soit *fini*.

On considère l'extension galoisienne $L = K(\wp^{-1}(C))$, engendrée par toutes les racines du polynôme $\wp(x) = c$, $c \in C$. Alors on a une injection

$$G_C = \mathrm{Gal}(K(\wp^{-1}(C))/K) \longrightarrow \prod_{c \in C/\wp(K)} \mathrm{Gal}(K(\wp^{-1}(c))/K).$$

C'est une extension abélienne d'exposante p puisque chaque groupe $\mathrm{Gal}(K(\wp^{-1}(c))/K)$ est cyclique d'ordre p.

On utilise l'application

$$\langle \cdot, \cdot \rangle \ : G_C \times C \longrightarrow \mathbb{F}_p, \text{ définie par } \langle \sigma, c \rangle = \sigma(\wp^{-1}(c)) - \wp^{-1}(c) \in \mathbb{F}_p \tag{13.3}$$

On vérifie aisement que l'application (13.3) est biadditive.

Proposition 13.2.1 *L'application (13.3) est* non-dégénérée*, c'est-à-dire, qu'elle induit des injections*

$$\varphi_1 : G_C \longrightarrow \mathrm{Hom}(C/\wp(K), \mathbb{F}_p), \sigma \longmapsto (\bar{c} \mapsto \langle \sigma, c \rangle) \tag{13.4}$$
$$\varphi_2 : C/\wp(K) \longrightarrow \mathrm{Hom}(G_C, \mathbb{F}_p), \bar{c} \longmapsto (\sigma \mapsto \langle \sigma, c \rangle) \tag{13.5}$$

Démonstration : Pour montrer l'injectivité de φ_1, on considère un $\sigma \in G$, avec $\sigma(\wp^{-1}(c)) = \wp^{-1}(c)$ pour tous les $c \in C$. Ceci implique $\sigma(a) = a$ pour tout $a \in K(\wp^{-1}(C))$, c'est-à-dire, que $\sigma = \mathrm{id}$. Donc φ_1 est injective. D'autre part, soit $c \in C$, avec $\sigma(\wp^{-1}(c)) = \wp^{-1}(c)$ pour tous les $\sigma \in G_C$, alors $\wp^{-1}(c) \in K$, donc $c \in \wp(K)$, donc φ_2 est aussi injective.

Corollaire 13.2.2 *Soit K un corps de caractéristique* $\mathrm{car}K = p > 0$.

Alors, il existe des bijections naturelles

$$\left\{ \begin{array}{c} \textit{Sous groupes } C \subset K \\ \textit{avec } \wp(K) \subset C \textit{et } C/\wp(K) \textit{fini} \end{array} \right\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \left\{ \begin{array}{c} \textit{Extensions abéliennes finies } L/K \\ \textit{de l'exposant } p \end{array} \right\} \tag{13.6}$$

$$C \overset{\Phi}{\longmapsto} L = K(\wp^{-1}(C)); \qquad L \overset{\Psi}{\longmapsto} \wp(L) \cap K. \tag{13.7}$$

Preuve : Par la proposition 13.2.1, il reste à montrer que Φ et Ψ sont inverses l'un de l'autre. On commence par $\Phi \circ \Psi = \mathrm{id}$, et considérons un sous groupe $C \subset K$ tel que $\wp(K) \subset C$et $C/\wp(K)$ est fini. On pose $C' = \wp(K(\wp^{-1}(C)) \cap K$. Alors par la définition $C \subset C'$, et de plus $K(\wp^{-1}(C)) = K(\wp^{-1}(C'))$.

Ensuite, la suite exacte des $G = G(L/K)$-modules

$$0 \longrightarrow \mathbb{F}_p \longrightarrow L \overset{\wp}{\longrightarrow} \wp(L) \longrightarrow 0.$$

Considérons les groupes de cohomologie (12.11) on obtient la longue suite exacte suivante

$$\begin{aligned} &H^0(G(L/K), \mathbb{F}_p) \longrightarrow H^0(G(L/K), L) \overset{\wp}{\longrightarrow} H^0(G(L/K), \wp(L)) \longrightarrow \\ &H^1(G(L/K), \mathbb{F}_p) \longrightarrow H^1(G(L/K), L) \overset{\wp}{\longrightarrow} H^1(G(L/K), \wp(L)) \longrightarrow \cdots . \end{aligned} \tag{13.8}$$

Puisque le groupe $G(L/K)$ opère trivialement sur $\mathbb{F}_p$, il vient que $H^1(G(L/K), \mathbb{F}_p)$ coïncide avec le groupe $\mathrm{Hom}(G(L/K), \mathbb{F}_p)$. Le groupe $H^0(G(L/K), L)$ est le sous groupe de tous les éléments fixés par le groupe de Galois, i.e. $H^0(G(L/K), L) = L^{G(L/K)} = K$, de plus $H^0(G(L/K), \wp(L)) = K \cap \wp(L) \supset C$, et on a montré que $K \cap \wp(L) = C$.

Ensuite, $H^0(G(L/K), \mathbb{F}_p) = \mathbb{F}_p$, et $H^1(G(L/K), L) = \{0\}$ par le théorème de Hilbert 90 (forme additive). On obtient donc la suite exacte suivante

$$0 \longrightarrow \mu_n \longrightarrow K \overset{\wp}{\longrightarrow} C \longrightarrow \mathrm{Hom}(G(L/K), \mathbb{F}_p) \longrightarrow 0,$$

équivalent à l'isomorphisme d'Artin-Schreier :

$$C/\wp(K) \cong \mathrm{Hom}(G(L/K), \mathbb{F}_p).$$

Remarque. Pour décrire les extensions abéliennes finies L/K de l'exposante p^n, on utilise l'anneau de Witt $W_n(L)$, muni d'opérateur de Frobenius F [Se63], p.49, [Bosch], p.224, où on prouve que

$$H^1(G(L/K), W_n(L)) = 0.$$

La description souhaitée vient de la suite exacte :

$$0 \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow W_n(L) \xrightarrow{F-1} (F-1)(W_n(L)) \longrightarrow 0.$$

14 Exercices de préparation à l'examen

14.1 Contrôle continu (élargi) du jeudi 17 mars 2005, 10h15–12h15, AMPHI A

1. (a) Trouver le nombre des polynômes unitaires irréductibles de degré 6 sur $\mathbb{F}_4$.
(b) Trouver le produit de tous les polynômes unitaires irréductibles de degré 6 sur $\mathbb{F}_4$.

2. (a) Construire un corps K et une extension galoisienne L/K, tels que le groupe de Galois $\mathrm{Gal}(L/K)$ est isomorphe au groupe symétrique S_4.
(b) Trouver toutes les sous-extensions galoisiennes F/K, $F \subset L$.
(c) Pour toute telle sous-extension F/K, trouver un élément $\beta \in F$, telle que $F = K(\beta)$.
(d) Pour toute telle sous-extension F/K, construire une base normale
3. On considère une extension galoisienne L/K de groupe de Galois $\mathrm{Gal}(L/K)$, isomorphe au groupe symétrique S_4.

Donner un exemple de deux sous-extensions E_1/K et E_2/K, ($E_1 \subset L$, $E_2 \subset L$) telles que E_1, E_2 ne sont pas inclus, le composé $E_1 \cdot E_2$ ne soit pas égale à L, et que l'intersection $E_1 \cap E_2$ ne soit pas égale à K.
(b) Trouver explicitement un $\beta_1 \in E_1$ et un $\beta_2 \in E_2$ tels que $E_1 = K(\beta_1)$, $E_2 = K(\beta_2)$.

4. Soit $\mathbb{F}_q$ un corps fini de $q \geq 3$ éléments.
(a) Déterminant de Moore. Soit k un corps contenant $\mathbb{F}_q$, $\beta_1, \cdots, \beta_n \in k$. Montrer que

$$\begin{vmatrix} \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \cdots & \beta_2^{q^{n-1}} \\ \cdots & \cdots & \cdots & \cdots \\ \beta_n & \beta_n^q & \cdots & \beta_n^{q^{n-1}} \end{vmatrix} = \beta_1 \prod_{j=1}^{n-1} \prod_{c_1,\cdots,c_j \in \mathbb{F}_q} (\beta_{j+1} - \sum_{i=1}^{j} c_i \beta_i).$$

(considerer les deux parties comme des polynômes de β_n et utiliser la factorisation du polynôme $T^q - T$ sur $\mathbb{F}_q$).
(b) Produit des polynômes unitaires. On utilisera la notation $[n] := T^{q^n} - T$. En déduire que

$$P_n := \prod_{\substack{f \text{ unitaire} \\ \deg f = n}} f(T) = \prod_{m=1}^{n} [m]^{q^{n-m}} = \prod_{m=1}^{n} (T^{q^m} - T)^{q^{n-m}}.$$

(c) Factoriel de Carlitz. Soit

$$D_t = \prod_{\substack{f \text{ unitaire} \\ \deg f \leq t}} f(T)$$

Montrer que

$$D_t = \prod_{n=1}^{t} P_n = \prod_{n=1}^{t} \prod_{m=1}^{n} [m]^{q^{n-m}} = \prod_{n=1}^{t} \prod_{m=1}^{n} (T^{q^m} - T)^{q^{n-m}}.$$

14.2 Exercices supplémentaires

On considère le polynôme à coefficients rationnels

$$P(T) = T^3 - 3T - 1.$$

1. Montrer que P est irréductible sur $\mathbb{Q}$ et qu'il possède trois racines réelles α_1, α_2, α_3, telles que $\alpha_3 < \alpha_2 < 0 < \alpha_1$.

Indication : Le polynôme P est irréductible si et seulement si le polynôme P_1 défini par $P_1(T) = P(T+1) = T^3 + 3T - 3$ l'est ; c'est le cas (critère d'Eisenstein pour $p = 3$).

Le tableau des variation de la fonction continue $x \mapsto P(x)$ montre que P a trois racines réelles vérifiant $\alpha_3 < \alpha_2 < 0 < \alpha_1$.

2. (a) Montrer que si α est racine P, il en est de même de $2 - \alpha^2$. On pose $K = \mathbb{Q}(\alpha_1)$.

(b) Montrer que l'extension $K/\mathbb{Q}$ est galoisienne, et que tout élément de son groupe de Galois induit une permutation paire sur l'ensemble $\{\alpha_1, \alpha_2, \alpha_3\}$.

Indication : 2. (a) Si $P(\alpha) = 0$, on vérifie facilement que $P(2 - \alpha^2) = 0$. On remarque que $\alpha \neq 2 - \alpha^2$ (puisque $\{1, \alpha, \alpha^2\}$ est une base de $\mathbb{Q}(\alpha)/\mathbb{Q}$.

(b) La somme des racines de P vaut 0, donc la troisième racine est égale à $\alpha^2 - \alpha - 2$, et toutes les racines de P sont dans $\mathbb{Q}(\alpha)$.

Le corps K est le corps de décomposition d'un polynôme séparable sur $\mathbb{Q}$, donc l'extension $K/\mathbb{Q}$ est galoisienne de groupe de Galois Γ d'ordre $[K : \mathbb{Q}] = 3$. Tout élément de Γ permute les racines de P, et il est d'ordre 1 ou 3 : il induit donc une permutation paire de ces racines.

3. Pour chaque $i \in \{1, 2, 3\}$, on choisit un nombre complexe β_i, de sorte que $\beta_i^2 = \alpha_i$, et $\beta_1\beta_2\beta_3 = 1$. On pose $L = K(\beta_1, \beta_2, \beta_3)$.

(a) Déterminer $[K(\beta_1) : K]$ On pourra remarquer que tout élément de $K(\beta_1)$ est réel, et étudier les images de β_1 et de β_1^2 par les automorphismes de K si l'on suppose β_1 dans K).

(b) Montrer que $L = \mathbb{Q}(\beta_1, \beta_2)$, et déterminer $[L : \mathbb{Q}]$.

Indication : 3. Comme $\alpha_1\alpha_2\alpha_3 = 1$, on peut choisir les β_i tels que $\beta_1\beta_2\beta_3 = 1$.

(a) Soit g un élément de Γ tel que $g(\alpha_1) = \alpha_2$. Si β_1 était dans K, galoisienne, $g(\beta_1)$ le serait aussi, et serait réel. Si on aurait $g(\beta_1^2) = [g(\beta_1)]^2 = \alpha_2 < 0$, ce qui est impossible. Donc le polynôme $T^2 - \alpha_1 \in K[T]$ est irréductible, et $[K(\beta_1) : K] = 2$.

(b) Comme $\beta_1\beta_2\beta_3 = 1$, on a $L = K(\beta_1, \beta_2, \beta_3) = K(\beta_1, \beta_2)$; la racine β_2 est imaginaire pure, donc n'appartient pas à $K(\beta_1)$, et $[L : K(\beta_1)] = 2$; d'où $L = \mathbb{Q}(\alpha_1, \beta_1, \beta_2) = \mathbb{Q}(\beta_1, \beta_2)$.

4. (a) Montrer que l'extension $L/\mathbb{Q}$ est galoisienne. On note G son groupe de Galois, et H celui de l'extension L/K.

(b) Le groupe H est-il un sous-groupe distingué de G ? Que peut-on dire de nombre N_2 de 2-sous groupes de Sylow de G ?

Indication : 4. (a) Le polynôme $T^6 - 3T^3 - 1$ admet six racines distinctes dans L, $\pm\beta_1$, $\pm\beta_2$,$\pm\beta_3$. Donc L est corps de décomposition d'un polynôme séparable sur $\mathbb{Q}$, et l'extension $L/\mathbb{Q}$ est galoisienne.

(b) L'extension $K/\mathbb{Q}$ étant galoisienne, le groupe de Galois H de l'extension L/K est distingué dans G. D'autre part, H est d'ordre 4 dans G d'ordre 12 : c'est l'unique 2-sous groupe de Sylow de G, et $N_2 = 1$.

5. (a) Montrer que les éléments σ de G peuvent être définis par la donnée de $\sigma(\beta_1)$ et $\sigma(\beta_2)$. Retrouver de cette manière l'ordre du groupe G.

(b) Quelle est la structure de H ?

(c) Que vaut le nombre N_3 de 3-sous groupes de Sylow de G ?

(d) En déduire que G est isomorphe au groupe A_4 des permutations paires de 4 symboles.

Indication : 5. (a) Le corps L admet comme L-base $\{\beta_1^i\beta_2^j\}$, avec $0 \leq i \leq 5$, $0 \leq j \leq 1$. Tout élément de G est donc caractérisé par la donnée de $\sigma(\beta_1)$, et celle de $\sigma(\beta_2)$.

La valeur de $\sigma(\beta_1)$ est à prendre dans l'ensemble $\{\pm\beta_1, \pm\beta_2, \pm\beta_3\}$. Une fois que $\sigma(\beta_1)$ est fixé, les éléments $\sigma(\alpha_1)$, $\sigma(\alpha_2)$ et $\sigma(\alpha_3)$ le sont aussi, et $\sigma(\beta_2)$ est racine du polynôme $T^2 - \sigma(\alpha_2)$.

Cela donne douze possibilités, qui correspondent exactement aux douze éléments de G.

(b) Un élément σ de H laisse $K = \mathbb{Q}(\alpha_2)$ invariant, donc $\sigma(\beta_1^2) = \alpha_1$, et $\sigma(\beta_2) = \pm\beta_2$. Par suite, σ est d'ordre 1 ou 2, et comme H est d'ordre 4, H est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(c) Les théorèmes de Sylow donnent, pour un groupe d'ordre 12, $N_3 = 1$ ou $N_3 = 4$. Un 3-sous groupe de Sylow possède deux éléments d'ordre 3. On montre que $N_3 = 4$ en trouvant dans G trois élément d'ordre 3.

(d) Le groupe G est non abélien d'ordre 12, avec $N_2 = 1$ et $N_3 = 4$; on vérifie qu'il est donc isomorphe à A_4.

6. On pose $\theta_1 = \beta_1 + \beta_2 + \beta_3$.

(a) Donner les images de θ_1 par les éléments de G. En déduire $[\mathbb{Q}(\theta_1) : \mathbb{Q}]$.

(b) L'extension $\mathbb{Q}(\theta_1)/\mathbb{Q}$, est-elle galoisienne ?

Indication : 6. (a) Les images de θ_1 par les éléments de G sont les quatre éléments distincts suivants : $\theta_1 = \beta_1 + \beta_2 + \beta_3$, $\theta_2 = -\beta_1 + \beta_2 - \beta_3$, $\theta_3 = \beta_1 - \beta_2 - \beta_3$, $\theta_4 = -\beta_1 - \beta_2 + \beta_3$. Soit A le polynôme minimal de θ_1 sur $\mathbb{Q}$. Comme $L/\mathbb{Q}$ est galoisienne, A se décompose en produit de facteurs de degré 1 dans $L[T]$, et ses racines sont les images (distinctes) de θ_1 par les éléments de G. Donc E est de degré 4, et $[\mathbb{Q}(\theta_1) : \mathbb{Q}] = 4$.

(b) Le sous groupe de G qui laisse fixe $\mathbb{Q}(\theta_1)$, est d'ordre 3 ; comme $N_3 = 4$, ce sous groupe n'est pas distingué, et l'extension $\mathbb{Q}(\theta_1)/\mathbb{Q}$ n'est pas galoisienne.

7. Déterminer toutes les extensions intermédiaires de $L/\mathbb{Q}$.

Indication : Les sous groupes de A_4, distincts de A_4 et de $\{e\}$, sont d'ordre 2, 4 ou 3. Il n'y a qu'un sous groupe d'ordre 4, H, qui laisse fixe K, et trois sous groupes d'ordre 2 qui laissent fixes les corps $\mathbb{Q}(\beta_1)$, $\mathbb{Q}(\beta_2)$ et $\mathbb{Q}(\beta_3)$.

Les quatre sous groupes d'ordre 3 sont ceux qui laissent fixes les corps $\mathbb{Q}(\theta_1)$, $\mathbb{Q}(\theta_2)$, $\mathbb{Q}(\theta_3)$ et $\mathbb{Q}(\theta_4)$.

A Annexe : Factorisation des Polynômes (F. SERGERAERT)

- **Référence : Don Knuth, The Art of Computer Programming, vol. 2, pp. 381-398.**

```
> restart ;
> with(linalg) :
```

```
Warning, the protected names norm and trace have been redefined and
unprotected
```

- La factorisation des polynômes n'est pas un sujet vraiment facile, pas plus que la factorisation des entiers ! On présente ici le principal outil, la *méthode de Berlekamp*, qui concerne en fait la factorisation dans le cas du *corps de base fini*, puis on explique dans les cas les plus simples comment elle peut être utilisée pour obtenir la factorisation des polynômes à coefficients rationnels.

A.1 Rappels sur les corps finis.

- On rappelle que p est premier si et seulement si tous les coefficients du binôme C(p, k) sont divisibles par p pour $0 < k < p$:

```
> seq(evalb(binomial(13,k) mod 13 = 0), k = 0..13) ;
> seq(evalb(binomial(9,k) mod 9 = 0), k = 0..9) ;
```

false, *true*, *true*, *true*, *true*, *true*, *true*, *true*, *true*, *true*, *true*, *true*, *true*, *false*

false, *true*, *true*, *false*, *true*, *true*, *false*, *true*, *true*, *false*

- Il en résulte que si on travaille dans $Z/\ p$, la formule $(a+b)^p = a^p + b^p$ est valide, en particulier $(a+1)^p = a^p + 1$ et il en résulte par récurrence, partant de $1^p = 1$, que $a^p = a$ dans $Z/\ p$.

- Un corps K fini est de caractéristique bien définie p : c'est le plus petit entier positif vérifiant p x 1 = (déf.) 1 + 1 + ... + 1 (p fois) = 0. Nécessairement, p est *premier*, sinon on aurait dans K des diviseurs de 0. Le corps K contient donc en particulier le sous-corps {0, 1, 2, ..., $p-1$} = $Z/\ p$ qu'on notera simplement Z_p et K est donc un espace vectoriel sur Z_p de dimension d ; il a alors p^d éléments. La formule démontrant que le *morphisme de Frobenius* $a \to a^p$ est *Z-linéaire* (et donc aussi Z_p-linéaire) : $(a+b)^p = a^p + b^p$ reste valable, mais il est maintenant *faux*, sauf si d=1, que $a^p = a$ pour tout a de K. En effet, puisque $X^p - X$ est de degré p, il ne peut avoir que p racines dans K, à savoir les éléments de Z_p dans K. On verra que cette remarque est la clé de la *méthode de Berlekamp* pour factoriser un polynôme à coefficients dans Z_p.

- Le groupe *multiplicatif* des éléments non nuls de K a pour cardinal $p^d - 1$, et il en résulte que pour tous ces éléments, la relation $a^{(p^d-1)} = 1$ est satisfaite ; le polynôme $X^{(p^d)} - X$ a donc pour racines tous ces éléments, et de plus l'élément nul. Les éléments de K sont donc tous racines de ce polynôme,et il en résulte que $X^{(p^d)} - X = \prod_a (X - a)$ où a parcourt exactement tous les éléments de K. Donc K est un (donc *le*) corps de décomposition de ce polynôme et il en résulte qu'il n'existe qu'un seul corps de cardinal p^d.

- Soit P dans $Z_p[\,X]$ un polynôme *irréductible* de degré d. Alors le quotient $Z_p[\,X]/\,P$ est un corps à p^d éléments. Il résulte de ce qui précède que la *classe d'isomorphisme* de ce corps est indépendante de P. Le polynôme P divise nécessairement le polynôme $X^{(p^d)}$- X ; en effet, si x est la classe de X dans $Z_p\,[\,X]/\,P$, le polynôme minimal de x ne peut être que P, mais d'après ce qui est dit ci-dessus, x est aussi racine de $X^{(p^d)}$ - X et donc ce dernier polynôme est divisible par P. Il en résulte aussi que P est *entièrement* scindé dans K, donc une seule extension suffit toujours pour obtenir le corps de décomposition d'un polynôme irréductible : toute extension de Z_p est *galoisienne*.

Illustration.

```
> rnd := rand(0..2) :
```

- Contrairement au cas des coefficients entiers banals, il faut «tâtonner» un peu pour trouver un polynôme irréductible à coefficients dans Z_3.

```
> _seed := 1639 :
> P := sort(X^3 + add(rnd()*X^i, i=0..2)) ;
```

$$P := X^3 + 2\,X^2 + 1$$

```
> Irreduc(P) mod 3 ;
```

true

- Il en résulte que le même polynôme est Q-irréductible :

```
> irreduc(P) ;
```

true

- Mais la réciproque est *fausse* : il arrive souvent qu'un polynôme soit Q-irréductible, mais pas Z_p-irréductible ; il arrive même que ceci se produise *quel que soit* p pour le même polynôme Q-irréductible, c'est le cas de $X^4 + 1$.

```
> irreduc(X^4+1) ;
```

true

```
> Irreduc(X^4+1) mod 67 ;
```

false

```
> Factor(X^4+1) mod 67 ;
```

$$(X^2 + 47\,X + 66)\,(X^2 + 20\,X + 66)$$

```
> Factor(X^4+1) mod nextprime(10^6) ;
```

$$(X^2 + 410588\,X + 1000002)\,(X^2 + 589415\,X + 1000002)$$

- Pour travailler *sous Maple* dans des extensions de Z_p, on procède comme pour les extensions de Q, mais il n'y a *aucune différence* dans l'usage initial de **RootOf**, c'est seulement *en fin de calcul* qu'on précise qu'on veut travailler dans Z_p et ses extensions, en *suffixant* par «**mod p**».

```
> alias(alpha = RootOf(P)) ;
```

$$\alpha$$

- Le quotient $Z_3[\,X]/\,P$ est un espace vectoriel de degré 3 sur Z_3, dont les éléments sont tous de la forme $i + j\,\alpha + k\,\alpha^2$ pour i, j et k parcourant Z_3.

- Calcul du polynôme ayant *exactement* tous les éléments de $Z_3[\,X]/\,P$ comme racine

```
> mul(mul(mul(X-i-j*alpha-k*alpha^2,
> k=0..2),
> j=0..2),
> i=0..2) ;
```

$$X\,(X-\alpha^2)\,(X-2\,\alpha^2)\,(X-\alpha)\,(X-\alpha-\alpha^2)\,(X-\alpha-2\,\alpha^2)\,(X-2\,\alpha)\,(X-2\,\alpha-\alpha^2)$$
$$(X-2\,\alpha-2\,\alpha^2)\,(X-1)\,(X-1-\alpha^2)\,(X-1-2\,\alpha^2)\,(X-1-\alpha)\,(X-1-\alpha-\alpha^2)$$
$$(X-1-\alpha-2\,\alpha^2)\,(X-1-2\,\alpha)\,(X-1-2\,\alpha-\alpha^2)\,(X-1-2\,\alpha-2\,\alpha^2)\,(X-2)$$
$$(X-2-\alpha^2)\,(X-2-2\,\alpha^2)\,(X-2-\alpha)\,(X-2-\alpha-\alpha^2)\,(X-2-\alpha-2\,\alpha^2)$$
$$(X-2-2\,\alpha)\,(X-2-2\,\alpha-\alpha^2)\,(X-2-2\,\alpha-2\,\alpha^2)$$

- Développement du produit.

```
> Expand(%) mod 3 ;
```

$$2\,X+X^{27}$$

- ... autrement dit $X^{27}-X$. A comparer avec :

```
> collect(evala(expand(%%)), [X, alpha]) :
```

- Vérification de la propriété de divisibilité.

```
> Divide(X^27-X, P) mod 3 ;
```

true

- Et pour cause :

```
> Factor(P, alpha) mod 3 ;
```

$$(X+\alpha^2+\alpha+1)\,(X+2\,\alpha^2+1)\,(X+2\,\alpha)$$

- Car, comme expliqué plus haut, *une seule extension* suffit toujours à décomposer *complètement* le polynôme initial. Propriété en général fausse dans le cas rationnel :

```
> factor(P, alpha) ;
```

$$(X-\alpha)\,(X^2+2\,X+X\,\alpha+2\,\alpha+\alpha^2)$$

A.2 Bases de la méthode de Berlekamp

- On travaille dans l'anneau de polynômes $Z_p[\,X]$, pour un premier p, et sauf indication contraire, $Z_7[\,X]$ dans les exemples

- Soit P dans $Z_p[\,X]$ et $P = P_1 ... \,P_r$ sa décomposition en facteurs irréductibles. On suppose d'abord que P est sans facteur multiple, sinon ceci est détecté facilement par le PGCD du polynôme et du polynôme dérivé. Construisons un exemple de cette sorte.

```
> rnd := rand(0..6) :
> rndP := proc(n)
> RETURN(sort(X^n + add(rnd()*X^i, i=0..(n-1))))
> end :
> _seed := 1730 :
> P1, P2 := rndP(3), rndP(3) ;
```

$$P1,\ P2 := X^3 + X^2 + 2\,X + 4,\ X^3 + 4\,X^2 + 4\,X + 2$$

- Le polynôme qui suit va certainement avoir un facteur multiple, mais on *fait semblant* de ne rien savoir à ce propos.

```
> P := sort(Expand(P1^2 * P2) mod 7) ;
```

$$P := X^9 + 6\,X^8 + 3\,X^7 + 3\,X^4 + 5\,X^3 + 5\,X^2 + 5\,X + 4$$

- On détecte un facteur multiple éventuel par l'examen du PGCD entre le polynôme et son dérivé.

```
> Gcd(P, diff(P, X) mod 7) mod 7 ;
```

$$X^3 + X^2 + 2\,X + 4$$

- Et on commencerait par factoriser $X^3 + X^2 + 2\,X + 4$. Presque toujours (pas toujours, pourquoi ?) le polynôme initial est divisible par le carré de ce terme.

```
> Rem(P, %^2, X) mod 7 ;
```

$$0$$

```
> Quo(P, %%^2, X) mod 7 ;
```

$$X^3 + 4\,X^2 + 4\,X + 2$$

- ce qui redonne comme par hasard nos polynômes initiaux.

- On suppose donc désormais qu'il n'y a aucun facteur multiple dans P.

- Si $P = P_1 ... P_r$ est la décomposition de P en facteurs irréductibles, le *théorème du reste chinois* donne un isomorphisme canonique :

Z_p

$[\ X]/\ P = Z_p[\ X]/\ P_1 + ... Z_p[\ X]/\ P_r$. Les facteurs du second membre sont tous des corps, le premier membre n'est un corps que si P est irréductible, autrement dit si $r = 1$.

- Il en résulte, c'est l'astuce de Berlekamp, un test permettant, *sans connaître* r, de «deviner» sa valeur. Considérons en effet l'équation où l'inconnue V est un élément de $Z_p[\ X]/\ P$:

$V^P - V = 0$

- Si on traduit cette équation vers le second membre (qu'on ne connaît pas !), l'inconnue V devient un r-uplet $(\ V_1, ..., V_r)$, et comme l'isomorphisme utilisé *est un isomorphisme d'anneaux*, l'équation se transforme en r équations $V_i\ ^p = V_i$. Comme l'inconnue V_i est cette fois dans le *corps* $Z_p[\ X]/\ P_i$, on sait qu'il y a *exactement* les p racines 0, ..., $p-1$ dans $Z_p[\ X]/\ P_i$. On en déduit que le cardinal des solutions est *exactement* p^r. Ainsi le cardinal de l'ensemble des solutions va nous donner le nombre fatidique r. D'une façon très approximative, on peut dire que Berlekamp observe que *plus* P est réductible, *«moins»* $Z_p[\ X]/\ P$ est un corps, et plus l'ensemble des solutions de notre équation va être vaste.

- Le deuxième élément clé de la méthode de Berlekamp consiste à remarquer que puisque l'application $V \to V^p$ est *linéaire*, l'équation $V^p - V = 0$ est, malgré les apparences, une *équation linéaire*, et on dispose donc de tous les outils linéaires classiques pour la traiter.

- **Exemple.** Soit à étudier si notre polynôme **P1** est irréductible dans Z_7. Il faut construire la matrice de l'application linéaire $V \to V^p - V$ dans $Z_p[\ X]/\ P_1$. On prend la base canonique 1**,** X, X^2 (ou plus précisément leurs classes modulo P_1). L'image de X^j est donc la classe de $X^{(p\,j)} - X^j$, et les éléments de colonne correspondants sont les coefficients appropriés. On construit à part la procédure **BerlTerm** permettant le calcul du terme d'indices (i, j) de la *matrice de Berlekamp* du polynôme P par rapport à Z_p.

```
> BerlTerm := proc(p::posint, P::polynom(integer, X),
> i::posint, j::posint)
> RETURN(coeff(Rem(X^(p*(j-1))-X^(j-1), P, X) mod p,
> X, i-1))
> end :
> BerlMatrix1 := matrix(3, 3, (i,j) -> BerlTerm(7, P1, i,j)) ;
```

$$BerlMatrix1 := \begin{bmatrix} 0 & 0 & 1 \\ 0 & 3 & 0 \\ 0 & 6 & 1 \end{bmatrix}$$

- La *dimension du noyau* nous donne la dimension de l'espace des solutions, c'est-à-dire le nombre des facteurs irréductibles. On voit que le rang est 2, l'espace des solutions est donc de dimension 1, ce ne peut être que Z_7, solutions «inévitables», et notre polynôme est donc irréductible. Pour obtenir le rang de cette matrice dans le cas général, il faut utiliser la procédure **Nullspace** combinée avec **mod.**

```
> Nullspace(BerlMatrix1) mod 7 ;
```

$$\{[1,\ 0,\ 0]\}$$

- Vérification.

```
> Irreduc(P1) mod 7 ;
```

true

- Même travail avec P_2.

```
> BerlMatrix2 := matrix(3, 3, (i,j) -> BerlTerm(7, P2, i,j)) ;
```

$$BerlMatrix2 := \begin{bmatrix} 0 & 4 & 0 \\ 0 & 5 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

```
> Nullspace(BerlMatrix2) mod 7 ;
```

$$\{[1,\ 0,\ 0],\ [0,\ 0,\ 1]\}$$

```
> Irreduc(P2) mod 7 ;
```

false

- On voit qu'ici notre équation $V^p - V$ a 49 solutions, $49 = 7^2$, et notre polynôme a donc *deux* facteurs irréductibles. Il reste à les déterminer. Dans un cas si simple, c'est très facile, il suffit de chercher l'élément a de Z_7 nécessairement racine de P_2 et le quotient par $X - a$ donnera l'autre facteur irréductible. Mais on veut expliquer comment il faut procéder dans le cas général. C'est le sujet de la section suivante.

```
> for i from 0 to 6 do
> if Eval(P2, X=i) mod 7 = 0 then print(i) fi
> od ;
```

$$3$$

```
> Quo(P2, X-3, X) mod 7 ;
```

$$X^2 + 4$$

```
> Irreduc(%) mod 7 ;
```

$$true$$

```
> Factor(P2) mod 7 ;
```

$$(X^2 + 4)\,(X + 4)$$

A.3 Trouver les facteurs irréductibles.

- Les solutions de l'équation $V^p - V = 0$ ne donnent pas seulement le *nombre* de facteurs irréductibles, chaque solution donne aussi une décomposition, en général *partielle*, mais toujours *non triviale*, du polynôme proposé en facteurs de degrés plus petits. Ceci est dû au fait que dans Z_p, nous avons la décomposition :

$V^p - V = V\,(V - 1)$
... $(\ V - p - 1)$.

- Dire que V est une solution de $V^p - V$ dans $Z_p[\ X]/\ P$ revient à dire que P divise $V^p - V$, mais la factorisation ci-dessus de $V^p - V$ va justement nous permettre de «découper en tranches» le polynôme P.

- D'abord si P est irréductible, les seules solutions de $V^p - V = 0$ sont les éléments de Z_p, auquel cas le «polynôme» $V^p - V$ est non seulement divisible par P, il est même nul ! et aucune «information» ne peut être obtenue, heureusement.

- Par contre si P est factorisable, on va avoir des solutions différentes. Ces solutions vont être de «vrais» polynômes (non constants), et un tel polynôme V va être de degré forcément $< d = \text{degree}(P)$. On a alors le résultat suivant :

$P = \prod_{i=0}^{p-1} \text{PGCD}(P,\, V - i)$
.

- En effet $V^p - V$ est divisible par P, et donc tout facteur irréductible de P va diviser $V^p - V$ et se retrouver dans l'un des PGCD. Donc P divise le produit. Inversement, comme les $V - i$ sont *premiers deux à deux* (pourquoi ?), le même facteur de P ne peut pas se retrouver deux fois à droite. Compte tenu par ailleurs du fait que $\text{degree}(V - i) < d$, on voit donc qu'on a ainsi, quel que soit V solution «non constante» de $V^p - V = 0$, une factorisation non triviale de P.

- Essayons ce mécanisme avec notre polynôme P_2. Un V non trivial est à trouver dans le noyau de la matrice de Berlekamp :

```
> eval(BerlMatrix2) ;
```

$$\begin{bmatrix} 0 & 4 & 0 \\ 0 & 5 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

```
> Nullspace(BerlMatrix2) mod 7 ;
```

$$\{[1,\ 0,\ 0],\ [0,\ 0,\ 1]\}$$

- Le générateur [1,0,0] du noyau correspond aux solutions triviales de $V^p - V = 0$, mais l'autre, [0,0,1], expression dans notre base du polynôme X^2, est une solution non triviale.

```
> Divide(X^14-X^2, P2) mod 7 ;
```

$$true$$

```
> seq(Gcd(P2, X^2-i) mod 7, i=0..6) ;
```

$$1,\ 1,\ X+4,\ X^2+4,\ 1,\ 1,\ 1$$

- Et on a bien notre décomposition.

```
> evalb(P2 = Expand(mul(gcdi, gcdi=[%])) mod 7) ;
```

$$true$$

- Dans le cas général, il n'y a pas de raison que la décomposition *complète* de P soit ainsi obtenue à l'aide d'une seule solution non triviale V. C'est forcément ce qui arrive si le nombre de facteurs de P est plus grand que p. Construisons P de sorte qu'il ait au moins 8 facteurs.

```
> _seed := 1054 :
> for i from 1 to 8 do
> P||i := rndP(2)
> end do ;
```

$$P1 := X^2 + 4\,X + 2$$
$$P2 := X^2 + 2\,X + 3$$
$$P3 := X^2 + 3\,X + 2$$
$$P4 := X^2 + 2\,X$$
$$P5 := X^2 + 5\,X + 5$$
$$P6 := X^2 + 2\,X + 5$$
$$P7 := X^2 + 6\,X$$
$$P8 := X^2 + 5\,X + 1$$

```
> P := sort(Expand(mul(P||i, i=1..8)) mod 7) ;
```

$$P := X^{16} + X^{15} + 6\,X^{14} + 4\,X^{13} + 3\,X^{12} + 6\,X^{11} + 6\,X^{10} + 5\,X^9 + 3\,X^8 + 3\,X^7 + 5\,X^6 + X^5 + 2\,X^4 + X^3 + 2\,X^2$$

- Mais on peut avoir des facteurs multiples, qu'il faut éliminer pour que notre exemple soit correct.

```
> Gcd(P, diff(P,X) mod 7) mod 7 ;
```

$$X^5 + 6\,X^4 + 4\,X^3 + 5\,X^2 + 5\,X$$

```
> P := Quo(P, %, X) mod 7 ;
```

$$P := X^{11} + 2\,X^{10} + 4\,X^9 + 2\,X^8 + 2\,X^7 + 5\,X^6 + X^5 + X^4 + 4\,X^2 + 6\,X$$

```
> Gcd(P, diff(P,X) mod 7) mod 7 ;
```

$$1$$

- Donc plus de facteurs multiples.

```
> BerlMatrix := matrix(11,11, (i,j) -> BerlTerm(7,P,i,j)) :
> Kernel := Nullspace(%) mod 7 ;
```

$$\begin{aligned}Kernel := \{&[0, 5, 3, 5, 0, 0, 1, 0, 0, 0, 0], [0, 5, 2, 5, 0, 0, 0, 0, 0, 0, 1],\\ &[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0], [0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0],\\ &[0, 3, 0, 1, 0, 0, 0, 0, 0, 1, 0], [0, 1, 0, 3, 0, 1, 0, 0, 0, 0, 0],\\ &[0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0], [0, 4, 6, 4, 1, 0, 0, 0, 0, 0, 0]\}\end{aligned}$$

- Les éléments du noyau sont des *vecteurs*, ce qui est techniquement désagréable pour la suite, on les transforme tous en *listes*.

```
> Kernel := map(convert, Kernel, list) ;
```

$$\begin{aligned}Kernel := \{&[0, 5, 3, 5, 0, 0, 1, 0, 0, 0, 0], [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],\\ &[0, 5, 2, 5, 0, 0, 0, 0, 0, 0, 1], [0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0],\\ &[0, 3, 0, 1, 0, 0, 0, 0, 0, 1, 0], [0, 1, 0, 3, 0, 1, 0, 0, 0, 0, 0],\\ &[0, 4, 6, 4, 1, 0, 0, 0, 0, 0, 0], [0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0]\}\end{aligned}$$

```
> r := nops(Kernel) ;
```

$$r := 8$$

- Donc 8 facteurs irréductibles. On retire l'élément de noyau correspondant aux solutions triviales.

```
> Kernel := Kernel minus {[1, 0$10]} ;
```

$$\begin{aligned}Kernel := \{&[0, 5, 3, 5, 0, 0, 1, 0, 0, 0, 0], [0, 5, 2, 5, 0, 0, 0, 0, 0, 0, 1],\\ &[0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0], [0, 3, 0, 1, 0, 0, 0, 0, 0, 1, 0],\\ &[0, 1, 0, 3, 0, 1, 0, 0, 0, 0, 0], [0, 4, 6, 4, 1, 0, 0, 0, 0, 0, 0],\\ &[0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0]\}\end{aligned}$$

```
> Vvector1 := Kernel[1] ;
```

$$Vvector1 := [0, 5, 3, 5, 0, 0, 1, 0, 0, 0, 0]$$

```
> V1 := sort(add(Vvector1[i]*X^(i-1), i=1..11)) ;
```

$$V1 := X^6 + 5\,X^3 + 3\,X^2 + 5\,X$$

```
> factors1 := {seq(Gcd(V1-i, P) mod 7, i=0..6)} minus{1} ;
```

$$factors1 := \{X^2 + 2\,X + 5,\ X^2 + 5\,X + 5,\ X + 1,\ X^3 + 4\,X^2 + 6,\ X^3 + 4\,X^2 + 2\,X\}$$

```
> nops(factors1) ;
```

$$5$$

```
> evalb(P = Expand(mul(gcdi, gcdi=factors1)) mod 7) ;
```

$$true$$

- On voit qu'une décomposition non triviale de P est bien obtenue, mais ce n'est évidemment pas là la décomposition *complète* en facteurs irréductibles, puisqu'on a construit P comme un produit de facteurs de degré 2. Comme seulement 7 cases sont disponibles dans le résultat, certainement certains facteurs ainsi obtenus sont encore réductibles.

- Le point suivant consiste à dire qu'en essayant au besoin les autres éléments «non triviaux» du noyau de la matrice de Berlekamp, on va réussir, en *recoupant* les résultats, à obtenir la factorisation complète. Expliquons ce qu'il faut entendre par *recouper*.

- Prenons un autre vecteur de notre noyau.

```
> Vvector2 := Kernel[2] ;
```

$$Vvector2 := [0,\ 5,\ 2,\ 5,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1]$$

```
> V2 := sort(add(Vvector2[i]*X^(i-1), i=1..11)) ;
```

$$V2 := X^{10} + 5\,X^3 + 2\,X^2 + 5\,X$$

```
> factors2 := {seq(Gcd(V2-i, P) mod 7, i=0..6)} minus {1} ;
```

$$factors2 := \{X^2 + X,\ X + 2,\ X + 5,\ X^4 + 4\,X^3 + 5\,X^2 + 2\,X + 1,\ X^3 + 4\,X^2 + 2\}$$

```
> nops(factors2) ;
```

5

- On *voit* que la factorisation n'est pas la même que celle précédemment obtenue. On va démontrer juste après que c'est toujours le cas. On obtient donc une «meilleure» factorisation en prenant l'*intersection*, à coups de PGCD, des deux factorisations.

```
> factors12 := {seq(seq(Gcd(f1,f2) mod 7,
> f2 = factors2),
> f1 = factors1)}
> minus {1} ;
```

$$factors12 := \{X^2 + 2\,X + 3,\ X^2 + 2\,X + 5,\ X^2 + 5\,X + 5,\ X,\ X + 1,\ X + 2,\ X + 5,\ X + 6\}$$

```
> nops(factors12) ;
```

8

- La factorisation est donc complète. D'autres fois, il faut encore continuer.

- Expliquons pourquoi la méthode des *recoupements* aboutit. Pour mieux faire comprendre, on se contente du cas $r = 3$. Donc $P = P_1\,P_2\,P_3$ et :

$K\,[X]$ / $P = K\,[X]/\ P_1\ +\ K\,[X]/\ P_2\ +\ K\,[X]/\ P_3$.

- Toute solution de notre équation $V^p - V = 0$ a deux interprétations. Du côté «gauche», c'est un polynôme «modulo P» ; mais du côté droit, comme pour chaque facteur les seules solutions sont les polynômes «constants», ces solutions sont essentiellement des triplets (α_1, α_2, α_3) d'entiers modulo p. La correspondance de la droite vers la gauche n'est rien d'autre que le *théorème des restes chinois.* Le relèvement de (1,0,0) est le produit $B_1\,P_2\,P_3$ de la relation de Bezout $A_1\,P_1 + B_1\,P_2\,P_3 = 1$, car il s'agit d'avoir un polynôme divisible par P_2 et P_3, mais égal à 1 modulo P_1. De la même façon, le relèvement de (0,1,0) (resp. (0,0,1)) est le produit $B_2\,P_1\,P_3$ (resp. $B_3\,P_1\,P_2$) avec des interprétations analogues. Une solution «triviale» est de la forme (α, α, α). Donc une solution non triviale vérifie par exemple $\alpha_1 <> \alpha_2$. Soit V l'interprétation polynôme de cette solution. Alors $V - \alpha_1 = (\alpha_2 - \alpha_1)\,B_2\,P_1\,P_3 + (\alpha_3 - \alpha_1)\,B_3\,P_1\,P_2$, alors que $V - \alpha_2 = (\alpha_1 - \alpha_2)\,B_1\,P_2\,P_3 + (\alpha_3 - \alpha_2)\,B_3\,P_1\,P_2$. Il en résulte que $V - \alpha_1$ est divisible par P_1 et $V - \alpha_2$ est divisible par P_2. Donc le «traitement» de V va forcément «séparer» les facteurs P_1 et P_2. Maintenant l'ensemble des solutions à gauche correspond à l'ensemble des solutions à droite, et il y a donc forcément une solution à gauche correspondant (sans qu'on le «voie») à un cas où $\alpha_1 <> \alpha_2$. Il en est forcément de même pour l'un des vecteurs de la base du noyau, sinon on aurait $\alpha_1 = \alpha_2$ pour *tous* les éléments du noyau, ce qui est exclu. Le même travail peut être fait en général pour toutes les paires d'indices, d'où le fait que les éléments de la base du noyau suffisent à complètement factoriser. CQFD.

- On est prêt maintenant pour une procédure générale de factorisation. Elle va utiliser notre procédure **BerlTerm** déjà construite.

```
> Berl := proc(p::posint, P::polynom(integer, X))
> local d, r, i,
> BerlMatrix, Kernel,
> Vvector, V,
> result, new_factors ;
> d := degree(P, X) ;
> # Erreur si facteur multiple.
> if Gcd(P, diff(P, X)) mod p <> 1 then
> ERROR(`The polynom is not squarefree.`)
> fi ;
> BerlMatrix := matrix(d,d, (i,j) -> BerlTerm(p,P,i,j)) ;
> Kernel := Nullspace(BerlMatrix) mod p ;
> # r = nombre de facteurs irréductibles.
> r := nops(Kernel) ;
> # Si r = 1, le polynôme est irréductible.
> if r = 1 then RETURN([P]) fi ;
> Kernel := map(convert, Kernel, list) ;
> # Suppression de la solution triviale.
> Kernel := Kernel minus {[1, 0$(d-1)]} ;
> # Pour signaler le début de l'algorithme.
> result := {} ;
> # Il faut parcourir les solutions non triviales et # arrêter quand le nombre de facteurs requis est atteint.
> for Vvector in Kernel while nops(result) < r do
> # Expression polynômiale du nouveau vecteur solution considéré.
> V := add(Vvector[i]*X^(i-1), i=1..d) ;
> # Découpage en tranches.
> new_factors := {seq(Gcd(P, V-i) mod p, i=0..(p-1))}
> minus {1} ;
> # Recoupement (éventuel) avec ce qui a été précédemment fait.
> if nops(result) > 1 then
> result := {seq(seq(Gcd(f1,f2) mod p,
> f2 = new_factors),
> f1 = result)}
> minus {1}
> else result := new_factors
> fi
> od ;
> result := convert(result, list) ;
> result := map(sort, result) ;
> result := sort(result,
> (P1,P2)->evalb(degree(P1)<degree(P2))) ;
> RETURN(map(sort,result))
> end :
> fs := Berl(7, P) ;
```

$$fs := [X+6,\ X+5,\ X+2,\ X+1,\ X,\ X^2+5\,X+5,\ X^2+2\,X+5,\ X^2+2\,X+3]$$

```
> nops(fs) ;
```

$$8$$

```
> P - Expand(mul(f, f=fs)) mod 7 ;
```

$$0$$

```
> Berl(73, X^4+1) ;
```

$$[X+51,\ X+10,\ X+63,\ X+22]$$

- Des polynômes complexes peuvent ainsi être factorisés.

```
> _seed := 1535 :
> P := rndP(50) ;
```

$$P := X^{50} + 2\,X^{49} + 5\,X^{48} + 6\,X^{47} + 3\,X^{46} + 2\,X^{45} + X^{43} + X^{42} + 4\,X^{41} + 2\,X^{40} + 5\,X^{39} + 5\,X^{38} + 6\,X^{37} + 3\,X^{36} + 3\,X^{35} + 3\,X^{31} + 4\,X^{29} + 2\,X^{28} + 3\,X^{27} + 4\,X^{26} + 3\,X^{25} + X^{23} + 3\,X^{22} + 6\,X^{20} + X^{19} + X^{18} + 4\,X^{17} + 3\,X^{16} + 5\,X^{15} + 6\,X^{13} + X^{12} + 6\,X^{11} + 3\,X^{10} + 3\,X^9 + 6\,X^8 + X^7 + 3\,X^6 + 5\,X^5 + 3\,X^4 + 2\,X^3 + 5\,X + 6$$

```
> fs := Berl(7, P) :
> map(print, fs) :
```

$$X^2 + 5\,X + 2$$

$$X^{11} + X^{10} + X^9 + 6\,X^7 + 6\,X^6 + 5\,X^5 + 5\,X^4 + 4\,X^3 + 2\,X^2 + 4\,X + 4$$

$$X^{37} + 3\,X^{36} + 3\,X^{34} + 5\,X^{33} + X^{31} + 5\,X^{30} + 5\,X^{28} + 3\,X^{27} + 3\,X^{26} + 5\,X^{25} + 3\,X^{24} + 2\,X^{23} + 3\,X^{22} + 3\,X^{21} + 3\,X^{20} + X^{19} + 6\,X^{17} + 3\,X^{16} + 6\,X^{15} + 6\,X^{14} + 6\,X^{13} + 4\,X^{12} + 3\,X^{10} + 6\,X^9 + X^8 + 6\,X^7 + X^6 + 3\,X^5 + 2\,X^4 + 3\,X^3 + 5\,X + 6$$

```
> nops(fs) ;
```

$$3$$

```
> map(item -> Irreduc(item) mod 7, fs) ;
```

$$[true,\ true,\ true]$$

```
> P - Expand(mul(item, item=fs)) mod 7 ;
```

$$0$$

- Un cas irréductible.

```
> Berl(7, fs[1]) ;
```

$$[X^2 + 5\,X + 2]$$

A.4 Factorisation des polynômes à coefficients entiers.

- Les méthodes efficaces de factorisation des polynômes à coefficients entiers commencent toutes par $\mathbb{Z}_p$-factoriser pour un p premier, ou puissance d'un nombre premier, avec p assez grand. Par examen de la taille des coefficients pour une $\mathbb{Z}$-factorisation éventuelle, on finit par en déduire la $\mathbb{Z}$-factorisation cherchée. Le point clé dans cette direction consiste à majorer les racines (en général complexes) du polynôme à factoriser.

- Soit donc $P = X^n + a_{n-1}\,X^{(n-1)} + ... + a_0$ un polynôme *unitaire* à coefficients complexes. Alors toute racine de P est *strictement* majorée par : $A = 2\max(|a_i|^{\left(\frac{1}{,}n-i,\right)},\ i = 0..n-1)$. En effet on peut écrire $P = X^n\ \left(1 + \left(\sum_{i=1}^{n} \frac{a_{n-i}}{,} X^i,\right)\right)$ où $|a_{n-i}| \leq (\frac{A}{,}2,)^i$. La somme de la dernière expression devient une progression géométrique *strictement* majorée par $\frac{A}{,}2\,X,\ \frac{1}{,}1 - \frac{A}{,}2\,X,,= \frac{A}{,}2\,X - A,\ \leq 1$ si $A \leq |X|$. Donc la dernière inégalité implique P(X) non nul. Le raisonnement est en défaut si $A = 0$, mais ce cas est sans intérêt, car alors toutes les racines sont nulles. Procédure conséquente.

```
> RootsSup := proc(P::polynom(rational, X))
> local dgr ;
> dgr := degree(P, X) ;
> if coeff(P, X, dgr) <> 1 then
> ERROR(sprintf("Polynôme %a non unitaire.", P))
> fi ;
> RETURN(2 * max(seq(evalf(abs(coeff(P, X, i))^(1/(dgr-i))),
> i=0..(dgr-1))))
> end :
```

- Soit donc P un Z-polynôme *unitaire* (il est facile de se ramener à ce cas par «changement de variable») où les coefficients sont majorés par A. Il est élémentaire d'en déduire que les racines (complexes) sont aussi *strictement* majorées en module par $A+1$; il existe des inégalités sensiblement plus fines à ce sujet, mais pour simplifier, on se contentera ici de celle-ci. Puisqu'un facteur potentiel de P est un produit de $(X-\alpha)$ où α parcourt certaines racines de P, on en déduit des majorations pour les coefficients d'une Z-factorisation éventuelle. On peut alors conclure en examinant la Z_p-factorisation de P pour p assez grand.

- Examinons par exemple le cas de X^4+1. Ici $A=2$ mais on sait bien que les quatre racines sont de module 1. Tentons la Z_3-factorisation.

```
> RootsSup(X^4+1) ;
> Berl(3, X^4+1) ;
```

$$2.$$

$$[X^2+2\,X+2,\ X^2+X+2]$$

- Il en résulte qu'une Z-factorisation a au plus deux facteurs de degré 2, où les termes constants sont de la forme $3\,n+2$, mais ce pourrait être -1, et on ne peut conclure. On augmente p.

```
> Berl(5, X^4+1) ;
```

$$[X^2+3,\ X^2+2]$$

- Cette fois on a gagné, parce que l'un des facteurs a un terme constant de la forme $5\,n+2$, incompatible avec les modules connus des racines de X^4+1. Donc X^4+1 est Z-irréductible et donc (voir la démonstration du théorème de Gauss sur la factorialité de $Z[\,X]$) Q-irréductible.

```
> irreduc(X^4+1) ;
```

$$\mathit{true}$$

- Avec un polynôme moins trivial.

```
> _seed := 921 :
> P := rndP(10) ;
> RootsSup(P) ;
```

$$P := X^{10}+2\,X^9+3\,X^8+5\,X^7+2\,X^6+4\,X^5+4\,X^4+2\,X^3+5\,X^2+X+6$$

$$4.$$

- Toute racine est majorée par 4, et si une factorisation non triviale est possible, elle aura un facteur de degré au plus 5 où le coefficient du terme après le terme de plus haut degré sera donc majoré par 20 d'où l'idée d'utiliser 41.

```
> Berl(41,P) ;
```

$$[X^{10} + 2\,X^9 + 3\,X^8 + 5\,X^7 + 2\,X^6 + 4\,X^5 + 4\,X^4 + 2\,X^3 + 5\,X^2 + X + 6]$$

- On est chanceux, le polynôme est donc irréductible.

```
> _seed := 1529 :
> P := rndP(10) ;
> RootsSup(P) ;
```

$$P := X^{10} + 6\,X^9 + 3\,X^8 + 6\,X^7 + X^6 + 6\,X^5 + 2\,X^4 + 2\,X^3 + 5\,X^2 + 2\,X + 3$$

12.

- On essaie un nombre premier $> 10\ .\ 12 = 120$, par exemple 127

```
> Berl(127, P) ;
```

$$[X + 45,\ X + 6,\ X^3 + 86\,X^2 + 108\,X + 28,\ X^5 + 123\,X^4 + 105\,X^3 + 51\,X^2 + 13\,X + 19]$$

- Le facteur $X + 45$ seul ne peut pas provenir d'une Z-factorisation, ni le facteur de degré 3. Dans une telle situation il faut essayer si -6 est racine :

```
> subs(X=-6, P) ;
```

3361563

- Le produit $(X + 6)\,(X + 45)$ va commencer par $X^2 + 51\,X$ et est aussi exclu. Essayons un autre nombre premier, pour voir.

```
> Berl(131, P) ;
```

$$[X^2 + 104\,X + 55,\ X^8 + 33\,X^7 + 53\,X^6 + 15\,X^5 + 111\,X^4 + 82\,X^3 + 41\,X^2 + 5\,X + 112]$$

- Mais le facteur de degré 2 est impossible et le polynôme P est donc Q-irréductible. Vérification.

```
> irreduc(P) ;
```

true

- Il se trouve qu'on aurait pu essayer dans ce cas un entier un peu plus... petit. Ce polynôme est en effet déjà irréductible modulo 5 !

```
> Berl(5,P) ;
```

$$[X^{10} + 6\,X^9 + 3\,X^8 + 6\,X^7 + X^6 + 6\,X^5 + 2\,X^4 + 2\,X^3 + 5\,X^2 + 2\,X + 3]$$

- Un polynôme aléatoire est presque toujours irréductible. Forçons le choix d'un polynôme exercice certainement *réductible*.

```
> _seed := 940 :
> P1, P2 := rndP(4), rndP(6) :
> P := sort(expand(P1 * P2)) ;
```

$$P := X^{10} + 4\,X^9 + 7\,X^8 + 16\,X^7 + 30\,X^6 + 34\,X^5 + 49\,X^4 + 51\,X^3 + 28\,X^2 + 30\,X + 20$$

```
> RootsSup(P) ;
```

8.

```
> nextprime(2*5*8) ;
```

83

```
> Berl(83, P) ;
```

$$[X + 9,\ X + 74,\ X + 68,\ X + 2,\ X + 1,\ X^2 + 37\,X + 64,\ X^3 + 62\,X^2 + 40\,X + 67]$$

- On doit donc examiner si -1 et -2 sont racines.

```
> eval(P, X=-1) ;
```

$$0$$

```
> eval(P, X=-2) ;
```

$$0$$

- Le reste est un peu confus. Divisons et réexaminons la question.

```
> P2 := quo(P, (X+1)*(X+2), X) ;
```

$$P2 := X^8 + X^7 + 2\,X^6 + 8\,X^5 + 2\,X^4 + 12\,X^3 + 9\,X^2 + 10$$

```
> RootsSup(P2) ;
```

$$4.000000000$$

```
> Berl(37, P2) ;
```

$$[X^2 + 2,\ X^6 + X^5 + 6\,X^3 + 2\,X^2 + 5]$$

- Essai.

```
> rem(P2, X^2+2, X) ;
```

$$0$$

- D'où la Q-factorisation définitive. Vérification.

```
> factor(P) ;
```

$$(X + 1)\,(X + 2)\,(X^6 + X^5 + 6\,X^3 + 2\,X^2 + 5)\,(X^2 + 2)$$

- En «bricolant» de la sorte, on arrive en général à factoriser les polynômes pas trop compliqués, mais *programmer* une méthode *générale* est autrement complexe. Il serait confortable de savoir faire la factorisation modulo un *grand* nombre premier, mais la méthode de Berlekamp, telle qu'elle a été programmée précédemment, échoue alors, parce que l'équation de Berlekamp $V^p - V = 0$ devient trop difficile à résoudre, à cause de la taille de p.

```
> # Ne pas effectuer sous Maple 6.
> # Berl(nextprime(10^6), P) ;
```

- Beaucoup d'améliorations peuvent être intégrées à la procédure **Berl**, mais elle n'ira jamais très loin pour une factorisation par rapport à de *grands nombres premiers*. Le corps «fini» Z_p est bien trop grand pour mener les calculs bien loin. Penser en particulier à la factorisation qu'il faut utiliser $V^p - V = V\,(V-1)\,...\,V - p - 1$, où le nombre de facteurs est justement p!! Une autre solution devient alors beaucoup plus intéressante, basée sur le *lemme de Hensel*.

A.5 Lemme de Hensel.

- Le *lemme de Hensel* est une méthode largement utilisée en algèbre commutative consistant à résoudre un problème d'abord «approximativement» modulo un idéal m puis à *affiner* en travaillant modulo les puissances de cet idéal, puissances *de plus en plus petites*. Le problème de la factorisation des polynômes est justement un cadre parfait pour comprendre le mécanisme.

- L'outil essentiel pour démontrer le lemme de Hensel consiste à utiliser judicieusement une relation *à la Bezout* pour exprimer un élément quelconque, et pas seulement 1, en fonction de deux éléments u et v premiers entre eux dans un anneau principal.

- Commençons pour comprendre le principe par le cas entier.
  PROPOSITION A.5.1 *Si u et v sont deux entiers positifs premiers entre eux, alors tout entier x ε [0, uv[s'exprime d'une façon et d'une seule sous la forme :*

$$x = \alpha\, u + \beta\, v \bmod (u\, v)$$

  avec $\alpha \in [0, v[$ et $\beta \in [0, u[$.

  DÉMONSTRATION. Soit $1 = a\, u + b\, v$ une relation de Bezout entre u et v. Par multiplication par x, on obtient $x = x\, a\, u + x\, b\, v$, mais $x\, a$ et $x\, b$ sont en général trop grands ; on les divise donc respectivement par v et u, pour obtenir $x = \alpha\, u + \beta\, v + \gamma\, u\, v$ où on peut choisir α et β dans les intervalles requis. Si un autre choix était possible, on trouverait par différences une relation $\alpha\, u + \beta\, v = 0 \bmod (u\, v)$ avec α non nul et de module $< v$; mais ceci contredit la divisibilité de α par v.

- Programme conséquent.

```
> Bezout2 := proc(x::nonnegint, u::posint, v::posint)
> local a, b, gcd ;
> gcd := igcdex(u, v, 'a', 'b') ;
> if gcd <> 1 then ERROR(
> sprintf("les nombres %a et %a
> ne sont pas premiers entre eux.",
> u, v))
> fi ;
> RETURN(x*a mod v, x*b mod u)
> end :
> Bezout2(4, 6, 15) ;

Error, (in Bezout2) les nombres 6 et 15
            ne sont pas premiers entre eux.

> Bezout2(4, 3, 5) ;
                                        3, 2
> evalb(4 = 3 * 3 + 2 * 5 mod (3*5)) ;
                                        true
```

- Le même résultat est valide pour les polynômes à coefficients dans un corps, sous une forme encore plus confortable.
  PROPOSITION A.5.2 *Si U et V sont deux polynômes de degrés respectifs m et n, premiers entre eux, alors pour tout polynôme P de degré $< m + n$, il existe un unique polynôme A (resp. B) de degré $< n$ (resp. $< m$) tel que $P = A\, U + B\, V$.*

- La démonstration est la même mais un examen de degrés montre qu'on peut même se dispenser de l'imprécision «modulo $U\, V$». Le programme conséquent suit.

```
> Bezout3 := proc(P::polynom(rational, X),
> U::polynom(rational, X),
> V::polynom(rational, X))
> local gcd, A, B ;
> gcd := gcdex(U, V, X, 'A', 'B') ;
> if gcd <> 1 then ERROR(
> sprintf("les polynômes %a et %a
> ne sont pas premiers entre eux.",
> U, V))
> fi ;
> RETURN(rem(P*A, V, X), rem(P*B, U, X))
> end :
> _seed := 1925 :
> P, U, V := rndP(5), rndP(3), rndP(3) ;
```

$$P, U, V := X^5 + 5\,X^4 + 6\,X^3 + 2\,X^2 + 6\,X + 2,\ X^3 + X^2 + X + 6,\ X^3 + 2\,X^2 + 3$$

```
> A, B := Bezout3(P, U, V) ;
```

$$A, B := \frac{1}{6}, -\frac{7}{18}X^2 - \frac{2}{3}X,\ \frac{25}{18}X^2 + \frac{59}{18}X + \frac{1}{3},$$

```
> expand(P - A*U - B*V) ;
```

$$0$$

- Ceci est valable quel que soit le corps, par exemple Z_7, mais il faut adapter la procédure.

```
> `type/Z7` := proc(obj::anything)
> RETURN(type(obj, And(integer, Range(-1, 7))))
> end :
> type(3, Z7), type(-3, Z7) ;
```

$$\mathit{true},\ \mathit{false}$$

```
> Bezout4 := proc(P::polynom(Z7, X),
> U::polynom(Z7, X),
> V::polynom(Z7, X))
> local gcd, A, B ;
> gcd := Gcdex(U, V, X, 'A', 'B') mod 7 ;
> if gcd <> 1 then ERROR(
> ### WARNING: %x or %X format should be %y or %Y if used with
> floating point arguments
> ### WARNING: incomplete string;  use " to end the string
> sprintf("les polynômes %a et %a
> ne sont pas premiers entre eux.",
> U, V))
> fi ;
> RETURN(Rem(P*A, V, X) mod 7, Rem(P*B, U, X) mod 7)
> end :
```

- On prend les mêmes polynômes, mais l'interprétation est différente.

```
> A, B := Bezout4(P, U, V) ;
```

$$A, B := 4\,X + 6,\ X^2 + 6\,X + 5$$

```
> Expand(P - A*U - B*V) mod 7 ;
```

$$0$$

- Un énoncé équivalent est obtenu pour des polynômes à coefficients entiers, à condition de faire intervenir une égalité «modulo p» pour un premier p. Cet énoncé va pouvoir être généralisé au cas p^k où le quotient $Z/\ p^k$ n'est plus un corps.
  PROPOSITION A.5.3 *: soient U et V des polynômes unitaires à coefficients entiers dans [0, p[, p-premiers entre eux, de degrés respectifs m et $n > 0$. Alors pour tout polynôme P de degré $< m+n$, il existe des polynômes uniques A et B , à coefficients entiers dans [0, p[, de degrés respectifs $< n$ et $< m$, et un polynôme R de degré $< m+n$, tels que $P = A\,U + B\,V + p\,R$.*
  Il suffit en effet d'appliquer le résultat précédent, mais quand on finit le calcul, il n'est exact que modulo p. Il n'y a rien à changer à la procédure **Bezout4**, seule la fin de la vérification est différente.

```
> R := expand(P - A*U - B*V) / 7 ;
```

$$R := -X^4 - 3\,X^3 - 3\,X^2 - 6\,X - 7$$

- On énonce maintenant un résultat analogue modulo p^k. Cette fois l'anneau des polynômes à coefficients modulo p^k n'est plus principal, car il n'est même pas intègre. On se place donc dans une situation *où on suppose donnée* une relation de Bezout entre U et V.
  PROPOSITION A.5.4 *Soient U et V deux polynômes unitaires à coefficients entiers dans [0, p^k[, de degrés respectifs m et n. On suppose donnée une relation de Bezout : $1 = A\,U + B\,V + p^k\,C$ où le degré de A (resp. B, C) est $< n$ (resp. $< m$, $< m+n$). Alors, pour tout polynôme P à coefficients entiers de degré $< m+n$, il existe des polynômes uniques E (resp. F, G), de degré $< n$ (resp. $< m$, $< m+n$), à coefficients entiers dans [0, p^k[, (resp. dans [0, p^k[, entiers), tels que $P = E\,U + F\,V + p^k\,G$.*
  DÉMONSTRATION. Analogue avec les adaptations évidentes. Prendre $E = P\,A$ et $F = P\,B$ est tentant, mais les degrés sont trop grands. Comme V est unitaire, on peut diviser $P\,A$ par V pour obtenir un reste à coefficients entiers E qu'on réduit modulo p^k : $P\,A = Q\,V + E + p^k\,R$, et de même on divise $P\,B$ par U pour obtenir $P\,B = S\,U + F + p^k\,T$. En reportant dans $P = P\,A\,U + P\,B\,V + p^k\,P\,C$, il vient $P = E\,U + F\,V + (Q+S)\,U\,V + p^k\,(P\,C + R\,U + T\,V)$. La réduction modulo p^k de tous les termes laisse un polynôme $U\,V$ *unitaire* de degré $m+n$. Comme $P - E\,U - F\,V$ est de degré $< m+n$, il en résulte que le polynôme $Q+S$ est nul modulo p^k ; on peut donc «glisser» le terme $(Q+S)\,U\,V$ dans le facteur de p^k et finalement le degré résultant est nécessairement $< m+n$. Si on avait deux solutions différentes, on déduirait une relation $E\,U + F\,V = p^k\,R$; en multipliant par A, il vient $E\,A\,U + F\,A\,V = p^k\,A\,R$ ou, compte tenu de la relation presque-Bezout, $E - E\,B\,V + F\,A\,V = p^k\,(A\,R + E\,C)$. Mais si on réduit modulo p^k, E devient divisible par V, ce qui est incompatible avec V *unitaire* et degré de $E <$ degré de V , à moins que E soit nul. CQFD.

```
> Bezout5 := proc
> (p::posint, k::posint, P::polynom(integer, X),
> U::polynom(integer, X), V::polynom(integer, X),
> A::polynom(integer, X), B::polynom(integer, X))
> RETURN(Rem(P*A, V, X) mod p^k, Rem(P*B, U, X) mod p^k)
> end :
```

- On redéfinit **rndP** pour que l'entier modulaire soit libre.

```
> rndP := proc(p::posint, d::posint)
> local rnd ;
> rnd := rand(0..(p-1)) ;
> RETURN(sort(X^d + add(rnd()*X^i, i=0..(d-1))))
> end :
> _seed := 2210 :
> p, k := 7,2 ; U,V := seq(rndP(49,3), i=1..2) ;
```

$$p,\ k := 7,\ 2$$

$$U, V := X^3 + 43\,X^2 + 28\,X + 48,\ X^3 + 18\,X^2 + 12\,X + 24$$

```
> Gcdex(U, V, X, 'A', 'B') mod 49 ;
```

$$1$$

```
> sort(expand(1-A*U-B*V)/49) ;
```

$$-X^5 - 38\,X^4 - 63\,X^3 - 85\,X^2 - 56\,X - 23$$

```
> P := rndP(49, 5) ;
```

$$P := X^5 + 22\,X^4 + 26\,X^3 + 11\,X^2 + 39\,X + 4$$

```
> E, F := Bezout5(7, 2, P, U, V, A, B) ;
```

$$E, F := 43\,X^2 + 22\,X + 19,\ 7\,X^2 + 34\,X + 3$$

```
> expand(P-E*U-F*V)/49 ;
```

$$-X^5 - 41\,X^4 - 58\,X^3 - 84\,X^2 - 49\,X - 20$$

- Nous pouvons maintenant énoncer le *lemme de Hensel* pour les polynômes modulo une puissance de nombre premier.
  PROPOSITION A.5.5 (lemme de Hensel) *: On suppose qu'on dispose de deux relations :*

$$P = U\,V + p^k\,R;\quad 1 = A\,U + B\,V + p^k\,S;$$

où les degrés de U (resp. V, P, R, A, B, S) sont m (resp. n, $m+n$, $< m+n$, $< n$, $< m$, $< m+n$). Par ailleurs P, U et V sont supposés unitaires, et les coefficients de A, U, B et V sont des entiers dans $[0, p^k[$. Alors il existe U_0, V_0, R_0, A_0, U_0, B_0, V_0 et S_0 vérifiant les mêmes conditions à ceci près que p^k doit être remplacé par $p^{(2\,k)}$. De plus U_0, V_0, A_0 et B_0 sont uniques. Il en résulte la même propriété pour R_0 et S_0.

  DÉMONSTRATION. On pose $U_0 = U + p^k\,U_1$ et de même pour V, A et B. En reportant dans les équations à satisfaire et en réduisant modulo $p^{(2\,k)}$, il vient les équations suivantes.
$R = (V_1\,U + U_1\,V) \bmod p^k$
;
$S - A\,U_1 - B\,V_1 = (A_1\,U + B_1\,V) \bmod p^k$
. On va donc trouver les correctifs d'indice 1 par application de **Bezout5**. CQFD.

```
> Hensel := proc
> (p::posint, k::posint, P::polynom(integer, X),
> U::polynom(integer, X), V::polynom(integer, X),
> A::polynom(integer, X), B::polynom(integer, X))
> local R, S, U1, V1, A1, B1 ;
> R := expand(P - U*V)/p^k ;
> S := expand(1 - A*U - B*V)/p^k ;
> if not type(R, polynom(integer, X)) then
> ERROR("P, U, V not coherent for Hensel.")
> fi ;
> if not type(S, polynom(integer, X)) then
> ERROR("A, U, B, V not coherent for Hensel.")
> fi ;
> V1, U1 := Bezout5(p, k, R, U, V, A, B) ;
> A1, B1 := Bezout5(p, k, S-A*U1-B*V1, U, V, A, B) ;
> RETURN(p, 2*k, P, sort(U+p^k*U1), sort(V+p^k*V1),
> sort(A+p^k*A1), sort(B+p^k*B1))
> end :
```

- On a maintenant l'outil ad hoc pour augmenter très vite l'entier modulaire par rapport auquel on effectue une factorisation de polynômes à coefficients entiers. On trouve ainsi assez vite une factorisation éventuelle pour un polynôme à coefficients entiers, ou au contraire son irréductibilité.

```
> _seed := 1713 ;
> P := rndP(10, 10) ;
> RootsSup(P) ;
```

$$\_seed := 1713$$

$$P := X^{10} + 4\,X^9 + 8\,X^8 + 2\,X^7 + 9\,X^6 + 3\,X^5 + 4\,X^4 + X^3 + 9\,X^2 + 5$$

$$8.$$

```
> fs := Berl(11, P) ;
```

$$fs := [X^2 + 4\,X + 2,\ X^8 + 6\,X^6 + 8\,X^4 + 4\,X^3 + 5\,X^2 + 6\,X + 8]$$

- Deux facteurs, c'est la situation idéale pour Hensel. Il faut préparer les données.

```
> U, V := op(fs) ;
```

$$U, V := X^2 + 4\,X + 2,\ X^8 + 6\,X^6 + 8\,X^4 + 4\,X^3 + 5\,X^2 + 6\,X + 8$$

```
> Gcdex(U, V, X, 'A', 'B') mod 11 ;
```

$$1$$

```
> p,k,P,U,V,A,B := Hensel(11,1,P,U,V,A,B) : U ; V ;
```

$$X^2 + 92\,X + 68$$

$$X^8 + 33\,X^7 + 50\,X^6 + 55\,X^5 + 19\,X^4 + 81\,X^3 + 93\,X^2 + 94\,X + 41$$

- Le facteur de degré 2 n'est pas possible, car il devrait être $X^2 - 29\,X + ...$ mais ceci est incompatible avec la majoration par 8 des racines. Vérification.

```
> irreduc(P) ;
```

$$true$$

- Considérons comme plus haut un cas certainement factorisable.

```
> _seed := 16 :
> P := sort(expand(rndP(5,4)*rndP(5,6))) ;
> RootsSup(P) ;
```

$$P := X^{10} + 2\,X^8 + 4\,X^7 + 2\,X^6 + 12\,X^5 + 4\,X^4 + 16\,X^3 + 8\,X^2 + 8\,X + 8$$

$$3.287503660$$

```
> fs := Berl(11, P) ;
```

$$fs := [X + 4,\ X^4 + 2\,X^2 + 2,\ X^5 + 7\,X^4 + 5\,X^3 + 6\,X^2 + 9\,X + 1]$$

- Une racine est majorée par 3.3 et $X + 4$ ne peut pas venir d'un Z-facteur. Regroupons les deux premiers facteurs.

```
> U := Expand(fs[1]*fs[2]) mod 11 ; V := fs[3] ;
```

$$U := X^5 + 2\,X^3 + 2\,X + 4\,X^4 + 8\,X^2 + 8$$

$$V := X^5 + 7\,X^4 + 5\,X^3 + 6\,X^2 + 9\,X + 1$$

```
> Gcdex(U, V, X, 'A', 'B') mod 11;
```

$$1$$

```
> p,k,P,U,V,A,B := Hensel(11,1,P,U,V,A,B) : U ; V ;
```

$$X^5 + 70\,X^4 + 2\,X^3 + 19\,X^2 + 2\,X + 19$$
$$X^5 + 51\,X^4 + 60\,X^3 + 39\,X^2 + 53\,X + 45$$

- Mais les coefficients de X^4 sont impossibles. On essaie l'autre combinaison.

```
> U := Expand(fs[1]*fs[3]) mod 11 ; V := fs[2] ;
```

$$U := X^6 + 4\,X^3 + 4\,X + 4$$
$$V := X^4 + 2\,X^2 + 2$$

```
> Gcdex(U, V, X, 'A', 'B') mod 11;
```

$$1$$

```
> p,k,P,U,V,A,B := Hensel(11,1,P,U,V,A,B) : U ; V ;
```

$$X^6 + 4\,X^3 + 4\,X + 4$$
$$X^4 + 2\,X^2 + 2$$

- Cette fois les facteurs potentiels restent curieusement constants. Continuons.

```
> p,k,P,U,V,A,B := Hensel(11,2,P,U,V,A,B) : U ; V ;
```

$$X^6 + 4\,X^3 + 4\,X + 4$$
$$X^4 + 2\,X^2 + 2$$

```
> p,k,P,U,V,A,B := Hensel(11,4,P,U,V,A,B) : U ; V ;
```

$$X^6 + 4\,X^3 + 4\,X + 4$$
$$X^4 + 2\,X^2 + 2$$

- Cette fois il s'agit d'une factorisation certaine modulo :

```
> 11^8 ;
```

$$214358881$$

- On est donc certain d'avoir une vraie factorisation entière, qu'on aurait pu essayer plus vite. Vérification.

```
> factor(P) ;
```

$$(X^4 + 2\,X^2 + 2)\,(X^6 + 4\,X^3 + 4\,X + 4)$$

- Jouons à trouver ainsi des factorisations élevées de $X^4 + 1$;

```
> P := X^4+1 ;
```

$$P := X^4 + 1$$

```
> Berl(3, P) ;
```

$$[X^2 + 2\,X + 2,\ X^2 + X + 2]$$

```
> U,V := op(%) ;
> Gcdex(U,V,X,'A','B') mod 3 ;
> p,k := 3, 1 ;
```

$$U,\,V := X^2 + 2\,X + 2,\ X^2 + X + 2$$
$$1$$

$$p,\ k := 3,\ 1$$

```
> for i from 1 to 6 do
> p,k,P,U,V,A,B := Hensel(p,k,P,U,V,A,B)
> od :
> k, p^k ; U ; V ;
```

$$64,\ 343368382029251248465784908928 1$$

$$X^2 + 135295558823394433955461041579 2\,X + 343368382029251248465784908928 0$$

$$X^2 + 208072823205856814510323867348 9\,X + 343368382029251248465784908928 0$$

Références

Livres de base :

[Artin] Emil Artin, *Galois Theory*, Notre Dame Mathematical Lectures, Ed. Notre Dame, Indiana, 1942

[Bosch] Siegfried Bosch, *Algebra*, 3rd Ed., 1999

[La] Serge Lang , *Algebra.* Reading, Mass. : Addison–Wesley, 3rd Ed., 1993.

[Se70] J.– P. Serre, *Cours d'arithmétique.* Paris, Press Univ. France, 1970.

[VdW71] B.L. van der Waerden, *Algebra I,II*, New York : Springer Verlag, 1971, 1967.

Livres supplémentaires :

[Ayad] M. Ayad, *Théorie de Galois*, Niveau I, Niveau II, Paris : Ellipses, 1993.

[BS85] Z.I. Borevich, I.R.Shafarevich, *Number Theory.* Traduction anglaise. : New York/London : Academic Press, 1966.

[Li-Ni] Rudolf Lidl et Harald Niederreiter, *Introduction to finite fields and their applications.* Addison–Wesley : Reading, 1983

[He97] Yves Hellegouarch, Invitation aux mathématiques de Fermat-Wiles. Enseignement des Mathématiques. Paris : Masson. vii, 397 p. (1997)

[Ma-Pa] Yu.I. Manin et A.A.Panchishkin, *Introduction to Modern Number Theory*, Encyclopaedia of Mathematical Sciences, vol. 49 (2nd ed.), Springer-Verlag, 2005, 514 p.

[Se63] Serre, J.– P. (1963) : Corps locaux. Paris, Hermann, 1963.

[Se64] J.– P. Serre(1964) : Cohomologie galoisienne. Berlin e.a. : Springer – Verlag, 1964.

[Wei74] A.Weil (1974) : Basic Number Theory. 3rd ed. Berlin–Heidelberg–New York : Springer–Verlag, 1974.